

INTERVIEWS | 1 JULI 2019

CYBERGEDDON: EEN REËEL GEVAAR?

Auteur: Drs. Margot Hovestad RO - Raymond Wondergem MSc RO

Beeld: 123RF - Andrey Zaychuk - Jared Murray

Leestijd: 6 min



Peter Zinn is expert op het gebied van cybersecurity en was spreker op het IIA Congres afgelopen juni. In dit interview passeerden de gevaren van cybercrime, de kans op een Cybergeddon en de weerbaarheid van organisaties om dit te voorkomen, de revue.

Vertel eens iets over uzelf

"Ik heb informatica gestudeerd en daarnaast wat psychologie. Overdag was ik IT-er en 's avonds deed ik aan toneel. Na drie jaar in Canada maakte ik de overstap naar cybersecurity. Daar werd ik strategisch adviseur bij de politie bij het net opgerichte hightech crime team. Daar heb ik mijn twee kanten in balans gebracht, de technische IT-kant en de communicatiekant. Belangrijk in deze rol was het communiceren met de buitenwereld, bijvoorbeeld om mensen duidelijk te maken dat je wel aangifte kunt doen op het gebied van cybercrime. Daarnaast heb ik mij sterk gemaakt voor een cyberteam in iedere regio. Dat heb ik tien jaar gedaan. Het team is in die periode gegroeid van 15 naar 120 medewerkers.

Vervolgens ben ik voor mijzelf begonnen. Ik vind spreken leuk en geef lezingen over cybersecurity en -crime. En ik train specialisten op het gebied van cybersecurity om betere sprekers te worden. Deze specialisten hebben vaak veel kennis,

maar niet de vaardigheden om deze kennis goed over te brengen. Mijn belangrijkste doel is Nederland veiliger te maken op het gebied van cybersecurity, daar wil ik aan bijdragen.”



Peter Zinn: “De meeste mensen zijn van goede wil en moeten handvatten krijgen om te leren omgaan met cybercrime”

Wat kunnen we doen om cybercrime risico's te verminderen?

“Over het algemeen is het bewustzijn bij mensen er wel, alleen weten ze niet waar ze op moeten letten en wat ze moeten doen om een cyberaanval te voorkomen. De meeste mensen zijn van goede wil en moeten handvatten krijgen om te leren omgaan met cybercrime. Als iedereen in de keten zijn eigen verantwoordelijkheid neemt, dan kan 99% van de problemen voorkomen worden en is er niet eens zoveel aan de hand. Het begint bij het ontwikkelen van ‘patches’ door bijvoorbeeld Microsoft, vervolgens moet de IT-afdeling van een organisatie deze patches tijdig uitvoeren en de eindgebruiker zorgt voor zijn digitale hygiëne. Deze hygiëne bestaat onder andere uit het:

- aanstaan van automatische updates;
- aanzetten van de screensaver, zodat als je van je werkplek weggaat anderen niet kunnen meekijken;
- gebruiken van fatsoenlijke wachtwoorden (lange wachtwoorden, bijvoorbeeld vier woorden);
- gebruiken van verschillende wachtwoorden voor verschillende domeinen.

Ik vergelijk het altijd met gordels in de auto. Toen die werden ingevoerd was er veel tegenstand. Mensen vonden het vreemd en onwennig. Nu is het raar wanneer je geen gordel draagt. Dat is precies hetzelfde met het aanleren van nieuwe gewoonten op cybergebied. Het is niet fijn, want we moeten onze werkwijze veranderen. Maar als je de gewoonte eenmaal hebt, kost het geen extra tijd en voelt het niet meer vreemd.

“Welke risico's willen organisaties lopen op het gebied van cybersecurity? Het heeft geen zin om alles ‘dicht’ te zetten, want dan kunnen medewerkers hun werk niet doen”

Het doel van organisaties moet zijn om cybersecurity als onderdeel van hun risicobeheersing te zien. Welke risico's willen organisaties lopen op het gebied van cybersecurity? Het heeft geen zin om alles ‘dicht’ te zetten, want dan kunnen medewerkers hun werk niet doen. Als een organisatie vervolgens het slachtoffer wordt van ransomware is het belangrijk dat er een back-up is. Dus is het verstandig te zorgen voor een goed back-upbeleid, waarbij de back-ups ook

periodiek getest worden. Er zijn bedrijven failliet gegaan door ransomware.”

Kun je cybercrime voorkomen?

“Nee, nooit helemaal. Er blijven altijd slimme criminelen die nieuwe manieren bedenken om toch binnen te komen. Cybercriminelen zijn ontzettend creatief als het gaat om geld verdienen. Een maand geleden had ik een bijeenkomst met een groep CISO's (chief information security officers). Het onderwerp was dat de cybersecuritydijken steeds hoger worden. Maar wat gaan we doen als de dijken het begeven? Wat betekent het als een groep cybercriminelen ervoor zorgt dat je organisatie niet meer functioneert? Organisaties moeten een plan hebben als dit gebeurt, als de dijk overstroomt. Heb je dan een fall-backsysteem, ben je dan robuust genoeg om nog te functioneren als organisatie? Een van de uitkomsten was: we kunnen de dijken wel verhogen, maar ze zijn lek. Cybercriminelen zoeken naar lekken in de dijken en denken out of the box. Daar zit ook een kans voor auditors, niet om de dijken te verhogen, maar om de lekken te vinden.”

Op het IIA Congres sprak u over cybergeddon. Wat is dat?

“Cybergeddon is een woordspeling op armageddon en gaat over het einde van de wereld. De redenatie is dat we sinds de jaren zestig steeds meer afhankelijk zijn geworden van IT en dat groeit nog steeds. Door schaalvergroting van IT wordt de impact van een calamiteit ook groter. Het betekent dat je niet alleen meer aangevallen kunt worden door iemand uit je eigen omgeving, maar ook door een Russische crimineel die 2000 km verder op zit. De aanvalsoppervlakte is vergroot. De multinational Maersk is hier een goed voorbeeld van. Een aanval van Russische hackers op de IT-infrastructuur van Oekraïne leidde ertoe dat Maersk een tijdlang 'out of business' was.”



Hoe groot is de kans op een cybergeddon?

“Ik denk dat de kans klein is dat er een cybergeddon gaat plaatsvinden, maar het is niet onmogelijk. Als je bijvoorbeeld kijkt naar artificial intelligence, dan ben ik niet bang dat robots de wereld gaan overnemen. We zijn nu wel in de 'narrow-artificial-intelligencefase' beland, de fase dat robots één handeling ontzettend goed kunnen. Alleen zijn robots nog steeds afhankelijk van de aansturing door mensen. Kwaadwillenden kunnen enorme schade aanrichten met dit nieuwe gereedschap. Autoriteiten daarentegen wordt veiliger door artificial intelligence, want mensen zijn niet de beste chauffeurs. Maar er is ook de mogelijkheid om het artificial-intelligencesysteem negatief te beïnvloeden.

AUDIT

MAGAZINE

Om de kans op een cybergeddon te verkleinen, is het van belang om de security en de robuustheid van de samenleving te vergroten. Dat begint in je organisatie. Wat ga jij als organisatie doen als alle digitale gegevens weg zijn? Alleen kost robuustheid een organisatie veel geld. Er moet een terugvaloptie zijn en dat is ook logisch, ook als mens hebben we twee longen, twee nieren, twee ogen.”

De mens is vaak de zwakste schakel, waarom?

“Daar kan ik uren over vertellen. Voor software heb je updates, maar ons brein is al eeuwenlang niet geüpdatet. Wij hebben bepaalde patronen waar cybercriminelen gebruik van maken. Het is makkelijk om misbruik te maken van het vertrouwen van mensen om fysiek of digitaal binnen te komen. Wat doe je eraan? In ieder geval elkaar blijven vertrouwen. Anders worden de medewerkers paranoïde en werkt je organisatie niet meer. Het gaat om het aanpassen van patronen en gewoonten om de veiligheid vergroten. Bijvoorbeeld het aanzetten van een screensaver. Een ander belangrijk onderdeel is de cultuur van de organisatie. Vroeg of laat wordt een organisatie gehackt. Het is belangrijk dat medewerkers dit open en eerlijk kunnen vertellen. Er moet de mogelijkheid zijn dat medewerkers leren van hun fouten en ze er niet voor worden gestraft. Een open cultuur zorgt ervoor dat medewerkers hun gewoonten aanpassen.”

“Vroeg of laat wordt een organisatie gehackt. Het is belangrijk dat medewerkers dit open en eerlijk kunnen vertellen”

Wat is de rol van de top van een organisatie?

“Bewustwordingsprogramma’s hebben ook een plek in het voorkomen van cybercrime, maar daar moet het niet bij blijven. Cybersecurity is vooral een verantwoordelijkheid van de raad van bestuur, dus ook de bewustwording is dat. Op de werkvloer zijn best goede ideeën om cybercrime aan te pakken, maar de sturing hoort vanuit de top te komen. Top-down moet aangegeven worden dat cybersecurity belangrijk is. De raad van bestuur moet ook de opdracht geven om het IT-landschap in kaart te brengen en om de IT-afdeling op voldoende sterkte te brengen om cybercrime het hoofd te bieden. Dan hebben bewustwordingsprogramma’s toegevoegde waarde.”

Is er een standaardprofiel van de cybercrimineel?

“Er is geen standaardprofiel van de cybercrimineel. Het begint bij de tophackers. Ik deel ze grofweg in een aantal categorieën in, aan de hand van een berg:

- statelijke hackers (China, Rusland, Amerika, et cetera) en de tophackers;
- carrièrecriminelen;
- script kiddies die online tooltjes gebruiken zonder te weten wat ze doen.

Net zoals bij een berg het smeltwater naar beneden stroomt, stroomt bij deze indeling de informatie en het gebruik van de technologie ook naar beneden. De tophackers bedenken en schrijven nieuwe methoden om te hacken en wat later maakt de volgende groep hier gebruik van. Overigens zijn de tophackers niet meer zichtbaar. Je kunt het vergelijken met de kopstukken van de maffia. Die zijn ook niet in beeld.

AUDIT

MAGAZINE



Naast deze categorieën kun je hackers ook indelen naar motieven. Deze motieven zijn: geld (businessmodel); politiek; vandalisme; bekendheid; uitdaging. Het is belangrijk om te beseffen dat 90% van de hackers niet crimineel is. De meesten staan aan de goede kant en doen het voor de sport. Zij waarschuwen vervolgens de organisaties dat er een 'lek' is ('responsible disclosure'). Het is daarom van belang dat organisatie de regels voor responsible disclosure op hun website zetten. Organisaties moeten dit serieus nemen, het lek dichten en de hacker hiervan op de hoogte te brengen. In Nederland zijn we hier al heel ver mee."

Wat kunnen auditors leren van cybercriminelen?

"Creatief en lateraal denken. Denk als auditor vooral out of the box en probeer eens een andere techniek als de huidige niet werkt. Je hebt soms meerdere plannen nodig om je doel te bereiken. Dan heb je ook een back-upplan als het nodig is. Wees niet bang om een keer af te wijken van standaardpatronen, wees flexibel. Richt ook ruimte in om te pionieren en te klooiën."

Over

Peter Zinn studeerde informatica. Na een standaard IT-carrière stapte hij over naar het hightech crime team van de Nationale Politie. In 2016 startte Zinn zijn eigen bedrijf op het gebied van cybersecurity.

Tags: informatiebeveiliging

Bron url: <https://auditmagazine.nl/interviews/cybergeddon-een-reeel-gevaar/>