UIT: FINANCIEEL DAGBLAD zaterdag 11 februari 2017

Eerste studenten cyberveiligheid krijgen diploma

De vraag naar experts op het gebied van digitale veiligheid groeit hard. De Cyber Security Academy in Den Haag voorziet in die behoefte.

Nederland is sinds deze week 19 deskundigen op het gebied van cyberveiligheid rijker. Donderdag studeerde de eerste lichting studenten van de Cyber Security Academy in Den Haag af. Deze in 2014 opgerichte materopleiding geeft les op een mix van onderwerpen: niet alleen de techniek of de bestuurlijke kant van cyberveiligheid komen aan de orde, maar de verschillende kanten worden in samenhang behandeld.

Aanleiding voor het starten van de opleiding is het grote tekort op de arbeidsmarkt aan mensen met kennis van cybersecurity. Bedrijven en instellingen voeren een harde strijd om de mensen met technische kennis binnen te halen. Maar ook de behoefte aan mensen die op meer strategisch niveau kunnen werken is groot. Uit onderzoek van het ministerie van Justitie en Veiligheid in 2015 bleek dat er voldoende mensen afstuderen met relevante opleidingen, zoals bijvoorbeeld informatica, maar dat die vaak niet kiezen voor een carrière in de cyberveiligheid.

Als we cybercriminaliteit willen bestrijden moeten we de fora aanpakken

De Cyber Security Academy probeert in dit gat te springen. Om toegelaten te worden moeten studenten al kennis hebben van het fenomeen cyber security. De achtergrond van de studenten uit de eerste lichting liep sterk uiteen: van politie tot KPN, van ministerie van defensie tot kabelmaatschappijen. 'Die verschillen waren heel waardevol', zegt Herbert Leenstra. Hij werkt zelf bij telecombedrijf KPN en schreef zijn masterscriptie over de veiligheid van de zelfrijdende auto. Sommigen studenten waren meer technisch onderlegd, anderen hadden veel kennis op bestuurlijk gebied. Maar dat zorgde voor mooie discussies en we konden elkaar helpen. Zelf keek hij voor de opleiding vooral met een technische bril naar vraagstukken. 'Nu bekijk ik hetzelfde probleem op meerdere niveaus. Ik heb meer oog voor de samenhang tussen techniek, mens en bestuurlijke vragen.'

De opleiding past ook in het streven van de gemeente Den Haag om spil te worden in alles wat te maken heeft met veiligheid. De gemeente wil het imago van de stad van recht en vrede vergroten en heeft The Hague Security Delta (HSD) opgericht. Overheid, bedrijfsleven en kennisinstellingen moeten samenwerken. Door het stimuleren van innovaties op het gebied van nationale veiligheid, cybersecurity, vitale infrastructuur, stedelijke veiligheid, forensische technieken wordt gewerkt aan een veiliger Nederland en economische groei.

Naast bedrijven als Siemens, Philips en Thales bestaat HSD uit partijen zoals het Internationaal

Strafhof, het NFI, TNO en andere technologiebedrijven, diverse universiteiten en opsporingsinstanties. De potentie van HSD is groot, constateerde Policy Research Corporation. Tot 2020 zal de werkgelegenheid per jaar met bijna 3% toenemen, de omzet van de veiligheidssector kan uitgroeien tot € 2,5 mrd per jaar. Volgens het rapport kan HSD binnen vijf jaar in omvang verdubbelen en uitgroeien tot 'de nummer één van Europa'.

'Zaai verwarring onder cybercriminelen'

Gert Ras (51), onderzoeksonderwerp: Hackersfora (foto: Mark Horn voor het FD)

Het is nog net niet zo gemakkelijk als op internet een pizza bestellen. Maar feit is dat wie kwaad wil via internet, daar zelf geen specialistische kennis voor hoeft te bezitten. Malafide software om mee in te breken, te stelen of af te persen kan gewoon worden gekocht. Op hackersfora bieden cybercriminelen hun diensten aan.

Gert Ras, in het dagelijks leven hoofd van het Team High Tech Crime van de Nationale Politie, deed voor zijn scriptie onderzoek naar deze fora. Wie zitten erop en wat kun je er tegen doen? Ras: 'Als we cybercriminaliteit willen bestrijden moeten we de fora aanpakken. Daar worden producten en diensten aan de man gebracht. En daar wisselen cybercriminelen informatie uit.'

Ras ploos maandenlang een Russisch hackersforum minutieus uit. Hij analyseerde meer dan een miljoen berichten in 150.000 draadjes op het forum. De politieman vond onder meer uit dat het actieve deel van het forum veel kleiner was dan vooraf gedacht: zo'n 10% van de gebruikers schreef 80% van de berichten. 'Het beheer op zo'n forum is heel strikt. Een groot deel van de gebruikers wordt er al snel af gegooid, want iedereen wordt per definitie gewantrouwd.'

Door een netwerkanalyse kan de politie een forum gerichter aanpakken, stelt Ras. 'Zo'n forum opdoeken kan niet, dan duikt het elders gewoon weer op. Beter is het om de pilaren onder zo'n forum weg te trekken. Bijvoorbeeld door privéboodschappen in openbare draadjes te gooien of de identiteit van deelnemers te onthullen. 'Je kan wantrouwen en verwarring zaaien. Dan kwijnt zo'n forum vanzelf weg.'

Ras was politieman zonder specifieke cyberachtergrond. Maar sinds 2014 heeft hij zich op de aanpak van cybercriminaliteit gestort. De kennis bij de politie van cybercriminaliteit groeit snel, stelt hij. Maar die kennis is nu nog erg geconcentreerd, onder meer bij het team waar hij zelf aan het hoofd staat. 'Cybercriminaliteit raakt steeds meer verweven met de gewone criminaliteit. De aanpak ervan moet dus ook onderdeel worden van het gewone politiewerk.'

'Auto-industrie onderschat gevaar hackers'

Herbert Leenstra (46), onderzoeksonderwerp: Veiligheid van de zelfrijdende auto (foto: Mark Horn voor het FD)

Zelfrijdende auto's zijn de toekomst. De auto-industrie werkt hard aan modellen waarbij computers al het werk van de chauffeur uit handen nemen. Maar nu al komen veel auto's niet meer in beweging zonder chips en software. Moderne auto’s zijn rijdende computers en dus zijn ze een interessant doelwit voor hackers.

Maar tot zijn schrik ontdekte Herbert Leenstra tijdens het werken aan zijn scriptie voor de Cyber Security Academy dat de auto-industrie dat gevaar nog niet bepaald onderkent. 'Waarom zou iemand mijn mooie auto willen aanvallen?!', vroeg een verbaasde producent tijdens een interview voor de scriptie. Een naïeve gedachte, stelt Leenstra, die zich voor zijn werk bezighoudt met het ontwerpen van de cyber security architectuur om het KPN netwerk veilig te houden.

Leenstra schetst in zijn scriptie een reeks vraagstukken waar de industrie een antwoord op moet vinden, wil de zelfrijdende auto veilig de weg op kunnen. Hoe gaan de producenten bijvoorbeeld hun verschillende systemen en software afstemmen om auto's met elkaar te laten communiceren? Nu testen ze allemaal apart hun producten, op de weg rijdt alles door elkaar.

En ook: computers worden doorgaans binnen drie jaar afgeschreven. De gemiddelde auto in Nederland is tien jaar oud. Hoe zorg je dan dat je de autosoftware op een veilige manier op peil houdt?

Dat doe je in elk geval niet door je klanten een usb-stick met de nieuwste autosoftware te sturen. Autofabrikant Chrysler deed dit nadat ethische hackers bewezen op afstand een Jeep Cherokee te kunnen infiltreren. Ze zetten vanuit huis de stereo op maximaal volume, zetten airco en ruitenwissers aan en remden de auto - die op dat moment op de snelweg reed- af.

De update via usb, die dit soort praktijken onmogelijk moest maken, is volgens Leenstra een droom van hackers, en illustreert de onvolwassenheid van de auto-industrie op het gebied van cybercrime. 'De industrie moet auto's gaan zien als computers op wielen. Daar hoort een bepaalde kwetsbaarheid bij die je grotendeels kan oplossen in de architectuur en design van de ICT systemen van de auto.'

]

'Veilige verbindingen hoeven niet duur te zijn'

Nelly Ghaoui (31), onderzoeksonderwerp: VPN voor consumenten (foto: Mark Horn voor het FD)

Als beleidsmedewerker bij de Nationaal Coördinator Terrorisme en Veiligheid is Nelly Ghaoui zich bewust van het belang van digitalev eiligheid. Dus toen ze een jaar of wat geleden op vakantie ging, zorgde ze vooraf dat ze ook privé kon surfen op een beveiligde internetverbinding. 'In het hotel was wel wifi, maar dat is vaak open of slecht beveiligd. En dus is de informatie die via zo'n verbinding wordt verzonden makkelijk toegankelijk, ook voor partijen die kwaad willen.'

Ghaoui zorgde dat ze in het buitenland kon internetten via eenVPN-verbinding: met VPN-software wordt alle verstuurde informatie versleuteld. VPN bouwt eenbeveiligde tunnel op in je verbinding. Wie het verkeer op zo'n verbinding onderschept kan niks met versleutelde data. En zo kwam ze op het idee voor haar afstudeerscriptie. 'Ik vroeg me af wat er voor nodig zou zijn om iedereen van VPN te voorzien. In een werksituatie is het heel gewoon om het internetverkeer op deze manier te beveiligen. Maar consumenten doen het nog weinig.'

Waarom is een VPN-verbinding niet net zo gewoon als anti-virussoftware of firewalls?, vraagt Ghaoui zich af. 'Sommige diensten, bijvoorbeeld Gmail en WhatsApp zijn vanzelf al versleuteld. Maar veel internetverkeer is dat ook niet. Tegelijk zijn er wel steeds meer open wifi-verbindingen waar persoonlijke informatie overheen gaat.'

Echt duur is een VPN-verbinding niet. De kosten verschillen erg, maar voor een jaar is een consument misschien €50 kwijt. Oftewel, echt duur is het niet en het belang lijkt groot. Ghaoui: 'Ik was nieuwsgierig naar de mogelijkheden om dit te veiliger te maken.' Maar in de praktijk is het natuurlijk niet zo simpel, kwam de bestuurskundige achter. Ze onderzocht verschillende beleidsstrategieën, die mogelijk konden leiden tot veilig internetten voor iedereen.

De mogelijkheden variëren van zelfregulering tot een verplichting vanuit de overheid en wat van allebei. Haar conclusie is -weinig verrassend zegt Ghaoui zelf- dat zelfregulering het meest kansrijk is juist omdat er zoveel partijen zijn die een rol spelen en allemaal verantwoordelijkheid moeten nemen. Van leveranciers tot de overheid en de consument zelf.