‘IP-adressen *schaffen we af*, **straks heeft iedereen zijn eigen** *beveiligde stukje* **in de cloud’**

‘Wat heb ik aan *privacy* als ik *dood* ben?’

drs. Pieter Cobelens en Anouk Vos MA MSc

Tekst: Jacques Geluk

‘Cyberspace’, het internet dus, is na grond, water, lucht en ruimte inmiddels een volwaardig vijfde domein. Bij internationale conflicten speelt cyberoorlogvoering een steeds grotere rol. Cybermisdaad bedreigt vooral het bedrijfsleven, maar dat is zich daarvan nog te weinig bewust. Pieter Cobelens (oud-directeur van de Militaire Inlichtingen- en Veiligheidsdienst MIVD en strategisch directeur bij adviesbureau Policy Research Corporation) en Anouk Vos (leider van het PRC-Cyberteam) maken, ook tijdens gezamenlijke lezingen, duidelijk dat wie morgen pas actie onderneemt te laat kan zijn.

De media zeggen voortdurend dat ‘we’ steeds digitaler worden. Het frustrerende is dat vrijwel niemand beseft dat dit al dertig jaar zo is. Daarom kijken we allereerst naar technici om problemen met digitale onveiligheid op te lossen, maar juridische, economische en sociale aspecten zijn even belangrijk. Om gevaren te voorkomen en bestrijden moeten ondernemers de rol van ICT in hun organisatie op strategisch niveau beoordelen, zodat ze weten hoe kwetsbaar ze zich digitaal kunnen opstellen”, zegt Anouk Vos. Pieter Cobelens: “Leden van Raden van Bestuur van bedrijven die ik bezoek durven meestal niet te zeggen dat zij niets weten van cyber-IT. Ze willen niet overkomen als domme bestuurders. In feite zijn het echter veelal keizers met doorzichtige kleren, want meestal blijkt dat ze niet zijn voorbereid op de gevaren in cyberspace. Vaak is er geen speciale CIO die zich ermee bezighoudt en doet de financiële topman het ernaast. Bij problemen haalt hij het hoofd IT erbij. Dan weet je dat het niet goed zit. Als er wel een CIO is, blijkt die minder stemrecht te hebben dan de overige bestuursleden.” IT is, zegt Cobelens, niet te beschouwen als ondersteunend, want als computers een uur lang niet werken loopt de hele wereld piepend en krakend vast. Het bedrijfsleven moet, in navolging van overheid en particulieren, snel anders gaan kijken naar digitale veiligheid en nadenken over de vraag wanneer privacy ondergeschikt is aan veiligheid. Het aantal cybercrimegevallen (denk aan het hacken van websites en het buitmaken van e-mail- en gebruikersgegevens) neemt immers exponentieel toe.

‘Ik vertrouw de overheid. Per definitie’

VIJFDE DOMEIN

Na grond, lucht, zee en ruimte is cyberspace het vijfde domein. De beveiliging van deze nieuwe dimensie verschilt in essentie niet van die van de andere domeinen: het is altijd een afweging tussen de ernst van de bedreiging en de kosten van bescherming. Toch ziet Vos grote verschillen. Dit domein is niet statisch en volop in ontwikkeling. Bovendien is het geen natuurkracht, maar een geconstrueerd domein met een infrastructuur die voor ongeveer 85 procent in handen is van het bedrijfsleven. Cobelens: “Overheden hebben voor de andere domeinen veel zaken geregeld. Met cyberspace is dat niet het geval. Internet is van niemand. Iedereen heeft toegang. Saskia Stuiveling, tot mei 2015 president van de Algemene Rekenkamer, plaatste onlangs een ongelooflijk verstandige opmerking. Zij constateerde dat we er vierhonderd jaar over hebben gedaan regels te bedenken, zodat we vreedzaam kunnen samenleven. Het kan volgens haar niet zo zijn dat we in de virtuele wereld al die regels overboord gooien.” Als het om veiligheid gaat ziet Pieter Cobelens het, naar eigen zeggen, zwartwit. Prof. dr. ir. Erik Huizer, die aan de wieg van het wereldwijde web stond en nu deeltijd hoogleraar internettoepassingen is, presenteert volgens hem internet als een speelplaats waar geen regels gelden en iedereen vanaf moet blijven. “Natuurlijk moeten we tegen terrorisme en pedofielen zijn, zegt ook Huizer, maar hij wil dat we daarover met elkaar in gesprek gaan. Daar slaat hij de plank mis. Internet is er al heel lang. Het kan geen nieuwe wereld meer zijn zonder wetten en regels en zeker geen vrijplaats. Ik ben, indien

nodig, voor het koppelen van databanken, afluisteren en meer van dat soort zaken. Als het om veiligheid gaat komt privacy voor mij op de tweede plaats." Tijdens gezamenlijke lezingen verkondigt Cobelens als 'ouwe kerel' 'alle fouten ideeën' en verdedigt Vos, als vertegenwoordiger van de nieuwe generatie, 'de privacy tot op het bot'. De bedoeling is dat het publiek met die tegenstelling achterblijft en erover nadenkt. Dat is nodig, want de bewustzijnsfase mag dan voorbij zijn, lang niet iedereen heeft door wat zich in de cyberruimte afspeelt. Cobelens: "Er is nog zeker een generatie die niet is meegegaan. Ook Anouks generatie, die al heel ver is, is zich nog niet van alle gevaren bewust en soms heel onveilig bezig."

PRIVACY VERSUS VEILIGHEID

Op televisie vraagt Cobelens zich geregeld af wat hij aan privacy heeft als hij dood is. "Ik wil voorkomen dat ze me opblazen of pedofielen mijn kleinkinderen benaderen. Bovendien vertrouw ik de overheid. Per definitie, ook nu een nieuwe wet de politie de bevoegdheid geeft smartphones en computers vanop afstand te benaderen. Het is gek dat andere mensen, ondanks alle controlemaatregelen, dat vertrouwen niet hebben."

Als veiligheid goed is georganiseerd, zijn er volgens Vos geen privacy-problemen. "De tegenstelling tussen die twee wordt bijna kunstmatig in stand gehouden en blijft voer voor debat. Volgens mij gaan beide juist goed samen." Cobelens neemt graag nog wat 'misverstanden' over het aantasten van onze privacy weg. Zijn vertrouwen in de overheid betekent ook het afwijzen van de bewering dat autoriteiten terrorismedreiging als drogreden gebruiken voor het invoeren van allerlei privacy-beperkende maatregelen. "Het is onzin dat iedereen wordt afgeluisterd, pingedrag wordt bijgehouden en al onze gegevens worden bewaard. Ons land telt zeventien miljoen inwoners, onder wie negen miljoen volwassenen. Zij maken dagelijks per persoon meer dan 150 digitale bewegingen. Hoeveel mensen denk je dat de inlichtingendiensten in dienst moeten hebben om die allemaal één op één te kunnen opvolgen in steeds beter beveiligde systemen? Heb je een idee hoeveel dat kost? Daarvoor zijn ook bijzondere bevoegdheden en toestemmingen nodig. Dus gebeurt het alleen wanneer het echt noodzakelijk is."

FACEBOOK

"Bovendien zetten dezelfde mensen die klagen over het aantasten van hun privacy, hun hele hebben en houwen op sociale media als Facebook en laten ze door het invullen van bijvoorbeeld enquêtes of prijsvraagformulieren zelf allerlei gegevens achter. Ze beseffen niet dat het bedrijfsleven op die manier veel meer van ons te weten komt dan de overheid." Vos: "Bijna iedereen is online met iedereen verbonden en wil tegelijkertijd de illusie hebben in een privédomein te opereren. Als er iets misgaat wijst iedereen naar de overheid, terwijl bedrijven en particulieren natuurlijk ook een eigen verantwoordelijkheid hebben als het gaat om cyberveiligheid. Veel mensen beveiligen zich onvoldoende en hebben bij wijze van spreken nog steeds wachtwoorden die bestaan uit vier nullen." Aanslagen, zoals die in Parijs, zorgen ervoor dat meer mensen zich onveilig voelen en de weerstand tegen het aan elkaar plakken van databanken vermindert. "Tegenstanders daarvan verwijzen dan naar wat klokkenluider Edward Snowden aan het licht heeft gebracht over afluisterpraktijken en andere vermeende schendingen van de privacy door de overheid. Hij is geen heilige, maar een boef. Hij heeft dingen gedaan die niet mogen en de veiligheid juist in gevaar

gebracht. Als hij zaken had willen veranderen had hij in Amerika een rechtszaak moeten beginnen."

DIGITALE BRANDWEER

Anouk Vos pleit voor het oprichten van een digitale brandweer. "Als ergens brand uitbreekt bellen we 112 en rukken brandweer, politie en ambulancediensten uit. Wanneer het digitaal misgaat is er geen brandweer en weet niemand wie verantwoordelijk is. Dan roepen we de hulp in van een slim vriendje. Dat is vreemd, want een digitale aanval kan veel chaos en schade aan zowel de virtuele als fysieke infrastructuur veroorzaken. Ook hier is 'awareness' alleen niet genoeg en moeten de overheid en het bedrijfsleven, dat dit gekunstelde domein heeft opgestart, verantwoordelijkheid nemen. En hoeveel verantwoordelijkheidsgevoel, kennis en kunde moet de burger nu en straks hebben?" Vrouwen moeten bij het beantwoorden van die vraag een even grote rol spelen als mannen. Niet alleen als consument – "we zijn evenveel online" – maar ook professioneel. "Er zijn verschrikkelijk weinig vrouwen werkzaam in de cyberbeveiliging. Daarom heb ik mede aan de wieg gestaan van het online/offline netwerk Women in Cyber Security, dat contacten tussen de schaars vertegenwoordigde vrouwen in de verschillen domeinen wil stimuleren."

'Anouk vos pleit voor het oprichten van een digitale brandweer'

TOEKOMST

Naar de toekomst kijkend zegt Pieter Cobelens: "Gegevens en applicaties staan straks in de cloud. Iedereen kan daarvan een stukje gebruiken. IP-adressen schaffen we af, waarvan ik een groot voorstander ben, waardoor we de beveiliging van de cyberspace kunnen concentreren en daardoor versterken. Dan zijn het geen amateurs, zoals wij nu allemaal zijn, maar professionals die de boel in de gaten houden. Straks heeft iedereen een (zwevend) toetsenbord om beschermd verbinding te maken met zijn gegevens. Dat zijn er dan zoveel dat een computer van nu dat niet eens meer zou aankunnen. Ik hoop dat veel organisaties al halverwege zijn op weg naar deze nieuwe omgeving. Big data zijn ook een zegen voor de inlichtingendiensten. Nu halen die 60 à 70 procent van hun informatie uit het openbare domein, maar het aantal gegevens kwadrateert gemiddeld elke week. Dat betekent dat een gewone sterveling niet meer aan die data kan komen en ze dus ook niet kan manipuleren. Alleen mensen met veel meer ervaring en kennis op dit gebied zullen in staat zijn uit al die bronnen de gegevens te halen die nodig zijn voor analyses en prognoses. De veiligheid gaat dus omhoog."

CYBEROORLOGVOERING

Ook in conflicten tussen landen of groeperingen is cyberspace een belangrijk vijfde domein. "Niet alleen persoonsgegevens en communicatielijnen, ook vitale infrastructuur, zoals luchtverkeersleiding, pijpleidingtransport en banken, zijn grotendeels aan internet gekoppeld. Dat maakt dat offensieve cybercapaciteiten op afstand militaire operaties met fysieke gevolgen in gang kunnen zetten. Nederland kan zich in de internationale wapenwedloop onderscheiden door niet alleen te investeren in de nieuwste digitale technologieën, maar vooral de toepassing ervan. Cyberwapens verschillen van fysieke wapens doordat ze meestal eenmalig inzetbaar zijn, voor één doel zijn ontwikkeld en een beperkte levensduur hebben. Opvallend is dat men deze wapens vaak op conventionele wijze inzet en reacties op cyberaanvallen net zo traditioneel zijn." Cobelens wijst erop dat focus op strategie, naast investeren in technologie, militair pionieren voorkomt.

Een nieuwe doctrine voor cyberwapens kan bijdragen aan een open en veilig internet en fysiek militair optreden en humanitaire interventies ondersteunen. "Op internet komen de werkelijke en virtuele wereld bij elkaar, dus is iedereen het wel eens dat we een cyberverdediging moeten opbouwen. Nederland kan daarin veel betekenen. Positief is dat de overheid inmiddels meer geld voor dit doel vrijmaakt."

Anouk Vos MA MSc leidt het Cyberteam van de Policy Research Corporation en is mede-oprichter en president van de netwerkgemeenschap Women in Cyber Security. Eerder was ze onder meer senior beleidsadviseur cyberveiligheid van het ministerie van Veiligheid en Justitie.

anoukvos@speakersacademy.nl

Drs. Pieter Cobelens, generaal-majoor b.d. (bestuurskundige) was plaatsvervangend commandant Operatiën van de Groep Geleide Wapens, hoofd Militaire Opleidingen en Vorming aan de KMA en directeur van de Militaire Inlichtingen- en Veiligheidsdienst. Nu is hij verbindingsofficier van de organisatie Military Talent for Business Solutions (M4B) en strategisch adviseur bij advieskantoor Policy Research Corporation.

pietercobelens@speakersacademy.nl