Cybercrime: de digitale snelweg als breekijzer

Het is een groeiend maatschappelijk probleem: cybercrime. Iedereen krijgt ermee te maken, thuis of bij bedrijven en instellingen. Het digitale monster is al een tijdje wakker, nu de samenleving nog: „We móeten bang zijn voor internetcriminelen."

TEKST ILLUSTRATIES BENTI BANACH EN MARCO VAN KAMPEN

Pling! Een mailtje ploft in de inbox van een medewerker van een klein boekhoudkantoor in Noord-Limburg. We noemen hem voor het gemak Hans. In de naam van de afzender herkent hij een vaste klant. Het gaat om een te hoog opgegeven factuurbedrag, zo maakt Hans op uit het onderwerp. Hij opent het bericht. De afzender verwijst voor meer details naar een linkje, waar Hans nietsvermoedend op klikt. Een paar minuten later heerst er in het doorgaans zo serene kantoor een paniekerige sfeer. Alle bestanden in het systeem zijn plotseling vergrendeld. Niemand krijgt het voor elkaar om ook maar één document te openen. De pc's gaan op zwart. Hans kijkt hulpeloos om zich heen. Wat is er in hemelsnaam gebeurd? Dan verschijnt er een mededeling op zijn scherm. De vergrendeling kan worden opgeheven, luidt de boodschap. Op voorwaarde dat het bedrijfje 15.000 euro in bitcoins overmaakt.
Het geschetste boekhoudkantoor, waarvan we de naam om privacy-redenen niet noemen, is een van de vele bedrijven die het slachtoffer zijn geworden van gewiekste cybercriminelen. Onzichtbare vijanden die geen pistool of mes nodig hebben om te stelen, dreigen of chanteren, maar enkel digitaal geweld toepassen. Cybercrime kent vele gedaanten. Phishing, hacking, DDoS-aanvallen, malware, cryptojacking (zie kader): het is slechts een kleine greep uit een lange lijst van varianten van computercriminaliteit. Het zijn termen waar de man op straat nog steeds weinig mee kan. Als er een gebouw in brand staat, gaan alle alarmbellen af. Wordt 112 gebeld. En als iemand wordt geconfronteerd met een steekwapen, springt hij in de gordijnen en schreeuwt om hulp. Maar als 23 scholen platliggen vanwege een aanval van ransomware, heeft dat veel minder attentiewaarde. Het is nog te abstract. Digitale delicten blijven zodoende vaak onder de radar. Cybercriminelen opereren op kousenvoeten. Om in te breken op een server of computer hebben ze geen koevoet nodig en gijzelsoftware wordt geplaatst zonder bloedvergieten. Het is moeilijk te vatten voor de buitenstaander. Het is onzichtbaar. Niet tastbaar. Het geruisloze karakter van cybercrime bedient de digitale delinquenten dubbel: niet alleen zijn ze zo moeilijk te traceren, het zorgt ook voor schromelijke onderschatting van een maatschappelijk probleem dat almaar groeit.
Vorig jaar werd er in Nederland 4650 keer aangifte gedaan van cybercrime, een stijging van 64 procent ten opzichte van het jaar ervoor. Het aantal aangiftes blijft echter ver achter bij de hoeveelheid slachtoffers. Dat zat vorig jaar tussen de een en anderhalf miljoen. Hoe dat kan? Sommige mensen weten niet dat ze slachtoffer zijn van cybercrime, soms wordt het delict geregistreerd als 'afpersing'. Dit terwijl het ook een digitale component bevat en bij een hoop gevallen die bij het Centraal Bureau voor de Statistiek (CBS) onder 'cybercrime' vallen, zoals cyberpesten en bedreiging via internet, het nutteloos wordt geacht aangifte te doen bij de politie. Maar er speelt ook iets anders mee: schaamte. Met name bij MKB-bedrijven, een kwetsbaar en daardoor gewild doelwit van computercriminelen, is de aangiftebereidheid laag omdat ze vrezen voor reputatieschade. Ze zijn bang om het imago te krijgen van onderneming die haar zaakjes niet op orde heeft als uitlekt dat ze het slachtoffer waren van internetmisdadigers. En dus houden ze het liever onder de pet. Cybercrime wordt weggekeken. De enorme discrepantie tussen het aantal slachtoffers en het aantal aangiftes geeft dat eens te meer aan. Het digitale monster is al een tijdje klaarwakker, maar een groot deel van de samenleving verkeert nog in snooze-modus.

Digitale opsporing

In Den Haag lijkt het kwartje inmiddels gevallen. Zo maakte plaatsvervangend korpschef Henk van Essen vorig jaar bekend dat de capaciteit van de cybercrimeteams wordt verdubbeld met 145 fulltime medewerkers. Het feit dat de regering bereid is hierin te investeren, illustreert dat ook de politiek computercriminaliteit nu als serieus probleem erkent. Schoorvoetend, dat wel. Want eigenlijk is nog veel meer nodig met het oog op de toekomst, zo voorspellen insiders. De genoemde cybercrimeteams herbergen agenten die ervoor getraind zijn om onder meer DDoS-aanvallen, ransomware en hacks te bestrijden. Digitale rechercheurs. Ook de eenheid Limburg beschikt over zo'n brigade van specialisten. Twintig stuks, om precies te zijn. Van hen wordt een andere manier van werken gevraagd. Dat geldt op den duur ook voor de agenten buiten deze teams. De dienders in de wijk moeten evenzeer in de leer. Straks behoort het opsporen van cybercriminelen en alles wat daarbij hoort tot de basisvaardigheden. Maar voor het zover is, zijn we alweer een paar jaartjes verder. „De rol van de politie bij een steekincident is duidelijk", zegt analist

cybercrime Joke, die niet met haar achternaam in de krant wil. „Als het om internetcriminaliteit gaat, moet nog een hoop worden uitgekristalliseerd. Iedereen doet aan schiettraining maar de helft heeft nog nooit onderzoek op sociale media gedaan. We zijn nu die omslag aan het maken. Ja, voor sommigen is dat lastig. Maar ze moeten toch mee. Steeds meer bewijs is immers digitaal te vinden." Joke noemt het project Korenwolf. Een training waarbij agenten een fictieve casus voor de kiezen krijgen over een door cybercriminelen afgeperste directeur. De cursisten worden onder meer geconfronteerd met bitcoinsporen en het uitlezen van telefoonrapporten, zaken die ze in het digitale tijdperk steeds meer tegenkomen. De cybercrimeteams lopen voorop in de inhaalslag die de politie te wachten staat. Het verdubbelen van de capaciteit was welkom, aldus Rob van Kan, sectorhoofd Dienst Regionale Recherche van de politie Limburg. „Hoewel provinciale cijfers ontbreken, zien we een grote toename in het aantal cybercrime-delicten. Als je praat met de mensen op straat, merk je dat bijna iedereen er wel eens mee te maken heeft gehad. Bij cybercrime denkt men vaak aan grote hacks of aanvallen. Maar in de dagelijkse praktijk hebben we heel veel te maken met nepmails om geld over te maken naar een onbekende bankrekening of creditcardfraude. Ook daar zie je dat schaamte een grote rol speelt bij de keuze om geen aangifte te doen. Al deze gevallen vormen samen een *dark number*."
Dat niet iedereen staat te springen om zich te melden bij de politie, constateert ook Georges van den Eshof. Hij is officier van justitie van het Openbaar Ministerie in Limburg en sinds 2008 gespecialiseerd in cyberzaken. Van den Eshof doet het ingewikkelde werk. Hij maakt deel uit van het landelijke overleg van cyberofficieren en is ook vertrouwd met cybercrime op het allerhoogste niveau: als landen elkaar aanvallen. Aangifte doen is nooit zinloos, vindt hij. „Wij kunnen helpen om te kijken of er niet toch sleutels zijn om de boel bij een hack weer te ontgrendelen. Soms is die gewoon voorhanden. Maar ook als dat niet het geval is, heeft melden zin. Door te registreren kunnen we het fenomeen ook inzichtelijk maken. Ik denk dat we nu enkel het topje van de ijsberg zien. Ik snap het wel, hoor. Slachtoffers zijn altijd mensen die erin tuinen. Als een cybercrimineel via Nigeriaanse scams – de zogeheten 419-fraude - gaat bedelen, zijn er mensen die dan blind 60 mille overmaken. Grote bedrijven hebben de middelen om ict-ers in te schakelen. Familiebedrijven zijn typische slachtoffers, die betalen vaak meteen bitcoins en doen dan geen aangifte. Dat is immers slechte PR. De kans bestaat echter ook dat je losgeld betaalt en geen sleutel krijgt."
Soms moet er iets ergs gebeuren om de ernst van een probleem in te zien. Het befaamde verdronken kalf. De cyberhack bij de Universiteit in Maastricht van afgelopen december lijkt dat effect te hebben. De instelling werd gegijzeld door, vermoedelijk, Russische cybercriminelen die het systeem platlegden. Ze koos uiteindelijk eieren voor haar geld. De UM betaalde een slordige twee ton voor de sleutel die de hack ongedaan maakte. Een megabedrag. Maar liever dat dan weken- en misschien wel maandenlang uit de lucht zijn, zo werd beredeneerd. Het was niks minder dan een regelrechte ramp voor het UM. Én slechte public relations.
Echter, in plaats van het dood te zwijgen, trad de universiteit naar buiten. Sterker nog, ze organiseerde een uitgebreid symposium, met tweehonderd gasten uit alle windstreken, waarin alles uit de doeken werd gedaan. De toehoorders leerden over de modus operandi van de hackers, over de fouten die werden gemaakt door de UM zelf en over de lessen die eruit zijn te trekken voor de toekomst. De UM gaf zo niet alleen inzicht in de manier waarop doorgewinterde cybercriminelen werken, ze hielp zo ook een discussie over cybercrime op gang. Een belangrijke boodschap was dat iedereen dit kan overkomen. Niet alleen het sympathieke eenmansbedrijfje dat geen middelen heeft om zijn onderneming afdoende digitaal te beveiligen, maar ook een gerenommeerd instituut met knappe koppen als de Universiteit Maastricht, waar dagelijks 19.000 studenten worden klaargestoomd voor de toekomst. Zoals ook Hans van het boekhoudingskantoor inmiddels weet: je bent maar één onachtzame muisklik verwijderd van een cyberhack. Zo gebruikte de UM haar eigen tragiek om een belangrijk statement te maken.
Rob van Kan prijst de strategie van de UM. „Voorlichting is belangrijk bij de bestrijding van computercriminaliteit. Preventie is één van de kerntaken van het cybercrimeteam. En de universiteit heeft op deze manier een grote groep kunnen waarschuwen. Draai je updates! Sluit je digitale poorten! Ook als politie hebben we veel van deze hack geleerd."

Wake-upcall

John Bloebaum, specialist Intelligence bij de politie Limburg, sluit zich daarbij aan. ,,Dit draagt bij aan het grote besef dat nog moet komen. Het gebeurt hier ook. Dit is een wake-upcall voor andere bedrijven of instellingen."
Korpschef Eric Akerboom van de Nationale Politie omschreef het treffend: „Je bent een sukkel als je op de traditionele wijze inbreekt. Op de digitale manier verdien je meer en is de pakkans kleiner. Als je het goed aanpakt, laat je bijna geen sporen achter.'' Het bestrijden van cybercrime lijkt soms wat weg te hebben van een kat- en muisspel. Met de politie en justitie die spoken najagen, constant achter de feiten aanhollen. En de internetcriminelen als kwaadaardige genieën die hun opponenten telkens weer een stapje voor zijn. Volgens officier

van justitie Van den Eshof is het echter niet zo zwart-wit. „Wat preventie betreft zitten we op het goede spoor. Zo is er de bewustwordingscampagne 'Laat je niet hack maken' en loopt in Limburg het project Risk Factory, ook met het oog op scholieren. Maar de alertheid is nog niet groot genoeg. We moeten nóg meer doen aan preventie en opsporing. Volgens afspraak is 30 procent van alle zaken die ik draai gerelateerd aan cyber. Dat percentage mag wat mij betreft best wat hoger gezien het groeiende aanbod. Hoe ik een zaak aanpak? Het cybercrimeteam van de politie belt mij over een aangifte. Dan regelen we een huiszoeking en nemen we gegevensdragers in beslag. Soms doen we een telefoontap of een internettap. Je vraagt gegevens op van bijvoorbeeld een kluizenbedrijf. En je vraagt je altijd af of je de verdachte meteen oppakt of dat je zo veel mogelijk gegevens wil verkrijgen. Onze manier van werken heeft al regelmatig wat opgeleverd."

wraakporno

Een goed voorbeeld is hoe de politie ooit de zogenaamde 'Hansa market' overnam, een drugsmarkt op het darkweb, en wekenlang meekeek met criminelen. Of hoe ze erin slaagde om talloze versleutelde berichten op de PGP-smartphone van topcrimineel Ridouan Taghi te ontcijferen. Zelf boekt Van den Eshof ook regelmatig succesjes. Zijn grootste vangst deed hij twee jaar geleden. „Hackers braken in op een iCloud met pikante foto's. Ze ontmoetten elkaar op een Russische server voor wraakporno. We hebben het IP-adres nagetrokken, die draaide op een dataservicebedrijf in Wormer. Dat is een fabriek met alleen maar servers. We hebben de harde schijven van die servers in beslag genomen. De zaak had grote impact. Toen alles voorbij was, kreeg het team ontzettend veel bedankbrieven van slachtoffers."

Er is niettemin nog een hoop terrein te winnen, geeft ook politieman Van Kan toe. „Soms loop je tegen wetgeving aan die nog niet is toegerust op de laatste ontwikkelingen. Dan moet je de randjes opzoeken en soms over grenzen heengaan. Zo help je ook de jurisprudentie." Bij cybercrime speelt bovendien nog een gecompliceerde geografische component. Een Limburger kan hier aangifte doen, terwijl de bron van het delict in Panama zit. Van den Eshof: „Veel wetgeving wordt één op één uit de analoge naar de digitale wereld geprojecteerd. Eigenlijk zou er zoiets als recht voor cyberspace moeten bestaan."

Volgens de officier van justitie staat Nederland er goed voor op het gebied van digitale beveiliging. „We behoren tot de wereldtop en daar ben ik wel trots op. De infrastructuur hier is heel goed maar dat werkt soms ook tegen ons. Cybercriminelen profiteren daar immers ook van. Tevens een nadeel: we spreken goed Engels. Indiërs die internetfraude willen plegen zullen niet snel naar Frankrijk te bellen."

Waar de opsporingsdiensten steeds meer expertise vergaren en meer middelen ter beschikking hebben om internetbandieten het hoofd te bieden, gebeurt dat andersom ook. De gemiddelde cybercrimineel is allang niet meer die puisterige puber die vanaf zijn zolderkamertje gniffelend inbreekt op andermans computer om daar op een hackersforum met andere nerds over te pochen. Hij schiet niet langer met hagel in de hoop iets per ongeluk te raken, maar vuurt steeds gerichter op kwetsbare slachtoffers. Het digitale kwaad is in rap tempo geëvolueerd. De grappenmaker achter zijn toetsenbord is een professional geworden, als we Wilfred van Roij mogen geloven. En hij kan het weten als mede-eigenaar van het Horster bedrijf Digitale Opsporing, een recherchebureau gespecialiseerd in het bestrijden van cybercrime. De onderneming heeft drie takken: digitaal onderzoek, cyber security en opleidingen op het gebied van digitaal forensisch onderzoek en internetveiligheid. De tijd van klunzige mailtjes van Nigeriaanse prinsen die je in gebroken Nederlands proberen te verleiden tot het storten van geld op een bankrekening is inmiddels wel voorbij, stelt Van Roij. „De criminele activiteiten worden steeds geraffineerder uitgevoerd. Neem het nepbericht dat onlangs opdook waarin werd beweerd dat twee medewerkers van een Maastrichts hotel besmet waren met corona. Het leek rechtstreeks van de NOS af te komen, het was bijna niet van echt te onderscheiden. Je kunt het mensen niet eens kwalijk nemen dat ze erop klikken. Iedereen krijgt met cybercrime te maken. Het is allang niet meer de vraag óf maar wannéér."

Chanteren

Volgens Nick Raedts, consultant IT Security & Digital Forensics bij Digitale Opsporing Horst, is het einde van deze professionalisering nog lang niet in zicht. „Er zal steeds meer op de persoon worden gespeeld. Data zijn de nieuwe diamanten. Inactieve websites of sites van failliete bedrijven worden voor een prikkie opgekocht vanwege de data die erop staan. Je ziet nu al dat hackers mensen chanteren met persoons- of bedrijfsgegevens. Dan maakt het niks uit of je een back-up hebt van alle bestanden. Als de hacker eenmaal bij je binnen is, maakt het een kopie van alle gegevens en dreigt die dader vervolgens om privacygevoelige informatie online te gooien."

De Nederlander is extra kwetsbaar voor cybercriminelen, juist omdat we het hier zo goed voor elkaar hebben, stelt Van Roij. „We werken veel vanuit thuis, onze online infrastructuur is goed." Een andere valkuil is gemak, vult digitaal onderzoeker Engelbert van Essen aan. „We maken steeds meer gebruik van domotica, waar criminelen wel raad mee weten. Mensen hebben thuis een

smart-thermostaat, bedrijven beschikken over koffieautomaten die op internet draaien. Het zijn allemaal manieren voor cybercriminelen om hun slag te slaan. Dat maakt het makkelijk om te zien of we thuis zijn of op het werk. Het zijn gevaren die we accepteren, omwille van luxe. Bestellen op Ali Express, je Range Rover op afstand bedienen, camera's, brandmelders: internetcriminelen hebben weinig nodig om in te breken. We zetten de deuren zelf wagenwijd open." Ergo: de dreiging van een cyberhack of ander online delict wordt almaar groter in deze steeds verder digitaliserende maatschappij. De hamvraag: wat kunnen we eraan doen?

Volgens Van Roij, zelf oud-rechercheur, moeten we geen al te hoge verwachtingen hebben van de politie. „Het merendeel van de opsporing is afhankelijk van tips. Ze doen vooral aan cherry picking. Logisch, want ze krijgen veel op hun bordje. Ze hebben te maken met georganiseerde criminaliteit, levensdelicten, drugsbestrijding. Ze zitten in een spagaat. Internet is een specialisme, dat doe je er niet even bij. Ja, ze hebben nu zo'n unit cybercrime. Die kunnen dan bitcoinsporen volgen. Prima, en dan? Het is nog lang niet voldoende. Er lopen rechercheurs rond die niet eens weten hoe social media werken."

Wat dan wel de oplossing is? Het zou al heel wat schelen als er meer aan preventie wordt gedaan, aldus Van Roij. Risicochecks. Testen, testen en nog eens testen. De term ISO 27001 valt. Een keurmerk voor informatiebeveiliging, uitgegeven door vergunningenloket KIWA. „Om zo'n certificaat te verkrijgen, word je gedwongen om je zaakjes op orde te hebben en geef je cybercriminelen geen kans. Grote bedrijven en instellingen maken er al gebruik van." Om überhaupt aan zo'n keurmerk te denken, moet je de dreiging echter wel erkennen. En dat gebeurt vooralsnog te weinig. Van Roij: „Om dit uitdijende probleem het hoofd te kunnen bieden, is gedragsverandering nodig. We móeten bang zijn voor cybercriminelen. Het is er nu eenmaal en het zal elke dag erger worden. In 2017 waren er voor het eerst in de geschiedenis meer digitale delicten dan fietsendiefstallen, maar bijna niemand heeft het erover. Het wordt tijd dat dit thema een gespreksonderwerp wordt op feestjes."

Bemoedigend

Zover is het nog niet. Toch constateert Van Roij wel dat er een kentering gaande is. „We hebben een lijst van bedrijven in de buurt. Die bellen we elk jaar op met de vraag of we een keer langs kunnen komen voor een kopje koffie om te zien of we iets voor elkaar kunnen betekenen. Vijf jaar geleden kregen we nul positieve reacties. Het boeide niemand. Dit jaar gaat de helft van de benaderde bedrijven wél in op die uitnodiging. We worden ons dus steeds meer bewust van de gevaren van cybercrime en dat is bemoedigend."

Terug naar het boekhoudingskantoor van Hans. Nadat alle pc's op zwart zijn gegaan, meldt het bedrijfje zich bij Digitale Opsporing Horst. Helaas, zelfs de whizzkids kunnen er weinig meer aan doen. Het kwaad is al geschied. Wel slagen ze erin middels onderhandelingen het bedrag aan losgeld met een paar duizend euro te verlagen. Van Roij: „De overheid adviseert nooit te betalen, maar die zijn dan volgens mij nog nooit in het bedrijfsleven geweest."

Feit blijft dat het boekhoudkantoor te laat voor hulp op de deur klopte. Je moet die hack juist vóór zijn, is het devies van Van Roij. Negentig procent van ransomware wordt veroorzaakt door een medewerker die argeloos op een linkje in een mail klikt. Ben voorzichtig, ben alert en ben bewust. De bestrijding van de cybercrimineel begint bij Hans.