Vägledning om arbetet med informationssäkerhet och säkerhet

NIS-direktivet och den nya säkerhetsskyddslagen skärper kraven på företagens säkerhetsarbete. Energiföretagen följer utvecklingen och har från medlemmarna fått in frågor om hjälp i form av handledning. Läs vägledning om säkerheten här.

I grunden ska företagen i första hand vända sig till berörda myndigheter för hjälp och handledning i frågor som rör informationssäkerhet och säkerhet. Energiföretagen Sverige bistår dock medlemsföretagen genom att vägleda kring var information finns, svara på remisser och facilitera regelverksefterlevnad inom området.

Därför vill vi ge en kort vägledning kring arbetet med informationssäkerhet och säkerhet samt var det går att finna information. Vi delar in informationen i tre huvuddelar:

A) NIS-direktivet
B) Informationssäkerhet
C) Nya säkerhetsskyddslagen

Energiföretagens fortsatta arbete

Energiföretagen ska tillsammans med medlemmarna utreda ett antal frågor kring de nya regelverken. Dessa har listats och projektgrupper som ska hantera arbetet vidare formeras nu. Inom AG Säkerhet & beredskap och EBITS ska planer för arbetet tas fram.

AG Säkerhet & beredskap är en arbetsgrupp för säkerhetsansvariga i energibranschen för information och utveckling inom delar som följer av bland annat säkerhetsskyddslagen. EBITS är Energibranschens informationssäkerhetsgrupp och har ett liknande uppdrag som AG Säkerhet och beredskap har, men inom området informationssäkerhet.

Samtliga medlemsföretag i Energiföretagen Sverige är välkomna att delta i arbetet i dessa arbetsgrupper och har möjlighet att inkomma med frågor och förslag vad gäller gruppernas arbete. För kontakt med AG Säkerhet & beredskap går det bra att vända sig till gruppens samordnare Matz Tapper. EBITS samordnare är Anders Fredriksson. Kontaktuppgifter till Matz och Anders finns på Energiföretagens webbplats.

Utbildningar hösten 2019

Utöver detta samverkar Energiföretagen och de båda arbetsgrupperna regelbundet med Energimyndigheten, MSB och Svenska kraftnät. Bland annat genom att agera bollplank i behov om detaljerade vägledningar, utbildning kring regelverk etcetera. Ett exempel på detta är de av Energimyndigheten planerade utbildningarna kring NIS, hösten 2019:

- Stockholm, 2–3 september
- Göteborg, 9–10 september
- Arlanda, 11–12 september
- Umeå, 9–10 oktober
- Malmö, 14–15 oktober

Energiföretagen återkommer inom kort med mer information om innehåll samt var anmälan om deltagande kan göras. Särskild information kommer sändas ut genom nyhetsbrev och annonseras på Energiföretagens respektive Energimyndighetens webbplatser.

A) NIS-direktivet, vem omfattas och vad innebär det?

NIS-direktivet genomfördes i svensk rätt 2018 genom ”Lag (2018:1174) om informationssäkerhet för leverantörer av samhällsviktiga och digitala tjänster”.

Lagtexten finns att tillgå i sin helhet via Regeringens rättsdatabaser.

Syftet med lagen är att uppnå en hög nivå av säkerhet i nätverk och informationssystem för samhällsviktiga tjänster. Detta ska uppnås genom krav på införande av systematiskt säkerhetsarbete och incidentrapportering. Efterlevnad av regelverket följs upp genom tillsyn.

För att få information huruvida den egna organisationen omfattas av NIS-direktivet eller ej hänvisas till Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter för anmälan och identifiering (MSBFS 2018:7). Den egna organisationen bär själv ansvar för att undersöka om organisationen lyder under NIS-direktivet. Om så är fallet ska en anmälan göras till berörd myndighet. Vilken myndighet framgår av MSBFS 2018:7.

Vägledning för identifiering och anmälan från MSB kan läsas här.

Lyder organisationen under NIS ska organisationen bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. Organisationen ska också vidta säkerhetsåtgärder för att hantera risker och säkerställa kontinuitet. Kraven kring detta beskrivs i MSB:s föreskrift om informationssäkerhet för samhällsviktiga tjänster (MSBFS 2018:8).

B) Informationssäkerhet

Informationssäkerhet handlar precis om vad det låter som, nämligen att skydda och bevara viktig och/eller skyddsvärd information och informationstillgångar.

Historiskt har informationssäkerhet i mångt och mycket handlat om att låsa in och säkra olika slags handlingar. Idag finns många fler sätt att hantera information. Vi lagar information i våra datorer, på våra mobiltelefoner, i vår mail, på USB-minnen, i molnet och på många andra ställen.

Vi kan också räkna med att vårt informationsberoende och behov av tillgång till information snabbt och enkelt bara fortsätter att öka. Därför är det idag viktigt att vi hanterar vår information på ett systematiskt sätt. Det är också här själva arbetet med informationssäkerhet börjar, det vill säga i ordning, reda och systematik.

Vid sidan om att hålla god ordning så måste vi också se till att vi skyddar vår information så att den alltid finns tillgänglig då vi behöver den. Vi måste också kunna lita på att den är riktig och inte har blivit förvanskad eller manipulerad. Inom området informationssäkerhet talar man därför ofta om just **tillgänglighet**, **korrekthet** och **konfidentialitet**.

Informationssäkerhet handlar om att upprätta och implementera relevanta och ändamålsenliga regler för informationshantering och att skydda informationen med teknisk utrustning såsom lås, brandväggar, kryptering och brandskydd.

Informationssäkerhet är alltså egentligen en form av processer och rutiner, något som så gott som alla företag alltid jobbar med. Vi har också många exempel där processer och rutiner implementerats på mycket framgångsrika sätt. Exempel på det är implementering av ledningssystem för hälsa och miljö eller kvalitet. För informationssäkerhet finns också ett ändamålsenligt ledningssystem i form av ISO/IEC 27000 Ledningssystem för informationssäkerhet (på informationssäkerhet.se).

Hur gå tillväga?

Hur går man då tillväga för att komma igång med arbetet? MSB har tagit fram information om detta i form av en folder kallad ”Metodstöd för systematiskt säkerhetsarbete”.

Metodstödet utgör en översikt över de steg och processer som ingår i ett systematiskt informationssäkerhetsarbete.

Det som i grunden är viktigt att ta med från metodstödet är att det systematiska informationssäkerhetsarbetet omfattar hela organisationen. Arbetet måste förankras och ledningen måste tydligt stödja arbetet.

Här följer en sammanfattning av stegen i MSB:s metodstöd:

1. Analys

Av metodstödet framgår att det kan vara lämpligt att **börja arbetet genom att göra en genomlysning av både den egna verksamheten och omvärlden**.

Följande analyser bör genomföras:

1. Verksamhetsanalys
2. Omvärldsanalys
3. Riskanalys
4. Gapanalys

Verksamhetsanalysen omfattar en kartläggning av verksamhetens informationstillgångar och intressenters behov, förväntningar och förutsättningar. Ta hjälp av sakkunnig och berörd personal.

Omvärldsanalysen omfattar kartläggning av rättsliga krav, externa intressenters behov, förväntningar och förutsättningar samt hur relationerna med dessa ser ut. Följ även med i omvärldsbevakningen och värdera politiska förutsättningar. Ta hjälp av juridisk och politisk kompetens.

Riskanalysen innebär identifiering av hot och oönskade händelser. Riskanalys kan göras verksamhetsövergripande eller för enskilda objekt eller projekt. Riskanalys ska också innehålla bedömning av konsekvens och sannolikhet. Börja med de mest prioriterade riskerna och ta hjälp av verktyg såsom riskmatriser.

Gapanalysen beskriver skillnaden mellan önskad informationssäkerhetsnivå och befintlig nivå vid analystillfället. Detta ger möjlighet att identifiera åtgärder för att nå önskvärd nivå. Lista åtgärder och – om dessa existerar eller ej – när de ska vara genomförda och status.

2. Utforma

Genomtänkt och ändamålsenligt utformade stöd och verktyg hjälper dig att lyckas med informationssäkerhetsarbetet. Viktigt att tänka på är hur följande utformas:

1. Organisation
2. Informationssäkerhetsmål
3. Styrdokument
4. Klassningsmodell
5. Handlingsplan

Organisationens roll i informationssäkerhetsarbetet följer i praktiken på många sätt organisationens övriga arbete. Ansvar för informationssäkerhet följer av ordinarie verksamhetsansvar och det yttersta ansvaret ligger på ledningen. Det är också lämpligt att säkerställa att den eller de som tilldelas uppgifter inom området har samma möjlighet att stödja och samverka med verksamhetsansvariga som andra stödfunktioner, till exempel ekonomi eller juridik.

En CISO (informationssäkerhetschef) bör kanske rent av ingå som en resurs i ledningsgruppen. CISO:s roll är också strategisk och ska inte förväxlas med den roll som en IT-säkerhetsansvarig har. Istället är en CISO mer att likställa med PMO (projekt management office) i projektorganisationer. CISO vägleder med metoder, processer och rutiner men är inte själva utföraren.

Informationssäkerhetsmål indelas i kortsiktiga och långsiktiga mål. Utgå ifrån genomförda analyser och värdera olika behov. Informationssäkerhetsmålen bör hanteras på samma sätt som andra befintliga visioner, målsättningar och strategier i organisationen.

Styrdokument bör följa befintlig dokumentationshierarki, exempelvis policy, riktlinjer och instruktioner. Dokumenten ska tydliggöra vad som är ”ska-krav” respektive ”bör-krav”. Tänk på att instruktioner ska vara verksamhetsnära och att de på ett tydligt vis ska ange hur arbetet ska utföras.

Klassningsmodellen är central för ett väl fungerande informationssäkerhetsarbete. Klassning av information innebär en konsekvensbedömning kring vad det skulle innebära om informationens konfidentialitet, riktighet och/eller tillgänglighet ej upprätthålls. Klassningsmodellen ska ge konkret beskrivning och värden för olika nivåer. Den ska också harmonisera med konsekvensskalan för risker. MSB har utformat en klassningsmatris som kan utgöra ett gott stöd.

Handlingsplanen är till för att tydliggöra hur organisationen ska agera för att verkställa beslutade åtgärder. Handlingsplanen bör uppdateras på årsbasis och peka ut vilka åtgärder som ger bäst effekt. Ta stöd av gapanalysen för värdering och anpassa handlingsplanen till organisationens övriga verksamhetsplanering.

3. Använda

När ledningssystemet är utformat ska det implementeras och tillämpas.

Informationsklassningen innebär att den information som klassats ska tilldelas och inordnas i sådana rutiner och resurser som motsvarar informationens klassning. Detta gäller krav på till exempel tillämpade informationshanteringssystems robusthet och förmåga att hantera avbrott, frånkoppling, attacker eller intrångsförsök. System och resurser ska vara klassade för lägst den nivå som informationen som de omfattar klassas enligt. I det fall säkerhetsåtgärder kopplats till klassningsmodellen avgör klassningen vilka säkerhetsåtgärder som ska finnas för respektive informationstillgång.

Observera att det är informationsägarens ansvar att se till att klassning av information genomförs. CISO (informationssäkerhetschef) stödjer med metodik.

Genomföra och efterleva innebär att arbetet ständigt pågår. Verksamheten behöver också löpande stöd att efterleva styrdokumenten. Roller och ansvar ska därför vara tydliga och klart framgå. CISO måste tilldelas en sådan roll att denne både har befogenhet och rådighet i organisationen. CISO ska också kunna arbeta strategisk och inte i första hand vara utförare eller bindas upp i specifika projekt eller linjeaktiviteter.

Utbilda och kommunicera med personalen i alla led. Ledningen måste föregå och inspirera samt visa detta genom engagemang och goda exempel. Glöm inte heller bort att informationssäkerhet inte bara handlar om problem och hot. I första hand handlar informationssäkerhet om kvalitet och att skapa möjligheter. Ett väl utfört informationssäkerhetsarbete öppnar möjligheter för organisationen att utveckla nya initiativ och därmed sin affär. Informationssäkerhet är en konkurrensfördel då organisationer som är duktiga på detta får större förtroende hos berörda kunder.

4. Följ upp och förbättra

Informationssäkerhetsarbetet är ett kontinuerligt arbete. Det blir vad man gör det till och kan precis som arbete inom till exempel hälsa, säkerhet och miljö ständigt förbättras och effektiviseras. Informationssäkerhet är också färskvara. Organisationer, liksom omvärld och gränssnitt till olika intressenter såsom kunder, konsulter och leverantörer är en ständigt föränderlig materia. Genom strukturerad uppföljning, mätning och utvärdering ökar förutsättningarna för ett gott informationssäkerhetsarbete.

Monitorering innebär mätning av att informationssäkerhetsarbetet görs ändamålsenligt, verkan och huruvida det fungerar på tillfredsställande. Det viktiga är att komma igång med arbetet. Successivt kan sedan mätningen utökas. Ett sätt att starta kan vara att utvärdera hur uppsatta säkerhetsmål uppfylls och bedöma ledningssystemets tillräcklighet och verkan. Därefter kan man gå vidare med förnyade gapanalyser eller låta genomföra extern revision. Självklart måste utvärdering följa behov. En organisation med synnerligen känslig information ska genomföra grundlig revision av arbetet.

Ledningens genomgång av informationssäkerhetsarbetet och informationssäkerhetsläget bör göras regelbundet och i form av fysiska möten. Att CISO (informationssäkerhetschef) deltar i ledningens ordinarie sammankomster underlättar.

Till MSB:s metodstöd finns också en bilaga som listar framgångsfaktorer och exempel, som ger mer information om informationssäkerhet och handledning.

C) Kort om nya säkerhetsskyddslagen

Arbetet kring den nya säkerhetsskyddslagen pågår. Men ännu har vi inte tillgång till all information som behövs för att närmare beskriva förutsättningarna för efterlevnad. I takt med att regelverket blir klart och Säkerhetspolisens (SÄPO) utlovade handböcker publiceras (i juni 2019), så finns det dock en grund att utgå ifrån för att planera vilka branschspecifika dokument som behöver tas fram. Det finns i sammanhanget ett antal olika som tidigare har tagits fram i samverkan med eller av Svenska kraftnät. Dessa är dock i behov av uppdatering.

För att ytterligare komplicera det hela så presenterades en tilläggsutredning där det ges förslag på en del kompletteringar i den nya lagen, bland annat ett ändrat myndighetsansvar för fjärrvärmeverksamheten (idag på respektive länsstyrelse). Utredningen har varit ute på remiss och bereds nu (juni 2019) på Justitiedepartementet.

Mer information om säkerhetsskyddslagen finns här:

Säkerhetspolisen

Här finns det mesta runt det nya regelverket, inklusive de olika blanketter som behövs. Det som ännu saknas är handböcker som mer i detalj beskriver hur olika delar av regelverket ska hanteras.

Svenska kraftnät

Svenska kraftnät utarbetar föreskrifter som kompletterar Säkerhetspolisens. Dessa har varit ute på remiss och väntas bli klara efter sommaren 2019.

Ytterligare information om energisäkerhet
Energisäkerhetsportalen