Artikel gepubliceerd in Clique Magazine op 7 november 2020
Journalist: Hans Nieuwenhuis, Clique Media

Door coronacrisis wordt de strijd voor cyberweerbaarheid urgenter

Omdat de samenleving is ondergedompeld in de corona-manier van werken en leven, is zij nog sterker afhankelijk geworden van digitaal contact en digitale ontwikkelingen. Het plotselinge en onvoorbereide massale thuiswerken maakt ons extra kwetsbaar voor cybercriminaliteit. Er wordt nu van verschillende kanten actie ondernomen om de cyberweerbaarheid te vergroten.

Particulieren en bedrijven
De Cyber Security Raad (CSR), een adviesorgaan van het kabinet en via het kabinet ook het bedrijfsleven met als doel om op strategisch niveau de cybersecurity in Nederland zeker te stellen, heeft onlangs een urgentieverklaring opgesteld, om aandacht te vragen voor deze problematiek. Volgens Wiebe Draijer, bestuursvoorzitter van de Rabobank en lid van de CSR namens het bancaire domein, dateert de inhoudelijke boodschap van de verklaring al van voor de coronacrisis, maar wordt de timing plotseling urgenter: “Het is bewonderenswaardig om te zien hoe snel organisaties het thuiswerken hebben kunnen organiseren en tegelijkertijd de veiligheid van hun ICT-systemen hebben kunnen garanderen. Kleinere bedrijven met een bescheiden IT-afdeling zullen daar vooral moeite mee hebben gehad. De ‘gang naar huis’ gaat met aanvullende risico’s gepaard. Met de urgentieverklaring vraagt de CSR hier op korte termijn aandacht, coördinatie en regie voor.” Volgens Draijer is het gevoel van risico op dit vlak over het algemeen kleiner dan het daadwerkelijke gevaar. Het cyberbewustzijn moet worden vergroot. Bedrijven en particulieren moeten alert zijn, hun systemen op orde hebben en zorgen voor gedragsdiscipline. Gedrag is de kwetsbaarste schakel. “Dat vraagt ook de aandacht van de overheid, als coördinerend orgaan, om hier iets mee te doen. De krachten van de publieke en private sectoren moeten worden verbonden om sterker te kunnen optreden!”

Samenwerking en coördinatie
Samenwerking leidt vaker tot het vangen van hackers, en coördinatie helpt in de verdediging tegen grote cyberaanvallen op organisaties. Men moet weten waar deze aanvallen te verwachten zijn. “Daarvoor is intensieve informatie-uitwisseling tussen zoveel mogelijk partijen, ook de publieke sector, noodzakelijk. De overheid zou dit moeten coördineren. De strijd tegen cybercriminelen is kostbaar, maar ook de politiek moet beseffen dat het niet alleen belangrijk is om de economie financieel te ondersteun tijdens corona, maar dat er ook geld beschikbaar moet zijn om de cybersecurity zeker te stellen!”

Openbaar Ministerie
Valt er voor justitie nog veel te winnen in de strijd tegen cybercriminaliteit? Volgens Gerrit van der Burg, voorzitter van het college van procureurs-generaal en lid van de CSR vanuit de publieke sector, kan in de communicatie tussen OM en het bedrijfsleven nog wel wat worden verbeterd, teneinde de slagkracht in opsporing en vervolging van criminelen te vergroten en ook beter preventief te kunnen optreden. “Als een bedrijf last heeft van cybercriminaliteit zoals ransomware, kan intensieve communicatie met het OM waardevolle informatie opleveren. We leren van elke zaak, omdat we daardoor steeds meer inzicht krijgen in de gebruikte criminele technieken. Als we er niet bovenop zitten, dan blijft deze criminaliteit een verdienmodel.”

De strijd gaat altijd door

De strijd tegen cybercriminelen blijft een voortdurende uitdaging, zegt Van der Burg: “Net als bij de analoge criminaliteit lopen we altijd een stap achter. In de digitale criminaliteit gaat de ontwikkeling alleen veel sneller, en kan een crimineel bovendien de meest ingewikkelde technieken van cybercrime gewoon op het internet kopen. Cybercriminaliteit wordt bereikbaar voor een breed publiek. Dat maakt de uitdaging voor ons nog groter.” De raad is gevraagd het komend kabinet te adviseren over investeringen die nodig zijn voor enerzijds het vergroten van de weerbaarheid en anderzijds het versterken van opsporing, vervolging en berechting. “Weerbaarheid is essentieel, de drempel om dit soort criminaliteit te plegen moet zo hoog mogelijk!” Dit heeft zowel een menselijke als een technologische kant. De technologie moet zorgen voor gedegen veiligheidsmaatregelen, zoals firewalls en een goed wachtwoordbeheer, zodat binnendringen echt moeilijk wordt gemaakt. Voor de sociale kant geldt dat mensen voortdurend alert moet zijn. “Die alertheid geldt natuurlijk ook voor bedrijven. Vooral kleinere, kwetsbare bedrijven die moeite hebben om in de coronatijd sowieso overeind te blijven moeten goed opletten!” Hiervoor is ook voor het OM dringend geld en aandacht nodig van de politiek. “Langs de hele linie, vanaf preventie en weerbaarheid tot en met het onschadelijk maken van dreiging, de opsporing en de vervolging, moeten wij zodanig zijn uitgerust dat we onze tanden kunnen laten zien.”

Digitale oplossingen

De digitale ontwikkeling zelf biedt ook mogelijkheden om cybercriminaliteit op te sporen. Met data science kunnen bijvoorbeeld verdachte transacties bij banken op heel geavanceerde manier worden opgespoord. Peter de Kock, Professor of Practice aan de Jheronimus Academy of Data Science, legt uit waarom: “Waar mensen historisch slecht in zijn is dingen onthouden en dingen berekenen. Data science doet dat juist perfect. Datatechniek kan heel snel heel veel gegevens raadplegen, onthouden en vastleggen en kan daardoor heel snel, en objectief, afwijkingen in een dataverzameling naar boven halen. Een analist of rechercheur zou dat niet lukken. Waar mensen wel goed in zijn, en machines juist slecht, is het duiden van die informatie. Het bijeenbrengen van ogenschijnlijk ongerelateerde data kan tot verrassende resultaten leiden waar de analist zelf nooit op zou zijn gekomen. De analist kan besluiten om die resultaten verder te gaan onderzoeken, of niet.”

Combinatie van mens en machine

Als voorbeeld noemt De Kock het opsporen van verdachte transacties bij een bank. De verzamelde transacties vormen een dataset, ze leveren een schat aan informatie. “Het gaat om zoveel informatie, dat het voor een mens onmogelijk is om daar verdachte patronen in te ontdekken. Met data science kan dat wel, het legt relaties tussen transacties waar nooit iemand bij heeft stilgestaan. Het is aan de mens om die relaties te duiden. De combinatie van mens en machine maakt dat we cybercrime steeds voortvarender kunnen aanpakken.”