Datum
2018-02-23

Anders Fredriksson
070-164 44 39
anders.fredriksson@energiforetagen.se

Viktiga erfarenheter från årets cyberförsvarsdag

Cyberförsvarsdagen 2018

Den 14 februari anordnade branschorganisationen Säkerhets- och Försvarsföretagen (SOFF) den årliga cyberförsvarsdagen. Det var ett mycket välbesökt och intressant event med deltagare från en stor spännvidd av aktörer och myndigheter. Exempelvis MSB, Säpo, FRA, säkerhetsföretag och universitet.

Utmaningen

Mycket av innehållet i föreläsningarna handlade om den sårbarhet som ett allt mer uppkopplat samhälle står inför. Mycket av detta är redan känt, exempelvis olika cybervapen och hackeraktivisters verksamhet. Vad som däremot kanske inte är lika känt är säkerhetsutmaningen kring molntjänster som är beroende av internet och outsourcingaktiviteter.

Exempel på risker som målades upp var avbrott på internationella och kontinentala internetkablar. Här består inte risken bara av antagonistiska angrepp. Även olyckor och naturkatastrofer har lett till betydande bortfall av funktionalitet och information. Andra exempel är utmaningar i kontraktsskrivning vad gäller access och rätt till förfogande över kritiska data. Vad händer om en molntjänstleverantör går i konkurs eller köps upp av en mindre seriös aktör?

En annan utmaning är när aktörer lägger all data i molntjänster. Vissa molntjänster har god säkerhet, vissa inte. Exempel finns där hela verksamhetsidéer stulits inom loppet av 10 sekunder. Detta som en konsekvens av att en aktör inte nyttjat tillräckligt säkra molntjänster.

Att glappet mellan hot och skydd successivt växer utgör ett allt mer påtagligt problem. Teknikutvecklingen sker så fort att regelverk och säkerhetssystem inte alltid hinner med.

Vad ska man då göra?

Även om sårbarheten är komplex så finns det faktiskt mycket som går att göra. Ett huvudbudskap är att inte bli allt för beroende av internet. Det kan låta tråkigt med alla de möjligheter och allt det positiva som internet faktiskt också medför. Därför ska man istället ha inställningen att sunt förnuft gäller.

I detta gäller det också att kombinera det digitala skyddet med det fysiska, båda är nämligen ömsesidigt beroende av varandra. Det är också viktigt att delta i olika nätverk med god kännedom om den hotbild vi står inför och att man inom dessa nätverk vågar vara någorlunda öppen med proaktiv information.

Nyckelfaktorer för att bli framgångsrik i sitt säkerhetsarbete är:

- engagemang från ledning och ledningsgrupper.
- upprättande av planer för krishantering.
- fokus på effekten av incidenter.
- inrättande av team för krishantering.

Förmågan att hantera och avvärja cyberincidenter bygger vidare på att det avsätts resurser och personal till preventivt arbete. En tumregel är att det inom ett företag med hundra anställda krävs minst två personer med uppdrag att arbeta med säkerhetsfrågan.

Resursernas storlek, vilka åtgärder som krävs och vilken betydelse säkerhetsarbetet har, bygger på analys av vad som är skyddsvärt. Utifrån det kan sedan åtgärder vidtas för att öka medvetenheten om risker inom hela organisationen. Till det är det också viktigt med en kultur där alla, oavsett befattningsnivå, har rätt och möjlighet att påtala förekommande brister eller problem. Sist men inte minst: övning ger färdighet.

Regelverksförändringar

Vid cyberförsvarsdagen togs även NIS (nätverk och IT-säkerhet) och GDPR upp. Åter igen med koppling till outsourcing och molntjänster. Just outsourcing var det mest återkommande temat.

Outsourcing har dock ingen legal definition och uttrycks på olika sätt i olika sammanhang. När outsourcing sker till en aktör i ett annat land används ibland begreppet offshoring men inte heller för det begreppet finns någon enhetlig tillämpning. Med hänsyn till avsaknaden av en tydlig begreppsbildning samlas begreppen under en övergripande term; utkontraktering av säkerhetskänslig verksamhet.

En orsak till detta är med största sannolikhet de incidenter som skett i myndighetssfären och som beskrivits i media. Det som är viktigt att ha kontroll på är att det inte bara är våra myndigheter som omfattas av ett utökat säkerhetskrav.

Förslaget till ny säkerhetsskyddslag innebär ett förstärkt skydd för säkerhetskänslig verksamhet. Exempelvis kan detta innebära en tillåtlighetsprövning som ger Säkerhetspolisen och Försvarsmakten möjlighet att hindra eller ställa ytterligare villkor för utkontraktering, när det anses vara nödvändigt för att upprätthålla en verksamhets skyddsvärde eller om säkerhetsskyddsåtgärder är bristfälliga.

Den tolkning vi gör idag är att även privata aktörer, som omfattas av NIS-direktivets kommande definition av samhällsviktiga tjänster kring el, kan omfattas av tillåtlighetsprövning vad gäller utkontraktering.

Tillåtlighetsprövningen kommer att utföras av Säpo och Försvarsmakten men genom Svenska kraftnät. Exakt vad som gäller kring detta är dock ännu inte fullt ut utrett. Ett förtydligande kring vad som de facto kommer att gälla är därför nödvändigt. I det fall vår nuvarande tolkning är korrekt inträder dessa regler per den 1 januari 2019.