Pressmeddelande

2015-03-09

Bristande cybersäkerhet inom kritisk infrastruktur

Risken för allvarliga IT-incidenter som intrång, dataläckage och sabotage på vitala system har blivit ett allt större hot mot kritisk infrastruktur. Det anser cybersäkerhetsföretaget Advenica som under vecka 12 genomför ett antal seminarier på detta ämne i Malmö, Göteborg och Stockholm.

De utmaningar och möjligheter som finns framöver för att öka informationssäkerheten i anläggningar för kritisk infrastruktur är viktigt att belysa och diskutera. Advenica genomför därför en seminarie-turné den 17-19 mars som vänder sig främst till IT- och informationssäkerhetsansvariga samt anläggningsansvariga inom bland annat elproduktion/-distribution, vattenförsörjning, telekommunikation och transportnätverk.

Program och anmälan finns tillgängligt på www.advenica.com/infrastruktur.

För ytterligare information, vänligen kontakta:
Anders Strömberg, VP Marketing, 0708-16 09 47, anders.stromberg@advenica.com

Om Advenica

Advenica är en ledande europeisk leverantör av cybersäkerhet. Företaget utvecklar, tillverkar och säljer avancerade cybersäkerhetslösningar som förhindrar intrång, stöld och dataläckage vid informationsutbyten och möjliggör därmed samverkan mellan och inom nationer, organisationer och system med höga säkerhetskrav.

Om informationssäkerhet inom kritisk infrastruktur

Cybersäkerhet har idag en avgörande betydelse för en säker och tillförlitlig drift av all kritisk infrastruktur i samhället. Det kan till exempel handla om elproduktion/-distribution, vattenförsörjning, telekommunikation och transportnätverk, som alla är beroende av IT-system för drift, övervakning och styrning.

Till skillnad från tidigare är dagens styr- och kontrollsystem ofta integrerade med andra interna och externa nätverk. Vid till exempel produktion och distribution av elektricitet

behövs idag realtidsinformation från SCADA-nätverken, samt även extern information för att optimera verksamheten. En avgörande betydelse för att förstärka ICS/SCADA-säkerheten är dessutom att hålla de olika zonerna i arkitekturen isolerade och endast låta mycket specifik information överföras på ett säkert och kontrollerat sätt mellan dem.

Några viktiga områden att beakta avseende informationssäkerheten:

- IP-baserad fjärranslutning för extern service och underhåll blir allt vanligare. Det kan till exempel behövas tillgång till loggar och möjlighet att göra mjukvaruuppdateringar på utrustningen. Denna fjärranslutning, utanför anläggningens nätverk, måste vara säker mot intrång och godtagbar för anläggningsansvariga.

- Introduktionen av smarta nät (s.k. smart grids) har lett till en ökad automation och ett växande behov av aktuell och regelbunden data för att optimera produktion och distribution. Svårigheten är att genomföra en sammankoppling med bibehållen säkerhet i systemet.

- Regulatoriska standarder för kritisk infrastruktur uppdateras i en allt snabbare takt och det finns idag en osäkerhet vad dessa regler och formella krav de facto innebär för anläggningsägare. Detta försvårar också valet av ”rätt” teknikinvesteringar som behöver göras för att möjliggöra en efterlevnad av dessa regler/krav och förstärka informationssäkerheten.

Utan adekvata cybersäkerhetslösningar är risken för dataintrång i dessa system betydande. Lämpliga cybersäkerhetslösningar till stöd för verksamheten är krypterad VPN, datadioder och filter med hög säkerhet och assurans.