VEILIGER MET VOORKENNIS

Deel 2

"People think focus means saying 'Yes' to the thing you've got to focus on. But that's not what it means at all. It means saying 'No' to the hundred other good ideas that there are. You have to pick carefully. I'm actually as proud of the things we haven't done as the things I have done." – Steve Jobs

Voor organisaties is het belangrijker dan ooit om te weten hoe ze de steeds sneller ontwikkelende IT veilig kunnen benutten. In deel 1 heb ik aangegeven waarom een systematische analyse nuttig is om de effecten van veranderingen te bepalen en welke kennis organisaties meestal missen bij de invulling van risicomanagement. Onder de druk van prestatieverbetering en efficiency voeren organisaties nieuwe technologieën in, ook als de risico's voor de bedrijfsprocessen nog niet bekend zijn. In dit tweede deel van dit artikel belicht ik de risico's en kansen van enkele nieuwe ontwikkelingen, zoals de toenemende complexiteit, het voortdurend opschalen van organisaties en systemen en de invloed van quantum-computers.

Grotere complexiteit, toenemende onvoorspelbaarheid

Hoewel er steeds meer data beschikbaar is, leidt dat niet altijd tot goede informatie. Als de verwerking van data onvoldoende rekening houdt met ruis, vermindert dat de kwaliteit van beslissingen. Zo bleek uit een Ernst & Young ICT Barometer over 2009 dat ca. 38% van alle organisaties malware infecties rapporteerden. Het rapport over 2010 signaleerde voorzichtig een lichte verbetering ten opzichte van vorig jaar, omdat dit percentage was gezakt naar 33% [10]. Het is echter weinig aannemelijk dat in 2010 meer organisaties erin slaagden alle besmettingen te ontlopen. Beide E&Y rapporten geven namelijk ook aan dat cybercrime juist aan het toenemen is. Verder is bekend dat veel organisaties steeds huiveriger zijn om publiekelijk toe te geven dat hun systemen waren besmet met malware. Klopt het in eerste instantie ogenschijnlijk positieve signaal dus eigenlijk wel?

Beide rapporten bevatten de percentages van organisaties waarvan de systemen dat jaar niet, eenmalig of vaker zijn besmet, zodat een statistische analyse mogelijk is. Voor de analyse is het uitgangspunt dat opgetreden besmettingen onafhankelijk zijn van elkaar [11]. Uit de analyse volgt dat in 2009 ca. 49% van de organisaties in het rapport gemiddeld 1,50 besmettingen per jaar hadden [12]. Dezelfde analyse op de cijfers van 2010 laat echter zien dat voor ca. 42% van de organisaties het aantal jaarlijkse besmettingen groeide naar 1,54. Doordat meer organisaties "nul" besmettingen rapporteerden, ontstaat op basis van deze ruis een vertekend beeld: van 51% in 2009 tot 58% in 2010. Met de toenemende cyberdreiging is die stijging te verklaren door de toenemende achterstand van standaardmaatregelen zoals Antivirus en een groeiende weerstand van organisaties om toe te geven dat hun systemen zijn geïnfecteerd.

Uit het bovenstaande blijkt dat een oppervlakkige analyse een vals gevoel van veiligheid kan oproepen. Daarnaast levert een analyse met ongeschikte modellen vrijwel zeker verkeerde informatie op. Zo gaan berekeningen met de schade-indicatoren SLE en MTTR ervan uit dat je die waarden nauwkeurig kunt bepalen en dat de kansverdeling van deze factoren statistisch normaal is verdeeld. Dat wil zeggen dat de werkelijke waarde dicht bij het gemiddelde ligt en dat sterk afwijkende waarden zeer onwaarschijnlijk zijn. Het gebruik van de normale verdeling is aantrekkelijk, omdat er lineair gerekend kan worden met gemiddelde waarden. En met een interval van 2x de standaardafwijking rond het gemiddelde, zal 95% van de waarden in de praktijk in dat interval vallen.

Maar in de praktijk komen er naast de normale verdeling ook vaak andere kansverdelingen voor. De schaal van Richter voor aardbevingen en de verdelingen van inkomen en vermogen conform de 20-80 wet van Pareto zijn voorbeelden van kansverdelingen met een machtswet. Als de connectiviteit van knooppunten in een netwerk een machtswet volgt, dan bestaat er geen drempelwaarde voor infecties [13]. Dat betekent dat in dergelijke netwerken de verspreiding van infecties enorm wordt versterkt. Verschijnselen zoals hyperinflatie, vertragingen van projecten en verkeer, en verliezen op de beurs hebben mogelijk andere kansverdelingen, maar gedragen zich eveneens sterk niet-lineair [14,15]. Correlatie aantonen en onzekerheid verminderen zijn veel moeilijker met dergelijke kansverdelingen. De schade per beveiligingsincident kan voor een organisatie bijvoorbeeld

fluctueren tussen nul en een faillissement, zoals bij Diginotar. De kans op een faillissement door incidenten met een machtswet als kansverdeling is veel groter dan bij een normale verdeling. Dergelijke risico's zijn meestal niet betrouwbaar te schatten, omdat de schade van het risico ofwel geen gemiddelde waarde heeft, ofwel geen maximale waarde – en soms allebei [16].

Niet-lineaire effecten verschijnen ook regelmatig in de economie. In de periode 2004 tot 2008 verdrievoudigde de prijs van rijst, terwijl wereldwijd de toename van de vraag met 1% precies even groot was als de groei van de productie [17]. Niemand had die prijstoename voorspeld en zelfs met de kennis achteraf is onduidelijk of die überhaupt te voorspellen was.

"To know what you know and what you do not know, that is true knowledge" – Confucius

De individuele competenties van de betrokken medewerkers hebben grote invloed op de effectiviteit van informatiebeveiliging. Maar mensen gedragen zich soms anders dan verwacht en minder rationeel dan ze zelf denken [18]. Onze hersenen zijn evolutionair afgestemd op patroonherkenning, maar individueel missen we grotendeels het zicht op aanvallen die via het internet lopen. Bovendien heeft de betrouwbaarheid van de beschikbare informatie soms ernstig te lijden als de belangen groot zijn. Dat tweedracht zaaien effectief is, blijkt onder andere uit het langdurige gebrek aan consensus over het verband tussen roken en longkanker [19]. Door de schijn te wekken dat het "Intelligent Design" scheppingsverhaal een wetenschappelijk basis heeft, wist de Protestantse lobby in 2004 af te dwingen dat Amerikaanse schoolboeken moesten vermelden dat de evolutietheorie slechts één van de theorieën is [20]. Evolutiebiologen zoals Richard Dawkins die daartegen ageren worden soms persoonlijk aangevallen. Niet alle wetenschappers zullen daarom zin hebben om zich in zo'n discussie te mengen, waardoor pseudowetenschap langer blijft bestaan.

Omdat de mens kuddegedrag vertoont, blijft een dominante mening vaak (te) lang hangen. Kuddegedrag heeft zich evolutionair bewezen als methode waarbij de meerderheid kan overleven als de roofdieren aan een paar zwakke prooidieren voldoende hebben. Als het aantal roofdieren toeneemt, dan komen ook de sterkere leden van de kudde in gevaar. Daarom is een risicoschatting gebaseerd op de stelregel "als ik hetzelfde doe als de meerderheid, ben ik relatief veilig" in het internettijdperk achterhaald. Op het internet zijn we namelijk geen kudde die samenwerkt om aanvallers effectief te confronteren. Het breed delen van kennis compenseert dit gemis niet helemaal, omdat het ontwikkelen van kennis over cyberaanvallen en de (in)effectiviteit van beveiligingsmaatregelen wordt geremd door de eerder genoemde weerstand van organisaties om incidenten te melden.

Door miniaturisatie en de integratie van sensoren, dataopslag, processorcapaciteit en communicatie neemt het aantal slimme online apparaten steeds meer toe. Het gedrag van dergelijke Complexe Adaptieve Systemen (zoals The Internet of Things) is slecht te voorspellen, omdat oorzaak- en gevolgrelaties vaak onduidelijk zijn. Dat komt omdat het gezamenlijke gedrag van individuele systemen afhangt van hun (lokale) logica en de steeds geactualiseerde informatie die via het netwerk wordt uitgewisseld.

In de nabije toekomst zal de samenleving steeds afhankelijker worden van in aantal en omvang groeiende netwerken. In het verleden is gebleken dat met netwerkstructuren communicatie mogelijk blijft, zelfs al vallen veel verbindingen en knooppunten uit. Netwerkprotocollen zoals TCP/IP zijn daarvoor ontworpen. Die robuustheid vervalt echter als het netwerk zelf de oorzaken van uitval doorgeeft aan kwetsbare andere onderdelen, zoals bij malware of overbelasting het geval is. Naarmate zo'n netwerk groeit in omvang en connectiviteit, neemt de kwetsbaarheid voor uitval toe.

Het is nuttig als een model kan aangeven waar een netwerk kwetsbaar is en hoe de robuustheid ervan kan worden vergroot. Omdat technologie steeds complexer wordt, moeten modellen qua complexiteit meegroeien. Veel organisaties maken die stap niet en blijven eenvoudige modellen gebruiken. Maar ook met complexe modellen wordt het betrouwbaar anticiperen op incidenten moeilijker. De consequentie is dat er meer aandacht nodig is voor de voorbereiding van het signaleren en afhandelen van incidenten [21].

"The problem is that at a lot of big companies, process becomes a substitute for thinking. You're encouraged to behave like a little gear in a complex machine" – Elon Musk

Efficiency en kwetsbaarheid bij schaalvergroting

Outsourcing en schaalvergroting zijn meestal gericht op efficiencyverbetering. De basisgedachte is dat kleine organisaties schaalvoordelen missen en daardoor duurder zijn. Vanwege de toenemende bureaucratie worden de grootste organisaties ook duurder ingeschat. Conform deze vuistregel zijn middelgrote organisaties dus het meest efficiënt. Maar uit de twee onderstaande voorbeelden blijkt dat de grens tussen "middelgroot" en "groot" moeilijk te trekken is.

De TU Delft heeft na onderzoek vastgesteld dat het aantal Nederlandse ziekenhuizen zodanig afneemt door fusies, dat een gemiddeld Nederlands ziekenhuis nu al twee keer zo groot is als een gemiddeld ziekenhuis in New York. Bij verder fuseren ervaren Nederlandse ziekenhuizen daardoor schaalnadelen: als de productie met 1% stijgt, dan nemen de kosten met 1,23 % toe. Door schaalvergrotingen in de periode 2003 tot 2009 verloren de

Henk-Jan van der Molen is freelance docent bij de Security Academy.
De auteur wil iedereen bedanken die een positieve inbreng heeft geleverd aan dit artikel, in het bijzonder Jurgen van der Vlugt en Charlotte Rugers.

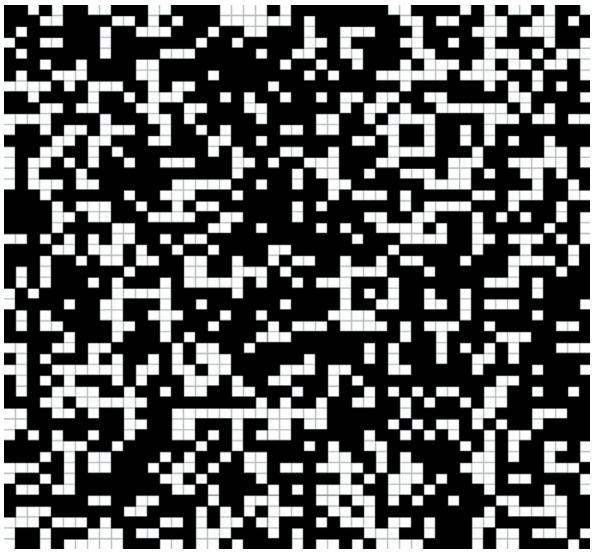
ziekenhuizen in Nederland bijna 5% aan productiviteit [22].
Hetzelfde resultaat volgt uit een onderzoek van het Centrum voor Onderzoek van de Economie van de Lagere Overheden naar de fusies van Nederlandse gemeenten [23]. Het onderzoek laat zien dat de kwaliteit van publieke voorzieningen na een gemeentelijke fusie niet verbetert. Ook is er geen efficiencywinst, in de nieuwe fusiegemeente blijven de bedrijfsvoeringkosten per hoofd van de bevolking gemiddeld even hoog.
Bij fusies van organisaties blijkt regelmatig dat het resultaat complexer is dan de som der delen, omdat bij schaalvergroting problemen abstracter worden [24]. Managers blijken minder effectief als de afstand tot de werkvloer te groot wordt [25].

Bij technische vooruitgang hoort dat er meer en complexere systemen worden ingezet. Als een systeem meer complexiteit bevat dan direct zichtbaar is, wordt de kwetsbaarheid van het totale systeem meestal te laag ingeschat. Voor het verhelpen van kwetsbaarheden is de standaardactie het uitrollen van een software-update. Vanwege de vele kwetsbaarheden die overblijven, geeft een snelle updateprocedure weinig garantie voor de toekomst. Naarmate een systeem meer componenten bevat, neemt het aantal defecte componenten en de instabiliteit toe [26]. Daardoor is een complex systeem makkelijker te hacken, omdat een aanvaller uit de vele kwetsbaarheden de eenvoudigste kan kiezen. In een technocratische samenleving waarin de capaciteit van elk systeem is geoptimaliseerd, zijn de gevolgen van uitval onvoorstelbaar groot en het moment waarop de uitval plaatsvindt grotendeels onvoorspelbaar.

"If something is fragile, anything you do to increase performance is inconsequential" – Nicolas Taleb

Zelfs met alleen maar veilige componenten kan een systeem als geheel nog steeds instabiel zijn. In de 19e eeuw is bij stoommachines al aangetoond dat maatregelen om de snelheid constant te houden soms grote oscillaties kunnen veroorzaken [27]. Uit een analyse van de black-out in de VS in 2001 bleek dat het elektriciteitsnetwerk afhankelijk is van een aantal kritieke componenten. Uit later onderzoek blijkt dat naast de geografie ook de fysische eigenschappen van het netwerk belangrijk zijn, zoals componenten die de meeste energie doorgeven in het netwerk [28]. Als die falen, leidt dat tot een onvoorspelbare en abrupte uitval van het hele netwerk [29]. Ook het Europese elektriciteitsnet is kwetsbaar, omdat de nationale netwerken zijn gekoppeld met synchrone wisselstroomkoppelingen die capaciteitsproblemen kunnen doorgeven. Op 28 september 2003 viel bijvoorbeeld in heel Italië de stroom uit, omdat een Zwitserse boom een hoogspanningsleiding uitschakelde. Gelijkstroomkoppelingen kunnen problemen in één netwerk afschermen van de andere netwerken, maar vervanging van alle synchrone wisselstroomkoppelingen is duur.

Als een organisatie te complex wordt, is deze niet meer effectief te managen. Vaak reduceren grote organisaties de complexiteit door processen en systemen te uniformeren. Na elke fusie informatiesystemen uniform maken en houden is echter duur en tijdrovend. Daarnaast is schaalvergroting meestal ongunstig voor de beveiliging, omdat in een grote organisatie de vele systemen de single-points-of-failure van dezelfde infrastructuur delen. In een ICT-monocultuur raakt een cascade uitval van systemen veel gebruikers, maar veel organisaties negeren het toegenomen continuïteitsrisico en staren zich blind op de verwachte efficiencywinst van schaalvergroting. Een eenvoudige analogie: om zoveel mogelijk winst te maken met het kweken van bomen, wil de eigenaar zijn perceel zo dicht mogelijk beplanten. De optimale dichtheid van bomen op het perceel is echter afhankelijk van de frequentie van bosbranden. Als de bomen te dicht op elkaar staan, dan zal met één bosbrand het hele perceel afbranden, zie afbeelding 4. In combinatie met meer online gekoppelde uniforme voorzieningen, meer complexiteit en de noodzaak sneller beslissingen te nemen, vergroot globalisatie het risico van een wereldwijde crisis. Het is verkeerd om je alleen te richten op de schaalvoordelen en tegelijkertijd de grotere kans op uitval te negeren.



Als de bezettingsgraad (p) van een perceel groter is dan 0,592.. dan vormen de ingevulde cellen met elkaar een "giant component" (hier: p=0,6) 12

Inmiddels hebben ook Fortune 500 organisaties ervaren dat ze kwetsbaar zijn voor cybercrime [30]. Om de robuustheid van grotere organisaties op acceptabel niveau te houden, zijn meer maatregelen nodig. Daarbij valt te denken aan de capaciteit om uitval snel te kunnen herstellen, redundantie van onderdelen en back-up systemen, maar belangrijker is alternatieve middelen achter de hand te hebben die geen kwetsbaarheden delen met de primaire productiesystemen. Deze alternatieve middelen vormen de "zekeringen" die belemmeren dat een enkel incident kan uitgroeien tot een grootschalige crisis. Als gekoppelde systemen onderling verschillend zijn, kan malware zich moeilijker verspreiden tussen systemen. Voor kritische voorzieningen kan het risico van malware worden gespreid door diversiteit in software. Om die diversiteit te bevorderen moeten organisaties software kiezen die Open Standaarden gebruiken [31].

Sommige architecturen zijn robuust omdat ze zijn gebaseerd op collectieve verantwoordelijkheid en decentrale sturing, zoals immuunsystemen en sommige sociale systemen [32]. In de biologie is de diversiteit aan soorten de beste verzekering tegen massale uitsterving. Ook innovatie gedijt het best

met diversiteit en flexibiliteit, niet als alles hetzelfde is en blijft. Economische diversiteit is de beste voorspeller van economische groei, beter zelfs dan de grootte van de investering in kennis [33].

Toch bieden outsourcing en schaalvergroting ook kansen. Omdat individuele organisaties cyberaanvallen steeds moeilijker kunnen detecteren, bieden security-diensten vanuit de Cloud voordelen. Als een Cloud oplossing incidenten bij een organisatie in real time kan signaleren, kunnen dezelfde incidenten worden voorkomen bij de andere aangesloten organisaties.

"It is often stated that of all the theories proposed, the silliest is quantum theory. In fact, some say that the only thing that quantum theory has going for it is that it is unquestionably correct" – Michio Kaku

De opkomst van quantum-computing

Op basis van de wet van Moore was het al nodig om voldoende lange encryptiesleutels te gebruiken voor het langdurig vertrouwelijk houden van geheime informatie [34]. Zodra een quantum-computer met voldoende rekenkracht ontwikkeld wordt, ontstaat een trendbreuk die direct grote invloed heeft op de sleutellengte en de methoden van encryptie.

De quantum-computer is voorspeld door de beroemde natuurkundige Richard Feynman en is gebaseerd op de quantum-mechanica, die onder andere stelt dat een elementair deeltje zich in superpositie of meerdere toestanden tegelijk kan bevinden. Ik belicht hier alleen het superpositie beginsel, niet de quantum-verstrengeling van twee elementaire deeltjes. Met twee mogelijke toestanden tegelijk neemt met elk toegevoegd deeltje het aantal toestanden van de deeltjesverzameling met een factor 2 toe. Met zijn briljante inzicht draaide Feynman dit om en speculeerde dat een "quantum-computer" op basis van dit concept een exponentiële rekenkracht zou hebben. In een quantum-computer kan een zogenaamd qubit gelijktijdig 0 en 1 zijn.

Met voldoende qubits kan een quantum-computer sommige rekenproblemen veel efficiënter oplossen dan klassieke computers. Met een inputvariabele in superpositie wordt namelijk de functiewaarde van ALLE mogelijke invoerwaarden in één operatie berekend. Daarmee is bijvoorbeeld de RSA-encryptie te kraken, die gebruikt wordt om encryptiesleutels over het internet uit te wisselen. RSA is gebaseerd op de moeilijkheid om uit een product van 2 grote priemgetallen (P x Q) de factoren P en Q te halen.

Het opstellen van een rekenmethode voor een quantum-computer is overigens niet eenvoudig. Omdat in superpositie elke functiewaarde statistisch evenveel kans heeft "getrokken" te worden, moet de rekenmethode borgen dat de correcte oplossing eruit springt en de foute oplossingen elkaar uitdoven. Bij algoritmes waarbij veelvouden van de kleinste oplossingen ook correct zijn, ontstaat er een piek in het frequentiespectrum van de berekende oplossingen. Het meerdere keren "trekken" van het resultaat van de berekening uit het frequentiespectrum vergroot de kans op een correcte oplossing. Voordat deze überhaupt bestond, heeft de wiskundige Peter Shor al in 1994 een methode gevonden waarmee een quantum-computer efficiënt die P en Q kan berekenen uit hun product [35]. Voor het kraken van encryptie bestaan er naast Grovers algoritme voor het efficiënt doorzoeken van databases enkele varianten op Shor's algoritme voor andere encryptiemethoden [36].

De vooruitgang in de nanotechnologie maakte experimenten met een quantum-computer mogelijk. Het bleek echter bijzonder moeilijk om qubits voldoende lang stabiel te houden om berekeningen mogelijk te maken. In 2011 is met een 4 qubit quantum-computer vastgesteld dat het product 143 bestaat uit de priemgetallen 11 en 13 [37]. De weg vooruit is nog lang, maar in de laatste jaren zijn veel doorbraken gerealiseerd om qubits te stabiliseren. Fysicus Leo Kouwenhoven heeft bijvoorbeeld in 2012 na een experiment met nanodraden sterke aanwijzingen gevonden voor de in 1937 theoretisch voorspelde Majorana deeltjes [38]. Die deeltjes zijn groter en stabieler dan elementaire deeltjes, maar vertonen nog steeds quantum-gedrag. Daardoor lijken Majorana deeltjes veelbelovende bouwstenen voor qubits. Op basis van de technologische vooruitgang worden rond 2030 de eerste quantum-computers verwacht die de huidige asymmetrisch encryptiesleutels kunnen kraken [39]. Dat betekent dat actie nodig is als asymmetrisch vercijferde informatie na 2030 geheim moet blijven!

In het post-quantum-computing-tijdperk zijn een aantal asymmetrische encryptiemethoden niet langer veilig [40]. Met Grovers algoritme halveert een quantum-computer ook de sleutellengte van symmetrische encryptiemethoden. De quantum-computer betekent echter niet het einde van alle systemen die gebaseerd zijn op (a)symmetrische encryptie. Wel zullen cryptosystemen in een soort Y2K-programma moeten overschakelen naar veilige encryptiemethoden waarvoor (nog) geen quantum-rekenmethode bestaat. Die encryptiemethoden vergen echter meer rekenkracht en langere sleutels om dezelfde toepassingen mogelijk te maken [41]. Met voldoende lange sleutels zijn encryptiemethoden zoals AES en SHA voorlopig nog veilig. De quantum-mechanica maakt daarnaast zelf ook een nieuwe encryptiemethode mogelijk. Maar om die methode in te zetten voor Quantum Key Distribution vergt op dit moment een directe optische verbinding tussen Alice en Bob, met alle bijbehorende nadelen. Het alternatief om terug te keren naar handmatige sleuteldistributie is echter nog minder aantrekkelijk. Mogelijk dat de ontwikkeling van quantum-netwerken hiervoor een oplossing kan bieden, samen met quantum-computing in the Cloud.

"If you do not change direction, you may end up where you are heading" – Lao Tzu

Conclusie

In de westerse wereld nemen de loonkosten steeds meer toe ten opzichte van de rest van de wereld. Onder deze druk neigen sommige organisaties ernaar op efficiency te concurreren. Helaas zijn gefuseerde organisaties en grote systemen vaak zo complex dat deze moeilijk veilig kunnen worden ingezet. Bovendien zit er aan efficiencywinst door opschaling een grens. Als een organisatie door fusies boven een bepaalde omvang komt, zal de efficiency afnemen. Bovendien kan je in veranderlijke tijden beter klein en wendbaar zijn.

Om met de rest van de wereld te kunnen blijven concurreren, heeft Nederland continu innovatie nodig. Een organisatie die binnen de snel veranderende context de kansen en bedreigingen van nieuwe technologie wil bepalen, heeft voorspellende modellen nodig. Een model verhoogt de transparantie, waardoor het effect van veranderingen op bedrijfsprocessen beter te voorspellen is. Kennis van techniek en statistiek is nodig om modellen te ontwikkelen die kunnen omgaan met ruis in de invoer en om deze te kunnen toetsen. Zelfs een goed model is niet in alle situaties een "silver bullet" en moet aan de context worden aangepast en regelmatig worden herijkt om missers te voorkomen. Dat komt ook doordat theoretische kennis ontbreekt om betrouwbare modellen te construeren en de interactie tussen individuele systemen en het netwerk te beschrijven. Bovendien moet kennis worden ontwikkeld om met een formele taal de consistentie en volledigheid van een model in de praktijk te verifiëren.

Informatiebeveiliging wordt steeds meer een enabler om nieuwe technologie veilig in te kunnen zetten. Er is echter inzicht in de werking nodig om de kansen en risico's van nieuwe technologie te kunnen bepalen. Bovendien moet de opgedane kennis van de (in)effectiviteit van beveiligings-maatregelen en de voorspellende waarde van modellen worden gedeeld, bijvoorbeeld met een meldplicht voor datalekken. Onvoldoende kennis bij het ontwikkelen en managen van beveiliging resulteert in meer onzekerheid en in meer kosten of grotere risico's.

Beveiliging is geen onderdeel dat aan het einde van een project op de geleverde producten kan worden geschroefd. Om de beveiligingsrisico's van projecten en de inzet van eindproducten te beheersen, moeten beveiligings-experts zo vroeg mogelijk worden betrokken bij de ontwikkeling. Daar waar deze experts onverantwoorde risico's signaleren, moeten processen worden aangepast of losser aan elkaar worden gekoppeld.

Het verminderen van complexiteit van systemen maakt risico's beter beheersbaar. Maar als standaardisatie van systemen binnen één sector te ver doorschiet, vergroot dat het risico op een cascade uitval. Organisaties kunnen bijvoorbeeld wel standaardsoftware kiezen, maar om risico's te spreiden mogen organisaties binnen kritische sectoren niet allemaal dezelfde software gebruiken. Meerdere bewegende doelen zijn namelijk moeilijker te raken dan één doel. Het toepassen van Open Standaarden bevordert diversiteit in gekoppelde systemen, en is daardoor een voorwaarde om single-points-of-failure te voorkomen. Een extra argument is dat innovatie naast flexibiliteit ook diversiteit vergt.

Na een aarzelende start vanuit een theoretisch model, ontwikkelt quantum-computing zich momenteel snel. De impact daarvan op de huidige encryptiemethodes moet worden bewaakt. Deze ontwikkeling illustreert dat de kennis van mensen èn opleidingen voor beveiliging met hun tijd moeten meegaan. Maar naast actuele en relevante kennis heeft de moderne informatiebeveiliger tegelijkertijd een "management interface" nodig – om binnen de organisatie realistische verwachtingen te scheppen en draagvlak te krijgen voor inhoudelijk goede plannen.

Referenties

[10] Zie "ICT Barometer over cybercrime", Jaargang 11, 25 maart 2011 op www.beveiligingswereld.nl

[11] Deze aanname is gebaseerd op "On Software Diversification, Correlated failures and Risk Management", blz 8, P. Chen e.a., 2006. Soms zijn malware besmettingen aan elkaar gerelateerd. Bijvoorbeeld de Citadel malware plaatste het Dorifel virus op computers die al onderdeel waren van het Citadel botnet. Dat geval wordt geteld als één besmetting, omdat Dorifel een manifestatie was van de Citadel malware.

[12] Aangenomen wordt dat het aantal jaarlijkse malware infecties Poisson verdeeld is en de populatie uit twee groepen bestaat. Groep 1 rapporteerde over 2009 (Ï1 = 0) malware infecties. Met de verhouding p(x > 1) / p(x = 1) kan Ï2 van groep 2 worden berekend. Daaruit volgt dat groep 1 uit 51% van de populatie bestaat, groep 2 omvat 49% en heeft (Ï2 = 1,5) infecties per jaar.

[13] "Epidemic outbreaks in complex hetergeneous networks", Y. Moreno e.a., 2002

[14] Zie Duitsland in 1922 (1$ = 1000.000.000.000 Mark) en Zimbabwe met (officieel) 100.000% inflatie in 2008.

[15] "Antifragility, Things that gain from Disorder", chapter 18, N. Taleb

[16] "Power Laws, Pareto distributions and Zipf's law", M.E.J. Newman, 2006

[17] Rapport over "Regional food prices", Juli 2010, Wordbank.org

[18] Zie Daniel Kahnemans Systeem I en II in "Thinking Fast and Slow".

[19] "Merchants of Doubt", N.Oreskes, E. Conway, 2010

[20] Zie de zaak Kitzmiller vs. Dover Area School District

[21] Zie het Computable.nl artikel "Incident Response broodnodig" deel 1 en deel 2, 2006.

[22] "Ziekenhuismiddelen in verband. Een empirisch onderzoek naar productiviteit en doelmatigheid in de Nederlandse ziekenhuizen 2003-2009", Jos Blank e.a., TU Delft, 2011

[23] "Gemeentelijke schaalvergroting levert geen geld op", Maarten Allers, Coelo.nl 2010.

[24] Andere fusies die als mislukt zijn gelabeld: Nuon en Essent (2007), UvA en HvA (2012), de provincies Noord-Holland, Utrecht en Flevoland (2014); zie ook "9 Mergers That Epically Failed"op huffingtonpost.com

[25] "Antifragile: things that gain from disorder", chapter 5, Nicolas Taleb, 2012

[26] "How Complex Systems Fail", R.I. Cook, 2005

[27] "On Governors", Maxwell, Proceedings of the Royal Society, No.100, 1868.

[28] "Vulnerability of Power Grids to Cascading Failures", T. Verma, 2012; "Damage Reduction of Cascade Tripping in High Voltage Power Grids by means of Intentional Islanding", B. Kamphorst, 2013

[29] "The extreme vulnerability of interdependent spatialy embedded networks", Nature Physics ,25 aug 2013

[30] "Massive hack hit 760 companies", http://money.cnn.com, 28 oktober 2011

[31] "Tackling Cybercrime: Divide and Conquer", H.J. van der molen, isaca.org, 2010

[32] "Globally networked risks and how to respond", D. Helbing, 2013.

[33] "The Atlas of Economic Complexity", Harvard, 2013

[34] "Selecting Cryptographic Key Sizes", A.K. Lenstra & E. Verheul, 2001

[35] "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", P.W. Shor, 1996

[36] "The Future of Cryptography Under Quantum Computers" M.A. Barreno, 2002

[37] "Quantum Factorization of 143 on a Dipolar-Coupling NMR system", N. Xu e.a., 2011

[38 "Signatures of Majorana Fermions in Hybrid Superconductor-Semiconductor Nanowire Devices", 2012, L. Kouwenhoven e.a..

[39] "Samen bouwen aan een quantumcomputer, interview met Leo Kouwenhoven", 2014, QuTech.nl

[40] Het gaat hier bijvoorbeeld om RSA, DSA, Diffie-Hellman, El Gamal, ECDSA en ECC.

[41] "Introduction to post-Quantum cryptography", 2008, Daniel J. Bernstein