Webinar cyberveiligheid: gebruik veiligheidsdenken uit chemie om digitale weerbaarheid te verhogen

vnci.nl/nieuws/nieuwsbericht

02.12.2021

Chemiebedrijven, groot én klein, kunnen in de problemen komen als ze te maken krijgen met een hack, attack of datalek. De bedrijfscontinuïteit kan hiermee op het spel komen te staan. De financiële en reputatieschade daarvan kunnen desastreus zijn, maar het kan ook de 'fysieke' veiligheid onder druk zetten.

De Koninklijke VNCI organiseerde op 1 december een webinar over cybersecurity. Experts van verschillende organisaties gaven de deelnemers een kijkje in de 'digitale' keuken van cybersecurity.

Elke dag worden er wereldwijd cyberaanvallen gedaan. Deze worden 24/7 gemonitord. De financiële sector is het grootste doelwit van cybercriminelen. Manufacturing, waar ook de olie- en chemiesector onder valt, staat op de vierde plek. De vraag is niet of maar wanneer je getroffen wordt door een cyberattack. Chemiebedrijven moeten hier goed op voorbereid zijn.

NCSC

Het Nationaal Cyber Security Centrum (NCSC) gaf een uitleg over wat zij doen om bedrijven en sectoren te helpen bij cyberveiligheid. NCSC stelt kennisproducten beschikbaar, geeft beveiligingsadviezen, organiseert bijeenkomsten en houdt zich bezig met monitoring en response. Ze zijn 24/7 bereikbaar als meldpunt voor cyberincidenten. De chemische industrie is door de overheid aangemerkt als vitale sector en dat betekent dat de productie onder alle omstandigheden moet kunnen blijven draaien. Een cyberaanval brengt dus grote risico's met zich mee. Het NCSC werkt ook samen in een groot netwerk van organisaties en kennisinstellingen om zoveel mogelijk informatie te verzamelen die weer gedeeld kan worden met andere bedrijven.

ISAC Olie en Chemie

De chemische industrie is deelnemer van de zogenaamde ISAC Olie en Chemie, het Information Sharing and Analysis Centre. In dit overlegplatvorm wordt gevoelige en vertrouwelijke informatie uitgewisseld over cyberincidenten, digitale dreigingen, kwetsbaarheden en maatregelen binnen de olie-en chemiesector. De ISAC wordt gefaciliteerd vanuit het Nationaal Cyber Security Centrum. Aan de hand van enkele praktijkvoorbeelden werd in het webinar de impact van cyberaanvallen toegelicht en de lessen die uit dergelijke incidenten getrokken kunnen worden. Een recent voorbeeld betrof een cyberaanval in mei van dit jaar bij Colonial Pipeline in Houston (Amerika). Het gevolg was dat tankstations geen brandstof meer hadden en vliegtuigen aan de grond bleven staan. Een aanval die misschien voorkomen had kunnen worden als er binnen de organisatie beter nagedacht was over de digitale veiligheid.

Leerpunten die op basis van deze casus aan de orde kwamen: scheid je OT (industriële controlesystemen) en je IT (kantoorsystemen), stel een business continuïteitsplan voor je IT-systemen op, hergebruik nooit je wachtwoorden (ook al zijn die nog zo sterk) en stel een multi-factor authenticatie in. Een eerste stap om veiligheidsmaatregelen door te voeren, begint met een bowtie-analyse. In deze 'vlinderstrik' maak je een analyse van bedreigingen, risico's en consequenties. Bijvoorbeeld: via een phishing mail (bedreiging) wordt je file server leeggehaald (risico) en komt gevoelige data op plekken terecht waar het niet hoort te komen (consequentie). Focus op preventie én recovery, was het devies. Een risicogerichte aanpak, zoals de bowtie-analyse, sluit aan bij het 'safety' denken in de petrochemie en is daardoor heel goed toepasbaar op cybersecurity.

Fox-IT

Fox-IT, een bedrijf dat zich bezighoudt met computer- en netwerkbeveiliging, ging in op het 'aanvalsplan' dat mede op basis van internationale ervaringen is opgesteld. In dit plan zijn verschillende stappen opgenomen waarmee (petro)chemiebedrijven hun cybersecurity weerbaarheid van industriële besturingssystemen (ook wel SCADA/ICS genoemd) kunnen versterken. Een belangrijke pijler van het aanvalsplan is managementcommitment. Cybersecurity is geen onderwerp meer van de IT-afdeling alleen. Het hoort structureel thuis in de boardroom. Andere bouwstenen zijn risk-assessment, awareness binnen de hele organisatie en het treffen van preventieve, mitigerende en responsmaatregelen.

Basis ingrediënten van 'veiligheid'

Een kijkje in de keuken van cybersecurity heeft de deelnemers geleerd dat de basis ingrediënten van digitale weerbaarheid een optelsom zijn van hard-, soft- en mindware. Deze aanpak draagt bij aan het versterken van de bedrijfscontinuïteit en daarmee een betrouwbare, veilige en gezonde operatie van de (petro)chemische bedrijven en het vertrouwen in de sector. De VNCI houdt de leden op de hoogte van toekomstige ontwikkelingen op het gebied van cybersecurity, onder andere nieuwe wet- en regelgeving.