bu

RENOVATIE STATION MAASTRICHT

SCHAALBAAR MODEL APPARTEMENTEN

1 OP 5 HEEFT SCHADE DOOR HACKERS

MOBILITEIT IN STEDELIJK NL

HOE BOUWEN VOOR MIDDENINKOMENS

BOUW EN UITVOERING
BEREIKT RUIM 73.100 LEZERS
JAARGANG 51 - 6 2019
HET VAKBLAD VOOR RIJK, PROVINCIE EN GEMEENTE
IN NEDERLAND EN BELGIE

IEDEREEN HEEFT MET HACKERS TE MAKEN

Cybercriminaliteit is de snelst groeiende vorm van misdaad. Jaarlijks levert het in Nederland voor ruim tien miljard euro schade op.

Wereldwijd wordt het geschat op zes biljoen euro. Maar liefst een op de vijf ondernemers wordt slachtoffer. In gesprek met Pieter van der Klooster van ISA die het gevecht aangaat tegen cybercriminelen.

TEKST **GERARD VOS**

De dreiging van cybercriminaliteit is enorm hoog, maar het kennisniveau is over het algemeen genomen laag, aldus directeur International Business Development bij ISA Pieter van der Klooster. “Als het om een onderwerp als Cybersecurity gaat heb je twee soorten bedrijven. Bedrijven die gehackt zijn en bedrijven die nog niet weten dat ze gehackt zijn. Het was zo dat bedrijven die vroeger het slachtoffer werden van een hack hierover zwegen. Maar inmiddels groeit het bewustzijn en zie je dat de wil er is om hier gezamenlijk iets tegen te doen.”

Waar bedrijven vroeger vooral lijdzaam aan het afwachten waren tot ze een keer gehackt werden, daar zie je nu dat bedrijven zich steeds vaker verenigen en opleidingen volgen bij een partij als ISA. De International Society of Automation (ISA) is een stichting die wereldwijd bijna veertigduizend leden telt. Van der Klooster: “ISA heeft een standaard ontwikkeld met betrekking tot cybersecurity. Grote bedrijven als Schneider Electric, Honeywell en Siemens zijn bij ons aangesloten. Experts binnen de proces-automatisering hebben de koppen bij elkaar gestoken en hebben de ISA-IEC 62243 standaard ontwikkeld. Die wordt steeds verder doorontwikkeld. We zijn constant in strijd met cybercriminelen.”

PAARD EN WAGEN

Dat cybercriminaliteit nu een snel groeiende vorm van misdaad is, is inherent aan de ontwikkeling van internet, schetst Van der Klooster. “Het is raar gelopen. Met de komst van internet hebben we eigenlijk alleen maar naar de voordelen gekeken. Ik vergelijk het weleens met de komst van de auto. We hadden paard en wagen en kregen de auto. Gaandeweg werden we ons bewust van de risico’s en kwamen er veiligheidsgordels, betere remmen, aangepaste verkeersregels, airbags.”

Geleidelijk aan zijn we ons bewust geworden van de risico’s van internet. Het slechte nieuws is dat iedereen doelwit is. “Het is toch vaak zo van: ‘mij gebeurt dat niet’, maar een hacker benadert tienduizend doelen tegelijk en kijkt vervolgens waar een deur openstaat. Als je cybercriminaliteit met het krijgen van een brand vergelijkt dan is het risico dat je op een dag gehackt wordt veel groter. Ik wil niet een standaard van angst creëren, het is realiteit. Iedereen heeft met hackers te maken, op alle niveaus.”

VEEL TE HACKEN

Feitelijk is er een continu gevecht gaande tussen hackers en beveiligers. Nadeel is dat er tegenwoordig ook best veel te hacken is. Want gebouwen zitten vol sensoren

STANDAARD ISA-IEC 62243

ISA-IEC 62443 is een specifieke cybersecurity standaard voor de industrie aan de OT-zijde, ontwikkeld door ISA in samenwerking met de IEC. Deze ISA-IEC 62443 standaard gaat goed naast elkaar met de ISO 27001 standaard die in de IT-sector wordt gebruikt. Verder is de ISA-IEC 62443 standaard geheel in lijn met de NIST cybersecurity framework. Het is een internationaal geaccepteerde standaard, die wereldwijd steeds meer in opkomst is.

Sinds 1949 wordt ISA internationaal erkend als deskundige bron voor normen en standaarden voor automatiserings- en besturingssystemen. ISA standaarden helpen automatiseringsprofessionals processen te stroomlijnen en de veiligheid, efficiëntie en winstgevendheid in de industrie te verbeteren (www.isaeurope.org).


ISA

voor verwarming, ventilatie en airconditioning. Dan heb je nog intelligente camera's en gebouwautomatiseringssystemen. Het vormt allemaal een ingang voor cybercriminelen. Het onderzoeksbureau Gartner heeft voorspeld dat er tegen 2021 maar liefst 25 miljard aangesloten apparaten in gebruik zullen zijn via het Internet of Things. Van der Klooster: "Neem een airco, die kun je op afstand op veertig graden zetten. Dat zien we in de praktijk al gebeuren. Dat als een gebruiker van een gebouw niet met geld over de brug komt, de thermostaat continu op veertig graden wordt gezet. Het is maar een van de vele voorbeelden."

RIJKSWATERSTAAT

Bij Rijkswaterstaat liepen ze ook tegen de opmars van de moderne tijd aan en staken ze de hand in eigen boezem. Rijkswaterstaat bracht naar buiten dat tunnels, bruggen, sluizen en waterkeringen niet voldoen aan de gestelde veiligheidsmaatregelen tegen cybersecurity. De bouwwerken zijn kwetsbaar. Van der Klooster: "Een aantal jaar geleden is er een sluis gehackt in Veere. De bedieningssystemen zijn gemaakt om dertig jaar mee te gaan en zo'n vijftien jaar geleden geplaatst. Wat moet je als

112 GEHACKT

RTL Nieuws berichtte half juni dat tientallen miljoenen mensen in Argentinië, Uruguay en Paraguay werden getroffen door een grote stroomstoring. Bedrijven en hulpinstellingen moesten een beroep doen op noodstroom. Treinen kwamen tot stilstand, verkeerslichten vielen uit, tankstations werkten niet en in de grote steden reden geen metro's meer. Het is uitzonderlijk dat hele landen zonder stroom zitten, meestal gaat het om een wijk, een stad of hooguit een regio. De regering onderzoekt nu wat er precies is misgegaan. Daarbij wordt een cyberaanval niet uitgesloten.

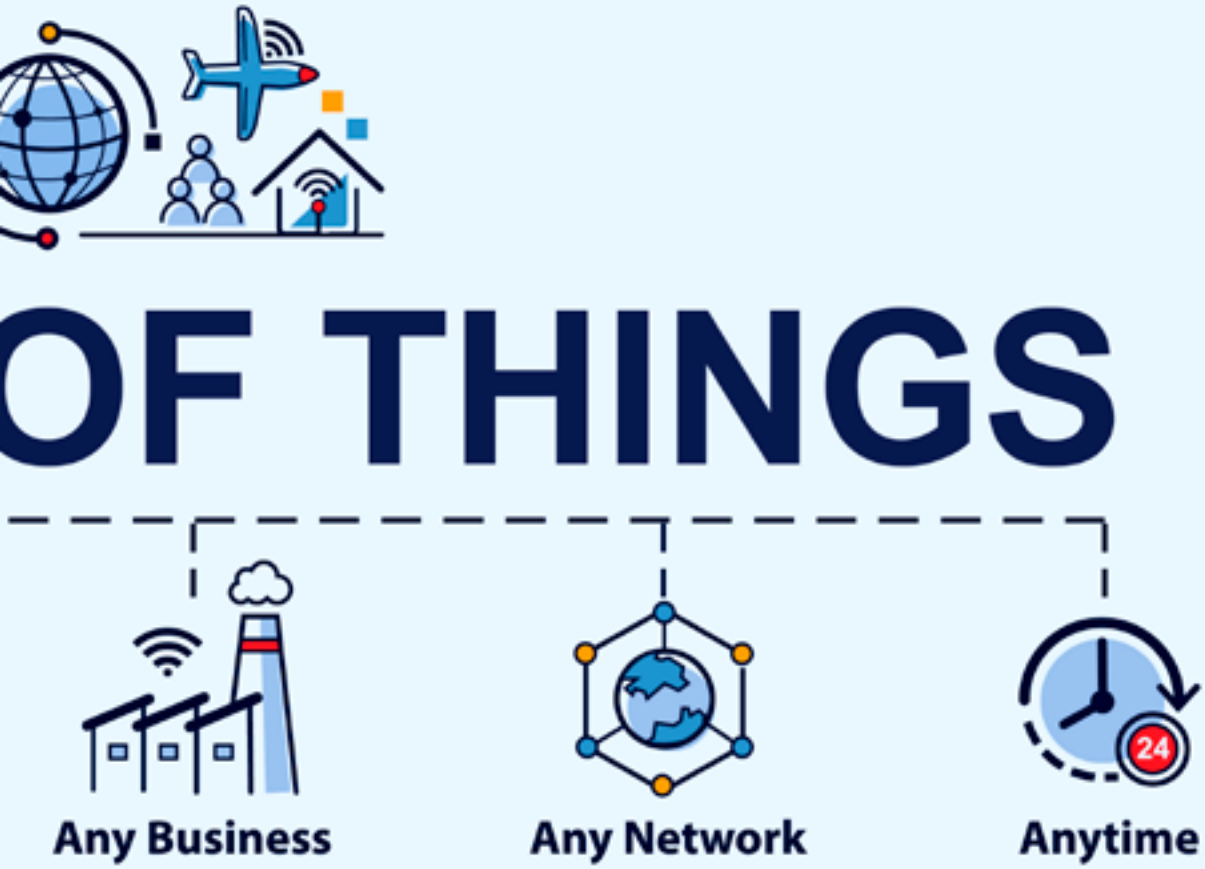
Van der Klooster: "Ook de elektriciteitsnetwerken in Europa zijn aan elkaar gekoppeld. Als je daar eenmaal iets gaat uitschakelen dan vallen de netwerken als dominosteentjes om. Moet je voorstellen dat je een week lang zonder stroom moet leven.

CYBERSECURITY EXPERT

ISA leidt medewerkers van bedrijven op in vier trainingen die in totaal elf dagen beslaan. Aan deze trainingen zit een officieel erkend certificeringsprogramma vast. Degene die de examens met goed gevolg afleggen, mogen zich Cybersecurity Expert noemen. Meer informatie: https://cybersecurity-expert.com

› Rijkswaterstaat dan? De systemen vervangen? Daar is het geld niet voor. Je kunt het Rijkswaterstaat nauwelijks kwalijk nemen. Maar het levert wel een gevaar op voor de samenleving, want nu is er de mogelijkheid dat delen van het land onder water worden gezet."

Weliswaar zijn fabrikanten inmiddels zover dat ze veilige producten in de markt zetten. Maar die veilige producten zijn nog niet in groten getalen aanwezig, ziet Van der Klooster.
"Je bent als Rijkswaterstaat op veel fronten kwetsbaar. Dat kan ook gelden voor gemeenten die veel gebruik maken van SCADA-systemen. Soms is er bij zulke systemen zelfs geen wachtwoord nodig om binnen te komen. De reactiesnelheid van overheid en bedrijfsleven verbaast me soms wel. Dan is er bij een partij de bewustwording van 'hier moeten we iets aan gaan doen'. Maar voordat er daadwerkelijk een stap is genomen, ben je soms jaren verder."



TIPS

Hoe kun je als Rijkswaterstaat of bouwbedrijf nu het beste cybercriminelen weren? “Je moet door de ogen van een crimineel kijken. Waar ben je kwetsbaar? Als een cybercrimineel jouw proces kan beïnvloeden dan kunnen ze je kapot maken. Stel dat ze op afstand de receptuur van jouw beton kunnen veranderen of de blueprint van prefab modules kunnen hacken, dan zijn de gevolgen voor jouw bedrijf niet te overzien.”

Neem afdoende maatregelen. Het begint met mensen, leid medewerkers op en maak ze bewust. Door misschien ook net iets slimmer te beveiligen dan je concurrent, ben je een stuk minder aantrekkelijk voor criminelen. Helemaal veilig bestaat niet, schetst Van der Klooster. “Of je zult weer terug moeten naar de tijd dat je met een GSM belt en met een adressenmolen werkt en alles met de typemachine tikt. Lachend... en vervolgens je brieven met de postduif versturen.” BOUWENUITVOERING

HACKEN IS KINDERSPEL

Wie denkt dat je een whizzkid nodig hebt om een bedrijf plat te leggen, heeft het mis.
Met een DDoS-aanval is dat kinderlijk eenvoudig. Voor een klein bedrag is het mogelijk om een account te kopen op een website. Hoe meer iemand betaalt, hoe frequenter en krachtiger de DDoS-aanvallen. Van der Klooster: “Voor honderd dollar koop je al een DDoS-aanval en leg je een bedrijf een week plat als het niet goed is beveiligd.”