Veiligheid, who cares?

Ernst Roelofs

Zorgen over veiligheid is van alle dagen, en gebonden aan plaats en tijd, zowel qua beleving als feitelijke veiligheid. Voor schorpioenen of buffels hoef je in Nederland niet snel bang te zijn. Hier zijn het onder andere auto(bestuurders), slordige systeembeheerders en hackers. Uit media-publicaties en over eigen waarnemingen.

Waarom kun je op sommige plekken op deze wereld rustig je boodschappen een hele dag aan je scooter later hangen (die geen slot heeft), terwijl op de middelbare school een vergeten pennenetui van mijn zoon al na enkel uren van eigenaar verandert? Heeft welvaart hier iets mee te maken, of de toenemende tweedeling tussen arm en rijk, of is het een mentaliteitskwestie?

'Alleen slecht nieuws is nieuws'

Ondanks het graaien in data door overheden en overheidsinstanties met almaar toenemende bevoegdheden, lijkt het er maar niet echt veiliger op te worden, al kan dat natuurlijk deels perceptie zijn, want 'alleen slecht nieuws is nieuws'. Automatisch boetes uitdelen door bestanden te koppelen is voor de overheid natuurlijk gemakkelijk verdiend geld, maar maakt de samenleving niet per se veiliger.

ICT kan onze beste vriend zijn, maar net zo gemakkelijk onze ergste nachtmerrie worden. Het is natuurlijk superhandig als via de cloud ongevraagd je nieuwe mobiele telefoon gesynchroniseerd wordt met je adresboek en andere gegevens zodat je dat niet zelf hoeft te doen, als je al weet hoe dat moet ;>)).

Identiteitsdiefstal

Kwaadwillenden wordt het aan de andere kant wel erg gemakkelijk om een schat aan informatie te vergaren voor b.v. persoonsdiefstal als ze je eenmaal je loginnaam en wachtwoord ontfutseld hebben. Bijvoorbeeld door te 'sniffen' (netwerkverkeer afluisteren) bij onbeveiligde Wi-Fi-hotspots. Zodra een hacker daar binnen is, kan deze zich steeds verder ingraven. Het romantische beeld van de hacker die dat alleen doet om de veiligheid te testen, is al lang niet meer van deze tijd, al bestaan ze nog steeds. Steeds vaker zit er geldelijk gewin achter en werken spammers en hackers meer en meer samen; alleen of voor criminele organisaties. Gelukkig zijn onze lezers nog enigszins bedreven, maar veel mensen weten nog amper wat de techniek voor hun doet. Als het netwerk op het werk 'platgaat' merk je weer hoe afhankelijk we van ICT zijn geworden.

Veiliger zonder internetverbinding?

Zonder mogelijkheid e-mails te ontvangen en te versturen wordt het steeds moeilijker om met de buitenwereld te communiceren. Het wordt daardoor steeds lastiger om je omwille van veiligheid en vrijheid van de digitale wereld af te sluiten. Met name ouderen, die 'niets met computers hebben' en zich te oud vinden om zich erin te verdiepen, ondervinden dat steeds vaker. Zij merken dat ze bij steeds minder informatie kunnen en dat steeds meer instanties alleen nog via het internet en per e-mail bereikbaar zijn. Wie geen internetverbinding heeft, lijkt relatief veilig. Ook hier is, weliswaar kleiner, de kans gehackt te worden. Dat komt omdat de zwakste schakel bepalend is. De zwakste schakel is niet per se de burger met een eenvoudig te raden wachtwoord. Het kan net zo gemakkelijk de slecht beveiligde website van een webwinkel of (semi-) overheidsinstantie zijn.

Perikelen met wachtwoorden

Uit Tweakers: '2012: de digitale wereld blijft onveilig, door Joost Schellevis, maandag 31 december 2012.

Verander uw wachtwoord regelmatig, let erop waarop u klikt, en vooral: gebruik een virusscanner. Dat is in de basis wat internetters wordt aangeraden om onheil als virussen en phishing te voorkomen. Maar wat in 2012 nog meer dan in voorgaande jaren duidelijk is geworden: dat helpt slechts ten dele. Je kunt je wachtwoord nog zo vaak wijzigen, als een database met inloggegevens wordt gestolen en ook nog eens slecht beveiligd blijkt te zijn, dan heb je niets aan je goede gedrag.

Of neem het niet-klikken op verdachte links. De gedachte is dat je daarmee voorkomt dat malware zich via gaten in niet bijgewerkte of ongepatchte software op je systeem nestelt. Nog los van het feit dat je niet altijd kunt inschatten wat er achter een link schuilgaat, blijkt dat advies compleet nutteloos wanneer populaire websites of advertentienetwerken worden gehackt om malware te serveren.'

Kritische systemen slecht beveiligd

Dat de beveiliging van kritische systemen als kerncentrales soms te wensen overlaat, was op zaterdag 19 januari op BBC News te lezen: 'US warns over key computer systems.' De strekking van het verhaal is dat veel kritische systemen online bereikbaar zijn en hun beveiliging te vaak te wensen overlaat. Dat is wereldwijd het geval, wat vergaande consequenties kan hebben. Als een hacker een kerncentrale in 'verweggistan' al dan niet voor de lol in de problemen laat komen, kan dat ook voor ons gevolgen hebben. Zo had de ramp met de kernreactor in Chernobyl consequenties tot in Schotland; toch niet direct om de hoek!

Manipulatie van gegevens

Een ander veiligheidsprobleem vormen al dan niet door overheden verplichte achterdeurtjes, backdoors in hard- en software. In de Duitse blad Chip (12-2012) was de vrees te lezen voor Chinese spionage via backdoors in (Huawei) routers, maar de VS doet dat al jaren via Echelon, opgezet om te beschermen tegen terroristische aanvallen maar (ook) gebruikt voor bedrijfsspionage ten gunste van Amerikaanse bedrijven. Ook kunnen overheden opdracht geven om ongewenste informatie in buitenlandse kranten te monitoren of aan te passen. Gelukkig hebben wij in Nederland het CBP, College Bescherming Persoonsgegevens, dat als waakhond optreedt en probeert te voorkomen dat bedrijven en overheidsinstanties al te gretig data over ons verzamelen. Ook zij kunnen echter niet altijd voorkomen dat gegevens, buiten afspraken om, op creatieve wijze gecombineerd worden. Zo worden in Groningen op het NS-station met (infrarood)camera's en gegevens van mobiele telefoons mensenstromen

gemonitord. Echter, wie of wat verhindert dat iemand de gegevens combineert en zo b.v. nagaat wie er hebben in- en uitgecheckt? Want door combinatie van de gegevens kunnen ze gedeanonimiseerd worden en daarmee herleidbaar naar personen, zoals de jongeman die fraudeert met z'n OV-chipkaart.

Ondoordachtheid en sociale media

Een uitwas die minder met nationale veiligheid en meer met persoonlijke integriteit te maken heeft, is cyberpesten. Cyberpesten kan, mede dankzij de onzichtbaarheid, tot veel persoonlijk leed leiden. Via (sociale) media verspreide (onjuiste) berichtgeving kan tot wanhoop, isolement en in sommige gevallen een zelfgekozen dood leiden. Probleem is dat het allemaal zo gemakkelijk kan en er, zeker door jongeren, niet altijd goed nagedacht wordt. Wie ziek thuis is, en op Facebook vertelt hoe geweldig het stappen afgelopen nacht was, vertelt twee waarheden. Zo ook kan die gewaagde foto van je vriendin er vijf jaar later voor zorgen dat zij die gewenste baan niet krijgt.

Daarnaast kunnen op de computer beeld, geluid en berichten gemakkelijk bewerkt worden, waardoor er een andere 'werkelijkheid' ontstaat. Leuk, zolang er door een goede vriend(in) of de overheid geen werkelijkheidswaarde aan wordt toegekend. Als via een gehackt Facebook-, Twitter- of e-mailaccount in jouw naam allerlei nare berichten de wereld in worden geslingerd die jou in een kwaad daglicht stellen kan dat op z'n minst verwarrend uitpakken; immers, wat moeten ze nu geloven?
Op het internet bestaat alleen levenslang en daaraan voorbij. Daarom biedt sinds enige tijd het Netwerk Notarissen de social media-executeur aan: die sluit bij overlijden je accounts, omdat die anders nog jaren actief kunnen blijven.

Identiteitsfraude

Identiteitsfraude heeft volgens Hans Leijtens, luitenant-generaal van de Koninklijke Marechaussee, meer impact dan een overval (Volkskrant). Criminelen hebben het volgens hem steeds vaker op onze identiteit gemunt, met als gevolg een materiële schade die jaarlijks oploopt tot in de miljarden. Een identiteitsdiefstal duurt volgens Leijtens de rest van je leven, omdat dat als zodanig geregistreerd staat.
Ook in de Volkskrant was te lezen dat van een kwart miljoen Twitteraars de account-gegevens gestolen waren; eerder was dat al het geval bij LinkedIn. In de VPRO gids (nr. 6, 2013) is ter introductie van de tv-serie Bellicher (Cel) , die identiteitsfraude als onderwerp heeft, te lezen hoe het in het echt kan uitpakken. Wired redacteur Mat Honan was 'binnen een uur zijn gehele identiteit kwijt'; zelfs de babyfoto's van z'n dochter werden door de digitale vandalen gewist.

Gestolen e-mails

Omdat door de toenemende complexiteit je tegenwoordig ook voor de meest onbenullige websites wachtwoorden moet opgeven, wordt het steeds lastiger om al die wachtwoorden te onthouden. 'Gelukkig' zijn er de behulpzame helpdesks of anders is er software om wachtwoorden te achterhalen; niet altijd voor de rechtmatige eigenaren, zoals hieronder is te lezen in een bericht, overgenomen uit Tweakers Nieuws. Soms is inbreken, eerder dan echt hacken, een kwestie van social engineering en het de juiste personen zand in de ogen strooien, om zo cruciale informatie los te krijgen:

'Amerikaan die inbrak op e-mail Scarlett Johansson krijgt tien jaar cel.
Door Arnoud Wokke, dinsdag 18 december 2012 11:59, views: 20.163

Een man die inbrak in de mailaccounts van onder meer actrice Scarlett Johansson en zangeres Christina Aguilera, heeft een celstraf gekregen van tien jaar. De 36-jarige Amerikaan had ingebroken bij in totaal meer dan vijftig 'celebrities'.
De 36-jarige man brak in op de e-mailaccounts via de 'Wachtwoord vergeten'-dienst van de mailprovider, waarna hij, door beveiligingsvragen juist te beantwoorden, toegang kreeg tot de e-mails. Vervolgens liet hij alle inkomende e-mails naar zichzelf doorsturen, waardoor de 'celebrity's' ook nadat ze weer toegang kregen tot hun e-mailaccount in de gaten werden gehouden. Op die manier kon de 36-jarige man uit de Amerikaanse staat Florida zich toegang verschaffen tot onder meer financiële informatie, filmscripten en privéfoto's. Daaronder waren naaktfoto's van actrice Scarlett Johansson, die hij vervolgens aanbood aan media.'

Handhaaf een 'gezonde achterdocht'

Kortom, je kunt, ook als je voorzichtig bent, het slachtoffer worden als anderen slordig met jouw gegevens omgaan. Wat ook niet helpt is een overheid die, omwille van de eigen controledwang, steeds meer gegevens verzamelt en recent zelfs overwoog de weigering om de decryptiesleutel van persoonlijke bestanden aan justitie te geven, strafbaar te stellen (NRC). Lastig als je op je computer beveiligde bestanden hebt staan waarvan je al lang het wachtwoord vergeten bent.

En wees niet 'hebberig'

Wat je zelf kunt doen is regelmatig je wachtwoorden veranderen en met gezonde achterdocht alles uit de digitale wereld te benaderen gelijk de 'echte' wereld. Je hebt geen cruise gewonnen zonder ergens aan te hebben meegedaan, banken hebben jouw wachtwoorden en hoeven die niet op te vragen, en miljonairs in Afrika hebben jou echt niet nodig om hun miljoenen veilig te stellen.
Gebruik een virusscanner en overweeg het monitoren van uitgaand verkeer zoals Little Snitch voor de Mac. Zo'n programma laat goed zien met welke servers er allemaal contact wordt opgenomen.

Wachtwoordensystematiek

Lastige wachtwoorden kun je zelf maken door een systeem te bedenken. Bijvoorbeeld door klinkers weg te laten en te combineren met letters uit namen van partner, kinderen danwel huisdieren op een bepaalde manier die alleen voor jou betekenisvol en gemakkelijk te raden zijn. Voor onzin-sites kun je gemakkelijk te onthouden wachtwoorden met een vaste combinatie gebruiken waarin je b.v. de naam van de aanbieder verwerkt met een letter of getal. Voor meer kritische systemen als de bank kun je op die moeilijk te raden combinaties terugvallen.

Enkele links:

http://nl.wikipedia.org/wiki/ECHELON
http://www.cbpweb.nl/Pages/home.aspx
http://tweakers.net/reviews/2836/2012-de-digitale-wereld-blijft-onveilig.html
http://www.obdev.at/products/littlesnitch/index.html