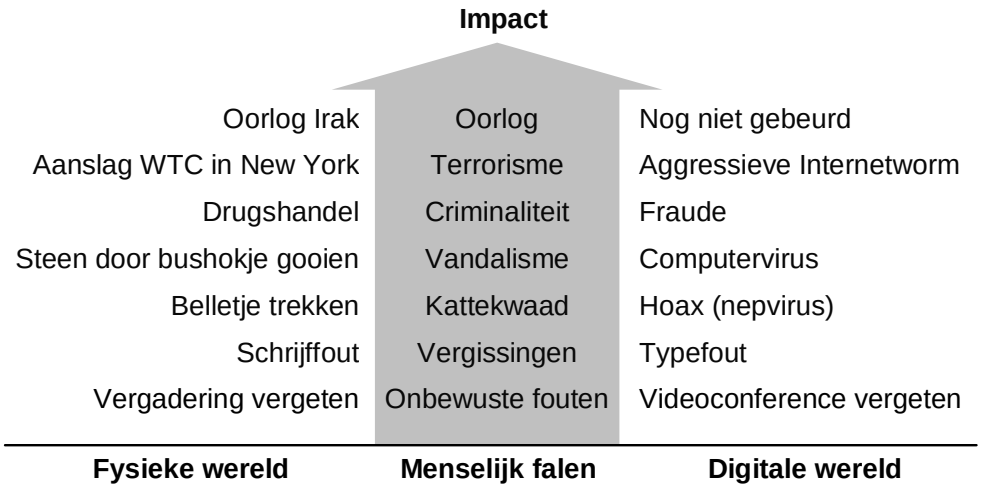
Digitale veiligheid voor burgers

Marcel Spruit
Lector Informatiebeveiliging

De burger van tegenwoordig vertoeft niet alleen in een fysieke wereld, maar ook in een digitale wereld, waarin digitale informatie verwerkt wordt met behulp van computersystemen en telecommunicatieapparatuur. Een wereld die drijft op informatietechnologie, oftewel IT.[1] Oudere burgers hebben de opkomst van de IT meegemaakt, jongere burgers zijn van jongs af aan opgegroeid met de ins and outs van IT. De IT zit zo vervlochten in onze maatschappij, dat het voor niemand meer te ontwijken is. De digitale wereld biedt veel mogelijkheden, maar ook veel gevaren. Veel bedreigingen die we al lang kennen uit de fysieke wereld krijgen een equivalent in de digitale wereld. In figuur 1 zijn hiervan een paar voorbeelden gegeven.



Figuur 1: Voorbeelden van menselijk falen in de fysieke en de digitale wereld.

Dit artikel gaat in op enkele belangrijke bedreigingen en oplossingen voor twee belangrijke spelers in de digitale wereld, namelijk de digitale burger en de digitale overheid.

De digitale burger

De burger van tegenwoordig is een frequente gebruiker van IT. De IT zit niet alleen in computers, maar ook in (mobiele) telefoons, audiovisuele apparatuur, auto's, wasmachines, koelkasten, klokken, pinpassen, et cetera. We zijn zo langzamerhand gewend geraakt aan al die IT. Het valt de meesten van ons niet eens meer op dat er IT in bijvoorbeeld een wasmachine zit. En we kijken er ook niet meer van op als een wasmachinemonteur aan komt zetten met een draagbare computer om een storing op te sporen. Al die IT is gemeengoed

geworden. We bellen mobiel, we sparen met een airmiles-kaart in plaats van zegeltjes te plakken, we betalen met een pinpas in plaats van geld, we sturen een e-mail in plaats van een brief, we doen onze bankzaken via het Internet, et cetera. We accepteren de extra comfort die met IT gerealiseerd wordt als een vanzelfsprekendheid.

Deze vanzelfsprekendheid heeft ook een keerzijde, namelijk dat we ons nauwelijks bewust zijn van de gevaren die aan het gebruik van IT kleven.[2] Toch ontstaan nieuwe bedreigingen juist bij de introductie van nieuwe technologieën. Zo leidde de komst van de videorecorder tot illegale videohandel, de komst van de computer tot computervirussen, en pinpassen tot pinpasfraude. Ook bij de introductie van nieuwe toepassingen van bestaande technologieën ontstaan veelal nieuwe bedreigingen. Toen computers gemeengoed waren, leidde grootschalige koppeling ervan tot nieuwe bedreigingen, waaronder hacking; de mobiele telefoon leidde tot extra verkeersongelukken doordat er gebeld werd tijdens het rijden, e-mail leidde tot spam, et cetera.

De laatste jaren worden niet alleen computers aan elkaar gekoppeld, maar ook de daarop draaiende informatiesystemen.[3] Hierdoor komen allerlei gegevens over mensen terecht bij organisaties die daar voorheen geen toegang toe hadden. Zo laat een airmiles-spaarder een spoor aan aankoopinformatie achter, die de deelnemende bedrijven dankbaar gebruiken voor marketing en omzetoptimalisatie. Over vrijwel iedereen is een schat aan gegevens opgeslagen bij verschillende instanties, denk aan gegevens over inkomsten, koopgedrag, kredietwaardigheid, abonnementen, leesgedrag, gezondheid, et cetera. Tot voor kort waren deze gegevens verspreid over verschillende instanties. Zo kende de specialist van het ziekenhuis via het medische netwerk wel uw hele medische doopceel, maar hij wist niets over uw koopgedrag, de verenigingen waarvan u lid bent, en of u aan goede doelen schenkt. Die andere gegevens waren wel bij andere bedrijven of instanties bekend.

Met het koppelen van informatiesystemen krijgen steeds meer derden toegang tot steeds meer gegevens over uw handel en wandel. Zo kan de belastinginspecteur als vanouds bij uw financiële gegevens, maar nu wellicht ook nog bij de gegevens over uw gezondheid, uw rook- en drinkgedrag, uw kredietwaardigheid, leesgedrag, et cetera. Als we aannemen dat alle belastinginspecteurs volledig te vertrouwen zijn, dan zouden we kunnen veronderstellen dat er niet zoveel aan de hand is. Echter, gegevens die op één plaats of voor één instantie beschikbaar zijn, zijn niet goed te beveiligen tegen kennisname door derden. En als die derden een criminele inslag hebben, dan zullen ze wellicht niet schromen om deze gegevens te gelde te maken. De consequentie daarvan laat zich raden. Als bijvoorbeeld uw rook- en drinkgedrag aan uw werkgever doorgespeeld wordt, dan besluit deze wellicht dat hij de eerstvolgende promotie liever aan een gezondere persoon aanbiedt. De veelgehoorde opvatting “iedereen mag alles over me weten, want ik heb toch niets te verbergen” is in dit licht bezien wat te kort door de bocht.

Een nog vervelender scenario is dat criminelen niet alleen inzicht in de gegevens over u hebben, maar ze ook kunnen wijzigen.[4] Om u in diskrediet te brengen kan iemand bijvoorbeeld in het politieregister een paar ernstige vergrijpen achter uw naam zetten. Dit

uiterst onwenselijke scenario hoeft overigens helemaal niet door criminelen in gang gezet te worden, het is ook mogelijk dat de gegevens rechtmatig maar onterecht gewijzigd worden.[5] Zo kan het voorkomen dat een bank u op basis van een vergissing niet-kredietwaardig verklaart. Het duurt even voordat deze fout hersteld is. In de tussentijd is uw niet-kredietwaardigheid bij iedere aangesloten instantie bekend, van bank tot supermarkt, en van ziekenhuis tot bibliotheek. De oorzaak van verkeerde gegevens kan ook liggen bij het feit dat zeer grote gegevensbestanden nooit foutvrij zijn. U kunt dus ook per toeval als niet-kredietwaardig te boek staan. Om een dergelijke fout te herstellen moet vaak eerst bekend zijn waar de fout ontstaan is, maar dat kan de nodige tijd en moeite kosten.

Door de koppeling van steeds meer informatiesystemen met persoonsgegevens, komt een andere niet zo bekende bedreiging ineens in een ander daglicht te staan, namelijk identiteitsfraude. Bij identiteitsfraude maakt iemand oneigenlijk gebruik van andermans identiteit. Dit soort fraude komt al jaar en dag regelmatig voor. Een voorbeeld is de crimineel die zijn auto voorziet van een ander nummerbord. Als deze auto op de plek van de misdaad gefotografeerd of gefilmd wordt, dan krijgt de eigenaar van het betreffende kenteken de politie op bezoek. Een ander voorbeeld van identiteitsfraude is het afkijken van iemands pincode en vervolgens de pinpas stelen. De dief kan zich met behulp van de pinpas en de bijbehorende code voordoen als de eigenaar van de bijbehorende bankrekening, en die plunderen. Zolang alle informatiesystemen nog los van elkaar opereren is de schade te overzien. De eigenaar van het kenteken hoeft alleen een alibi te hebben, en de pinpasdiefstal resulteert maximaal in een schade ter hoogte van het banksaldo. Maar als de bijbehorende informatiesystemen gekoppeld zijn aan een conglomeraat van andere systemen, dan kan degene die de bankrekening plundert ook gegevens van het slachtoffer wijzigen in het bibliotheekregister, het gemeenteregister, en gegevens voor chantage vergaren. Identiteitsfraude is een bedreiging die weliswaar al lang voorkomt, maar met steeds verdergaande koppeling van informatiesystemen neemt de impact van deze bedreiging sterk toe. Daarmee wordt ook de aantrekkingskracht op criminele organisaties steeds groter.

Al met al leidt het koppelen van informatiesystemen tot een concentratie van informatie die zelfs met de huidige vergevorderde technieken niet goed te beschermen is. Onopzettelijke fouten in het conglomeraat van informatiesystemen leiden tot ernstig ongemak voor toevallige burgers. Opzettelijk misbruik van de gegevens door criminele organisaties leidt tot nog groter ongemak voor nog veel meer burgers.

De digitale overheid

Naast het koppelen van informatiesystemen is een trend waarneembaar van digitalisering. Informatie en informatiestromen die voorheen niet digitaal waren, worden steeds meer gedigitaliseerd. Zo wordt er tegenwoordig digitaal geschreven, gebeld, gemaild, gefotografeerd, muziek geluisterd, et cetera. Ook bedrijven en instellingen zijn aan het digitaliseren. Steeds meer organisaties scannen alle papieren post bij het binnenkomen en

sturen deze vervolgens als e-mails verder de organisatie in. Ook worden documenten, boeken en tekeningen door scannen gedigitaliseerd. De voordelen hiervan zijn dat de opslag van digitale informatie veel minder ruimte kost, en dat digitale informatie veel sneller op te halen en te verspreiden is.

De toenemende digitalisering is niet aan de overheid voorbijgegaan.[6] Veel papieren informatiestromen zijn inmiddels gedigitaliseerd. Informatie van en over burgers wordt digitaal verwerkt en opgeslagen. De overheid heeft steeds meer digitale informatie over burgers beschikbaar, zoals persoonsgegevens, belastinggegevens, reisgegevens, justitiële gegevens, et cetera. De overheid heeft deze informatie nodig om haar verzorgende rol ten aanzien van haar ingezetenen te kunnen vervullen. Overigens mag de verkregen informatie alleen gebruikt worden voor het doel waarvoor ze verkregen is. Bovendien mag de informatie ook niet zomaar aan derden ter beschikking gesteld worden. De wettelijke regels voor het omgaan met informatie over personen zijn beschreven in de privacywet (Wet Bescherming Persoonsgegevens).[7] Voor sommige overheidsregisters, zoals bijvoorbeeld de gemeentelijke bevolkingsadministratie en het politieregister, bestaat aanvullende wetgeving.

Naast een verzorgende rol heeft de overheid ook de taak om te waken over de veiligheid in het land. Iedereen behoort zich in zijn omgeving veilig te kunnen voelen. Voor het beschermen van de veiligheid heeft de overheid ook informatie nodig, maar dat is andere informatie dan ze voor haar verzorgende rol nodig heeft. In feite heeft de overheid informatie nodig die indruist tegen de privacyregels.[8] Dat is formeel alleen toegestaan als er zwaarwegende argumenten zijn om de privacy te schenden. Als iemand van criminele of terroristische activiteiten verdacht wordt, dan mag de privacy van de verdachte geschonden worden. Maar op voorhand is vaak nog niet duidelijk wie er verdacht wordt van criminele of terroristische activiteiten. Daarom moet er eerst veel tijd en moeite gestoken worden in het effectief identificeren van verdachten, om vervolgens alleen deze personen te volgen. In een tijd dat de hele overheid continu aan het bezuinigen en reorganiseren is, is deze aanpak niet populair. Er wordt dan ook verlangend gekeken naar een andere aanpak, namelijk alle mogelijke informatiebronnen aan de opsporingsinstanties ter hand stellen. Als van iedere Nederlander op elk tijdstip bekend is waar hij of zij is, en wat hij of zij daar uitvoert, dan is het opsporen van overtreders een fluitje van een cent.

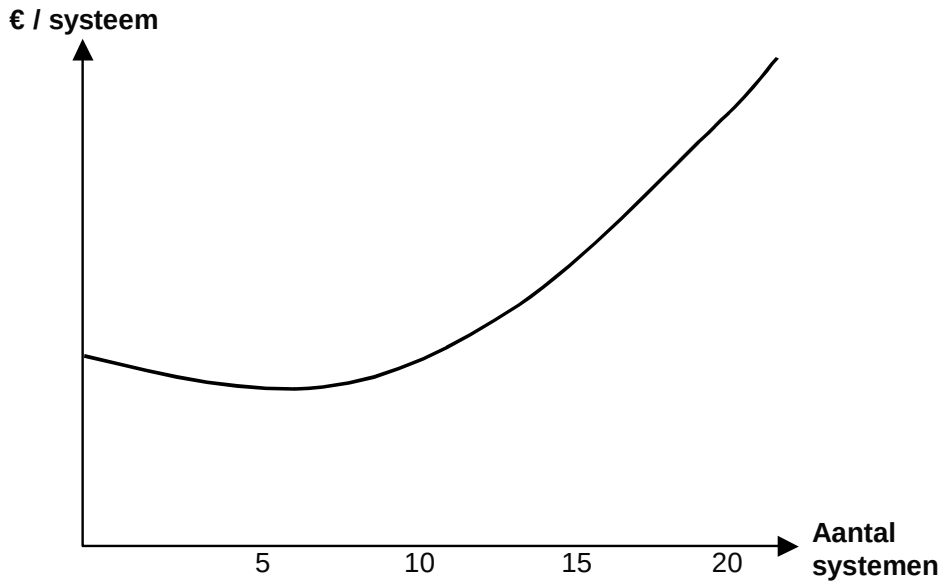
De laatstgenoemde aanpak is die welke de overheid nastreeft. Door koppeling van zoveel mogelijk van haar eigen informatiesystemen ontstaat een schat aan informatie. Nu al wordt steeds meer van deze informatie ter beschikking gesteld aan opsporingsinstanties. De opsporingsinstanties voegen hier zelf nog digitale gegevens aan toe die afkomstig zijn van onder meer camerasurveillance en het aftappen van telefoon, e-mail en Internet. Hiermee wordt een conglomeraat aan informatiesystemen gecreëerd dat door één of enkele opsporingsinstanties geraadpleegd en wellicht ook gewijzigd kan worden. Echter, gegevens die op één plaats of voor één instantie beschikbaar zijn, zijn niet goed te beveiligen tegen kennisname door derden. Dit wordt dus een aantrekkelijk object voor criminelen die graag hun voordeel doen met kennis over de gedetailleerde handel en wandel van iedere

Nederlander. Daarnaast is een dergelijk conglomeraat van informatiesystemen ook zeer aantrekkelijk voor terroristische organisaties.

Terroristische organisaties hebben ook vanuit een ander perspectief veel interesse voor een centraal toegankelijk conglomeraat van informatiesystemen. Een dergelijk conglomeraat is namelijk zo belangrijk voor de overheid, dat het wegvallen ervan de hele overheid kan verlammen. Het platleggen van het centrale informatiesysteem van bijvoorbeeld de Rijksdienst voor het Wegverkeer is vanuit terroristisch perspectief gezien nauwelijks interessant, maar als het mogelijk is om met één gecoördineerde actie vanuit een centraal punt verscheidene belangrijke informatiesystemen tegelijk te treffen dan is dat wel een heel interessant doel. Hoe groter het conglomeraat aan gekoppelde informatiesystemen, hoe groter de terroristische dreiging.

Oplossingen

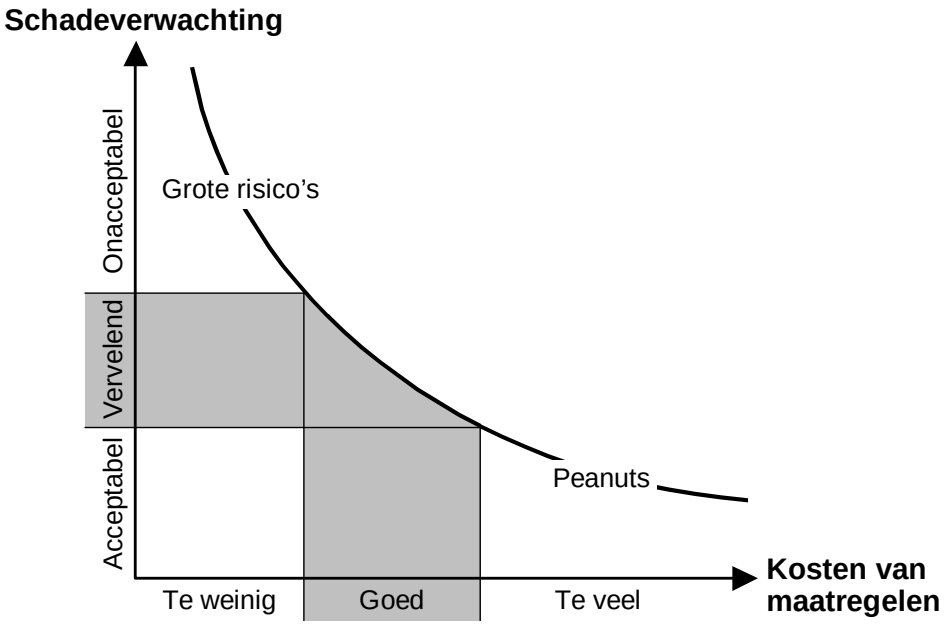
Uit het voorgaande is duidelijk geworden dat het onbeperkt koppelen van informatiesystemen belangrijke nadelen heeft. Met name de overheid die veel informatiesystemen heeft, moet erg oppassen dat ze niet teveel doorschiet in haar koppelingsdrang. Daarentegen kan het koppelen van informatiesystemen in bepaalde gevallen heel wenselijk zijn.[9] Er is dan ook sprake van een optimum: koppeling is nuttig, maar met mate. De richtlijn zou moeten zijn dat informatiesystemen alleen gekoppeld worden als het nodig is voor de processen die er gebruik van maken. Oftewel: alleen koppelen wat nodig is, en niet alles wat mogelijk is. Dus koppelen omdat daardoor misschien wel eens nuttige informatie over verdachten gevonden zou kunnen worden is geen goed idee. Aparte, en eventueel onderling gekoppelde, informatiesystemen die toegespitst zijn op opsporing zijn daarentegen wel nuttig.



Figuur 2: De globale kosten van een informatiesysteemconglomeraat als functie van het aantal gekoppelde systemen.

Door koppeling van informatiesystemen zijn schaalvoordelen te behalen. Bovendien kan de effectiviteit van een dergelijk conglomeraat groter zijn dan die van de individuele systemen. Door beperkt te koppelen loopt men deze voordelen gedeeltelijk mis. Daar staat tegenover dat in de praktijk gebleken is dat het koppelen van meer dan een handvol systemen onevenredig duur is. Dit wordt onder meer veroorzaakt door interfaceproblemen en ophoping van fouten. De richtlijn om alleen te koppelen wat nodig is, en niet alles wat mogelijk is, blijkt dus ook nog eens relatief goedkoop en effectief te zijn (zie figuur 2).

De kwetsbaarheid van beperkt gekoppelde informatiesystemen is weliswaar minder dan die van onevenredig gekoppelde informatiesystemen, het is toch zaak om de beveiliging van deze systemen goed op orde te hebben. Criminele en terroristische organisaties krijgen steeds meer kennis over digitale informatiesystemen. Het niveau van beveiliging van deze systemen moet dus navenant toenemen om de risico's niet teveel te laten stijgen. Ook vanwege een andere reden is verdergaande beveiliging van informatiesystemen nodig. Hoe belangrijker informatiesystemen zijn, des te groter de schade bij een incident. Daarom moeten informatiesystemen niet alleen tegen criminele en terroristische bedreigingen beschermd worden, maar ook tegen allerlei andere bedreigingen, zoals onopzettelijke fouten, brand, bliksem, storm, apparatuurstoring, et cetera.[10] Toch is het rücksichtslos treffen van beveiligingsmaatregelen geen goed idee. Naast het nemen van te weinig maatregelen is het namelijk ook mogelijk om te veel maatregelen te treffen. Om dit inzichtelijk te maken is in figuur 3 het verband geschetst tussen de risico-omvang, ofwel de te verwachten schade door bedreigingen, en de kosten van de getroffen maatregelen. In de onderste zone van de figuur bevinden zich de overbodige maatregelen, waar euro's uitgegeven worden om dubbeltjes te beveiligen. De kunst is om voldoende maatregelen te treffen, niet te weinig maar ook niet te veel.[11]



Figuur 3: Schadeverwachting versus kosten van maatregelen

Daarnaast heeft de digitale burger ook een verantwoordelijkheid in het realiseren van veilige informatiesystemen. Veel mensen koesteren hun zwaarbevochten rechten nauwelijks. Het is onvoorstelbaar hoe makkelijk mensen hun privacygevoelige informatie vrijwillig opgeven. Denk aan het razendsnelle succes van de airmiles-kaart. Men gaat er te gemakkelijk vanuit dat men er zelf geen last van zal krijgen, maar dat is in het algemeen niet waar. Men merkt het echter pas als het te laat is. En zelfs dan zijn velen er zich niet eens van bewust dat de hinder door het weggeven van eigen informatie is ontstaan. Zo zijn bijvoorbeeld spam, hoaxen (nepvirussen), en het 's avonds steeds gebeld worden door colporteurs, alleen mogelijk doordat we links en rechts onze adresinformatie weggeven. Een wet zoals de privacywet stelt paal en perk aan misbruik van gegevensinformatie. Toch hoeft maar iemand het woord terrorismebestrijding te noemen en we geven zonder veel discussie de rechten die in die wet staan op. Hier past wat meer behoedzaamheid van de digitale burger.

Een bedachtzame digitale overheid en bedachtzame digitale burgers kunnen gezamenlijk de strijd aangaan tegen de gevaren van de digitale wereld. Als ze dat goed aanpakken, profiteren ze ten volle van de mogelijkheden van de digitale wereld.

Referenties

[1] W. Stallings, *Data and computer communications*, Prentice-Hall, Upper Saddle River, 2003.

[2] P. Neumann, Illustrative risks to the public in the use of computer systems and related technology, http://www.csl.sri.com/users/neumann/illustrative.html

[3] R.M. Stair en G.W. Reynolds, *Principles of Information Systems*, Course Technology, Cambridge, 2003.

[4] Zie een voorbeeld scenario-uitwerking in de film *The Net*, Irwin Winkler, Colombia Pictures, 1985.

[5] J.T. Reason, *Human error*, Cambridge University Press, Cambridge, 1998.

[6] P. Mettau, *Mijnoverheid.nl*, Het Expertise Centrum, Den Haag, 2005.

[7] *Wet Bescherming Persoonsgegevens*, 6 juli 2000, zie www.wetten.overheid.nl en www.cbpweb.nl

[8] *Wet op de Inlichtingen- en Veiligheidsdiensten 2002*, 7 februari 2002, zie www.wetten.overheid.nl

[9] W. van Gelder en E.J. Mulder, *De elektronische overheid: na dromen nu daden*, Management & Informatie, nummer 3, 2003, pagina's 4-9.

[10] P. Overbeek, E. Roos Lindgreen en M. Spruit, *Informatiebeveiliging onder controle*, Pearson, Amsterdam, 2005.

[11] M. Spruit, *Waardevol maakt kwetsbaar: het belang van informatiebeveiliging*, Haagse Hogeschool, Den Haag, 2004.