Datum
2023-11-24

Energisystem
Emma Johansson, 08-677 25 05
emma.johansson@energiforetagen.se

Positionsdokument avseende cybersäkerhet

Cybersäkerhetsfrågan är av största vikt för energisektorn

Den digitala teknikutvecklingen sker i mycket hög takt och Sverige har som högteknologiskt land en ambition att vara bäst i världen på att använda digitaliseringens möjligheter. Digitaliseringen drivs därför på genom en nationell digitaliseringsstrategi. Samtidigt har det säkerhetspolitiska läget mycket kraftigt försämrats. Detta adresseras på både EU-nivå och nationell nivå genom nya och reviderade författningar.

Energisektorn, och särskilt elförsörjningen, har en nyckelroll i det civila försvaret och totalförsvarets motståndskraft då andra samhällsviktiga verksamheter, företag såväl som försvar av Sverige och civil befolkningen har ett betydande beroende till el. Parallellt med ovanstående samhällstrender pågår en harmonisering av energisektorns förutsättningar på EU-nivå. Branschaktörerna söker också aktivt nya affärsmöjligheter och anpassade roller inom ramen för de förändrade förutsättningarna som klimatomställning och digitalisering innebär. En stor andel av energisektorns aktörer är även delaktiga i kommunikationssektorn genom bredbandsutbyggnad och drift av stadsnät.

I ett synkront sammankopplat el överföringssystem, med Norden och övriga Europa, är aktörerna ömsesidigt beroende av varandras säkerhet mycket omfattande, inte minst på cybersäkerhetsområdet. Branschen är medveten om cybersäkerhetens strategiska betydelse och arbetar intensivt med att åstadkomma den nödvändiga utvecklingen som krävs för att skapa resilient energisystem. För att nå framgång krävs ett väl inriktat stöd från och samspel med myndigheterna.

Kompetensförsörjning ett viktigt fokusområde

Det behövs stora insatser med kompetensutveckling i energibranschen för att påverka beställande, design samt drift- och underhåll av IT- och OT-system så att cybersäkerhetsfrågorna hanteras väl. Tillräcklig digital säkerhetskompetens är en nationell bristvara. Samtidigt sker säkerhetspåverkande beställningar av många olika roller i en verksamhet.

Idag bidrar bland annat ENISA, MSB och FOI med en god grund för kunskapssammanställning. Men utbildning och konkret praktisk handledning behöver nå fram till berörda individer för att etablera förståelse och fungerande angreppssätt hos alla roller i branschen. Kompetenser behöver inte enbart komma energibolag till del utan även leverantörer och underentreprenörer av utrustning samt andra externa aktörer som bedriver utveckling och arbeten inom energibranschen. Detta kan göras genom att:

- Öka antalet utbildningsplatser inom cybersäkerhet samt rikta särskilt fokus på cybersäkerhet för energisektorns och industrins operationella styrsystem.

- Det behövs grundläggande stöd för tillämpning av hur författningar med påverkan på cybersäkerhetsområdet är kopplade till olika verksamhetsområden.
- Det behövs enkel och konkret vägledning och ”branschstandard” för hanteringen av leverantörsrelationer med hänsyn till olika nivåer av skyddsbehov.
- Det behövs enkel och branschanpassad vägledning av cybersäkerhet och specifikt om OT-säkerhet för aktörer med mallar och checklistor att utgå ifrån.

Samordningsbehov

Energibranschens olika verksamhetsdelar förhåller sig till ett stort antal myndigheter som driver utveckling av regelverk och myndighetsutövning med påverkan på cybersäkerhetsområdet. Dels är det olika myndigheter kopplade till respektive energitjänster, dels flera myndigheter på det digitala området. För att respektive verksamhets systematiska informationssäkerhetsarbete och strukturerade cybersäkerhetsåtgärder ska vara möjliga att åstadkomma på ett effektivt sätt, måste regelverk och myndighetsutövning vara förenliga och samordnade. Detta avser både angreppssätt och vilka aspekter av utvecklingen som prioriteras i olika skeden. Önskvärda åtgärder är:

- Samordning av myndighetsansvar
- Harmonisering av regelverk inom EU och nationellt
- Samordnad utveckling av kravområden, tex föreskrifter
- Förenkling och tydlighet i rapportering

Samarbetsbehov

Vi ser också att det krävs ett utvecklat samarbete inom energisektorn och mellan sektorer, med viktiga intressenter och med myndigheterna för att möta hot och risker samt stödjande på området. För att uppnå en tillräcklig säkerhetsnivå totalt sett är alla aktörer beroende av varandras förmåga. Särskilt god samverkan krävs i den operativa hanteringen vid incidenter. Önskvärda åtgärder är:

- Enhetlig bedömning vid informationsklassning
- Tillgängliggöra dimensionerande hotbeskrivningar aggregerade på nationell nivå
- Tillsätta resurser för robusta och krypterade kommunikationskanaler för säkerhetskänslig samverkan
- Strukturer för operativt utbyte av information om hot och incidenter som säkerställer att informationens riktighet och tillgänglighet genom redundans

Ekonomiska aspekter

Energisektorn omfattar både privata och offentliga energibolag, som bedriver både konkurrensutsatt och reglerad verksamhet. Tillkommande investeringsbehov och driftkostnader kopplat till nya och utvecklade regelverk får inte leda till snedvriden konkurrens eller indirekt utarmning av energisystemen på grund av försämrad lönsamhet. Därför behövs tydlighet i:

- Förutsättningar för investeringsstöd för cybersäkerhetsåtgärder
- Möjligheten att täcka kostnader inom intäktsramen

Vägledning inom tekniska fokusområden

Med ovanstående aspekter i beaktande ser branschen ett antal fokusområden som är av särskild vikt att ge god vägledning inom för att hantera och minimera riskerna som teknikutvecklingen för med sig samtidigt som möjligheter och innovation kan tas tillvara för att stärka säkerheten:

1. Tillämpning av regelverk och säkerhetsskyddslag

   En ökad samsyn behöver uppnås mellan tillsynsmyndigheterna avseende tolkning av EU förordningar och nationella regelverken samt överlappningar. Delar som återkommer i alla verksamheter och som inte är lösningsspecifika kan hanteras sektors gemensamt. I övriga sektorspecifika delar behövs praktisk vägledning, checklistor och mallar.

2. Tillämpad informationssäkerhet

   Det finns stora mängder stödmaterial att tillgå inom informationssäkerhet. En sektorspecifik insats kan inrikta sig på urval av praktiska stöd och vägledningar beroende på verksamhetens storlek och mognad inom informationssäkerhet. Ett startpaket för ledningssystem för informationssäkerhet för små energiföretag kan vara ett konkret stöd.

3. Sektor gemensam energi CERT (Computer Emergency Response Team)

   Det är viktigt att energibranschen får en snabb tillgång till en central varningsfunktion i stil med norska KraftCert och dansk energi-CERT. En svensk energi CERT bör få förutsättningar samverka effektivt med CERT-SE och det Nationella cybersäkerhetscentret på ett sätt som inte är realistiskt för enskilda verksamheter. Energiföretagen tillsammans med ledande energibolag skulle kunna starta detta med stöd av myndigheterna i någon skala.

4. Design och skydd av OT-miljön

   Fungerande och säkra operationella styrsystem är en central fråga för operativa samhällsviktiga funktioner i energisystemen. Det behövs konkret vägledning och kompetensutveckling kring hur verksamheter bygger robusta och säkra lösningar samt skyddar dessa mot OT-attacker.

5. Användande av molntjänster

   Skalbara molntjänster har många fördelar och uppfattas ofta som en snabb och framkomlig väg för IT-organisationerna. Det finns dock fallgropar, viktiga avväganden och vägval som kräver medvetenhet för att skydda skyddsvärda delar av verksamheten. Det behövs därför konkret och tydlig vägledning för många av branschens företag för att navigera rätt.

6. Internet of Things och AI-teknik

   Industriell IoT (Internet of Things) och AI (artificiell intelligens) används för att energioptimera och effektivisera lösningar i kritisk energiinfrastruktur. Fler uppkopplade enheter ökar samtidigt attackytan. Det krävs stöd för en grundläggande säkerhetsdesign redan från början så att inte denna utveckling skapar sårbarheter.

7. Kryptering

   Kryptering kan vara ett lämpligt skydd. Men det krävs medvetenhet för att avgöra när det är rätt lösning och vad det ställer för krav på organisationen för att det inte ska leda till andra risker. Det krävs praktisk vägledning för att säkerställa rätt effekt.

8. Leverantörsförhållanden

   Beroendena till leverantörer är betydande medan beställarkompetensen och kravställandet kring cybersäkerhetsaspekter i många fall har brister. Många tekniska lösningar och tillgängliga leverantörer är gemensamma för stora delar av branschen. Det finns därför stora vinster i en nationell samordnad kravställning och tillämpning såväl för beställare som leverantörer i upphandling.

9. Robusta komponenter

   Branschen är i hög grad beroende av importerade komponenter för sina IT- och OT-system. Att säkerställa robust och säker funktion i alla lägen och att komponenter inte innehåller planterade sårbarheter är kritiskt för en trygg energiförsörjning.

10. Globala handelsflöden

    Energisektorns beroendet av högriskleverantörer i länder utanför Europa för kritiska komponenter skapar både kritiska försörjningskedjor och cybersårbarheter i energisystemet. Myndigheter behöver aktivt bevaka och analysera kritiska komponenter såsom råvaror och halvledare som är av stor betydelse för fortsatt digital utveckling och konkurrenskraft.