Bedreiging of incident

De Wannacry ransomware en de pseudo-ransomware Petya maakten het onderwerp cybersecurity aan het begin van deze zomer weer 'lekker actueel'. Heel vervelend voor de getroffen bedrijven, maar nauwelijks reden tot brede paniek, vindt Hafkamp. Tot incidenten bij Nederlandse banken hebben beide aanvallen ook niet geleid. Rabobank houdt dat soort ontwikkelingen goed in de gaten met eigen cybersecurity intelligence. Die beantwoordt relevante vragen door met getroffenen te spreken, zich een beeld van de bronnen te vormen en informatie te duiden.

Hafkamp vertelt om wat voor soort vragen het gaat: 'Waarom is het gebeurd? Waar is het gebeurd? Zijn we zelf doelwit geweest en zijn we kwetsbaar? Is het incident bedreigend voor eigen processen en diensten? In welke bredere ontwikkeling van cybersecurity kun je de incidenten plaatsen? Een dergelijke inschatting van de situatie maakt het ons mogelijk om te anticiperen op veranderingen in cybersecurity, om ontwikkelingen te herkennen en om er deels eigenhandig en deels samen met anderen antwoorden op te formuleren.'

Strategische samenwerking

De wereld verandert en gezamenlijke afstemming op het gebied van cybersecurity is één van die veranderingen, aldus Hafkamp. 'Zo zijn we onlangs met ING, ABN AMRO en TNO in een samenwerking voor wetenschappelijk (middel)langetermijndenken over cybersecurity gestapt. Dat is een doorbraak. Bedrijven hebben een behoefte aan strategische oplossingen voor de toekomst en co-creatie met leveranciers. Dat vraagt een zekere mate van openheid die zich zal uitbetalen. Veel bedrijven zijn nog niet bereid tot die relatieve openheid.'

Het draait bij de samenwerking niet om het maken van direct bruikbare veiligheidsproducten. 'Maar het zou fijn zijn als de samenwerking wel halffabricaten kan opleveren die we tot eigen eindproducten kunnen uitwerken,' merkt Hafkamp op. 'Denk bijvoorbeeld aan toepassingen op het gebied van authenticatie van klanten of aan monitoring om met big data-achtige technieken anomalieën in de datastromen te achterhalen.'

POORTEN OPEN VOOR BETERE BEVEILIGING

Chief Information Security Officer Wim Hafkamp van Rabobank Nederland is niet pessimistisch over cybersecurity. Samenwerking met collega-bedrijven en kennisinstellingen zal zich voor de middellange termijn uitbetalen in oplossingsrichtingen, denkt hij. 'Een belangrijke belemmering is wel dat onderzoekers graag met echte data willen werken, terwijl bedrijven die niet prijs kunnen geven. Het zou mooi zijn als daar een model voor kwam.'

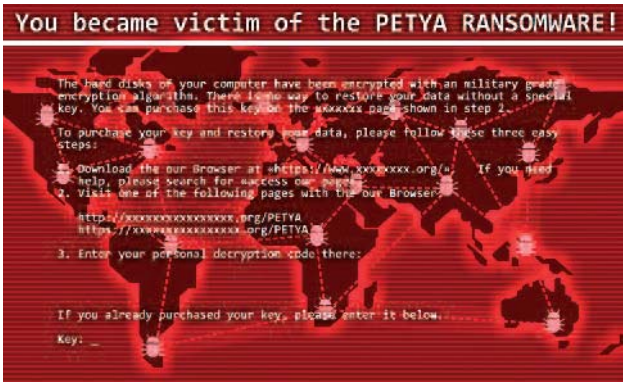
Door Leendert van der Ent
Foto's Sjoerd van der Hucht, Shutterstock

Cybersecurity onderzoeksagenda

Hafkamp is daarnaast als voorzitter van de adviesraad betrokken bij dcypher, het Dutch cybersecurity platform higher education & research. Dit publiek-private platform is verantwoordelijk voor een nog breder initiatief, de Nationale Cyber Security Research Agenda. De tweede versie daarvan, die dateert uit 2013, loopt inmiddels af. 'De NCSRA II heeft een paar aardige spin-offs opgeleverd. De vraag of de agenda de cybersecurity daadwerkelijk op een hoger plan heeft gebracht laat zich lastig beantwoorden. Zowel de good guys als de bad guys zijn tenslotte voortdurend in beweging. Nieuwe technologische ontwikkelingen kunnen ons helpen en hebben tegelijk bedreigingen in zich. Het is nooit anders geweest. Ik ben daar niet pessimistisch over.'
Het is daarbij volgens Hafkamp goed dat er coördinatie plaatsvindt: 'Ik vind de komst van een derde versie van de NCSRA dan ook zeer wenselijk. Een nieuwe versie zal wel een iets andere insteek krijgen. De huidige negen onderzoeksthema's zouden misschien plaats kunnen maken voor een meer sectorgerichte aanpak. Een goede aansluiting bij bedrijfssectoren, bij de topsectoren en van daaruit bij de Europese Researchagenda is belangrijk.'
In de tweede versie hadden de technische domeinen de overhand, constateert Hafkamp. 'Misschien is cybersecurity in de gamma-wereld onvoldoende bekend. Het is tijd om dat recht te zetten. We zoeken nog goede bouwstenen voor de NCSRA III. Het is in elk geval duidelijk dat privacy, artificial intelligence, Internet-of-Things en big data er prominente plekken in verdienen.'

Uitdagingen

Er is al met al een tendens naar meer samenwerking in cybersecurity: tussen bedrijven en met kennisinstellingen en toeleveranciers. Helemaal zonder uitdagingen is een dergelijke samenwerking niet, benadrukt Hafkamp. 'Het moeilijkste is niet om systemen dicht te timmeren. De uitdaging is juist om de benodigde beveiliging in systemen zo aan te brengen, dat het gebruiksgemak van klanten en medewerkers er niet onder lijdt. Nieuwe oplossingen moeten de tevredenheid van de mensen die ermee werken verhogen, en dat in een aanvaardbare balans met de kosten. Dat perspectief moet voor onderzoekers helder zijn.'
Een tweede probleem is dat onderzoekers snakken naar klantdata om goede oplossingen te kunnen ontwikkelen. Ondertussen zijn



'Openheid zal zich uitbetalen'

bedrijven onder andere vanwege privacyregels gedwongen daar uiterst terughoudend mee om te gaan. Hafkamp: 'Beide standpunten zijn begrijpelijk. Om verder te komen moeten er werkbare compromissen komen. Nu moet je elke keer door een moeizaam juridisch traject dat projecten afremt. Anonimiseren van data is een mogelijkheid, maar gaat veel te langzaam. Het zou mooi zijn als er een gestandaardiseerd model zou kunnen komen om daar mee om te gaan. Dat zou de ontwikkeling flink kunnen versnellen.'

De koppelingen tussen de Rabobank en de onderzoekswereld zijn de laatste jaren flink gegroeid. 'We zijn bijvoorbeeld ook actief in een wereldwijd Startup Bootcamp op het gebied van cybersecurity. Regelmatig vormen promovendi startups, waarmee wij vervolgens in zee gaan. Zij hebben behoefte aan launching partners, wij hebben behoefte aan veiligheidsoplossingen. Daar vinden we elkaar.'