EUROPEISKA UNIONEN
Fonden för inre säkerhet

Nationell övning för cyberattack mot kärntekniska anläggningar planeras

Bild av: Camilla Duse Göran Kessell är projektledare för iPilot 2017.

Polisen ska tillsammans med andra myndigheter och privata aktörer öva samverkan i projektet iPilot 2017, som beviljats medel ur EU:s fond för inre säkerhet (ISF).

Syftet med iPilot 2017 är att vara nätverks- och kompetensuppbyggande för funktioner inom det svenska systemet som blir involverade vid allvarlig cyberattack mot kärntekniska anläggningar eller annan elproduktion. Användningen av IT och digitala styr- och kontrollsystem vid kärntekniska anläggningar ökar och därmed även risken för sårbarhet som kan exploateras.

– Cyberattacker är ett högaktuellt område. Vi har redan sett exempel på så kallade överbelastningsattacker. Cyberövningar är en viktig del i att utveckla, förbättra och fokusera på samarbete vid storskaliga och allvarliga IT-incidenter, säger projektledaren Göran Kessell vid gruppen för Krisberedskap/Nationell samordning/Operativa enheten/NOA.

iPilot 2017 är ett samarbetsprojekt mellan Polismyndigheten, Strålsäkerhetsmyndigheten (SSM), Myndigheten för samhällsskydd och beredskap (MSB), Svenska kraftnät (SvK), Kustbevakningen (KBV), Säkerhetspolisen (SÄPO) och Försvarets radioanstalt (FRA), och har sin grund i en sen tidigare etablerad samverkansgrupp för myndigheterna. I projektet ingår även aktörer från elsektorn, främst sk. tillståndshavare – stora elbolag som av SSM beviljats tillstånd att driva en kärnteknisk anläggning.

Aktörerna har olika uppdrag:

- Förhindra radiologiska utsläpp eller stöld av radioaktiva ämnen (tillståndshavarna, SSM)
- Förhindra störning av elproduktion (elproducerande industri, SvK)
- Kunna lagföra antagonist samt verka brottsförebyggande (polisen)

Bakgrund och finansiering

2015 genomfördes en nationell övning om ett angrepp mot en kärnbränsletransport i samverkansgruppens regi. Övningens genomförande fick beröm från IAEA (International Atomic Energy Agency) och blev input till en handbok som organisationen tog fram.

– IAEA vände sig sen till Strålsäkerhetsmyndigheten och frågade om man inte ville genomföra en pilot för att planera, utvärdera och genomföra en cyberövning. Det ville vi i samverkansgruppen, säger Göran Kessell.

Sen kom möjligheten till delfinansiering genom att söka medel ur EU:s fond för inre säkerhet på polisens ekonomiavdelning. Projektet har beviljats totalt 2 917 649 kr ur fonden, vilket utgör 75 % av projektets totala kostnad. 500 000 kr har även beviljats ur Elsäkerhetsfonden. Resterande del, som framför allt utgörs av kostnader för arbetstid, står deltagande aktörer för.

Så går övningen till

Del 1 är en teknisk operativ övning där en cyberattack simuleras mot IT samt styr- och kontrollsystem liknande de som finns vid svenska kärnkraftverk. Myndigheter och representanter från kärnkraftverken kommer att delta samt även representanter från IAEA. För polisens del är det IT-forensiker som kommer att ingå med huvuduppdrag att säkra spår för att möjliggöra lagföring.

Försvarshögskolan (FHS) kommer att leda övningen enligt beprövad metodik. FOI (Totalförsvarets forskningsinstitut) ansvarar för att driva och konfigurera övningsmiljön. Övningen är preliminärt planerad till v.43.

Del 2 är en seminarieliknande övning där lednings- och styrfunktioner kommer att utvärdera och diskutera ansvar och roller. Övningen är preliminärt planerad till v.45.

Vad ska projektet resultera i?

Övningens resultat kommer att utvärderas enligt metodik från MSB och resultera i en rapport. Resultatet kommer att utgöra underlag för uppdatering av styrdokument och i kravställning mot elindustrin (tillståndshavarna). Att bygga upp kunskapen inom elsektorn är viktigt.

Planerandet, utformningen och genomförandet av övningen kommer att utvärderas och spridas till IAEA. Det är därmed troligt att iPilot 2017 får internationell spridning på samma sätt som 2015 års övning.

– Något som är jätteviktigt är det brottsförebyggande och särskilt det förtroendeskapande arbetet – att vi får de privata aktörernas förtroende och att man vågar påtala säkerhetsproblem och risker. Det kan vara känsligt eftersom det kan skada varumärket, säger Göran Kessell.

Text av: Camilla Duse

Kontakt: Göran Kessell