SVENSKA KRAFTNÄT

2013-12-19 Dnr: 2012/331

Hotkatalog för Elbranschen

Hot mot IT-, informationshantering, processkontroll och automation

Version 1.0

SVENSKA KRAFTNÄT

BOX 1200
172 24 SUNDBYBERG
STUREGATAN 1

WWW.SVK.SE
REGISTRATOR@SVK.SE

TEL 08 475 80 00
FAX 08 475 89 50

1 Förord

En väl fungerande elförsörjning är en nödvändig förutsättning för ett fungerande samhälle. Företag verksamma inom elförsörjningen utsätts varje dag för olika slags angrepp, bl. a. i form av inbrott, skadegörelse eller IT-angrepp.

Hot inom IT är ett område som måste ägnas särskild uppmärksamhet då i dagsläget i stort sett all informationshantering sker med stöd av IT.

Under 2013 har Svenska Kraftnät gett ut nya föreskrifter och allmänna råd om säkerhetsskydd, SvKFS 2013:1.

En arbetsgrupp vid Svenska Kraftnät har tillsammans med representanter från Svensk Energi med arbetat med att ta fram denna hotkatalog. Hotkatalogen syftar till att hjälpa alla företag verksamma inom elförsörjningen i sitt säkerhetsarbete allmänhet och det som rör nämnda föreskrifter i synnerhet. I arbetet har särskild vikt lagts på att belysa IT-relaterade hot och risker.

Syftet med hotkatalogen är att utgöra referensmaterial för personer inom elbranschen som arbetar med säkerhetsfrågor. Målet med hotkatalogen är att den ska kunna utgöra källmaterial och inspiration i säkerhetsarbete i allmänhet och i samband med riskanalyser i synnerhet.

Denna hotkatalog är ett levande dokument som löpande underhålls och förvaltas. Detta gör att det kan saknas hot men som läggs till allteftersom texten uppdateras. Saknar du hotexempel, kontakta oss gärna med förslag på tillägg eller ändringar.

Hotkatalogen används med fördel tillsammans med andra dokument, främst vägledning för IS/IT-säkerhet och säkerhetsskydd samt Svenska Kraftnäts föreskrifter.

Vi vill tacka alla som deltagit i arbetsgruppen, referensgruppen och övriga som lämnat värdefulla bidrag för att vägledningen ska bli ett användbart hjälpmedel i säkerhetsarbetet

2 Innehåll

3 Ingress och beskrivning

Detta dokument är en katalog över olika säkerhetsproblem som existerar idag. Katalogen sammanställer vanliga hot som förekommer i det moderna samhället i allmänhet och mot aktörer inom elsektorn i synnerhet. Sammanställning av olika hot berör främst sådant som är relevanta i sammanhang där informationsteknik samt processkontroll och automation förekommer. Hoten är strukturerade enligt en bred och enkel kategorisering.

Texten är tänkt att utgöra en startpunkt, och kunskapsmässig grund, för att göra det möjligt att bättre genomföra inventeringar och analyser över såväl allmänna men också aktuella hot. Med hjälp av en strukturerad katalog över olika hot så kan aktörer inom El- och energibranschen i Sverige lättare förstå vilka hot, och därmed risker, som finns inom den egna verksamheten eller i branschen.

Tanken med dokumentet är att det skall kunna fungera som ett *källmaterial*, *inspirationskälla, exempelsamling* eller *checklista* vid exempelvis risk- och sårbarhetsanalyser, framställande av attackträd eller annat metodiskt säkerhetsarbete. Genom att samla *exempel* och *typfall* så kan

- en analysledare vid ett riskanalysseminarium ha en bra startpunkt
- deltagare i en riskanalys kan ha detta som källa och exempel när de skall vara kreativa och komma på hot mot det som riskanalysen omfattar
- en projektledare sätta sig in i hot och säkerhetsproblem som finns inom ett område
- en processingenjör vill skapa sig en bättre förståelse för vilka hot automation och införande av IT-teknik kan innebära
- olika ämnesexperter kan fördjupa sig i hot och risker inom de områden som de är experter
- beslutsfattare ha underlag som rör hot när de måste fatta olika typer av beslut
- en person som arbetar med att upprätta eller underhålla ett riskregister som en del av organisationens övergripande riskarbete kunna stämma av vanliga hot inom områdena informationssäkerhet, IT-säkerhet och säkerhetsskydd.

Andra användningsområden är för en säkerhetsansvarig att på ett systematiskt sätt kunna gå igenom katalogen och se hur olika hot förhåller sig mot de standarder, främst ISO/IEC 27002 och ISO/IEC 27019, och de där angivna kraven. På så sätt går det att använda texten som ett uppslagsverk där man strukturerat kan se ifall den egna organisationen har skydd mot hoten och hur kraven i standarden säger att de skall hanteras.

Dokumentet skall helt enkelt ge *exempel på olika typer av vanliga hot* som förekommer i allmänhet vad det gäller informationshantering. Ofta är hot riktade mot informationshantering exempelvis i informationssystem, men hot finns även mot manuell hantering av information.

Denna hotkatalog används med fördel tillsammans med den vägledning om informationssäkerhet för den svenska elbranschen som Svenska Kraftnät har gett ut. Där beskrivs riskanalysmetoder, säkerhetsanalys, hotbilder med mera mer ingående än detta dokument, som mer är en encyklopedi över olika typer av hot.

I texten görs ingen sannolikhetsbedömning eller konsekvensbedömning av de olika hoten, då detta kan vara specifikt för varje organisation och att sannolikheten för att ett hot realiseras kan ändras över tid beroende på olika förutsättningar.

Ett annat sätt att läsa dokumentet är att som säkerhetsansvarig gå igenom det från början till slut och ha det som en checklista, för att kontrollera att alla relevanta hot som listas täcks in av de skyddsåtgärder som den egna organisationen har på plats.

Det går att argumentera att publicering och offentliggörande av beskrivningar av hot är *ett hot i sig*. Det är därför viktigt att poängtera att de hot som beskrivs i denna text redan allmänt kända, finns beskrivna i böcker, finns att bevittna på filmer som ligger på Internet, eller finns tillgängliga på annat sätt. Således torde nyttan i att lätt hitta en sammanställning av dessa hot för elbranschen i allmänhet och för de som arbetar med säkerhetsfrågor i synnerhet, vara övervägande.

Det skall för tydlighetens skull nämnas att de exempel på händelser och konsekvenser som ges i hotkatalogen är fiktiva, men visar på visar på möjliga händelser och möjliga konsekvenser som kan drabba ett elföretag.

3.1 Dokumentets struktur och uppbyggnad

Hotkatalogen är en sammanställning över flera olika typer av hot som kan påverka den egna verksamheten. I de flesta fall beskrivs hot på detaljnivå, men i några fall så beskrivs hoten mer generellt, och då får läsaren själv göra egna tolkningar för de specialfall och varianter av hotet som kan vara aktuellt i dennes situation och med dem förutsättningar som denne har.

Varje hot är beskrivet i form av ett översiktligt ***hotkort***. Detta kort ger en inledande beskrivning av hotet. Därefter följer en kategorimarkering av hotet och därefter ett stycke som beskriver orsak eller aktör som ligger bakom hotet. Hotkortet innehåller också exempel på händelser där hotet sätts i ett sammanhang samt exempel på konsekvenser av att hotet realiseras. Det finns korsreferenser mellan olika hot samt externa referenser, ofta till relevanta kapitel och stycken i standarder som SS-ISO/IEC 27002:2005 och 27019:2013, vilket är anpassningar och utökningar av 27002 för elbranschen.

Hotkatalogen har också en egen ordlista som beskriver flera av de vanligast förekommande facktermerna som används i texten. Denna ordlista finns i slutet på dokumentet.

Mot slutet av dokumentet finns det även ett alfabetiskt sakregister i vilket man kan slå upp eller söka efter olika hot och termer för att se var någonstans i dokumentet detta hot avhandlas.

Sist i dokumentet finns en lista på referenser som kan användas för fördjupning. För den läsare som är intresserad av en fördjupning av området hot och vill ha mer exempel på hot, så rekommenderas bilaga C till SS-ISO/IEC 27005 samt den tyska myndighetens BSI:s hotkatalog. Det finns en engelskspråkig förkortad variant, som fortfarande är omfattande. För den som förstår tyska finns en närmast gigantisk hotkatalog i BSI:s material om grundskydd för IT-system.

Dokumentet är av allmän natur och borde därför kunna existera under lång tid utan att åldras eller bli inaktuellt. Det skall dock tilläggas att vissa hot som vi inte identifierat under detta arbete kommer identifieras av andra, att nya hot under tidens lopp kommer att tillkomma, men även att vissa varianter av de befintliga hot kommer att uppstå. Det är tänkt att materialet skall uppdateras och underhållas så att dessa nya varianter kommer att kunna ingå i nya utgåvor.

3.2 Grundläggande definitioner

Följande termer förekommer i texten eller är basala för att förståelsen av innehållet i denna text. Förutom dessa grundläggande definitioner som närmare beskriver ord som är av vikt för att förstå texten i sin helhet så finns det en ordlista på sid 347 som beskriver allmänna termer om IT- och informationssäkerhet som förekommer i texten.

I texten förekommer orden SCADA och ICS för att beskriva industriella kontrollsystem. Ordet SCADA kommer ifrån förkortningen *Supervisory Control And Data Aquisition* , vilket är en specifik typ av industriellt kontrollsystem, ofta ett överliggande kontrollsystem som geografiskt distribuerat över stora områden. Förkortningen SCADA har dock i många fall, såsom i detta dokument, fått en mer allmängiltig betydelse, att betyda industriella kontrollsystem i allmänhet. ICS är en också en engelskspråkig förkortning som betyder Industrial Control System, Industriella Kontrollsystem, en på samma sätt som SCADA vedertagen allmänbenämning på denna typ av system.

Nedanstående definitioner är baserade på den terminologi som lagts fast i *SIS Handbok 550, utgåva 3 – Terminologi för informationssäkerhet*.

Med ***hot*** menas i denna text

> *En möjlig, oönskad händelse med negativa konsekvenser för verksamheten*

Med ***hotbild*** menas i denna text

> *En uppsättning hot som bedöms föreligga mot en viss del av verksamheten*

Med ***hotbedömning*** menas i denna text

> *En bedömning gjord av det eller de hot som föreligger*

Med ***sårbarhet*** menas i denna text

> *svaghet gällande en tillgång eller grupp av tillgångar, vilken kan utnyttjas av ett eller flera hot*

Med ***risk*** menas i denna text

> *Kombination av sannolikheten för att ett givet hot realiseras och därmed uppkommande skadekostnad*

Kostnad i detta sammanhang innebär inte alltid monetära kostnader, utan kan exempelvis också vara skada mot hälsa, liv och miljö.

Med ***riskanalys*** menas i denna text

> *Process som identifierar hot mot verksamheten och uppskattar storleken hos relaterade risker*

Med ***riskhantering*** menas i denna text

> *Samordnade aktiviteter för identifiering, styrning och kontroll av risk*

Med ***sannolikhet*** menas i denna text

> *Ett mått på hur troligt det är att en viss händelse inträffar*

Med ***konsekvens*** menas i denna text

> *Resultat av en händelse med negativ inverkan*

*Med **administrativa hot** avses*

> *Hot av administrativ natur eller som negativt påverkar administration*

Administration innefattar administrativa processer, procedurer, rutiner, aktiviteter inom en organisation.

Med ***fysiska hot*** avses

> *Hot som kan påverka, eller resultera i konsekvenser, saker i den fysisk världen*

Fysisk avser här även att hoten kommer från fysiska händelser eller att de är riktade mot fysiska saker.

Med ***logiska hot*** avses

> *Hot som kan påverka, eller resultera i konsekvenser, saker i den logiska, digitala världen*

Logisk avser här att hoten kan komma från digitala händelser, exempelvis användandet av ett datorprogram för att utföra ett angrepp, eller för där konsekvenserna uppstår i den digitala värden.

*Med **organisatoriska hot** avses*

> *Hot av organisatorisk natur eller som negativt påverkar organisationen*

Organisation i detta fall betyder ofta *roller*, *ansvar och mandat* inom organsationen.

Med ***tekniska hot*** avses hot som

> *Är av teknisk natur eller som negativt kan påverka teknik, tekniska lösningar och tekniska system.*

Tekniska hot kan vara IT-teknik, men även andra typer av tekniska system, exempelvis processkontrollutrustning, maskiner, eltekniksystem med mera.

Det skall påpekas att det ibland finns beroenden mellan de olika typerna av hot, t.ex. att ett logiskt hot kan få fysiska konsekvenser och vice versa, t.ex. påverkan på elsystemets drift. Dålig administrativa rutiner kan leda till skador i den digitala världen, med mera.

4 Administrativa och organisatoriska hot

*Definition: Med **administrativa** hot avses*

Hot av administrativ natur eller som negativt påverkar administration

*Definition: Med **organisatoriska** hot avses*

Hot av organisatorisk natur eller som negativt påverkar organisationen

Innehållsförteckning kapitlet *administrativa och organisatoriska hot*

4.1 Säkerhetsskydd

Med säkerhetsskydd avses i Sverige skydd mot *spionerі*, *sabotage* och *andra brott som kan hota rikets säkerhet*. Säkerhetsskydd ska även *skydda uppgifter som omfattas av sekretess* enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet. Vidare omfattar Säkerhetsskydd även *skydd mot terroristbrott, även om sådana brott inte hotar rikets säkerhet*.

4.1.1 Ej utförd säkerhetsprövning

Beskrivning
En så kallad säkerhetsprövning skall göras innan en person deltar i verksamhet som har betydelse för rikets säkerhet eller är viktig till skydd mot terrorism. Säkerhetsprövningens är avsedd att klarlägga om personen i fråga är lämplig, det vill säga lojal och pålitlig ur säkerhetssynpunkt.

Det är enklare att utföra säkerhetsprövning av svenska personer som är anställda i Sverige än exempelvis utländska medborgare som är anställda i ett annat land, men som är tänkta att utföra ett arbete hos ett svenskt företag.

Kategori
Administrativt hot

Orsak/Aktör
Inkompetens, avsaknad av erfarenhet, slarv, avsaknad av rutiner, felaktiga processer

Exempel
- Ej utförd säkerhetsprövning av personal i samband med nyrekrytering
- Ej utförd säkerhetsprövning av personal från ett företag baserat i Sverige
- Ej utförd säkerhetsprövning av personal från ett företag baserat i Europa
- Ej utförd säkerhetsprövning av personal från ett företag baserat utom Europa

Se också
4.1.2

Referenser
SS-ISO/IEC 27002:2005 kap 8.1.2 ”Kontroll av personal”
ISO/IEC 27019:2013 kap 8.1.2 ”Screening”
Svenska Kraftnäts Föreskrifter, SvKFS 2013:1
Säkerhetsskyddslag (1996:627)
Säkerhetsskyddsförordningen (1996:633)

4.1.2 Ej utförd säkerhetsskyddad upphandling

Beskrivning
Bolaget har inte genomfört en säkerhetsskyddad upphandling, vilket de enligt tillsynsmyndighetens föreskrifter är skyldiga att genomföra, för de arbeten som faller under säkerhetsskyddslagens krav.

Kategori
Administrativt hot

Orsak/Aktör
Inkompetens, slarv, avsaknad av rutiner, felaktiga upphandlingsrutiner

Exempel
- Inköp av utrustning som skall installeras i anläggning. Utrustningen måste installerad av leverantörens personal
- Underhåll av maskiner eller utrustning i anläggning. Underhållet utförs av tredjepartspersonal
- Utveckling av programvara och system som skall användas och hantera information som anses som känslig och behöver skyddas enligt säkerhetsskyddslagen.

Se också
4.1.1, 4.1.3

Referenser
SS-ISO/IEC 27002:2005 kap 8.1.2 ”Kontroll av personal”
ISO/IEC 27019:2013 kap 8.1.2 ”Screening”
Svenska Kraftnäts Föreskrifter, SvKFS 2013:1
Säkerhetsskyddslag (1996:627)
Säkerhetsskyddsförordningen (1996:633)

4.1.3 Felaktigt utförd säkerhetsskyddad upphandling

Beskrivning
Bolaget har genomfört en säkerhetsskyddad upphandling, vilket de enligt tillsynsmyndighetens föreskrifter är skyldiga att genomföra, för de arbeten som faller under säkerhetsskyddslagens krav.

Kategori
Administrativt hot

Orsak/Aktör
Inkompetens, slarv, avsaknad av rutiner, felaktiga upphandlingsrutiner

Exempel
- All personal som skall med i uppdraget är inte omfattade av förfrågningsunderlag eller enkäter som skickats ut, så underlag för registerkontroll är inte komplett
- Alla bolag som skall med i uppdraget är inte omfattade av förfrågningsunderlag eller enkäter som skickats ut, så underlag för registerkontroll är inte komplett

Se också
4.1.1, 4.1.3

Referenser
SS-ISO/IEC 27002:2005 kap 8.1.2 ”Kontroll av personal”
ISO/IEC 27019:2013 kap 8.1.2 ”Screening”
Svenska Kraftnäts Föreskrifter, SvKFS 2013:1
Säkerhetsskyddslag (1996:627)
Säkerhetsskyddsförordningen (1996:633)

4.1.4 Ej utförd säkerhetsanalys(enl. 5 § säkerhetsskyddsförordningen)

Beskrivning
De organisationer som omfattas av säkerhetsskyddslagstiftningen är enligt lag skyldiga att undersöka vilka uppgifter i verksamheten som ska hållas hemliga med hänsyn till rikets säkerhet. Organisationerna ska också undersöka vilka anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller till skydd mot terrorism. Denna formella typ av undersökning kallas säkerhetsanalys och resultatet av undersökningen måste dokumenteras.

Bolaget har inte genomfört någon säkerhetsanalys vilket de enligt tillsynsmyndighetens föreskrifter är skyldiga att genomföra minst vartannat år, eller vid behov.

Kategori
Administrativt hot

Orsak/Aktör
Inkompetens, slarv, avsaknad av rutiner, felaktiga processer

Exempel
Skyldigheten att genomföra nämnda analys kan vara okänd för den eller de i bolaget som formellt sett har uppgiften att genomföra och dokumentera den. Detta kan bero på okunskap om hur föreskrifterna gäller för bolag eller otillräcklig säkerhetsutbildning i allmänhet.

Exempel på potentiella konsekvenser
- Det går inte att utesluta att man i säkerhetsanalys skulle komma fram till att bolaget hanterar uppgifter eller anläggningar som rör rikets säkerhet. Således kan utebliven säkerhetsanalys medföra felaktig hantering av sådana uppgifter. Vidare kan det föranleda att anläggningar har en otillräcklig skyddsnivå.

- Avsaknad av säkerhetsanalys innebär ett brott mot rättsliga krav i säkerhetsskyddslagstiftningen.

Se också
4.1.5

Referenser
Svenska Kraftnäts Föreskrifter, SvKFS 2013:1
Säkerhetsskyddslag (1996:627)
Säkerhetsskyddsförordningen (1996:633)

4.1.5 Felaktig säkerhetsanalys(enl. 5 § säkerhetsskyddsförordningen)

Beskrivning
De organisationer som omfattas av säkerhetsskyddslagstiftningen är enligt lag skyldiga att undersöka vilka uppgifter i verksamheten som ska hållas hemliga med hänsyn till rikets säkerhet. Organisationerna ska också undersöka vilka anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller till skydd mot terrorism. Denna formella typ av undersökning kallas säkerhetsanalys och resultatet av undersökningen måste dokumenteras.

Bolaget har genomfört en säkerhetsanalys enligt tillsynsmyndighetens, men denna är på ett eller annat sätt felaktig – den är inte korrekt gjord, den saknar väsentliga delar av de objekt eller analyser som borde ingått, de som har utfört den har dragit felaktiga slutsatser.

Kategori
Administrativt hot

Orsak/Aktör
Inkompetens, slarv, avsaknad av rutiner, felaktiga processer

Exempel
- Skyldigheten att genomföra nämnda analys kan vara okänd för den eller de i bolaget som formellt sett har uppgiften att genomföra och dokumentera den. Detta kan bero på okunskap om hur föreskrifterna gäller för bolag eller otillräcklig säkerhetsutbildning i allmänhet.

Exempel på potentiella konsekvenser
- Det går inte att utesluta att man i säkerhetsanalys skulle komma fram till att bolaget hanterar uppgifter eller anläggningar som rör rikets säkerhet. Således kan utebliven säkerhetsanalys medföra felaktig hantering av sådana uppgifter. Vidare kan det föranleda att anläggningar har en otillräcklig skyddsnivå.

Se också
4.1.4

Referenser
Svenska Kraftnäts Föreskrifter, SvKFS 2013:1
Säkerhetsskyddslag (1996:627)
Säkerhetsskyddsförordningen (1996:633)

4.1.6 Insider röjer skyddsvärd information till obehörig

Beskrivning
En person som, exempelvis genom sitt arbete, är behörig att ta del av och hantera skyddsvärda uppgifter röjer sådana uppgifter till någon som är obehörig att ta del av dem.

Kategori
Administrativt hot, hot mot sekretess/konfidentialitet

Orsak/Aktör
Egen personal, Inkompetens, avsaknad av erfarenhet, slarv, avsaknad av rutiner, felaktiga processer

Exempel
- Person med insyn i den ekonomiska processen röjer känsliga prissättningsuppgifter till konkurrenter.
- Person med insyn i det fysiska skyddets utformning för en skyddsvärd anläggning röjer uppgifter om detta som kan användas för att underlätta inbrott eller sabotage.

Exempel på potentiella konsekvenser
- Negativ påverkan av bolagets ekonomiska förutsättningar.
- Ökad risk för inbrott eller annan oönskad påverkan av anläggningsresurser.

Se också
4.1.7

Referenser

4.1.7 Oavsiktligt röjande av skyddsvärda uppgifter

Beskrivning
En person som, exempelvis genom sitt arbete, är behörig att ta del av och hantera skyddsvärda uppgifter röjer av misstag sådana uppgifter till obehörig.

Kategori
Administrativt hot, hot mot sekretess/konfidentialitet

Orsak/Aktör
Inkompetens, avsaknad av erfarenhet, slarv, avsaknad av rutiner, felaktiga processer

Exempel
- Person med insyn i den ekonomiska processen saknar säkerhetsutbildning, alternativt kännedom om att uppgifterna faktiskt är skyddsvärda, och röjer känsliga prissättningsuppgifter genom publicering i sociala medier i samband med socialt nätverkande.
- Person med insyn i det fysiska skyddets utformning för en skyddsvärd anläggning röjer uppgifter om detta som kan användas för att underlätta inbrott eller sabotage genom att lämna ut uppgifter på begäran utan föregående bedömning av uppgifternas skyddsvärde.

Exempel på potentiella konsekvenser
- Negativ påverkan av bolagets ekonomiska förutsättningar.
- Ökad risk för inbrott eller annan oönskad påverkan av anläggningsresurser.

Se också
4.1.5, 4.1.6

Referenser

4.2 Kontrakt, avtal

Detta kapitel beskriver olika hot som har en knytning till olika typer av affärsdokument, främst kontrakt och avtal.

4.2.1 Avsaknad av styrande kontrakt och avtal

Beskrivning
Inom varje verksamhet finns det tecknade avtal och kontrakt mot andra enheter inom det egna bolaget, mot tredje part i form av leverantörer, entreprenörer, inhyrd personal eller liknande. Det kan hända att dessa typer av formella dokument saknas, utan leveranser eller tjänster köps in, hyrs eller nyttjas baserat på förenklade muntliga överenskommelser.

Det saknas relevanta kontrakt, avtal och andra styrande dokument som reglerar ansvar, nivåer och leverans.

Kategori
Administrativt hot

Orsak/Aktör
Inkompetens, avsaknad av erfarenhet, slarv, avsaknad av rutiner, felaktiga processer

Exempel
- Avsaknad av avtal för IT-konsulter
- Avsaknad av avtal för IT-utvecklare
- Avsaknad av avtal för driftleverantörers åtagande för drift av IT-system
- Avsaknad av avtal för entreprenörer i anläggning

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 6.2.3 ”Hantering av säkerhet i tredjepartsavtal”
ISO/IEC 27019:2013 kap 6.2.3 ”Addressing security in third-party agreements”

4.2.2 Ofullständiga styrande kontrakt och avtal

Beskrivning
Inom varje verksamhet finns det tecknade avtal och kontrakt mot andra enheter inom det egna bolaget, mot tredje part i form av leverantörer, entreprenörer, inhyrd personal eller liknande. Det kan hända att dessa typer av formella dokument saknas, utan leveranser eller tjänster köps in, hyrs eller nyttjas baserat på förenklade muntliga överenskommelser.

De kontrakt, avtal och andra styrande dokument som skall reglera ansvar, nivåer och leverans är inte tillräckligt omfattande eller innehåller ofullständig underlag.

Kategori
Administrativt hot

Orsak/Aktör
Inkompetens, avsaknad av erfarenhet, slarv, avsaknad av rutiner, felaktiga processer

Exempel
- Ofullständiga avtal för IT-konsulter
- Ofullständiga avtal för IT-utvecklare
- Ofullständiga avtal för driftleverantörers åtagande för drift av IT-system
- Ofullständiga avtal för entreprenörer i anläggning

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 6.2.3 ”Hantering av säkerhet i tredjepartsavtal”

4.2.3 Avsaknad av säkerhetsbilagor till kontrakt och avtal

Beskrivning
De kontrakt, avtal och andra styrande dokument som reglerar ansvar, nivåer och leverans som finns saknar de relevanta säkerhetsbilagor som reglerar myndigheternas eller organisationens egna säkerhetskrav på kontraktsparten.

Kategori
Administrativt hot

Orsak/Aktör
Inkompetens, avsaknad av erfarenhet, slarv, avsaknad av rutiner, felaktiga processer

Exempel
- Det saknas bilagor till avtal som reglerar sekretess mellan parter
- Det saknas bilagor som reglerar IT-säkerheten på den utrustning som leverantören skall använda i beställaren anläggningar och mot de system som beställaren har
- Det saknas bilagor som reglerar informationssäkerheten för den information som leverantören förfogar över härrör från beställaren eller som är skyddsvärd utifrån beställarens perspektiv
- Det saknas bilagor som reglerar överträdelser av de säkerhetskrav som upprättats
- Myndigheter eller andra nationella eller internationella organisationer ställer krav som i sin tur berör området säkerhet, sekretess, tillgänglighet. Dessa krav är inte närmare specificerade i avtal, kontrakt, säkerhetsbilagor eller liknande

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 6.2.3 ”Hantering av säkerhet i tredjepartsavtal”
ISO/IEC 27019:2013 kap 6.1.6 ”Contact with authorities”

4.2.4 Avsaknad av uppföljning av existerande styrande kontrakt och avtal

Beskrivning
Det är en allmän avsaknad av uppföljning – ur ett säkerhetsperspektiv – av olika existerande kontrakt, avtal och andra styrande dokument som reglerar ansvar, nivåer och leverans.

Kategori
Administrativt hot

Orsak/Aktör
Inkompetens, avsaknad av erfarenhet, slarv, avsaknad av rutiner, felaktiga processer, avsaknad av resurser

Exempel
- Avsaknad av uppföljning av avtal vid leverans av nya lösningar, så kallad acceptanstest
- Avsaknad av uppföljning av avtal vid leverans av tjänster som används över tid
- Avsaknad av uppföljning av avtal vid leverans av tjänster som enstaka gång

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 6.2.3 ”Hantering av säkerhet i tredjepartsavtal”

4.3 Styrdokument

Detta kapitel avhandlar olika hot relaterade till hanteringen av dokument som behövs för styrning och ledning. Typer av hot är

- Avsaknad av styrdokument
- Styrdokument som saknar förankring
- Felaktiga styrdokument

4.3.1 Avsaknad av styrdokument

Beskrivning
Styrdokument är samlingsnamn på dokument som beskriver vad som styr verksamheten, vad man ska förhålla sig till och hur man ska utföra vissa moment. Ett styrdokument beskriver processer, rutiner, ansvar, roller, arbetsmoment. Detta hot utgör att dessa typer av dokument saknas i enstaka eller i mer omfattande fall, då dessa inte tagits fram.

Kategori
Administrativt hot

Orsak/Aktör
Okunskap, slarv, felprioritering, icke kommunicerade behov eller krav

Exempel
- Avsaknad av säkerhetspolicy
- Avsaknad av riktlinjer för säkerhets, IT-säkerhets eller informationssäkerhetsarbete
- Avsaknad av handböcker för säkerhets, IT-säkerhets eller informationssäkerhetsarbete
- Avsaknad av vägledningar för säkerhets, IT-säkerhets eller informationssäkerhetsarbete

Se också
4.3.2 ,4.3.3, 4.3.4

Referenser
SS-ISO/IEC 27002:2005 kap 5.1.1 ”Policydokument för informationssäkerhet”
SS-ISO/IEC 27002:2005 kap 5.1.2 ”Granskning av informationssäkerhetspolicyn”
SS-ISO/IEC 27002:2005 kap 10.8.1 ”Policyer och rutiner för informationsutbyte”
SS-ISO/IEC 27002:2005 kap 11.1.1 ”Åtkomstpolicy”
SS-ISO/IEC 27002:2005 kap 15.2.1 ”Efterlevnad av säkerhetspolicyer och –standarder”

4.3.2 Styrdokument som saknar förankring

Beskrivning
Styrdokument är samlingsnamn på dokument som beskriver vad som styr verksamheten, vad man ska förhålla sig till och hur man ska utföra vissa moment. Ett styrdokument beskriver processer, rutiner, ansvar, roller, arbetsmoment. Detta hot utgör att styrande dokument inte är förankrade hos ledningen kan leda till att organisationen inte känner att de måste följa de olika typer av direktiv som ges i dokumenten.

Kategori
Administrativt hot

Orsak/Aktör
Okunskap, slarv, felprioritering, icke kommunicerade behov eller krav

Exempel
- Säkerhetspolicyn är inte förankrad hos ledningen
- Säkerhetspolicyn är inte förankrad hos säkerhetsavdelningens personal
- Vägledningar, handböcker, riktlinjer är inte förankrad hos den personal som skall arbeta med sakfrågorna

Se också
4.3.1, 4.3.3, 4.3.4

Referenser
SS-ISO/IEC 27002:2005 kap 5.1.1 ”Policydokument för informationssäkerhet”
SS-ISO/IEC 27002:2005 kap 5.1.2 ”Granskning av informationssäkerhetspolicyn”
SS-ISO/IEC 27002:2005 kap 10.8.1 ”Policyer och rutiner för informationsutbyte”
SS-ISO/IEC 27002:2005 kap 11.1.1 ”Åtkomstpolicy”
SS-ISO/IEC 27002:2005 kap 15.2.1 ”Efterlevnad av säkerhetspolicyer och –standarder”

4.3.3 Ofullständiga styrdokument

Beskrivning
Styrdokument är samlingsnamn på dokument som beskriver vad som styr verksamheten, vad man ska förhålla sig till och hur man ska utföra vissa moment. Ett styrdokument beskriver processer, rutiner, ansvar, roller, arbetsmoment. Detta hot utgör att dessa typer av dokument är ofullständiga i enstaka eller i mer omfattande fall.

Kategori
Administrativt hot

Orsak/Aktör
Okunskap, slarv, felprioritering

Exempel
- Styrdokument finns, men de är ej uppdaterade att reflektera aktuellt arbetssätt, aktuell lagstiftning och juridiska krav, aktuella affärskrav, teknologiska nyheter, etc
- Styrdokument finns, men de beskriver ej arbetssätt, aktuell lagstiftning och juridiska krav, aktuella affärskrav, teknologiska nyheter, då de tagits fram av personer utan rätt kompetens eller insyn i arbetet

Se också
4.3.1, 4.3.2 , 4.3.4

Referenser
SS-ISO/IEC 27002:2005 kap 5.1.1 ”Policydokument för informationssäkerhet”
SS-ISO/IEC 27002:2005 kap 5.1.2 ”Granskning av informationssäkerhetspolicyn”
SS-ISO/IEC 27002:2005 kap 10.8.1 ”Policyer och rutiner för informationsutbyte”
SS-ISO/IEC 27002:2005 kap 11.1.1 ”Åtkomstpolicy”
SS-ISO/IEC 27002:2005 kap 15.2.1 ”Efterlevnad av säkerhetspolicyer och –standarder”

4.3.4 Felaktiga styrdokument

Beskrivning
Styrdokument är samlingsnamn på dokument som beskriver vad som styr verksamheten, vad man ska förhålla sig till och hur man ska utföra vissa moment. Ett styrdokument beskriver processer, rutiner, ansvar, roller, arbetsmoment. Detta hot utgör att dessa typer av dokument är felaktiga i enstaka eller i mer omfattande fall.

Kategori
Administrativt hot

Orsak/Aktör
Okunskap, slarv, felprioritering

Exempel
- Styrdokument finns, men de är ej uppdaterade att reflektera aktuellt arbetssätt, aktuell lagstiftning och juridiska krav, aktuella affärskrav, teknologiska nyheter, etc
- Styrdokument finns, men de beskriver ej arbetssätt, aktuell lagstiftning och juridiska krav, aktuella affärskrav, teknologiska nyheter, då de tagits fram av personer utan rätt kompetens eller insyn i arbetet

Se också
4.3.1, 4.3.2 ,4.3.3

Referenser
SS-ISO/IEC 27002:2005 kap 5.1.1 ”Policydokument för informationssäkerhet”
SS-ISO/IEC 27002:2005 kap 5.1.2 ”Granskning av informationssäkerhetspolicyn”
SS-ISO/IEC 27002:2005 kap 10.8.1 ”Policyer och rutiner för informationsutbyte”
SS-ISO/IEC 27002:2005 kap 11.1.1 ”Åtkomstpolicy”
SS-ISO/IEC 27002:2005 kap 15.2.1 ”Efterlevnad av säkerhetspolicyer och –standarder”

4.4 Övergripande om processer och rutiner

Detta kapitel avhandlar olika hot relaterade till hanteringen av processer och rutiner som behövs för styrning och ledning. Typer av hot är

- Avsaknad av processteg
- Avsaknad av rutiner
- Felaktiga rutiner
- Avsaknad av kunskap

4.4.1 Avsaknad av processteg och rutiner för att göra tillräckligt kravarbete i samband med projektering, inköp eller utveckling

Beskrivning

För att slutresultatet skall hålla en god kvalitet krävs det att adekvata krav, rätt nivå på krav, rätt mängd krav, ställs i samband med de olika stegen innan resultatet färdigställs. Det är därför viktigt att alla processteg är på plats och att dessa processteg innehåller rutiner för att ta fram, analysera och hantera krav.

Kategori
Administrativt hot

Orsak/Aktör
Felaktigt ledningssystem, felaktig styrning, felaktigt analyserade behov, felaktig processmodell

Exempel
- Ingen systematik så att all relevant lagstiftning beaktas och påverkar projektleverans eller design
- Det saknas metodstöd i projektmodell för att hitta rätt typ eller tillräckligt med krav i samband med projektering
- Det saknas metodstöd i utvecklingsmodell för att hitta rätt typ eller tillräckligt med krav i samband med programutvecklingsaktivitet

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 6.1.1 Ledningens engagemang för informationssäkerhet”
SS-ISO/IEC 27002:2005 kap 6.1.2 ”Samordning av informationssäkerhetsarbetet”
SS-ISO/IEC 27002:2005 kap 6.2.1 ”Identifiering av risker med utomstående parter”
SS-ISO/IEC 27002:2005 kap 12.1.1 ”Analys och specifikation av säkerhetskrav”
SS-ISO/IEC 27002:2005 kap 12.5 ”Säkerhet i utvecklings- och underhållsprocesser”

4.4.2 Avsaknad av processteg och rutiner för att göra tillräcklig hantering i samband med projektavslut, avslutad anställning eller avslutat uppdrag

Beskrivning
I samband med olika typer av avslut, såsom projektavslut eller avslutande av en anställning, krävs det ordentlig hantering vid själva avslutet. Det är därför viktigt att alla processteg är på plats och att dessa processteg innehåller rutiner för att ta kunna se till att avslutandet görs på ett kontrollerat och välordnat sätt.

Kategori
Administrativt hot

Orsak/Aktör
Felaktigt ledningssystem, felaktig styrning, felaktigt analyserade behov

Exempel
- Ingen utfasning av anställda som håller på och avslutar sin anställning
- Inget överlämning av kunskap
- ingen kontroll av att all lånad utrustning återlämnas
- ingen kontroll av att databärare och information återlämnas

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 6.1.1 Ledningens engagemang för informationssäkerhet”
SS-ISO/IEC 27002:2005 kap 6.1.2 ”Samordning av informationssäkerhetsarbetet”
SS-ISO/IEC 27002:2005 kap 6.2.1 ”Identifiering av risker med utomstående parter”
SS-ISO/IEC 27002:2005 kap 9.2.7 ”Avlägsnande av egendom”
SS-ISO/IEC 27002:2005 kap 8.3.3 ”Indragning av åtkomsträttigheter”
SS-ISO/IEC 27002:2005 kap 12.1.1 ”Analys och specifikation av säkerhetskrav”
SS-ISO/IEC 27002:2005 kap 12.5 ”Säkerhet i utvecklings- och underhållsprocesser”

4.4.3 Avsaknad av processteg och rutiner för att göra tillräcklig hantering i samband med utrangering av datamedia, system eller infrastrukturutrustning

Beskrivning
I samband med att vissa system eller infrastrukturutrustning tas ur drift eller skall utrangeras, eller att databärare såsom hårddiskar, DVD-skivor eller backupband inte skall användas mer, så är det viktigt att dessa tas omhand om, så att inte information oavsiktligt kommer obehöriga tillhanda. Det är därför viktigt att alla processteg är på plats och att dessa processteg innehåller rutiner för att ta kunna se till att avslutandet och utrangeringen görs på ett kontrollerat och välordnat sätt.

Kategori
Administrativt hot

Orsak/Aktör
Felaktigt ledningssystem, felaktig styrning, felaktigt analyserade behov

Exempel
- ingen kontroll av att databärare och datamedia förstörs i samband med att dessa utrangeras eller kasseras
- ingen kontroll av att databärare och datamedia tas bort ur datorer i samband med att dessa utrangeras eller kasseras
- ingen kontroll av att databärare och datamedia tas bort ur kringutrustning såsom skrivare i samband med att dessa utrangeras eller kasseras
- ingen kontroll av att databärare och datamedia rensas eller tas bort ur infrastrukturutrustning i samband med att dessa utrangeras eller kasseras

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.6 ”Säker avveckling eller återanvändning av utrustning”
SS-ISO/IEC 27002:2005 kap 9.2.7 ”Avlägsnande av egendom”

4.4.4 Avsaknad av kunskap om processer, processteg och rutiner

Beskrivning
Personal har inte kunskap om de övergripande processer som finns inom organisationen. Personal har inte kunskap om de olika processteg som utgör processerna. Personal har inte kunskap om de olika rutiner som ingår i de olika processtegen.

Kategori
Administrativt hot

Orsak/Aktör
Felaktig kompetens, felaktigt kommunicerade interna arbetsmetoder, avsaknad av att kommunicera interna arbetsmetoder

Exempel
- Personal har inte nödvändig kunskap om de processer, processteg eller rutiner som gäller
- Personal i lägre ansvarsställning har inte nödvändig kunskap om de processer, processteg eller rutiner som gäller
- Personal i högre ansvarsställning har inte nödvändig kunskap om de processer, processteg eller rutiner som gäller
- Bolagets ledning har inte nödvändig kunskap om de processer, processteg eller rutiner som gäller

Se också
4.4.5, 4.4.6

Referenser
SS-ISO/IEC 27002:2005 kap 5.1.1 ”Policydokument för informationssäkerhet”

4.4.5 Processer, processteg och rutiner har ofullständig eller felaktig dokumentation

Beskrivning
På grund av ofullständig eller felaktig dokumentation så har personal inte kunskap om de övergripande processer som finns inom organisationen. På grund av ofullständig eller felaktig dokumentation så har personal inte kunskap om de olika processteg som utgör processerna. På grund av ofullständig eller felaktig dokumentation så har personal inte kunskap om de olika rutiner som ingår i de olika processtegen.

Kategori
Administrativt hot

Orsak/Aktör
Inkompetens, felaktigt ledningssystem, felaktig styrning, felaktigt analyserade behov, felaktig prioritering

Exempel
- Personal har inte nödvändig kunskap om de processer, processteg eller rutiner som gäller eftersom dessa är ofullständigt eller felaktigt dokumenterade
- Personal i lägre ledande position har inte nödvändig kunskap om de processer, processteg eller rutiner som gäller eftersom dessa är ofullständigt eller felaktigt dokumenterade
- Personal i högre ledande position har inte nödvändig kunskap om de processer, processteg eller rutiner som gäller eftersom dessa är ofullständigt eller felaktigt dokumenterade

Se också
4.4.4, 4.4.6

Referenser
SS-ISO/IEC 27002:2005 kap 5.1.1 ”Policydokument för informationssäkerhet”

4.4.6 Processer, processteg och rutiner är ej dokumenterade

Beskrivning
Personal har inte kunskap om de övergripande processer som finns inom organisationen eftersom dessa ej är dokumenterade. Personal har inte kunskap om de olika processteg som utgör processerna eftersom dessa ej är dokumenterade. Personal har inte kunskap om de olika rutiner som ingår i de olika processtegen eftersom dessa ej är dokumenterade.

Kategori
Administrativt hot

Orsak/Aktör
Inkompetens, felaktigt ledningssystem, felaktig styrning, felaktigt analyserade behov, felaktig prioritering

Exempel
- Personal har inte nödvändig kunskap om de processer, processteg eller rutiner som gäller eftersom dessa ej är dokumenterade
- Personal utför felaktiga moment eftersom de inte nödvändig kunskap om de processer, processteg eller rutiner som gäller eftersom dessa ej är dokumenterade
- Personal utför säkerhetsvidriga moment eftersom de inte nödvändig kunskap om de processer, processteg eller rutiner som gäller eftersom dessa ej är dokumenterade

Se också
4.4.4, 4.4.5

Referenser
SS-ISO/IEC 27002:2005 kap 5.1.1 ”Policydokument för informationssäkerhet”

4.4.7 Ingen uppföljning och utvärdering av effekt, kvalitet eller konsekvens hos processer, processteg och rutiner

Beskrivning
Avsaknad av uppföljning och utvärdering kan i sig själv innebära säkerhetsrisker, då olika saker som är felaktiga, säkerhetsvidriga eller innebära risk för organisationen kan ha pågått under en tid utan upptäckt.

Kategori
Administrativt hot

Orsak/Aktör
Inkompetens, felaktigt ledningssystem, felaktig styrning, felaktigt analyserade behov, felaktig prioritering

Exempel
- Ingen utvärdering eller uppföljning av upphandlings- och inköpsprocessen att säkerhetskrav har ingått i de avtal som slutits
- Ingen utvärdering eller uppföljning av utvecklingsprocessen att säkerhetskrav fångas, analyseras och behandlats

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 5.1.2 ”Granskning av informationssäkerhetspolicyn”

4.5 Utkontraktering och utläggning av tjänster och information

Detta kapitel handlar om hot i samband med att man köper eller på annat sätt avtalar om utkontraktering eller utläggning av informationshantering.

Olika typer av utläggningar kan exempelvis vara

- Utläggning av drift (s.k. co-location, colo)
- Upphandling av allmänna elektroniska tjänster, exempelvis elektronisk post
- Upphandling av molntjänster, exempelvis infrastructure as a service (IAAS), platform as a service (PAAS)

4.5.1 Avsaknad av kravställning på leverantör i samband med utkontraktering

Beskrivning
I samband med att drift läggs ut till tredjepart att sköta åt organisationen så ska avtal slutas och i dessa avtal ska det finnas med olika typer av detaljer som regleras, vilka har härletts ur krav och kravställning.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, taktiskt spel med avseende på kostnadsbesparingar

Exempel
- Det saknas säkerhetskrav över huvudtaget i upphandlingen av utkontraktering
- Vissa allmänna, högtravande och övergripande skrivelser om säkerhet finns i upphandlingsunderlag, vilket gör dem till extrema tolkningsfrågor som leverantören kommer tolka till sin fördel. Men precisa krav på skydd, skyddsnivåer, processer, hanteringsformer och rutiner för säkerhet saknas
- Avsaknad krav rörande under utkontrakteringsperioden nyskapad information, exempelvis metadata, driftstatistik, användarprofiler eller liknande har oklart ägandeskap då detta inte regleras i krav eller avtal

Se också
4.5.3, 4.5.2

Referenser
SS-ISO/IEC 27002:2005 kap 6.2.1 ”Identifiering av risker med utomstående parter”
SS-ISO/IEC 27002:2005 kap 6.2.3 ”Hantering av säkerhet i tredjepartsavtal”
SS-ISO/IEC 27002:2005 kap 10.2.1 ”Tjänsteleverans”
ISO/IEC 27019:2013 kap 12.1.1 ”Security requirement analysis and specification”

4.5.2 Felaktig kravställning på leverantör i samband med utkontraktering

Beskrivning
De krav som ställs i samband med ukontrakteringen är felaktiga, exempelvis är säkerhetskraven fel, eller att andra krav är fel vilket leder till säkerhetsrelaterade problem i förlängningen.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, taktiskt spel med avseende på kostnadsbesparingar

Exempel
- Vissa allmänna, högtravande och övergripande skrivelser om säkerhet finns i upphandlingsunderlag, vilket gör dem till extrema tolkningsfrågor som leverantören kommer tolka till sin fördel. Men precisa krav på skydd, skyddsnivåer, processer, hanteringsformer och rutiner för säkerhet saknas
- De allmänna, högtravande och övergripande skrivelser om säkerhet finns i upphandlingsunderlag, är inte i linje med gällande lagstiftning och juridiska krav som finns på organisationen och organisationens informationshantering, tex personuppgiftslagen, offentlighet- och sekretesslag, säkerhetsskyddslag
- De allmänna, högtravande och övergripande skrivelser om säkerhet finns i upphandlingsunderlag, är inte i linje med organisationens egna interna krav på säkerhet och informationssäkerhet
- Allmänna krav exempelvis rörande informationskvalitet eller lagringformat, har uttryckts oklart, formulerats fel, eller innehåller felaktig information vilket leder till säkerhetsrelaterade problem i förlängningen
- Felaktigt uttryckta krav rörande under utkontrakteringsperioden nyskapad information, exempelvis metadata, driftstatistik, användarprofiler eller liknande har oklart ägandeskap då detta inte korrekt regleras i krav eller avtal

Se också
4.5.3, 4.5.2

Referenser
SS-ISO/IEC 27002:2005 kap 6.2.1 ”Identifiering av risker med utomstående parter”
SS-ISO/IEC 27002:2005 kap 6.2.3 ”Hantering av säkerhet i tredjepartsavtal”
SS-ISO/IEC 27002:2005 kap 10.2.1 ”Tjänsteleverans”
ISO/IEC 27019:2013 kap 12.1.1 ”Security requirement analysis and specification”

4.5.3 Avsaknad av avtalsvillkor på leverantör i samband med utkontraktering

Beskrivning
I samband med att drift läggs ut till tredjepart att sköta åt organisationen så ska avtal slutas och i dessa avtal ska det finnas med olika typer av detaljer som regleras, vilka har härletts ur krav och kravställning. Ett antal av dessa krav ska vara ställda till leverantören om dennes kvalitet, säkerhet, etc.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, taktiskt spel med avseende på kostnadsbesparingar

Exempel
- De utfästelser som leverantören gör i marknadsföring av sin tjänst för utkontraktering av IT och IT-drift kommer inte med i avtalstext eller avtalsvillkor
- De krav som ställs i samband med allmänna diskussioner om utkontraktering kommer inte med i avtalstext eller avtalsvillkor
- De krav som ställs i samband med förhandling om utkontraktering kommer inte med i avtalstext eller avtalsvillkor
- De krav som ställs i samband med första omgången kontraktstext som utgör underlag för utkontraktering kommer inte med i den slutliga avtalstext eller avtalsvillkor

Se också
4.5.3, 4.5.1,4.5.2 4.5.4

Referenser
SS-ISO/IEC 27002:2005 kap 6.2.1 ”Identifiering av risker med utomstående parter”
SS-ISO/IEC 27002:2005 kap 6.2.3 ”Hantering av säkerhet i tredjepartsavtal”
SS-ISO/IEC 27002:2005 kap 10.2.1 ”Tjänsteleverans”
ISO/IEC 27019:2013 kap 12.1.1 ”Security requirement analysis and specification”

4.5.4 Felaktiga avtalsvillkor på leverantör i samband med utkontraktering

Beskrivning
I samband med utkontraktering eller utläggning tecknas avtal. De avtalsvillkor som finns i kontrakt, avtal eller avtalsbilagor innehåller felaktigheter som kan innebära säkerhetsproblem och är ett hot mot informationshanteringen.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, taktiskt spel med avseende på kostnadsbesparingar

Exempel
- De krav som ställs i samband med utkontrakteringen kommer inte med i avtalstext eller avtalsvillkor
- De krav som ställs i samband med utkontrakteringen är ändrade och stämmer inte med ursprungskrav det som uttrycks i avtalstext eller avtalsvillkor
- De villkor som uttrycks avtalstext eller avtalsvillkor innehåller felaktigheter vilket kan innebära säkerhetsproblem. Det kan exempelvis vara hur länge information sparas i samband med säkerhetskopiering, frekvens på säkerhetskopiering,vad som skall loggas, hur dessa loggar skall sparas, med mera

Se också
4.5.3, 4.5.1, 4.5.2

Referenser
SS-ISO/IEC 27002:2005 kap 6.2.1 ”Identifiering av risker med utomstående parter”
SS-ISO/IEC 27002:2005 kap 6.2.3 ”Hantering av säkerhet i tredjepartsavtal”
SS-ISO/IEC 27002:2005 kap 10.2.1 ”Tjänsteleverans”
ISO/IEC 27019:2013 kap 12.1.1 ”Security requirement analysis and specification”

4.5.5 Utläggning och hantering av skyddsvärd information på projektplatser

Beskrivning
Utläggning av en viss tjänst till en tredjepartsleverantör, där informationen skall användas i projekt och därmed delas med projektmedlemmar.

I samband med utläggningen överförs information till denna projektplats, alternativt att det skapas information, såsom dokument och ritningar, som läggs upp på denna projektplats löpande.

Kategori
Administrativt hot

Orsak/Aktör
Okunskap om gällande juridiska krav, handhavandefel

Exempel
- Det kan vara information som enligt olika juridiska krav måste hanteras på ett visst sätt, exempelvis hanteras inom landet eller inom EES-länderna, men som läggs ut på en nätplats eller elektronisk projektplats som är placerad på okänd ort.
- Det kan vara information som enligt organisationens egna interna regler måste hanteras på ett visst sätt, exempelvis att informationen skall gallras på ett visst sätt med ett visst intervall. Hanteringen sker inte på detta sätt därför att det läggs ut hos en tjänsteleverantör som inte har kännedom eller möjlighet att hantera informationen på det sätt som reglerna säger.

Se också
4.5.3, 4.5.1

Referenser
SS-ISO/IEC 27002:2005 kap 6.2.1 ”Identifiering av risker med utomstående parter”
SS-ISO/IEC 27002:2005 kap 6.2.3 ”Hantering av säkerhet i tredjepartsavtal”
SS-ISO/IEC 27002:2005 kap 10.2.1 ”Tjänsteleverans”

4.6 Specifika hot rörande processer och rutiner

Detta kapitel avhandlar olika hot relaterade till hanteringen av specifika processer och detaljerade rutiner, exempelvis behörighetsadministration.

4.6.1 Felaktig behörighetsadministration

Beskrivning
Personal som jobbar med kontoadministration eller administration av behörighetsinställningar för användarkonton gör fel vid sitt arbete. Alternativt de förlagor, skript, program eller rutiner som skapats och används för behörighetsadministrationen är felaktiga.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar, underbemanning på säkerhetsfunktionen

Exempel
- Administratörer kan skapa konton utan spårbarhet vem som skapat kontot
- Administratörer i en del av organisationen kan skapa konton för nya användare tillhörande fiktiva personer i annan del av organisationen utan spårbarhet vem som skapat kontot

Se också
4.6.2, 4.6.3, 4.6.4, 4.6.5

Referenser
SS-ISO/IEC 27002:2005 kap 8.1.1 ”Roller och ansvar”

4.6.2 För höga behörigheter hos användare

Beskrivning
Användarkonton i system, applikationer eller för åtkomst till elektroniska tjänster är felaktiga, och medger större åtkomst eller mer funktionalitet än avsett.

Personal som jobbar med kontoadministration eller administration av behörighetsinställningar för användarkonton gör fel vid sitt arbete så att behörigheterna blir för höga. Alternativt de förlagor, skript, program eller rutiner som skapats och används för behörighetsadministrationen är felaktiga.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning på säkerhetsfunktionen

Exempel
- Åtkomst till en webbplats för läsning av webbsidor möjliggör både läsning och skrivning
- Åtkomst till en RTU för läsning av värden möjliggör både läsning och skrivning av värden
- Åtkomst till en PLC för normal access ger även administrativ åtkomst

Se också
4.6.1, 4.6.3, 4.6.4, 4.6.5

Referenser
SS-ISO/IEC 27002:2005 kap 8.1.1 ”Roller och ansvar”

4.6.3 För höga behörigheter hos personal i helpdesk

Beskrivning
Användarkonton som används av personal i användarstödsfunktioner och helpdesk för att komma åt system, applikationer eller för åtkomst till elektroniska tjänster är felaktiga, och medger större åtkomst eller mer funktionalitet än avsett.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning på säkerhetsfunktionen

Exempel
- Helpdeskpersonal kan skapa nya konton i system där de enbart skall ha läsåtkomst
- Helpdeskpersonal kan stänga av loggning och spårbarhet i system där de enbart skall ha läsåtkomst
- Helpdeskpersonal kan skapa nya konton med administrativ behörighet i system

Se också
4.6.1, 4.6.2, 4.6.4, 4.6.5

Referenser
SS-ISO/IEC 27002:2005 kap 8.1.1 ”Roller och ansvar”

4.6.4 För höga behörigheter hos personal som jobbar med utveckling

Beskrivning
Personal som jobbar med mjukvaruutveckling har ibland för höga behörigheter i det eller de system de jobbar med programutveckling i. Baserat på de tester och användningsfall de jobbat med, kan detta få till resultat att de program eller programmoduler de utvecklar har ett felaktig förhållande till skydd, exempelvis filskydd.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning på säkerhetsfunktionen

Exempel
- En utvecklare utvecklar en webblösning som inte förstår filskydd och behörighet på filer
- En utvecklare utvecklar ett som inte förstår begränsningar för socketanrop och nätverksåtkomst

Se också
4.6.1, 4.6.2, 4.6.3, 4.6.5

Referenser
SS-ISO/IEC 27002:2005 kap 8.1.1 ”Roller och ansvar”

4.6.5 För höga behörigheter hos personal som arbetar med testning

Beskrivning
Personal som arbetar med testning av applikationer, subsystem, infrastruktur eller system använder konton med behörighetsinställningar som är för höga. Detta kan leda till problem då detta kan skapa situationer där testerna utförs med förutsättningar som inte motsvarar de som är i en mer restriktivt uppsatt produktionsmiljö.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning på säkerhetsfunktionen

Exempel
- Testfallen motsvarar inte de situationer som används i produktionssatta servrar, då av säkerhetsskäl dessa program som används i dessa servrar inte kör med höga behörigheter
- Testfallen motsvarar inte de situationer som används i produktionssatta servrar, då av säkerhetsskäl de konton som används i dessa servrar inte kör med höga behörigheter

Se också
4.6.1, 4.6.2, 4.6.3, 4.6.4

Referenser
SS-ISO/IEC 27002:2005 kap 8.1.1 ”Roller och ansvar”

4.6.6 Avsaknad av rutiner för att underhålla skydd mot skadlig kod

Beskrivning
Skydd mot skadlig kod kräver aktiv hantering i flera fall, inklusive nyinstallation av programvara, uppdatering av programvara, hantering av mjuvarulicenser, ändringar i programinställningar och konfiguration.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning på säkerhetsfunktionen

Exempel
- Viktiga IT-komponenter saknar installerat skydd mot skadlig kod
- Viktiga IT-komponenter i SCADA/IECS-miljön saknar installerat skydd mot skadlig kod
- Viktiga IT-komponenter har installerat skydd mot skadlig kod, men detta är inte uppdaterat sedan länge
- Viktiga IT-komponenter har installerat skydd mot skadlig kod, men detta är felaktigt uppsatt sedan länge

Se också
4.6.7

Referenser
SS-ISO/IEC 27002:2005 kap 8.1.1 ”Roller och ansvar”
ISO/IEC 27019:2013 kap 12.4.1 ”Control of operational software”

4.6.7 Felaktiga rutiner för att underhålla skydd mot skadlig kod

Beskrivning
Skydd mot skadlig kod kräver aktiv hantering i flera fall, inklusive nyinstallation av programvara, uppdatering av programvara, hantering av mjuvarulicenser, ändringar i programinställningar och konfiguration.

De rutiner som finns (automatiserade eller manuella) är felaktigt utformade.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning på säkerhetsfunktionen

Exempel
- Viktiga IT-komponenter saknar installerat skydd mot skadlig kod
- Viktiga IT-komponenter i SCADA/IECS-miljön saknar installerat skydd mot skadlig kod
- Viktiga IT-komponenter har installerat skydd mot skadlig kod, men detta är inte uppdaterat sedan länge
- Viktiga IT-komponenter har installerat skydd mot skadlig kod, men detta är felaktigt uppsatt sedan länge, och detta upptäcks inte
- Uppdateringsrutiner fungerar inte som avsett, dvs uppdatering sker inte korrekt

Exempel på konsekvenser
- Automatiserade rutiner gör att skyddet mot skadlig kod startar om utrustning i driftcentraler och kontrollrum vid oönskade eller rent farliga tillfällen (t.ex. vid storstörning)

Se också
4.6.7

Referenser
ISO/IEC 27019:2013 kap 12.4.1 ”Control of operational software”

4.6.8 Avsaknad av rutiner för hantering av säkerhet och skydd

Beskrivning
Hos användare av IT-system och applikationer måste det finnas hantering av säkerhetsinställningar och olika skyddsmekanismer. Det bör finnas dokumenterade rutiner för hur dessa hanteras.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning på säkerhetsfunktionen

Exempel
- Avsaknad av rutiner för hur administration skall ske av brandväggar
- Avsaknad av rutiner för hur administration skall ske av loggskapande, logginsamling och analys av loggar
- Avsaknad av rutiner för hur härdning och uppsättning av säkerhet skall ske i klient- och serverdatorer
- Avsaknad av rutiner för hur säkerhetsadministration skall ske av utrustning som används i SCADA/IECS-miljö, exempelvis RTU, PLC eller IED.

Se också
4.6.6

Referenser
SS-ISO/IEC 27002:2005 kap 8.1.1 ”Roller och ansvar”

4.6.9 Felaktiga rutiner för hantering av säkerhet och skydd

Beskrivning
Hos användare av IT-system och applikationer måste det finnas hantering av säkerhetsinställningar och olika skyddsmekanismer. Det bör finnas dokumenterade rutiner för hur dessa hanteras.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar

Exempel
- Felaktiga rutiner för hur administration skall ske av brandväggar
- Felaktiga rutiner för hur administration skall ske av loggskapande, logginsamling och analys av loggar
- Felaktiga rutiner för hur härdning och uppsättning av säkerhet skall ske i klient- och serverdatorer
- Felaktiga rutiner för hur säkerhetsadministration skall ske av utrustning som används i SCADA/IECS-miljö, exempelvis RTU, PLC eller IED.

Se också
4.6.6

Referenser
SS-ISO/IEC 27002:2005 kap 8.1.1 ”Roller och ansvar”

4.6.10 Avsaknad av rutiner för hantering av kryptonycklar och kryptoteknik

Beskrivning
När kryptoteknik används är det ur säkerhetssynpunkt viktigt att den installeras, sätts upp och konfigureras rätt. Om inte krypteringstekniken används på rätt sätt, så kan skyddet istället bli ihåligt och bara vara en chimär.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Det finns inga rutiner för hur kryptolösningar skall installeras
- Det finns inga rutiner för hur inställningar på rörande algoritmer, nyckellängder, livslängd på när en viss nyckel används, med mera
- Det finns inga rutiner för vem, hur eller när kryptonycklar och certifikat skall skapas för webbplatser för att möjliggöra TLS/SSL-åtkomst till dessa webbplatser
- Det finns inga rutiner för vem, hur eller när kryptonycklar och certifikat skall skapas för interaktiv inloggning till servrar eller komponenter som används i SCADA/IECS-miljön

Se också
4.6.7, 4.6.11

Referenser
SS-ISO/IEC 27002:2005 kap 8.1.1 ”Roller och ansvar”
SS-ISO/IEC 27002:2005 kap 15.1.6 ”Reglering av kryptering”

4.6.11 Felaktiga rutiner för hantering av kryptonycklar och kryptoteknik

Beskrivning
När kryptoteknik används är det ur säkerhetssynpunkt viktigt att den installeras, sätts upp och konfigureras rätt. Om inte krypteringstekniken används på rätt sätt, så kan skyddet istället bli ihåligt och bara vara en chimär. Det är därför viktigt att de rutiner som är framtagna är korrekta och effektiva.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Rutinerna inkluderar inte moment för att hantera byte av utgågna certifikat, vilket gör att det får ske ad hoc, ofta efter att certifikatet blivit utgånget och krypteringen temporärt stängts av
- Rutinerna innehåller inte nödvändiga steg för att välja en stark och adekvat krypteringsalgoritm för nätverkskryptering
- Rutinerna innehåller inte nödvändiga steg för att välja en stark och adekvat krypteringsalgoritm för skydd av inloggningsuppgifter
- Rutinerna innehåller inte nödvändiga steg för att välja en stark och adekvat krypteringsalgoritm för skydd av filer på disk

Se också
4.6.7, 4.6.10

Referenser
SS-ISO/IEC 27002:2005 kap 8.1.1 ”Roller och ansvar”
SS-ISO/IEC 27002:2005 kap 15.1.6 ”Reglering av kryptering”

4.6.12 Felaktiga rutiner för att ta bort icke aktiva användare

Beskrivning
Kontoadministration är en central del i skyddet av system och applikationer, skydd av IT-infrastruktur, med mera. En viktig, och ofta förbisedd del av kontoadministrationen, är att spärra, blockera samt ta bort inaktiva konton. Om dessa konton ligger kvar, öppet åtkomliga, i system så kan dessa återanvändas av obehöriga som lyckats komma över autentiseringsinformation. Det är därför väldigt viktigt att de rutiner som finns för detta är korrekta och effektiva.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Rutinerna tar inte bort konton i alla nödvändiga delar av infrastrukturen, utan exempelvis fjärrinloggningsmöjligheter finns kvar, även om en användare eller ett konto tagits bort ifrån ett visst system
- Konton rapporters borttagna, men är i själva verket fortfarande kvar i vissa system
- Konton blockeras för en viss typ av inloggning, tex genom att lösenordet sätts till ett nytt framslumpat lösenord, men är fortfarande möjliga att använda för obehöriga, då det finns andra sätt att logga in på kontona, exempelvis med kryptocertifikat

Se också
4.6.13

Referenser
SS-ISO/IEC 27002:2005 kap 8.1.1 ”Roller och ansvar”
SS-ISO/IEC 27002:2005 kap 9.2.6 ”Säker avveckling eller återanvändning av utrustning”

4.6.13 Avsaknad av rutiner för att ta bort icke aktiva användare

Beskrivning
Kontoadministration är en central del i skyddet av system och applikationer, skydd av IT-infrastruktur, med mera. En viktig, och ofta förbisedd del av kontoadministrationen, är att spärra, blockera samt ta bort inaktiva konton. Om dessa konton ligger kvar, öppet åtkomliga, i system så kan dessa återanvändas av obehöriga som lyckats komma över autentiseringsinformation. Det är därför väldigt viktigt att det finns rutiner för detta.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Avsaknad av rutiner för att ta bort eller spärra oanvända konton ur Windowsmiljö
- Avsaknad av rutiner för att ta bort eller spärra oanvända konton ur Unix- eller Linuxmiljö
- Avsaknad av rutiner för att ta bort eller spärra oanvända konton ur applikationer
- Avsaknad av rutiner för att ta bort eller spärra oanvända konton ur fjärråtkomstlösningar
- Avsaknad av rutiner för att ta bort eller spärra oanvända konton ur SCADA/IECS-utrustning

Se också
4.6.12

Referenser
SS-ISO/IEC 27002:2005 kap 8.1.1 ”Roller och ansvar”
SS-ISO/IEC 27002:2005 kap 9.2.6 ”Säker avveckling eller återanvändning av utrustning”

4.6.14 Avsaknad av rutiner för att utrangera gammal utrustning

Beskrivning
Vid utrangering av utrustning som inte längre används behövs det särskilda rutiner för att se till att inte information, programinställningar, programvara, licensnycklar, särskilda hårdvarukomponenter eller liknande slängs eller görs tillgängliga för obehöriga. Det är därför viktigt att det finns rutiner för korrekt och effektiv hantering av utrangering av utrustning..

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Rutinerna för utrangering av utrustning är saknas, och utrangerad utrustning har inställningsfiler på utrustningen som beskriver och tillåter fjärranslutning in mot SCADA/IECS-nätverket
- Rutinerna för utrangering av utrustning är felaktiga och missar att det finns information på utrustningen som beskriver elnätets utformning, uppbyggnad, anläggningars geografiska position, anläggningars betydelse för elsystemet, med mera

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.6 ”Säker avveckling eller återanvändning av utrustning”

4.6.15 Felaktiga rutiner för att utrangera gammal utrustning

Beskrivning
Vid utrangering av utrustning som inte längre används behövs det särskilda rutiner för att se till att inte information, programinställningar, programvara, licensnycklar, särskilda hårdvarukomponenter eller liknande slängs eller görs tillgängliga för obehöriga. Det är därför viktigt att det finns rutiner för korrekt och effektiv hantering av utrangering av utrustning.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Rutinerna för utrangering av utrustning är felaktiga och missar att det finns inställningsfiler på utrustningen som beskriver och tillåter fjärranslutning in mot SCADA/IECS-nätverket
- Rutinerna för utrangering av utrustning är felaktiga och missar att det finns information på utrustningen som beskriver elnätets utformning, uppbyggnad, anläggningars geografiska position, anläggningars betydelse för elsystemet, med mera

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.6 ”Säker avveckling eller återanvändning av utrustning”

4.6.16 Avsaknad av rutiner för kontroll av spårdata och loggar

Beskrivning
En viktig funktion i hanteringen av incidenter är att kunna arbeta med, exempelvis analysera och korsreferera information från loggar och annan spårdata i system. Det är därför viktigt att det finns rutiner för hur denna kontroll skall gå till.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Rutiner saknas för att kontrollera att loggning är aktiverad och korrekt uppsatt i IT-komponenter
- Rutiner saknas för att kontrollera att loggning är aktiverad och korrekt uppsatt i IT-komponenter i SCADA/IECS-miljön, såsom RTU, PLC eller IED
- Rutiner saknas för att kontrollera loggning och spårdata från IT-komponenter
- Rutiner saknas för att kontrollera loggning och spårdata från IT-komponenter i SCADA/IECS-miljön såsom RTU, PLC eller IED

Se också
4.6.17

Referenser
SS-ISO/IEC 27002:2005 kap 10.10.2 ”Övervakning av systemanvändning”

4.6.17 Felaktiga rutiner för kontroll av spårdata och loggar

Beskrivning
En viktig funktion i hanteringen av incidenter är att kunna arbeta med, exempelvis analysera och korsreferera information från loggar och annan spårdata i system. Det är därför viktigt att de rutiner som finns för hur denna kontroll skall gå till är korrekta och effektiva.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Rutiner för att kontrollera att loggning är aktiverad och korrekt uppsatt i IT-komponenter är felaktig och missar att kontrollera vissa loggar eller visst spårdata
- Rutiner för att kontrollera att loggning är aktiverad och korrekt uppsatt i IT-komponenter i SCADA/IECS-miljön, såsom RTU, PLC eller IED är felaktig och missar att kontrollera vissa loggar eller visst spårdata
- Rutiner för att kontrollera loggning och spårdata från IT-komponenter är felaktig och missar att kontrollera vissa loggar eller visst spårdata
- Rutiner för att kontrollera loggning och spårdata från IT-komponenter i SCADA/IECS-miljön såsom RTU, PLC eller IED är felaktig och missar att kontrollera vissa loggar eller visst spårdata

Se också
4.6.17

Referenser
SS-ISO/IEC 27002:2005 kap 10.10.2 ”Övervakning av systemanvändning”

4.6.18 Avsaknad av rutiner för hantering av larm och akuta händelser

Beskrivning
I vissa situationer så kan system eller applikationer generera larm och det kan uppstå akuta situationer på grund av att systemet eller applikationen har hamnat i en situation där omedelbara insatser krävs, exempelvis att hårddiskar har fyllts upp, att nätverket inte fungerar, att systemfiler inte kan läsas, att det blir systemfel som beskriver att en hårdvarukomponent inte fungerar som det skall.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Det saknas rutiner för hantering av larm från tekniska system eller infrastrukturutrustning
- Det saknas rutiner för hantering av larm från SCADA/IECS-system eller IT-komponenter som finns i SCADA/IECS-miljön

Se också
4.6.19

Referenser
SS-ISO/IEC 27002:2005 kap 10.10.2 ”Övervakning av systemanvändning”

4.6.19 Felaktiga rutiner för hantering av larm och akuta händelser

Beskrivning
I vissa situationer så kan system eller applikationer generera larm och det kan uppstå akuta situationer på grund av att systemet eller applikationen har hamnat i en situation där omedelbara insatser krävs, exempelvis att hårddiskar har fyllts upp, att nätverket inte fungerar, att systemfiler inte kan läsas, att det blir systemfel som beskriver att en hårdvarukomponent inte fungerar som det skall. Det är viktigt att dessa rutiner är korrekta och effektiva.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Rutinerna för att hantera att det inte finns något ledigt lagringsutrymme föreskriver att man skall ta bort loggfiler, utan att först sparat undan dessa någon annanstans. Detta gör att man helt plötsligt tappar loggar för en viss tid
- Rutinerna för att hantera att det larmar inkluderar inte en analys som involverar att man skall kontrollera ifall det finns uppsåtliga förändringar i systemet, utan den är skapad utifrån förutsättningarna att det är ett systemfel som uppstått

Se också
4.6.18

Referenser
SS-ISO/IEC 27002:2005 kap 10.10.2 ”Övervakning av systemanvändning”
SS-ISO/IEC 27002:2005 kap 13.2.1 ”Ansvar och rutiner”

4.6.20 Avsaknad av rutiner för hantering av säkerhetsrelaterade IT-incidenter

Beskrivning
Avsaknad av rutiner eller aktiviteter för hantering av säkerhetsrelaterade IT-incidenter.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Det saknas rutiner för att hantera intrång i Windows-mijön
- Det saknas rutiner för att hantera intrång i Linux-mijön
- Det saknas rutiner för att hantera misstänkt intrång eller datamanipulation i databaser
- Det saknas rutiner för att hantera intrång i SCADA/IECS-mijön

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 13.2.1 ”Ansvar och rutiner”
SS-ISO/IEC 27002:2005 kap 13.2.3 ”Insamling av bevis”

4.6.21 Felaktiga rutiner för hantering av säkerhetsrelaterade IT-incidenter

Beskrivning
Felaktiga rutiner för hantering av säkerhetsrelaterade IT-incidenter.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Rutinerna är felaktigt utformade så de tar inte med behovet att fastställa orsak och insamlandet av elektroniska bevis, utan är bara fokuserade på att återställa driftstatus till normal drift
- Rutinerna saknar delar för hantering av media och medias roll
- Rutinerna inkluderar inte information om vem som skall informeras vid vissa skeenden och beslut

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 13.2.1 ”Ansvar och rutiner”
SS-ISO/IEC 27002:2005 kap 13.2.3 ”Insamling av bevis”

4.6.22 Avsaknad av rutiner för uppföljning av säkerhetsrelaterade IT-incidenter

Beskrivning
Avsaknad av rutiner för uppföljning av säkerhetsrelaterade IT-incidenter. Då en incident har inträffat så finns det anledning till att utföra analys av orsaker, att ta fasta på positiva och negativa lärdomar från den egna insatsen, med mera.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Ingen utvärdering av den egna insatsen finns med i uppföjning av en incident
- Ingen utvärdering av själva grundorsaken till IT-incidenten finns med i uppföljning

Se också
4.6.23

Referenser
SS-ISO/IEC 27002:2005 kap 13.2.1 ”Ansvar och rutiner”

4.6.23 Felaktiga rutiner för uppföljning av säkerhetsrelaterade IT-incidenter

Beskrivning
Felaktiga rutiner för uppföljning av säkerhetsrelaterade IT-incidenter. Då en incident har inträffat så finns det anledning till att utföra analys av orsaker, att ta fasta på positiva och negativa lärdomar från den egna insatsen, med mera

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Ingen utvärdering av den egna insatsen finns med i uppföjning av en incident
- Ingen utvärdering av själva grundorsaken till IT-incidenten finns med i uppföljning

Se också
4.6.22

Referenser
SS-ISO/IEC 27002:2005 kap 13.2.1 ”Ansvar och rutiner”

4.6.24 Avsaknad av rutiner för gallring av information

Beskrivning
Gallring av information är formella och strukturerade sätt att ta bort information ur filer, databaser eller andra informationssamlingar. Avsaknad av rutiner för gallring kan medföra att uppgifter och information som skall tas bort, från lagkrav eller utfästelse till kunder eller för att hålla god registerkvalitet, inte blir borttagen.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Rutiner för gallring av information i kundregister saknas
- Komplexa kedjor av mellanhänder och relationer mellan elföretag och slutkund gör att det inte är klart att en kund har avslutat sitt abonnemang
- Rutiner för gallring av information i anläggningsregister saknas
- Rutiner för gallring av information i underhållssystem saknas
- Rutiner för gallring av information på servrar saknas

Se också
4.6.25

Referenser
ISO/IEC 27019:2013 kap 6.2.2 ”Addressing security when dealing with customers”

4.6.25 Felaktiga rutiner för gallring av information

Beskrivning
Gallring av information är formella och strukturerade sätt att ta bort information ur filer, databaser eller andra informationssamlingar. Felaktiga rutiner för gallring kan medföra att uppgifter och information som skall tas bort, från lagkrav eller utfästelse till kunder eller för att hålla god registerkvalitet, inte blir borttagen

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Rutiner för gallring av information i kundregister är felaktiga
- Rutiner för gallring av information i anläggningsregister är felaktiga
- Rutiner för gallring av information i underhållssystem är felaktiga
- Rutiner för gallring av information på servrar är felaktiga

Se också
4.6.24

Referenser

4.6.26 Avsaknad av rutiner för destruktion av information och informationsbärare

Beskrivning
Det saknas rutiner för destruktion av information och informationsbärare, vilket medför att information inte förstörs på ett tillämpligt sätt och att informationsbärare kan innehålla gammal information som inte skall göras tillgänglig för obehöriga.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Information finns kvar i system långt efter dess att den praktiska användbarheten av informationen är över
- Information görs tillgängliga för tredje part
- Information görs tillgängliga för obehörig intern personal

Se också
4.6.27

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.6 ”Säker avveckling eller återanvändning av utrustning”

4.6.27 Felaktiga rutiner för destruktion av information och informationsbärare

Beskrivning
Det är felaktiga rutiner för destruktion av information och informationsbärare, vilket medför att information inte förstörs på ett tillämpligt sätt och att informationsbärare kan innehålla gammal information som inte skall göras tillgänglig för obehöriga.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Information finns kvar i system långt efter dess att den praktiska användbarheten av informationen är över
- Information görs tillgängliga för tredje part
- Information görs tillgängliga för obehörig intern personal

Se också
4.6.26

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.6 ”Säker avveckling eller återanvändning av utrustning”

4.6.28 Avsaknad av rutiner för dokumentation av systemkonfiguration

Beskrivning
Det saknas rutiner för rutiner som gäller dokumentation av systemuppsättningar och systemkonfiguration. Därför blir det ingen korrekt systemdokumentation.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Dokumentation av brandväggen uppsättning saknas
- Dokumentation av filservrar uppsättning saknas
- Dokumentation över autentiseringsservrar uppsättning saknas
- Dokumentation över loggservrar uppsättning saknas

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 10.7.4 ”Säkerhet för systemdokumentation”
SS-ISO/IEC 27002:2005 kap 10.7.4 ”Revisionsloggning”

4.6.29 Avsaknad av rutin för skärmlåsning eller lösenordslåst skärmsläckare

Beskrivning
Det saknas rutiner, eller krav på, eller teknisk implementation av rutinen, att det skall finnas lösenordsskyddade skärmsläckare då man lämnar arbetsplatsen och temporärt slutar arbeta med sin dator.

I elbranschsammanhang kan det för vissa situationer och för vissa fall vara rätt att undanta vissa datorer från kravet på skärmlåsning, se ISO/IEC 27019:2013 kap 11.5.5 ”Session time-out”

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Avsaknad av rutin gör att datorer förblir olåsta, vilket i sin tur möjliggör att obehöriga kan använda datorn
- Avsaknad av rutin gör att datorer förblir olåsta, vilket i sin tur möjliggör att andra medarbetare kan smyga fram och göra saker i en annan användares namn

Se också
4.6.30

Referenser
ISO/IEC 27019:2013 kap 11.1.1 ”Access control policy”
ISO/IEC 27019:2013 kap 11.3.1 ”Password use”
ISO/IEC 27019:2013 kap 11.5.5 ”Session time-out”

4.6.30 Felaktig rutin för skärmlåsning eller lösenordslåst skärmsläckare

Beskrivning
Rutiner eller kraven på att det skall finnas lösenordsskyddade skärmsläckare då man lämnar arbetsplatsen och temporärt slutar arbeta med sin dator är felaktiga.

I elbranschsammanhang kan det för vissa situationer och för vissa fall vara rätt att undanta vissa datorer från kravet på skärmlåsning, se ISO/IEC 27019:2013 kap 11.5.5 ”Session time-out”

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar

Exempel
- De felaktiga rutinerna för lösenordslåsta skärmlås gör att datorer förblir olåsta, vilket i sin tur möjliggör att obehöriga kan använda datorn
- De felaktiga rutinerna för lösenordslåsta skärmlås gör att datorer förblir olåsta, vilket i sin tur möjliggör att andra medarbetare kan smyga fram och göra saker i en annan användares namn

Se också
4.6.29

Referenser
ISO/IEC 27019:2013 kap 11.1.1 ”Access control policy”
ISO/IEC 27019:2013 kap 11.3.1 ”Password use”
ISO/IEC 27019:2013 kap 11.5.5 ”Session time-out”

4.6.31 Avsaknad av rutin för policy/rutin Rent skrivbord och tom skärm

Beskrivning
Det saknas rutiner för s.k. policy/rutin Rent skrivbord och tom skärm (ibland kallad *clean desk policy*), att arbetsytor skall tömmas på värdefullt eller känsligt material efter arbetsdagens slut eller då man lämnar arbetsplatsen.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Avsaknad av rutin gör att lappar och dokument med affärshemligheter lämnas framme
- Avsaknad av rutin gör att dokument med nätkartor lämnas framme
- Avsaknad av rutin gör att dokument med anläggningsinformation lämnas framme
- Avsaknad av rutin gör att dokument med elproduktionsinformation lämnas framme

Se också
4.6.32

Referenser
SS-ISO/IEC 27002:2005 kap 11.3.3 ”Policy för renstädat skrivbord och tom bildskärm”

4.6.32 Felaktig rutin för policy/rutin Rent skrivbord och tom skärm

Beskrivning
Det är felaktiga rutiner för s.k. policy/rutin Rent skrivbord och tom skärm (ibland kallad *clean desk policy*), rutiner som reglerar att arbetsytor skall tömmas på värdefullt eller känsligt material efter arbetsdagens slut eller då man lämnar arbetsplatsen.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Felaktig rutin gör att lappar och dokument med affärshemligheter lämnas framme
- Felaktig rutin gör att dokument med nätkartor lämnas framme
- Felaktig rutin gör att dokument med anläggningsinformation lämnas framme
- Felaktig rutin gör att dokument med elproduktionsinformation lämnas framme

Se också
4.6.29, 4.6.33, 4.6.34

Referenser
SS-ISO/IEC 27002:2005 kap 11.3.3 ”Policy för renstädat skrivbord och tom bildskärm”

4.6.33 Avsaknad av rutin för hur whiteboards och informationsmaterial i mötesrum och andra mer allmänna platser hanteras

Beskrivning
Det saknas rutiner för hur material och information på whiteboards eller utdelat informationsmaterial skall hanteras. Detta material lämnas omedvetet eller via slarv kvar till andra personer att ta del av.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Whiteboards i sammanträdeslokaler lämnas med känslig information ritad och skriven på
- Whiteboards i kontorslokaler lämnas med känslig information ritad och skriven på

Se också
4.6.34

Referenser
SS-ISO/IEC 27002:2005 kap 11.3.3 ”Policy för renstädat skrivbord och tom bildskärm”

4.6.34 Felaktig rutin för hur whiteboards och informationsmaterial i mötesrum och andra öppna utrymmen hanteras

Beskrivning
Det är felaktiga rutiner för hur material och information på whiteboards eller utdelat informationsmaterial skall hanteras. Detta material lämnas omedvetet eller via slarv kvar till andra personer att ta del av

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Whiteboards i sammanträdeslokaler lämnas med känslig information ritad och skriven på
- Whiteboards i kontorslokaler lämnas med känslig information ritad och skriven på

Se också
4.6.33

Referenser
SS-ISO/IEC 27002:2005 kap 11.3.3 ”Policy för renstädat skrivbord och tom bildskärm”

4.6.35 Avsaknad av rutin för hur datorskärmar och informationsbärare placeras i utrymmen med yttre insyn

Beskrivning
Det saknas rutiner för hur datorskärar och andra informationsbärare skall placeras i utrymmen med yttre insyn. Denna avsaknad medför risk att externa parter kan se känslig information.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Skärmar placeras så att det går att se dem från utsidan av fastigheter eller anläggningar via fönster
- Projektordukar för OH-projekteror är placerade så att det går att se innehåll på dem från utsidan av fastigheter eller anläggningar via fönster
- Storbildsskärmar är placerade så att det går att se innehåll på dem från utsidan av fastigheter eller anläggningar via fönster

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 11.3.3 ”Policy för renstädat skrivbord och tom bildskärm”

4.6.36 Avsaknad av rutin för besökshantering

Beskrivning
Hantering av besök och externa personers tillträde till lokaler är ett eget område som kräver en viss eftertanke. Det bör tas fram genomtänkta rutiner för vem som får anmäla besök, hur besök får ske, var och när externa får besöka utrymme, anläggningar, fastigheter eller liknande.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Besök får bara anmälas av vissa personer, exempelvis anställd personal men inte av konsulter eller temporäranställda
- Besök får inte ske till alla typer av utrymmen
- Besök får inte ske utöver ordinarie arbetstid

Se också
4.6.37

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.2 ”Tillträdeskontroll”

4.6.37 Felaktig rutin för besökshantering

Beskrivning
Hantering av besök och externa personers tillträde till lokaler är ett eget område som kräver en viss eftertanke. Om det inte tas fram genomtänkta rutiner för vem som får anmäla besök, hur besök får ske, var och när externa får besöka utrymme, anläggningar, fastigheter eller liknande, så finns det risk att dessa rutiner blir felaktiga.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Felaktigheterna består i att vem som helst får anmäla besök
- Felaktigheterna består i att vem som helst får besöka alla typer av utrymmen

Se också
4.6.36

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.2 ”Tillträdeskontroll”

4.6.38 Avsaknad av rutin för brandsyn

Beskrivning
Organisationen bör ha genomtänkta och väl utformade rutiner för regelbunden brandsyn av lokaler, anläggningar, fastigheter med mera.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Avsaknad av brandsyn gör att det ansamlas kartonger i datorhallar och IT-driftsutrymmen
- Avsaknad av brandsyn gör att de brandsläckare som finns utplacerade inte är godkända
- Avsaknad av brandsyn gör att de brandsläckare som finns utplacerade inte är korrekta för den verksamhet som bedrivs i de lokaler de är placerade i
- Avsaknad av brandsyn gör att det inte finns rök- eller branddetektorer i lokaler där dessa borde vara placerade

Se också
4.6.39

Referenser

4.6.39 Felaktig rutin för brandsyn

Beskrivning
Organisationen bör ha genomtänkta och väl utformade rutiner för regelbunden brandsyn av lokaler, anläggningar, fastigheter med mera. Felaktig rutin eller rutiner för brandsyn kan leda till att det ändå uppstår fara för bränder eller att de brandskydd som anskaffats inte är verkningsfulla.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Felaktiga rutiner för brandsyn gör att det ansamlas kartonger i datorhallar och IT-driftsutrymmen
- Felaktiga rutiner för brandsyn gör att de brandsläckare som finns utplacerade inte är godkända
- Felaktiga rutiner för brandsyn gör att de brandsläckare som finns utplacerade inte är korrekta för den verksamhet som bedrivs i de lokaler de är placerade i
- Felaktiga rutiner för brandsyn gör att det inte finns rök- eller branddetektorer i lokaler där dessa borde vara placerade

Se också
4.6.38

Referenser

4.7 Klassning och analys

Detta kapitel avhandlar hot mot klassning av information och system. Med klassning menas i detta dokument informationsklassning respektive systemklassning.

4.7.1 Avsaknad av informationsklassning

Beskrivning
Med informationsklassning menas här klassning eller klassificering av en organisations information eller informationsresurser utifrån sekretess, riktighet och tillgänglighet baserat på den egna organisationens modeller, principer, metoder och verktyg. För vissa typer av organisationer såsom myndigheter och kommuner anges det i lagar, förordningar eller andra juridiska kravdokument fast att viss typ av information skall omfattas av sekretess.

Avsaknad av informationsklassning kan bero på att organisationen inte har en klassningsmodell på plats, att principerna inte är kommunicerade, att det saknas metoder och verktyg i verksamheten för att underlätta eller göra det praktiskt möjligt för medarbetare att klassificera information.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Avsaknad av informationsklassning av informationen i ett nationellt SCADA-system
- Avsaknad av informationsklassning av informationen i ett GIS-system som används för nätplanering
- Avsaknad av informationsklassning av informationen i ett anläggningsregister som beskriver all utrustning och funktion hos de olika fysiska anläggningarna som används inom verksamheten
- Avsaknad av informationsklassning av informationen i kontorsautomationssystem för elektronisk post (e-mail)
- Avsaknad av informationsklassning av informationen i ett ärendehanteringssystem som hanterar kundtjänstärenden

Se också
4.7.2, 4.7.3, 4.7.4

Referenser
SS-ISO/IEC 27002:2005 kap 7.2 ”Klassificering av information”
SS-ISO/IEC 27002:2005 kap 7.2.1 ”Riktlinjer för klassificering”
SS-ISO/IEC 27002:2005 kap 7.2.2 ”Märkning och hantering av information”

4.7.2 Avsaknad av rutin för informationsklassning

Beskrivning
Med informationsklassning menas här klassning eller klassificering av en organisations information eller informationsresurser utifrån sekretess, riktighet och tillgänglighet baserat på den egna organisationens modeller, principer, metoder och verktyg. För vissa typer av organisationer såsom myndigheter och kommuner anges det i lagar, förordningar eller andra juridiska kravdokument fast att viss typ av information skall omfattas av sekretess.

Avsaknad av informationsklassning kan bero på att organisationen inte har en klassningsmodell på plats, att principerna inte är kommunicerade, att det saknas metoder och verktyg i verksamheten för att underlätta eller göra det praktiskt möjligt för medarbetare att klassificera information.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Avsaknad av informationsklassning av informationen i ett nationellt SCADA-system
- Avsaknad av informationsklassning av informationen i ett GIS-system som används för nätplanering
- Avsaknad av informationsklassning av informationen i ett anläggningsregister som beskriver all utrustning och funktion hos de olika fysiska anläggningarna som används inom verksamheten
- Avsaknad av informationsklassning av informationen i kontorsautomationssystem för elektronisk post (e-mail)
- Avsaknad av informationsklassning av informationen i ett ärendehanteringssystem som hanterar kundtjänstärenden

Se också
4.7.1, 4.7.3, 4.7.4

Referenser
SS-ISO/IEC 27002:2005 kap 7.2 ”Klassificering av information”
SS-ISO/IEC 27002:2005 kap 7.2.1 ”Riktlinjer för klassificering”
SS-ISO/IEC 27002:2005 kap 7.2.2 ”Märkning och hantering av information”
ISO/IEC 27019:2013 kap 6.1.6 ”Contact with authorities”

4.7.3 Felaktig informationsklassning

Beskrivning
Med informationsklassning menas här klassning eller klassificering av en organisations information eller informationsresurser utifrån sekretess, riktighet och tillgänglighet baserat på den egna organisationens modeller, principer, metoder och verktyg. För vissa typer av organisationer såsom myndigheter och kommuner anges det i lagar, förordningar eller andra juridiska kravdokument fast att viss typ av information skall omfattas av sekretess..

Med *felaktig informationsklassning* avser resultatet av själva informationsklassningsaktiviteten. Dessutom kan det förekomma *felaktiga rutiner för informationsklassning*, vilket avser fel i själva klassningsaktiviteten

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Felaktig informationsklassning av informationen i ett nationellt SCADA-system
- Felaktig informationsklassning av informationen i ett GIS-system som används för nätplanering
- Felaktig informationsklassning av informationen i ett anläggningsregister som beskriver all utrustning och funktion hos de olika fysiska anläggningarna som används inom verksamheten
- Felaktig informationsklassning av informationen i kontorsautomationssystem för elektronisk post (e-mail)
- Felaktig informationsklassning av informationen i ett ärendehanteringssystem som hanterar kundtjänstärenden

Se också
4.7.1, 4.7.2, 4.7.4

Referenser
SS-ISO/IEC 27002:2005 kap 7.2 ”Klassificering av information”
SS-ISO/IEC 27002:2005 kap 7.2.1 ”Riktlinjer för klassificering”
SS-ISO/IEC 27002:2005 kap 7.2.2 ”Märkning och hantering av information”
ISO/IEC 27019:2013 kap 6.1.6 ”Contact with authorities”

4.7.4 Felaktig rutin för informationsklassning

Beskrivning
Med informationsklassning menas här klassning eller klassificering av en organisations information eller informationsresurser utifrån sekretess, riktighet och tillgänglighet baserat på den egna organisationens modeller, principer, metoder och verktyg. För vissa typer av organisationer såsom myndigheter och kommuner anges det i lagar, förordningar eller andra juridiska kravdokument fast att viss typ av information skall omfattas av sekretess.
.

Med *felaktiga rutiner för informationsklassning* avses fel i själva klassningsaktiviteten. Dessutom förekommer *felaktig informationsklassning, vilket* avser resultatet av själva informationsklassnings-aktiviteten.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Felaktig informationsklassning av informationen i ett nationellt SCADA-system på grund av felaktiga rutiner vid klassningen
- Felaktig informationsklassning av informationen i ett GIS-system som används för nätplanering på grund av felaktiga rutiner vid klassningen
- Felaktig informationsklassning av informationen i ett anläggningsregister som beskriver all utrustning och funktion hos de olika fysiska anläggningarna som används inom verksamheten på grund av felaktiga rutiner vid klassningen
- Felaktig informationsklassning av informationen i kontorsautomationssystem för elektronisk post (e-mail) på grund av felaktiga rutiner vid klassningen
- Felaktig informationsklassning av informationen i ett ärendehanteringssystem som hanterar kundtjänstärenden på grund av felaktiga rutiner vid klassningen

Se också
4.7.1, 4.7.2, 4.7.3

Referenser
SS-ISO/IEC 27002:2005 kap 7.2 ”Klassificering av information”
SS-ISO/IEC 27002:2005 kap 7.2.1 ”Riktlinjer för klassificering”
SS-ISO/IEC 27002:2005 kap 7.2.2 ”Märkning och hantering av information”

4.7.5 Avsaknad av systemklassning

Beskrivning
Med systemklassning menar vi här att system är identifierade, beskrivna och bedömda enligt en klassningsmodell utifrån systemets olika egenskaper och verksamhetens krav på systemet. Arbetet med att införa och underhålla de skydd som behövs enligt den systemklassningsnivå som bestämts finns beskrivna i systemets förvaltningsplan.

Systemägare eller systemförvaltare som ansvarar för att det sker en systemklassning.

Avsaknad av systemklassning kan bero på att organisationen inte har en klassningsmodell på plats, att principerna inte är kommunicerade, att det saknas metoder och verktyg i verksamheten för att underlätta eller göra det praktiskt möjligt för medarbetare att klassificera system.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Ett nationellt SCADA-system som saknar systemklassning
- Ett processkontrollssystem i en anläggning för eldistribution som inte är klassat ur ett systemklassningsperspektiv.
- IT-infrastrukturutrustning (nätverkskomponenter) som är kritisk för att en tjänst skall fungera är inte systemklassad, har ingen systemägare, ingen förvaltningsplan etc.

Se också
4.7.6, 4.7.7

Referenser
SS-ISO/IEC 27002:2005 kap 7.1 ”Ansvar för tillgångar”
SS-ISO/IEC 27002:2005 kap 7.1.1 ”Förteckning över tillgångar”
SS-ISO/IEC 27002:2005 kap 7.1.2 ”Ägarskap för tillgångar”
SS-ISO/IEC 27002:2005 kap 7.1.3 ”Godtagbar användning av tillgångar”
ISO/IEC 27019:2013 kap 7.1.1 ”Inventory of assets”

4.7.6 Felaktig systemklassning

Beskrivning
Med systemklassning menar vi här att system är identifierade, beskrivna och bedömda enligt en klassningsmodell utifrån systemets olika egenskaper och verksamhetens krav på systemet. Arbetet med att införa och underhålla de skydd som behövs enligt den systemklassningsnivå som bestämts finns beskrivna i systemets förvaltningsplan.

Systemägare eller systemförvaltare som ansvarar för att det sker en systemklassning.

Felaktig systemklassning kan bero på att organisationen inte har en klassningsmodell på plats, att principerna inte är kommunicerade, att det saknas metoder och verktyg i verksamheten för att underlätta eller göra det praktiskt möjligt för medarbetare att klassificera system.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Ett nationellt SCADA-system har en felaktigt systemklassning
- Ett processkontrollssystem i en anläggning för eldistribution som blivit felaktigt klassat ur ett systemklassningsperspektiv.
- IT-infrastrukturutrustning (nätverkskomponenter) som är kritisk för att en tjänst skall fungera har fått en felaktig systemklassning

Se också
4.7.5, 4.7.7

Referenser
SS-ISO/IEC 27002:2005 kap 7.1 ”Ansvar för tillgångar”
SS-ISO/IEC 27002:2005 kap 7.1.1 ”Förteckning över tillgångar”
SS-ISO/IEC 27002:2005 kap 7.1.2 ”Ägarskap för tillgångar”
SS-ISO/IEC 27002:2005 kap 7.1.3 ”Godtagbar användning av tillgångar”
ISO/IEC 27019:2013 kap 7.1.1 ”Inventory of assets”

4.7.7 Felaktiga rutiner för systemklassning

Beskrivning
Med systemklassning menar vi här att system är identifierade, beskrivna och bedömda enligt en klassningsmodell utifrån systemets olika egenskaper och verksamhetens krav på systemet. Arbetet med att införa och underhålla de skydd som behövs enligt den systemklassningsnivå som bestämts finns beskrivna i systemets förvaltningsplan.

Systemägare eller systemförvaltare som ansvarar för att det sker en systemklassning.

Felaktiga rutiner systemklassning kan bero på att organisationen inte har en klassningsmodell på plats, att principerna inte är kommunicerade, att det saknas metoder och verktyg i verksamheten för att underlätta eller göra det praktiskt möjligt för medarbetare att klassificera system.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Ett nationellt SCADA-system har en felaktigt systemklassning som följd av felaktiga rutiner för systemklassning.
- Ett processkontrollssystem i en anläggning för eldistribution som blivit felaktigt klassat ur ett systemklassningsperspektiv som följd av felaktiga rutiner för systemklassning.
- IT-infrastrukturutrustning (nätverkskomponenter) som är kritisk för att en tjänst skall fungera har fått en felaktig systemklassning som följd av felaktiga rutiner för systemklassning.

Se också
4.7.5, 4.7.6

Referenser
SS-ISO/IEC 27002:2005 kap 7.1 ”Ansvar för tillgångar”
SS-ISO/IEC 27002:2005 kap 7.1.1 ”Förteckning över tillgångar”
SS-ISO/IEC 27002:2005 kap 7.1.2 ”Ägarskap för tillgångar”
SS-ISO/IEC 27002:2005 kap 7.1.3 ”Godtagbar användning av tillgångar”
ISO/IEC 27019:2013 kap 7.1.1 ”Inventory of assets”

4.7.8 Avsaknad av riskanalys

Beskrivning
Organisationer bör utföra systematiska riskbedömningar för att identifiera, kvantifiera och prioritera olika risker mot kriterier för accepterade nivåer av risker och mål som är relevanta för organisationen. Resultaten från dessa riskbedömningar bör vägleda och avgöra lämpliga åtgärder och prioriteringar från ledningens sida i syfte att hantera informationssäkerhetsrisker och för att införa säkerhetsåtgärder utvalda som skydd mot dessa risker. Systematisk riskbedömning bör innefatta ett sätt att uppskatta riskernas omfattning, så kallad riskanalys.

Avsaknad av riskanalys kan bero på att organisationen inte har en riskanalysmodell på plats, att principerna för hur eller när en riskanalys skall utföras inte är kommunicerade, att det saknas metoder och verktyg i verksamheten för att underlätta eller göra det praktiskt möjligt för medarbetare att utföra riskanalys.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Ett införandeprojektet har missat att utföra riskanalys på en nybyggd anläggning, inklusive de automationssystem och processkontrollsystem som finns där
- Linjeverksamheten har inte utfört riskanalys av det centrala SCADA-systemet
- Linjeverksamheten har inte utfört riskanalys av infrastruktur för nätverk och centrala IT-tjänster som är nödvändiga för processkontrollsystem.

Se också
4.7.9

Referenser
SS-ISO/IEC 27002:2005 kap 4.1 ”Bedömning av säkerhetsrisker”

4.7.9 Felaktig riskanalys

Beskrivning
Organisationer bör utföra systematiska riskbedömningar för att identifiera, kvantifiera och prioritera olika risker mot kriterier för accepterade nivåer av risker och mål som är relevanta för organisationen. Resultaten från dessa riskbedömningar bör vägleda och avgöra lämpliga åtgärder och prioriteringar från ledningens sida i syfte att hantera informationssäkerhetsrisker och för att införa säkerhetsåtgärder utvalda som skydd mot dessa risker. Systematisk riskbedömning bör innefatta ett sätt att uppskatta riskernas omfattning, så kallad riskanalys.

Felaktigt utförda riskanalyser kan bero på att organisationen inte har en riskanalysmodell på plats, att principerna för hur eller när en riskanalys skall utföras inte är kommunicerade, att det saknas metoder och verktyg i verksamheten för att underlätta eller göra det praktiskt möjligt för medarbetare att utföra riskanalys.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Ett införandeprojektet har utfört riskanalys på en nybyggd anläggning, inklusive de automationssystem och processkontrollsystem som finns där, men har inte fått med väsentliga hot och sårbarheter.
- Linjeverksamheten har utfört felaktig riskanalys av det centrala SCADA-systemet.
- Linjeverksamheten har utfört felaktig riskanalys av infrastruktur för nätverk och centrala IT-tjänster som är nödvändiga för processkontrollsystem.

Se också
4.7.8

Referenser
SS-ISO/IEC 27002:2005 kap 4.1 ”Bedömning av säkerhetsrisker”

4.8 Kontinuitetshantering och krishantering

Kontinuitetshantering kallas ibland för krishantering, katastrofhantering eller BCP, business continuity planning.

Detta kapitel avhandlar olika aspekter av hot mot krishantering, bla

- Avsaknad av kontinuitetsplanering
- Felaktig kontinuitetsplanering
- Ej övad kontinuitetsplanering

4.8.1 Avsaknad av kontinuitetsplanering

Beskrivning
Kontinuitetsplanering är planering för att en verksamhet skall kunna fortgå även om kriser och allvarligare incidenter inträffar. Det är därför viktigt att organisationen har utfört och utvecklat krisplaner.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Avsaknad av processer och rutiner för att hantera kriser
- Avsaknad av en strategi för hur verksamhetens kontinuitet skall fortgå i samband med störningar, kriser och allvarligare incidenter

Se också
4.8.2, 4.8.3, 4.8.4, 4.8.5

Referenser
SS-ISO/IEC 27002:2005 kap 14.1.1 ”Att inkludera informationssäkerhet i verksamhetens kontinuitetsplaneringsprocess”
SS-ISO/IEC 27002:2005 kap 14.1.2 ”Kontinuerlig verksamhet och riskbedömning”
SS-ISO/IEC 27002:2005 kap 14.1.3 ”Utveckling och införande av kontinuitetsplaner innefattande informationssäkerhet”
SS-ISO/IEC 27002:2005 kap 14.1.4 ”Ramverk för kontinuitetsplanering i verksamheten”
SS-ISO/IEC 27002:2005 kap 14.1.5 ”Test, underhåll och omprövning av kontinuitetsplaner”
ISO/IEC 27019:2013 kap 14.1.1 ”Including information security in the business continuity management process”

4.8.2 Felaktig kontinuitetsplanering

Beskrivning
Kontinuitetsplanering är planering för att en verksamhet skall kunna fortgå även om kriser och allvarligare incidenter inträffar. Det är därför viktigt att organisationen har utfört och utvecklat realistiska, fungerande och korrekta krisplaner

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Felaktiga processer och rutiner för att hantera kriser
- Felaktig strategi för hur verksamhetens kontinuitet skall fortgå i samband med störningar, kriser och allvarligare incidenter

Se också
4.8.1, 4.8.3, 4.8.4, 4.8.5

Referenser
SS-ISO/IEC 27002:2005 kap 14.1.1 ”Att inkludera informationssäkerhet i verksamhetens kontinuitetsplaneringsprocess”
SS-ISO/IEC 27002:2005 kap 14.1.2 ”Kontinuerlig verksamhet och riskbedömning”
SS-ISO/IEC 27002:2005 kap 14.1.3 ”Utveckling och införande av kontinuitetsplaner innefattande informationssäkerhet”
SS-ISO/IEC 27002:2005 kap 14.1.4 ”Ramverk för kontinuitetsplanering i verksamheten”
SS-ISO/IEC 27002:2005 kap 14.1.5 ”Test, underhåll och omprövning av kontinuitetsplaner”
ISO/IEC 27019:2013 kap 14.1.1 ”Including information security in the business continuity management process”

4.8.3 Ej uppdaterad kontinuitetsplanering

Beskrivning
Kontinuitetsplanering är planering för att en verksamhet skall kunna fortgå även om kriser och allvarligare incidenter inträffar. Det är därför viktigt att organisationen har utfört och utvecklat krisplaner som är uppdaterade och i takt med nuvarande verksamhet, placering av verksamheten och omfattning av verksamheten.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- De processer och rutiner för att hantera kriser är inte uppdaterade att reflektera verksamhetens art, omfattning eller inriktning
- Den strategi som finns för hur verksamhetens kontinuitet skall fortgå i samband med störningar, kriser och allvarligare incidenter är inte uppdaterade att reflektera verksamhetens art, omfattning eller inriktning

Se också
4.8.1, 4.8.2, 4.8.4, 4.8.5

Referenser
SS-ISO/IEC 27002:2005 kap 14.1.1 ”Att inkludera informationssäkerhet i verksamhetens kontinuitetsplaneringsprocess”
SS-ISO/IEC 27002:2005 kap 14.1.2 ”Kontinuerlig verksamhet och riskbedömning”
SS-ISO/IEC 27002:2005 kap 14.1.3 ”Utveckling och införande av kontinuitetsplaner innefattande informationssäkerhet”
SS-ISO/IEC 27002:2005 kap 14.1.4 ”Ramverk för kontinuitetsplanering i verksamheten”
SS-ISO/IEC 27002:2005 kap 14.1.5 ”Test, underhåll och omprövning av kontinuitetsplaner”
ISO/IEC 27019:2013 kap 14.1.1 ”Including information security in the business continuity management process”

4.8.4 Ej övad kontinuitetsplanering

Beskrivning
Kontinuitetsplanering är planering för att en verksamhet skall kunna fortgå även om kriser och allvarligare incidenter inträffar. Det är därför viktigt att organisationen övar krisplaner som är uppdaterade och i takt med nuvarande verksamhet, placering av verksamheten och omfattning av verksamheten

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- De processer och rutiner som finns i kontinuitetsplaneringen kommer inte fungera i verkligheten då ingen känner till dem närmare, då detta inte är övat
- De processer och rutiner som finns i kontinuitetsplaneringen kommer inte fungera i verkligheten då det finns oklarheter för vem de egentligen gäller och vem som har vilken roll i själva kontinuitetshanteringen, då detta inte är övat

Se också
4.8.1, 4.8.2, 4.8.3, 4.8.5

Referenser
SS-ISO/IEC 27002:2005 kap 14.1.1 ”Att inkludera informationssäkerhet i verksamhetens kontinuitetsplaneringsprocess”
SS-ISO/IEC 27002:2005 kap 14.1.2 ”Kontinuerlig verksamhet och riskbedömning”
SS-ISO/IEC 27002:2005 kap 14.1.3 ”Utveckling och införande av kontinuitetsplaner innefattande informationssäkerhet”
SS-ISO/IEC 27002:2005 kap 14.1.4 ”Ramverk för kontinuitetsplanering i verksamheten”
SS-ISO/IEC 27002:2005 kap 14.1.5 ”Test, underhåll och omprövning av kontinuitetsplaner”
ISO/IEC 27019:2013 kap 14.1.1 ”Including information security in the business continuity management process”

4.8.5 Ej efterlevnad av kontinuitetsplaner

Beskrivning
I händelse med kris och allvarligare incident, eller för att förebygga kriser och allvarligare incidenter, så inte följer organisationen och de som är utsedda att vara krisledning den eller de planer som är uppgjorda. Detta leder till mindre strukturerad hantering, förvirring i organisationen och sämre hanterad kris eller incident.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Enligt krisplaner får inte hela företagsledningen dela färdmedel vid tex konferensresa. Detta följs inte då man chartrat ett helt flygplan för stora delar av företaget, för att spara reskostnader.
- Nyckelpersoner följer inte de förebyggande krishantering som finns i krisplanerna

Se också
4.8.1, 4.8.2, 4.8.3, 4.8.4

Referenser
SS-ISO/IEC 27002:2005 kap 14.1.1 ”Att inkludera informationssäkerhet i verksamhetens kontinuitetsplaneringsprocess”
SS-ISO/IEC 27002:2005 kap 14.1.2 ”Kontinuerlig verksamhet och riskbedömning”
SS-ISO/IEC 27002:2005 kap 14.1.3 ”Utveckling och införande av kontinuitetsplaner innefattande informationssäkerhet”
SS-ISO/IEC 27002:2005 kap 14.1.4 ”Ramverk för kontinuitetsplanering i verksamheten”
SS-ISO/IEC 27002:2005 kap 14.1.5 ”Test, underhåll och omprövning av kontinuitetsplaner”
ISO/IEC 27019:2013 kap 14.1.1 ”Including information security in the business continuity management process”

4.9 Uppföljning, intern och extern kontroll

Detta kapitel avhandlar olika aspekter av hot mot områdena uppföljning, intern kontroll, extern kontroll.

4.9.1 Avsaknad av testning och kvalitetskontroll

Beskrivning
Uppföljning kan genomföras med testning och kvalitetskontroll. Det saknas rutiner och processer för att utföra testning eller kvalitetskontroller.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Det utförs inte acceptanstester i samband med leverans
- Det utförs inte tester av beställda elektroniska tjänster
- Det sker ingen slumpmässig kvalitetskontroll av levererade tjänster

Se också
4.9.2

Referenser
SS-ISO/IEC 27002:2005 kap 10.1.2 ”Ändringshantering”
SS-ISO/IEC 27002:2005 kap 12.4.2 ”Skydd av testdata”
SS-ISO/IEC 27002:2005 kap 12.5 ”Säkerhet i utvecklings- och underhållsprocesser”
ISO/IEC 27019:2013 kap 12.4.1 ”Control of operational software”

4.9.2 Otillräcklig testning och kvalitetskontroll

Beskrivning
Uppföljning kan genomföras med testning och kvalitetskontroll. Det genomförs otillräckliga tester testning eller kvalitetskontroller.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Det utförs inte tillräckliga acceptanstester i samband med leverans
- Det utförs inte tillräckliga tester av beställda elektroniska tjänster
- Det sker inte tillräckligt många slumpmässig kvalitetskontroll av levererade tjänster

Se också
4.9.1

Referenser
SS-ISO/IEC 27002:2005 kap 10.1.2 ”Ändringshantering”
SS-ISO/IEC 27002:2005 kap 12.4.2 ”Skydd av testdata”
SS-ISO/IEC 27002:2005 kap 12.5 ”Säkerhet i utvecklings- och underhållsprocesser”
ISO/IEC 27019:2013 kap 12.4.1 ”Control of operational software”

4.9.3 Avsaknad av uppföljning och/eller kontroll

Beskrivning
Det sker ingen systematisk och strukturerad uppföljning och kontroll, vilket skulle kunna användas för att upptäcka brister i processer, brister i rutiner, kvalitetsbrister i utförda tjänster, kvalitetsbrister i levererade tjänster

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel

- Inga tekniska säkerhetstester
- Inga utredningar av behörighetsstrukturer
- Ingen uppföljning av hur väl styrdokument följs
- Inga uppföljning av statistik från skydd- och säkerhetsfunktioner såsom antivirusprogram, brandväggar, behörighetssystem

Se också
4.9.4

Referenser
SS-ISO/IEC 27002:2005 kap 13.2.1 ”Ansvar och rutiner”

4.9.4 Otillräcklig uppföljning och/eller kontroll

Beskrivning
Det sker ingen systematisk och strukturerad uppföljning och kontroll i rätt omfattning, vilket skulle kunna användas för att upptäcka brister i processer, brister i rutiner, kvalitetsbrister i utförda tjänster, kvalitetsbrister i levererade tjänster

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel

- Inte tillräckliga, eller tillräckligt förekommande, tekniska säkerhetstester
- Inte tillräckliga, eller tillräckligt förekommande utredningar av behörighetsstrukturer
- Inte tillräckliga, eller tillräckligt förekommande uppföljning av hur väl styrdokument följs
- Inte tillräckliga, eller tillräckligt förekommande uppföljning av statistik från skydd- och säkerhetsfunktioner såsom antivirusprogram, brandväggar, behörighetssystem

Se också
4.9.3

Referenser
SS-ISO/IEC 27002:2005 kap 13.2.1 ”Ansvar och rutiner”

4.10 Ansvar och roller

Detta avsnitt handlar om det ansvar och de roller som delas ut i en organisation och de hot som är associerade med dessa.

4.10.1 Ej utdelat ansvar

Beskrivning
Det har ej delats ut formellt ansvar i den omfattning som behövs för att organisationen skall kunna fungera effektivt.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Eftersom ansvar inte blivit formellt utdelat så sker det en massa aktiviteter av personal utan att de fått det formella ansvaret att utföra dessa moment
- Eftersom ansvar inte blivit formellt utdelat vet personer inte vem som har det egentliga ansvaret för att vissa moment skall utföras

Se också
4.10.2, 4.10.3

Referenser
SS-ISO/IEC 27002:2005 kap 6.1.1 ”Ledningens engagemang för informationssäkerhet”
SS-ISO/IEC 27002:2005 kap 6.1.3 ”Tilldelning av ansvar för informationssäkerhet”
SS-ISO/IEC 27002:2005 kap 13.2.1 ”Ansvar och rutiner”

4.10.2 Oklara ansvarsförhållanden

Beskrivning
Det ansvar som delats ut till vissa roller är ej fastlagt, ej dokumenterat eller ej kommunicerat i organisationen. Därför uppstår det oklarheter rörande omfattning av ansvar, ansvarsförhållande och liknande.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Ej dokumenterade roller
- Ej dokumenterade omfattning av ansvar
- Ej kommunicerade roller och ansvarsförhållanden

Se också
4.10.1, 4.10.3

Referenser
SS-ISO/IEC 27002:2005 kap 6.1.1 ”Ledningens engagemang för informationssäkerhet”
SS-ISO/IEC 27002:2005 kap 6.1.3 ”Tilldelning av ansvar för informationssäkerhet”
SS-ISO/IEC 27002:2005 kap 13.2.1 ”Ansvar och rutiner”

4.10.3 Delade ansvarsförhållanden

Beskrivning
Flera personer kan ha flera en roll och därmed också delat ansvar. Detta kan leda till flera situationer som är problematiska för organisationen.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Tillikabefattningar som innefattar både kravställande roller (tex säkerhetschef) och utförande roller (tex IT-chef) där deras olika roller kan vara i konflikt med varandra
- Ansvarsförhållanden kan vara uppdelade så att vissa ansvarsområden missas, eftersom de som delar på ansvaret inte är klara med vad den som de delar med gjort eller inte gjort

Se också
4.10.1, 4.10.2

Referenser
SS-ISO/IEC 27002:2005 kap 6.1.1 ”Ledningens engagemang för informationssäkerhet”
SS-ISO/IEC 27002:2005 kap 6.1.3 ”Tilldelning av ansvar för informationssäkerhet”
SS-ISO/IEC 27002:2005 kap 13.2.1 ”Ansvar och rutiner”

4.10.4 Felaktiga behörighetstilldelningar

Beskrivning
De behörigheter som är utdelade är felaktiga, oftast med för breda och tillåtande rättigheter, gör att personer kan utföra aktiviteter, komma åt information och resurser på ett sådant sätt som de med en mer korrekt och strikt behörighet.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, tidsbrist, taktiskt spel med avseende på kostnadsbesparingar

Exempel
- Samma konton delas av flera användare
- Alltför breda behörigheter delas ut till de personer som får systemåtkomst

Se också
4.10.5, 4.10.6

Referenser
SS-ISO/IEC 27002:2005 kap 10.1.3 ”Uppdelning av arbetsuppgifter”
SS-ISO/IEC 27002:2005 kap 10.9.2 ”Direktanslutna transaktioner”
SS-ISO/IEC 27002:2005 kap 11 ”Styrning av åtkomst”

4.10.5 Gruppkonton

Beskrivning
Ett användarkonto i ett datorsystem som på förhand skapats för att en grupp av människor skall dela på kontot och därmed åtkomst till datorsystemet.

Ett problem med att använda gruppkonton istället för personliga konton är att spårbarhet saknas. Ett annat problem med att använda gruppkonton istället för personliga konton är att behörigheten på det delade kontot kan ha för bred behörighet saknas.

Kategori
Administrativt hot, internt hot

Orsak/Aktör
Felaktig styrning av behörigheter i IT-system, handhavandelfel

Exempel
- Funktionskonto för operatörer i en driftcentral/ett kontrollrum där man delar på samma kontonamn när man loggar in i SCADA-systemet.
- Funktionskonto för leverantörer i en driftcentral/ett kontroll där man delar på samma kontonamn när man loggar in i SCADA-systemet.
- Delat konto som används för åtkomst till fältutrustning såsom PLC, RTU och liknande är delat av alla som behöver åtkomst till utrustningen.

Se också
4.10.4, 4.10.6

Referenser
SS-ISO/IEC 27002:2005 kap 10.1.3 ”Uppdelning av arbetsuppgifter”
SS-ISO/IEC 27002:2005 kap 10.9.2 ”Direktanslutna transaktioner”
SS-ISO/IEC 27002:2005 kap 11 ”Styrning av åtkomst”
ISO/IEC 27019:2013 kap 9.1.7 ”Securing control centers”

4.10.6 Delade konton i datorsystem

Beskrivning
Ett användarkonto i ett datorsystem som delas av en grupp av människor och därmed delar åtkomst till datorsystemet under ett och samma användaridentitet.
Ett problem med att använda delade istället för personliga konton är att spårbarhet saknas. Ett annat problem med att använda delade konton istället för personliga konton är att behörigheten på det delade kontot kan ha för bred behörighet saknas.

Kategori
Administrativt hot, internt hot

Orsak/Aktör
Felaktig styrning av behörigheter i IT-system, handhavandelfel

Exempel
- En chef vars sekreterare eller assistent kan logga in som chefen, då denne delat med sig av sitt kontonamn och lösenord
- För inloggning till datorer i driftcentralen eller ett kontroll används ett och samma användarkonto. Detta konto är alltid inloggat och delas av alla de personer som jobbar i driftcentralen eller kontrollrumet.

Se också
4.10.4, 4.10.5

Referenser
SS-ISO/IEC 27002:2005 kap 11.2 ”Styrning av användares rättigheter”
ISO/IEC 27019:2013 kap 9.1.7 ”Securing control centers”
ISO/IEC 27019:2013 kap 11.1.1 ”Access control policy”
ISO/IEC 27019:2013 kap 11.3.1 ”Password use”

4.10.7 Avsaknad av systemägare

Beskrivning
Enligt många förvaltningsmodeller inom organisationer så skall det finnas formellt utsedda systemägare för de informationssystem som organisationen har för att skapa och hantera information inom organisationen. Detta systemägarskap innefattar vissa krav på den utsedde personen, exempelvis att denne har ett visst mått av ansvar för systemet. Ett särskilt hot är att organisationen inte har formellt utpekade systemägare.

Kategori
Organisatoriskt hot, internt hot

Orsak/Aktör
Felaktig ledning och styrning av organisationens resurser

Exempel
- Ett IT-system inom industriell processkontroll, tex i en driftcentral, har inte någon formellt utsedd ägare, vilket gör att förvaltning inte sköts aktivt.
- Infrastrukturkomponenter, exempelvis nätverksutrustning eller nätverkstjänster såsom tidsserver, saknar systemägare för att de inte identifierats som ”system” enligt en intern klassificering.

Se också
4.10.8

Referenser
SS-ISO/IEC 27002:2005 kap 7.1 ”Ansvar för tillgångar”
ISO/IEC 27019:2013 kap 7.1.2 ”Ownership of assets”

4.10.8 Systemägare som inte känner till sitt ansvar

Beskrivning
Enligt många förvaltningsmodeller inom organisationer så skall det finnas formellt utsedda systemägare för de informationssystem som organisationen har för att skapa och hantera information inom organisationen. Detta systemägarskap innefattar vissa krav på den utsedde personen, exempelvis att denne har ett visst mått av ansvar för systemet. Ett särskilt hot är att utpekade systemägare inom en organisation inte känner till vad denna roll medför för ansvar och mandat.

Kategori
Organisatoriskt hot, administrativt hot, internt hot

Orsak/Aktör
Felaktig ledning och styrning av organisationens resurser

Exempel
- processkontrollsystemets utsedda systemägare känner inte till vad systemägarskapet innebär och har därför inte kravställt korrekt vid det förändringsarbete som görs i systemet.

Se också
4.10.7

Referenser
SS-ISO/IEC 27002:2005 kap 7.1 ”Ansvar för tillgångar”
ISO/IEC 27019:2013 kap 7.1.2 ”Ownership of assets”

4.10.9 Avsaknad av informationsägare

Beskrivning
Enligt många förvaltningsmodeller inom organisationer så skall det finnas formellt utsedda informationsägare för den information som skaps och hanteras inom organisationen. Detta informationsägarskap innefattar vissa krav på den utsedde personen, exempelvis att denne har ett visst mått av ansvar för hur informationen används i såväl automatiserad som manuell informationshantering. Ett särskilt hot är att organisationen inte har formellt utpekade informationsägare.

Kategori
Organisatoriskt hot, Internt hot

Orsak/Aktör
Felaktig ledning och styrning av organisationens resurser

Exempel
- Information i ett system saknar ägare
- Informationen i ett system har en ägare som inte längre är kvar inom organisationen
- Omorganisationer har lett till att den person som står som informationsägare inte längre är ansvarig för det område, eller jobbar med systemet, eller på annat sätt är relaterad till systemet som informationen finns i eller till informationen som sådan

Se också
4.10.10

Referenser
SS-ISO/IEC 27002:2005 kap 7.1 ”Ansvar för tillgångar”
ISO/IEC 27019:2013 kap 7.1.2 ”Ownership of assets”

4.10.10 Informationsägare som inte känner till sitt ansvar

Beskrivning
Enligt många förvaltningsmodeller inom organisationer så skall det finnas formellt utsedda informationsägare för den information som skaps och hanteras inom organisationen. Detta informationsägarskap innefattar vissa krav på den utsedde personen, exempelvis att denne har ett visst mått av ansvar för hur informationen används i såväl automatiserad som manuell informationshantering. Ett särskilt hot är att den person som är utsedd till informationsägare för ett visst system inte känner till vad det innebär att vara informationsägare eller inte känner till allt ansvar för informationen som just denna förvaltningsmodell lagt i rollen informationsägare.

Kategori
Organisatoriskt hot, Internt hot

Orsak/Aktör
Felaktig ledning och styrning av organisationens resurser

Exempel
- Information i ett system saknas ägare på grund av att informationsägaren inte är medveten om att denne person formellt är utsedd till informationsägare
- Informationen i ett system har en ägare som inte längre är kvar inom organisationen
- Omorganisationer har lett till att den person som står som informationsägare inte längre är ansvarig för det område, eller jobbar med systemet, eller på annat sätt är relaterad till systemet som informationen finns i eller till informationen som sådan

Se också
4.10.9

Referenser
SS-ISO/IEC 27002:2005 kap 7.1 ”Ansvar för tillgångar”

4.11 Resursbrist

Detta kapitel avhandlar olika aspekter av hot mot området organisatoriska hot, exempelvis personalresurser.

4.11.1 Temporär frånvaro eller underskott av personal

Beskrivning
Varje organisation har ett behov av personal för att utföra sin verksamhet. Finns inte rätt antal personer för att utföra vissa moment inom arbetet, eller att vissa roller och personalkategorier tillfälligtvis eller permanent saknas, så kan det innebära att viss verksamhet helt enkelt inte går att utföra.
På liknande sätt så kan det inom en organisation över tid ske personalneddragningar tack vare rationalisering, effektiviseringar och liknande. Detta kan innebära att ordinarie verksamhet, inom vissa snäva toleransramar, kan genomföras, men att varje typ av avvikelse eller händelser som kräver särskild hantering.

Kategori
Internt hot, felaktig ledning och styrning av organisationens resurser

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Temporär övergång från automatiserad processkontroll till lokal kontroll ute i anläggning går inte att hantera på grund av att rationalisering av personal har lett till bemanningsproblem då dessa inte räcker till att bemanna alla aktuella anläggningar.

Se också
4.11.2

Referenser
SS-ISO/IEC 27002:2005 kap 8.1.1 ”Roller och ansvar”
ISO/IEC 27019:2013 kap 8.1.1 ”Roles and responsibilities”

4.11.2 Permanent frånvaro eller underskott av personal

Beskrivning
Varje organisation har ett behov av personal för att utföra sin verksamhet. Finns inte rätt antal personer för att utföra vissa moment inom arbetet, eller att vissa roller och personalkategorier tillfälligtvis eller permanent saknas, så kan det innebära att viss verksamhet helt enkelt inte går att utföra.
På liknande sätt så kan det inom en organisation över tid ske personalneddragningar tack vare rationalisering, effektiviseringar och liknande. Detta kan innebära att ordinarie verksamhet, inom vissa snäva toleransramar, kan genomföras, men att varje typ av avvikelse eller händelser som kräver särskild hantering.

Kategori
Internt hot, felaktig ledning och styrning av organisationens resurser

Orsak/Aktör
Avsaknad av kompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, tidsbrist, taktiskt spel med avseende på kostnadsbesparingar

Exempel
- Temporär övergång från automatiserad processkontroll till lokal kontroll ute i anläggning går inte att hantera på grund av att rationalisering av personal har lett till bemanningsproblem då dessa inte räcker till att bemanna alla aktuella anläggningar.
- Systematisk och kronisk underskott på personalresurser som leder till att roller och ansvar blir felaktiga

Se också
4.11.1

Referenser
SS-ISO/IEC 27002:2005 kap 8.1.1 ”Roller och ansvar”
ISO/IEC 27019:2013 kap 8.1.1 ”Roles and responsibilities”

4.12 Kompetens

Detta kapitel avhandlar olika aspekter av hot mot området organisatoriska hot, exempelvis säkerhetskompetens.

4.12.1 Felaktig kunskapsnivå

Beskrivning
Varje organisation har behov av personal inom olika personalkategorier och roller som har olika typer av baskunskap och fack- eller specialistkunskap. Organisationen kan ha personal som har felaktig nivå på sitt kunnande och sin kompetens på grund av felrekryteringar, avsaknad av grundutbildning av befintlig personal, avsaknad av vidareutbildning av befintlig personal, med mera.

Kategori
Internt hot, felaktig ledning och styrning av organisationens resurser

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Ledningsgruppsmedlemmar som inte förstår verksamheten, verksamhetens behov, marknadens utveckling, externa krav, med mera
- Processkontrollingenjörer som inte är utbildade på den aktuella versionen av de programvaror som används för styr- och reglering av processen
- Säkerhetsspecialister som inte har kunskap om moderna sårbarheter, hot, attackmetoder

Se också
4.12.2, 4.12.3, 4.12.4

Referenser
SS-ISO/IEC 27002:2005 kap 8.2.2 ”Informationssäkerhetsmedvetande, utbildning och övning”

4.12.2 Otillräcklig kompetensförsörjning

Beskrivning
Inom en organisation behövs personal inom olika personalkategorier och roller som har olika typer av baskunskap och fack- eller specialistkunskap. Ofta måste personalens kompetens underhållas och utvecklas över tid, då verksamhetens behov och krav är föränderlig. Därför kan kompetensbehovet behöva stärkas vid såväl nyrekrytering som för befintlig personal. Om så inte sker, så kan ett glapp uppstå mellan verksamhetens reella behov och den inom organisationen existerande kompetensen.

Kategori
Internt hot, utarmning, felaktig ledning och styrning av organisationens resurser

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Otillräckliga kontinuerliga utbildningsinsatser
- Felaktiga utbildningsinsatser
- Otillräcklig uppföljning på att inköpta nätkurser brukas

Se också
4.12.1, 4.12.3, 4.12.4

Referenser
SS-ISO/IEC 27002:2005 kap 8.2.2 ”Informationssäkerhetsmedvetande, utbildning och övning”

4.12.3 Kompetensutarmning

Beskrivning
Med kompetensutarmning så menas att kunnande och kompetens minskar över tid. Ett exempel på detta är att organisationen tappar erfarna och kompetenta medarbetare på grund av pensionsavgångar.

Kategori
Internt hot, utarmning, felaktig ledning och styrning av organisationens resurser

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, taktiskt spel med avseende på kostnadsbesparingar eller underbemanning av säkerhetsfunktionen

Exempel
- Kunnig personal försvinner i samband med pensionsavgångar
- Kunnig personal försvinner i samband med utkontraktering av tjänster
- Personal sägs upp på grund av övertalighet, vikande marknad, konjunktur mm
- Personal avslutar sin anställning

Se också
4.12.1, 4.12.2, 4.12.4

Referenser
SS-ISO/IEC 27002:2005 kap 8.2.2 ”Informationssäkerhetsmedvetande, utbildning och övning”

4.12.4 Nyckelpersonberoenden

Beskrivning
Beroenden av enstaka personer som utan förvarning kan försvinna (avsked, sjukdom, dödsfall, mm) från en organisation, eller vara otillgängliga vid kritiska tidpunkter då deras kunskap, erfarenheter eller handlag särskilt behövs.

Kategori
Internt hot**,** felaktig ledning och styrning av organisationens resurser

Orsak/Aktör
Avsaknad av kompetens, avsaknad av erfarenhet, avsaknad av rutiner, felaktiga rutiner, tidsbrist, taktiskt spel med avseende på kostnadsbesparingar

Exempel
- Enstaka IT-tekniker som har byggt en IT-lösning och är den/de enda som som har helhetsförståelse eller viktig detaljförståelse om systemets uppbyggnad, funktion, behov av underhåll, mm.
- Ämnesexperter inom områden som processkontroll, elsystemsteknik, fysik eller liknande som behövs för att praktiskt kunna bedriva verksamheten
- Personal vars kunnande och roller behövs för att tillståndsmässigt få bedriva verksamheten

Se också
4.11.1, 4.11.2, 4.12.1, 4.12.2, 4.12.3

Referenser
SS-ISO/IEC 27002:2005 kap 8.2.2 ”Informationssäkerhetsmedvetande, utbildning och övning”

5 Tekniska hot

*Definition: Med **tekniska hot** avses hot som*

Är av teknisk natur eller som negativt kan påverka teknik, tekniska lösningar och tekniska system.

Innehållsförteckning kapitlet *Tekniska hot*

5.1 Felaktigt utformad IT-miljö eller IT-infrastruktur

Detta kapitel avhandlar olika aspekter av hot mot området tekniska hot, exempelvis

- brister i IT-miljöns utformning
- Avsaknad av IT-arkitektur
- Felaktig integration
- mm

5.1.1 Avsaknad av sammanhållande IT-arkitektur

Beskrivning
En IT-arkitektur är en sammanhållande och övergripande tanke och design för IT-miljön och dess olika komponenter. Att ha en fastslagen IT-arkitektur som fungerar som mall och referens mot vilken nya lösningar utformas innebär en slags standardisering och enhetlighet i såväl utformning som i olika kvalitetsaspekter, inte minst IT- och informationssäkerhet.

Kategori
Tekniskt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, designfel

Exempel
- Avsaknad av IT-arkitektur gör att många system är installerade på ett ostrukturerat och osystematiskt sätt. Detta gör att många varianter av installationer finns, med olika versioner på programvaror och olika konfigurationsinställningar. Detta i sin tur kan leda till att flera typer säkerhetsbrister förekommer, än om en standardiserad lösning med mer genomtänkta lösningsförslag existerade.
- IT-arkitekturen omfattar bara kontorsautomatisering och den IT-miljö som används på kontorssidan. Det saknas IT-arkitektur för SCADA- och processautomationssidan. Detta leder till en stor flora av olika lösningar, installationer, varianter av lösningar på SCADA- och processautomationssidan. Därmed så täcks flera olika IT-lösningar och programversioner in, vilket i sin tur leder till ökade möjligheter för en angripare att hitta felaktigt installerade eller installationer med äldre programvara som har välkända säkerhetshål.

Exempel på potentiella konsekvenser
- Eftersom övergripande IT-arkitektur saknas så får eventuella säkerhetsincidenter mycket större konsekvenser, inklusive påverkan på processkontroll och automationsmiljö

Se också

Referenser

5.1.2 Avsaknad av sammanhållande säkerhetsarkitektur

Beskrivning
Avsaknad av en sammanhållande säkerhetsarkitektur kan leda till att vissa kritiska komponenter skyddas med direkta säkerhetsskydd, men att andra komponenter, på vilka den kritiska komponenten är beroende, inte har samma nivå av skyddet. Därmed kan en säkerhetspåverkande händelse eller IT-säkerhetsincident som involverar någon av de mindre kritiska komponenterna även påverka den mer kritiska komponenten.

Kategori
Tekniskt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säerhetskompetens, designfel

Exempel
- Säkerhetsarkitektur saknas helt och hållet, varpå de olika insatser som görs för att skapa säkerhet då snarast blir sporadiska och ostrukturerade.
- I en organisation där en säkerhetsarkitektur finns, men inte helt ut följs kan vissa infrastrukturkomponenter hamna utanför att omfattas säkerhetsarkitekturen, till exempel servers som erbjuder DNS (översättning mellan domännamn och IP-adresser), DHCP (tilldelning av dynamiska domännamn), NTP (tidsynkronisering), syslog (fjärrloggning till en loggserver), då dessa inte har en utpekad systemägare. Därmed installeras inte dessa tjänster på serverdatorer som säkrats upp till en högre nivå (s.k. härdning) och inte heller underhålls dessa tjänster löpande med avseende på programvaruuppdateringar. Därmed står dessa komponenter utanför säkerhetsarkitekturen och kan bli akilleshälar i samband med automatiserad spridning av skadlig kod via nätverket eller riktade angrepp mot just dessa tjänster. Och andra plattformar, system och datorer som är beroende av dessa tjänster och funktioner kan som en sekundäreffekt bli påverkade på olika sätt.
- I en organisation där en säkerhetsarkitektur finns, så kanske den bara omfattar kontorsautomation och ”vanlig IT-miljö”, men inte de IT-komponenter som finns inom elproduktion, eldistribution eller elhandel. Därför kan dessa, oftast verksamhetskritiska system, helt lämnas utanför den säkerhetsarkitektur som finns.

Exempel på potentiella konsekvenser
- De säkerhetsfunktioner som normalt är installerade eller aktiverade finns inte på den utrustning som köpts/installerats, vilket medför att de nödvändiga skyddsnivåer som arkitektekturen är skapad att erbjuda inte hålls i realiteten.

Se också

Referenser

5.1.3 Felaktigt utformad IT-miljö

Beskrivning
En felaktig utformad IT-miljö kan komma av att den är underdimensionerad, t.ex. utformad för ett småföretag när organisationen har växt och behöver bättre underhållen och förvaltad IT.
Den felaktiga IT-miljön kan komma av att ingen övergripande strategi har funnits i samband med att IT-miljön ursprungligen skapades eller att denna strategi inte har justerats i samband med att IT-miljön har vuxit eller dess användning har ändrats över tid.

Kategori
Tekniskt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, designfel

Exempel
- IT-miljön för ett medelstort företag är fortfarande utformat som för ett väldigt litet företag där varje medarbetare får helt sköta sin egen utrustning, det finns ingen eller liten centraliserad hantering och förvaltning av IT och informationshanteringen.
- Mer kritiska funktioner hanteras i samma system, med samma skydd, och under samma administrativa procedurer som mindre skyddsvärda funktioner
- Mer skyddsvärd information hanteras i samma system, med samma skydd, och under samma administrativa procedurer som mindre skyddsvärd information

Exempel på potentiella konsekvenser
- Var och en som underhåller sin egen dator sköter detta på olika sätt, detta medför att inte alla tar säkerhetskopior av sin information på rätt sätt. Vid en hårddiskkrash för en chef så tappas viktig och svårersättlig information.
- Då kontorsdatorer och datorer som används för elverksamhet inte hålls separerade utan blandas i ett och samma nät så leder ett virusutbrott på en kontorslaptop till att även servrar och klientdatorer som hör till de industriella informations- och styrsystemen blir drabbade.

Se också

Referenser
ISO/IEC 27002:2005 kap 11.6.2 ”Isolering av känsliga system”
ISO/IEC 27019:2013 kap 9.1.8 ”Securing equipment rooms”

5.1.4 Felaktigt utformade försörjningssystem för IT-miljön

Beskrivning
För att bedriva IT i lite större skala så behövs anpassade försörjningssystem till olika delar av IT-miljön. Olika försörjningssystem inkluderar elförsörjning till datorhallar och korskopplingsrum, kylning av luft i datorhallar och korskopplingsrum, kommunikationsanslutningar, mm.
Om dessa försörjningssystem saknas, är underdimensionerade eller felaktigt utformade så kan det få konsekvenser för exempelvis tillgänglighet av utrustning.

Kategori
Tekniskt hot

Orsak/Aktör
Avsaknad av kompetens, designfel

Exempel

- Reservkraftsystemen är felaktigt inkopplade, så att dessa i en värsta händelse kan slås ut samtidigt som primärkraftmatningen.
- Kylsystem för datorhall eller liknande, är ej kopplat på reservkraftssystemet, vilket för med sig att värmeproblem snabbt uppstår i samband med att det blir störningar på primärkraftmatning.
- Det finns bara ett kylaggregat i det kylsystem som används för datorhall, kommunikationsrum eller liknande, vilket för med sig att värmeproblem snabbt uppstår i samband med att det blir störningar på det enda kylaggregatet.

Exempel på potentiella konsekvenser
- Servrar som används för SCADA eller industriell kontroll slås ut i direkt eller kort efter det att försörjningssystemen i datorhall, kommunikationsrum eller liknande slås ut.

Se också
5.1.5, 5.4.13

Referenser
ISO/IEC 27019:2013 kap 9.1.8 ”Securing equipment rooms”
ISO/IEC 27019:2013 kap 14.2.1 ”Emergency communication”

5.1.5 Underdimensionerade försörjningssystem för IT-miljön

Beskrivning
För att bedriva IT i lite större skala så behövs anpassade försörjningssystem till olika delar av IT-miljön. Olika försörjningssystem inkluderar elförsörjning till datorhallar och korskopplingsrum, kylning av luft i datorhallar och korskopplingsrum, kommunikationsanslutningar, mm.
Om dessa försörjningssystem saknas, är underdimensionerade eller felaktigt utformade så kan det få konsekvenser för exempelvis tillgänglighet av utrustning.

Kategori
Tekniskt hot

Orsak/Aktör
Avsaknad av kompetens, designfel

Exempel
- Reservkraftsystemen är underdimensionerade, detta innebär att dessa inte kan strömmata utrustning i rätt omfattning i händelse att primärkraftmatningen faller från. Reservkraftstiden är ytterst begränsad
- Det finns för lite kylkapacitet i det kylsystem som används för datorhall, kommunikationsrum eller liknande, vilket för med sig att det är latenta värmeproblem i utrymmet.
- Det finns bara ett kylaggregat i det kylsystem som används för datorhall, kommunikationsrum eller liknande, vilket för med sig att värmeproblem snabbt uppstår i samband med att det blir störningar på det enda kylagreggatet.

Exempel på potentiella konsekvenser
- Servrar som används för SCADA eller industriell kontroll slås ut i direkt eller kort efter det att försörjningssystemen i datorhall, kommunikationsrum eller liknande slås ut.

Se också
5.1.4, 5.4.13

Referenser
ISO/IEC 27019:2013 kap 9.1.8 ”Securing equipment rooms”

5.1.6 Felaktig integration mellan IT-miljöer

Beskrivning
Tidigare som har det funnits många direktkopplingar mellan olika servrar. För att få bättre kontroll över informations- och dataflödet samt bättre överblick på beroenden mellan system så har olika typer av integrationslösningar införts i många organisationer.
När integration införs går det att göra på flera olika sätt, med centraliserade eller decentraliserade integrationspunkter, servrar som sköter integration mellan andra servrar, dit flöden ansluts.

Kategori
Tekniskt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, designfel

Exempel

- All integration går via en eller enstaka integrationsservrar. Dessa blir periodvis överlastade av all trafik med långsam hantering som följd
- All integration går via en eller enstaka integrationsservrar. Om dessa blir otillgängliga, till exempel via ett hårdvarufel eller via ett angrepp, så står all dataöverföring och all integration drabbas.
- Ingen separation i integrationslösningen mellan stora, långa mer batchorienterade dataöverföringar och korta, snabba realtidsöverföringar, utan dessa går via samma integrationsmotor. Detta får en negativ påverkan på de transaktioner som har höga krav på snabb överföring och korta svarstider.

Exempel på potentiella konsekvenser

- Integration mellan olika SCADA/IECS delar som har högre tidskrav blir drabbade av databasdumpar och stora filöverföringar som sker via samma integrationshub.
- Insamling av mätvärden från automatiska elmätare kan inte ske på grund av fel (driftstopp, överlastning, temporär felkonfiguration, mm) i integrationslösningen
- Arbetsordrar till fältpersonal kan inte distribueras ut från arbetsordersystem till handdatorer

Se också

Referenser

5.1.7 Felaktigt utformad lagringslösning

Beskrivning
Data lagras på olika typer av lagringsmedium, traditionellt ofta magnetiska hårddiskar. Olika lösningar för lagring skapas, exempelvis är NAS (Network Attached Storage), en enklare server som är dedicerad för lagring och delar ut sitt lagringsutrymme via nätdiskar.
Ofta byggs större lösningar upp där man centraliserar lagring för servrar och därmed skapas så kallade lagringsnät (SAN, Storage Area Network).

Kategori
Tekniskt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, designfel

Exempel

- Samma lagringslösning används för primärlagring och säkerhetskopiering, vilket innebär att fysiska hot såsom brand påverkar alla kopior av sparad data.
- Samma lagringslösning (diskskåp, lagringsnät) används i DMZ-området, vilket innebär att man kortsluter olika nätverk.

Exempel på potentiella konsekvenser

- Ett utslaget lagringsnät kan innebära driftstörningar för SCADA-system, där SCADA-servrar blir helt utslagna, där funktionalitet blir drabbad, eller där information inte kan lagras eller läsas korrekt.

Se också

Referenser
ISO/IEC 27019:2013 kap 11.4.5 ”Segregation in networks”

5.1.8 Felaktigt utformad fjärråtkomstlösning

Beskrivning

Fjärråtkomst kan innebära åtkomst via nätverket från andra datorer på samma nät. Fjärråtkomst kan också innebära åtkomst från datorer som befinner sig på långa avstånd, tillexempel från leverantörer som sitter på sina kontor i utlandet och ger support eller utför fjärrdiagnostik.
Fjärråtkomst kan i vissa mer begränsade fall ge åtkomst till enstaka applikationer eller i mindre restriktiva fall åtkomst till hela nätverk och samtliga till det nätet anslutna datorer.
Felaktigt utformad fjärråtkomst kan medföra olika typer av risker, exempelvis extern exponering av infrastruktur, obehörig åtkomst.

Kategori
Tekniskt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, designfel

Exempel
- Standardlösenord är fortfarande satt på välkända konton, vilket medför att någon som ”hittar” datorn på nätet lätt kan gissa sig till lösenordet och skaffa sig åtkomst.
- Alltför stor åtkomst är utdelad. Istället för att exportera en enstaka applikation som skall kunna nås på distans, så exporteras hela skrivbordet (arbetsytan i windows) med höga behörigheter så att valfria program kan startas.
- Delade gruppkonton (ett användarnamn och tillhörande lösenord) används av supportpersonal som delar på service- och support. Detta medför att man inte vet vilken fysisk person som varit inloggad, varpå man tappar spårbarhet och oavvislighet.

Exempel på potentiella konsekvenser
- En SCADA-leverantör loggar in och utför systemförändringar via ett gruppkonto som används för såväl lokal administration som fjärradministration. Systemfel uppstår efter en viss fördröjning, där flera andra fjärrinloggningar och lokala inloggningar har utförts via samma konto. Det är svårt eller omöjlig att förstå eller hitta vilken person som gjort ändringar som är grunden för systemfelet.
- Personal på IT-avdelningen loggar in via fjärråtkomst för att utföra administrativa uppgifter. De är inloggade på en HMI-dator samtidigt som operatörer arbetar på den. Arbetet som IT-avdelningens personal utför måste avslutas med en omstart av datorn. Datorn startas om utan att SCADA-operatörerna i kontrollrummet informeras.
- Fjärråtkomstlösningen öppnar upp för obehörig åtkomst, varpå obehöriga använder sig av denna ingång för att skaffa sig åtkomst till ett industriellt kontrollsystem. Via denna fjärringång påverkar dessa obehöriga styrningen av den fysiska processen.

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 6.2.1 ”Identifiering av risker med utomstående parter”
ISO/IEC 27019:2013 kap 6.2.1 ”Identification of risks related to external parties”
ISO/IEC 27019:2013 kap 11.1.1 ”Access control policy”
ISO/IEC 27019:2013 kap 12.4.1 ”Control of operational software”

5.2 Hot baserade på felaktig programvaruutveckling

Dessa hot omfattar fel när det uppstår säkerhetsproblem som ett resultat av att den egna organisationen, eller när något företag eller några personer, utför programvaruutveckling. Vad det gäller säkerhetsproblem som uppstår i samband med köpt programvara, se kapitel ”5.3 Programvarufel” sid 148 och framåt.

5.2.1 Felaktig analys

Beskrivning
I samband med systemutveckling sker ett analyssteg där behovet analyseras närmare för att kunna uttryckas i form av en kravlista. Analysen kan bestå i att samla in explicita krav som finns hos beställare, verksamhetsföreträdare, i styrdokument, mm.

Kategori
Tekniskt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, felaktigt utformad utvecklingsmetodik

Exempel

- Alla krav tas inte med på grund av att projektledningen inte har avsatt tillräckligt med tid eller resurser för analysarbetet.
- Alla krav tas inte med på grund av att ansvarig analysledare inte har tillräckligt med kompetens för analysarbetet.
- Alla krav tas inte med på grund av underlaget saknar viktiga delar, exempelvis finns inte styrdokument för säkerhet på plats för att säkerhetskraven skall vara framtagna och färdiga att kunna ingå som befintligt underlag.
- Att inte krav redan existerar föranleder inte att analysledaren själv på eget bevåg tar fram nödvändiga grundkrav för säkerhet, som sedan stäms av mot verksamheten, utan säkerhetsfrågorna utelämnas

Exempel på potentiella konsekvenser

- Ett industriellt styrsystem införs utan grundläggande IT-skydd och säkerhetsfunktioner, då ingen fann att det ställdes krav på att sådana skulle tas med i lösningen i samband med systemutveckling.
- Ett industriellt styrsystem införs utan grundläggande IT-skydd och säkerhetsfunktioner, då ingen fann att det ställdes krav på att sådana skulle tas med i lösningen i samband med projektering, upphandling och införandeprojekt.

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 12.1.1 ”Analys och specifikation av säkerhetskrav”
SS-ISO/IEC 27002:2005 kap 12.5.5 ”Utlagd programvaruutveckling”

5.2.2 Felaktig analys av kravbild, felaktig förståelse för hotbild

Beskrivning

I samband med systemutveckling sker ett analyssteg där behovet analyseras närmare för att kunna uttryckas i form av en kravlista. Denna kravlista skall sedan analyseras och omformas till olika lösningar, lösningsdelar eller skydd som uppfyller kraven.

Kategori
Tekniskt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, felaktigt utformat utvecklingsmetodik

Exempel
- Projektet bedrivs som på samma sätt som det alltid gjorts, och ingen hänsyn tas till att IT och IT-kommunikation, fått en mer central del i lösningarna. De hot som därmed finns mot lösningen inkluderar moderna IT-hot. Detta tar man inte höjd för i samband med projektering och kravhantering
- I samband med projektarbetet genomförs en riskanalys. Denna riskanalys är dock fokuserad på projektrisker, inte på risker i den leverabel som projektet tar fram. Därför blir hotbilden mot lösningen felaktig eller inte framtagen.
- Då projektet själv saknar relevant kompetens inom IT, nätverk, IT-risker, informationssäkerhet, nätverkssäkerhet, med mera så görs banala misstag vad det gäller utformning av skydd

Exempel på potentiella konsekvenser
- Grundläggande krav på exempelvis säkerhetsskydd saknas i ett industriellt kontrollsystem för en elanläggning som är av stort regional betydelse.
- Grundläggande krav på exempelvis rollbaserad åtkomst, spårdata och nätverkssäkerhet saknas i ett industriellt kontrollsystem för en elanläggning som är av stort regional betydelse.

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 12.1.1 ”Analys och specifikation av säkerhetskrav”
SS-ISO/IEC 27002:2005 kap 12.5.5 ”Utlagd programvaruutveckling”
ISO/IEC 27019:2013 kap 11.4.5 ”Segregation in networks”

5.2.3 Felaktig programvaruutvecklingsmetodik

Beskrivning
Moderna programvaruutvecklingsmetodiker inkluderar moment eller steg i vilka man genomför olika typer av IT-säkerhetstester, antingen teoretiska eller praktiska. Med felaktig programvaruutvecklingsmetodik menar vi här att man antingen utvecklar på ett sådant sätt och på en sådan nivå att man ignorerar aktuella hotbilder och angreppsmetoder, samt att man ignorerar de metoder som ingår i utvecklare, systemarkitekters och designers verktygslådor för att analysera de potentiella säkerhetsproblem och sårbarheter som kan uppstå. Felaktig programvaruutvecklingsmetodik får anses vara ett kvalitetsproblem som innebär att inte säkerhet, säkerhetsmekanismer, säkerhetsnivåer, skydd mm kravställs i samband med utformningen av programvaran.

Kategori
Tekniskt hot, administrativt hot

Orsak/Aktör
Avsaknad av kompetens, avsaknad av säkerhetskompetens, avsaknad av kvalitetskontroll och uppföljning

Exempel
- Utvecklarna utför inte enhetstester som fokuserar på säkerhetsproblem, såsom indatavalidering, så att otestad kod innehåller fel i datavalideringsfunktionen vilket i sin tur leder till att en angripare senare kan införa oönskad tredjepartsprogramkod som exekveras.
- Utvecklarna tillämpar ej defensiv programmering och utför felkontroll och felhantering överallt i sitt program. Därför finns det ett antal moduler och funktioner i programmet som är sårbara för olika typer av angrepp. Dessa sårbarheter kommer sedan att ligga latent.
- Utvecklarna loggar inte felaktigheter och programfel i rätt omfattning. Detta medför att attackförsök eller olika typer av missbruk går att utföra utan att någon kan komma att uppmärksamma dem.
- Utvecklarna tillämpar rätt typ av versionshantering på den utvecklade källkoden, vilket medför att när buggar i ett senare tillfälle upptäcks så är det svårt att se när buggarna uppstod i utvecklingsarbetet och av vem, samt i vilka utgåvor av programmet som buggarna finns.

Exempel på potentiella konsekvenser
- Ett SCADA-system blir utsatt för olika typer av intrångsförsök. Ingenstans loggas relevanta loggar som påvisar att mängder med felaktig indata skickas till systemet. Alla felaktigheter hanteras tyst tills ett korrekt nätverkspaket slutligen når systemet, vilket blir manipulerat.
- Buggar hittas i ett industriellt styrssystem, dessa rapporteras in till ICS-CERT som är en central intrernationell samarbetsorganisation för att hantera IT-säkerhetsfel i industriella styrsystem. Dessa kontaktar leverantören som inte kan verifiera buggarna för den har inte den struktur och ordning-och-reda som behövs för att kunna återskapa situationen där buggarna uppstod. Detta beror på att de inte har testmiljöer, versionshantering för att kunna hantera att olika kunder har olika versioner av programvaran installerad, etc.

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 12.5 ”Säkerhet i utvecklings- och underhållsprocesser”
ISO/IEC 27019:2013 kap 10.1.4 ”Separation of development, test and operational facilities”

5.2.4 Felaktigt utformade skydd

Beskrivning
I de IT-system som utvecklas så skapas olika skyddsmekanismer, exempelvis behörighetshantering, åtkomstkontroll, brandväggsfunktionalitet för nätverksmässig åtkomstkontroll, logghantering, med mera.

I detta hotkort beskrivs hotet att de skydd som tas fram är otillräckliga eller felaktigt utformade. Detta i sig leder till säkerhetsproblem med skydden, vilket i sin tur leder till att det som skall skyddas i sin tur är sårbart och åtkomligt.

Kategori
Tekniskt hot

Orsak/Aktör
Designfel, kompetensbrist, avsaknad av säkerhetskompetens, avsaknad av kravinsamling

Exempel
- Hårdkodade lösenord som ligger i firmware och ej går att byta
- Lösenord som programmet använder sig av sparas i klartext istället för i krypterad form.
- Avsaknad av åtkomstkontroll
- Avsaknad av nätverksmässig åtkomstkontroll
- Det går ej att stänga av vissa nätverksfunktioner, så dessa ligger kvar och kan potentiellt nås och missbrukas av andra parter senare.

Exempel på potentiella konsekvenser
- PLC-utrustning i fält som har standardlösenord som inte går att byta. Dessa är åtkomliga via nätverksåtkomst eller fysisk åtkomst. Någon obehörig som kommer åt konsolport eller nättjänster kan komma in i PLC-utrustningen med kända lösenord och sedan ändra I/O-inställningar, programsekvenser, med mera. PLC-utrustningen uppför sig därefter inte som avsett av anläggningsägaren. Detta leder till att styrningen av den fysiska processen inte är felfri utan det uppstår skador på utrustning i anläggningen.
- RTU-utrustning i fält som har enkla fjärradministrationsingångar via Telnet samt standardlösenord som inte går att byta. Någon obehörig som kommer åt den administrativa nättjänsten kan komma in i RTU-utrustningen med kända lösenord och sedan ändra I/O-inställningar, protokollhantering med mera. RTU-utrustningen uppför sig därefter inte som avsett av anläggningsägaren. Detta leder till att styrningen av den fysiska processen inte är felfri utan det uppstår skador på utrustning i anläggningen.

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 12.1.1 ”Analys och specifikation av säkerhetskrav”
SS-ISO/IEC 27002:2005 kap 12.2 ”Korrekt bearbetning i tillämpningar”
SS-ISO/IEC 27002:2005 kap 12.3 ”kryptering”
SS-ISO/IEC 27002:2005 kap 12.5.5 ”Skydd av systemfiler”
SS-ISO/IEC 27002:2005 kap 12.6.1 ”Skydd för tekniska sårbarheter”
ISO/IEC 27019:2013 kap 11.1.1 ”Access control policy”
ISO/IEC 27019:2013 kap 11.3.1 ”Password use”

5.2.5 Felaktigt utformade programmeringsgränssnitt (API)

Beskrivning

Programmerings-API (*eng. application programming interface*) används för att från ett program skall kunna anropa annan programkod (program eller programbibliotek), antingen lokalt på den egna datorn eller som fjärranrop till ett annat program via nätverket.

Kategori
Tekniskt hot

Orsak/Aktör
Designfel, kompetensbrist, brister i utvecklingsmetodik

Exempel

- Delar av APIt är åtkomligt utan någon form av åtkomstkontroll, vilket gör att obehöriga kan utföra känsliga operationer
- Programmeringsgränssnittet är inte ortagonalt, vilket medför att vissa operationer kan utföras utan att åtkomst- och behörighetskontroller utförs på den som utför angropen mot gränssnittet för dessa operationer
- Vissa grundläggande och nödvändiga säkerhetsfunktioner saknas i programmeringsgränssnittet, exempelvis åtkomstkontroll och behörighetskontroll

Exempel på potentiella konsekvenser
- Ett WebService-baserat API som tillhör ett industriellt styrsystem har inget ordentligt behörighetskontrollsystem som kan verifiera WebServiceanropens källa. Anropet kan missbrukas för att stänga ned olika tjänster i styrsystemet, exempelvis övervarvningsskyddet i en transformator som styrs och kontrolleras från systemet.
- Ett OPC-baserat program för miljöövervakning i ett kraftvärmeverk är åtkomligt via nätverket. Då denna version av OPC går på en windowsserver och bygger på MS RPC-protokollet, vilket har fått sin behörighetskontroll (windows AD-baserad användarrättighetskontroll) avstängd i enlighet med OPC foundations riktlinjer. Eftersom OPC-programmet inte heller har någon egen behörighetskontroll så är det möjligt för en obehörig tredje part att koppla in sig och manipulera miljödata i databasen, varpå oriktig miljödata finns sparad

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 12.1.1 ”Analys och specifikation av säkerhetskrav”

5.2.6 Felaktigt utformade användargränssnitt

Beskrivning
Felaktigheter i användargränssnitt kan leda till mänskliga misstag eller felanvändning av en applikation eller ett system. I vissa fall kan felaktigheter i användargränssnittet även leda till felaktigheter som har bärighet på säkerhet inträffar.
Grafiska användargränssnitt kan ibland vara utformade på ett sådant sätt att man förleds att tro att vissa operationer är blockerade eller omöjliga att utföra. De kan vara så att de enbart är spärrade i användargränssnittet, men via programmeringsgränssnitt så är de fullt åtkomliga.

Kategori
Tekniska hot

Orsak/Aktör
Designfel, kompetensbrist, brister i utvecklingsmetodik, brister i utvärdering, brist i testning

Exempel

- Användargränssnittet är utformat på ett sådant sätt så att en användare förleds att *utföra* säkerhetsmässigt felaktiga operationer.
- Användargränssnittet är utformat på ett sådant sätt så att en användare tar fram och exponerar känslig information i onödan.
- Användargränssnittet är utformat på ett sådant sätt så att en användare förleds att tro att ett skydd är aktivt då det faktiskt har inaktiverats.

Exempel på potentiella konsekvenser

- Felaktigheter i det industriella styrsystemets grafiska användargränssnitt kan leda till att en anläggning är strömsatt då den skall vara strömlös.

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 12.1.1 ”Analys och specifikation av säkerhetskrav”

5.2.7 Felaktig testning i samband med programvaruutveckling

Beskrivning

I samband med programvaruutveckling måste en viss mängd testning ske. Testningen är att till för att se att programvaran beter sig som tänkt och som avsett i förhållande till den analys, de funktionella krav och den design som gjorts.

Korrekt och seriös testning utförs på såväl komponentnivå som på systemnivå samt med en stor mängd olika testfall och olika testdata.

En särskild kategori testning som är viktig är säkerhetstester, där olika säkerhetsfunktioners riktighet och funktionalitet kontrolleras.

Kategori
Tekniskt hot, administrativt hot

Orsak/Aktör
Kompetensbrist, avsaknad av säkerhetskompetens, brister i utvecklingsmetodik

Exempel

- Otillräcklig mängd testning, bara enklare testfall har tagits fram
- Bara funktionella tester, inga säkerhetstester ingår i testfallen
- Felaktig typ av testning. Enbart positiva testfall används, inga negativa testfall finns med i testerna
- Felaktig testdata används som del av testningen. Exempelvis kan skarp persondata från produktionssystem användas, vilket innebär brott mot finalitetsprincipen i personuppgiftslagen.

Exempel på potentiella konsekvenser

- Ett ICS-system som utvecklas och saluförs har bara testats utifrån ett snävt utsnitt av testfall som berör kontroll av elektromekanik. Inga testfall negativa testfall, såsom IT-mässiga lasttester eller IT-angrepp, har funnits med i testningen. När en oväntad hög last inträffar i ett produktionssatt system så fryser och hänger programmet, då intern datahantering inte är dimensionerad att hantera ett sådant läge, och att detta randfall har man inte upptäckt på grund av otillräcklig testning.
- Till ett inköpt system för hantering av inlästa mätvärden hos slutkund har man hos leverantören ett separat testsystem. För att få så realistiska tester som möjligt så har man i denna testmiljö valt att läsa över riktig produktionsdata, inklusive anläggnings-ID, adresser och personuppgifter. Detta testsystem har avsevärt lägre säkerhet än det produktionssatta systemet och blir slutligen hackat.

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 12.1.1 ”Analys och specifikation av säkerhetskrav”
ISO/IEC 27019:2013 kap 10.1.4 ”Separation of development, test and operational facilities”

5.3 Programvarufel

Med programvarufel menas

- Formgivningfel (designfel)
- Implementationsfel

Ett exempel implementationsfel kan vara att inte kontrollera inläst data efter

- Riktighet – att det var rätt typ av data som matchar den typ som efterfrågades
- Rätt längd – för mycket eller för lite data kan leda till problem vid tolkning
- Otillåtna tecken, binärdata eller annat som påverkar inläsningsfunktion och tolkning

Effekten av ett sådant implementationsfel kan vara att det i sin tur programexekveringen, antingen genom att programmet krashar eller att ny av angriparen uppladdad programkod exekveras.

Ofta kallas dessa fel i mjukvara för ”buggar”.

Programfel kan finnas latent under långa tidsperioder i installerad programvara. Ofta påverkas dessa genom att programmet uppdateras till helt nya versioner, eller att en bugg upptäcks och att leverantörer kommer ut med en särskild rättning till just den buggen, en såkallad patch eller fix (hotfix).

5.3.1 Programfel som påverkar stabilitet i programvaran

Beskrivning

Mjukvara som används i digitala system kan i sig självt innehålla logiska fel, vara felaktigt utformad eller bero på underliggande mjukvarukomponenter som innehåller fel. Programfel kan finnas latent under långa tidsperioder i installerad programvara och endast inträffa när vissa särskilda förutsättningar uppstår, t.ex. vid ett visst klockslag, när en systemresurs är otillgängligt (t.ex. ett filsystem blir fullt) eller på visst stimuli såsom indatainmatning.

Kategori
Tekniskt hot

Orsak/Aktör
Programvarufel, brist i utvecklingsmetodik, brist i test- och kvalitetskontroll

Exempel
- Program kraschar eller hänger.
- Delsystem (databashanterare, transaktionsmotor, applikationsserver, mm) kraschar eller hänger
- Underliggande operativsystem kraschar eller hänger.

Exempel på potentiella konsekvenser
- Program kraschar eller hänger på ett sådant sätt så att den fysiska processen inte kan övervakas (*loss of view*)
- Program kraschar eller hänger på ett sådant sätt så att den fysiska processen inte kan styras (*loss of control*).
- En programkomponent eller funktion krashar eller hänger på ett sådant sätt att själva mjukvaruplattformen (Windows, Linux, inbyggt system, mm) blir instabil.
- En programkomponent som är tänkt att använda på en interaktiv PC har används i systemutvecklingen och körs nu på ett inbyggt system. Programkomponenten visar upp en modal popupp-ruta (fönster som kräver att man klickar på den för att körningen skall fortgå) på en utrustning som inte har skärm, tangentbord eller mus inkopplad. Programexekveringen blockeras tills vidare. (*loss of control*).
- Program krashar på ett sådant sätt så att mjukvaruplattformen (Windows, Linux, inbyggt system, mm) också krashar

Se också
5.3.2, 5.3.3, 5.3.4

Referenser
SS-ISO/IEC 27002:2005 kap 12.1.1 ”Analys och specifikation av säkerhetskrav”

5.3.2 Programfel som påverkar säkerhetskritisk funktion eller delar av programvara

Beskrivning
I princip alla program innehåller programfel, såkallade buggar. Vissa buggar är funktionella fel, andra är kvalitetsbrister och ytterligare andra är säkerhetspåverkande fel. Programfel kan finnas latent under långa tidsperioder i installerad programvara. Dessa fel kan upptäckas efter lång tid. Om upptäckten görs av illasinnade kan dessa programfel och sårbarheter utnyttas i syfte.

Kategori
Tekniskt hot

Orsak/Aktör
Programvarufel, brister i utvecklingsmetodik, brist i test- och kvalitetskontroll

Exempel

- Säkerhetskritiska program eller systemkomponenter, såsom brandväggsfunktionalitet eller minnesskydd som skiljer exekverande program åt i ett datorsystem, har programfel så att de inte erbjuder det skydd som förväntas
- Program kan manipuleras på sådant sätt att en säkerhetsmekanism sätts ur funktion eller inte längre fungerar korrekt

Exempel på potentiella konsekvenser

- Om en säkerhetskritisk funktion (IT-säkerhetsskydd) fallerar, kan någon kan obehörigt ta sig förbi ett skydd på ett nätverk och ta sig till andra delar i nätverket, exempelvis in i ett SCADA- eller ICS-nätverk och där i ett andra steg nå ansluten utrustning som manipuleras.

Se också
5.3.1, 5.3.3, 5.3.4

Referenser

5.3.3 Programvarufel som leder till informationsläckage

Beskrivning
I princip alla program innehåller programfel, så kallade buggar. Vissa buggar är funktionella fel, andra är kvalitetsbrister och ytterligare andra är säkerhetspåverkande fel. Programfel kan finnas latent under långa tidsperioder i installerad programvara. Dessa fel kan upptäckas efter lång tid. Om upptäckten görs av illasinnade kan dessa programfel och sårbarheter utnyttas i syfte.

Kategori
Tekniskt hot

Orsak/Aktör
Programvarufel, brist i utvecklingsmetodik, brist i test- och kvalitetskontroll

Exempel

- En webbtjänst som är installerad är åtkomlig för alla med nätverksåtkomst. Ett programvarufel i webbplattformen gör att denna webbtjänst delar ut information utan behörighetskontroll.

Exempel på potentiella konsekvenser

- En webbtjänst i ett grafiskt informationssystem som används av elbolaget som stödsystem för teknisk dokumentation och dokumentation över ledningsdragningar, är installerad är åtkomlig för alla med nätverksåtkomst. Ett programvarufel gör att denna webbtjänst delar ut information utan behörighetskontroll.

Se också
5.3.1, 5.3.2, 5.3.4

Referenser
SS-ISO/IEC 27002:2005 kap 12.4.1 ”Styrning av programvara i drift”
SS-ISO/IEC 27002:2005 kap 12.5.4 ”Informationsläckage”

5.3.4 Programvarufel som leder till obehörig programexekvering

Beskrivning
I princip alla program innehåller programfel, så kallade buggar. Vissa buggar är funktionella fel, andra är kvalitetsbrister och ytterligare andra är säkerhetspåverkande fel. Programfel kan finnas latent under långa tidsperioder i installerad programvara. Dessa fel kan upptäckas efter lång tid. Om upptäckten görs av illasinnade kan dessa programfel och sårbarheter utnyttas i syfte.

Kategori
Tekniskt hot

Orsak/Aktör
Programvarufel, brist i utvecklingsmetodik, brist i test- och kvalitetskontroll

Exempel

- Ett fel i indatavalidering i en applikation möjliggör felaktig och obehörig uppladdning av programkod som sedan kan exekveras på.

Exempel på potentiella konsekvenser

- Ett SCADA-system har kommunikationsmoduler som har felaktig indatavalidering för MODBUS-protokollet. Felaktiga nätverkspaket kan medföra att en angripare kan skicka falska MODBUS-paket som också innehåller programkod som kommer exekveras tack vare felaktigheter i MODBUS-koden.
- Ett industriellt styrstystem har kommunikationsmekanismer som bygger på XML och som har felaktig indatavalidering för XML-paket. Felaktiga nätverkspaket kan medföra att en angripare kan skicka felaktiga nätverkspaket med XML-data som också innehåller programkod som kommer exekveras tack vare felaktigheter i XML-parsern.

Se också
5.3.1, 5.3.2, 5.3.3

Referenser
SS-ISO/IEC 27002:2005 kap 12.4.1 ”Styrning av programvara i drift”

5.4 Driftstörningar

Denna sektion listar olika typer av hot som introducerar driftstörningar baserade på tekniska fel.

5.4.1 Felaktig dokumentation som leder till driftstörning

Beskrivning
Detta hot beskriver olika typer av teknisk dokumentation som innehåller sakfel eller är tvetydig på ett sådant sätt att det leder till olika typer av följdfel såsom handhavandefel eller fungerar som felaktigt beslutsunderlag.

Kategori
Tekniska hot, administrativa hot

Orsak/Aktör
Handhavandefel, felbeslut

Exempel

- Användardokumentation som innehåller sakfel vilket leder till handhavandfel hos slutanvändare.
- Driftdokumentation som innehåller sakfel vilket leder till handhavandfel hos systemadministratörer.
- Systemdokumentation som innehåller sakfel vilket leder till handhavandfel hos nätadministratörer.

Exempel på potentiella konsekvenser

- Planerade ändringar i nätverkskonfiguration av ett industriellt styr- och kontrollsystem, baserat på otydligheter i systemdokumentation, leder till intermittenta driftstörningar i form av långa fördröjningar och time-outer. DNS-inställningar har påverkats på ett sådant sätt att DNS-uppslag inte längre fungerar som avsett.
- Planerade ändringar i nätverkskonfiguration av ett industriellt styr- och kontrollsystem, baserat på otydligheter i nätverksdokumentation, leder till intermittenta driftstörningar i form av långa fördröjningar och time-outer. Det visar sig ett par komponenter har fått samma IP-adresser. Att IP-adresserna redan var upptagna var inte klart utifrån den befintliga dokumentationen.

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 10.1.1 ”Dokumenterade driftsrutiner”

5.4.2 Avsaknad av dokumentation vilket leder till driftstörning

Beskrivning
Dokumentation är en grundläggande informationselement som över tid beständigt kan beskriva tekniska och andra egenskaper hos det objekt för vilket dokumentationen avser.

IT-miljön saknar väsentliga dokumentationsdelar, exempelvis i form av nätverksdokumentation, systemdokumentation, driftsdokumentation, användardokumentation, med mera.

Kategori
Tekniska hot, administrativa hot

Orsak/Aktör
Handhavandefel, felbeslut, kompetensbrist

Exempel

- Avsaknad av uppdaterade nätverkskartor
- Avsaknad av uppdaterade IP-adresslistor och IP-planer
- Avsaknad av funktionsbeskrivning vilket leder till att det inte är klart vilken funktionalitet som finns och erbjuds i lösningen, t.ex. att det finns en DNS-server på vilken andra tjänster är beroende
- Avsaknad av driftsdokumentation som beskriver löpande rutiner, exempelvis säkerhetskopiering.

Exempel på potentiella konsekvenser

- Avsaknad av beskrivning av routing och nätverkstopologi, vilket leder till att ”default route” sätts felaktigt på en nyinstallerad datorkomponent, vilket i sin tur leder till att den inte kommer in och ansluts på ett korrekt sätt i IT-miljön. Detta kan vara en ny server i SCADA-miljön eller exempelvis en RTU som skall fjärrkontrolleras via nätverket.

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 10.1.1 ”Dokumenterade driftsrutiner”
SS-ISO/IEC 27002:2005 kap 10.1.2 ”Ändringshantering”

5.4.3 Otillräckligt, eller felaktigt, uttestade programuppdateringar

Beskrivning
Programfel kan finnas latent under långa tidsperioder i installerad programvara. Mjukvaruleverantörer ger periodiskt eller i på förekommen anledning ut programvarauppdateringar som lagar olika typer av felaktigheter i program. Programuppdateringarna kan ibland hantera och tillrättalägga enklare programfel, ibland tillföra ny funktionalitet och ibland ändra programkod som innehåller säkerhetshål eller har säkerhetsproblem. Dessa programvaruuppdateringar kallas ibland för patchar, fixar, hotfixar (vissa typer av fixar från Microsoft), CPU (Critical Program Update, namn som leverantören Oracle använder) etc. Det har hänt att patchar i sig introducerar nya fel, till exempel att de inneburit att system kraschat eller hängt, att applikationer slutar fungera, att nya säkerhetshål har öppnats upp. Ibland beror dessa problem på den kombination av programvara eller de förutsättningar som gäller i den lokala IT-miljön. Det är därför viktig att patchar testas lokalt innan de införs i den lokala produktionsmiljön.
.

Kategori
Tekniskt hot, administrativt hot

Orsak/Aktör
Handhavandefel, felbeslut

Exempel

- Patchningen utförs direkt mot produktionssystem, då det är bråttom och viktigt att patchen läggs på för att hantera en annan driftstörning
- Hårdvaruleverantören utger uppgraderingar av firmwara för grundläggande hårdvarukomponenter, såsom nätverkskort eller diskkontrollerkort. Dessa testas inte tillräckligt innan de införs i produktionssystemet, eftersom det inte finns något testsystem med motsvarande hårdvara installerad. Testsystemet finns vara i en virtuell miljö.
- Systemleverantören utger patchar för grundläggande systemprogramvaran, operativsystemet
- Systemleverantören utger patchar för systemkomponenter, exempelvis databassubsystem. Dessa testas inte tillräckligt innan de införs i produktionssystemet, eftersom det inte finns något testsystem med databassubsystem installerad på motsvarande sätt. Testsystemet finns vara i en virtuell miljö och den databas som används ingår i det allmänna databashotellet (databas delad med många andra applikationer)

Exempel på potentiella konsekvenser

- Databasen på en historian blir korrupt som ett resultat av att patchar av databasprogramvaran läggs in utan att detta har stämts av mot SCADA-systemets leverantör.
- Firmwareuppgraderingar av ett SAN-skåp i ett lagringsnät gör att nya driftstörningar introduceras. Servrar som nyttjar diskar i lagringsnätet tappar periodiskt kontakten med lagringsservern. Detta leder till att SCADA-servrarna periodvis hänger och inte kan kontrollera eller övervaka den fysiska processen

Referenser
SS-ISO/IEC 27002:2005 kap 10.1.1 ”Dokumenterade driftsrutiner”
SS-ISO/IEC 27002:2005 kap 10.1.2 ”Ändringshantering”

5.4.4 Kommunikationsfel på lokalt nät med driftstörning som följd

Beskrivning
Mycket av den moderna användningen av IT åtföljs av datorkommunikation mellan olika IT-system. Att kommunikationen finns och fungerar är således en livsnerv. Inte sällan finns det reservvägar och alternativa kommunikationsmetoder för att kunna klara kommunikations-störnningar. Vid kortare kommunikationsavbrott kan vissa lösningar vara utformade så att system och distribuerad utrustning kan fortsätta att fungera autonomt. Vid längre kommunikationsstörningar och avbrott kan det få en direkt påverkan på verksamheten.

Kategori
Tekniskt hot

Orsak/Aktör
Tekniska fel, handhavandefel, väder, antagonistiska fel

Exempel
- Radioutrustning som störts ut
- På grund av rådande väderförhållanden är satellitkommunikation, som reservkanal, är utslagen samtidigt som den primära kommunikationskanalen
- WAN-länkar som temporärt blivit otillgängliga på grund av kabelbrott
- Störningar på lokala nätsegment som en följd av felaktigt ansluten utrustning

Exempel på potentiella konsekvenser
- HMI kan inte prata med backend-system och visar därför upp processöversikter som inte är aktuella
- Information som skall skickas från utrustning och servrar till historian kan inte skickas, utan paket tappas, varpå historian-informationen inte blir komplett
- Kommunikation mellan ICS-servrar och PLC/RTU blir utstörd varpå kommandon från det centrala systemet inte kan styra de distribuerade enheterna i fält.
- Kriskommunikation störs ut eller slås ut helt

Se också
5.4.5

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.1 ”Placering och skydd av utrustning”
SS-ISO/IEC 27002:2005 kap 9.2.2 ”Tekniska försörjningssystem”
SS-ISO/IEC 27002:2005 kap 9.2.5 ”Säkerhet för utrustning utanför egna lokaler”
SS-ISO/IEC 27002:2005 kap 10 ”Styrning av kommunikation och drift”
ISO/IEC 27002:2005 kap 11.6.2 ”Isolering av känsliga system”
SS-ISO/IEC 27002:2005 kap 14.1.4 ”Ramverk för kontinuitetsplanering i verksamheten”
ISO/IEC 27019:2013 kap 14.2.1 ”Emergency communication”

5.4.5 Kommunikationsfel på regionalt nät med driftstörning som följd

Beskrivning
Mycket av den moderna användningen av IT åtföljs av datorkommunikation mellan olika IT-system. Att kommunikationen finns och fungerar är således en livsnerv. Inte sällan finns det reservvägar och alternativa kommunikationsmetoder för att kunna klara kommunikations-störnningar. Vid kortare kommunikationsavbrott kan vissa lösningar vara utformade så att system och distribuerad utrustning kan fortsätta att fungera autonomt. Vid längre kommunikationsstörningar och avbrott kan det få en direkt påverkan på verksamheten.

Kategori
Tekniskt hot

Orsak/Aktör
Tekniska fel, handhavandefel, väder, antagonistiska fel

Exempel
- Radioutrustning som störts ut
- På grund av rådande väderförhållanden är satellitkommunikation, som reservkanal, är utslagen samtidigt som den primära kommunikationskanalen
- WAN-länkar som temporärt blivit otillgängliga på grund av kabelbrott
- Störningar på lokala nätsegment som en följd av felaktigt ansluten utrustning

Exempel på potentiella konsekvenser
- HMI kan inte prata med backend-system och visar därför upp processöversikter som inte är aktuella
- Information som skall skickas från utrustning och servrar till historian kan inte skickas, utan paket tappas, varpå historian-informationen inte blir komplett
- Kommunikation mellan ICS-servrar och PLC/RTU blir utstörd varpå kommandon från det centrala systemet inte kan styra de distribuerade enheterna i fält.
- Kriskommunikation störs ut eller slås ut helt

Se också
5.4.4, 5.4.6

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.1 ”Placering och skydd av utrustning”
SS-ISO/IEC 27002:2005 kap 9.2.2 ”Tekniska försörjningssystem”
SS-ISO/IEC 27002:2005 kap 9.2.5 ”Säkerhet för utrustning utanför egna lokaler”
SS-ISO/IEC 27002:2005 kap 10 ”Styrning av kommunikation och drift”
SS-ISO/IEC 27002:2005 kap 14.1.4 ”Ramverk för kontinuitetsplanering i verksamheten”
ISO/IEC 27019:2013 kap 14.2.1 ”Emergency communication”

5.4.6 Felaktiga kablage som medför glapp eller andra fel

Beskrivning
Eftersom datorkommunikation är en central del i all modern IT, så är det viktigt att den fysiska infrastrukturen för datorkommunikationen är felfri. Kabelfel är en felkälla med många olika facetter och varianter.

Kategori
Tekniskt hot, fysiskt hot

Orsak/Aktör
Tekniskt fel, handhavandefel av installatör, fabrikationsfel

Exempel

- Ethernetkablar som saknar hake för att knäppa fast kontakten i nätverksporten
- Glapp mellan kabel och kontakt
- Felaktigt fastlödda kontakter
- Fiberkablar som blivit felaktigt svetsade
- Fiberkablar som blivit klämda eller böjda så att fibrerna skadats
- Fiberkontakter som blivit nedsmutsade

Exempel på potentiella konsekvenser

- HMI kan inte prata med backend-system och visar därför upp processöversikter som inte är aktuella
- Information som skall skickas från utrustning och servrar till historian kan inte skickas, utan paket tappas, varpå historian-informationen inte blir komplett
- Kommunikation mellan ICS-servrar och PLC/RTU blir utstörd varpå kommandon från det centrala systemet inte kan styra de distribuerade enheterna i fält.

Se också
5.4.4, 5.4.5

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.1 ”Placering och skydd av utrustning”
SS-ISO/IEC 27002:2005 kap 9.2.2 ”Tekniska försörjningssystem”
SS-ISO/IEC 27002:2005 kap 9.2.5 ”Säkerhet för utrustning utanför egna lokaler”
SS-ISO/IEC 27002:2005 kap 10 ”Styrning av kommunikation och drift”
SS-ISO/IEC 27002:2005 kap 14.1.4 ”Ramverk för kontinuitetsplanering i verksamheten”
ISO/IEC 27019:2013 kap 14.2.1 ”Emergency communication”

5.4.7 Felaktigt underhållsarbete

Beskrivning
Underhållsarbete i anläggning är en typ av arbete som kan leda till såväl temporära stopp men också till följdfel eller fel som uppstår på grund av att den som utförde det första underhållsarbetet inte var medveten om den utrustningen som fanns i fält.

Kategori
Tekniskt hot, administrativt hot

Orsak/Aktör
Handhavandefel**,** tekniska fel

Exempel

- Elektriska arbeten med reservkraft som leder till att annan utrustning som sitter på reservkraftverket blir utan ström när arbetet påbörjas
- Elektriska arbeten med datornätverk som leder till att felaktiga spänningsnivåer och strömnivåer leds ut i datornätverket med fysisk förstörelse av anslutna komponenter, eller dess nätverkskort, som följd

Exempel på potentiella konsekvenser

- Elektriska arbeten med reservkraft som leder till att annan utrustning som sitter på reservkraftverket (t.ex. servrar till DCS- eller SCADA-system) blir utan ström när arbetet påbörjas

Se också
5.4.8

Referenser
SS-ISO/IEC 27002:2005 kap 14.1.4 ”Ramverk för kontinuitetsplanering i verksamheten”

5.4.8 Systemförändringar utanför planerade underhållsfönster

Beskrivning
Underhållsfönser är tidsperioder för vilka man planerar in olika typer av systemarbete som skall utföras i datorer, på nätverk, med mjukvaruuppdateringar och liknande.

I IT-sammanhang innebär ofta underhållsfönster att arbete utförs utanför ordinarie arbetstid, t.ex. på helger eller nätter. Ett problem uppstår när IT-underhåll sköts utanför ordinarie inplanerade underhållsfönster, vilket kan leda till störningar och problem i övriga system (IT-system, automationssystem, mm) som uppstår som en konsekvens.

Kategori
Tekniskt hot, administrativt hot

Orsak/Aktör
Handhavandefel, planeringsfel, avsaknad av helhetssyn

Exempel
- Mjukvaruupgradering av företagets mailservrar samtidigt som ett arbete med nätverksanslutningen till internet utförs. Detta försvårar möjligheten att testa att mailservern har kommit igång igen och fungerar som det skall, eftersom ingen extern e-post kan skickas eller tas emot.
- Underhåll av företagets integrationsnav samtidigt som ett viktigt system som ansluter till integrationsnavet också underhålls.
- Programvaruuppdatering av klientarbetsstationer samtidigt som det pågår en storstörning och alla arbetsstationer i ett kontrollrum måste vara åkomliga och kunna hållas bemannade.

Exempel på potentiella konsekvenser
- Möjlighet att ha kontrollrummet bemannat och att kunna styra arbetet därifrån kan påverkas negativt i samband med att underhållsarbete sammanfaller och stör verksamhet under ett kritiskt skede
- Att IT-underhållet sker på tid när det inte stör kan leda till driftstörningar för processtyrningen vid tidpunkter då man är dåligt bemannade, exempelvis nattetid.

Se också
5.4.7, 5.4.9

Referenser
SS-ISO/IEC 27002:2005 kap 14.1.4 ”Ramverk för kontinuitetsplanering i verksamheten”

5.4.9 Icke samordnade underhållsfönster

Beskrivning
Underhållsfönser är tidsperioder för vilka man planerar in olika typer av systemarbete som skall utföras i datorer, på nätverk, med mjukvaruuppdateringar och liknande.

I IT-sammanhang innebär ofta underhållsfönster att arbete utförs utanför ordinarie arbetstid, t.ex. på helger eller nätter. Ett problem uppstår när IT-underhåll sköts utanför ordinarie arbetstid är att ordinarie processkontrollpersonal inte är på plats att hantera eventuella störningar och problem som uppstår som en konsekvens.

Kategori
Tekniskt hot, administrativt hot

Orsak/Aktör
Handhavandefel, planeringsfel, avsaknad av helhetssyn

Exempel
- Mjukvaruupgradering av företagets mailservrar samtidigt som ett arbete med nätverksanslutningen till internet utförs. Detta försvårar möjligheten att testa att mailservern har kommit igång igen och fungerar som det skall, eftersom ingen extern e-post kan skickas eller tas emot.
- Underhåll av företagets integrationsnav samtidigt som ett viktigt system som ansluter till integrationsnavet också underhålls.
- Programvaruuppdatering av klientarbetsstationer samtidigt som det pågår en storstörning och alla arbetsstationer i ett kontrollrum måste vara åkomliga och kunna hållas bemannade.

Exempel på potentiella konsekvenser
- Möjlighet att ha kontrollrummet bemannat och att kunna styra arbetet därifrån kan påverkas negativt i samband med att underhållsarbete sammanfaller och stör verksamhet under ett kritiskt skede
- Att IT-underhållet sker på tid när det inte stör kan leda till driftstörningar för processtyrningen vid tidpunkter då man är dåligt bemannade, exempelvis nattetid.

Se också
5.4.7, 5.4.8

Referenser
SS-ISO/IEC 27002:2005 kap 14.1.4 ”Ramverk för kontinuitetsplanering i verksamheten”

5.4.10 Test och utveckling i produktionsmiljö

Beskrivning
Vid avsaknad av en riktig utvecklingsmiljö kan ibland utveckling helt eller delvis utföras i den produktionssatta miljön, där förändringar av produktionsmiljön till följd av utvecklingsarbete kan få Vid avsaknad av en riktig testmiljö kan ibland testning helt eller delvis utföras i den produktionssatta miljön, där förändringar av produktionsmiljön till följd av testning och testarbete kan få påverkan på de egentliga tjänsterna.

Kategori
Administrativt hot, tekniskt hot

Orsak/Aktör
Intern/extern

Exempel
- Installation av nya versioner av programbibliotek (t.ex. .DLL-filer) som krävs för en testa en ny version av programvaran gör att den nuvarande installerade versionen av programvara delvis slutar fungera.
- För att utvecklingen skall kunna utföras i samma server som den produktionssatta servern, så installeras utvecklingsverktyg, debug-verktyg och testverktyg i samma miljö. Dessa extra verktyg kan användas av en angripare för att lättare manipulera systemet, installerade applikationer.

Exempel på potentiella konsekvenser
- Ett SCADA-system får intermitenta fel på grund av att det installerats nya programbibliotek (.DLL-filer) som gör att vissa funktioner i den underliggande programkomponenter har blivit ändrade
- Att köra testning i produktionsmiljön ledde till att testfall påverkade PLC-utrustningen och de inställningar som finns där för att styra processen.

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 10.1.4 ”Uppdelning av utvecklings-, test- och driftresurser”
ISO/IEC 27019:2013 kap 10.1.4 ”Separation of development, test and operational facilities”
ISO/IEC 27019:2013 kap 12.4.1 ”Control of operational software”

5.4.11 Felaktigt utförd produktionssättning med driftstörning som följd

Beskrivning
Produktionssättning är den procedur som innebär att hård- och mjukvara sätts in i produktionsmiljö och startas. Denna drifttagning kan vara omgärdad med formella rutiner och formella krav.
Produktionssättning av ny mjukvara kräver viss testning och inkörning av de nya mjukvarukomponenterna.
Produktionssättning av ny hårdvara kräver viss testning och inkörning av de nya komponenterna.

Kategori
Administrativt hot, tekniskt hot

Orsak/Aktör
Felaktig testning, fel driftsättningsteknik, fel rutiner

Exempel

- Produktionssättning av programvara som inte testats tillräckligt mycket innan stjälva produktionsättningen leder till att intermittenta fel uppstår
- Installation av hårdvara vars uppsättning inte har testats tillräckligt mycket innan själva produktionssättningen leder till att inte rätt prestanda uppnås för att spara disk.
- Produktionssättning av ändrade parametrar och inställningar som påverkar systemets funktion på ett oförväntat sätt

Exempel på potentiella konsekvenser

- Nätverksstörningar som i sin tur påverkar industriella styrsystemet och dess möjlighet att styra processen
- Produktionssättningen är inte testad i sig i ett testsystem eller verifikationsmiljö, vilket gör att drifttagandet och driftövergången i sig påverkar styrningen av den industriella styrprocessen.

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 10.1.4 ”uppdelning av utvecklings-, test- och driftresurser”

5.4.12 Felaktigt utförda säkerhetstester med driftstörning som följd

Beskrivning
Säkerhetstester är testning där målet är att kunna undersöka säkerhetsnivån i ett installerat system eller i en IT-miljö. Säkerhetstesterna utförs med hjälp av olika testverktyg som är anpassade att utföra angrepp och attacker.

Dessa säkerhetstester kallas ibland penetrationstester då de simulerar en aktiv angripares möjlighet att via nätverket ta sig in i systemet.

Ibland måste säkerhetstesterna utföras i driftsatt miljö på grund av att inga andra alternativa testmiljöer finns tillgängliga.

Kategori
Tekniskt hot

Orsak/Aktör
Felaktig testning, fel driftsättningsteknik, fel rutiner

Exempel

- Penetrationstest som av misstag överutnyttjar kommunikationsbandbredd eller systemresurser, vilket får till effekt att funktioner störs eller slås ut med driftstörning som följd
- Penetrationstestarna glömmer att slå av ”överlastningsattacker” i sitt verktyg vilket får till följd att även denna typ av attacker testas. Dessa attacker lyckas med sin överlastning av nätverk eller systemtjänster
- Penetrationstest som nyttjar attackvertyg som i sin tur gör buffertöverskrivningsattacker och injiceringsattacker av skadlig kod, vilket får till effekt att funktioner störs eller slås ut med driftstörning som följd

Exempel på potentiella konsekvenser

- SCADA-systemet hänger på grund av att penetrationstesterna har förbrukat systemresurser (inte möjligt att starta nya processer, fullt på disk, etc)
- SCADA-systemet hänger på grund av att penetrationstesterna påverkat och hängt en programkomponent som SCADA-systemet väntar på

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 15.2.2 ”Kontroll av teknisk efterlevnad”

5.4.13 Felaktigt installerad strömmatning

Beskrivning
Strömtillförseln till IT-miljön är felaktig, exempelvis underdimensionerad (för lite strömmatning), underdimensionerad kabeldragning, felbalanserad med tanke på fasfördelning, felaktigt installerade kontaktdon, etc

Kategori
Tekniskt fel

Orsak/Aktör
Kompetensbrist, handhavandefel, tekniskt fel

Exempel

- Felaktig anslutning till jord
- Avsaknad av överspänningsskydd
- Avsaknad av avbrottsfri kraft för IT-utrustning
- Avsaknad av avbrottsfri kraft för maskiner
- Felaktig uppmärkning av uttag

Exempel på potentiella konsekvenser

- Driftavbrott på IT-utrustning, processkontrollutrustning, fältutrustning som sitter ansluten till strömmatningen
- Skador på IT-utrustning, processkontrollutrustning, fältutrustning som sitter ansluten till strömmatningen

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.2 ”Tekniska försörjningssystem”

5.4.14 Elektroniskt certifikat som har passerat giltighetsdatum

Beskrivning

De vanligast använda standarderna för elektroniska certifikat X.509 har en inbyggt giltighetstid under vilket certifikatet är giltigt och användbart. När giltighetstiden har passerats så kommer många programvaror som använder sig av elektroniska certifikat att inte godkänna att dessa används.

Kategori
Tekniskt fel, administrativt fel

Orsak/Aktör
Felaktig övervakning, felaktiga kontrollrutiner, felaktiga system

Exempel

- Utgångna elektroniska certifikat kan leda till att inloggningar inte fungerar
- Utgångna elektroniska certifikat kan leda till att kommunikationskanaler inte etableras.

Exempel på potentiella konsekvenser

- Krypterade kanaler mellan ett HMI och en SCADA-server kan inte etableras
- Krypterade kanaler mellan en SCADA-server och en PLC kan inte etableras
- Krypterade kanaler mellan en SCADA-server och en integrationsplattform kan inte etableras
- Webbaserad kommunikation från fältpersonal mot ICS/SCADA-lösning fungerar inte

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 10.9.2 ”Direktanslutna transaktioner”
SS-ISO/IEC 27002:2005 kap 12.3.2 ”Nyckelhantering”
SS-ISO/IEC 27002:2005 kap 15.1.6 ”Reglering av kryptering”

5.5 Hot på nätsäkerhetsnivå

Detta kapitel beskriver ett stort antal olika hot som existerar i nätverk, som är relaterat till datorkommunikation och uppbyggnad av datornätverk som infrastruktur.

5.5.1 Okända informationsflöden, oklara informationsutbyten

Beskrivning
IT-miljöer är ofta uppsatta för lång tid sedan och det sker ständiga förändringar i dom. Att kunna veta vilka system som integrerar med vilka andra system är viktigt för att kunna förstå vilka framtida förändringar som kan göras.

Inte sällan finns det i IT-miljön olika typer av dataytbyten och informationsflöden som: Innehåller okänd information, går i okända riktningar, går mellan okända system och noder. Det är en utmaning att i en sådan miljö försöka börja dokumentera upp trafikmönster.

Kategori
Tekniska hot, administrativa hot

Orsak/Aktör
Ej utförd inventering, ej utförd dokumentation, kompetensbrist

Exempel
- Informationsutbyte mellan SCADA-system och verksamhetssystem som inte är dokumenterat
- Informationsutbyte mellan processinformationssystem och miljöövervakningssystem som inte är dokumenterat
- Filöverföring mellan verksamhetssystem och SCADA-system. Oklart vilka filer och vilka trafikriktningar som gäller för filöverföringen
- Intern DNS-uppsättning och domännamnsinformation är tillgänglig för externa.

Exempel på potentiella konsekvenser
- Ändringar i brandväggsinställningar kan påverka trafik och överförd data, som helt plötsligt blockeras och därmed påverkar integrationer mot SCADA/IECS-miljön
- Okända informationsutbytesvägar påverkas i samband med underhållsarbete på delar av ett nätverk, vilket påverkar informationsutlämning/informationsinhämtning till SCADA/IECS-miljön

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 12.5.4 ”Informationsläckor”
SS-ISO/IEC 27002:2005 kap 10.8.1 ”Policyer och rutiner för informationsutbyte”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”

5.5.2 Felaktigheter i katalogserver för domännamnshantering

Beskrivning
Domännamnskatalogen DNS. DNS är en distribuerad databas i vilket dator- och domännamn för olika datorer finns lagrade. Denna databas tillfrågas i samband med namnuppslagningar där dator- och domännamn översätts till såkallade IP-adresser.

Kategori
Tekniskt fel, administrativt fel

Orsak/Aktör
Handhavandefel, kompetensbrist, slarv, felaktig dokumentation

Exempel
- Felaktig information i domännamnsservern, så att namnuppslagningar inte fungerar som de skall. Detta resulterar i fördröjningar i samband med namnuppslagning.
- Avsaknad av information i domännamnsservern, så att namnuppslagningar inte fungerar som de skall. Detta resulterar i fördröjningar i samband med namnuppslagning.

Exempel på potentiella konsekvenser
- I en SCADA-server uppstår intermittenta fördröjningar och ”hängningar” eftersom det finns beroenden och kopplingar mot en domännamnsserver som inte går att nå, exempelvis på grund av felaktigheter i katalogens konfiguration

Se också
5.7.2, 5.7.3, 5.7.4, 5.7.5

Referenser
SS-ISO/IEC 27002:2005 kap 11.4.6 ”Styrning av nätverksanslutning”
SS-ISO/IEC 27002:2005 kap 11.4.7 ”Styrning av routing”

5.5.3 Obehörig åtkomst till managementinterface

Beskrivning
På mycket infrastrukturutrustning finns det särskilda administratörsinterface som tillåter specialåtkomst till utrustningens inställningar samt åtkomst till olika gränssnitt (webb eller kommandoradsåtkomst) för systemåtkomst och systemadministrativa åtgärder

Kategori
Tekniskt fel

Orsak/Aktör
Antagonist, Felaktig nätverksdesign, tekniskt fel, slarvigt uppsatt skydd

Exempel
- Obehörig åtkomst till s.k. ILO-interface som möjliggör systemadministrativ åtkomst till en utrustning, exempelvis för att kunna stänga av strömmen till utrustningen.
- Webinterface för fjärradministration är fortfarande aktiverat på nätverksutrustning, tillsammans med standardkonto och standardlösenord
- Telnetinterface för fjärradministration är fortfarande aktiverat på nätverksutrustning, tillsammans med standardkonto och standardlösenord
- Seriell konsolport för administration är fortfarande aktiverat på nätverksutrustning, tillsammans med standardkonto och standardlösenord

Exempel på potentiella konsekvenser
- Många PLC/RTU/IED-utrustningar har en, ofta oskyddad, konsolport via vilken man kan få systemadministrativ åtkomst till utrustningen. Obehörig åtkomst till denna kan innebära att systemförändringar kan göras, att inställningar i utrustningen kan förändras vilket i förlängningen kan påverka hur man övervakar eller styr den fysiska processen
- Många PLC/RTU/IED-utrustningar har nätverksmässiga gränssnitt, ofta via en webbingång men också via telnet eller ssh-ingångar, via vilken man kan få systemadministrativ åtkomst till utrustningen. Obehörig åtkomst till denna kan innebära att systemförändringar kan göras, att inställningar i utrustningen kan förändras vilket i förlängningen kan påverka hur man övervakar eller styr den fysiska processen

Se också
5.5.4, 5.8.4

Referenser
SS-ISO/IEC 27002:2005 kap 9.2 ”skydd av utrustning”,
SS-ISO/IEC 27002:2005 kap 10.8.1 ”policyer och rutiner för informationsutbyte”
SS-ISO/IEC 27002:2005 kap 11.4.4 ”Skydd av extern diagnos- och konfigurationsport”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”
ISO/IEC 27019:2013 kap 11.1.1 ”Access control policy”
ISO/IEC 27019:2013 kap 11.3.1 ”Password use”

5.5.4 Obehörig åtkomst till fjärrövervakningsinterface

Beskrivning
Mycket infrastrukturutrustning, såsom servrar, nätverksutrustning, lagringsutrustning och liknande har inbyggda fjärrövervakningsinterface. Via dessa gränssnitt går det att övervaka utrustningens funktionalitet och tillgänglighet.

Även många ICS-komponenter såsom PLC:er eller IEDer har också inbyggd fjärrövervaknings-interface, såsom SNMP[1]-gränssnitt, för att tillåta övervakning av utrustningens funktionalitet och tillgänglighet.

Ett vanligt problem är att ”lösenordet” för många fjärröverfakningsinterface är välkända, såsom ifallet med SNMP där man använder såkallade ”community names” som är mer än väl kända.

Kategori
Tekniskt fel

Orsak/Aktör
Antagonist, Felaktig nätverksdesign, tekniskt fel, slarvigt uppsatt skydd

Exempel
- Obehörig åtkomst till s.k. SNMP-interface som möjliggör systemadministrativ åtkomst till en utrustning, exempelvis för att *kunna läsa ut information* om utrustningen eller om infrastruktur.
- Obehörig åtkomst till s.k. SNMP-interface som möjliggör systemadministrativ åtkomst till en utrustning, exempelvis för att *kunna fjärrförändra inställningar* i utrustningen.

Exempel på potentiella konsekvenser
- Om en PLC med SNMP-tjänsten aktiv har standard ”lösenord” för SNMP-tjänsten så kan någon obehörigen ansluta mot PLC:n och därefter *ta ut olika* inställningar och konfigurationsparametrar.
- Om en RTU med SNMP-tjänsten aktiv har standard ”lösenord” för SNMP-tjänsten så kan någon obehörigen ansluta mot RTU:n och därefter *ändra eller påverka* inställningar och konfigurationsparametrar.

Se också
5.5.3, 5.5.5

Referenser
SS-ISO/IEC 27002:2005 kap 9.2 ”skydd av utrustning”,
SS-ISO/IEC 27002:2005 kap 10.8.1 ”policyer och rutiner för informationsutbyte”
SS-ISO/IEC 27002:2005 kap 11.4.4 ”Skydd av extern diagnos- och konfigurationsport”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”
ISO/IEC 27019:2013 kap 11.1.1 ”Access control policy”
ISO/IEC 27019:2013 kap 11.3.1 ”Password use”

[1] Simple Network Management Protocol

5.5.5 Exponering av intern infrastruktur

Beskrivning
Ofta finns det en särskillnad på externt synlig och intern IT-infrastruktur i en organisation. Externt synlig och åtkomlig är enbart vissa nättjänster som behövs för att kunna utväxla information eller erbjuda tjänster.

Kategori
Tekniskt hot

Orsak/Aktör
Felaktig nätverksdesign, handhavandefel, tekniskt fel

Exempel
- Adressöversättning som inte skyddar och blockerar insyn i hur de interna nätverksadresserna ser ut
- Routinginformation som via routingprotokoll läcker ut så att externa parter kan se och analysera routingarkitektur
- E-postmeddelanden som innehåller namn på interna domäner och system, vilka har vidarebefordrat eller på andra sätt har hanterat e-postmeddelandet.

Exempel på potentiella konsekvenser
- Kartläggning av intern nättopologi där man kan förstå hur olika nätverk är separerade från varandra, exempelvis hur eller var SCADA- och processkontrollnät är separerade från koncernnät.

Se också
5.5.3, 5.5.4

Referenser
SS-ISO/IEC 27002:2005 kap 9.2 ”skydd av utrustning”
SS-ISO/IEC 27002:2005 kap 10.6.1 ”säkerhetsåtgärder för nätverk”
SS-ISO/IEC 27002:2005 kap 11.4.3 ”identifiering av utrustning i nätverk”
SS-ISO/IEC 27002:2005 kap 11.6.2 ”Isolering av känsliga system”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”

5.5.6 Felaktigt elektroniskt skalskydd

Beskrivning
Det elektroniska skalskyddet är den logiska gräns mellan den egna organisationen och övrig omvärld där ett lager av skydd behövs för att skydda mot åtkomst av interna IT-system och informationsresurser.

Ett felaktigt elektroniskt skalskydd kan vara att det inte skyddar mot alla typer av åtkomst, att det finns luckor i det (exempelvis trådlösa nätverk som öppnar för åtkomst).

Kategori
Tekniskt hot

Orsak/Aktör
Felaktig nätverksdesign, handhavandefel, tekniskt fel

Exempel
- Avsaknad av brandväggar för att separera olika nätverk och därmed skapa ett elektroniskt skalskydd
- Felaktiga inställningar i befintliga brandväggar så att separation och trafikkontroll inte uppnås
- Radiobaserad nätverksteknik används och innebär att det elektroniska skalskyddet utsträcker sig långt utanför fysiskt skalskydd eller fysiskt områdesskydd.

Exempel på potentiella konsekvenser
- Trådlöst nätverk i en anläggning medför att obehöriga utanför områdesskyddet kan nå de datornätverk som finns installerade i anläggningen.
- Trådbundla nätverk som används för att ansluta IP-anslutna övervakningskameror finns utdragna i anläggningen och det kringliggande området inom och utanför skalskyddet. En obehörig kan dra ut kabeln till en kamera och ansluta en egen utrustning. Beroende på hur nätverket ser ut kan säkerhetssystem nås, processkontrollsystem bli åtkomliga, åtkomst till resterande av företagsnätet.

Se också
5.5.5, 5.5.7, 5.5.8

Referenser
SS-ISO/IEC 27002:2005 kap 9.2 ”skydd av utrustning”
SS-ISO/IEC 27002:2005 kap 11.4.3 ”identifiering av utrustning i nätverk”
SS-ISO/IEC 27002:2005 kap 11.4.5 ”nätverkssegmentering”
SS-ISO/IEC 27002:2005 kap 11.6.2 ”Isolering av känsliga system”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”
ISO/IEC 27019:2013 kap 11.4.5 ”Segregation in networks”

5.5.7 Felaktig fysisk separation av olika nätverk

Beskrivning
Ett nätverk får anses vara fysiskt separerat i de fall som två nätverk inte har galvanisk eller fysisk sammankoppling.

Nätverk av olika typ kan behöva fysisk separation från varandra. Det kan finnas såväl säkerhetsmässiga kriteria såväl som formella kriterier för denna typ av separation.

Kategori
Tekniskt hot

Orsak/Aktör
Felaktig nätverksdesign, Handhavandefel, kompetensbrist, tekniskt fel

Exempel
- Två nätverk som ej får kopplas ihop fysiskt blir ändå fysiskt ihopkopplade i en kommunikationsutrustning med avsikten att ”logiskt separera näten i olika VLAN”. När utrustningen i ett senare skede tappar sin nuvarande konfiguration så kopplas nätverken ihop.
- Två nätverk som ej får kopplas ihop fysiskt blir ändå fysiskt ihopkopplade i en kommunikationsutrustning på grund av ett handhavandefel.

Exempel på potentiella konsekvenser
- Säkerhetsnätverket för fysiska säkerhetfunktioner såsom passagesystem, larm, kameraövervakning är sammankopplat med det stations-LAN och anläggningsnät som finns i nätverket i övrigt. Detta medför att någon som kan komma åt en nätverksport för vare sig stations-LAN:et eller för det fysiska säkerhetsnätverket kan nå över och få åtkomst till det andra nätverket.

Se också
5.5.6, 5.5.8

Referenser
SS-ISO/IEC 27002:2005 kap 9.2 ”skydd av utrustning”
SS-ISO/IEC 27002:2005 kap 11.4.3 ”identifiering av utrustning i nätverk”
SS-ISO/IEC 27002:2005 kap 11.4.5 ”nätverkssegmentering”
SS-ISO/IEC 27002:2005 kap 11.4.6 ”styrning av nätverksanslutning”
SS-ISO/IEC 27002:2005 kap 11.6.2 ”Isolering av känsliga system”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”

5.5.8 Felaktig logisk separation av olika nätverk

Beskrivning
Många nätverksutrustningar har möjligheter att införa olika typer av logisk separation av nätverk, till exempel att dela upp bakplan i kommunikationsutrustning, att dela upp nätverk i olika logiska nät med hjälp av virtuella LAN.

Kategori
Tekniskt hot

Orsak/Aktör
Felaktig nätverksdesign, Handhavandefel, tekniskt fel

Exempel
- Två nätverk som ej får kopplas ihop logiskt blir ändå fysiskt ihopkopplade i en kommunikationsutrustning med avsikten att ”logiskt separera näten i olika VLAN”. När utrustningen i ett senare skede tappar sin nuvarande konfiguration så kopplas nätverken ihop.
- Två nätverk som ej får kopplas ihop logiskt eller fysiskt blir ändå fysiskt ihopkopplade i en kommunikationsutrustning på grund av ett handhavandefel.

Exempel på potentiella konsekvenser
- Säkerhetsnätverket för fysiska säkerhetfunktioner såsom passagesystem, larm, kameraövervakning är sammankopplat med det stations-LAN och anläggningsnät som finns i nätverket i övrigt. Detta medför att någon som kan komma åt en nätverksport för vare sig stations-LAN:et eller för det fysiska säkerhetsnätverket kan nå över och få åtkomst till det andra nätverket.

Se också
5.5.6, 5.5.7

Referenser
SS-ISO/IEC 27002:2005 kap 9.2 ”skydd av utrustning”,
SS-ISO/IEC 27002:2005 kap 11.4.3 ”identifiering av utrustning i nätverk”,
SS-ISO/IEC 27002:2005 kap 11.4.5 ”nätverkssegmentering”,
SS-ISO/IEC 27002:2005 kap 11.4.6 ”styrning av nätverksanslutning”,
SS-ISO/IEC 27002:2005 kap 11.6.2 ”Isolering av känsliga system”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”

5.5.9 Felaktig åtkomstkontroll för åtkomst till nätverk

Beskrivning
Felaktig nätverksmässig åtkomstkontroll kan innebära att inte obehörig utrustning låses ute, utan att utrustning kan ansluta till nätverket även fast man tro sig ha installerat och aktiverat någon typ av åtkomstkontroll.

Ett annat namn för nätverksmässig åtkomstkontroll är NAC *(eng. network access control*).
Ett exempel på en nätverksmässig åtkomstkontroll är standarden 802.1x, ett annat är manuell blockering av nätverksportar som inte används och låsning av de nätverksportar som används till den utrustning som är ansluten.

Kategori
Tekniskt hot

Orsak/Aktör
Handhavandefel, tekniskt fel

Exempel
- Vem som helst som har tillgång till ett nätverksuttag kan ansluta valfri datorutrustning och därefter få åtkomst till nätverket och därtill anslutna system
- Vem som helst som är inom radiomässig avstånd för att sända- och mottaga datatrafik kan ansluta valfri datorutrustning och därefter få åtkomst till nätverket och därtill anslutna system
- Det finns kvarglömda modem som ger analog åtkomst in till nätverk eller till ansluten utrustning. Dessa kanske används sällan och för särskilda ändamål, varpå de glöms bort att de även kan användas för annan åtkomst.

Exempel på potentiella konsekvenser
- En fälttekniker ansluter en diagnostik-PC till, vad han tror är ett ofarligt nätverk, där datorn blir virussmittad. Senare ansluts samma dator direkt till ett stations-LAN, där den tillåts ansluta utan att den nätverksmässiga åtkomstkontrollen fungerar, och virussmittan kan sprida sig till andra datorer och annan IT-utrustning på samma stations-LAN.

Se också
5.5.5, 5.5.6, 5.5.7, 5.5.8

Referenser
SS-ISO/IEC 27002:2005 kap 9.2 ”skydd av utrustning”
SS-ISO/IEC 27002:2005 kap 11.4.3 ”identifiering av utrustning i nätverk”
SS-ISO/IEC 27002:2005 kap 11.4.5 ”nätverkssegmentering”
SS-ISO/IEC 27002:2005 kap 11.4.6 ”styrning av nätverksanslutning”
SS-ISO/IEC 27002:2005 kap 11.6.2 ”Isolering av känsliga system”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”

5.5.10 Passiv avlyssning av nätverkstrafik

Beskrivning
Avlyssning kan utföras med linjelyssnare, protokollanalysatorer, spektrumanalysatorer eller liknande utvecklings- och felavhjälpningsmedel. Dessutom finns det specialskrivna program, såkallade sniffers, som har som uppgift att spela in nätverkstrafik och kunna stjäla all eller viss typ av uppfångad information.

Passiv avlyssning innebär att trafiken inte påverkas för att avlyssning skall kunna ske.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, medarbetare som överträder befogenheter

Exempel
- Obehörigt installerad snifferprogramvara installerad på en dator i nätverket spelar in nåbar nättrafik för senare analys från angriparen.
- Obehörig användning av inspelningsfunktion i nätverksutrustning (RMON eller liknande)

Exempel på potentiella konsekvenser
- Avlyssningen fångar upp användarnamn och lösenord som kontinuerligt skickas mellan en SCADA-server och en PLC i vilken det sker nätverksinloggningar för att hämta värden
- Avlyssningen fångar upp användarnamn och lösenord för filöverföringssessioner som kontinuerligt skickas mellan en ICS-server och server som finns på kontornätverket

Se också
5.5.11, 5.5.12, 5.5.13

Referenser
SS-ISO/IEC 27002:2005 kap 9.2 ”skydd av utrustning”,
SS-ISO/IEC 27002:2005 kap 10.8.1 ”policyer och rutiner för informationsutbyte”
SS-ISO/IEC 27002:2005 kap 11.4.4 ”Skydd av extern diagnos- och konfigurationsport”
SS-ISO/IEC 27002:2005 kap 11.5.1 ”säker påloggningsrutin”,
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”
ISO/IEC 27019:2013 kap 11.1.1 ”Access control policy”
ISO/IEC 27019:2013 kap 11.3.1 ”Password use”

5.5.11 Aktiv avlyssning av nätverkstrafik

Beskrivning
Avlyssning kan utföras med linjelyssnare, protokollanalysatorer, spektrumanalysatorer eller liknande utvecklings- och felavhjälpningsmedel. Dessutom finns det specialskrivna program, såkallade sniffers, som har som uppgift att spela in nätverkstrafik och kunna stjäla all eller viss typ av uppfångad information.

Aktiv avlyssning innebär att trafiken påverkas, exempelvis länkats om, för att avlyssning skall kunna utföras.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, medarbetare som överträder befogenheter

Exempel
- Obehörigt installerad snifferprogramvara installerad på en dator i nätverket spelar in nåbar nättrafik för senare analys från angriparen.
- Obehörig användning av inspelningsfunktion i nätverksutrustning (RMON eller liknande)

Exempel på potentiella konsekvenser
- Avlyssningen fångar upp användarnamn och lösenord som kontinuerligt skickas mellan en SCADA-server och en PLC i vilken det sker nätverksinloggningar för att hämta värden
- Avlyssningen fångar upp användarnamn och lösenord för filöverföringssessioner som kontinuerligt skickas mellan en ICS-server och server som finns på kontornätverket

Se också
5.5.10, 5.5.12, 5.5.13, 5.5.15

Referenser
SS-ISO/IEC 27002:2005 kap 9.2 ”skydd av utrustning”,
SS-ISO/IEC 27002:2005 kap 10.8.1 ”policyer och rutiner för informationsutbyte”
SS-ISO/IEC 27002:2005 kap 11.5.1 ”säker påloggningsrutin”,
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”
ISO/IEC 27019:2013 kap 11.1.1 ”Access control policy”
ISO/IEC 27019:2013 kap 11.3.1 ”Password use”

5.5.12 Manipulation av överförd nätverkstrafik

Beskrivning
Datorkommunikation som överförs via nätverk kan manipuleras på många ställen under själva befordran, antingen i någon av de existerande kommunikationsutrustningarna eller via en dator med särskilda program som kopplas in i nätverket.

Om en obehörig utrustning kopplas i serie (eng. inline) i nätverket, så kan ett nätverkspaket fångas upp, analyseras och manipuleras innan det skickas vidare.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, Tekniska fel, medarbetare som överträder befogenheter

Exempel
- Filöverföringar där den överförda filen blir manipulerad, exempelvis ersatt med en virussmittad fil
- Överföring av styrkommandon som blir manipulerade och ersatta med andra kommandon
- Överföring av inläst driftstatus och avlästa givare blir manipulerade och ersatta med andra driftstatus och andra givarvärden
- Tekniska fel i nätverket gör att bitfel uppstår och enstaka paket blir felaktiga

Exempel på potentiella konsekvenser
- Inläst övervakningsdata som visar att en transformator håller på och överhettar manipuleras och istället visas att transformatorn håller normal temperatur
- Manipulerat inläst övervakningsdata visar att varvtalet på en stegmotor i en speciell centrifug visar att motorn håller normalt varvtal, medan motorn i själva verket håller en onormal hastighet. Resultatet blir att centrifugen körs på ett sådant sätt att egenfrekvensen uppnås och centrifugen går sönder
- Ett styrkommando som skall skickas till en PLC förändras av en obehörig som har anslutit utrustning som avlyssnar och sedan manipulerar trafiken. Styrkommandot som avsåg att öppna justera öppningen på en dammlucka gick inte igenom som avsett.

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 9.2 ”skydd av utrustning”,
SS-ISO/IEC 27002:2005 kap 10.8.1 ”policyer och rutiner för informationsutbyte”
SS-ISO/IEC 27002:2005 kap 11.5.1 ”säker påloggningsrutin”,
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”

5.5.13 Obehörig styrning av kommunikationsflöden

Beskrivning
Datorkommunikation som överförs via nätverk kan manipuleras på många ställen under själva befordran, antingen i någon av de existerande kommunikationsutrustningarna eller via en dator med särskilda program som kopplas in i nätverket.

Styrning av kommunikationsflödet sker via så kallad routing. De routers som finns i nätverket utväxlar information sinsemellan och bygger därmed upp en förståelse av nätets topologi och de policybeslut som tagits vad gäller framförande av nätverkstrafik. Påverkan av denna routinginformation medför att man kan styra nätverkstrafikens väg i nätet.

Om en obehörig utrustning kopplas i serie (eng. inline) i nätverket, så kan ett nätverkspaket fångas upp, analyseras och manipuleras innan det skickas vidare.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, medarbetare som överträder befogenheter

Exempel
- Angrepp mot routers, switchar och annan infrastrukturutrustning med tillhörande intrång. I själva utrustningen kan sedan routingval påverkas
- Manipulation av routinginformation som skickas via routingprotokoll mellan routers, vilket sen påverkar vägval och styrning av kommunikationsflöden på nätet

Exempel på potentiella konsekvenser
- nätverkstrafik i ett större distribuerat processkontrollsystem (SCADA) når inte mellan de kommunicerande ändpunkterna på grund av att någon aktivt har påverkat kommunikationsvägarna med påverkan av routingen. Kommunikationen blir effektivt utslagen
- nätverkstrafik i ett större distribuerat processkontrollsystem (SCADA) mellan de kommunicerande ändpunkterna styrs om genom att någon aktivt har påverkat kommunikationsvägarna med hjälp av att påverkan av routingen. Via denna omstyrning kan de avlyssna och manipulera nätverkstrafiken så att styrning och inhämtning av data inte längre är tillitbar.

Se också
5.5.11, 5.5.12

Referenser
SS-ISO/IEC 27002:2005 kap 9.2 ”skydd av utrustning”,
SS-ISO/IEC 27002:2005 kap 10.8.1 ”policyer och rutiner för informationsutbyte”
SS-ISO/IEC 27002:2005 kap 11.5.1 ”säker påloggningsrutin”,
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”

5.5.14 Felaktig innehållskontroll av data överfört på nätverk

Beskrivning
Organisationen har införskaffat någon typ av extra utrustning, alternativt köpt brandväggar som har utökad funktionalitet, för att utföra *innehållskontroll av överförd nätverkstrafik*. Innehållskontroll innebär att inte bara nätverkspaketets pakethuvud med avsändare, mottagare etc kontrolleras utan även det som överförs i själva paketet. Nätpaket kan ha innehåll som man vill analysera och blockera i de fall de exempelvis innehåller skadlig kod.

Kategori
Tekniskt hot

Orsak/Aktör
Designfel, tekniskt fel, handhavandefel

Exempel
- Ingen eller för lite kontroll av webbplatser som används av personer inom organisationen, vilket i sin tur medför att webbplatser med skadlig kod besöks som smittar klientdatorer varifrån webbsurfning utförs.
- Den eller de proxyservrar som organisationen använder är felaktigt uppsatta så att de inte erbjuder det skydd som de förväntas ge.
- Licenser för den innehållskontrollstjänst som används i organisationen har gått ut utan att någon uppmärksammat detta. Som ett resultat av detta sker ingen innehållskontroll längre

Exempel på potentiella konsekvenser
- HMI-datorer i kontrollrummet blir smittade av skadlig kod för att en operatör har surfat på internet på en webbplats som spred skadlig kod.
- En laptop som används som engineering workstation som normalt är kopplat till kontorsnätet har blivit smittad av skadlig kod för att utvecklaren har surfat ifrån datorn. När laptopen senare ansluts till processnätet förs smittan in till den utrustning som är ansluten där.

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 9.2 ”skydd av utrustning”,
SS-ISO/IEC 27002:2005 kap 10.8.1 ”policyer och rutiner för informationsutbyte”
SS-ISO/IEC 27002:2005 kap 11.5.1 ”säker påloggningsrutin”,
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”

5.5.15 Obehörig avsiktlig blockering av nätverkstrafik

Beskrivning
En obehörig person kan med hjälp av programvara påverka trafikflödet i nätverket genom att på olika sätt manipulera nätets styrning. Ett sätt att påverka trafikflödet är att blockera att nätverkstrafik kommer fram.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist

Exempel
- Avsiktligt och uppsåtligt installerat nätverksfilter i kommunikationsutrustning
- Manipulation av s.k. ARP-tabeller och ARP-förfrågningar så att datorers möjlighet att förmedla nätvertrafik slås ut**.**
- Routinginformation manipuleras så att vägval på nätverksnivå blir felaktig
- I radiobaserade nätverk kan andra radiosändare, annan radioteknik eller annan teknisk utrustning som avger radiostrålning (exempelvis mikrovågsugnar) utgöra störkällor.
- Ethernetkiller, att koppla ut starkström i nätverksuttagen, och därmed slå ut kommunikationsutrustning eller ansluten utrustning
- Störsändare som aktivt stör ut radiosignaler för trådlösa nätverk
- Störsändare som aktivt stör ut radiosignaler för satellitkommunikation

Exempel på potentiella konsekvenser
- Nätverkstrafiken mellan ett HMI och en server blockeras så att det inte längre skickas uppdateringar till skärmen och inte heller går att skicka kontrollkommandon från HMI till servern.
- Nätverkstrafiken mellan en PLC och en server blockeras så att det inte längre skickas givarvärden från PLC till servern och att det inte heller går att skicka kontrollkommandon från servern till PLC:n

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 9.2 ”skydd av utrustning”,
SS-ISO/IEC 27002:2005 kap 10.8.1 ”policyer och rutiner för informationsutbyte”
SS-ISO/IEC 27002:2005 kap 11.5.1 ”säker påloggningsrutin”,
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”
ISO/IEC 27019:2013 kap 14.2.1 ”Emergency communication”

5.5.16 Avsaknad av nödkommunikation

Beskrivning
En obehörig person kan med hjälp av programvara påverka trafikflödet i nätverket genom att på olika sätt manipulera nätets styrning. Ett sätt att påverka trafikflödet är att blockera att nätverkstrafik kommer fram. En sådan typ av nätverkstrafik eller kommunikation är så kallad nödkommunikation.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist

Exempel
- På grund av budgetmissar har nödkommunikation inte köpts in
- På grund av planeringsmissar har nödkommunikation inte köpts in
- På grund av planeringsmissar har nödkommunikation köpts in, men inte installerats
- Drifttelefoner saknas
- TETRA/RAKEL-utrustning saknas
- TETRA/RAKEL-utrustning är placerad på annan ort och ej tillgänglig för de som behöver utrustningen
- Satellittelefoner saknas
- Satellittelefoner är placerad på annan ort och ej tillgänglig för de som behöver utrustningen

Se också
5.5.17

Referenser
ISO/IEC 27019:2013 kap 14.2.1 ”Emergency communication”

5.5.17 Obehörig avsiktlig blockering av nödkommunikation

Beskrivning
En obehörig person kan med hjälp av programvara påverka trafikflödet i nätverket genom att på olika sätt manipulera nätets styrning. Ett sätt att påverka trafikflödet är att blockera att nätverkstrafik kommer fram. En sådan typ av nätverkstrafik eller kommunikation är så kallad nödkommunikation.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist

Exempel
- Avsiktligt och uppsåtligt installerat nätverksfilter i kommunikationsutrustning
- Manipulation av s.k. ARP-tabeller och ARP-förfrågningar så att datorers möjlighet att förmedla nätvertrafik slås ut**.**
- Routinginformation manipuleras så att vägval på nätverksnivå blir felaktig
- I radiobaserade nätverk kan andra radiosändare, annan radioteknik eller annan teknisk utrustning som avger radiostrålning (exempelvis mikrovågsugnar) utgöra störkällor.
- Ethernetkiller, att koppla ut starkström i nätverksuttagen, och därmed slå ut kommunikationsutrustning eller ansluten utrustning
- Störsändare som aktivt stör ut radiosignaler för trådlösa nätverk
- Störsändare som aktivt stör ut radiosignaler för satellitkommunikation

Exempel på potentiella konsekvenser
- Telefoni i anläggning slås ut
- Drifttelefoner slås ut
- TETRA/RAKEL-kommunikation slås ut
- Satellittelefoner slås ut

Se också
5.5.16

Referenser
SS-ISO/IEC 27002:2005 kap 9.2 ”skydd av utrustning”,
SS-ISO/IEC 27002:2005 kap 10.8.1 ”policyer och rutiner för informationsutbyte”
SS-ISO/IEC 27002:2005 kap 11.5.1 ”säker påloggningsrutin”,
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”
ISO/IEC 27019:2013 kap 14.2.1 ”Emergency communication”

5.5.18 Avsaknad av loggning från serverdatorer

Beskrivning
Med loggning menas här skapandet och sparande av spårdata i systemet. Denna spårdata kan sedan användas för att påvisa systemaktiviteter. Normalt sett så har serverdatorer en viss nivå av loggning aktiverad som standard, men det går att slå på utökad loggning. Med avsaknad av loggning menar vi här att systemets eller applikationernas inställningar för loggning är fel så att loggning inte utförs, att loggning uttrycklingen blivit avstängt av behörig personal, att loggning blivit avstängt av obehöriga, och liknande

Kategori
Tekniskt hot

Orsak/Aktör
Handhavandefel, designfel, felaktigt uppsatt system

Exempel
- Fullständigt avsaknad av loggning: systemloggar, säkerhetsloggar, felloggar, applikationsloggar
- Partiell avsaknad av loggning: systemloggar, säkerhetsloggar, felloggar, applikationsloggar
- Partiell avsaknad av loggning av en enstaka loggtyp: systemloggar, säkerhetsloggar, felloggar, applikationsloggar

Exempel på potentiella konsekvenser
- Obehöriga försök att komma in i en SCADA-server uppmärksammas inte på grund av att systemloggningen är felaktigt inställd och ingen loggning sker. Inte alla grundläggande aktiviteter loggas.
- Obehöriga försök att komma in i en PLC loggas inte. Loggning är inte aktiverad i PLC alls

Se också
5.5.19, 5.5.20, 5.5.21, 5.5.22, 5.5.25

Referenser
SS-ISO/IEC 27002:2005 kap 10.10.1 ”revisionsloggning”,
SS-ISO/IEC 27002:2005 kap 10.10.2 ”övervakning av systemanvändning”,
SS-ISO/IEC 27002:2005 kap 10.10.3 ”skydd av logginformation”,
SS-ISO/IEC 27002:2005 kap 10.10.4 ”administratörs- och operatörsloggar”,
SS-ISO/IEC 27002:2005 kap 10.10.5 ”loggning av fel”
ISO/IEC 27019:2013 kap 10.10.1 ”Audit logging”

5.5.19 Felaktig loggning från serverdatorer

Beskrivning
Med loggning menas här skapandet och sparande av spårdata i systemet. Denna spårdata kan sedan användas för att påvisa systemaktiviteter. Med felaktig loggning menar vi här att systemets eller applikationernas inställningar för loggning är fel, att det finns något fel i själva uppsättningen av loggningen eller liknande

Kategori
Tekniskt hot

Orsak/Aktör
Handhavandefel, designfel, felaktigt uppsatt system

Exempel
- Loggningen är felinställd, så den visar inte obehöriga systemaktiviteter såsom upprepade försök att starta ett administratörsprogram som kan påverka systeminställningar
- Loggningen är felinställd, så den visar inte obehöriga systemaktiviteter såsom exempelvis upprepade inloggningsförsök, försök att komma åt skyddade informationsobjekt
- Loggningen är felinställd, så den loggar upprepade inloggningsförsök, men den loggar inte lyckade inloggningar. Därför går det inte se ifall de misslyckade försöken följs av ett lyckat försök
- Loggningen är felinställd så den sparar loggdata till en alltför liten disk. Loggarna skrivs över för ofta vilket medför att antalet dagar eller timmar som finns sparade av spårdata är alltför lite för att i praktiken vara användbart vid en felsökning, hantering av säkerhetsincident eller liknande

Exempel på potentiella konsekvenser
- Obehöriga försök att komma in i en SCADA-server uppmärksammas inte på grund av att systemloggningen är felaktigt inställd. Inte alla grundläggande aktiviteter loggas, och de som loggas sparas lokalt i en loggfil som är alltför begränsad.

Se också
5.5.20, 5.5.21, 5.5.22, 5.5.25

Referenser
SS-ISO/IEC 27002:2005 kap 10.10.1 ”revisionsloggning”,
SS-ISO/IEC 27002:2005 kap 10.10.2 ”övervakning av systemanvändning”,
SS-ISO/IEC 27002:2005 kap 10.10.3 ”skydd av logginformation”,
SS-ISO/IEC 27002:2005 kap 10.10.4 ”administratörs- och operatörsloggar”,
SS-ISO/IEC 27002:2005 kap 10.10.5 ”loggning av fel”
ISO/IEC 27019:2013 kap 10.10.1 ”Audit logging”

5.5.20 Avsaknad av loggning från nätverksutrustning

Beskrivning
Med loggning menas här skapandet och sparande av spårdata i systemet. Denna spårdata kan sedan användas för att påvisa systemaktiviteter. Normalt sett så har nätverksutrustning en viss nivå av loggning aktiverad som standard, men det går att slå på utökad loggning. Med avsaknad av loggning menar vi här att systemets eller applikationernas inställningar för loggning är fel så att loggning inte utförs, att loggning uttrycklingen blivit avstängt av behörig personal, att loggning blivit avstängt av obehöriga, och liknande

Kategori
Tekniskt hot

Orsak/Aktör
Handhavandefel, designfel, felaktigt uppsatt system

Exempel
- Routers som inte fjärrloggar händelser i utrustningen, konfigurationsändringar, säkerhetshändelser
- Brandväggar som inte loggar eller fjärrloggar händelser i utrustningen, konfigurationsändringar, säkerhetshändelser

Exempel på potentiella konsekvenser
- Kommunikationsutrustning i anläggningen är inte konfigurerad för att generera logg i händelse av systemfel, säkerhetsöverträdelser, etc. Obehöriga kan utan upptäckt under lång tid försöka hitta olika vägar in i anläggningen och där kunna ansluta till processkontrollssystemets olika komponenter och delar
- Kommunikationsutrustning (router, brandvägg eller liknande) som avskiljer processnätet från företagsnätet i övrigt är inte konfigurerad för att generera logg i händelse av systemfel, säkerhetsöverträdelser, etc. Obehöriga kan utan upptäckt under lång tid försöka hitta olika vägar in i processnätet och där kunna ansluta till processkontrollssystemets olika komponenter och delar

Se också
5.5.18, 5.5.19, 5.5.21, 5.5.22, 5.5.25

Referenser
SS-ISO/IEC 27002:2005 kap 10.10.1 ”revisionsloggning”,
SS-ISO/IEC 27002:2005 kap 10.10.2 ”övervakning av systemanvändning”,
SS-ISO/IEC 27002:2005 kap 10.10.3 ”skydd av logginformation”,
SS-ISO/IEC 27002:2005 kap 10.10.4 ”administratörs- och operatörsloggar”,
SS-ISO/IEC 27002:2005 kap 10.10.5 ”loggning av fel”
ISO/IEC 27019:2013 kap 10.10.1 ”Audit logging”

5.5.21 Felaktig loggning från nätverksutrustning

Beskrivning
Med loggning menas här skapandet och sparande av spårdata i systemet. Denna spårdata kan sedan användas för att påvisa systemaktiviteter. Normalt sett så har nätverksutrustning en viss nivå av loggning aktiverad som standard, men det går att slå på utökad loggning. Med felaktig loggning menar vi här att systemets eller applikationernas inställningar för loggning är fel så att loggning inte utförs,att bara vissa aktiviteter loggas, och liknande

Kategori
Tekniskt hot

Orsak/Aktör
Handhavandefel, designfel, felaktigt uppsatt system

Exempel
- Loggning i router är inställd så att bara vissa typer av administrativa operationer genererar logg eller larm. Andra viktiga förändringar i utrustningen innebär inte larm eller logg
- Brandväggar loggar bara vissa händelser och aktiviteter till exempel att vissa paket blockeras, men inte att andra paket och trafiktyper blockeras
- Brandväggar loggar bara vissa händelser och aktiviteter till exempel att vissa paket blockeras, men inte att annan trafik släpps igenom

Exempel på potentiella konsekvenser
- Kommunikationsutrustning i anläggningen är felaktigt konfigurerad för att ej korrekt generera logg i händelse av systemfel, säkerhetsöverträdelser, etc. Obehöriga kan utan upptäckt under lång tid försöka hitta olika vägar in i anläggningen och där kunna ansluta till processkontrollssystemets olika komponenter och delar
- Kommunikationsutrustning (router, brandvägg eller liknande) som avskiljer processnätet från företagsnätet i övrigt är inte ej korrekt konfigurerad för att generera logg i händelse av systemfel, säkerhetsöverträdelser, etc. Obehöriga kan utan upptäckt under lång tid försöka hitta olika vägar in i processnätet och där kunna ansluta till processkontrollssystemets olika komponenter och delar

Se också
5.5.18, 5.5.19, 5.5.20, 5.5.22, 5.5.25

Referenser
SS-ISO/IEC 27002:2005 kap 10.10.1 ”revisionsloggning”,
SS-ISO/IEC 27002:2005 kap 10.10.2 ”övervakning av systemanvändning”,
SS-ISO/IEC 27002:2005 kap 10.10.3 ”skydd av logginformation”,
SS-ISO/IEC 27002:2005 kap 10.10.4 ”administratörs- och operatörsloggar”,
SS-ISO/IEC 27002:2005 kap 10.10.5 ”loggning av fel”
ISO/IEC 27019:2013 kap 10.10.1 ”Audit logging”

5.5.22 Avsaknad av loggning från SCADA/IECS-utrustning

Beskrivning
Med loggning menas här skapandet och sparande av spårdata i systemet. Denna spårdata kan sedan användas för att påvisa systemaktiviteter. Normalt sett så har nätverksutrustning en viss nivå av loggning aktiverad som standard, men det går att slå på utökad loggning. Med avsaknad av loggning menar vi här att systemets eller applikationernas inte har kapacitet eller funktionalitet att skapa logg, att inställningar för loggning är fel så att loggning inte utförs, att bara vissa aktiviteter loggas, och liknande

Kategori
Tekniskt hot

Orsak/Aktör
Handhavandefel, designfel, felaktigt uppsatt system

Exempel
- Felaktiga inloggningsförsök i PLC/RTU/IED loggas inte
- Förändringar i layout och funktionalitet i HMI loggas inte
- Addering av nya användare i SCADA-systemet loggas inte
- Ändring av användarrättigheter i SCADA-systemet loggas inte
- Tillägg till SQL-kod i bakomliggande databas loggas inte

Exempel på potentiella konsekvenser
- Nya logik laddas in i en PLC och själva funktionaliteten ändras. Detta loggas inte. PLCns funktionalitet ändras så att den fysiska processen inte längre styrs på ett korrekt sätt. Hur länge denna felaktiga styrning har pågått går inte i efterföljande utredning att fastställas
- Nya konton skapas i SCADA/IECS-miljöns utrustning, men denna administrativa åtgärd av säkerhetsnatur loggas inte
- Förändringar i system och komponenter går inte att spåra, så någon kan manipulera komponenter i SCADA/ICS-systemet utan att det går att följa att detta har skett

Se också
5.5.18, 5.5.19, 5.5.20, 5.5.22, 5.5.25

Referenser
SS-ISO/IEC 27002:2005 kap 10.10.1 ”revisionsloggning”,
SS-ISO/IEC 27002:2005 kap 10.10.2 ”övervakning av systemanvändning”,
SS-ISO/IEC 27002:2005 kap 10.10.3 ”skydd av logginformation”,
SS-ISO/IEC 27002:2005 kap 10.10.4 ”administratörs- och operatörsloggar”,
SS-ISO/IEC 27002:2005 kap 10.10.5 ”loggning av fel”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”
ISO/IEC 27019:2013 kap 10.10.1 ”Audit logging”

5.5.23 Felaktig loggning från SCADA-utrustning

Beskrivning
Med loggning menas här skapandet och sparande av spårdata i systemet. Denna spårdata kan sedan användas för att påvisa systemaktiviteter. Normalt sett så har nätverksutrustning en viss nivå av loggning aktiverad som standard, men det går att slå på utökad loggning. Med felaktig loggning menar vi här att systemets eller applikationernas inställningar för loggning är fel så att loggning inte utförs,att bara vissa aktiviteter loggas, och liknande

Kategori
Tekniskt hot

Orsak/Aktör
Handhavandefel, designfel, felaktigt uppsatt system

Exempel
- Inloggningsförsök i PLC/RTU/IED loggas inte korrekt. Tidsstämplar är helt fel jämfört med korrekt tidpunkt för den aktuella händelsen.
- Inloggningsförsök i PLC/RTU/IED loggas inte korrekt. IP-adresser för källaadressen där inloggningsförsöken skedde ifrån finns inte med i logginformationen.
- Omstart av PLC/RTU/IED loggas inte korrekt.

Exempel på potentiella konsekvenser
- Nya logik laddas in i en PLC och själva funktionaliteten ändras. Detta loggas inte. PLCns funktionalitet ändras så att den fysiska processen inte längre styrs på ett korrekt sätt. Hur länge denna felaktiga styrning har pågått går inte i efterföljande utredning att fastställas
- Förändringar i system och komponenter går inte att spåra, så någon kan manipulera komponenter i SCADA/ICS-systemet utan att det går att följa att detta har skett

Se också
5.5.18, 5.5.19, 5.5.20, 5.5.22, 5.5.25

Referenser
SS-ISO/IEC 27002:2005 kap 10.10.1 ”revisionsloggning”,
SS-ISO/IEC 27002:2005 kap 10.10.2 ”övervakning av systemanvändning”,
SS-ISO/IEC 27002:2005 kap 10.10.3 ”skydd av logginformation”,
SS-ISO/IEC 27002:2005 kap 10.10.4 ”administratörs- och operatörsloggar”,
SS-ISO/IEC 27002:2005 kap 10.10.5 ”loggning av fel”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”
ISO/IEC 27019:2013 kap 10.10.1 ”Audit logging”

5.5.24 Avsaknad av loggning från säkerhetsfunktioner

Beskrivning
Med loggning menas här skapandet och sparande av spårdata i systemet. Denna spårdata kan sedan användas för att påvisa systemaktiviteter. Loggning av säkerhetsfunktioner inkluderar att generera spårdata för händelser som har säkerhetspåverkan, såsom att skapa nya användare, byta lösenord på en användare, lägga till administrativ behörighet på en användare, att stänga av ett skydd eller en säkerhetskontroll, etc.

Kategori
Tekniskt hot

Orsak/Aktör
Handhavandefel, designfel, felaktigt uppsatt system

Exempel
- Loggning i brandvägg är skapad eller inställd så att den inte loggar blockerad nättrafik. Godkänd trafik genererar ¨heller inga loggar, varpå både misslyckade och lyckade attackförsök kan föregå utan någon spårbarhet.
- Vid intrång i en dator stängs loggningen av. Detta loggas inte eller uppmärksammas inte

Exempel på potentiella konsekvenser
- Nya användare läggs in i SCADA-miljön, utan att någon uppmärksammas att nya användare skapats. Detta då inga loggar eller larm skapats utifrån denna händelse

Se också
5.5.18, 5.5.19, 5.5.20, 5.5.21, 5.5.25

Referenser
SS-ISO/IEC 27002:2005 kap 10.10.1 ”revisionsloggning”,
SS-ISO/IEC 27002:2005 kap 10.10.2 ”övervakning av systemanvändning”,
SS-ISO/IEC 27002:2005 kap 10.10.3 ”skydd av logginformation”,
SS-ISO/IEC 27002:2005 kap 10.10.4 ”administratörs- och operatörsloggar”,
SS-ISO/IEC 27002:2005 kap 10.10.5 ”loggning av fel”
ISO/IEC 27019:2013 kap 10.10.1 ”Audit logging”

5.5.25 Felaktig loggning från säkerhetsfunktioner

Beskrivning
Med loggning menas här skapandet och sparande av spårdata i systemet. Denna spårdata kan sedan användas för att påvisa systemaktiviteter. Loggning av säkerhetsfunktioner inkluderar att generera spårdata för händelser som har säkerhetspåverkan, såsom att skapa nya användare, byta lösenord på en användare, lägga till administrativ behörighet på en användare, att stänga av ett skydd eller en säkerhetskontroll, etc.

Felaktig loggning från säkerhetsfunktioner inkluderar att inte alla händelser loggas, att inte relevant eller nödvändig information (såsom tidpunkt, subjekt (användare) eller objekt (den systemresurs som operationen avser)) saknas.

Kategori
Tekniskt hot

Orsak/Aktör
Tekniskt fel, handhavandefel, designfel

Exempel
- Loggning i brandvägg är inställd så att bara blockerad nättrafik genererar logg eller larm. Godkänd trafik genererar inga loggar, varpå lyckade attackförsök kan föregå utan någon spårbarhet.
- Vid intrång i en dator stängs loggningen av. Detta loggas inte eller uppmärksammas inte

Exempel på potentiella konsekvenser
- Nya användare läggs in i SCADA-miljön, utan att någon uppmärksammas att nya användare skapats. Detta då inga loggar eller larm skapats utifrån denna händelse

Se också
5.5.18, 5.5.19, 5.5.20, 5.5.21, 5.5.22

Referenser
SS-ISO/IEC 27002:2005 kap 10.10.1 ”revisionsloggning”,
SS-ISO/IEC 27002:2005 kap 10.10.2 ”övervakning av systemanvändning”,
SS-ISO/IEC 27002:2005 kap 10.10.3 ”skydd av logginformation”,
SS-ISO/IEC 27002:2005 kap 10.10.4 ”administratörs- och operatörsloggar”,
SS-ISO/IEC 27002:2005 kap 10.10.5 ”loggning av fel”
ISO/IEC 27019:2013 kap 10.10.1 ”Audit logging”
ISO/IEC 27019:2013 kap 11.1.1 ”Access control policy”
ISO/IEC 27019:2013 kap 11.3.1 ”Password use”

5.5.26 Felaktigt skydd av loggar och loggdata

Beskrivning
Den spårdata som skapas och samlas in skyddas inte på rätt sätt. Detta kan medföra att obehöriga kan läsa känslig information som sparas in i loggarna. Beroende på hur loggarna sparas, exempelvis på hur filskyddet för loggfilerna är uppsatt eller hur operativsystemet skyddar åtkomst till filerna, kan det också medföra att obehöriga kan förändra sparade loggar. Vissa loggprotokoll skickar loggar i klartext över nätverket. Det medför att loggarna kan avlyssnas eller förändras när loggdatat är i transit.

Kategori
Tekniskt hot

Orsak/Aktör
Designfel, handhavandefel

Exempel
- En nätverksutrustning skickar loggmeddelanden via syslogprotokollet. Då syslog normalt sett skickar loggmeddelanden i klartext via UDP-protokollet kan en obehörig blockera nätverkstrafiken, avlyssna nätverkstrafiken eller manipulera nätverkstrafiken.

Exempel på potentiella konsekvenser
- Loggmeddelanden från en PLC eller RTU som skickar meddelanden via syslogprotokollet kan manipuleras när de skickas över nätverket. Det kan medföra att viktig information om systemförändringar gås förlorade.

Se också
5.5.18, 5.5.19, 5.5.20, 5.5.21, 5.5.22

Referenser
SS-ISO/IEC 27002:2005 kap 10.10.1 ”revisionsloggning”,
SS-ISO/IEC 27002:2005 kap 10.10.2 ”övervakning av systemanvändning”,
SS-ISO/IEC 27002:2005 kap 10.10.3 ”skydd av logginformation”,
SS-ISO/IEC 27002:2005 kap 10.10.4 ”administratörs- och operatörsloggar”,
SS-ISO/IEC 27002:2005 kap 10.10.5 ”loggning av fel”
ISO/IEC 27019:2013 kap 10.10.1 ”Audit logging”

5.5.27 Avsaknad av tidssynkronisering mellan nätansluten utrustning

Beskrivning
Ett vanligt problem i IT-sammanhang är att utrustning inte håller korrekt tid.
Ett vanligt sätt att få en korrekt och gemensam tidsuppfattning i en IT-miljö är att via datakommunikation synkronisera tid mellan olika utrustning. Detta hot beskriver vad som kan inträffa om man inte har gemensam eller korrekt tidsuppfattning.

Kategori
Tekniskt hot

Orsak/Aktör
Designfel, tekniska fel, handhavandefel

Exempel
- Den lokala klockan i de olika PLC-utrustningarna är satt till lokal tid, men är inte synkroniserade med varandra. Allteftersom utrustningen hålls driftsatt så driver klockornas tidsuppfattning alltmer från varandra.
- Klockan nätverksutrustning är inte synkroniserad, varpå de loggar, SNMP-trappar och liknande larm som genereras från denna utrustning inte innehåller en korrekt tid eller samma tid som annan utrustning i nätverket

Exempel på potentiella konsekvenser
- Avsaknad av tidssynkronisering innebär att loggar inte får korrekta tidsstämplar
- Avsaknad av tidssynkronisering försvårar felsökning när man måste veta exakt när en händelse inträffade
- Avsaknad av tidssynkronisering försvårar incidenthantering när man måste veta exakt när en viss säkerhetspåverkande händelse inträffade

Se också
5.5.28

Referenser
SS-ISO/IEC 27002:2005 kap 10.10.6 ”klocksynkronisering”
ISO/IEC 27019:2013 kap 10.10.6 ”Clock synchronization”

5.5.28 Felaktig tidssynkronisering mellan nätansluten utrustning

Beskrivning
Ett vanligt problem i IT-sammanhang är att utrustning inte håller korrekt tid.
Ett vanligt sätt att få en korrekt och gemensam tidsuppfattning i en IT-miljö är att via datakommunikation synkronisera tid mellan olika utrustning. Detta hot beskriver vad som kan inträffa om man inte har gemensam eller korrekt tidsuppfattning.

Kategori
Tekniskt hot

Orsak/Aktör
Designfel, tekniska fel, handhavandefel

Exempel
- Den lokala klockan i de olika PLC-utrustningarna är satt till lokal tid, men är inte synkroniserade med varandra. Allteftersom utrustningen hålls driftsatt så driver klockornas tidsuppfattning alltmer från varandra.
- Klockan nätverksutrustning är inte synkroniserad, varpå de loggar, SNMP-trappar och liknande larm som genereras från denna utrustning inte innehåller en korrekt tid eller samma tid som annan utrustning i nätverket

Exempel på potentiella konsekvenser
- Felaktig tidssynkronisering leder till att inkomna meddelanden inte processas korrekt när de skall läggas i SCADA/IECS-systemets data historian-lagring.
- Felaktig tidssynkronisering innebär att loggar inte får korrekta tidsstämplar
- Felaktig tidssynkronisering försvårar felsökning när man måste veta exakt när en händelse inträffade
- Felaktig tidssynkronisering försvårar incidenthantering när man måste veta exakt när en viss säkerhetspåverkande händelse inträffade

Se också
5.5.26

Referenser
SS-ISO/IEC 27002:2005 kap 10.10.6 ”klocksynkronisering”
ISO/IEC 27019:2013 kap 10.10.6 ”Clock synchronization”

5.6 Handhavandefel

Med handhavandefel menas olika typer av mänskliga misstag som påverkar informationshanteringen.

5.6.1 Administratörer av IT-systems felaktiga handhavande

Beskrivning
Systemadministratörer är personal som arbetar med drift och förvaltning av IT-system. De har ett viktigt och ansvarsfullt arbete att se till att IT-systemen jämt fungerar och att de fungerar felfritt. När olika typer av fel inträffar måste de utföra felsökning. Om en systemadministratör begår ett handhavandefel kan det få långtgående konsekvenser för systemet tillgänglighet och robusthet, systemet integritet, eller dataintegritet i den information som hanteras av det systemet.

Kategori
Tekniskt hot, administrativt hot

Orsak/Aktör
Handhavandefel

Exempel
- De systemadministratörer som arbetar med installation av nya datorer utför ett undermåligt jobb, vilket lämnar de nyinstallerade datorerna utan tillräckligt skydd
- En systemadministratör som skall göra en förändring av nätverksinställningarna raderar en extra rad i en konfigurationsfil. En nätverkstjänst som skall finnas på systemet blir plötsligt inaktiverad.
- En systemadministratör som skall göra en förändring av nätverksinställningarna klickar fel i ett konfigurationsprogram. En nätverkstjänst som skall finnas på systemet blir plötsligt inaktiverad.
- En systemadministratör som skall göra en förändring av lagringsinställningar klickar fel i ett konfigurationsprogram. En disk eller ett filsystem som skall finnas tillgängligt till systemet blir plötsligt borttaget.

Exempel på potentiella konsekvenser
- Ett SCADA-system blir otillgängligt på grund av handhavandefel under driftsunderhåll

Se också
5.6.2, 5.6.3, 5.6.4, 5.6.5

Referenser
SS-ISO/IEC 27002:2005 kap 10.10.4 ”Administratörs- och operatörsloggar”

5.6.2 Administratörer av nätverk felaktiga handhavande

Beskrivning
En nätverksadministratör är personal som arbetar med drift och förvaltning av nätverk och nätverksutrustning. De har ett viktigt och ansvarsfullt arbete att se till att nätverksutrustningen jämt fungerar och att de fungerar felfritt. När olika typer av fel inträffar måste de utföra felsökning. Om en nätverksadministratör begår ett handhavandefel kan det få långtgående konsekvenser för nätverksutrustningen och nätverkets tillgänglighet och robusthet, utrustningens integritet, eller dataintegritet för den nätverkstrafik som hanteras av den nätverksutrustningen.

Kategori
Tekniskt hot, administrativt hot

Orsak/Aktör
Kompetensbrist, Handhavandefel

Exempel
- En nätverksadministratörer som ombesörjer installation av ny nätverksutrustning utför ett undermåligt jobb, vilket lämnar de nyinstallerade utrustningen utan tillräckligt skydd. Normalt sett skall alla administrationsingångar enbart vara åtkomliga från aministrationsnätet.

Exempel på potentiella konsekvenser
- Nätverket slås ut, vilket påverkar direktansluten utrustning samt utrustning på annan plats i andra nätverk som är beroende av tjänster som är placerade på datorer i detta nät. Om exempelvis delar av kontorsnätet slås ut, med integrationsnav, filservrar, katalogtjänster, med mera, så kan det påverka SCADA/IECS-miljön för de delar som är beroende av dessa funktioner

Se också
5.6.1, 5.6.3, 5.6.4, 5.6.5

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.3 ”Kablageskydd”
SS-ISO/IEC 27002:2005 kap 10.10.4 ”Administratörs- och operatörsloggar”

5.6.3 Administratörer av kringutrustnings felaktiga handhavande

Beskrivning
Systemadministratörer är personal som arbetar med drift och förvaltning av IT-system. De har ett viktigt och ansvarsfullt arbete att se till att IT-systemen jämt fungerar och att de fungerar felfritt. När olika typer av fel inträffar måste de utföra felsökning. Om en systemadministratör begår ett handhavandefel kan det få långtgående konsekvenser för systemet tillgänglighet och robusthet, systemet integritet, eller dataintegritet i den information som hanteras av det systemet..

Kategori
Tekniskt hot, administrativt hot

Orsak/Aktör
Handhavandefel, kompetensbrist

Exempel
- Administratören som handhar installation av skrivare gör fel vid installationen av den nya multifunktionsutrustningen och lämnar det trådlösa nätverket kvar aktiverat. Det medför att obehöriga kan nå skrivarutrustningen och inställningsmenyerna för utrustningen. Detta betyder i förlängningen att utskrifter går att styras om.
- Administratören som arbetar med datalagret och lagringsmedia gör ett fel vid installation av nya diskar vilket leder till att hela datalagret slås ut med påföljande driftstopp för alla anslutna servrar.

Exempel på potentiella konsekvenser
- SCADA-servrar som nyttjar ett disklager kan få driftstörningar i samband med nätverksarbeten, arbeten med kringutrustning i datalagret.

Se också
5.6.1, 5.6.2, 5.6.4, 5.6.5

Referenser
SS-ISO/IEC 27002:2005 kap 10.10.4 ”Administratörs- och operatörsloggar”

5.6.4 Operatörers felaktiga handhavande

Beskrivning
Operatörer är en typ av användare som ofta har vissa systemadministrativa uppgifter eller i uppgift att starta och köra vissa typer av jobb i datorerna, till exempel utskriftsjobb, säkerhetskopiering, underhåll av databaser, med mera.

Kategori
Tekniskt hot, administrativt hot

Orsak/Aktör
Handhavandefel, kompetensbrist

Exempel
- En operatör som felaktigt startar ett jobb gör att hela serverdatorn låses på grund av att jobbet tar för mycket av systemets resurser.
- En operatör som startar ett databasexport jobb gör att hela serverdatorn krashar på grund av att jobbet tar upp all ledig diskyta med den exporterade databasen.

Exempel på potentiella konsekvenser
- Ett SCADA-system blir otillgängligt på grund av att en operatör gjort värddatorn som SCADA-programvaran går på överbelastad.
- Ett SCADA-system blir otillgängligt på grund av att en operatör använt sin klientdator mot Internet på ett sätt som leder till att servrar och andra klienter blir smittade av skadlig kod som operatören klientdator smittats av.

Se också
5.6.1, 5.6.2, 5.6.3, 5.6.5

Referenser
SS-ISO/IEC 27002:2005 kap 10.10.4 ”Administratörs- och operatörsloggar”

5.6.5 Datoranvändares felaktigt handhavande

Beskrivning
En datoranvändare kan uföra vissa handhavanden i IT-systemet på felaktigt sätt, exempelvis radera systemfiler som inte skall raderas, fylla upp all lagringsutrymme på disk så att det inte finns något mer ledigt utrymme.

Kategori
Tekniskt hot, administrativt hot

Orsak/Aktör
Handhavandefel, kompetensbrist

Exempel
- Program startas om och om igen, vilket slutar med att datorn blir otillgänglig på grund av den höga lasten av de många kopiorna av programmet som exekverar samtidigt
- En användare sparar stora mängder filer från internet på den lokala hårddisken som fylls upp och leder till att det inte finns något ledigt diskutrymme kvar
- En användare skriver ut stora mängder filer vilket skapar en extremt lång kö till skrivarna. All utskrift blir otillgänglig under lång tid tills en systemadministratör eller operatör kommer och rensar skrivarkön.
- En användare tar av misstag bort systemfiler vilket gör att operativsystemet på datorn inte fungerar som det skall
- En användare tar av misstag bort applikationsfiler vilket gör att den applikation som skall köras på datorn inte fungerar som den skall

Exempel på potentiella konsekvenser
- En engineering workstation som används för att programmera PLC-utrustning blir förstörd för att användaren råkar ta bort systemfiler av misstag. Eftersom datorn är specialinstallerad så ingår den inte i windowsdomänen på sedvanligt maner, och därför finns det heller inte några säkerhetskopior på datorn.
- En klientdator som används som HMI (human-machine interface) mot ett SCADA-system blir förstörd av en användare som råkar ta bort systemfiler av misstag. Eftersom datorn är specialinstallerad så ingår den inte i windowsdomänen på sedvanligt maner, och därför finns det heller inte några säkerhetskopior på datorn.

Se också
5.6.1, 5.6.2, 5.6.3, 5.6.4

Referenser
SS-ISO/IEC 27002:2005 kap 11.2 ”Styrning av användares åtkomst”
SS-ISO/IEC 27002:2005 kap 11.3 ”Användares ansvar”

5.6.6 Skyddsvärd information ligger kvar i skrivare efter utskrift

Beskrivning
Någon glömmer att hämta eller underlåter att hämta utskriven information från skrivare.

Kategori
Administrativt hot

Orsak/Aktör
Slarv/oaktsamhet personal, bristande utbildning personal

Exempel
- Utskrift av skyddsvärd information på gemensam skrivare.
- Utskrift av skyddsvärd information på egen skrivare men där optiskt röjande är möjligt genom insyn (fönster motsv.).

En väldigt vanlig händelse som ofta leder till att informationens integritetsvärde måste prövas i en menbedömning.

Exempel på potentiella konsekvenser
- Ritningar kan komma obehöriga tillhanda
- Anläggningsinformation kan komma obehöriga tillhanda
- Affärshemligheter kan komma obehöriga tillhanda
- Skyddsvärd information som exponerats utan kontroll måste betraktas som röjd

Se också
4.1.5

Referenser
SS-ISO/IEC 27002:2005 kap 10.8.1 ”Policyer och rutiner för informationsutbyte”

5.6.7 GIS-Information, med koordinater och/eller attributinformation kommer obehörig tillhanda

Beskrivning
Detaljerad grafisk information om anläggning eller motsvarande lämnas ut, stjäls, tappas bort eller förkommer på annat sätt. En förkommen skyddsvärd handling måste betraktas som röjd.

Kategori
Administrativt hot

Orsak/Aktör
Slarv/oaktsamhet personal, Brottsling, extremist eller terrorist

Exempel
- Någon lämnar ut alldeles för detaljerad information till exempelvis en tidning, ett forskningsprojekt eller motsvarande som begär att få ta del av informationen utan att ha ett otillbörligt uppsåt.
- Personal eller motsvarande person som hanterar GIS-information blir på ett eller annat sätt av med densamma. Slarv, oaktsamhet eller rent felaktig hantering, exempelvis som följd av bristande utbildning.
- Någon stjäl eller ger sig på annat sätt tillgång till GIS-information otillbörligt.

Exempel på potentiella konsekvenser
Detaljerad GIS-information med koordinater eller attributinformation kan användas för att kartlägga och planera angrepp på ett företags system, anläggningar och elnät. Det bör här särskilt påpekas att sådana angrepp även kan vara av elektronisk/IT-baserad karaktär.

Se också

Referenser

5.7 Antagonistiska angrepp mot IT-infrastruktur

Med antagonistiska angrepp menas angrepp bakom det finns en eller flera mänskliga angripare som med vett och vilja kan styra angrepp och händelser. Av detta följer också att de kan agera och reagera på eventuella skydd och motåtgärder som sätts in för att stävja angreppen.

Fokus i detta kapitel är angrepp mot *infrastruktur* och *infrastrukturtjänster*

5.7.1 Attacker mot infrastrukturtjänster med kartläggning som mål

Beskrivning
En angripare kan ha som mål eller delmål att kartlägga en IT-miljö och IT-infrastruktur. Detta kan vara i en recognoceringsfas som föregår det riktiga angreppet. Målet med att kartlägga IT-infrastruktur och infrastrukturtjänster kan vara att få ut uppgifter om nätets topologi, vilka IT-resurser som finns i miljön, få ut listor på användare eller få ut hela kontodatabaser, etc.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, medarbetare som överträder sina befogenheter

Exempel
Exempel på attackerbara infrastrukturtjänster är:
- Namnuppslagningstjänster (DNS, DHCP)
- Autentiseringstjänster (ActiveDirectory)
- Routingtjänst
- Nättjänster för loggning och spårdata som slås ut så att spårdata skapas eller sparas korrekt
- Databaser åtkomliga via nätverket
- Molntjänster

Exempel på potentiella konsekvenser
- Uppgifter om processkontrollnätverket och därtill ansluten utrustning kan hämtas ut och en kartbild över IT-miljön byggas upp av obehöriga.

Se också
5.7.2, 5.7.3, 5.7.4, 5.7.5, 5.8.1, 5.8.2, 5.8.3, 5.8.4, 5.8.5, 5.8.6, 5.8.7, 5.8.8, 5.8.9, 5.8.10

Referenser
SS-ISO/IEC 27002:2005 kap 10.6.1 ”Säkerhetsåtgärder för nätverk”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”

5.7.2 Attacker mot infrastrukturtjänster med mål att stjäla information

Beskrivning

En angripare kan ha som mål eller delmål att stjäla information ur en IT-miljö och IT-infrastruktur. Målet med att stjäla information ur IT-infrastruktur och infrastrukturtjänster kan vara att få ut uppgifter om utrustnings konfiguration, nätets topologi, vilka IT-resurser som finns i miljön, få ut listor på användare eller få ut hela kontodatabaser, etc.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, medarbetare som överträder sina befogenheter

Exempel
Exempel på attackerbara infrastrukturtjänster är:
- Namnuppslagningstjänster (DNS, DHCP)
- Autentiseringstjänster (ActiveDirectory)
- Routingtjänst
- Nättjänster för loggning och spårdata som slås ut så att spårdata skapas eller sparas korrekt
- Databaser åtkomliga via nätverket
- Molntjänster

Exempel på potentiella konsekvenser
- Någon stjäl information ur Windows ActiveDirectory och får ut kontodatabaser, uppgifter om datorutrustnings beskaffenhet med mera. Detta kan leda till att någon får uppgifter om vilka konton och datorer som kör de mest kritiska delarna av, eller tillgång till, SCADA-systemet.
- Någon stjäl information ur katalogtjänsten LDAP och får ut kontodatabaser, uppgifter om datorutrustnings beskaffenhet med mera. Detta kan leda till att någon får uppgifter om vilka konton och datorer som kör de mest kritiska delarna av, eller tillgång till, SCADA-systemet.

Se också
5.7.1, 5.7.3, 5.7.4, 5.7.5, 5.8.1, 5.8.2, 5.8.3, 5.8.4, 5.8.5, 5.8.6, 5.8.7, 5.8.8, 5.8.9, 5.8.10

Referenser
SS-ISO/IEC 27002:2005 kap 10.6.1 ”Säkerhetsåtgärder för nätverk”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”

5.7.3 Attacker mot infrastrukturtjänster med mål att slå ut en funktion

Beskrivning
En angripare slår mot IT-infrastrukturutrustning med målet att slå ut eller överlasta nätverks- och infrastrukturfunktionalitet. Med olika överlastningsattacker på nätverksnivå går det att göra enskilda nättjänster, enskilda lokala nätverk eller hela nät otillgängliga.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, medarbetare som överträder sina befogenheter

Exempel
Exempel på attackerbara infrastrukturtjänster är:
- Namnuppslagningstjänster (DNS, DHCP)
- Autentiseringstjänster (ActiveDirectory)
- Tidssynkroniseringstjänster (NTP)
- Routingtjänst
- Nättjänster för loggning och spårdata som slås ut så att spårdata skapas eller sparas korrekt
- Databaser åtkomliga via nätverket
- Molntjänster

Exempel på potentiella konsekvenser
- Nätverksutrustning blir utslagen av en överlastningsattack, vilket innebär att det centrala SCADA-systemet inte kan prata med underliggande enheter. Autonom drift sker på de isolerade PLC-enheterna. Den utrustning som sitter ansluten med RTU:er går dock inte att kontrollera
- En nätbaserad katalogtjänst som används i ICS blir utslagen med driftstörningar (hängningar, tappad informationsinsamling) i processmiljön som följd
- Källan för tidssynkronisering via nätverket slås ut, varpå tidssynkroniseringen inte fungerar, vilket gör att utrustning sakteliga får en tid som inte längre är korrekt

Se också
5.7.1, 5.7.2, 5.7.4, 5.7.5, 5.8.1, 5.8.2, 5.8.3, 5.8.4, 5.8.5, 5.8.6, 5.8.7, 5.8.8, 5.8.9, 5.8.10

Referenser
SS-ISO/IEC 27002:2005 kap 10.6.1 ”Säkerhetsåtgärder för nätverk”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”

5.7.4 Attacker mot infrastrukturkomponenter med mål att kontrollera IT-funktion

Beskrivning
Antagonister kan angripa olika IT-infrastrukturkomponenter med avsikt att kontrollera dem. Om exempelvis nätverksutrustning angrips så kan den nätverkstrafik som passerar utrustningen manipuleras. På samma sätt, om nätverksutrustning angrips, så kan felaktig information om nätets uppbyggnad, såkallad routing, skickas ut till annan nätutrustning, vilket får till effekt att nätverkstrafik kan länkas eller styras om.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, medarbetare som överträder sina befogenheter

Exempel

Exempel på infrastrukturkomponenter som kan bli attackerade, inkluderar
- switchar
- routers
- sensorsystem
- fysiska styrsystemskomponenter (reläer, brytare, pumpar, motorer, nätverksportar)
- komponenter såsom PLC, RTU, IED

Exempel på potentiella konsekvenser
- Om en obehörig kan kontrollera en nätverksutrustning i ett processnät kan den styra om nätverkstrafiken till annan utrustning som de kontrollerar. Där kan trafiken manipuleras på ett sådant sätt att styrkommandon ändras eller inhämtade sensor- och givarvärden ändras. Konsekvenserna av det kan bli att den fysiska processen inte kontrolleras på det sätt som är tänkt eller reglerat att den skall skötas.

Se också
5.7.1, 5.7.2, 5.7.3, 5.7.5, 5.8.1, 5.8.2, 5.8.3, 5.8.4, 5.8.5, 5.8.6, 5.8.7, 5.8.8, 5.8.9, 5.8.10

Referenser
SS-ISO/IEC 27002:2005 kap 10.6.1 ”Säkerhetsåtgärder för nätverk”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”

5.7.5 Attacker mot infrastrukturkomponenter med mål att slå ut eller störa funktion

Beskrivning
En angripare slår mot IT-infrastrukturutrustning med målet att slå ut eller överlasta nätverks- och infrastrukturfunktionalitet. Med olika överlastningsattacker på nätverksnivå går det att göra enskilda nättjänster, enskilda lokala nätverk eller hela nät otillgängliga

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, medarbetare som överträder sina befogenheter

Exempel

Exempel på infrastrukturkomponenter som kan bli attackerade, inkluderar

- switchar
- routers
- sensorsystem
- fysiska styrsystemskomponenter (reläer, brytare, pumpar, motorer, nätverksportar)
- komponenter såsom PLC, RTU, IED

Exempel på potentiella konsekvenser

- Nätverksutrustning blir drabbad av intermittenta störningar till följd av en överlastningsattack. Detta i sin tur innebär att det centrala SCADA-systemet inte kan prata med underliggande enheter. Autonom drift sker på de isolerade PLC-enheterna. Den utrustning som sitter ansluten med RTU:er går dock inte att kontrollera

Se också
5.7.1, 5.7.2, 5.7.3, 5.7.4, 5.8.1, 5.8.2, 5.8.3, 5.8.4, 5.8.5, 5.8.6, 5.8.7, 5.8.8, 5.8.9, 5.8.10

Referenser
SS-ISO/IEC 27002:2005 kap 10.6.1 ”Säkerhetsåtgärder för nätverk”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”

5.8 Antagonistiska angrepp mot IT-system

Med antagonistiska angrepp menas angrepp bakom det finns en eller flera mänskliga angripare som med vett och vilja kan styra angrepp och händelser. Av detta följer också att de kan agera och reagera på eventuella skydd och motåtgärder som sätts in för att stävja angreppen.

Fokus i detta kapitel är angrepp mot *IT-system* och *tjänster som finns i systemen*

5.8.1 Attack mot informationssystem som innehåller personuppgifter

Beskrivning

Hotet innebär olika typer av IT-attacker mot informationssystem som innehåller personuppgifter. Konsekvenserna av IT-attackerna kan i sin tur innebära sådant som:

- Informationsläckage, där personuppgifter stjäls eller exponeras mot obehöriga
- Otillgänglighet av funktioner i systemet, så att tillgång till personuppgifterna blockeras för behöriga användare

Kategori
Tekniskt hot

Orsak/Aktör
Extern angripare, intern personal, riktad skadlig kod, ej riktad skadlig kod

Exempel

- Kunduppgifter i kunddatabaser
- Statistik, förbrukninsunderlag
- Information som knyter abonnentinformation/anläggningsinformation till personinformation

Exempel på potentiella konsekvenser

- Databas med anläggningsuppgifter, och därtill knuten abonnentinformation, stjäls och publiceras på Internet
- Databas med anläggningsuppgifter, och därtill knuten abonnentinformation, stjäls och används i ett senare steg för riktade angrepp mot en enstaka kund

Se också
5.8.2, **Fel! Hittar inte referenskälla.**

Referenser
SS-ISO/IEC 27002:2005 kap 15.1.4 ”Skydd av personuppgifter”

5.8.2 Attack mot informationssystem innehållande personer som har skyddade personuppgifter

Beskrivning

Hotet innebär olika typer av IT-attacker mot informationssystem som innehåller personuppgifter, i detta fall även för personer med skyddade personuppgifter. Konsekvenserna av IT-attackerna kan i sin tur innebära sådant som:

- Informationsläckage, där personuppgifter stjäls eller exponeras mot obehöriga
- Otillgänglighet av funktioner i systemet, så att tillgång till personuppgifterna blockeras för behöriga användare

Kategori
Tekniskt hot

Orsak/Aktör
Extern angripare, intern personal, riktad skadlig kod, ej riktad skadlig kod

Exempel

- Kunduppgifter i kunddatabaser
- Statistik, förbrukninsunderlag
- Information som knyter abonnentinformation/anläggningsinformation till personinformation

Exempel på potentiella konsekvenser

- Personer med skyddade personuppgifter kan få sina uppgifter, inklusive hemadress och kontaktinformation röjd. Detta kan i sin tur leda till att dessa personer måste flytta och ändra adress.
- Databas med anläggningsuppgifter, och därtill knuten abonnentinformation, stjäls och publiceras på Internet
- Databas med anläggningsuppgifter, och därtill knuten abonnentinformation, stjäls och används i ett senare steg för riktade angrepp mot en enstaka kund med skyddade personuppgifter

Se också
5.8.1, **Fel! Hittar inte referenskälla.**

Referenser
SS-ISO/IEC 27002:2005 kap 15.1.4 ”Skydd av personuppgifter”
http://www.polisen.se/Utsatt-for-brott/Hjalp-och-stod-fran-samhallet/Om-du-behover-skydd/Skyddade-personuppgifter/

5.8.3 Attack mot webbtjänst

Beskrivning
Någon eller något (attackprogramvara, skadlig kod) angriper en webbplats via dess exponering mot Internet. Denna attack kan ske mot själva webbserverprogramvaran, applikationsservern som går på webbservern, de java/javascript/PHP eller andra program som är inbäddade i webbsidorna.

En typ av angrepp mot webbplatser är att kunna stjäla information (data, källkod) från webbplatsen. Ibland går det att via angrepp nå bakomliggande komponenter såsom databaser, till vilken man via olika typer av manipulerade webbanrop går att ställa direktfrågor och där hämta valfri mängd och valfri typ av information. Om denna nivå av åtkomst uppnås, så kan även manipulation av data i databasen utföras. Om webbsidorna blir angripna och manipulerade, så kan attacken sprida sig mot andra som besöker webbplatsen, exempelvis via så kallad cross-side scripting (XSS) eller att de blir drabbade av skadlig kod i form av nedladdad skadlig programvara s.k. dropper.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern personal/medarbetare som utför otillåten verksamhet, skadlig kod allmän, riktat angrepp med skadlig kod

Exempel
- Manipulation av information åtkomlig på extern webbserver i syfte att påvisa på att webbservern är dåligt uppsäkrad.
- Manipulation av information åtkomlig på intern webbserver i syfte att påvisa på att webbservern är dåligt uppsäkrad.
- Manipulation av information åtkomlig på extern webbserver i syfte att sprida egen information från denna server, exempelvis politiska eller religiösa budskap
- Manipulation av information åtkomlig på extern webbserver i syfte att sprida information från denna server, falska produktionssiffror eller felaktig avbrottsinformation.
- Stöld av information från externt åtkomlig webbserver.
- Stöld av information från databaskomponent externt åtkomlig webbserver genom injicering av programkod, s.k. SQLi eller SQL injection attack.

Exempel på potentiella konsekvenser
- Webbgränssnittet som finns är en administrationsingång till en PLC-utrustning. Denna utrustning kraschar i samband med att intrångsförsöken görs, då programkoden för webben inte är robust
- Webbgränssnittet är en åtkomstmetod för fältpersonal som skall komma åt anläggningsinformation, därför exponeras detta gränssnitt utanför SCADA/IECS-nätet. Detta gränssnitt innehåller sårbarheter och när dessa missbrukas så kan webbingången användas som en språngbräda för att nå andra delar av SCADA/IECS-systemet.

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 10.6.1 ”Säkerhetsåtgärder för nätverk”
SS-ISO/IEC 27002:2005 kap 10.9.3 ”Offentligt tillgänglig information”

5.8.4 Attack mot IT-infrastrukturutrustning

Beskrivning
Via nätverk går det ofta att nå vanliga administrationsgränssnitt på infrastrukturutrustning. Ofta är åtkomsten via webbgränssnitt, men det finns ofta interaktiv inloggning via telnet, ssh eller liknande nätverksprotokoll.
På samma sätt går det ofta att via nätverket nå *speciella administrationsgränssnitt* på en hel del infrastrukturutrustning, exempelvis nätverksinfrastrukturutrustning, servrar med mera. Via dessa speciella tjänster kan grundläggande hårdvaru- och systemfunktionalitet påverkas.
Angrepp mot infrastrukturutrustning kan antingen ske via någon av dessa administrationsingångar, men också mot de tjänster som utrustningen tillhandahåller, eller mot svagheter i det processande av information som utrustningen gör.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern personal/medarbetare som utför otillåten verksamhet, skadlig kod allmän, riktat angrepp med skadlig kod

Exempel
- Attack mot nätverksswitchar, exempelvis gissning av lösenord i webb- eller telnetinterface, med därpå följande manipulation av nätverksinställningar
- Attack mot nätverksrouters, exempelvis gissning av lösenord i webb- eller telnetinterface, med därpå följande manipulation av nätverksinställningar
- Attack mot diskservrar i lagringsnät med påföljande manipulation av lagringsnätets uppbyggnad och åtkomst till vissa nätdiskar
- Attack mot tjänst som tillhandahåller tid via nätverket, vilket leder till manipulation av klockan, vilket i sin tur leder till att loggar får fel tidsstämplar, autentiseringsfunktioner som beror på tid påverkas, etc.
- Administrationsingångar (IPMI, ILO, etc) på servrar som går att nå via de allmänna nätverken (kontorsnät, Internet, etc) istället enbart uppsatta att nå via administrationsnätverk, används för att manipulera hårdvaru- och systeminställningar på servrar.

Exempel på potentiella konsekvenser
- Nätverksutrustning i SCADA/IECS-nätverket slås ut i samband med attackförsök
- Nätverksutrustning i SCADA/IECS-nätverket manipuleras så att nätverkstrafik styrs om i samband med attackförsök
- Åtkomst till lagringsnät och lagrad data som tillhör SCADA/IECS-miljön möjliggörs för en angripare. Delar av det lagrade informationen är klassad med högsta sekretess då den berör rikets säkerhet

Se också
5.5.3, 5.5.4, 5.5.5, 5.5.6, 5.5.7, 5.5.8, 5.5.9

Referenser
SS-ISO/IEC 27002:2005 kap 10.6.1 ”Säkerhetsåtgärder för nätverk”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”

5.8.5 Attack mot IT-infrastrukturtjänster som sköter säkerhet

Beskrivning
Via nätverk går det ofta att nå vanliga administrationsgränssnitt på infrastrukturutrustning. Ofta är åtkomsten via webbgränssnitt, men det finns ofta interaktiv inloggning via telnet, ssh eller liknande nätverksprotokoll.

På samma sätt går det ofta att via nätverket nå *speciella administrationsgränssnitt* på en hel del infrastrukturutrustning, exempelvis nätverksinfrastrukturutrustning, servrar med mera. Via dessa speciella tjänster kan grundläggande hårdvaru- och systemfunktionalitet påverkas.
Angrepp mot infrastrukturutrustning kan antingen ske via någon av dessa administrationsingångar, men också mot de tjänster som utrustningen tillhandahåller, eller mot svagheter i det processande av information som utrustningen gör.

Olika infrastrukturtjänster som har bäring på säkerhet inkluderas autentiseringsfunktioner, auktorisationsfunktioner (katalogtjänster), loggtjänster som sköter spårbarhet, tidstjänster, etc.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern personal/medarbetare som utför otillåten verksamhet, skadlig kod allmän, riktat angrepp med skadlig kod

Exempel
- Att temporärt blockera eller slå ut en autentiseringstjänst via en överlastningsattack så att inga mer inloggningar kan utföras då konton med tillhörande lösenord inte går att verifiera
- Att temporärt blockera eller mer permanent slå ut en tjänst som tar emot loggar via nätverket för analys, larm, sparande av spårdata

Exempel på potentiella konsekvenser
- Extra användare med administratörsrättigheter skapas i SCADA/IECS-miljön. Dessa missbrukas av angripare till att komma åt SCADA/IECS-systemet.

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 10.6.1 ”Säkerhetsåtgärder för nätverk”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”
ISO/IEC 27019:2013 kap 11.1.1 ”Access control policy”
ISO/IEC 27019:2013 kap 11.3.1 ”Password use”

5.8.6 Attack mot informationssystem som innehåller elnätsinformation

Beskrivning
Hotet består i olika IT-angrepp mot IT-system som innehåller information om elnätets uppbyggnad, exempelvis var anläggningar är placerade, databaser med anläggningsinformation, information om produktionskapacitet, information om kabelsträckningar, etc

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern personal/medarbetare som utför otillåten verksamhet, skadlig kod allmän, riktat angrepp med skadlig kod

Exempel
Angripna system kan vara av typen, eller innehålla information av typen:
- GIS-system
- Nätkartor
- Förbrukningsinformation
- Kopplingar kund, anläggnings-ID / littera, etc

Exempel på potentiella konsekvenser
- Terroristgrupper kan planera var det är mest effektivt att utföra angrepp
- Främmande makt kan planera var det är mest effektivt att utföra angrepp
- Främmande makt kan se vilken reservkapacitet som finns i produktionen
- Konkurrenter kan se vilken reservkapacitet som finns i produktionen
- Konkurrenter kan se underhållscykler och återinvesteringsplaner

Se också
5.8.7,5.8.8, 5.8.9, 5.8.10

Referenser
SS-ISO/IEC 27002:2005 kap 10.6.1 ”Säkerhetsåtgärder för nätverk”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”

5.8.7 Attack mot system som styr och kontrollerar elproduktion

Beskrivning
Hotet består i olika IT-angrepp mot IT-system som kontrollerar elproduktion, såsom exempelvis ett SCADA-system. Om själva styr- och kontrollsystemet slås ut kan produktionen bli påverkad, antingen så att den inte fungerar eller att man måste ersätta den automatiserade kontrollen med bemannad drift av anläggningarna.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern personal/medarbetare som utför otillåten verksamhet, skadlig kod allmän, riktat angrepp med skadlig kod

Exempel
- Angrepp mot SCADA-system som sköter kontrollen av ett vattenkraftverk
- Angrepp mot processkontrollsystemet som sköter kontrollen av ett kraftvärmeverk
- Angrepp mot kontrollsystemet som kontrollen av ett vindkraftverk

Exempel på potentiella konsekvenser
- Terroristgrupper kan helt eller delvis slå ut elproduktion i en eller flera anläggningar
- Främmande makt kan helt eller delvis slå ut elproduktion i en eller flera anläggningar
- Obehöriga hackers kan helt eller delvis slå ut elproduktion i en eller flera anläggningar

Se också
5.8.6, 5.8.8, 5.8.9, 5.8.10

Referenser
SS-ISO/IEC 27002:2005 kap 10.6.1 ”Säkerhetsåtgärder för nätverk”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”

5.8.8 Attack mot system som styr och kontrollerar eldistribution

Beskrivning

Hotet består i olika IT-angrepp mot IT-system som kontrollerar eldistribution och eldistributionsanläggningar. En eller flera antagonister angriper IT-mässigt IT-system som sköter den automatiserade kontrollen av eldistributionen.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern personal/medarbetare som utför otillåten verksamhet, skadlig kod allmän, riktat angrepp med skadlig kod

Exempel

- Angrepp mot DCS-system som sköter kontrollen i eldistributionen i en region
- Angrepp mot SCADA-system som sköter kontrollen i eldistributionen i nationellt för det företaget

Exempel på potentiella konsekvenser

- Terroristgrupper kan helt eller delvis slå en eller flera eldistributionsanläggningar
- Främmande makt kan helt eller delvis slå ut en eller flera eldistributionsanläggningar
- Obehöriga hackers kan helt eller delvis slå ut en eller flera eldistributionsanläggningar

Se också
5.8.6, 5.8.7, 5.8.9, 5.8.10

Referenser
SS-ISO/IEC 27002:2005 kap 10.6.1 ”Säkerhetsåtgärder för nätverk”
ISO/IEC 27019:2013 kap 10.6.3 ”Securing process control data communication”

5.8.9 Attack mot system som styr och kontrollerar elhandel

Beskrivning

Hotet består i olika IT-angrepp mot IT-system används inom elhandel. En eller flera antagonister angriper IT-mässigt de IT-system ingår i marknadsplatsen eller handlarstationer och produktionsplaneringssystem hos de företag som agerar på marknadsplatsen för elhandel.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern personal/medarbetare som utför otillåten verksamhet, skadlig kod allmän, riktat angrepp med skadlig kod

Exempel

- Handlarplats uppvisar felaktig underlag på marknadspriser
- Handlarplats uppvisar felaktig underlag för produktionsnivåer
- Marknadsplatsens backend-system sänder ut felaktig marknadsnoteringar till handlarna

Exempel på potentiella konsekvenser

- Det uppstår en diskreptens mellan den produktionskapacitet som organisationen har åtagit sig att producera enligt det man sålt på elmarknaden och den faktiska produktionsnivån.

Se också
5.8.6, 5.8.7, 5.8.8, 5.8.10

Referenser
SS-ISO/IEC 27002:2005 kap 10.6.1 ”Säkerhetsåtgärder för nätverk”

5.8.10 Attack mot informationssystem som innehåller information av betydelse för rikets säkerhet eller skyddet mot terrorism

Beskrivning
Viss typ av information och vissa typer av informationssystem är klassa som betydelse för rikets säkerhet enligt säkerhetsskyddslagen. Därför är det viktigt att denna typ av system och information skyddas på ett korrekt sätt.
Även anläggningar eller information om anläggningar och elinfrastruktur som inte klassats ha betydelse för rikets säkerhet kan behöva en viss nivå på skydd som en del av skyddet mot terrorism.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern personal/medarbetare som utför otillåten verksamhet, skadlig kod allmän, riktat angrepp med skadlig kod

Exempel
- Databas som innehåller information om totalförsvarskunder
- GIS-system som innehåller information om lednings- och kabelsträckningar till totalförsvarskunder

Exempel på potentiella konsekvenser
- Informationsläckage om anläggningar, förbrukningsinformation, redundans, geografisk information och annan känslig information om anläggningar och förbrukare som är av betydelse för rikets säkerhet

Se också
5.8.6, 5.8.7, 5.8.8, 5.8.9

Referenser
SS-ISO/IEC 27002:2005 kap 10.6.1 ”Säkerhetsåtgärder för nätverk”

5.9 Skyddsfunktioner

I elsystemssammanhang finns det ofta skyddsfunktioner som är implementerade för att skydda elsystemet, komponenter som finns i elsystemet och andra delar som kan skadas eller slås ut i händelse av att kontrollsystemet slås ut.

5.9.1 Avsaknad av skyddsfunktion

Beskrivning
En av de skyddsfunktioner som skall skydda en utrustning, en anläggning, komponenter i anläggningen (transformatorer, generatorer, omvandlare) eller elnät saknas.

Kategori
Tekniskt hot

Orsak/Aktör
Felaktig byggnation, slarv, inkompetens, felaktig avsyn

Exempel

- Ett transformatorskydd saknas
- Ett brytarfelsskydd saknas
- Ett ledningsskydd saknas

Exempel på potentiella konsekvenser

- En transformator skadas på grund av att transformatorskyddet inte är aktivt/fungerar
- En ledning skadas på grund av att ledningsskyddet inte är aktivt/fungerar

Se också
5.9.2, 5.9.3, 5.9.4, 5.9.5

Referenser
ISO/IEC 27019:2013 kap 10.12 ”Safety functions”

5.9.2 Felaktigt utformad skyddsfunktion

Beskrivning
En av de skyddsfunktioner som skall skydda en utrustning, en anläggning, komponenter i anläggningen (transformatorer, generatorer, omvandlare) eller elnät är felaktigt utformad.

Kategori
Tekniskt hot

Orsak/Aktör
Felaktig byggnation, slarv, inkompetens, felaktig avsyn

Exempel
- Ett transformatorskydd är felaktigt utformat
- Ett brytarfelsskydd är felaktigt utformat
- Ett ledningsskydd är felaktigt utformat

Exempel på potentiella konsekvenser
- En transformator skadas på grund av att transformatorskyddet är felaktigt utformat
- En ledning skadas på grund av att ledningsskyddet inte är felaktigt utformat

Se också
5.9.1, 5.9.3, 5.9.4, 5.9.5

Referenser
ISO/IEC 27019:2013 kap 10.12 ”Safety functions”

5.9.3 Antagonistiskt angrepp mot en skyddsfunktion i syfte att slå ut skyddsfunktionen

Beskrivning
En av de skyddsfunktioner som skall skydda en utrustning, en anläggning, komponenter i anläggningen (transformatorer, generatorer, omvandlare) eller elnät är nåbar via nätverk och missbrukas av en antagonistisk användare.

Kategori
Tekniskt hot

Orsak/Aktör
Felaktig byggnation, slarv, inkompetens, felaktig avsyn

Exempel

- Ett transformatorskydd är kopplat mot stationsnätet och är nåbart från detta nät. Detta har som syfte att slå ut skyddsfunktionen eller lösa ut den så att själva transformatorn kopplas bort.
- Ett brytarfelsskydd är kopplat mot stationsnätet och är nåbart från detta nät. Detta har som syfte att slå ut skyddsfunktionen eller lösa ut den så att själva effektbrytaren kopplas bort.
- Ett ledningsskydd är kopplat mot stationsnätet och är nåbart från detta nät. Detta har som syfte att slå ut skyddsfunktionen eller lösa ut den så att själva ledningen kopplas bort.

Se också
5.9.1, 5.9.2, 5.9.4, 5.9.5

Referenser
ISO/IEC 27019:2013 kap 10.12 ”Safety functions”

5.9.4 Antagonistiskt angrepp mot en skyddsfunktion i syfte att manipulera skyddsfunktionen

Beskrivning
En av de skyddsfunktioner som skall skydda en utrustning, en anläggning, komponenter i anläggningen (transformatorer, generatorer, omvandlare) eller elnät är nåbar via nätverk och missbrukas av en antagonistisk användare.

Kategori
Tekniskt hot

Orsak/Aktör
Felaktig byggnation, slarv, inkompetens, felaktig avsyn

Exempel

- Ett transformatorskydd är kopplat mot stationsnätet och är nåbart från detta nät. Detta har som syfte att manipulera skyddsfunktionen för att skada transformatorn
- Ett brytarfelsskydd är kopplat mot stationsnätet och är nåbart från detta nät. Detta har som syfte att manipulera skyddsfunktionen för att skada effektbrytaren.
- Ett ledningsskydd är kopplat mot stationsnätet och är nåbart från detta nät. Detta har som syfte att manipulera skyddsfunktionen för att skada själva ledningen.

Se också
5.9.1, 5.9.2, 5.9.3, 5.9.5

Referenser
ISO/IEC 27019:2013 kap 10.12 ”Safety functions”

5.9.5 Otillräcklig separation mellan kontrollsystem, anläggningsnät och skyddsfunktioner

Beskrivning
En av de skyddsfunktioner som skall skydda en utrustning, en anläggning, komponenter i anläggningen (transformatorer, generatorer, omvandlare) eller elnät är nåbar via nätverk och missbrukas av en antagonistisk användare.

Kategori
Tekniskt hot

Orsak/Aktör
Felaktig byggnation, slarv, inkompetens, felaktig avsyn

Exempel

- Ett transformatorskydd är kopplat mot stationsnätet och är nåbart från detta nät. Effekterna av denna kortslutning kan leda till spridning av skadlig kod, åtkomst för angripare, etc
- Ett brytarfelsskydd är kopplat mot stationsnätet och är nåbart från detta nät. Effekterna av denna kortslutning kan leda till spridning av skadlig kod, åtkomst för angripare, etc
- Ett ledningsskydd är kopplat mot stationsnätet och är nåbart från detta nät. Effekterna av denna kortslutning kan leda till spridning av skadlig kod, åtkomst för angripare, etc

Exempel på potentiella konsekvenser

Se också
5.9.1, 5.9.2, 5.9.3, 5.9.4

Referenser
ISO/IEC 27019:2013 kap 10.12 ”Safety functions”

5.10 Programmatiska hot

Programmatiska hot innefattar

- Skadlig kod i form av datorvirus och datamaskar som sprider sig över nätverk
- Bakdörrar
- Logiska bomber

Programmatiska hot kan avsiktligt, som i fallet med Stuxnet, eller oavsiktligt, som när ”vanliga” virus drabbar process-IT-miljöer, leda till driftstörningar.

5.10.1 Skadlig kod: allmän

Beskrivning
Skadlig kod är program som utvecklats med ett skadligt syfte – ofta att infektera en dator och ta kontroll över den. Den skadliga koden kan spridas på mängder med olika sätt, allt ifrån infekterade datorer som sprider koden vidare via anslutna nätverk, via smittade USB-minnen till e-post med smittade bilagor.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern medarbetare, riktad eller icke-riktad attack

Exempel

- Avsiktligt skadlig kod som är formgivet som en s.k. buggdoor, vilket är en medveten svaghet som lagts dit av programutvecklaren för att kunna missbrukas i ett senare skede
- Avsiktligt skadlig kod som är formgivet som en bakdörr

Exempel på potentiella konsekvenser

- Bakväg in i en PLC eller RTU med vilken någon obehörig kan ta sig obemärkt in och direkt styra anslutna maskiner och utrustning, eller manipulera insamlade värden från sensorer och givare. Detta kan innebära felbeslut av en operatör eller att den fysiska processen inte längre är under kontroll av styr- och kontrollsystemet.

Se också
5.10.2, 5.10.3, 5.10.4, 5.10.5, 5.10.6, 5.10.7, 5.10.8, 5.10.9, 5.10.10, 5.10.11, 5.10.12

Referenser
SS-ISO/IEC 27002:2005 kap 10.4.1 ”Säkerhetsåtgärder mot skadlig kod”
SS-ISO/IEC 27002:2005 kap 10.4.2 ”Säkerhetsåtgärder mot mobil kod”
ISO/IEC 27019:2013 kap 10.4.1 ”Controls against malicious code”

5.10.2 Phishing

Beskrivning
Phishing är en attack som via e-post söker locka mottagaren att besöka en förfalskad webbplats, varvid känsliga uppgifter kan stjälas.
Kallas ibland på svenska för nätfiske.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern medarbetare, riktad eller icke-riktad attack

Exempel

- Allmänt e-postutskick som bland annat når en person i driftcentralen eller kontrollrummet där mottagaren ombeds besöka en webbsida, där denne sedan bes ange sina inloggningsuppgifter
- Allmänt e-postutskick som bland annat når en person i driftcentralen eller kontrollrummet där mottagaren ombeds klicka på medskickad PDF-fil, som är smittad.

Exempel på potentiella konsekvenser

- Obehöriga kommer åt inloggningsinformation till SCADA-systemet
- Obehöriga kommer åt inloggningsinformation till fjärranslutningslösningen som bland annat också används för att nå SCADA-systemet
- Obehöriga kommer åt inloggningsinformation till industriella informationssystem, exempelvis GIS-systemet, anläggningsregister, underhållsregister, logistikregister, med mera

Se också
5.10.1, 5.10.3, 5.10.4, 5.10.5, 5.10.6, 5.10.7, 5.10.8, 5.10.9, 5.10.10, 5.10.11, 5.10.12

Referenser
SS-ISO/IEC 27002:2005 kap 10.4.1 ”Säkerhetsåtgärder mot skadlig kod”
SS-ISO/IEC 27002:2005 kap 10.4.2 ”Säkerhetsåtgärder mot mobil kod”
ISO/IEC 27019:2013 kap 10.4.1 ”Controls against malicious code”

5.10.3 Spearphishing

Beskrivning

Spearphishing är en riktad variant av en attack som via e-post söker locka mottagaren att besöka en förfalskad webbplats, varvid känsliga uppgifter kan stjälas.
Ibland riktas angreppet direkt mot den eller de som är offren. Ibland är angreppen mer sofistikerade och sker mot andra parter, som är mer ovetande om hot och risker, men som används som ett mellanled för att nå det slutliga målet.
Kallas ibland på svenska för riktat nätfiske.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern medarbetare, riktad eller icke-riktad attack

Exempel

- Riktat e-postutskick som bland annat når en person i driftcentralen eller kontrollrummet där mottagaren ombeds besöka en webbsida, där denne sedan bes ange sina inloggningsuppgifter
- E-post riktad till en driftingenjör där mottagaren uppges se informationsbladet i PDF som beskriver en ny SCADA-produkt. PDF-filen är smittad av skadlig kod.
- E-post riktad till driftschefen där mottagaren uppges klicka på det medskickade excelarket. Excelfilen är smittad av skadlig kod.

Exempel på potentiella konsekvenser

- Obehöriga kommer åt inloggningsinformation till SCADA-systemet
- Obehöriga kommer åt inloggningsinformation till fjärranslutningslösningen som bland annat också används för att nå SCADA-systemet
- Obehöriga kommer åt inloggningsinformation till industriella informationssystem, exempelvis GIS-systemet, anläggningsregister, underhållsregister, logistikregister, med mera

Se också
5.10.1, 5.10.2, 5.10.4, 5.10.5, 5.10.6, 5.10.7, 5.10.8, 5.10.9, 5.10.10, 5.10.11, 5.10.12

Referenser
SS-ISO/IEC 27002:2005 kap 10.4.1 ”Säkerhetsåtgärder mot skadlig kod”
SS-ISO/IEC 27002:2005 kap 10.4.2 ”Säkerhetsåtgärder mot mobil kod”
ISO/IEC 27019:2013 kap 10.4.1 ”Controls against malicious code”

5.10.4 Datorvirus

Beskrivning
Skadlig kod är program som utvecklats med ett skadligt syfte – ofta att infektera en dator och ta kontroll över den. Den skadliga koden kan spridas på mängder med olika sätt, allt ifrån infekterade datorer som sprider koden vidare via anslutna nätverk, via smittade USB-minnen till e-post med smittade bilagor.
Datorvirus är både ett samlingsbegrepp som ofta omfattar alla typer av skadlig kod, men också ett mer specifikt begrepp som betyder en viss typ av skadlig kod som sprider sig mellan, och infekterar, programfiler.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern medarbetare, riktad eller icke-riktad attack

Exempel
- En bild i jpeg-format innehåller skadlig kod som sprids mellan datorer
- En ljudfil innehåller skadlig kod. Ljudfilen flyttas mellan olika datorer
- En projektfil i WinCC blir smittad och för med sig skadlig kod mellan datorer
- Ett datavirus kan sprida sig mellan datorer som sitter på olika nät, såsom till fysiskt frånskilda processkontrollnät, exempelvis
    - när servicepersonal ansluter bärbara datorer som används för service- och underhåll
    - när utvecklare har en bärbar engineering workstation som de temporärt ansluter för att uppdatera programvara

Exempel på potentiella konsekvenser
- Den skadliga koden körs på en dator, vilken därefter inte längre får anses tillitbar, då den tappat sin systemintegritet. En dator som används inom processkontroll som inte har sin ursprungsfunktion, utan även okänd tillagd funktionalitet, kan leda till alla typer av konsekvenser, såsom att
    - Fördröjningar i systemet vilket leder till tappad information, exempelvis inrapporterad status från sensorer
    - Hängningar och krashar av applikationer eller själva operativsystemet
    - Den fysiska processen styrs på ett annat sätt än som avses genom processkontrollen,
    - Den fysiska processen inte styrs alls
    - Den fysiska processen körs på ett sätt men rapporterar till SCADA-systemet att det kör på ett annat sätt
    - etc.

Se också
5.10.1, 5.10.2, 5.10.3, 5.10.5, 5.10.6, 5.10.7, 5.10.8, 5.10.9, 5.10.10, 5.10.11, 5.10.12

Referenser
SS-ISO/IEC 27002:2005 kap 10.4.1 ”Säkerhetsåtgärder mot skadlig kod”
SS-ISO/IEC 27002:2005 kap 10.4.2 ”Säkerhetsåtgärder mot mobil kod”
ISO/IEC 27019:2013 kap 10.4.1 ”Controls against malicious code”

5.10.5 Maskar

Beskrivning
Skadlig kod är program som utvecklats med ett skadligt syfte – ofta att infektera en dator och ta kontroll över den. Den skadliga koden kan spridas på mängder med olika sätt, allt ifrån infekterade datorer som sprider koden vidare via anslutna nätverk, via smittade USB-minnen till e-post med smittade bilagor.

En mask är skadlig kod som kan replikera sig över nätverk och sprida sig mellan datorer

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern medarbetare, riktad eller icke-riktad attack

Exempel

- En laptop har blivit infekterad och har därmed masken körandes, denna söker aktivt efter nya nätanslutna datorer för att sprida sig till
- En mask kan sprida sig mellan datorer som sitter på olika nät, såsom till fysiskt frånskilda processkontrollnät, exempelvis
    - när servicepersonal ansluter bärbara datorer som används för service- och underhåll
    - när utvecklare har en bärbar engineering workstation som de temporärt ansluter för att uppdatera programvara

Exempel på potentiella konsekvenser

- Den skadliga koden körs på en dator, vilken därefter inte längre får anses tillitbar, då den tappat sin systemintegritet. En dator som används inom processkontroll som inte har sin ursprungsfunktion, utan även okänd tillagd funktionalitet, kan leda till alla typer av konsekvenser, såsom att
    - Fördröjningar i systemet vilket leder till tappad information, exempelvis inrapporterad status från sensorer
    - Hängningar och krashar av applikationer eller själva operativsystemet
    - Den fysiska processen styrs på ett annat sätt än som avses genom processkontrollen,
    - Den fysiska processen inte styrs alls
    - Den fysiska processen körs på ett sätt men rapporterar till SCADA-systemet att det kör på ett annat sätt
    - etc.

Se också
5.10.1, 5.10.2, 5.10.3, 5.10.4, 5.10.6, 5.10.7, 5.10.8, 5.10.9, 5.10.10, 5.10.11, 5.10.12

Referenser
SS-ISO/IEC 27002:2005 kap 10.4.1 ”Säkerhetsåtgärder mot skadlig kod”
SS-ISO/IEC 27002:2005 kap 10.4.2 ”Säkerhetsåtgärder mot mobil kod”
ISO/IEC 27019:2013 kap 10.4.1 ”Controls against malicious code”

5.10.6 Keylogger

Beskrivning
Skadlig kod är program som utvecklats med ett skadligt syfte – ofta att infektera en dator och ta kontroll över den. Den skadliga koden kan spridas på mängder med olika sätt, allt ifrån infekterade datorer som sprider koden vidare via anslutna nätverk, via smittade USB-minnen till e-post med smittade bilagor.

En keylogger är ett program som är speciellt avsett för att spela in tangentbordsinmatning, exempelvis för att kunna fånga användarnamn och lösenord, men även annan känslig information som matas in.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern medarbetare, riktad eller icke-riktad attack

Exempel

- En keylogger i form av en programvara är installerad på en publik dator på en flygplats, i ett bibliotek, i ett klassrum, i en 7-11-butik
- En keylogger i form av en hårdvara är installerad på en särskild dator inom ett företag, exempelvis på en dator i mötesrum, i driftcentralen, i ett kontrollrum, hos en systemoperatör

Exempel på potentiella konsekvenser

- Obehöriga kommer över inloggningsuppgifter till SCADA-systemet. Dessa uppgifter används för att gå in och manipulera styrningen av processen
- Obehöriga kommer över inloggningsuppgifter till fjärråtkomstlösningen för att nå SCADA-systemet. Dessa uppgifter används för att gå in och manipulera styrningen av processen

Se också
5.10.1, 5.10.2, 5.10.3, 5.10.4, 5.10.5, 5.10.7, 5.10.8, 5.10.9, 5.10.10, 5.10.11, 5.10.12

Referenser
SS-ISO/IEC 27002:2005 kap 10.4.1 ”Säkerhetsåtgärder mot skadlig kod”
SS-ISO/IEC 27002:2005 kap 10.4.2 ”Säkerhetsåtgärder mot mobil kod”
ISO/IEC 27019:2013 kap 9.1.7 ”Securing control centers”
ISO/IEC 27019:2013 kap 10.4.1 ”Controls against malicious code”

5.10.7 Rootkit

Beskrivning
Skadlig kod är program som utvecklats med ett skadligt syfte – ofta att infektera en dator och ta kontroll över den. Den skadliga koden kan spridas på mängder med olika sätt, allt ifrån infekterade datorer som sprider koden vidare via anslutna nätverk, via smittade USB-minnen till e-post med smittade bilagor.

Ett rootkit är en variant av skadlig kod som döljer sig från upptäckt som syftar till att ge angriparen full kontroll över den angripna datorn.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern medarbetare, riktad eller icke-riktad attack

Exempel
- Ett datavirus som sprids via filer innehåller en rootkit-del
- En mask som sprider sig över nätet innehåller en rootkit-del

Exempel på potentiella konsekvenser
- Den skadliga koden körs på en dator, vilken därefter inte längre får anses tillitbar, då den tappat sin systemintegritet. En dator som används inom processkontroll som inte har sin ursprungsfunktion, utan även okänd tillagd funktionalitet, kan leda till alla typer av konsekvenser, såsom att
    - Fördröjningar i systemet vilket leder till tappad information, exempelvis inrapporterad status från sensorer
    - Hängningar och krashar av applikationer eller själva operativsystemet
    - Den fysiska processen styrs på ett annat sätt än som avses genom processkontrollen,
    - Den fysiska processen inte styrs alls
    - Den fysiska processen körs på ett sätt men rapporterar till SCADA-systemet att det kör på ett annat sätt
    - etc.

Se också
5.10.1, 5.10.2, 5.10.3, 5.10.4, 5.10.5, 5.10.6, 5.10.8, 5.10.9, 5.10.10, 5.10.11, 5.10.12

Referenser
SS-ISO/IEC 27002:2005 kap 10.4.1 ”Säkerhetsåtgärder mot skadlig kod”
SS-ISO/IEC 27002:2005 kap 10.4.2 ”Säkerhetsåtgärder mot mobil kod”
ISO/IEC 27019:2013 kap 10.4.1 ”Controls against malicious code”

5.10.8 Trojansk häst

Beskrivning
Skadlig kod är program som utvecklats med ett skadligt syfte – ofta att infektera en dator och ta kontroll över den. Den skadliga koden kan spridas på mängder med olika sätt, allt ifrån infekterade datorer som sprider koden vidare via anslutna nätverk, via smittade USB-minnen till e-post med smittade bilagor.

En trojansk häst är ett program som innehåller annan funktionalitet än den funktionalitet som den utges innehålla. Denna funktionalitet är ofta avsiktligt skadlig kod.
Den trojanska hästen kan i vissa fall vara innehålla gömd funktionalitet som går att komma åt av en lokal användare, eller i vissa andra fall av en fjärranvändare. Den sista varianten kallas ibland för RAT, remote access trojan på engelska.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern medarbetare, riktad eller icke-riktad attack

Exempel
- Ett spelprogram som även innehåller en bakdörr
- Ett nyttoprogram som innehåller en bakdörr som möjliggör fjärråtkomst

Exempel på potentiella konsekvenser
- Den skadliga koden körs på en dator, vilken därefter inte längre får anses tillitbar, då den tappat sin systemintegritet. En dator som används inom processkontroll som inte har sin ursprungsfunktion, utan även okänd tillagd funktionalitet, kan leda till alla typer av konsekvenser, såsom att
    - Fördröjningar i systemet vilket leder till tappad information, exempelvis inrapporterad status från sensorer
    - Hängningar och krashar av applikationer eller själva operativsystemet
    - Den fysiska processen styrs på ett annat sätt än som avses genom processkontrollen,
    - Den fysiska processen inte styrs alls
    - Den fysiska processen körs på ett sätt men rapporterar till SCADA-systemet att det kör på ett annat sätt
    - etc.

Se också
5.10.1, 5.10.2, 5.10.3, 5.10.4, 5.10.5, 5.10.6, 5.10.7, 5.10.9, 5.10.10, 5.10.11, 5.10.12

Referenser
SS-ISO/IEC 27002:2005 kap 10.4.1 ”Säkerhetsåtgärder mot skadlig kod”
SS-ISO/IEC 27002:2005 kap 10.4.2 ”Säkerhetsåtgärder mot mobil kod”
ISO/IEC 27019:2013 kap 10.4.1 ”Controls against malicious code”

5.10.9 Bakdörrar i programvara

Beskrivning
Skadlig kod är program som utvecklats med ett skadligt syfte – ofta att infektera en dator och ta kontroll över den. Den skadliga koden kan spridas på mängder med olika sätt, allt ifrån infekterade datorer som sprider koden vidare via anslutna nätverk, via smittade USB-minnen till e-post med smittade bilagor. Bakdörr är i sig inget som har med spridningsmekanismen att göra.
Ibland kan bakdörrar vara inlagda utan direkt ont uppsåt, mer som en reservväg in för att felsöka och avhjälpa fel, som programutvecklare lägger in mot bättre vetande.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern medarbetare, riktad eller icke-riktad attack

Exempel

- Styrprogramvaran (firmware) till PLC innehåller bakdörr som möjliggör inloggning med användare och lösenord som inte är dokumenterade
- Styrprogramvaran (firmware) till infrastrukturkomponenter såsom nätverksswitchar och routers innehåller bakdörr som möjliggör inloggning med användare och lösenord som inte är dokumenterade

Exempel på potentiella konsekvenser

- Bakväg in i en PLC eller RTU med vilken någon obehörig kan ta sig obemärkt in och direkt styra anslutna maskiner och utrustning, eller manipulera insamlade värden från sensorer och givare. Detta kan innebära felbeslut av en operatör eller att den fysiska processen inte längre är under kontroll av styr- och kontrollsystemet.
- Den skadliga koden körs på en dator, vilken därefter inte längre får anses tillitbar, då den tappat sin systemintegritet. En dator som används inom processkontroll som inte har sin ursprungsfunktion, utan även okänd tillagd funktionalitet, kan leda till alla typer av konsekvenser, såsom att
    - Fördröjningar i systemet vilket leder till tappad information, exempelvis inrapporterad status från sensorer
    - Hängningar och krashar av applikationer eller själva operativsystemet
    - Den fysiska processen styrs på ett annat sätt än som avses genom processkontrollen,
    - Den fysiska processen inte styrs alls
    - Den fysiska processen körs på ett sätt men rapporterar till SCADA-systemet att det kör på ett annat sätt
    - etc.

Se också
5.10.1, 5.10.2, 5.10.3, 5.10.4, 5.10.5, 5.10.6, 5.10.7, 5.10.8, 5.10.10, 5.10.11, 5.10.12

Referenser
SS-ISO/IEC 27002:2005 kap 10.4.1 ”Säkerhetsåtgärder mot skadlig kod”
SS-ISO/IEC 27002:2005 kap 10.4.2 ”Säkerhetsåtgärder mot mobil kod”
ISO/IEC 27019:2013 kap 10.4.1 ”Controls against malicious code”

5.10.10 Botnet

Beskrivning
Ett botnät är en samling datorer, ibland så stor som 10000-tals eller 100000-tals datorer, som blivit hackade och därefter ställts under
Kallas ibland på svenska för zombienät.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern medarbetare, riktad eller icke-riktad attack

Exempel

- En klientdator blir smittad och ingår i ett botnät som används för att skicka spam (skräppost)
- En klientdator blir smittad och ingår i ett botnät som används för att utföra överlastningsattacker (DDoS-attacker) mot tredje part
- En klientdator blir smittad och ingår i ett botnät som används för att sprida skadlig kod mot tredje part

Exempel på potentiella konsekvenser

- En operatörsdator i driftcentralen eller i ett kontrollrum är medlem i ett botnet och används för att sprida spam, utföra DDoS-attacker och hacka andra system på Internet. Någon operatör har använt datorn för att nå Internet och där blivit drabbad av skadlig kod som gjort att datorn därefter anslutits till botnätet. Att operatörsdatorn är smittad kan få som följd att såväl datorns systemintegritet är åsidosatt, att nätverket fylls med oönskad trafik, att andra datorer på processnätverket blir smittade.
- Om en av organisationens datorer används på ett botnät kan misstankar och krav ställas mot organisationen, då man medverkat i brottslig verksamhet

Se också
5.10.1, 5.10.2, 5.10.3, 5.10.4, 5.10.5, 5.10.6, 5.10.7, 5.10.8, 5.10.9, 5.10.11, 5.10.12

Referenser
SS-ISO/IEC 27002:2005 kap 10.4.1 ”Säkerhetsåtgärder mot skadlig kod”
SS-ISO/IEC 27002:2005 kap 10.4.2 ”Säkerhetsåtgärder mot mobil kod”
ISO/IEC 27019:2013 kap 10.4.1 ”Controls against malicious code”

5.10.11 Logiska bomber

Beskrivning
Skadlig kod är program som utvecklats med ett medvetet skadligt syfte. Logiska bomber är medvetet skadlig kod som innehar en dold funktion i ett program eller en programfunktion som under vissa villkor utlöser en oönskad aktivitet.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, intern medarbetare, riktad eller icke-riktad attack

Exempel

- Tidstyrda funktioner som vid en given tidpunkt aktiverar skadlig programkod som utför oönskade operationer.
- Funktioner som vid en viss användarinteraktion aktiverar skadlig programkod som utför oönskade operationer.
- Funktioner som vid frånvaron av en viss användarinteraktion eller användaraktivitet, exempelvis att en viss medarbetare slutat, aktiverar skadlig programkod som utför oönskade operationer.

Exempel på potentiella konsekvenser

- Den skadliga koden körs på en dator, vilken därefter inte längre får anses tillitbar, då den tappat sin systemintegritet. En dator som används inom processkontroll som inte har sin ursprungsfunktion, utan även okänd tillagd funktionalitet, kan leda till alla typer av konsekvenser, såsom att
    - Fördröjningar i systemet vilket leder till tappad information, exempelvis inrapporterad status från sensorer
    - Hängningar och krashar av applikationer eller själva operativsystemet
    - Den fysiska processen styrs på ett annat sätt än som avses genom processkontrollen,
    - Den fysiska processen inte styrs alls
    - Den fysiska processen körs på ett sätt men rapporterar till SCADA-systemet att det kör på ett annat sätt
    - etc.

Se också
5.10.1, 5.10.2, 5.10.3, 5.10.4, 5.10.5, 5.10.6, 5.10.7, 5.10.8, 5.10.9, 5.10.10, 5.10.12

Referenser
SS-ISO/IEC 27002:2005 kap 10.4.1 ”Säkerhetsåtgärder mot skadlig kod”
SS-ISO/IEC 27002:2005 kap 10.4.2 ”Säkerhetsåtgärder mot mobil kod”
ISO/IEC 27019:2013 kap 10.4.1 ”Controls against malicious code”

5.10.12 Advanced Persistent Threat, APT

Beskrivning
APT är ett samlingsnamn som ofta beskriver statsaktörer, eller statsbackade grupper, som med stora resurser och *avancerade* och komplexa attacker försöker utföra olika typer av aktiviteter såsom industrispionage, sabotage eller liknande. Ofta används olika former av skadlig kod som ett sätt att skaffa sig ett brohuvud hos den organisation eller person som angrips. Ordet *persistent* kommer av att det kan vara en långvarig operation, under både rekognoserings- och uppbyggnadsfas samt utförandefas.

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist, statsaktör, riktad attack

Exempel

- En statsbackad gruppering ger sig på ägare av kritisk samhällsinfrastruktur med uppsåtet att infiltrera, inventera IT-system och stjäla information i syfte att förbereda eventuella framtida angrepp
- En statsbackad grupp hackar sig in i SCADA-mijön i ett elföretag och placerar ny kod med bakdörrar, logiska bomber och annan dold funktionalitet i på diverse utrustning som är central för drift och skötsel av eldistribution
- En statsbackad grupp hackar sig in i ICS-mijön och placerar ny kod med bakdörrar, logiska bomber och annan dold funktionalitet i på diverse utrustning som är central för elproduktion

Exempel på potentiella konsekvenser

- Obehöriga kan komma in i ICS-system och påverka den fysiska processen och där genom väl uttänkt missbruk av styrningen skada och sabotera utrustning och maskiner såsom transformatorer, generatorer, pumpar, ventiler eller liknande

Se också
5.10.2, 5.10.3, 5.10.4, 5.10.5, 5.10.6, 5.10.7, 5.10.8, 5.10.9, 5.10.10, 5.10.11

Referenser
SS-ISO/IEC 27002:2005 kap 10.4.1 ”Säkerhetsåtgärder mot skadlig kod”
SS-ISO/IEC 27002:2005 kap 10.4.2 ”Säkerhetsåtgärder mot mobil kod”
ISO/IEC 27019:2013 kap 10.4.1 ”Controls against malicious code”

5.11 Fysiska skador på IT miljö

5.11.1 Avsaknad av brandskydd

Beskrivning

Hotet består i att anläggningar i vilken det bedrivs verksamhet eller där det finns IT-resurser som behövs för att verksamheten skall fungera saknar adekvat brandskydd.

Kategori
Tekniskt hot

Orsak/Aktör
Designfel, kompetensbrist

Exempel

- Avsaknad av släcksystem i datorhallar
- Avsaknad av handsläckare utanför datorhallar
- Avsaknad av handsläckare utanför kommunikationsutrymmen
- Avsaknad av sensorer och rökdetektorer

Exempel på potentiella konsekvenser

- Datorhall där SCADA- eller DCS-system finns installerar blir helt utbränd
- Datorhall där SCADA- eller DCS-system finns installerar blir rökskadad och den utrustning som finns däri blir svårt skadad och går ej att använda
- Datorhall där SCADA- eller DCS-system finns installerar blir vattenskadad till följd av släckningsarbetet. Den utrustning som finns däri blir svårt skadad och går ej att använda

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.1 ”Skalskydd”
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”
ISO/IEC 27019:2013 kap 9.1.1 ”Physical security perimeter”
ISO/IEC 27019:2013 kap 9.1.8 ”Securing equipment rooms”
ISO/IEC 27019:2013 kap 9.1.9 ”Securing peripheral sites”

5.11.2 Felaktigt utformat brandskydd

Beskrivning
Hotet består i att anläggningar i vilken det bedrivs verksamhet eller där det finns IT-resurser som behövs för att verksamheten skall fungera har ett felaktigt (underdimensionerat, ej lämpligt, ej på kritiska platser) brandskydd

Kategori
Tekniskt hot

Orsak/Aktör
Designfel

Exempel
- Felaktiga släcksystem i datorhallar
- Felaktiga handsläckare utanför datorhallar
- Felaktiga handsläckare utanför kommunikationsutrymmen
- Felaktiga av sensorer och rökdetektorer

Exempel på potentiella konsekvenser
- Datorhall där SCADA- eller DCS-system finns installerar blir helt utbränd
- Datorhall där SCADA- eller DCS-system finns installerar blir rökskadad och den utrustning som finns däri blir svårt skadad och går ej att använda
- Datorhall där SCADA- eller DCS-system finns installerar blir vattenskadad till följd av släckningsarbetet. Den utrustning som finns däri blir svårt skadad och går ej att använda

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.1 ”Skalskydd”
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”
ISO/IEC 27019:2013 kap 9.1.1 ”Physical security perimeter”
ISO/IEC 27019:2013 kap 9.1.8 ”Securing equipment rooms”
ISO/IEC 27019:2013 kap 9.1.9 ”Securing peripheral sites”

5.11.3 Avsaknad av inbrottsskydd

Beskrivning
Hotet består i att anläggningar i vilken det bedrivs verksamhet eller där det finns IT-resurser som behövs för att verksamheten skall fungera har avsaknad av ett inbrottsskydd

Kategori
Tekniskt hot

Orsak/Aktör
Designfel, felaktiga beslut

Exempel
- Avsaknad av galler i fönster
- Avsaknad av förstärkta väggar
- Avsaknad av förstärkta dörrar in i anläggningen
- Avsaknad av förstärkta dörrar i anläggningen

Exempel på potentiella konsekvenser
- Stöld av utrustning som leder till driftavbrott i driftcentral eller ett kontrollrum
- Stöld av utrustning som leder till driftavbrott kontroll och övervakning av eldistribution
- Stöld av utrustning som leder till driftavbrott kontroll och övervakning av elproduktion
- Sabotage av utrustning som leder till driftavbrott kontroll och övervakning av eldistribution
- Sabotage av utrustning som leder till driftavbrott kontroll och övervakning av elproduktion

Se också
5.11.4, 5.11.5, 5.11.6

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.1 ”Skalskydd”
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”
ISO/IEC 27019:2013 kap 9.1.7 ”Securing control centers”
ISO/IEC 27019:2013 kap 9.1.8 ”Securing equipment rooms”
ISO/IEC 27019:2013 kap 9.1.9 ”Securing peripheral sites”

5.11.4 Felaktigt utformat inbrottsskydd

Beskrivning

Hotet består i att anläggningar i vilken det bedrivs verksamhet eller där det finns IT-resurser som behövs för att verksamheten skall fungera har ett felaktigt (underdimensionerat, ej lämpligt, ej på kritiska platser) inbrottsskydd.

Kategori
Tekniskt hot

Orsak/Aktör
Designfel, kompetensbrist, felaktiga beslut

Exempel
- Felaktiga galler i fönster
- Felaktig förstärkning av väggar. Alla väggpartier är inte förstärkta
- Felaktigt placering och förstärkning av dörrar in i anläggningen

Exempel på potentiella konsekvenser
- Stöld av utrustning som leder till driftavbrott i driftcentral eller kontrollrum
- Stöld av utrustning som leder till driftavbrott kontroll och övervakning av eldistribution
- Stöld av utrustning som leder till driftavbrott kontroll och övervakning av elproduktion
- Stöld av utrustning, maskiner och reservdelar som finns på uppställningsplatser, i lager, i arkiv, med mera
- Sabotage av utrustning som leder till driftavbrott kontroll och övervakning av eldistribution
- Sabotage av utrustning som leder till driftavbrott kontroll och övervakning av elproduktion

Se också
5.11.3, 5.11.5, 5.11.6

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.1 ”Skalskydd”
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”
ISO/IEC 27019:2013 kap 9.1.1 ”Physical security perimeter”
ISO/IEC 27019:2013 kap 9.1.8 ”Securing equipment rooms”
ISO/IEC 27019:2013 kap 9.1.9 ”Securing peripheral sites”

5.11.5 Avsaknad av inbrottslarm

Beskrivning

Hotet består i att anläggningar i vilken det bedrivs verksamhet eller där det finns IT-resurser som behövs för att verksamheten skall fungera saknar installerat inbrottslarm.

Kategori

Orsak/Aktör
Designfel, felaktiga beslut

Exempel
- Delar av anläggningen omfattas inte av inbrottslarm
- Hela anläggningen omfattas inte av inbrottslarm

Exempel på potentiella konsekvenser
- Stöld av utrustning som leder till driftavbrott i driftcentral eller kontrollrum
- Stöld av utrustning som leder till driftavbrott kontroll och övervakning av eldistribution
- Stöld av utrustning som leder till driftavbrott kontroll och övervakning av elproduktion
- Stöld av utrustning, maskiner och reservdelar som finns på uppställningsplatser, i lager, i arkiv, med mera
- Sabotage av utrustning som leder till driftavbrott kontroll och övervakning av eldistribution
- Sabotage av utrustning som leder till driftavbrott kontroll och övervakning av elproduktion

Se också
5.11.3, 5.11.4, 5.11.6

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.1 ”Skalskydd”
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”
ISO/IEC 27019:2013 kap 9.1.1 ”Physical security perimeter”
ISO/IEC 27019:2013 kap 9.1.7 ”Securing control centers”
ISO/IEC 27019:2013 kap 9.1.8 ”Securing equipment rooms”
ISO/IEC 27019:2013 kap 9.1.9 ”Securing peripheral sites”

5.11.6 Felaktigt utformat inbrottslarm

Beskrivning
Hotet består i att anläggningar i vilken det bedrivs verksamhet eller där det finns IT-resurser som behövs för att verksamheten skall fungera har ett felaktigt (underdimensionerat, ej lämpligt, ej på kritiska platser) inbrottslarm.

Kategori

Orsak/Aktör
Designfel, felaktiga beslut

Exempel
- Delar av anläggningen omfattas inte av inbrottslarm
- I samband med installation av nya övervakningskameror, passagesystem, porttelefoner och liknande så har datornätverket dragits ut utanför de områden som omfattas av inbrottslarm. De kommunikationsskåp som sätts upp är inte larmade
- Installationen av inbrottslarm i anläggningen är inte ändamålsenlig

Exempel på potentiella konsekvenser
- Stöld av utrustning som leder till driftavbrott i driftcentral eller kontrollrum
- Stöld av utrustning som leder till driftavbrott kontroll och övervakning av eldistribution
- Stöld av utrustning som leder till driftavbrott kontroll och övervakning av elproduktion
- Stöld av utrustning, maskiner och reservdelar som finns på uppställningsplatser, i lager, i arkiv, med mera
- Sabotage av utrustning som leder till driftavbrott kontroll och övervakning av eldistribution
- Sabotage av utrustning som leder till driftavbrott kontroll och övervakning av elproduktion

Se också
5.11.3, 5.11.4, 5.11.5

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.1 ”Skalskydd”
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”
ISO/IEC 27019:2013 kap 9.1.1 ”Physical security perimeter”
ISO/IEC 27019:2013 kap 9.1.8 ”Securing equipment rooms”
ISO/IEC 27019:2013 kap 9.1.9 ”Securing peripheral sites”

5.11.7 Felaktigt placerad dator- eller serverhall

Beskrivning
Placering av datorhallar eller serverhallar kan få svåra konsekvenser. Dels kan datorhallen bli utsatt för olika typer av naturkrafter och naturkatastrofer, dels kan datorhallen bli utsatt för olika händelser i dess omvärld.

Kategori
Administrativt hot, tekniskt hot

Orsak/Aktör
Fel i planering, felbeslut, inkompetens, avsaknad av tillräckliga underlag

Exempel
- Dator- eller serverhall placerad i bottenvåning i en anläggning eller hus. Risk för översvämning är stor då dagvatten kan komma in via golvbrunnar eller häftiga regn man forcera att regnvatten kan tränga ner via trappor och ingångar.
- Dator- eller serverhall placerad i närheten av verksamhet där det finns stor risk för brand, exempel kemiskteknisk processhantering.
- Viktiga försörjningssystem för datorhallen kan bli svåra att sköta. Exempelvis om datorhallen är placerad högt upp i en byggnad och reservkraft i form av dieselaggregat och tillhörande dieseltankar är placerade på taket.

Exempel på potentiella konsekvenser
- Datorhallen och dess IT-utrustning kan bli otillgänglig och förstörd på grund av översvämning. Detta kan i sin tur leda till att SCADA- eller DCS-system slås ut och fjärrstyrning och automatiserad kontroll av processen inte längre fungerar.
- Datorhallen och dess IT-utrustning kan bli otillgänglig och förstörd på grund av brand. Detta kan i sin tur leda till att SCADA- eller DCS-system slås ut och fjärrstyrning och automatiserad kontroll av processen inte längre fungerar.

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.1 ”Skalskydd”
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”
ISO/IEC 27019:2013 kap 9.1.1 ”Physical security perimeter”
ISO/IEC 27019:2013 kap 9.1.8 ”Securing equipment rooms”
ISO/IEC 27019:2013 kap 9.1.9 ”Securing peripheral sites”
ISO/IEC 27019:2013 kap 9.2.1 ”Equipment siting and protection”

5.12 SPOF (single point of failure) och cykliska beroenden

Med SPOF *(eng. single point of failure*) så menas beroenden på enstaka komponenter som, vilka om dom går sönder eller slutar fungera korrekt, får en fullständig systempåverkan.

Med cykliska beroenden menas här då flera utrustningar eller system är beroenden på varandra, exempelvis i samband med återuppstart efter ett strömavbrott

5.12.1 Icke identifierade SPOF

Beskrivning
Med SPOF *(eng. single point of failure*) så menas beroenden på enstaka komponenter som, vilka om dom går sönder eller slutar fungera korrekt, får en fullständig systempåverkan.

Kategori
Tekniskt hot

Orsak/Aktör
otillräcklig inventering eller analys, kompetensbrist

Exempel
- Enstaka hårddisk som används som systemdisk i en större datorlösning där det finns redundans på andra nivåer, exempelvis speglade datadiskar. Om denna systemdisk går sönder så slås datorlösningen ändå ut, även om datadiskarna är redundanta.
- En nätkomponent som saknar redundans i ett processnät, varpå all nätverkstrafik i den delen av nätverket slås ut om den går sönder eller måste tillfälligt göras otillgänglig på grund av underhållsarbete

Exempel på potentiella konsekvenser
- DCS-system blir drabbat av tillgänglighetsförlust på grund av en diskkrash. Automationen av processen stängs temporärt ner. Konsekvensen blir manuell bemanning i anläggningen under en period.
- SCADA-system blir drabbat av tillgänglighetsförlust på grund av ett nätverksfel. Automationen av processen stängs temporärt ner. Konsekvensen blir manuell bemanning i anläggningen under en period.

Se också
5.12.2

Referenser
SS-ISO/IEC 27002:2005 kap 10.3.1 ”Kapacitetsplanering”

5.12.2 Icke åtgärdad eller hanterad SPOF

Beskrivning
Med SPOF *(eng. single point of failure*) så menas beroenden på enstaka komponenter som, vilka om dom går sönder eller slutar fungera korrekt, får en fullständig systempåverkan.

Kategori
Tekniskt hot

Orsak/Aktör
Otillräcklig inventering, otillräcklig planering, kompetensbrist

Exempel

- Enstaka hårddisk som används som systemdisk i en större datorlösning där det finns redundans på andra nivåer, exempelvis speglade datadiskar. Om denna systemdisk går sönder så slås datorlösningen ändå ut, även om datadiskarna är redundanta.
- En nätkomponent som saknar redundans i ett processnät, varpå all nätverkstrafik i den delen av nätverket slås ut om den går sönder eller måste tillfälligt göras otillgänglig på grund av underhållsarbete

Exempel på potentiella konsekvenser

- DCS-system blir drabbat av tillgänglighetsförlust på grund av en diskkrash. Automationen av processen stängs temporärt ner. Konsekvensen blir manuell bemanning i anläggningen under en period.
- SCADA-system blir drabbat av tillgänglighetsförlust på grund av ett nätverksfel. Automationen av processen stängs temporärt ner. Konsekvensen blir manuell bemanning i anläggningen under en period.

Se också
5.12.1

Referenser
SS-ISO/IEC 27002:2005 kap 10.3.1 ”Kapacitetsplanering”
SS-ISO/IEC 27002:2005 kap 14.1.3 ”Kontinuerlig verksamhet och riskbedömning”

5.12.3 Icke identifierade cykliska beroenden

Beskrivning
Med cykliska beroende *(eng. cyclic dependencies*) så menas beroenden mellan enstaka komponenter som, vilka om dom går sönder eller slutar fungera korrekt, får en fullständig systempåverkan.

Kategori
Tekniskt hot

Orsak/Aktör
Otillräcklig inventering, otillräcklig planering, kompetensbrist

Exempel
- Ett datorsystem startar inte upp på grund av att det är beroende av ett annat datorsystem som skall starta först, men som ännu inte startat upp
- Interna system och utrustning är beroende av extern strömförsörjning, även när de används under reservdrift

Se också
5.12.4

Referenser
ISO/IEC 27019:2013 kap 9.2.2 ”Supporting utilities”

5.12.4 Icke åtgärdade cykliska beroenden

Beskrivning
Med cykliska beroende *(eng. cyclic dependencies*) så menas beroenden mellan enstaka komponenter som, vilka om dom går sönder eller slutar fungera korrekt, får en fullständig systempåverkan.

Kategori
Tekniskt hot

Orsak/Aktör
Otillräcklig inventering, otillräcklig planering, kompetensbrist

Exempel
- Ett datorsystem startar inte upp på grund av att det är beroende av ett annat datorsystem som skall starta först, men som ännu inte startat upp
- Interna system och utrustning är beroende av extern strömförsörjning, även när de används under reservdrift

Se också
5.12.3

Referenser
ISO/IEC 27019:2013 kap 9.2.2 ”Supporting utilities”

5.13 Informationsläckage och informationsextrahering

Informationsläckage, också kallat röjande signaler (*eng. compromising emanation*). Ett exempel på informationsläckage är så kallad Van Eck-strålnin . På engelska pratar man ofta sammanfattningsvis om *TEMPEST*. TEMPEST är ett samlingsbegrepp för standarder, analyser, insamlingar, mätningar med mera som rör fenomenet röjande signaler. Ordet TEMPEST myntades i slutet av 60-talet och som ett kodord för den klassificerade verksamhet som National Security Agency (NSA) i USA bedrev dels för att säkra egna system mot otillåten avlyssning, dels samla in och tolka signaler från andra länders system och kommunikationssystem.

5.13.1 Röjande signaler via radiovågor

Beskrivning
Detta hot beskriver röjande signaler (RÖS) via elektromekaniska signaler som alstras i samband med att information behandlas i en eldriven utrustning.

Kategori
Tekniskt hot

Orsak/Aktör
Otillräckligt skydd, kompetensbrist

Exempel
- Video-RÖS från kabeln mellan dator och skärm
- Tecken-RÖS från tangentbord till dator
- Radio-RÖS där utrustning som har någon sändarkapacitet läcker information även när sändaren inte skall vara aktiv
- Radio-RÖS där utrustning som har någon sändarkapacitet läcker information via överlagrad information som sänds ut i samband med ordinarie sändning

Exempel på potentiella konsekvenser
- Obehöriga kan stjäla inloggningsuppgifter till SCADA- eller ICS-system.
- Obehöriga kan stjäla nätkartor och översiktsbilder från operatörsstation i SCADA- eller ICS-system.
- Obehöriga kan stjäla nätkartor och översiktsbilder från operatörsstation ifrån GIS-system
- Obehöriga kan stjäla information om anläggningar, intern driftsinformation

Se också
5.13.2, 5.13.3

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.1 ”Placering och skydd av utrustning”

5.13.2 Röjande signaler via akustik

Beskrivning
Detta hot beskriver röjande signaler (RÖS) via akustiska signaler som alstras i samband med att information behandlas i en eldriven utrustning.

Kategori
Tekniskt hot

Orsak/Aktör
Otillräckligt skydd, kompetensbrist

Exempel
- Ljud från skrivare, exempelvis matrisskrivare, så kallad matris-rös
- Ljud från skrift på tangentbord

Exempel på potentiella konsekvenser
- Obehöriga kan stjäla inloggningsuppgifter till SCADA- eller ICS-system.
- Obehöriga kan stjäla information om anläggningar, intern driftsinformation

Se också
5.13.1, 5.13.3

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.1 ”Placering och skydd av utrustning”

5.13.3 Röjande signaler via optik

Beskrivning
Detta hot beskriver röjande signaler (RÖS) via akustiska signaler eller samtal som sedan kan uppfångas via optiska teknologier

Kategori
Tekniskt hot

Orsak/Aktör
Otillräckligt skydd, kompetensbrist

Exempel
- Avlyssning av konversioner som sker i ett mötesrum via lasermätning av rörelser i fönsterglas eller en lasermikrofon mot fönster
- Avlyssning av konversioner som sker i ett mötesrum via HSR-kameror
- Avlyssning av konversioner som sker i en driftcentral eller i kontrollrum

Exempel på potentiella konsekvenser
- Obehöriga kan stjäla inloggningsuppgifter till SCADA- eller ICS-system.
- Obehöriga kan stjäla nätkartor och översiktsbilder från operatörsstation i SCADA- eller ICS-system.
- Obehöriga kan stjäla nätkartor och översiktsbilder från operatörsstation ifrån GIS-system
- Obehöriga kan stjäla information om anläggningar, intern driftsinformation

Se också
5.13.1, 5.13.2

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.1 ”Placering och skydd av utrustning”
ISO/IEC 27019:2013 kap 9.1.7 ”Securing control centers”

5.13.4 Flygfotografier av anläggningar eller motsvarande kommer obehörig tillhanda.

Beskrivning
Privatflygare fotograferar område utan att ta hänsyn till markägares säkerhetsintressen eller Lag om skydd av landskapsinformation (1993:1742).
Ungdomar eller annan entusiast filmar eller fotograferar skyddsvärt område från luften och publicerar materialet.

Angripare filmar eller fotograferar skyddsvärt område från luften och använder materialet för att förbereda angrepp.

Kategori
Tekniskt/Fysiskt hot

Orsak/Aktör
Person som inte känner till gällande lagstiftning.
Terrorism, organiserad brottslighet, enskilda brottslingar och rättshaverister.

Exempel
- Privatflygplan av mindre eller medelstor typ filmar eller fotograferar skyddsvärda resurser under överflygning.
- Någon använder sig av modellflygfarkost, modellflygplan, modellhelikopter eller quadrokopter för att filma, kartlägga, fotografera ett område och ende3ra publicera materialet eller utnyttja detta för att planera angrepp.

Exempel på potentiella konsekvenser
Det finns två huvudsakliga konsekvenser som i sin tur kan leda till oönskade händelser.
1. 1 Materialet (foto, film etc.) publiceras i större eller mindre forum och sprids utan att resursägaren har vetskap eller kontroll över detta.
2. 2 Materialet används direkt i planering av angrepp eller liknande på skyddsvärd resurs.

Se också

Referenser
AR2 Drone: http://ardrone2.parrot.com/
Exempel på annan utrustning: http://www.quadrocopter.com/

5.14 Andra problem med IT system

I detta kapitel beskrivs hot mot IT och IT-system som inte tidigare i texten placerats in i en specifik kategori.

5.14.1 Elektromekanisk puls – EMP

Beskrivning
Detta hot beskriver elektromagnetisk puls, EMP. EMP är det fenomen som uppstår vid kärnvapensprängningar. Den elektromagnetiska pulsen som uppstår i samband med explosionen slår ut elektronisk utrustning genom att inducera hög spänning och ström i ledande material.

Kategori
Tekniskt hot

Orsak/Aktör
Otillräckligt skydd, kompetensbrist

Exempel

- Egen kommunikationsutrustning slås ut av elektromagnetisk puls
- Kommunikationsutrustning i allmänna kommunikationsnät slås ut av elektromagnetisk puls
- Egen datorutrustning slås ut av elektromagnetisk puls
- datorutrustning som tillhandahåller kritiska allmänna infrastrukturtjänster, såsom domännamnshantering, tidssynkronisering, nätverksmässiga vägval, med mera slås ut av elektromagnetisk puls

Exempel på potentiella konsekvenser

- Automation av processen slås ut
- Fjärrstyrning av processen slås ut
- Själva processen kan slås ut då utrustning och maskiner som används i processen påverkas

Se också
5.14.2, 6.6.9, 6.6.10

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.1 ”Placering och skydd av utrustning”
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

5.14.2 High powered microwave - HPM

Beskrivning
HPM, High powered microwave. Angrepp med elektromagnetisk verkan i syfte att slå ut avancerad mikroelektronik, såsom datorer, nätverkskomponenter och annan typ av elektronik som bygger på integrerade kretsar. Olika typer av mobila vapen för att generera denna elektromagnetiska verkan har utvecklats.

Kallas ibland på svenska även för Högeffekt Pulsad Mikrovågsstrålningsvapen. .

Kategori
Tekniskt hot

Orsak/Aktör
Antagonist

Exempel

- Egen kommunikationsutrustning slås ut av mikrovågspuls
- Kommunikationsutrustning i allmänna kommunikationsnät slås ut av mikrovågspuls
- Egen datorutrustning slås ut av mikrovågspuls
- datorutrustning som tillhandahåller kritiska allmänna infrastrukturtjänster, såsom domännamnshantering, tidssynkronisering, nätverksmässiga vägval, med mera slås ut av mikrovågspuls

Exempel på potentiella konsekvenser

- Automation av processen slås ut
- Fjärrstyrning av processen slås ut
- Själva processen kan slås ut då utrustning och maskiner som används i processen påverkas

Se också
5.14.1, 6.6.9, 6.6.10

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.1 ”Placering och skydd av utrustning”
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

5.14.3 För snabb adaption av ny teknologi

Beskrivning
För snabbt anammande av nya tekniska lösningar, som medför nya – ibland okända eller dolda – risker. Ibland beror dessa hot och risker på att lösningen inte hunnit mogna, att de som byggt den nya tekniken har gjort implementationsfel och i andra fall på att den nya tekniken medför nya lösningar som har nya risker. Dessa risker kan uppstå i samband med att dessa tekniska lösningar tas i drift, eller att de varit drifttagna en stund.

Kategori
Tekniskt hot

Orsak/Aktör
Kompetensbrist, brist på erfarenhet, avsaknad av risktänk

Exempel
- Införande av molntjänster
- Införande av utrustning för ökat mobilt arbete och fjärrarbete
- Införande av fjärråtkomstlösning till system som är olämplig att ha fjärråtkomst till
- Införande av trådlösa nätverk i anläggningar där man borde låta bli att exponera nätverket utanför skal- eller områdesskydd
- Införande av virtualisering för vissa miljöer där virtualiseringslösningen kan påverka applikationens responstider, eller kompatibilitetsproblem eller liknande kan uppstå, utan att egentligen ha undersökt riskerna noggrant

Exempel på potentiella konsekvenser
- Exponering av intern infrastruktur till obehöriga
- Öppnande av attackvägar in mot känsliga system eller känslig infrastruktur
- Driftstörningar på grund av att den nya tekniken inte är fullt mogen
- Driftstörningar på grund av att den egna personalen inte är erfaren med den nya tekniska lösningen

Se också
5.14.4

Referenser

5.14.4 Införande av teknisk lösning som inte är känd av driftspersonal

Beskrivning
För snabbt anammande av nya tekniska lösningar, som medför nya – ibland okända eller dolda – risker. Det finns en dimension av risker som bottnar i att driftspersonalen inte är bekant eller har erfarenhet av den tekniska lösningen och därmed gör fel, missar vissa signaler, utför riskabla moment, med mera . Dessa risker kan uppstå i samband med att dessa tekniska lösningar tas i drift, eller att de varit drifttagna en stund.

Kategori
Tekniskt hot

Orsak/Aktör
Kompetensbrist, brist på erfarenhet, avsaknad av risktänk, avsaknad av utbildning och fortbildning

Exempel
- Införande av molntjänster
- Införande av IPv6
- Införande av en annan virtualiseringslösning

Exempel på potentiella konsekvenser
- Öppnande av attackvägar in mot känsliga system eller känslig infrastruktur
- Driftstörningar på grund av att personalen inte vill använda den nya tekniken
- Driftstörningar på grund av att den egna personalen inte är erfaren med den nya tekniska lösningen

Se också
5.14.3

Referenser
SS-ISO/IEC 27002:2005 kap 6.1.7 ”Kontakt med särskilda intressegrupper”

5.14.5 Användning av föråldrad systemprogramvara utan adekvata skydd

Beskrivning
Installationen av IT-miljön består av äldre komponenter, både hård- och mjukvara. Den gamla systemprogramvaran består av operativsystem som saknar modernare skydd mot angrepp och säkerhetskritiska händelser.

Kategori
Tekniskt hot

Orsak/Aktör
Kompetensbrist, brist på erfarenhet, avsaknad av risktänk

Exempel
- Äldre versioner av Windows saknar bra skydd mot buffertöverskrivningsattacker (exempelvis DEP, Data Execution Prevention , och ASLR, Adress Space Localisation Randomization)
- Äldre versioner av databashanterare saknar skydd för kryptering av data i databaser eller vid koppling mot klientprogram
- Många äldre programvaror är inte skyddade mot modernare klasser av angrepp, tex injiceringsattacker, buffertöverskrivningsattacker, mm

Exempel på potentiella konsekvenser
- Avsaknad av moderna inbyggda skydd i systemprogramvara gör det är lättare att utföra olika typer av angrepp mot en dator som används som HMI i ett ICS-system eller mot servrar i samma lösning. Dessa system kan angripas och kan efter lyckat angrepp kontrolleras av angriparen, varpå systemets integritet är komprometterad. Det går därefter inte att lita på systemets korrekthet och därmed är inte heller den fysiska processen längre under kontroll.

Se också
5.14.6

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.4 ”Underhåll av utrustning”

5.14.6 Användning av föråldrad applikationsprogramvara utan adekvata skydd

Beskrivning
Installationen av IT-miljön består av äldre komponenter, både hård- och mjukvara. Den gamla systemprogramvaran består av operativsystem som saknar modernare skydd mot angrepp och säkerhetskritiska händelser.

Kategori
Tekniskt hot

Orsak/Aktör
Kompetensbrist, brist på erfarenhet, avsaknad av risktänk

Exempel

- Den webbserverprogramvara som ingår i lösningen saknar skydd mot grundläggande webbangrepp, exempelvis directory traversal-attacker, injicering av kod (SQL-injektionsattacker)
- De programkomponenter som är installerade saknar skydd mot fjärranvändning då systemet ursprungligen utformats så att man enbart trott att det skall användas av lokala användare.

Exempel på potentiella konsekvenser
Avsaknad av moderna adekvata skydd i applikationsprogramvaror gör det är lättare att utföra olika typer av angrepp mot datorer som används som i ett ICS-system eller mot servrar i samma lösning. Dessa system kan angripas och kan efter lyckat angrepp kontrolleras av angriparen, varpå systemets integritet är komprometterad. Det går därefter inte att lita på systemets korrekthet och därmed är inte heller den fysiska processen längre under kontroll.

Se också
5.14.1

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.4 ”Underhåll av utrustning”

6 Fysiska hot

Definition: Med **fysiska hot** avses

Hot som kan påverka, eller resultera i konsekvenser, saker i den fysiska världen

6.1 Oavsiktlig förlust av information

Detta kapitel handlar om olika sätt som information kan gå förlorad eller exponeras mot obehöriga eller informationsbehandlingsresurser kan gå förlorade.

6.1.1 Förlust av utrustning

Beskrivning
Förlust av utrustning som tillhör organisationen. Förlusten innebär i sin tur förlust av information och möjlig exponering av denna information mot obehörig tredje part.

Kategori
Fysiskt hot

Orsak/Aktör
Glömska, slarv, kompetensbrist, stöld

Exempel
- Tappad bärbar dator
- Tappad mobiltelefon
- Tappad läsplatta
- Tappad kommunikationsutrustning

Exempel på potentiella konsekvenser
- Användarnamn och lösenord till känsliga system såsom SCADA/ICS-system kan komma obehöriga tillhanda, dessa kan sedan missbrukas för systemaccess, vilket i sin tur kan påverka tillgänglighet eller riktighet i styrningen av den fysiska processen för elproduktion, eldistribution eller liknande
- Utrustningen kan ha automatiserad fjärrinloggning till känsliga system såsom SCADA/ICS-system kan komma obehöriga tillhanda, dessa kan sedan missbrukas för systemaccess, vilket i sin tur kan påverka tillgänglighet eller riktighet i styrningen av den fysiska processen för elproduktion, eldistribution eller liknande
- Intern information, till exempel ritningar eller nätkartor, kan vara informationstillgångar som fanns på den förlorade utrustningen, vilket sedan kan komma obehöriga tillhanda

Se också
6.1.2, 6.1.3

Referenser

SS-ISO/IEC 27002:2005 kap 9.2.1. ”Placering och skydd av utrustning”

6.1.2 Avyttring av utrustning, egendom och information

Beskrivning
Avyttring av utrustning, utan att ta bort databärare eller informationen från den utrustning som avvecklas. Avyttringen av utrustningen innebär i sin tur förlust av information och möjlig exponering av denna information mot obehörig tredje part.

Kategori
Fysiskt hot

Orsak/Aktör
Glömska, slarv, kompetensbrist

Exempel
- Avyttring av bärbar dator
- Avyttring av serverdator
- Avyttring av mobiltelefon
- Avyttring av RTU-enheter
- Avyttring av PLC-enheter
- Avyttring av läsplatta
- Avyttring av kommunikationsutrustning

Exempel på potentiella konsekvenser
- Användarnamn och lösenord till känsliga system såsom SCADA/ICS-system kan komma obehöriga tillhanda, dessa kan sedan missbrukas för systemaccess, vilket i sin tur kan påverka tillgänglighet eller riktighet i styrningen av den fysiska processen för elproduktion, eldistribution eller liknande
- Utrustningen kan ha automatiserad fjärrinloggning till känsliga system såsom SCADA/ICS-system kan komma obehöriga tillhanda, dessa kan sedan missbrukas för systemaccess, vilket i sin tur kan påverka tillgänglighet eller riktighet i styrningen av den fysiska processen för elproduktion, eldistribution eller liknande
- Intern information, till exempel ritningar eller nätkartor, kan vara informationstillgångar som fanns på den förlorade utrustningen, vilket sedan kan komma obehöriga tillhanda

Se också
6.1.1, 6.1.3

Referenser
ISO/IEC 27019:2013 kap 11.1.1 ”Access control policy”
ISO/IEC 27019:2013 kap 11.3.1 ”Password use”

6.1.3 Avveckling av utrustning

Beskrivning
Avveckling av utrustning, utan att ta bort databärare eller informationen från den utrustning som avvecklas. Avvecklingen av utrustningen innebär i sin tur förlust av information och möjlig exponering av denna information mot obehörig tredje part.

Kategori
Fysiskt hot

Orsak/Aktör
Glömska, slarv, kompetensbrist

Exempel
- Avveckling av bärbar dator
- Avveckling av serverdator
- Avveckling av mobiltelefon
- Avveckling av läsplatta
- Avveckling av kommunikationsutrustning

Exempel på potentiella konsekvenser
- Användarnamn och lösenord till känsliga system såsom SCADA/IECS-system kan komma obehöriga tillhanda, dessa kan sedan missbrukas för systemaccess, vilket i sin tur kan påverka tillgänglighet eller riktighet i styrningen av den fysiska processen för elproduktion, eldistribution eller liknande
- Utrustningen kan ha automatiserad fjärrinloggning till känsliga system såsom SCADA/IECS-system kan komma obehöriga tillhanda, dessa kan sedan missbrukas för systemaccess, vilket i sin tur kan påverka tillgänglighet eller riktighet i styrningen av den fysiska processen för elproduktion, eldistribution eller liknande
- Intern information, till exempel ritningar eller nätkartor, kan vara informationstillgångar som fanns på den förlorade utrustningen, vilket sedan kan komma obehöriga tillhanda

Se också
6.1.1, 6.1.2

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.6 ”Säker avveckling eller återanvändning av utrustning”

6.2 Olyckor

Detta stycke handlar om olika hot som består i olyckor av olika slag eller som resulterar i olyckor.

6.2.1 Olycka som medför personskada av nyckelperson inom organisationer

Beskrivning
Olyckor kan uppstå på arbetsplatsen eller i det privata. Den eller de personer som skadas kan vara personer med nyckelpositioner, med särskild kunskap eller färdigheter, som är väsentliga för organisationen.

Kategori
Fysiskt hot

Orsak/Aktör
Kompetensbrist, brist på erfarenhet, slarv, tekniska fel

Exempel

- Arbetsplatsolycka på plats i en anläggning
- Olycka i samband med elarbete
- Olycka under färd till eller från ett arbetspass

Exempel på potentiella konsekvenser

- Nyckelpersoner med anläggningskunskap skadas och blir otillgängliga under en tid
- Nyckelpersoner med kunskap och färdigheter i driftoperativa delar av verksamheten skadas och blir otillgängliga under en tid

Se också

Referenser

6.2.2 Olycka

Beskrivning
Det uppstår en eller flera olyckor som drabbar personer på ett sådant sätt att de blir arbetsoförda

Kategori
Fysiskt hot

Orsak/Aktör
Kompetensbrist, brist på erfarenhet, slarv, tekniska fel

Exempel

- Arbetsplatsolycka på plats i en anläggning
- Olycka i samband med elarbete
- Olycka under färd till eller från ett arbetspass
- En organisation med vilka man samarbetar, har som underleverantör, är beorende av, drabbas av en olycka

Exempel på potentiella konsekvenser

- Många personer blir skadade så man inte kan hålla drift
- Personer utanför organisationen blir skadade
- De organisationer man samarbetar med kan inte leverera till den nivå som är överrenskommet på grund av att de saknar nyckelpersoner

Se också

Referenser

6.2.3 Olycka orsakad av transport av farligt gods

Beskrivning
Olycka som orsakats av transport av farligt gods

Kategori
Fysiskt hot

Orsak/Aktör
Kompetensbrist, brist på erfarenhet, slarv, tekniska fel

Exempel

- Järnväg
- Långtradare
- Flyg
- Gasol
- Petrokemiska produkter

Exempel på potentiella konsekvenser

- Det går under en kortare tid inte nå arbetsplatser för den personal som arbetar där
- Det går under en längre tid inte nå arbetsplatser för den personal som arbetar där
- Anläggningar blir direkt skadade av olyckan
- Kablage blir skadade av olyckan
- Ledningar blir skadade av olyckan

Se också
6.2.4

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.2.4 Olycka med farligt gods i närområdet

Beskrivning
Med närområde här avses både det som är inom avstånd från kontor och andra personalutrymmen, men även andra typer av anläggningar såsom datorcentraler.

Kategori
Fysiskt hot

Orsak/Aktör
Kompetensbrist, brist på erfarenhet, slarv, tekniska fel

Exempel
- Cisterner och behållare
- Industriell verksamhet
- Gasol, acetylen
- Petrokemiska produkter

Exempel på potentiella konsekvenser
- Det går under en kortare tid inte nå arbetsplatser för den personal som arbetar där
- Det går under en längre tid inte nå arbetsplatser för den personal som arbetar där
- Anläggningar blir direkt skadade av olyckan
- Kablage blir skadade av olyckan
- Ledningar blir skadade av olyckan

Se också
6.2.3

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.2.5 Olycka som medför personskada för tredje part

Beskrivning
Det uppstår en olycka som medför personskada för tredje part, exempelvis leverantörer eller entreprenörer med tillgång till anläggning. Det kan också vara personer som tagit sig in på anläggningen och därmed tagit sig förbi de skydd och hinder som skapats för att skydda mot obehörig åtkomst.

Kategori
Fysiskt hot

Orsak/Aktör
Kompetensbrist, brist på erfarenhet, slarv, tekniska fel

Exempel
- Områdesskydd saknas, varpå personer kommer in i anläggning och skadas
- Områdesskydd är skadat så att det underlättar för tredje part att få åtkomst, varpå personer kommer in i anläggning och skadas
- Extern personal som är på plats i anläggning skadas

Exempel på potentiella konsekvenser
- Strömavbrott i anläggning som slår ut fältplacerad utrustning
- Skador på utrustning placerad i anläggning

Se också
6.2.6, 6.2.7

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.2.6 Olycka som medför egendomsskada

Beskrivning
Det uppstår en olycka som medför egendomsskada, antingen för den egna organisationen eller för tredje part, exempelvis i samband med att leverantörer eller entreprenörer med tillgång till anläggning utför arbete. Det kan också vara personer som tagit sig in på anläggningen och därmed tagit sig förbi de skydd och hinder som skapats för att skydda mot obehörig åtkomst

Kategori
Fysiskt hot

Orsak/Aktör
Kompetensbrist, brist på erfarenhet, slarv, tekniska fel

Exempel

- Skada på andras fastigheter i samband med nybyggnation
- Skada på andras fastigheter i samband med ombyggnation
- Skada på andras markegendomar i samband med nybyggnation
- Skada på andra nätägares utrustning

Exempel på potentiella konsekvenser

- Skadeståndsskyldighet
- driftsbortfall

Se också
6.2.5, 6.2.7

Referenser

6.2.7 Olycka som medför miljöskada

Beskrivning
Det uppstår en olycka som medför miljöskada, antingen för den egna organisationen eller för tredje part, exempelvis i samband med att leverantörer eller entreprenörer med tillgång till anläggning utför arbete

Kategori
Fysiskt hot

Orsak/Aktör
Kompetensbrist, brist på erfarenhet, slarv, tekniska fel

Exempel

- Brand i transformator, olja läcker ut i naturen
- Översvämning av damm

Exempel på potentiella konsekvenser

- Skador i miljön som ansluter till anläggningen
- Skador i miljön på längre avstånd i anläggningen

Se också
6.2.5, 6.2.6

Referenser

6.3 Upplopp och civil oro inom land där organisationen bedriver verksamhet

Beskrivning
Det uppstår upplopp och civil oro i ett land där organisationen bedriver sin verksamhet. Denna verksamhet kan direkt eller indirekt påverka organisationen.

Kategori
Fysiskt hot

Orsak/Aktör
Kriminella, externa aktörer

Exempel
- Genom blockader, vandalism och liknande kan man drabbas av
  - Svårigheter att nå anläggningar, arbetsplatser och liknande
  - Att utrustning, anläggningar förstörs helt eller i delar

Exempel på potentiella konsekvenser
- Driftstörningar
- Förstörd utrustning som har långa tider för att få fram ersättningsutrustning

Se också
6.4

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.1 ”Skalskydd”
SS-ISO/IEC 27002:2005 kap 9.1.2 ”Tillträdeskontroll”
SS-ISO/IEC 27002:2005 kap 9.1.3 ”Skydd av kontor, rum och faclilitеter”
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.4 Upplopp och civil oro inom land där underleverantörer av IT-tjänster har drift av IT-stöd och IT-resurser å organisationens vägnar

Beskrivning
Det uppstår upplopp och civil oro i ett land där underleverantörer, exempel IT-driftspartners, till organisationen bedriver sin verksamhet. Denna verksamhet kan direkt eller indirekt påverka organisationen

Kategori
Fysiskt hot

Orsak/Aktör
Kriminella, externa aktörer

Exempel

- Genom blockader, vandalism och liknande kan partnerföretaget drabbas av
  - Svårigheter att nå anläggningar, arbetsplatser och liknande
  - Att utrustning, anläggningar förstörs helt eller i delar

Exempel på potentiella konsekvenser

- Driftstörningar
- Förstörd utrustning som har långa tider för att få fram ersättningsutrustning

Se också
6.3

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.1 ”Skalskydd”
SS-ISO/IEC 27002:2005 kap 9.1.2 ”Tillträdeskontroll”
SS-ISO/IEC 27002:2005 kap 9.1.3 ”Skydd av kontor, rum och facliliteter”
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.5 Fysiska hot

Detta kapitel omfattar hot som innebär skada på fysiska objekt, exempelvis anläggningar eller utrustning.

6.5.1 Problem med försörjningssystem: kylning

Beskrivning
I datorhallar, kommunikationsrum, korskopplingsrum, driftcentraler eller kontrollrum med tillhörande IT-rum och andra utrymme där IT-system och IT-komponenter är installerade behövs det ofta kylanläggningar för att kyla bort den överskottsvärme som uppstår av att utrustningen är driftsatt.

Kategori
Fysiskt hot, tekniskt hot

Orsak/Aktör
Tekniskt fel, designfel, underdimensionerad lösning, felkoppling

Exempel
- Lokalt kylsystem i datorhall går sönder och slutar att fungera, varpå utrustning skadas av värmehöjningen.
- Strömavbrott gör att reservkraft används till datorhall och driftcentral eller kontrollrum, men reservkraften är inte kopplad till kylsystemet vilket gör att datorhall får värmeproblem

Exempel på potentiella konsekvenser
- Bortfall i elproduktion
- Bortfall av eldistribution
- Bortfall av stödsystem och automation, vilket leder till manuell bemanning i anläggning

Se också
6.5.2, 6.5.3, 6.5.4

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.2 ”Tekniska försörjningssystem”
ISO/IEC 27019:2013 kap 9.1.7 ”Securing control centers”

6.5.2 Problem med försörjningssystem: elförsörjning

Beskrivning
I datorhallar, kommunikationsrum, korskopplingsrum, driftcentraler eller kontrollrum med tillhörande IT-rum och andra utrymme där IT-system och IT-komponenter är installerade behövs det ofta tillräcklig och kvalitativ strömförsörjning. Av detta följer att elförsörjningen måste vara rätt dimensionerad och att det ofta behövs avbrottsfri elförsörjning för att klara temporära strömbortfall.

Kategori
Fysiskt hot, tekniskt hot

Orsak/Aktör
Tekniskt fel, designfel, underdimensionerad lösning, felkoppling

Exempel
- Otillräcklig kapacitet i reservkraft
- Felaktigt inkopplad reservkraft
- Felaktigt kopplad elmatning
- Felaktigt dimensionerad elmatning
- Felaktigt jordad elanslutning
- Inte kontrollerat att reservkraften fungerar när ett skarpt läge inträffar, utan de tester som gjorts har inte gjorts i full skala eller med riktig frånkoppling

Exempel på potentiella konsekvenser
- Bortfall i elproduktion
- Bortfall av eldistribution
- Bortfall av stödsystem och automation, vilket leder till manuell bemanning i anläggning

Se också
6.5.1, 6.5.3, 6.5.4

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.2 ”Tekniska försörjningssystem”

6.5.3 Problem med försörjningssystem: kommunikation

Beskrivning
Till IT-system och IT-miljöer behövs det ofta datorkommunikation i form av lokala, regionala samt organisations- och koncernövergripande nätverkskopplingar. Om det uppstår kommunikationsproblem någonstans i detta nätverk så kan det drabba funktionalitet, datakvalitet och tillgänglighet i såväl system som applikationer.

Kategori
Fysiskt hot, tekniskt hot

Orsak/Aktör
Tekniskt fel, designfel, underdimensionerad lösning, felkoppling

Exempel
- Ingen reservkapacitet eller reservvägar för kommunikation
- Kabelbrand
- Avgrävd eller avbrott på kommunikationskablar
- Otillräcklig reservkraft i samband med elavbrott, vilket gör att kommunikationssystem slutar att fungera, ibland innan reservkraft till datorhallar eller annan utrustning.
- Händelser i den externa miljön vilket påverkar kommunikationsutrustning eller kommunikationskanaler, tex bränder, väder, temporärt uppförda anläggningar såsom byggnadsställningar eller kranbilar, etc

Exempel på potentiella konsekvenser
- Bortfall i elproduktion
- Bortfall av eldistribution
- Bortfall av stödsystem och automation, vilket leder till manuell bemanning i anläggning

Se också
6.5.1, 6.5.2, 6.5.4

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.2 ”Tekniska försörjningssystem”

6.5.4 Otillräcklig övervakning av försörjningssystem

Beskrivning
De försörjningssystem i form av kyla, elförsörjning eller datorkommunikation som finns för att IT-miljön skall finnas och fungera kan behöva övervakas. Till exempel så kan den avbrottsfria kraftförsörjningen och dess batterireserver kan behöva övervakas, så att återladdning sker korrekt och att den avbrottsfria kraften är aktiverad att kunna ta över elförsörjningen.

Kategori
Fysiskt hot, tekniskt hot

Orsak/Aktör
Designfel, kompetensbrist, otillräckliga resurser

Exempel
- Övervakningsmekanismer och övervakningssystem är inte installerade för att övervaka försörjningsystem eller när man temporärt försörjs av reservsystem
- Alarm skickas inte när ett försörjningssystem (kyla, el, kommunikation) försvinner och drift övergår till reservsystem
- Alarm skickas, men mottas inte, inte när ett försörjningssystem (kyla, el, kommunikation) försvinner och drift övergår till reservsystem

Exempel på potentiella konsekvenser
- Fältutrustning slås ut på grund av att övervakningen av den avbrottsfria kraften inte är korrekt. Reservkraftskapaciteten är kortare än beräknat och utrustningen blir snabbt strömlös.
- Bortfall i elproduktion
- Bortfall av eldistribution
- Bortfall av stödsystem och automation, vilket leder till manuell bemanning i anläggning

Se också
6.5.1, 6.5.2, 6.5.3

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.2 ”Tekniska försörjningssystem”

6.5.5 Mekaniska fel i utrustning

Beskrivning
Datorer och IT-utrustning är ofta till stor del baserad på elektroniska kretsar, men ett fåtal mekaniska delar finns i modern IT-utrustning, såsom exempelvis fläktar som kyler processorn, fläktar som kyler hela system datorenheten, stegmotorer som används för att flytta läs- och skrivhuvud på diskar, etc. I denna typ av komponenter kan det uppstå mekaniska fel i utrustningen .

Kategori
Fysiskt hot, tekniskt hot

Orsak/Aktör
Tekniskt fel

Exempel
- Lagringsmedia går sönder med informationsförlust som resultat
- Fläktar i kabinett eller system går sönder med resultat att värmeutvecklingen påverkar systemen kvalitet och tillgänglighet
- Motorstyrning i hårddiskar av stegmotorer som flyttar läs och skrivhuvud

Exempel på potentiella konsekvenser
- Bortfall i elproduktion
- Bortfall av eldistribution
- Bortfall av stödsystem och automation, vilket leder till manuell bemanning i anläggning

Se också

Referenser

6.5.6 Sabotage mot IT system

Beskrivning
Sabotage med särskild inriktning mot IT-system, IT-systemkomponenter, IT-komponenter.
.

Kategori
Fysiskt hot, tekniskt hot

Orsak/Aktör
Antagonistiska angrepp från statsaktörer, extremistgrupper, terroristgrupper, organiserad brottslighet, kriminella

Exempel
- Förstörelse av datorenheter
- Förstörelse av nätverksportar
- Förstörelse av lagringsmedia och lagringsenheter
- Avklippta nätverkskablar

Exempel på potentiella konsekvenser
- Temporärt avbrott i kommunikationen mellan olika komponenter i ett SCADA-system, exempelvis fältplacerad utrustning och centrala SCADA-servrar.
- Bortfall i elproduktion
- Bortfall av eldistribution

Se också
6.5.5, 6.5.7

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.1 ”Skalskydd”
SS-ISO/IEC 27002:2005 kap 9.1.2 ”Tillträdeskontroll”
SS-ISO/IEC 27002:2005 kap 9.1.3 ”Skydd av kontor, rum och faciliteter”
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”
SS-ISO/IEC 27002:2005 kap 9.1.5 ”Arbete i säkra utrymmen”
SS-ISO/IEC 27002:2005 kap 9.2.1 ”Placering och skydd av utrustning”
SS-ISO/IEC 27002:2005 kap 9.2.3 ”Kablageskydd”
ISO/IEC 27019:2013 kap 9.1.1 ”Physical security perimeter”

6.5.7 Sabotage mot kommunikationsinfrastruktur

Beskrivning
Sabotage med särskild inriktning mot kommunikationsinfrastruktur i ett IT-system, IT-systemkomponenter, IT-komponenter. .

Kategori
Fysiskt hot, tekniskt hot

Orsak/Aktör
Antagonistiska angrepp från statsaktörer, extremistgrupper, terroristgrupper, organiserad brottslighet, kriminella

Exempel
- Förstörelse av nätverkskomponenter såsom switchar, routers, radioutrustning, satellitmottagare
- Förstörelse av nätverksportar
- Avklippta nätverkskablar

Exempel på potentiella konsekvenser
- Temporärt avbrott i kommunikationen mellan olika komponenter i ett SCADA-system, exempelvis fältplacerad utrustning och centrala SCADA-servrar.
- Bortfall i elproduktion
- Bortfall av eldistribution

Se också
6.5.6, 6.5.8

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.1 ”Skalskydd”
SS-ISO/IEC 27002:2005 kap 9.1.2 ”Tillträdeskontroll”
SS-ISO/IEC 27002:2005 kap 9.1.3 ”Skydd av kontor, rum och faciliteter”
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”
SS-ISO/IEC 27002:2005 kap 9.1.5 ”Arbete i säkra utrymmen”
SS-ISO/IEC 27002:2005 kap 9.2.1 ”Placering och skydd av utrustning”
SS-ISO/IEC 27002:2005 kap 9.2.3 ”Kablageskydd”

6.5.8 Sabotage mot elsystem

Beskrivning
Sabotage med särskild inriktning mot elförsörjningsdelarna i ett IT-system, IT-systemkomponenter, IT-komponenter.

Kategori
Fysiskt hot, tekniskt hot, antagonistiskt hot

Orsak/Aktör
Statsaktörer, extremistgrupper, terroristgrupper, organiserad brottslighet, kriminella

Exempel
- Angrepp och sabotage mot inkommande strömmatning och strömförsörjning
- Angrepp och sabotage mot UPS-systemet och dess batterilager tillhörande datorhall
- Angrepp och sabotage mot dieselaggregat och dieseltankar tillhörande datorhall

Exempel på potentiella konsekvenser
- Bortfall i elproduktion
- Bortfall av eldistribution
- Sabotage mot reservdelslager kan innebära längre ställtider eller leveranstider på alternativ ersättningsutrustning

Se också
6.5.6, 6.5.7

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.1 ”Skalskydd”
SS-ISO/IEC 27002:2005 kap 9.1.2 ”Tillträdeskontroll”
SS-ISO/IEC 27002:2005 kap 9.1.3 ”Skydd av kontor, rum och faciliteter”
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”
SS-ISO/IEC 27002:2005 kap 9.1.5 ”Arbete i säkra utrymmen”
SS-ISO/IEC 27002:2005 kap 9.2.1 ”Placering och skydd av utrustning”
SS-ISO/IEC 27002:2005 kap 9.2.3 ”Kablageskydd”
ISO/IEC 27019:2013 kap 9.1.1 ”Physical security perimeter”

6.5.9 Sabotage/kortslutning av högspänningsledning

Beskrivning
Någon kortsluter en högspänningsledning genom att med exempelvis pil och båge eller modellraket med kopplad ledande släpkabel skjuta över faslinorna och på detta sätt orsaka en omedelbar och total kortslutning av den aktuella högspänningsledningen.

Kategori
Tekniskt/Fysiskt hot

Orsak/Aktör
Terrorism, organiserad brottslighet, enskilda brottslingar och rättshaverister

Exempel
- Kolfiberlina med anpassad längd och änd-krok skjuts från säkert avstånd i en båge över faslinorna.
- Modellraket av mid- eller high power typ kopplas till koppar eller stålwire av betydande längd som sedan riktas över faslinorna i en redan utprovad avfyringsvinkel. Denna kan sedan fjärrutlösas med hjälp av mobiltelefon, personsökare eller annan fjärrteknologi så som exempelvis SMS-aktiveringskontakter för att slå på värme över telefon i sommarstugor.

Exempel på potentiella konsekvenser
När en kraftledningsstolpe fallerar genom att helt eller till del falla eller ”niga” så medför detta att faslinor kommer inom överslagsavstånd från vegetation, byggnader eller något annat. Det elektriska överslaget kan resultera i eldsvåda eller eldstorm beroende på omständigheter. Risken för personskador är uppenbar.

Se också

Referenser
Kortslutning med kopparlina: http://www.youtube.com/watch?v=mqRT7J86rco
Exempel på annan kortslutning: http://www.youtube.com/watch?v=ZIuHbQSPjEA

6.5.10 Sabotage/staglinor påverkas för att brista och få kraftledningsstolpe att haverera och falla

Beskrivning
Någon påverkar mekaniskt eller kemiskt staglinor till kraftledningsstolpe i ett utsatt läge där haveri kan förväntas om staglinorna fallerar.

Kategori
Tekniskt/Fysiskt hot

Orsak/Aktör
Terrorism, organiserad brottslighet, enskilda brottslingar och rättshaverister

Exempel
- Någon applicerar exempelvis batterisyra (svavelsyra) genom att rikligt pensla denna på samtliga staglinor eller staglinor på ena sidan av stolpe så att denna försvagas i en riktning. Syra kommer sakta att lösa upp materialet i staglinorna över tiden om inte miljörelaterade faktorer eller annat ingripande stoppar processen.
- Mekaniskt angrepp direkt på staglinor med exempelvis batteridriven vinkelkap eller tigersåg.
- Staglinor eller fästen riggas och påverkas med sprängämnen som tillverkats med stöd av information som finns på Internet, exempelvis TATP (triacetontriperoxid) eller pikrinsyra.

  Applicering av syra eller sprängämne kan riggas i förväg i kapsling och sedan fjärrutlösas med hjälp av mobiltelefon, personsökare eller annan fjärrteknologi så som exempelvis SMS-aktiveringskontakter för att slå på värme över telefon i sommarstugor.

Exempel på potentiella konsekvenser
När en kraftledningsstolpe fallerar genom att helt eller till del falla eller ”niga” så medför detta att faslinor kommer inom överslagsavstånd från vegetation, byggnader eller något annat. Det elektriska överslaget kan resultera i eldsvåda eller eldstorm beroende på omständigheter. Risken för personskador är uppenbar.

Se också

Referenser
TATP: http://www.youtube.com/watch?v=JuILFQIaLrQ
Pikrinsyra: http://www.youtube.com/watch?v=E97QGKzjwAE
Kortslutning med kopparlina: http://www.youtube.com/watch?v=mqRT7J86rco
Exempel på annan kortslutning: http://www.youtube.com/watch?v=ZIuHbQSPjEA

6.5.11 Sabotage/påverkan av anläggning eller motsvarande för att minska eller förhindra tillgängligheten till anläggningen

Beskrivning
Någon påverkar anläggningens ingångspunkter mekaniskt eller elektroniskt så att dessa inte går att öppna på ordinarie vis.

Kategori
Tekniskt/Fysiskt hot

Orsak/Aktör
Terrorism, organiserad brottslighet, enskilda brottslingar och rättshaverister

Exempel
- Införsel av metall i låskolvar genom exempelvis inslagning av mjuk spik, lödtenn etc.
- Påverkan av låskolvar med syra, exempelvis batterisyra.
- Påverkan av karmar med starkt lim, PL400, super epoxi eller motsvarande.
- Innästling av låswires i grindar och öppningsbara staket.
- Påverkan av elektronik i elektroniska lås, exempelvis genom att aktivera en magnetron och rikta denna på nära avstånd mot det elektroniska låset. En magnetron kan plockas ur en mikrovågsugn, komplett med drivelektronik.

Påverkan av låskolvar är en klassisk metod för att förhindra eller försena tillgänglighet. På Internet finns allmänt tillgänglig information om hur man kan utnyttja komponenter från bland annat mikrovågsugnar för att bygga utrustning som i något avseende kan jämföras med förstörande elektroniska vapen.

Exempel på potentiella konsekvenser
Ett angrepp av ovan angiven karaktär syftar uteslutande till att påverka tillgängligheten till den berörda anläggningen och sekundärt produktion i verksamheten.

Se också
4.1.5

Referenser

http://www.youtube.com/watch?v=4FoS8f8VXLg
http://www.youtube.com/watch?v=Bhnp2-l1cxY

6.5.12 Sabotage/påverkan av damm, ställverk eller annan anläggning

Beskrivning
Någon påverkar anläggningen med smitta av kemisk/biologisk eller radiaktyp.

Kategori
Tekniskt/Fysiskt hot

Orsak/Aktör
Terrorism, organiserad brottslighet, enskilda brottslingar och rättshaverister

Exempel
- Gift av exempelvis nedan beskriven art appliceras på dörrhandtag, karmar, beslag eller annan utrustning. Genom att först göra giftet mindre flyktigt genom uppblandning i vaselin, tapetklister, sirap eller annan trög vätska eller hushållskemikalie ökar uthålligheten i ett sådant angrepp.
- Radioaktivt material, exempelvis Americium 241, finfördelas till pulver eller damm och används som ovan eller genom dispenser i ventilationskanaler eller motsvarande.

Idag finns information om hur man anskaffar eller framställer mycket farligt gift allmänt tillgängligt på Internet. Exempel på sådana gifter är kaliumcyanid, nikotin, ricin, arsenik, tallium m.fl. Americium 241, som här endast är ett exempel, finns i de vanligaste brandvarnarna på marknaden. Att göra om det metalliska radioaktiva ämnet till pulver kan ske med verktyg tillgängliga på hobbymarknaden.

Exempel på potentiella konsekvenser
Ett angrepp av ovan angiven karaktär syftar uteslutande till att påverka personal och i och med detta försämra tillgängligheten på primärt resurser och sekundärt produktion i verksamheten.

Se också
4.1.5

Referenser

6.5.13 Bombhot

Beskrivning
En typ av hot är ett förtäckt hot där någon påstår sig placera sprängämnen eller bomber i eller i anslutning till en för organisationen intressant anläggning eller byggnad. Hotet om att utlösa en explosion tas ofta på allvar och leder vanligtvis till att man temporärt får utrymma byggnader.

Kategori
Fysiskt hot, antagonistiskt hot

Orsak/Aktör
Statsaktörer, extremistgrupper, terroristgrupper, organiserad brottslighet, kriminella

Exempel
- Bombhot mot en driftcentral eller ett kontrollrum som innebär att den måste utrymmas
- Bombhot mot en produktionsanläggning (vattenkraftverk, värmeverk, etc) som innebär att anläggningen måste utrymmas
- Bombhot mot en kontorsarbetsplats där servicepersonal arbetar

Exempel på potentiella konsekvenser
- Tillfälligtvis blir en anläggning eller en tjänst obemannad, vilket i sin tur kan få följdverkningar om något annat inträffar samtidigt som kräver en insats eller åtgärd från personalen.
- Om hotet realiseras och en bomb exploderar så finns risk för bortfall i elproduktion
- Om hotet realiseras och en bomb exploderar så finns risk för bortfall av eldistribution

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.1 ”Skalskydd”
SS-ISO/IEC 27002:2005 kap 9.1.2 ”Tillträdeskontroll”
SS-ISO/IEC 27002:2005 kap 9.1.3 ”Skydd av kontor, rum och faciliteter”
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”
SS-ISO/IEC 27002:2005 kap 9.2.1 ”Placering och skydd av utrustning”
ISO/IEC 27019:2013 kap 9.1.1 ”Physical security perimeter”
ISO/IEC 27019:2013 kap 9.1.7 ”Securing control centers”

6.6 Miljöskada

Detta kapitel omfattar hot som innebär skada på fysiska objekt med relation till miljö, exempelvis översvämning och brand.

6.6.1 Miljöskada: allmänt

Beskrivning
Olika former av miljöskada som påverkar anläggningar, elsystemsutrustning, IT-utrustning, med mera. Dessa miljöskador kan temporärt eller permanent påverka utrustning..

Kategori
Fysiskt hot

Orsak/Aktör
Naturkatastrof, oavsiktlig mänsklig påverkan, felaktigt utförd lösning

Exempel
- Nedsmutsning
- Damm
- Rost
- Brand

Exempel på potentiella konsekvenser
- Skada på driftutrustning som gör att den temporärt slås ut
- Skada på driftutrustning som gör att den permanent slås ut

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.6.2 Miljöskada: Vatten

Beskrivning
Vatten kan vara ett hot mot mycket utrustning och maskiner men också mot att en arbetsplats skall kunna vara användbar.. .

Kategori
Fysiskt hot

Orsak/Aktör
Naturkatastrof, oavsiktlig mänsklig påverkan, felaktigt utförd lösning

Exempel
- Felaktigheter i fastighetsautomation, tex kylanläggning vilket leder till vätskeutsläpp
- Felaktigheter i fastighetsautomation, tex uppvärmning, vilket leder till vätskeutsläpp
- Felaktigheter i fastighetsautomation, tex avlopp, vilket leder till vätskeutsläpp
- Felaktigheter i ledningar som bär vätska leder till vätskeutsläpp
- Felaktigheter i sprinklersystem, vilket leder till vätskeutsläpp

Exempel på potentiella konsekvenser
- Utrustning och maskiner blir skadade av vatten
- Utrustning och maskiner blir skadade av kortslutningar och elfel som en följd av att vatten kommit ut i utrymmen
- Anläggningar och arbetsutrymmen blir obrukbara som ett resultat av vätskeutsläpp

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.6.3 Miljöskada: Översvämning i terräng

Beskrivning
Av olika skäl, exempelvis nederbörd i terrängen eller att en vattenledning springer läck, så blir det översvämning i terräng. Denna typ av översvämning kan få följdverkningar på anläggningar, utrustning, maskiner och människor.

Kategori
Fysiskt hot

Orsak/Aktör
Naturkatastrof, oavsiktlig mänsklig påverkan, felaktigt utförd lösning

Exempel
- Översvämningar som följd av regn och smältvatten som skadar anläggningar
- Utrymmen där IT-utrustning förvaras är icke ändamålsenlig och befinner sig under gatuplan, vilket gör att översvämning i terrängen tränger in i utrymmet

Exempel på potentiella konsekvenser
- Delar av anläggningar kan ställas under vatten som en följd av översvämning i terräng
- Hela anläggningen kan ställas under vatten som en följd av översvämning i terräng
- Utrymmen som används som arbetsplatser kan ställas under vatten som följd av översvämning i terräng
- Utrymmen som används för IT- och kommunikationsutrustning kan ställas under vatten som följd av översvämning i terräng

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.6.4 Miljöskada: Brand

Beskrivning
Brand som utbryter i ett utrymme eller i dess direkta närhet. .

Kategori
Fysiskt hot

Orsak/Aktör
Naturkatastrof, oavsiktlig mänsklig påverkan, felaktigt utförd lösning

Exempel

- Brand i anläggning
- Brand i anslutning anläggning
- Brand på arbetsplats
- Brand i anslutning till arbetsplats
- Brand i datorhall
- Brand i kommunikationsutrymme
- Utrymme där kablage är framdraget blir eldhärjat

Exempel på potentiella konsekvenser

- Driftcentral eller kontrollrum måste utrymmas och lämnas obemannad
- Utrymme som innehåller datorer eller elektronisk kommunikationsutrustning skadas, vilket påverkar drift och produktionsstatus på elproduktion
- Utrymme som innehåller datorer eller elektronisk kommunikationsutrustning skadas, vilket påverkar drift och produktionsstatus på eldistribution
- Utrymme som innehåller datorer eller elektronisk kommunikationsutrustning skadas, vilket påverkar drift och produktionsstatus på elhandel

Se också
6.6.5, 6.6.6, 6.6.7

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”
ISO/IEC 27019:2013 kap 9.1.7 ”Securing control centers”

6.6.5 Miljöskada: Skogsbrand

Beskrivning
Brand utbryter i skog och kringliggnade miljö. Denna brand är alltså utanför den egna tomten eller det område som man själv kontrollerar..

Kategori
Fysiskt hot

Orsak/Aktör
Naturkatastrof, oavsiktlig mänsklig påverkan, felaktigt utförd lösning

Exempel
- Skada på elstolpar av stål eller trä
- Skada på elanläggningar
- Skada på kablage för eldistribution
- Skada på kablage för kommunikation

Exempel på potentiella konsekvenser
- Strömavbrott i anläggning
- Egendomsskada på själva anläggningen
- Egendomsskada på utrustning som finns i anläggningen

Se också
6.6.4, 6.6.6, 6.6.7

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.6.6 Miljöskada: Farlig brandrök

Beskrivning
I samband med brand kan det uppstå farlig rökutveckling som påverkar människor och utrustning. Hälsofarlig rök kan påverka människor och nitrösa gaser som kan ingå i röken kan påverka såväl utrustning som människor.

Kategori
Fysiskt hot

Orsak/Aktör
Naturkatastrof, oavsiktlig mänsklig påverkan, felaktigt utförd lösning

Exempel
- Nitrösa gaser som påverkar elektronisk utrustning
- Nitrösa gaser som påverkar kablage till elektronisk utrustning
- Nitrösa gaser som påverkar maskiner

Exempel på potentiella konsekvenser
- Utrustning som används för att styra och övervaka elproduktion slås ut
- Utrustning som används för att styra och övervaka eldistribution slås ut
- Människor kan inte vistas i utrymmen där den hälsovådliga röken finns

Se också
6.6.4, 6.6.5, 6.6.7

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.6.7 Miljöskada: Värmeutveckling

Beskrivning
I samband med brand kan det uppstå värmeutveckling. Denna värmeutveckling kan ledas i byggnadsdelar, igenom väggar eller annat, och på så sätt påverka utrustning eller driftsplatser som inte direkt blir skadade av själva branden.

Kategori
Fysiskt hot

Orsak/Aktör
Naturkatastrof, oavsiktlig mänsklig påverkan, felaktigt utförd lösning

Exempel

- Värmeutveckling i anslutning till en driftsplats kan påverka och ha sönder utrustning, maskiner, kablage och annat som finns på driftsplatsen.

Exempel på potentiella konsekvenser

- Temporärt och kortvarigt driftstopp
- Långvarigt driftstopp då driftsplatsen blivit påverkad
- Långvarigt driftstopp då utrustning placerad på driftsplatsen blivit skadad

Se också
6.6.4, 6.6.5, 6.6.6

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.6.8 Miljöskada: Dammpartiklar

Beskrivning
Luften i en miljö där organisationen bedriver verksamhet fylls med dammpartiklar. Dessa dammpartiklar kan orsaka skada på en mängd olika sätt i elektronisk utrustning samt vara hälsoproblem för de personer som behöver vistas i denna miljö .

Kategori
Fysiskt hot

Orsak/Aktör
Naturkatastrof, oavsiktlig mänsklig påverkan, felaktigt utförd lösning

Exempel

- Dammpartiklar kan sätta igen filter till fläktar in i utrymmen där känslig elektronisk utrustning förvaras och är drifttagen
- Dammpartiklar kan sätta igen filter till fläktar in i utrustning som är drifttagen
- Uttag och anslutningsportar fylls igen så att det uppstår glappkontakt
- Brand kan uppstå om dammpartiklarna är av sådan natur att de är brandfarliga

Exempel på potentiella konsekvenser

- Utrustning placerad i fält kan slås ut då den inte får tillräcklig kyla från fläktar och tilluftssystem
- Brand kan uppstå i ett driftutrymme eller anläggning om dammpartiklarna är av sådan natur att de är brandfarliga

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.6.9 Miljöskada: Elektromagnetisk strålning

Beskrivning
Stark elektromagnetisk strålning kan påverka elektronisk utrustning så att den temporärt eller permanent skadas..

Kategori
Fysiskt hot, tekniskt hot

Orsak/Aktör
Naturkatastrof, oavsiktlig mänsklig påverkan, felaktigt utförd lösning

Exempel

- Omformare i en elanläggning avger elektromagnetisk strålning som stör IT-komponenter
- Transformator i en elanläggning avger elektromagnetisk strålning som stör IT-komponenter
- Mikrovågsugn är placerad i närheten av utrustning för ett trådlöst nätverk, vilket stör nätverkstrafiken

Exempel på potentiella konsekvenser

- Lagringsmedia bestående av hårddiskar blir påverkade och tappar information
- Identitets- och passagekort med magnetremsa blir påverkade och tappar information

Se också
5.14.1, 5.14.2, 6.6.10

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.1 ”Placering och skydd av utrustning”
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.6.10 Miljöskada: Radioaktiv strålning

Beskrivning
Radioaktiv strålning från en strålkälla som kan påverka personer och utrustning, kan få en plats att vara radioaktivt nedsmutsad vilket gör att den inte kan beträdas av människor i vanliga kläder och under vanliga former..

Kategori
Fysiskt hot, tekniskt hot

Orsak/Aktör
Avsiktlig mänsklig påverkan, oavsiktlig mänsklig påverkan, felaktigt utförd lösning

Exempel

- Personal kan ta skada av radioaktiviteten
- Utrustning kan ta skada av radioaktiviteten
- En anläggning kan ta skada av radioaktiviteten och anses vara radioaktivt smittad
- Ett område kan ta skada av radioaktiviteten och anses vara radioaktivt smittad

Exempel på potentiella konsekvenser

- Kommunikationsutrustning kan slås ut, så att det inte går att kommunicera med annan utrustning
- Ett område som under normala fall används som en vanlig arbetsplats, exempelvis en driftcentral eller ett kontrollrum, är radioaktivt nedsmutsat och därför kan personal inte längre arbeta i denna arbetsplats

Se också
6.6.9

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”
ISO/IEC 27019:2013 kap 9.1.7 ”Securing control centers”

6.7 Väder

Detta kapitel omfattar hot som innebär skada på fysiska objekt med relation till väder, exempelvis storm och blixtnedslag.

6.7.1 Väder: Storm

Beskrivning
Kraftiga stormväder kan påverka byggnader, anläggningar, ledningar- och ledningsstolpar.
Stormoväder kan också påverkar personers möjlighet att ta sig till och från ordinarie arbetsplatser.

Kategori
Fysiskt hot

Orsak/Aktör
Naturkraft

Exempel

- Kraftiga vindar som gör att träd faller på elledningar
- Kraftiga vindar som gör att träd faller på telefonledningar
- Kraftiga vindar som gör att träd faller tak till anläggningar
- Kraftiga vindar som gör att tak blåser av

Exempel på potentiella konsekvenser

- Kommunikationsstörningar mellan driftcentral eller ett kontrollrum och anläggningar
- Elavbrott i en anläggning
- Att en anläggning blir fysiskt skadad och måste repareras

Se också
6.7.2, 6.7.3, 6.7.4, 6.7.5, 6.7.6, 6.7.7, 6.7.8, 6.7.9

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.7.2 Väder: Regn och blixtnedslag

Beskrivning
Väderfenomen med nederbörd i form av regn eller hagel samt åska och blixtnedslag.

Kategori
Fysiskt hot

Orsak/Aktör
Naturkraft

Exempel
- Regn som fyller utrymme i anläggning
- Regn som fyller utrymme i datahall
- Regn som fyller utrymme i kommunikationsplats
- Blixtnedslag som orsakar utslagning av utrustning
- Blixtnedslag som orsakar brand

Exempel på potentiella konsekvenser
- Blixtnedslag som leder till att utrustning går sönder
- Blixtnedslag som leder till att försörjningssystem (kyla, el, kommunikation) slås ut
- Regn som leder till att översvämningar inträffar som fyller driftsutrymmen, gör att utrustning får vattenskador, mm

Se också
6.7.1, 6.7.3, 6.7.4, 6.7.5, 6.7.6, 6.7.7, 6.7.8, 6.7.9

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.7.3 Miljöskada: Snö

Beskrivning
Snönederbörd som leder till sådana rikliga mängder snö så att det innebär praktiska problem i samhället.

Kategori
Fysiskt hot

Orsak/Aktör
Naturkraft

Exempel

- Snö lägger sig på tak som ramlar in och förstör utrustning i den byggnad som hade taket
- Kyla som leder till att utrustning fryser sönder
- Snötyngda grenar lägger sig på ledningar som går av eller som orsakar kortslutning
- Snö medför att personal inte kan ta sig till jobbet
- Snö medför att leveranser av nödvändig utrustning eller tillbehör inte kan utföras

Exempel på potentiella konsekvenser

- Datorhall slås ut av att taket ramlat in

Se också
6.7.1, 6.7.2, 6.7.4, 6.7.5, 6.7.6, 6.7.7, 6.7.8, 6.7.9

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.7.4 Väder: snöoväder

Beskrivning
Snönederbörd som leder till sådana rikliga mängder snö så att det innebär det praktiska problem i samhället. .

Kategori
Fysiskt hot

Orsak/Aktör
Naturkraft

Exempel

- Kyla som leder till att utrustning fryser sönder
- Snötyngda grenar lägger sig på ledningar som går av eller som orsakar kortslutning

Exempel på potentiella konsekvenser

- Fjärråtkomst från SCADA-system och DCS-system till anläggningar drabbas då kommunikationsförbindelser slås ut av snöstormen. Anläggningarna får köras i lokal drift / lokal kontroll.

Se också
6.7.1, 6.7.2, 6.7.3, 6.7.5, 6.7.6, 6.7.7, 6.7.8, 6.7.9

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.7.5 Väder: Hagelstorm

Beskrivning
Nederbörd i form av frusna isklumpar som, i de fall de är större, kan orsaka omfattande materiell skada.

Kategori
Fysiskt hot

Orsak/Aktör
Naturkraft

Exempel

- Hagel som skadar transformatorer i elnätet
- Hagel som skadar antenner och kommunikationsutrustning för styrning av elnätet
- Hagel som förstör bilar och masstransport, vilket förhindrar folk att ta sig till arbetet

Exempel på potentiella konsekvenser

- Fjärråtkomst från SCADA-system och DCS-system till anläggningar drabbas då elektroniska kommunikationsförbindelser slås ut av hagelstormen. Anläggningarna får köras i lokal drift / lokal kontroll.

Se också
6.7.1, 6.7.2, 6.7.3, 6.7.4, 6.7.6, 6.7.7, 6.7.8, 6.7.9

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.7.6 Väder: Isstorm

Beskrivning
En isstorm är ett omfattande vinterväder som består av underkylt eller frysande regn. Isstormen kan orsaka svår halka och ge omfattande och svåra skador på infrastruktur, exempelvis kan kraft- och teleledningar bli svårt nedtyngda av isen.

Kategori
Fysiskt hot

Orsak/Aktör
Naturkraft

Exempel

- Avbrott i elförsörjning som följd av nedtyngda kraftledningar
- Avbrott i tele- och datakommunikationerna som följd av nedtyngda teleledningar

Exempel på potentiella konsekvenser

- Fjärråtkomst från SCADA-system och DCS-system till anläggningar drabbas då kommunikationsförbindelser slås ut av isstormen. Anläggningarna får köras i lokal drift / lokal kontroll.

Se också
6.7.1, 6.7.2, 6.7.3, 6.7.4, 6.7.5, 6.7.7, 6.7.8, 6.7.9

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”
https://www.msb.se/Upload/Kunskapsbank/utvarderingar-strategiska-analyser/bedomningar/Isstormsscenario_rapport_101210_webb.pdf

6.7.7 Väder: Sandstorm

Beskrivning
Sandstorm kan vara ett naturfenomen och en naturkraft som kan ha stor negativ påverkan på IT-miljö och komponenter som normalt finns i en IT-miljö, speciellt då finkorning sand kan tränga in sätta för luftfilter, tränga in och påverka motorer i fläktar, stegmotorer i CD/DVD-läsare, stegmotorer i hårddiskar, med mera.

Sandstormar är i Sverige ovanliga, men de går inte att utesluta att fenomen som liknar sandstormar kan uppstå i samband med hårda vindar under torra perioder. Likaså kan sandstormar inträffa i situationer där man har utlagd drift eller har driftsplatser utomlands.

Kategori
Fysiskt hot

Orsak/Aktör
Naturkraft

Exempel
- Finkorning sand tränger in i datorhall och förstör servrar
- Finkorning sand tränger in i kontrollrum och förstör klientdatorer
- Finkorning sand tränger in i datorhall och förstör storage-servrar
- Finkorning sand tränger in i korskopplingsrum och förstör switchar och routers

Exempel på potentiella konsekvenser
- Primär och sekundärservrar som används i en SCADA-miljö slås ut av den finkorniga sanden som tränger in
- Primär (trådbunden WAN-kopplingen) och sekundär (satellit) kommunikationsutrustning som används i en SCADA-miljö slås ut av den finkorniga sanden som tränger in

Se också
6.7.1, 6.7.2, 6.7.3, 6.7.4, 6.7.5, 6.7.6, 6.7.8, 6.7.9

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.7.8 Naturkatastrofer

Beskrivning
Naturkatastrof är en händelse orsakad av en eller flera naturkrafter vilket medför stora negativa konsekvenser för den omgivande miljön och de olika organismer som lever i denna miljö.

Kategori
Fysiskt hot

Orsak/Aktör
Naturkraft

Exempel

- Översvämning . .
- Jordbävningar . .
- Ler- och jordskred . . .
- Orkaner . .
- Tsunami .
- Vulkanisk aktivitet.

Exempel på potentiella konsekvenser

- Driftcentral eller kontrollrum blir utslagen på grund av översvämning
- Datorhall med servrar för SCADA-system blir utslagna på grund av översvämning
- Kommunikationsknutpunkt för datakommunikation, inklusive nätverk för processkontroll, blir skadade på grund av ler- och jordskred.

Se också
6.7.1, 6.7.2, 6.7.3, 6.7.4, 6.7.5, 6.7.6, 6.7.7, 6.7.9

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”
ISO/IEC 27019:2013 kap 9.1.7 ”Securing control centers”

6.7.9 Extrema naturkatastrofer

Beskrivning
Här definierar vi extrema naturkatastrofer såsom naturkatastrofer som omfattar mer än en enstaka nation eller enstaka kontinent.

Ett exempel på mer ovanliga och mer allvarliga händelser är så kallat extremt rymdväder med extrema solstormar. Dessa händelser skapar elektromagnetiska störningar som kan ha stor påverkan på elsystemet.

Kategori
Fysiskt hot

Orsak/Aktör
Naturkraft

Exempel

- Extremt rymdväder med extrema solstormar . .. som påverkar hela elsystemets eller vitala komponenter i elsystemet .
- Extrema stormsystem spridda över geografiskt stora områden

Exempel på potentiella konsekvenser

- Elsystemsutrustning blir utslagen, vilket gör att själva elsystemet inom en region helt eller i delar blir utslaget.
- Känslig IT-utrustning som används för styrning, övervakning och kommunikation i samband med kontroll av elsystemet slås ut.

Se också
6.7.1, 6.7.2, 6.7.3, 6.7.4, 6.7.5, 6.7.6, 6.7.7, 6.7.8

Referenser
SS-ISO/IEC 27002:2005 kap 9.1.4 ”Skydd mot externa hot och miljöhot”

6.8 Kriminella hot

Med kriminella hot avses hot som uppstår av en brottslig handling.

Till kriminella hot kan vi räkna:

- Bedrägeri
- Förskingring
- Utpressning
- Stöld av fysiska resurser
- Företagsspionerі
- Sabotage

Civilrättsliga hot inkluderar främst förtal

6.8.1 Bedrägeri

Beskrivning
Någon blir vilseledd eller utnyttjad till att utföra en handling eller att avstå from att utföra och på så sätt lurad på ett sådant sätt att en person eller en organisation lider en ekonomisk skada samtidigt som en annan part gör en ekonomisk vinst.

Man kan definiera interna och externa bedrägerier, beroende på om den som utför själva handlingen är en anställd/konsult (s.k. insider) eller en utomstående person.

Kategori
Fysiskt hot, tekniskt hot, kriminellt hot

Orsak/Aktör
Kriminella, organiserad brottslighet, insider

Exempel
- Strömstölder. Attack mot, eller manipulation av, automatiserad elmätare
- Strömstölder. Attack mot, eller manipulation av, analog elmätare
- Falska elektroniska fakturor

Exempel på potentiella konsekvenser
- Felaktig debiteringsunderlag, då elmätare blivit manipulerad
- Felaktig debiteringsunderlag, då insamlingsutrustning kopplad mot elmätare blivit manipulerad
- Felaktig debiteringsunderlag, då kunduppgifter och abonnentuppgifter blivit manipulerade

Se också
6.8.2

Referenser
SS-ISO/IEC 27002:2005 kap 4.2 ”Behandling av säkerhetsrisker”

6.8.2 Förskingring

Beskrivning
Brott där en person fått förtroende att förvalta annans egendom i besittning, men tillägnar sig den själv för egen vinnings skull.

Kategori
Fysiskt hot, kriminellt hot

Orsak/Aktör
Kriminella, organiserad brottslighet, insider

Exempel

- Interna som gör beställningar som inte är ämnade för företaget[2]
- Intern personal som även är kund hos företaget men som i sin anställning får tillgång till system där man kan manipulera information om sitt eget kundunderlag
- Intern personal som för vänner, bekanta eller andra som är kund hos företaget ändrar i system där man kan manipulera information om dessas kundunderlag

Exempel på potentiella konsekvenser

- Förfalskade beställningar
- Förfalskade räkningar

Se också
6.8.1

Referenser
SS-ISO/IEC 27002:2005 kap 4.2 ”Behandling av säkerhetsrisker”

[2] http://na.se/nyheter/sverige/1.1824606-haktade-for-forskingring-mot-bahnhof

6.8.3 Utpressning

Beskrivning
Försök att tvinga någon till handling eller underlåtenhet genom att hota med våld, sabotage, skandal eller liknande. Utpressning är ett brott enligt Brottsbalken 9 kap 4§.
. .
Kategori
Fysiskt hot, logiskt hot, kriminellt hot

Orsak/Aktör
Kriminella, organiserad brottslighet, insider

Exempel

- Hot om angrepp mot IT-infrastruktur
- Hot om angrepp mot el-infrastruktur
- Stöld av information, exempelvis kunddatabaser och affärsplaner, vilka hotas släppas om inte pengar ges
- Utspärrning eller blockering av åtkomst till informationsresurser, tex obehörig kryptering av databaser, vars krypteringsnyckel återfås mot pengar[3]

Exempel på potentiella konsekvenser

- IT-system som styr och kontrollerar elproduktion blir angripna som ett sätt att visa att en angripare har styrmöjlighet över den fysiska processen för elproduktion
- IT-system som styr och kontrollerar eldistribution blir angripna som ett sätt att visa att en angripare har styrmöjlighet över den fysiska processen för eldistribution
- IT-system som styr och kontrollerar elhandel blir angripna som ett sätt att visa att en angripare har styrmöjlighet över den logiska processen för elhandel

Se också
6.8.1, 6.8.2

Referenser
SS-ISO/IEC 27002:2005 kap 4.2 ”Behandling av säkerhetsrisker”

[3] http://www.smh.com.au/it-pro/security-it/hackers-hold-australian-medical-records-to-ransom-20121210-2b4xe.html

6.8.4 Stöld av fysiska resurser

Beskrivning
Stöld är då någon eller några utan tillåtelse tillförskaffar sig fysiska föremål eller fysiska pengar som tillhör någon annan.

Kategori
Fysiskt hot, kriminellt hot

Orsak/Aktör
Kriminella, organiserad brottslighet, insider

Exempel
- Kopparstöld. Stöld av kablage
- Stöld av el-utrustning, exempelvis transformatorer
- Stöld av IT-utrustning som används för att styra och kontrollera de fysiska processerna (elproduktion, eldistribution, stöd- och försörjningssystem)
- Stöld av kringutrustning, verktyg eller hjälpmedel såsom transformatorolja

Exempel på potentiella konsekvenser
- Elavbrott som en följd av kopparstöld
- Kommunikationsavbrott för industriella informations- och styrsystem som en följd av kopparstöld i kommunikationsledningar

Se också
6.8.5

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.1 ”Placering och skydd av utrustning”

6.8.5 Stöld av elektroniska digitala resurser

Beskrivning
Stöld är då någon eller några utan tillåtelse tillförskaffar sig digitala föremål eller digitala pengar som tillhör någon annan

Kategori
Logiskt hot, kriminellt hot

Orsak/Aktör
Kriminella, organiserad brottslighet, insider

Exempel

- Stöld av CPU-tid .
- Stöld av kommunikationskapacitet
- Stöld av elektroniska betalningsmedel .
- Stöld av lagringsplats

Exempel på potentiella konsekvenser

- Driftstörningar på grund av att systemet som blivit drabbat inte har tillräcklig kapacitet gällande CPU-prestanda
- Driftstörningar på grund av att systemet som blivit drabbat inte har tillräcklig kapacitet gällande lagringskapacitet

Se också
6.8.4

Referenser

6.8.6 Spionage

Beskrivning
En individ, företag eller en regering försöker komma över, eller har kommit över, information som får betraktas som hemlig och konfidentiell utan tillstånd från den som besitter informationen

Kategori
Tekniskt hot, administrativt hot, kriminellt hot

Orsak/Aktör
Antagonist, statsaktör

Exempel

- Elektroniskt företagsspionage via IT-komponenter
- Stöld av fysisk dokumentation .
- Stöld av digital dokumentation .

Exempel på potentiella konsekvenser

- Obehöriga får åtkomst till information som rör rikets säkerhet
- Obehöriga får åtkomst till information som rör påverkar möjligheten att skydda anläggningar mot terroristangrepp
- Obehöriga får åtkomst till information som handlar om anläggningar och driftsinformation
- Obehöriga stjäl forskningsinformation rörande typer av anläggningar, utrustning eller processer som är nya och inte tidigare kända utanför den egna organisationen.

Se också

Referenser

6.8.7 Trolöshet mot huvudman

Beskrivning
Ett brott enligt svensk rätt vilket regleras i brottsbalken 10 kap 5§. Brottet i sig innebär att man missbrukar sin förtroendeställning gentemot någon annan då man fått i uppgift att sköta ekonomiska angelägenheter, kvalificerad teknisk uppgift eller ska övervaka skötseln av sådan uppgift och detta missbruk innebär skada för den s.k. huvudmannen, exempelvis arbetsgivaren .

Kategori
Administrativt hot, kriminellt hot

Orsak/Aktör
Intern personal

Exempel

- Tjänsteman inom företaget begår handlingar som är trolöshet mot huvudman i samband med en entreprenadupphandling
- Tjänsteman inom företaget begår handlingar som är trolöshet mot huvudman i samband upphandling av ett nytt IT-system
- Tjänsteman inom företaget begår handlingar som är trolöshet mot huvudman i samband upphandling av byggnation

Se också

Referenser
Brottsbalken 10 kap 5§.

6.8.8 Upphovsrättsbrott

Beskrivning
Upphovsrättsbrott kan enkelt beskrivas som kopiering av programvara eller information utan tillstånd. .

Kategori
kriminellt hot

Orsak/Aktör
Meningsmotståndare, aktivister, kriminella

Exempel

- Kopiering av programvara
- Egen personal utför installation av kopierad programvara
- Tredjepartspersona har utfört installation av kopierad programvara
- Egen personal laddar ner och förvarar upphovsrättsskyddad musik på en arbetsplats
- Egen personal laddar ner och förvarar upphovsrättsskyddad film på en arbetsplats

Exempel på potentiella konsekvenser

- Systemkomponenter tas i förvar i samband med en licensrevision
- Personal misstänkliggörs i samband med att filer med musik och film hittas på en intern server
- Programvara slutar att fungera på grund av att den inte är korrekt licensierad

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 6.1.5 ”Konfidentialitetsavtal”

6.8.9 Brott mot lagen om elektronisk kommunikation

Beskrivning
Lag (2003:389) om Elektronisk Kommunikation , ofta kallad LEK. LEK är skapades en teknikneutral lagstiftning för alla typer av elektroniska kommunikationsnät och kommunikationsformer

Kategori
kriminellt hot

Orsak/Aktör
Meningsmotståndare, aktivister, kriminella

Exempel

- Företaget meddelar inte att man sätter s.k. kakor på sin webbplats
- Företaget bryter mot anmälningsplikt för de nät de skapat som kräver anmälningsplikt
- Företaget använder sig av viss typ av utrustning som fungerar som störsändare

Se också

Referenser
Lag (2003:389) om elektronisk kommunikation

6.8.10 Brott mot lagen om ansvar för elektroniska anslagstavlor

Beskrivning
Sedan i slutet av 90-talet finns det en lag kallad Lag (1998:112) om ansvar för elektroniska anslagstavlor[4] som omfattar elektroniska tjänster som förmedlar meddelanden. Avsikten med lagen är att fastställa det ansvar som finns för den som tillhandahåller tjänsten, och att dennes ansvar är att hålla uppsikt över anslagstavlan och ta bort vissa typer av meddelanden, exempelvis de som är hets mot folkgrupp, gör intrång i upphovsrätt, är olaga våldsskildring, med mera.

Kategori
kriminellt hot

Orsak/Aktör
Meningsmotståndare, aktivister, kriminella

Exempel

- Att vissa meddelanden i elektroniska anslagstavlor, i form av chattar, inte tas bort
- Att vissa meddelanden i elektroniska anslagstavlor, i form av kommentarsfält, inte tas bort

Exempel på potentiella konsekvenser

- En tjänst som företaget har skapat måste stänga ner på grund av brott mot lagen o m ansvar för elektroniska anslagstavlor
- En av företagets anställda hålls ansvarig för att en tjänst som företaget har skapat innehåller meddelanden som måste tas bort enligt lagen o m ansvar för elektroniska anslagstavlor

Se också

Referenser
Lag (1998:112) om ansvar för elektroniska anslagstavlor

[4] I dagsläget måste man här även inkludera sådana tekniker som finns inom sociala medier, såsom twitter, facebook, med mera

6.8.11 Förtal

Beskrivning
Det är ett brott att sprida kränkande uppgifter om enstaka personer eller folkgrupp. Spridning av kränkande information mot en organisation är i lagens mening inte Förtal, men kan ändå med betydande konsekvenser. Oftast måste en förtalad själv väcka talan, för vissa speciella fall kan även en åklagare väcka talan

Kategori
kriminellt hot, civilrättsliga hot

Orsak/Aktör
Meningsmotståndare, aktivister, kriminella

Exempel

- En anställd förtalar en annan person på företaget i elektroniska sociala medier
- En anställd förtalar en annan person utanför företaget i elektroniska sociala medier
- En extern person förtalar en person på företaget i elektroniska sociala medier, som en följd av det arbete personen gör på företaget

Se också

Referenser
SS-ISO/IEC 27002:2005 kap 9.2.1 ”Placering och skydd av utrustning”

6.9 Indirekta hot

Hot som inte direkt drabbat den egna organisationen, utan kanske drabbat en aktör inom branschen eller någon som använder samma typ av utrustning eller teknik.

Ett exempel är från Stuxnetincidenten. Det var en riktad attack med skadlig kod som slog mot Siemens utrustning och programvara. Andra organisationer än den som den ursprungliga attacken var riktat mot fick vidta bl.a. nedanstående åtgärder

- Hantera mediakontakter och frågor från allmänhet och myndigheter rörande frågan ifall de blivit drabbade av Stuxnet
- Genomföra en intern utredning för att se om den egna organisationen i delar blivit drabbad, eftersom Stuxnet fick en spridning utanför den ursprungliga organisationen som attackerades

6.9.1 Indirekt information om sårbarhet i produkt/teknologi som används inom den egna organisationen

Beskrivning
Den egna organisationen har produktionssatt IT-system och IT-lösningar som innehåller kända säkerhetsproblem och säkerhetshål. Dessa hål har inte åtgärdats av någon anledning, utan finns latent kvar i systemet.

Det blir känt utanför organisationen att man använder ”den sårbara produkt X”, vilket leder till att

- Media ställer frågor om detta
- Möjliga angripare kan fundera på att testa ifall man kan nyttja dessa hål

Kategori
Tekniskt hot, administrativt hot

Orsak/Aktör
Extern aktör, aktör på insidan

Exempel

- Man använder sig av operativsystem som innehåller kända säkerhetsbrister
- Man använder sig av applikationer som innehåller kända säkerhetsbrister
- Man använder infrastrukturutrustning på nätverket som har kända säkerhetsluckor
- Man använder sig av komponenter på el-infrastruktursidan, såsom RTU, PLC eller IED, som innehåller programvara som har kända säkerhetshål

Exempel på potentiella konsekvenser

- Möjlighet att ta sig in i infrastrukturutrustning och ändra inställningar på nätverksöverföringar, störa datakommunikationen
- Möjlighet att ta sig in i komponenter och enskilda objekt på ICS-sidan och där komma åt RTU, PLC, IED eller liknande och där ändra inställningar eller avaktivera vissa funktioner som behövs

Se också
0

Referenser

6.10 Branschproblem

Detta kapitel beskriver ett antal olika hot som uppstår någon annan stans än i den egna organisationen, eller drabbar någon annan i samma bransch, men som ändå kan få konsekvenser eller påverkan på organisationen.

6.10.1 IT-incident inom annat bolag i branschen leder till granskningar, ryktesspridning och misstro mot den egna organisationen eller mot branschen som helhet

Beskrivning
Ett IT-problem uppstår hos ett annat företag eller annan organisation, vilket får medial återspegling och i förlängningen även myndigheters intresse. Denna händelse kan leda till grundade eller ogrundade misstankar mot andra organisationers hanterande av information eller deras IT-system.

Kategori
Tekniska hot

Orsak/Aktör
Okänd extern part

Exempel
- Om någon upptäcker och publicerar säkerhetshål, om information om en IT-incident läcker ut, eller en svaghet i ett system som används inom elbranschen, så kan detta leda till följdhändelser och följdeffekter.
    - Detta gäller särskilt för ny, IT-baserad, teknik såsom *SmartGrid* eller aktiva elmätare (*smarta elmätare*).
    - Detta gäller också för branschspecifika IT-lösningar
    - Detta kan gälla för vissa sektorer, exempelvis kärnkraftssektorn
- Om en organisation blir utsatt för ett intrång eller annan IT-incident kan den händelsen få sekundäreffekter eller leda till frågeställningar om möjliga följdverkningar tack vare olika typer av integration, datautbyte med andra organisationer

Exempel på potentiella konsekvenser
- Obehöriga försöker göra intrång eller utföra otillåtna ”säkerhetstester” för att se ifall organisationens egen utrustning innehåller samma typ av säkerhetshål
- Det kan spridas ogrundade rykten
- Det kan leda till missförstånd och vanföreställningar

Se också
6.10.2

Referenser
ISO/IEC 27019:2013 kap 6.1.6 ”Contact with authorities”

6.10.2 Allmän kunskap om sårbarhet i produkt/teknologi som används inom den egna organisationen

Beskrivning
Den egna organisationen har produktionssatt IT-system och IT-lösningar som innehåller kända säkerhetsproblem och säkerhetshål. Dessa hål har inte åtgärdats av någon anledning utan finns latent kvar i systemet.

Kategori
Tekniskt hot, administrativt hot

Orsak/Aktör
Extern aktör, aktör på insidan

Exempel
- Man använder sig av operativsystem som innehåller kända säkerhetsbrister
- Man använder sig av applikationer som innehåller kända säkerhetsbrister
- Man använder infrastrukturutrustning på nätverket som har kända säkerhetsluckor
- Man använder sig av komponenter på el-infrastruktursidan, såsom RTU, PLC eller IED, som innehåller programvara som har kända säkerhetshål

Exempel på potentiella konsekvenser
- Möjlighet att ta sig in i infrastrukturutrustning och ändra inställningar på nätverksöverföringar, störa datakommunikationen
- Möjlighet att ta sig in i komponenter och enskilda objekt på ICS-sidan och där komma åt RTU, PLC, IED eller liknande och där ändra inställningar eller avaktivera vissa funktioner som behövs

Se också
0

Referenser

7 Övriga typer av hot

Denna kategori inkluderar

- *generella hot* som slår över flera kategorier
- hot som inte låter sig placera sig i en traditionell kategori

7.1 Globala sjukdomar och smittspridning

Detta kapitel beskriver hot som bygger på sjukdom och spridning av smitta, vilket kan få konsekvenser för personal, att funktioner inte kan bemannas, etc.

7.1.1 Epidemi

Beskrivning
En infektionssjukdom som sprids och drabbar en stor andel av befolkningen i ett land.

Smitta eller smittspridning kan leda till att arbetskraft inte kan ta sig till jobbet på grund av att kollektivtrafiken inte fungerar. Det kan också leda till att det inte går att bemanna maskiner, driftcentraler, kontrollrum, eller att fältpersonal inte finns tillgängliga på grund av egen eller annans sjukdom. Detta kan i sin tur leda till onormalt högt utnyttjande av fjärranslutningsmöjligheter till arbetsplatsen. Vissa system har redan fjärråtkomstmöjligheter, medan andra av säkerhetsskäl saknar uppkoppling mot omvärlden.

Kategori
Fysiskt hot

Orsak/Aktör
Smittsam sjukdom

Exempel

- Personal saknas på grund av att de är insjuknade
- Nyckelpersonal saknas på grund av att de är insjuknade
- Personal saknas på grund av att de är rädda att bli smittade i folksamlingar på arbetet eller under färd till/från arbete
- Nyckelpersonal saknas på grund av att de är rädda att bli smittade i folksamlingar på arbetet eller under färd till/från arbete

Exempel på potentiella konsekvenser

- Svårighet med bemanning i driftcentral eller kontrollrum
- Svårighet med bemanning i linjeverksamhet för drift- och underhåll av elnätet
- Svårighet med bemanning i linjeverksamhet för drift- och underhåll av IT-system

Se också
7.1.2

Referenser

7.1.2 Pandemi

Beskrivning
En infektionssjukdom som sprids över hela världen och drabbar en stor andel av befolkningen i varje land.

Smitta eller smittspridning kan leda till att arbetskraft inte kan ta sig till jobbet på grund av att kollektivtrafiken inte fungerar. Det kan också leda till att det inte går att bemanna maskiner, driftcentraler, kontrollrum, eller att fältpersonal inte finns tillgängliga på grund av egen eller annans sjukdom. Detta kan i sin tur leda till onormalt högt utnyttjande av fjärranslutningsmöjligheter till arbetsplatsen. Vissa system har redan fjärråtkomstmöjligheter, medan andra av säkerhetsskäl saknar uppkoppling mot omvärlden.

Kategori
Fysiskt hot

Orsak/Aktör
Smittsam sjukdom

Exempel
- Personal saknas på grund av att de är insjuknade
- Nyckelpersonal saknas på grund av att de är insjuknade
- Personal saknas på grund av att de är rädda att bli smittade i folksamlingar på arbetet eller under färd till/från arbete
- Nyckelpersonal saknas på grund av att de är rädda att bli smittade i folksamlingar på arbetet eller under färd till/från arbete

Exempel på potentiella konsekvenser
- Svårighet med bemanning i driftcentral eller kontrollrum
- Svårighet med bemanning i linjeverksamhet för drift- och underhåll av elnätet
- Svårighet med bemanning i linjeverksamhet för drift- och underhåll av IT-system

Se också
7.1.1

Referenser

7.2 Juridiska spörsmål

Underlåtelse att följa lagar som man inte anser vara relevanta eller uppdaterade för att följa det moderna, IT-baserade arbetssättet

- Lag (1993:1792) om skydd av landskapsinformation
- Personuppgiftslag (1998:204)
- Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk (Upphovsrättslag)
- Lag om skydd av företagshemligheter
- Ellag (1997:857) och Elförordning (2013:208)

7.2.1 Oklart lagrum

Beskrivning
Det uppstår oklarheter om lagrum, vilka juridiska krav som gäller eller vilket lands lagstiftning som gäller för någon viss typ av IT-användning, hantering av information eller liknande. .

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av processer, Avsaknad av rutiner, kompetensbrist

Exempel
- Ett IT-system finns placerat i ett visst land, dess användare finns i ett annat land, dess systemadministratörer finns i ett tredje land. Det uppstår frågor rörande obehörig åtkomst till informationen – man misstänker att någon användare har kommit åt information.
- Vid projektarbete där ett nytt system skall införas så väljer man mellan egen drift och att köpa in funktionen som en tjänst åtkomlig via Internet. Det är oklart var tjänsteleverantören har sin IT placerad. Projektet tar inte hänsyn till lagrum när lösningen implementeras
-

Se också
7.2.3, 7.2.4, 7.2.5

Referenser
SS-ISO/IEC 27002:2005 kap 15.1.1 ”Identifiering av tillämplig lagstiftning”
SS-ISO/IEC 27002:2005 kap 15.1.5 ”Förhindrande av missbruk av informationsbehandlingsresurser”

7.2.2 Hantering av personuppgifter

Beskrivning
En vanligt förekommande uppgift inom de flesta större organisationer är att hantera information om kunder, personal, eller andra personer som organisationen har någon relation till. Denna information är ofta vad man kan beteckna som personuppgifter.

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av processer, Avsaknad av rutiner, kompetensbrist

Exempel
- Underlåtande att utse personuppgiftsombud
- Inte införa adekvata tekniska skydd av system och applikationer som hanterar personuppgifterna
- Omedveten export eller utförsel av personuppgifter utanför EU
- Medveten export eller utförsel av personuppgifter utanför EU

Exempel på potentiella konsekvenser
- Lagöverträdelser av nationella lagar
- Överträdelser av utfästelser mot tredje part, ofta kunder, vilka man lovat en viss hantering av personuppgifterna i den integritets- och personuppgiftspolicy man har publicerat
- Informationsläckage av vanliga personuppgifter, vilket leder till att stora mängder personuppgifter ur kundregister görs allmänt tillgängliga
- Informationsläckage av personuppgifter för personer med skyddad identitet, vilket leder till att mängder personuppgifter ur kundregister görs allmänt tillgängliga. De personer vars exempelvis adress- och kontaktuppgifter har röjts får problem och måste byta bostad, telefonnummer med mera.

Se också
5.8.1, 5.8.2, 7.2.3, 7.2.4, 7.2.5

Referenser
SS-ISO/IEC 27002:2005 kap 15.1.1 ”Identifiering av tillämplig lagstiftning”
SS-ISO/IEC 27002:2005 kap 15.1.4 ”Skydd av personuppgifter”

7.2.3 Felaktig hantering av landskapsinformation

Beskrivning
Landskapsinformation kan behöva hanteras enligt de hanterandekrav som upprättats av tillsynsmyndigheten och i enlighet med det tillstånd som man erhållit från Lantmäteriet.

Kategori
Administrativt hot

Orsak/Aktör
Handhavandefel, felaktig hantering, okunskap

Exempel
- Landskapsinformation sparas i system utan att dessa har fullgott skydd
- Landskapsinformation sparas i system utan att organisationen har tillstånd att framställa eller sprida landskapsinformationen

Exempel på potentiella konsekvenser
- Lagöverträdelser av nationella lagar
- Överträdelse mot de tillstånd och hanterandekrav man erhållit från ansvarig myndighet
- Landskapsinformation innehållande information om installationer, anläggningar, mm blir stulen. Information om känsliga anläggningar blir allmänt röjda då den publiceras på Internet.

Se också
7.2.4, 7.2.5

Referenser
SS-ISO/IEC 27002:2005 kap 15.1.1 ”Identifiering av tillämplig lagstiftning”
ISO/IEC 27019:2013 kap 6.1.6 ”Contact with authorities”

7.2.4 Upphovsrättsbrott

Beskrivning
Material som används inom organisationen, av organisationens anställda, ägs av någon annan person eller organisation och vår organisation eller våra anställda har inte ägande-, förfogande- eller nyttjanderätt till informationen. Genom att nyttja informationen, exempelvis en text, en bild, en film eller en ljudupptagning, så begår vi ett upphovsrättsbrott .

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av processer, Avsaknad av rutiner, kompetensbrist

Exempel
- Information i form av bilder har laddats ner från Internet från olika webbsidor. Dessa bilder används utan upphovsmannens tillåtelse i marknadsföringen för bolaget i trycksaker, på webben, med mera
- Medarbetare inom bolaget laddar ner piratkopierade filmer till en av företagets datorer. Filerna ligger kvar på datorn efter det att användaren laddat ner dem

Se också
7.2.3, 7.2.4, 7.2.5

Referenser
SS-ISO/IEC 27002:2005 kap 15.1.1 ”Identifiering av tillämplig lagstiftning”
SS-ISO/IEC 27002:2005 kap 15.1.2 ”Immaterialrätt”
SS-ISO/IEC 27002:2005 kap 15.1.5 ”Förhindrande av missbruk av informationsbehandlingsresurser”

7.2.5 Brott mot lagen om skydd av företagshemligheter

Beskrivning
Personal inom bolaget utför handlingar mot bolaget som innebär brott mot lag (1990:409) om skydd av företagshemligheter ..

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av processer, Avsaknad av rutiner, kompetensbrist, uppsåtliga lagöverträdelser, spionage

Exempel
- Personal inom bolaget utför stöld av forskningsresultat
- Personal inom bolaget utför Stöld av kundinformation
- Personal inom bolaget utför stöld av affärsplaner

Se också
7.2.3, 7.2.4

Referenser
SS-ISO/IEC 27002:2005 kap 15.1.1 ”Identifiering av tillämplig lagstiftning”

7.2.6 Brott mot ellagen eller elförordningen

Beskrivning
Enligt Ellag (1997:857) och Elförordning (2013:208) finns det ett antal skyldigheter för den som bedriver elverksamhet. Av någon orsak så följs inte ellagen eller elförordningen av organisationen. .

Kategori
Administrativt hot

Orsak/Aktör
Avsaknad av processer, Avsaknad av rutiner, kompetensbrist, felaktigt implementerade lösningar

Exempel
- De skyldigheter att mäta och beräkna överförd el utförs inte korrekt, varpå felaktiga kostnader framräknas och överförs på kund
- Felaktiga administrativa rutiner gör att man inte överför information om ansökningar rörande nätkoncession till nätmyndigheten korrekt
- Risk- och sårbarhetsanalyser eller åtgärdsplaner biställs inte nätmyndigheten i den form eller under de former som nätmyndigheten kräver

Se också
7.2.3, 7.2.4

Referenser
SS-ISO/IEC 27002:2005 kap 15.1.1 ”Identifiering av tillämplig lagstiftning”

8 Ordlista

Administrativt hot hot mot administrativa rutiner och organisatoriska lösningar.

Aktivt hot Ett hot som anses existera och är aktivt mot verksamheten.

Aktör Den person, de personer, eller den stat, som agerar i ett hot, som är angriparen eller angriparna. Jämför med naturkatastrofer eller infrastrukturellt betingade sårbarheter.

Anläggning En fast byggnadskonstruktion på land eller i vatten. I anläggning inkluderas infrastruktur för styrnings- och övervakningssystem och talkommunikationer

Antagonist motståndare. Ofta i bemärkelsen att det finns personer inblandade som styr och kontrollerar händelser och händelsekedjor

Antagonistisk attack Ett angrepp i vilken en motståndare i form av en eller flera personer medverkar.

Användare Person som nyttjar en *informationstillgång,* exempelvis en dator eller ett program.

Avlyssning Möjlighet för obehörig part att ta del av kommunikation och förmedlad information. Se vidare aktiv och passiv avlyssning.

Avsiktligt hot är ett hot som iscensätts eller realiseras med vett och vilja.

Bakdörrar i programvara

Behörighet Användarrättighet att nyttja *informationstillgång* på specificerat sätt

Botnet nätverk av infekterade datorer med installerad skadlig kod som via utskickade kommandon kan utföra specialla och samordnade åtgärder. Kallas ibland på svenska även för zombienät

Brandvägg Datatekniskt skydd som på nätverksnivå separerar två eller fler nätverk från varandra.

Chipping Att på låg nivå införa dolda funktioner i hårdvara som på kommando eller givna förutsättningar kan ändra hårdvarufunktionalitet.

Certifiering .formellt fastställande av resultat, från exempelvis en evaluering av ett system.

Certifikat Se elektroniska certifikat

CSMS .Se Cyber Security Management System

Cyber Security Management System. Se Ledningssystem för cybersäkerhet

Datorvirus .Se skadlig kod

Dimensionerande hotbild En allmän beskrivning av en tänkt hotaktörs förmåga och tillvägagångssätt. Kallas också ibland för dimensionerande hotbeskrivning.

DNS Domain name system, samlingsnamn för det system och de metoder som används för att översätta mellan namn som är förståeliga för människor (t.ex. www.dn.se) och de nummer som är bättre att arbeta med för datorer.

DNSspoofing Attack mot DNS som avser att påverka trafiken så att den når en falsk adress istället för den adress som offret tror sig skall nå.

DoS-attack (eng. Denial of Service) Se överlastningsattack

DDoS-attack (eng. Distributed Denial of Service) Se överlastningsattack

Driftcentral Fast eller rörlig central för drift- och övervakning av produktionsanläggningar, stationer och/eller elnät

Driftkommunikationsnät kommunikationsnät för inhämtning av driftdata och styrning av anläggningar och/eller enskilda objekt.

Driftstörning Störning som kan påverka produktionsfärdighet och driftstatus hos en verksamhet

Dynamiska hot hot som kan ha både negativa och positiva konsekvenser

Elberedskap planering, ledning och samordning elförsörjningens resurser för att undvika elbrist samt tillgodose samhällets behov av el i olika sammanhang inklusive i kris och krig.

Elektroniskt certifikat digital information som knyter ihop information med en viss utställare eller utgivare

Elektronisk signatur uppgifter i elektroniskt format som är fogade till, eller logiskt knutna till, andra elektroniska uppgifter och som används som en metod för att autentisera dessa uppgifter

Elnät En nätkoncessionsinnehavares sammankopplade elektriska anläggningar för överföring av el som innehas med nätkoncession för linje eller med nätkoncession för område.

Extremt rymdväder Ändringar och händelser i solens heta områden, koronan, som kan påverka förhållanden på jorden.

Fjärrangrepp Angrepp som sker på distans, ofta via kopplande datanätverk, där angriparen från en eller flera datorer kan ge sig på andra anslutna datorer.

Fjärrstyrning Distansåtkomst till utrustning på vilket sätt som medför styrning och kontroll av utrustningen. Behörig eller obehörig fjärrstyrning kan vara antingen via legitim och medvetet installerad och använd fjärrstyrningsprogramvara eller via bakdörrar som antingen ursprungligen lämnats där av tillverkarna eller som senare installerats av någon som angripit utrustningen.

Fjärråtkomst Anslutning på distans, ofta via kopplande datanätverk, där användaren från en eller flera datorer kan nå andra anslutna datorer. Används ofta för support, diagnostik och underhåll av leverantörer eller personal som har jour.

Forcering av krypto Analys av ett kryptosystem och dess kryptotexter, eventuellt med viss tillgång till klartexter för att utröna kryptonyckel eller klartext

Forensisk undersökning Teknisk post-mortem analys av en inträffad händelse. I detta fall så är undersökningen inriktad mot IT-system och IT-händelser

Fysiska hot Hot som kan påverka, eller resultera i konsekvenser, saker i den fysisk världen

Fysiskt skydd omgivande skydd av IT-system och dess resurser som skyddar mot direkt fysisk åtkomst av obehörig.

GIS Geografiska informationssystem. IT-lösningar som behandlar och presenterar landskapsdata och geografisk information.

Hemlig handling är en handling som skyddas enligt offentlighets- och sekretesslagen eller den tidigare sekretesslagen.

Hot En möjlig, oönskad händelse med negativa konsekvenser för verksamheten

Hotbedömning *En bedömning gjord av det eller de hot som föreligger*

Hotbild En uppsättning hot som bedöms föreligga mot en viss del av verksamheten

Hot mot rikets säkerhet Hot som anses riskera rikets fortsatta existens och dess grundläggande institutioner samt viktiga principer som grundlagen bygger på.

Händelse Används ibland som synonym till hot

ICS *eng. Industrial Control System.* En vanligt förekommande förkortning som används för att beteckna industriella kontrollsystem

ICT *eng. Information and Communication Technology.* En vanligt förekommande förkortning som används för att beteckna industriella kontrollsystem

IKT Förkortning för informations- och kommunikationsteknik (*eng. Information and Communication Technology, ICT*). Vanligt förekommande term för de sammansatta IT och kommunikationsområdena.

Identitetsstöld stöld av identitetsuppgifter i syfte att senare sälja, nyttja eller missbruka dessa uppgifter på nätet eller i verkligheten.

Incident I dessa sammanhang avser ordet oftast ”IT-incident” då incidenten involverar informationsteknik i någon utformning

Incidenthantering Hanteringen, inklusive utredning, av en IT-incident och de konsekvenser denna incident medfört

Industriella styr- och informationssystem

Information Ett uttryck av kunskap eller budskap i konkret form samt innehåller ofta, men inte alltid, en samling fakta.

Informationsklassning Klassning av en organisations informationstillgångar. Är en grundläggande aktivitet och en förutsättning för att lyckas med andra säkerhetsaktiviteter och för att skapa en effektiv informationssäkerhet.

Informationsläckage Hotet att information lämnas ut av behöriga som medvetet överträder sina befogenheter och det förtroende som de tilldelats. Kan också vara automatiskt uthämtning eller utlämning, av ett program eller ett system som är felaktigt.

Informationstillgång en organisations eller persons informationsrelaterade tillgångar såsom dokument, strukturerad elektronisk och digital data, tjänster, datorer, applikationer, med mera.

Informationsstöld Stöld av informationstillgångar

Informationssäkerhet bevarande av konfidentialitet (sekretess), riktighet och tillgänglighet hos information. Andra egenskaper såsom autenticitet, spårbarhet, oavvislighet och tillförlitlighet inbegrips vanligen också.

Informationssäkerhetsincident enskild eller en serie oönskade eller oväntade informationssäkerhetshändelser vilka med stor sannolikhet kan äventyra verksamheten och hota informationssäkerheten

Informationsägare person som har det övergripande ansvaret för informationen i en funktion.

Intrång Oönskad interaktion med system i strid med systemets policy eller som kan medföra förändring, störning eller skada. Det kan förekomma både fysiskt eller logiskt intrång.

Intrångsdetekteringssystem Automatiserad detektion och analys av händelser som kan uppfattas som säkerhetsöverträdelser, intrångsförsök eller liknande.

Insiderhot Hot som har sitt ursprung inom den egna organisationen.

IT Förkortning för Informationsteknologi (*eng. Information Technology, IT*).. Se IKT

IT-sabotage Angrepp, eller hot om angrepp, med avsikt att förstöra system, infrastruktur eller information

IT-säkerhet IT-systems och dess kringutrustning och kringtjänsters förmåga att hindra obehörig hantering, störning, åtkomst, förändring.

Janusattack Se mannen-i-mitten-attack

Keylogger Program- eller hårdvara som obehörigt spelar in knapptryckningar på tangentbordet.

Konsekvens Resultat av en händelse med negativ inverkan

Kriminella hot Hot som har sitt ursprung i en kriminell handling eller som syftar till att begå en kriminell gärning.

Kryptering Omvandling av klartext till kryptotext medelst ett kryptosystem och en aktuell kryptonyckel i syfte att förhindra obehörig åtkomst till konfidentiell information.

Ledningssystem för cybersäkerhet

Styrning av säkerhetarbetet rörande cybertillgångar. Definieras i standarden IEC 62443.

Ledningssystem för informationssäkerhet Delmängd av en organisations ledningssystem som övergripande styr verksamhetens informations-säkerhetsarbete. Arbetet innefattar införande, upprätthållande, underhåll och övervakning, granskning och förbättring av informationssäkerheten inom organisationen. Det finns internationell standard för organisationers ledningssystem för informationssäkerhet kallad SS-ISO/IEC 27000

LIS Se ledningssystem för informationssäkerhet

Logg Insamlad information i syfte att skapa *spårbarhet* innefattande tidpunkter, händelser, aktiviteter, användare, med mera.

Logiska hot Hot som kan påverka, eller resultera i konsekvenser, saker i den logiska, digitala världen

Logisk bomb Skadlig kod innefattande en dold funktion i ett program eller programsystem som under vissa villkor utlöser en oönskad aktivitet

Mannen-i-mitten-attack . En obehörig tredje part sitter mellan två kommunicerande enheter och fångar upp, och möjligtvis även förändrar, överförd information mellan de två enheterna. Attacken kan exempelvis utföras på ett datornätverk, mellan kortläsare och dator, mellan tangentbord och dator, med mera. Attacken är även kallad janusattack

Maskar Ett program som mångfaldigar sig över ett nätverk

MITM Se Mannen-i-mitten-attack.

Oavsiktligt hot Hot som existerar trots att illasinnad avsikt saknas.

Oavvislighet Ett skyddsmål att en handling inte i efterhand skall kunna förnekas av utföraren.

Operativa risker risken för förluster till följd av icke ändamålsenliga eller misslyckade processer, mänskliga fel, felaktiga system eller externa händelser

Organisatorisk hot Hot av organisatorisk natur eller som negativt påverkar organisationen.

Passivt hot Hot för obehörig läsning eller avlyssning

Patch Programuppdatering för att fixa enstaka eller fåtal fel i programkod. Det finns såväl källkodspatchar som binärpatchar som utför rättningar i ursprungskällkoden respektive i redan kompilerad och installerad programvara. Att inte installera en patch medför att man har en kvarvarande risk då programfelet, exempelvis ett säkerhetsrelaterat programfel, är latent och möjligt att missbruka.

Personuppgift All slags information som direkt eller indirekt kan knytas till en fysisk person som är i livet räknas enligt personuppgiftslagen som personuppgifter.

Phishing En typ av attack som via e-post söker locka mottagaren att besöka en förfalskad webbplats, varvid känsliga uppgifter kan stjälas.

Policy övergripande avsikt och viljeinriktning formellt uttryckt av ledningen.

Process En samling i förväg uttänkta aktiviteter som skall användas inom en organisation varje gång organisationen skall skapa ett vist resultat, exempelvis till en kund

Processägare En roll som innebär att införa, förvalta och följa upp en process och alla dess aktiviteter.

Redundans Egenskap hos ett system eller systemkomponent för att begränsa konsekvenser av uppkomna fel.

Revision Oberoende granskning och uttalande om information eller vissa förhållanden.

Riktighet Skyddsmål att information inte förändras, vare sig obehörigen, av misstag eller på grund av en funktionsstörning.

Risk Kombination av sannolikheten för att ett givet hot realiseras och därmed uppkommande skadekostnad

Riskacceptans Hur mycket risk en organisation eller en person är villig att acceptera. Kallas ibland även riskvillighet eller riskaptit

Riskanalys Process för att identifiera verksamhetshot samt storlek och konsekvenser av de risker som relaterar till hoten.

Riskaptit Hur mycket risk en organisation eller en person är villig att acceptera. Kallas ibland även riskacceptans eller riskaptit

Riskhantering *Samordnade aktiviteter för identifiering, styrning och kontroll av risk*

Riskutvärdering Utvärdering att jämföra uppskattad risk mot en given riskbedömningsgrund för att fastställa riskens betydelse

Router Nätverksenhet som kopplar samman flera lokala datornätverk samt dirigerar datakommunikation mellan dessa nät

Routing Processen att utföra vägval i ett datornätverk

Rutin fastslagna, ofta dokumenterade, procedurer och tillvägagångssätt

Röjande signaler icke önskvärda elektromagnetiska eller akustiska signaler som alstras i informationsbehandlande utrustningar och som, om de kan tydas av obehöriga, kan bidra till att konfidentiell information röjs

Sabotage Förstörande eller skadande av egendom som har avsevärd betydelse för rikets försvar, folkförsörjning, rättsskipning eller förvaltning eller upprätthållande av allmän ordning och säkerhet i riket.

SCADA Supervisory and Control and Data Aquisition. I detta sammanhang en allmänbetydelse för industriella informations- och kontrollsystem

Sektorsmyndighet En myndighet på central nivå som av regeringen har utsetts till att ha ett särskilt ansvar inom sitt område.

Sekretess . En i IT- och informationssäkerhetssammanhang vanlig synonym är konfidentialitet.

Skada fel som uppstått eller orsakats vid ett särskilt tillfälle

Skadekostnad sammanlagt värde av ett angrepps konsekvenser

Skadlig kod Samlingsnamn för virus, maskar, logiska bomber, bakdörrar och annat som skapats med uppsåt att ha en försåtlig funktion

Skydd effekt av handlingar, rutiner och tekniska arrangemang som syftar till att minska sårbarhet

Skydd mot terrorism Begrepp som införs i säkerhetsskyddslagen om att en verksamhet skall ha skydd mot terroristbrott, vilket består i olika former av sabotage, grovt sabotage eller hot om detta.

Skyddet mot terrorism innefattar även skydd av IT-system som är centrala eller kritiska komponenter i energisystemet eller som används som centrala eller kritiska delar i fysiska eller logiska säkerhetssystem.

Skyddsobjekt är vissa byggnader, andra anläggningar, områden och andra objekt som enligt skyddsag (2010:305) kan behöva förstärkt skydd mot sabotage, terroristbrott, spioneri eller grovt rån

Spam oönskad skräppost

Spionprogram Ett program som körs på en användares dator utan dennes godkännande och som samlar in och vidarebefordrar information till en annan part.

Spearphishing Är en riktad version av en typ av attack som via e-post söker locka mottagaren att besöka en förfalskad webbplats, varvid känsliga uppgifter kan stjälas.

Spårbarhet Identifikationsmöjlighet av användare, händelser, aktiviteter på ett entydigt sätt efter det en händelse eller aktivitet har inträffat.

Station Anläggning med elektrisk utrustning för att transformera eller fördela elektrisk energi, med en eller flera transformatorer.

Styrdokument Dokument som enligt organisationens ledningssystem skall ha en formell betydelse för att styra organisationens verksamhet

Systemförvaltare En roll som har ansvaret för administration och drift av ett eller flera datorsystem

Systemägare Ett överordnande ansvar för administration och förvaltning för ett eller flera datorsystem. Ofta delegeras delar eller hela detta till en sysyemförvaltare

Switch
Nätverkskommunikationsutrustning som används för att ansluta datorutrustning och vidarebefordra nätverkspaket mellan olika infrastrukturkomponenter (routers, switchar) eller ansluten utrustning. Se även router

Sårbarhet svaghet gällande en tillgång eller grupp av tillgångar, vilken kan utnyttjas av ett eller flera hot

Säkerhetsanalys En inventering av skyddsvärda resurser kopplat till hot, risk och sårbarheter. Resultatet skall vara en konkret handlings- och åtgärdsplan

Säkerhetsarkitektur Strategiskt ramverk, byggt på en enhetlig struktur och sammanhållande principer för de säkerhetsfunktioner som finns och den säkerhetsnivå dessa skall hålla

Säkerhetschef En roll i beslutsställning som överser, styr och rådger i arbetet med säkerhet inom en organisation.

Säkerhetshändelse förändring av tillståndet hos en informationstillgång då säkerheten påverkats negativt.

Säkerhetsskyddsförordning Är en förordning kopplad till säkerhetsskyddslag. Säkerhetsskyddsförordning (1996:633) som ger bestämmelser till säkerhetsskyddslagen (1996:627)

Säkerhetsskyddslag Lag som reglerar säkerhetsskydd, d.v.s. skydd mot spioneri, sabotage och andra brott som kan hota rikets säkerhet. För mer detaljinformation se säkerhetsskyddslagen (1996:627)

Säkerhetsskyddschef Utpekad person som utövar kontroll över säkerhetsskyddet. Vid myndigheter skall säkerhetsskyddschefen vara direkt underställd myndighetens chef.

Säkerhetsåtgärd
medel för hantering av risk, innefattandes policyer, rutiner, riktlinjer, förfaranden eller organisationsstrukturer vilka kan vara av administrativ, teknisk, ledningsmässig eller juridisk karaktär

TCP/IP Arkitektur för datakommunikation över nätverk med en struktur som delas upp i lager. TCP/IP är ett allmänt förekommande samlingsnamn för en samling protokoll, där varje deltagande dator har en IP-adress.

Tekniskt hot Är av teknisk natur eller som negativt kan påverka teknik, tekniska lösningar och tekniska system.

Tekniska sårbarheter Sårbarheter som har sitt ursprung i tekniska orsaker, ofta IT-tekniska fel, exempelvis programfel, konfigurationsfel i applikationer eller system

Tillgänglighetsförlust övergång till ett tillstånd hos ett system där det inte i erforderlig utsträckning eller inom önskad till kan leverera tjänster

Tillsyn Granskning som genomförs med stöd av lag och en möjlighet för tillsynsmyndigheten att besluta om någon form av ingripande.

Tillsynsmyndighet En myndighet som utövar tillsyn över viss verksamhet.

Trojansk häst Ett datorprogram som utger sig för en sak, men som i själva verket har dold funktionalitet som lurar användare. Se även skadlig kod

Uttömmande sökning Metod i vilken man avser att utföra en genomsökning av samtliga möjliga alternativ eller kombinationer. Uttömmande sökning är ofta en vanlig metod för att testa lösenord från en stulen lösenordsdatabas. Uttömande sökning är ofta den sista metod som tas till vid exempelvis angrepp mot krypterad information.

Virtuellt lokalt nätverk . En metod för att på nivå 2 i ett nätverk göra en logisk uppdelning mellan olika nätverkadressrymder. Ofta kallat VLAN

Virtuellt privat nätverk . En metod för att utsträcka lokala nätverk över ett publikt nätverk, oftast i form av krypterade tunnlar. Ofta kallat VPN

VLAN . *(eng. Virtual Local Area Network)* Se virtuellt lokalt nätverk

VPN . *(eng. Virtual Private Network)* Se virtuellt privat nätverk

Yttre hot . . Hot som har sitt ursprung utanför organisationen

Zombie En nod i ett botnät, vilket innebär att en dator kan befallas att utföra vissa funktioner på ett givet kommando

Ö-drift Ett speciellt driftsförhållande som råder då ett elområde vid bortfall från ett

överliggande elnät, matas från ett eller flera lokala kraftverk.

Överlastningsattack Angrepp med avsikt att slå ut eller allvarligt lasta ned målet (en dator, ett nät, en funktion, mm).

Övning Träning för skicklighetskrävande uppgifter, exempelvis övning av IT-incidenthantering

9 Sakregister

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V,W

X

Y

Z

Å

Ö

10 Referenser

Offentlighets- och sekretesslag (2009:400)

Offentlighets- och sekretessförordning (2009:641)

Elberedskapslag (1997:288)

Förordning (1997:294) om elberedskap

Lag (1993:1742) om skydd för landskapsinformation

Förordning (1993:1745) om skydd för landskapsinformation

Personuppgiftslag (1998:204)

Personuppgiftsförordning (1998:1191)

Skyddslag (2010:305)

Skyddsförordning (2010:523)

Säkerhetsskyddslag (1996:627)

Säkerhetsskyddsförordningen (1996:633)

Svenska Kraftnäts Föreskrifter, SvKFS 2013:1 *”Affärsverket svenska kraftnäts föreskrifter och allmänna råd om säkerhetsskydd*”
http://www.svk.se/Global/07_Tekniska_krav/Pdf/Foreskrifter/SvKFS-2013-1-webb.pdf

Svenska Kraftnäts Föreskrifter, SvKFS 2013:2 *”Affärsverket svenska kraftnäts föreskrifter och allmänna råd om elberedskap”*
http://www.svk.se/Global/07_Tekniska_krav/Pdf/Foreskrifter/SvKFS-2013-2.pdf

BSI Threat catalogue
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.pdf?__blob=publicationFile

Reference source for threats, vulnerabilities, impacts and controls in IT risk assessment and risk management , version 1.0
http://www.enisa.europa.eu/activities/risk-management/files/deliverables/reference-source-for-threats-vulnerabilities-impacts-and-controls-in-it-risk-assessment-and-risk-management/at_download/fullReport

SIS HB 550 “Terminologi för informationssäkerhet, utgåva 3” ISBN 978-91-7162-705-6

SS-ISO/IEC 27000:2009 ”Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Översikt och terminologi”

SS-ISO/IEC 27001:2006 “Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav”

SS-ISO/IEC 27002:2005 ”Informationsteknik – Säkerhetstekniker – Riktlinjer för styrning av informationssäkerhet”

SS-ISO/IEC 27003:2010 ”Informationsteknik – Säkerhetstekniker – Vägledning för införande av ledningssystem för informationssäkerhet ”

SS-ISO/IEC 27005:2008 “ Informationsteknik – Säkerhetstekniker – Riskhantering för informationssäkerhet”

SS-ISO/IEC 27019:2013 ”Information technology — Security techniques — Information security management guidelines based on SS-ISO/IEC 27002 for process control systems specific to the energy utility industry”

SS-ISO/IEC 31000:2009 “Risk management – Principles and guidelines”

IEC 62443-1-1/TS “Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models” Edition 1.0 2009-07

IEC 62443-2-1 “Industrial communication networks – Network and system security –
Part 2-1: Establishing an industrial automation and control system security program” Edition 1.0 2010-11

IEC/TR 62443-3-1 “Industrial communication networks – Network and system security –
Part 3 1: Security technologies for industrial automation and control systems”

IEC 62443-3-3 “Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels” Edition 1.0 2013-08

OWASP Top 10
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Robust control systems Networks: How to achieve Reliable Control After Stuxnet
Ralph Langner
ISBN 978-1-60650-300-3