schermt cyber security, en wat niet? Waar liggen de kwetsbaarheden en de prioriteiten? Is cyber security een technisch probleem, of ontberen bedrijven de prikkel om te investeren? Hoe kan ik mezelf beschermen? Wie is verantwoordelijk voor het treffen van solide beveiligingsbeleid? Nederland timmert op sommige terreinen goed aan de weg. Maar kunnen lokaal beleid en recht nog een verschil maken in een snel veranderende en globaliserende wereld?

De conclusie van dit dossier is puntsgewijs geformuleerd in The Long View (pag. 45): wat heeft een robuuste informatiesamenleving nodig om langdurig de creativiteit, economische kansen en vrijheid te koesteren die het internet biedt?

> ***"Internetveiligheid is een technisch probleem***

Het DigiNotar moment

In juni 2011 brak de 'comodohacker' in bij DigiNotar. Paniek alom. Het Beverwijkse bedrijf – opgericht in de schoot van het Nederlandse notariaat – verzorgde een klein maar vitaal beveiligingsonderdeel van veel websites, waardoor gebruikers erop kunnen vertrouwen dat ze met de echte eigenaar te maken hebben. Dankzij het 'certificaat' van DigiNotar konden burgers bijvoorbeeld hun belastingaangifte veilig insturen. De inbraak leidde niet alleen tot het bankroet van DigiNotar. Het was ook de wake-upcall voor de overheid, die vervolgens een Taskforce instelde om bestuurders bewust te maken van het cybergevaar.

Pas na de inbraak bij DigiNotar werd de overheid zich bewust van haar kwetsbaarheid.

2. Laat wet

BART JACOBS

Willen we ons online net zo veilig voelen als op straat, dan moeten overheden en bedrijven laten zien wat ze allemaal in de gaten houden.

De Britse filosoof Isaiah Berlin heeft een onderscheid geïntroduceerd tussen positieve en negatieve vrijheid. De eerste is 'vrijheid om', namelijk vrijheid om de dingen te doen die je kiest. De tweede is 'vrijheid van', waarmee vrijheid van dwang of bemoeienis wordt bedoeld. In de digitale wereld werd aanvankelijk vooral de positieve vrijheid versterkt: mensen konden zich op nieuwe wijzen manifesteren (webpagina's, blogs, tweets) en kregen mogelijkheden om informatie te verzamelen of te publiceren. Maar hoe meer narigheid het internet gaf – van aanstootgevende, opruiende, discriminerende en misleidende webpagina's tot nieuwe vormen van misdaad – is het belang van negatieve vrijheid toegenomen. Velen van ons wensen daar vrij van te zijn en er niet mee geconfronteerd te worden. Het oorspronkelijke naïeve idee dat internet alleen het goede in de mens naar boven zou brengen, is onjuist gebleken. Hoe controversieel ook in sommige kringen, regulering van toegang en van activiteiten op internet is noodzakelijk. Beschik-

Historische datalekken

II

Enigma

Een geavanceerde typemachine waarmee het Duitse leger in de jaren dertig en veertig zijn interne draadloze communicatie versleutelde. Al in 1932 wist de Poolse contraspionage de Duitse codes te kraken. Nieuwe versies van de machine maakten de code vrijwel onbreekbaar, maar doordat de Duitsers slordig omgingen met hun eigen procedures wist de Britse contraspionage tijdens WO II de codes telkens opnieuw te kraken.

€74 De geschatte jaarlijkse kosten van cybercriminaliteit wereldwijd.

600.000 Facebook heeft per dag 600.000 logins waarvan het niet met zekerheid kan zeggen dat de rechtmatige accounteigenaar inlogt.

en wat je monitort

baarheid en toegankelijkheid van informatie en diensten is een groot goed, maar vergt gepaste controle om misbruik en oplichting tegen te gaan en de betrokkenen te beschermen. Daarmee wordt de digitale wereld meer zoals de dagelijkse, niet-digitale wereld.

Deze negatieve vrijheid op internet omvat niet alleen het vrij zijn van criminele activiteiten, maar ook het vrij zijn van uitgebreide monitoring en registratie van gedrag. In de gewone wereld hebben we een redelijk beeld van waar en wanneer we in de gaten gehouden worden, zoals bij snelheidscontroles, bij videobewaking, of bij toegang tot sommige gebouwen of andere landen. Maar op internet vindt de monitoring veel ondoorzichtiger en systematischer plaats. Weet u wat uw iPhone allemaal aan Apple of aan appbeheerders doorgeeft, wat cookies in uw webbrowser aan informatie verzamelen, of wat uw digitale, op internet aangesloten televisie, allemaal verstuurt naar de fabrikant of de kabelmaatschappij? In de digitale wereld heerst schaamteloze, onbegrensde en geniepige verzamelwoede. De informatiegiganten, inclusief inlichtingendiensten, menen dat alle informatie waar ze grip op kunnen krijgen door hen verzameld en verwerkt mag worden.

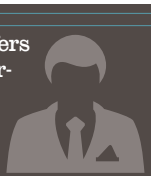
Bart Jacobs
Hoogleraar Computerbeveiliging, Radboud Universiteit Nijmegen

Aan die verzamelwoede moet paal en perk worden gesteld. Vooral vanuit Europa wordt dat geprobeerd via regels en technische vereisten. Maar regels werken het beste wanneer ze gebaseerd zijn op een breed gedragen visie op wat wel en wat niet gepast is. Op internet ontbreekt het aan zo'n visie. Neem deze voorbeelden van ongepastheid in het dagelijks leven: u zit in een trein en de passagier tegenover u maakt zomaar foto's van u. U telefoneert in de publieke ruimte en omstanders bemoeien zich met uw gesprek. U bent in een supermarkt en een andere klant maakt foto's van de inhoud van uw karretje. U zou steeds verbaasd en waarschijnlijk geërgerd opkijken. Het gaat hier om situaties waarbij al dan niet privacygevoelige informatie over u publiekelijk beschikbaar is voor degene die er aandacht aan schenkt. Desondanks ervaren we het als zeer ongepast als deze informatie door anderen geregistreerd of gebruikt wordt.

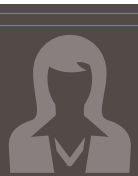
Juist de vluchtigheid van de sporen van ons dagelijks doen en laten is een belangrijk onderdeel van ons sociale functioneren. Daarom is het ongepast wanneer een grootgrutter stiekem en ongevraagd systematisch bijhoudt welke boodschappen u doet. Als dat zou gebeuren door bij de kassa u en uw boodschappen iedere keer te fotograferen zou u waarschijnlijk snel uw beklag doen. Maar op digitaal gebied wordt registratie en monitoring veelal onzichtbaar gedaan, om zulke klachten te voorkomen: men gebruikt klantenkaarten, webaccounts, IP-adressen, cookies, unieke nummers van smartphones, et cetera.

Als we ons op internet zo vrij willen voelen als in de gewone wereld, zal monitoring expliciet en zichtbaar moeten plaatsvinden, en zal de vluchtigheid van dagelijkse sporen gerespecteerd moeten worden. Wat in de gewone wereld niet hoort, hoort ook niet in de digitale wereld.

Slachtoffers van cybercrime



71% mannelijk



63% vrouwelijk

10.000

Er zijn wereldwijd meer dan 10.000 computervirussen bekend. Iedere maand komen daar zo'n 200 bij.