INTERVIEW MET NICK EBELS
DOOR PAUL JURRIENS
FOTOGRAFIE BERT JANSSEN

Voor CIO Nick Ebels van PGGM heeft cybersecurity topprioriteit

‘Zorg dat de binnendringer niet ver komt’

Cybercrime heeft zich ontwikkeld tot een uiterst professionele en lucratieve industrie met gespecialiseerde bedrijven. Voor grote financiële instellingen heeft cyberveiligheid dan ook topprioriteit. “Je kunt hacks echter nooit 100% weren”, stelt CIO Nick Ebels van PGGM. “Maar je kunt met mitigerende maatregelen de impact ervan wél zo klein mogelijk houden.”

Het was een van zijn eerste acties, nadat Nick Ebels oktober 2021 in dienst was gekomen bij PGGM. En nog steeds krijgen de medewerkers elke maand een of twee steeds complexere phishing mails. Zo test PGGM of werknemers nog voldoende digitaal alert zijn en niet impulsief via een aangeklikt linkje naïef in de fuik lopen van een cybercrimineel. Mede dankzij de trainingsmailtjes blijven ze zich bewust van de cybergevaren die elke dag op de loer liggen.
“Het liefst wil je dat mensen aan ons rapporteren dat ze een vreemd mailtje hebben ontvangen. Als dat in korte tijd een stuk of tien keer gebeurt, is dat voor ons een signaal om de e-mail te verwijderen, zodat anderen er niet meer in kunnen trappen. Ik vind de testmailtjes een van de meest waardevolle investeringen in cybersecurity ooit. Niet duur en gewoon leuk om te doen.”
Ebels nam de gewoonte mee van Nationale-Nederlanden. De laatste twee jaar van zijn loopbaan daar was hij chief information security officer. “Ik ben bij PGGM gaan werken omdat er in hoog tempo veel gaat veranderen in de pensioenwereld. De nieuwe pensioenregels voorop. De lat voor grote financials gaat op alle gebieden steeds hoger liggen. Denk maar aan wetgeving, kwaliteit van dienstverlening én security. Een leuke uitdaging.”

DRIE SOORTEN

Cybercrime staat bovenaan in het lijstje van de non-financial risico’s, zoals brand. Ebels onderscheidt voor financiële instellingen, zoals pensioenfondsen en verzekeraars, drie soorten cybercrime risico’s.
“De meeste impact hebben de operationele risico’s. Dan draait bijvoorbeeld de IT van een bedrijf kapot door ransomware (gijzel-software, red.). Als dat enkele weken niet werkt, is dat een groot risico in de bedrijfsvoering. Het tweede risico is reputatieschade. Zoals een datalek waardoor informatie op straat kan komen te liggen. Het lek ligt bij de provider, maar onze naam is eraan verbonden. Het financiële risico is het derde en laatste. Bij ons moet je dan geld weg frauderen, ofwel naar de rekening van de klant overmaken. Dat is best complex. Mijn aandacht gaat het meest uit naar operationele risico’s.”

Wat is daarbij jouw grootste uitdaging als CIO?
“De risicobeheersing versus de technische dreiging. Die werelden moeten dichter bij elkaar komen. DNB houdt toezicht op de risicobeheersmaatregelen. Maar hoe je het technisch hebt ingeregeld, is een heel ander niveau van discussie.”

24/7 SERVICEDESK

De jaarlijks economische schade door cybercrime loopt in de miljarden euro’s. Dagelijks worden er organisaties door getroffen. Bij cyber-criminaliteit gaat het om een uiterst professionele en lucratieve illegale ‘bedrijfstak’ met een keten vol specialisten die diensten leveren aan

NICK EBELS: “ER IS SPRAKE VAN EEN SUPERSNELLE TECHNISCHE INNOVATIE EN VAKKUNDIGHEID.”

elkaar. Zoals criminelen die alleen maar toegang proberen te verkrijgen tot een organisatie en de toegangsgegevens vervolgens verkopen aan hackers, die weer gespecialiseerd zijn in het verder binnendringen in het bedrijf. Of een 24/7 bereikbare servicedesk die uiterst klantvriendelijk losgeld lospeutert van getroffen partijen, inclusief kortingen.

JE KUNT NOOIT GARANDEREN DAT ER NIETS GEBEURT

Ebels: “Er is sprake van een supersnelle technische innovatie en vakkundigheid. Zo wordt tegenwoordig ransomware bijna altijd gecombineerd met data-exploitatie. Dus de data stelen en die dreigen te publiceren. Want de meeste grote bedrijven hebben intussen hun back-up wel zodanig op orde dat een ransomware niet meer het einde van het bedrijf betekent. Weliswaar is het heel vervelend dat je er één à twee weken uitligt, maar je komt wel weer terug. Waarom zou je dan miljoenen gaan betalen? De paar dagen die je later in de lucht bent, neem je dan voor lief. Maar als gevoelige data publiek worden gemaakt op websites die daarvoor zijn ingericht, loop je reputatieschade op. Je wilt voorkomen dat iedereen de gegevens van je pensioendeelnemers kan inzien.”

Websites die daarvoor zijn ingericht?
“Inderdaad, als een organisatie niet betaalt, dan worden haar data op een zogeheten leak site gezet, waar iedereen ze kan downloaden.”

TE COMPLEX

Inmiddels hebben organisaties zich op allerlei manieren gewapend tegen cybercriminaliteit. Enerzijds om deze buiten de deur te houden. Anderzijds om de gevolgen van een eventuele hack te verzachten – te mitigeren.
Ebels: “Je kunt hacks nooit helemaal weren. Daar is IT te complex voor. Je hebt zoveel verschillende manieren om ergens binnen te komen. En elke dag komen er nieuwe bij. Software is bovendien niet foutloos. Als iemand een onbekende bug ontdekt, houd je een hack niet tegen. Er zijn heel veel van zulke unknown unknowns. Je kunt dus nooit garanderen dat er niets gebeurt, tenzij je ganzenveren en papier gaat gebruiken.

Waar tegenhouden een illusie is, kun je de impact van hacks wel zo klein mogelijk houden. We hebben best veel mitigerende maatregelen om robuuster een aanval te kunnen opvangen. Bijvoorbeeld door binnendringers eerder te zien en door ons netwerk in stukjes te hakken. Gevoelige systemen, zoals onze betaalstraat, zijn extra zwaar beveiligd. Verder oefenen we met een crisisteam, bijvoorbeeld twee weken zonder IT. Redden we dat? Kunnen we dan nog pensioenen uitkeren? In dergelijke scenario’s steken we best veel oefentijd.

Zorg dus, naast de dijk aan de buitenkant, dat de binnendringer niet ver komt. Er is een ‘defense in depth’, met meerdere lagen van beveiliging. Daardoor kan de hacker niet makkelijk ongemerkt doordringen én blijft de impact dus beperkt. Anderzijds, als het in het ergste geval uiteindelijk toch helemaal misgaat: zorg dat je de recovery goed op orde hebt en dus de boel kunt herstellen.”

Kun je in die periode van enkele weken de pensioenen inderdaad uitbetalen?
“Pensioenen veranderen van maand op maand niet veel. Je kunt daarom bij een hack dezelfde bedragen uitkeren als een maand eerder. Dat probleem is te overzien. Veel minder erg dan dat je geen enkel pensioen kunt uitkeren.”

Werken jullie ook samen met andere financiële instellingen?
“Ja. Zo faciliteert DNB het programma Tiber waarin financials ervaringen delen. In Tiber vraag je een externe partij om bij jou in te breken. De lessen daaruit deel je met elkaar. Dan zie je dat we vaak soortgelijke problemen hebben. Dat helpt enorm.

We hebben ook meerdere overlegvormen. Wat zien we nou en wat leren we van elkaar? Super interessant zijn wereldwijde groepen. Wat zien zij? Want dat komt later onze kant op. Welke maatregelen werken en welke niet? En wat kunnen wij met onze IT-omgeving het beste doen?

Het meeste nut heeft de schaal van de cloud van grote leveranciers. Zo kijkt een Security Operations Center SOC 24/7 of er in ons netwerk rare dingen gebeuren. Voor een dergelijk en dermate specialistisch vakgebied heeft PGGM de schaal niet. We hebben dit dan ook uitbesteed aan FOX-IT. Het maakt op wereldniveau deel uit van het Engelse NCC. Dat leert weer van alles wat het ziet bij klanten. Dat levert voor ons veel voordeel op. Hetzelfde geldt voor Microsoft. Als dit met bepaalde software bijvoorbeeld een aanval ergens in Zuid-Amerika detecteert, profiteren wij daar ook van.”

HET LIJKT ME VOOR EEN ACTUARIS BEST TRICKY OM EEN CYBERRISICOVERZEKERING TE ONTWERPEN

WAPENWEDLOOP

Inmiddels vindt er een ware wapenwedloop plaats tussen steeds professionelere criminelen met gespecialiseerde dienstverlening en grote externe providers, zoals Microsoft en NCC. Daarbij is sprake van ‘haasje over’. Een nieuwe aanval wordt steevast gepatcht, gerepareerd. Ebels: “De afgelopen maanden zie je echter steeds vaker en serieuzer dat criminelen overheidsdiensten aanpakken. Bijvoorbeeld een oliepijplijn in de VS, een ziekenhuis of waterzuivering. Dit raakt de nationale belangen en veiligheid. Maatschappelijk onacceptabel. Overheden reageren daar niet alleen op, ze pakken steeds actiever en agressiever grote groepen aan. En andere landen. Ze gaan in de tegenaanval. Nederland loopt daarin voorop, met onder meer de VS, Engeland en Australië. Overheden mogen ook veel meer dan bedrijven, zoals terug hacken.”

Waar staat cybercrimerisico momenteel in het rijtje met pensioenrisico’s, zoals langleven en markt/rente?
“Die laatste zijn financiële risico’s. Cybercrime is een operationeel risico. Dat is – met mensenwerk aan twee kanten – veel dynamischer, ingewikkelder én lastiger af te dekken omdat het slecht grijpbaar is. Zo lijkt het me voor een actuaris best tricky om een cyberrisicoverzekering te ontwerpen. Een worsteling. En als door een geavanceerde hack al onze data weg zijn, inclusief back-ups, kunnen we de deur wel sluiten. Met al onze maatregelen is de kans daarop weliswaar miniem, maar niet nul.”

Ligt daar een groeiend werkterrein voor actuarissen?
“Er is veel vraag naar actuarissen die de securitytechniek begrijpen. Er ligt een potentieel supergrote markt in cyberverzekeringen voor bedrijven. Het gaat om een onzekere gebeurtenis. En een groot aantal bedrijven kan een extreme vorm ervan niet overleven. Dat klinkt als iets waar je een verzekering voor af zou willen sluiten. Het ingewikkelde is dus hoe je die prijst. Dat is het vakgebied van de actuaris.”

HET NADEEL VAN CYBERSECURITY IS DAT HET NIET ZICHTBAAR IS

Je kunt de verzekering ook koppelen aan nadere beveiligingsmaatregelen.
“Dat gaat zéker helpen. Maar dit is nog geen goed doorontwikkeld vakgebied. Je moet sterk in de details duiken om te weten of de – afgesproken – veiligheidsmaatregelen zodanig goed in elkaar zitten dat ze een lager cyberrisico opleveren. Het gaat erom hoe je deze details inregelt om korting op je verzekeringspremie te krijgen.

Het nadeel van cybersecurity is dat het niet zichtbaar is. Het is duur, met tools en mensen, en zolang het goed gaat, heb je het niet nodig. Maar als het misgaat, is het te laat. Zo’n verzekering kwantificeert de kosten voor dat geval. Dan betaal je dus de hoofdprijs zonder afdoende maatregelen. De maatregelen maken het goedkoper. Wel een rare omweg om de kosten van nietsdoen in te prijzen. Er zijn tevergeefs meerdere pogingen gedaan om de financiële impact van een cybersecuritysysteem objectief vast te stellen. Daar zouden actuarissen en econometristen best in kunnen helpen.”

Ligt er ook een particuliere markt in het verschiet?
“De vraag is wat je verzekert als al jouw privédata weg zijn. De bank regelt een en ander voor jou, dus daar ligt geen probleem. Maar je privéfoto’s? Moet je daarvoor 200 of 1.000 dollar betalen? Betaal je die dan niet liever om daarna wél een back-up te maken van de teruggekregen foto’s? Daar heb je geen verzekering voor nodig. En wat heb je aan een verzekeringsuitkering? Je dierbare foto’s krijg je er niet mee terug. En als je al een back-up hebt: wat is dan je risico? Ik denk dat je het beste een aantal basismaatregelen kunt nemen in plaats van een verzekering.”

Wat nog meer dan een back-up maken?
“Gebruik de genoemde passwordmanager, zodat je overal een uniek complex password hebt. In combinatie, als het even kan, met een multi factor authenticatie. Daarbij moet je op meerdere manieren verifiëren om toegang te krijgen tot applicaties en accounts. Bijvoorbeeld met een code. Zo wordt het gebruikersaccount extra beveiligd. Als je password dan toch wordt gelekt, kunnen criminelen niet die code krijgen. Je kunt het password ook koppelen aan biometrische identificatie. Zorg ook dat je operation systeem regelmatig een update krijgt. Nooit Windows updaten is vragen om problemen. Microsoft heeft overigens standaard antivirus. Daar hoef je geen extra beveiliging naast te nemen. Tot slot: denk gewoon na bij de mailtjes die je krijgt.”

Het valt nogal eens op dat specialisten in cyberveiligheid sporadisch aanwezig zijn op internet. Bij jou kom ik niet verder dan LinkedIn en een interview voor het Verbond van Verzekeraars. Om veiligheidsredenen?
“Nee hoor. Alleen Facebook is een bewuste keuze geweest. Social media zijn sowieso niet mijn ding. Het is veel ‘mooi maken’. Bij LinkedIn begrijp ik dat nog wel, in het kader van de arbeidsmarkt-communicatie: nuttig voor bedrijf en carrière.” ■

Nick Ebels (53) is sinds oktober 2021 chief information officer bij pensioenuitvoeringsorganisatie PGGM. Daarvoor, vanaf 2006, bekleedde hij diverse functies bij Nationale-Nederlanden en (eerder) ING. Zijn laatste functie bij de verzekeraar was chief information & security officer. Voor 2006 was Ebels tien jaar senior manager bij Accenture. Nick Ebels heeft bestuurlijke informatica gestudeerd aan de Erasmus Universiteit Rotterdam.