ISA lanceert Cybersecurity-expertprogramma

Cybercrime snelst groeiende vorm criminaliteit

Cybercriminaliteit is een van de snelst groeiende vormen van criminaliteit. Recent onderzoek wijst uit dat de wereldwijde omzet van cybercriminaliteit gelijk is aan die van de omzet in de drugshandel. En we zijn nog maar aan het begin! Beroepscriminelen organiseren zich steeds beter en maken gebruik van geavanceerde digitale aanvalsmethoden. Het afgelopen jaar vonden verschillende grootschalige aanvallen plaats met een hoge organisatiegraad, gericht op diefstal van geld en kostbare informatie. Naast de overheid waren bedrijven en burgers in toenemende mate het slachtoffer. Uit het Cybersecuritybeeld Nederland 2016 (CSBN 2016) blijkt dat beroepscriminelen daardoor een steeds grotere bedreiging vormen voor de digitale veiligheid in Nederland. Dat dit probleem ook internationaal speelt, blijkt uit het feit dat er bijvoorbeeld in België een actieve samenwerking is ontstaan tussen overheid en bedrijfsleven. Men heeft hier onder andere een emergency-responseteam opgericht om snel op cybersecurity-incidenten te kunnen reageren. ▷ Pieter van der Klooster

Cybercriminelen voeren langdurige, hoogwaardige en geavanceerde operaties uit en de campagnes van deze beroepscriminelen worden steeds geavanceerder. In het verleden waren de digitale aanvallen en bijbehorende campagnes van criminelen vaak van korte duur en gericht op snel geld verdienen door veel partijen te benadelen. Het afgelopen jaar hebben criminelen echter een aantal campagnes uitgevoerd, waarvoor hoge investeringen zijn gedaan en waaruit een hoge organisatiegraad blijkt. Tweederde van de getroffen bedrijven had deze aanvallen niet zelf waargenomen, dus de geregistreerde aanvallen zijn slechts het topje van de ijsberg. Cybercrime is zodoende hard op weg om voor bedrijven de grootste bedreiging te worden. Ruim 60 procent van de bedrijven maakt zich er ernstig zorgen om. Toch heeft slechts een 37 procent een plan klaarliggen om adequaat op cybercrime te reageren.

Traditionele aanpak is vragen om problemen

Remote access tools zijn zoals bekend zeer populair onder criminelen. Criminelen gebruiken deze om binnen computernetwerken van organisaties te zoeken naar waardevolle systemen en informatie. Ook zijn er online marktplaatsen - het zogenaamde Darknet - waar deze activiteiten voor iedereen gewoon als dienst te koop zijn. Virussen, phishing, drive-by-downloads; cybercrime kent vele soorten en vormen. Het mag inmiddels duidelijk zijn dat er flink wat gevaren zijn voor bedrijven die zich moeten zien te wapenen tegen cybercrime. Waan je niet te snel veilig; cybercrime staat nooit stil. De traditionele aanpak van het plaatsen van een firewall, het regelen van wat antivirussoftware en het beheer hiervan overlaten aan veelal onvoldoende gekwalificeerde engineers - die vaak nog een behoorlijk aantal andere taken hebben - is domweg vragen om problemen.

Meer behoefte aan kennis & tools

Bedrijven, instellingen maar ook de overheid moeten intensief gaan samenwerken om cyberaanvallen te kunnen afslaan. Elkaar goed informeren over cyberaanvallen en de geslaagde aanpak hiervan kan herhaling van dergelijke aanvallen bij andere bedrijven voorkomen. Samen sta je sterker. De steeds meer geavanceerde werkwijze van cybercriminelen maakt het noodzakelijk om als onderneming op een geheel andere wijze met cybercrime om te gaan. Het mag duidelijk zijn; er is dringend behoefte aan meer kennis maar ook aan veel beter gekwalificeerd personeel.

De ISA/IEC62443 standaard

ISA heeft al 70 jaar ervaring met het ontwikkelen en actueel houden van 150 verschillende standaarden. Een van de meest recente standaarden is de ISA-99 standaard - internationaal bekend als de ISA/IEC62443 standaard. Deze securitystandaard voor Industrial Automation and Control Systems (IACS) geeft richtlijnen om potentieel verwoestende cyberschade aan de industriële systemen en netwerken te voorkomen en/of te beperken.

ISA/IEC 62443 is ontwikkeld door vele toonaangevende internationale cybersecuritydeskundigen uit het bedrijfsleven, de overheid en de academische wereld ▶

en wordt beschouwd als ‘s werelds enige op consensus gebaseerde standaard voor IACS-systemen. Deze Industrial Automation and Control Systemen zijn helaas niet ontworpen om weerstand te bieden aan cyberaanvallen. Een cyberaanval kan de indringer waardevolle informatie opleveren, maar ook de veilige exploitatie van industriele installaties verstoren en deze installaties zelfs geheel onbruikbaar maken. De gevolgen zijn niet te overzien; concurrentievervalsing, grootschalige stroomuitval, explosies, chemische lekken of zelfs fabriekssluitingen.

‘Er is dringend behoefte aan meer kennis en aan veel beter gekwalificeerd personeel.’

Kennis haal je bij de bron

Om aan de dringende behoefte vanuit de industrie tegemoet te komen heeft ISA een complete reeks unieke industriële cybersecuritytrainingen ontwikkeld op het gebied van “Assessment, Design, Implementation, Operations and Maintenance”. Elk van de vier meerdaagse trainingen wordt afgesloten met een officieel erkend examen dat wordt afgenomen door Prometric. Deze organisatie is vooral bekend van de Microsoft- en Cisco-certificering en heeft in vrijwel elk land van de wereld een vestiging waar men nu ook het ISA-examen kan afleggen. ISA-cybersecuritycertificaten worden toegekend aan degenen die met succes de cursussen doorlopen en aansluitend de examens doen. Personen die alle vier de certificaatprogramma’s met succes voltooien, mogen de titel van ISA/IEC 62443 cybersecurityexpert voeren. Naar verwachting zullen de eerste cybersecurityexperts begin 2018 hun trainingstraject afronden. ■