## Ken de zwakke schakels in uw ict

# De digitale brandweer

Ethisch hacker en expert in cybersecurity Ramón Dohmen toont ons op 11 april op het congres Veilig Werken in Ahoy Rotterdam de achilleshielen van onze ict. Zowel op het werk als thuis.

tekst Ton Bennink

Zijn ergste nachtmerrie: een verstoring van complexe chemische processen die leidt tot een grote milieuramp in de haven van Rotterdam Een ding is zeker: wie zijn lezing bijwoont, is altijd alert. En thuiswerken? Het kan geen kwaad om als bedrijf toch maar wat extra zekerheid in te bouwen.

Ramón Dohmen is gecertificeerd cybersecurity-expert en ethisch hacker. Hij werkt als security officer ICT bij de DCMR Milieudienst Rijnmond en is lid van de FERM-werkgroep ("Stevig, standvastig en sterk. Geen afkorting, maar de Rotterdamse vertaling van resilience", zo meldt de website) die inhoud geeft aan de bewustwording in de haven van Rotterdam.
Zoals gezegd: Dohmens ergste nachtmerrie is dat er complexe chemische processen worden verstoord. Of erger nog, gehackt. Waardoor er een milieuramp plaatsvindt in de Rotterdamse haven waarvan de gevolgen reiken tot ver daarbuiten. Of dat er grote economische schade ontstaat omdat de loodsen niet meer uit kunnen varen als gevolg van een cyberaanval. "Of ik daartoe in staat zou zijn? Ik hoop van niet."

Als een *blessing in disguise* spookte na de start van FERM het NotPetya-virus rond in de haven. "Het deed zich voor als ransomeware: software die je systemen gijzelt om vervolgens losgeld te vragen. Maar er werd geen losgeld gevraagd, het virus richtte louter schade aan. Er was ook geen sprake van een gerichte aanval, maar van een mondiaal virus. Een bijzonder toeval, dat de noodzaak tot weerbaarheid nog eens benadrukt."

### Vier vormen

Dohmen onderscheidt vier vormen van cybercriminaliteit:

1. Hactivisten willen vanuit ideologische motieven een bedrijf platleggen. "Bijvoorbeeld omdat ze vinden dat een bedrijf vervuilend is. Vergelijk het met activisten die nertsen loslaten op een nertsfokkerij. Misschien horen nertsen niet te worden gefokt en een bedrijf niet te vervuilen, maar wij doen er natuurlijk alles aan om ervoor te zorgen dat er geen aanval plaatsvindt. Want die kan leiden tot nog grotere schade."
2. Dan zijn er de zogenoemde *script-kiddies*, jongeren die uit baldadigheid een ict-systeem platleggen of gewoon omdat het kan. "Eind januari had een aantal banken daarmee te maken. Er werd met de vinger naar Rusland gewezen. Zij zouden een DDos-aanval op onze vitale netwerken als banken hebben gepleegd. Het bleek een jongen uit Brabant van 18 jaar. Die jongens hebben vaak veel verstand van ICT, doen niks anders dan computeren en kunnen enorme schade aanrichten." Volgens Dohmen circuleren er op internet tools waarmee kwaadwillenden websites tegelijkertijd massaal kunnen bezoeken. "De banken kunnen daar wel wat tegen doen, maar dat is vrij technisch om uit te leggen. Ze hebben hopelijk hun boel verder goed op orde."

### Congres Veilig Werken

Ramón Dohmen vertelt u over de zwakke plekken in uw ict op het congres Veilig Werken. U heeft meteen toegang tot de vakbeurs Safety&Health@Work. www.congresveiligwerken.nl.


3. Dan zijn er natuurlijk lieden die vanuit terroristische motieven een cyberaanval willen plegen.
4. Of de broodcriminelen die een containertje door willen laten, dan wel achterover drukken.

"Wij zijn als de digitale brandweer en onderzoeken de risico's. Daarbij kijken we naar de zwakke schakels onder de bedrijven. We proberen iedereen te pushen alert te zijn op zwakke plekken in de cybersecurity."

## Bewustwording

Bewustwording is het sleutelwoord volgens Dohmen. Hij zal dan ook tijdens zijn lezing in Rotterdam laten zien hoe je in een paar muisklikken een webcam kunt overnemen. Of in een bedrijfsnetwerk kunt kijken. "Er vinden dagelijks talloze aanvallen plaats op onze systemen. Vaak vanuit het buitenland. Wat de intenties zijn en of er echt door landen aangestuurde lieden achter zitten? Dat weet ik niet, maar het gebeurt wel. Ik zal laten zien hoe vaak we bij de DCMR worden aangevallen. We doen er alles aan om hacks te voorkomen en tot nu toe zijn we ook 'schoon' gebleken door detectieapparatuur. Maar aanvallen zijn er continu. En garanties zijn er niet."

Hoe makkelijk het is om in iemands privéomgeving door te dringen, bewijzen bijvoorbeeld babyfoons met webcam die ook op afstand werken. "Dat vinden mensen wel gemakkelijk, want dan kunnen ze ook buitenshuis via de smartphone kijken. Maar die mensen moeten zich dan wel realiseren dat anderen even gemakkelijk meekijken. Wachtwoorden zijn vaak standaard en mensen passen ze zelden aan."
Serieuzer wordt het als het gaat om infiltratie van bedrijfssystemen, SCADA/ICS-systemen bijvoorbeeld. Daarmee kan een hacker zich op afstand toegang verschaffen tot bedrijfsproductiemiddelen. "Stel je voor wat er kan gebeuren als kwaadwillenden toegang krijgen tot verbrandingsovens of verwarmingsketels. En die mensen zijn er, want ze zoeken naar toegang. Ik zal dat op het congres ook laten zien via beveiligingsapparatuur die ik ook thuis gebruik. Want hackers bestoken niet alleen bedrijven, ook thuis zijn er continu bedreigingen."

## Thuiswerk

We zijn ons als maatschappij in het algemeen en bedrijfsleven in het bijzonder echt nog onvoldoende bewust van de gevaren die inbreuk in de digitale omgeving opleveren, aldus Dohmen. Ict brengt veel gemak met zich mee, maar misschien moeten we ook een stapje terug doen. "Ik laat tijdens de lezing een website zien die doorlopend op zoek is naar openstaande poortjes in systemen. Elk op het internet aangesloten systeem heeft duizenden van die poortjes. Die variëren van een poortje voor e-mail op nummer 25 tot die voor het bekijken van een website op nummer 80. Er hoeft er maar een niet goed dicht te zitten of er volgt een infiltratie. De website waar ik het over heb is overigens te goeder trouw.

Hoe dat invloed kan hebben op het werk? Nou, ik zou bijvoorbeeld bij thuiswerk de toegang tot het bedrijfsnetwerk op bepaalde punten ontzeggen. Sommige handelingen, zoals het bedienen van systemen, kun je maar beter echt op het werk doen." «