De digitale transitie die zich momenteel voltrekt, verbindt wereldwijd systemen en netwerken. Dat schept niet alleen ongekende mogelijkheden, het vergt ook extra aandacht voor informatiebeveiliging.

Huub Stiekema

Geen kostenpost, maar een voorwaarde

Digitale veiligheid

Waar kritische infrastructuur bewaakt worden, en waar fysieke- en monetaire infrastructuren extra beveiligd worden, blijft de beveiliging van digitale infrasructuren een zorgenkindje

Anno 2015 leven we in een wereld die volop in beweging is, steeds groter wordt, waar technische systemen steeds verder geïntegreerd worden met als gevolg dat de controle op technologie steeds vaker buiten de grenzen van de eigen organisatie valt.
Die snel veranderende wereld heeft twee drivers. Ten eerste de digitale transformatie die leidt tot een netwerkeconomie van ongekende omvang *(zie Informatie, december 2014)*. Een tweede belangrijke aanjager is de ontwikkeling van het Internet of Things (IoT) of ook wel het Internet of Everything (IoE) genoemd.
De netwerkteconomie en het Internet of Everything (IoE) bieden ongekende kansen en mogelijkheden en kunnen derhalve een zeer positieve impact op de maatschappij hebben (kader Thingfullness). Dat kan echter alleen als de onderliggende infrastructuur toegankelijk, beschikbaar, betaalbaar, veilig, interoperabel, veerkrachtig en stabiel is en blijft. Systemen in beweging (transitie) zijn over het algemeen kwetsbaar en de mate waarin die kwetsbaarheid geappreciëerd wordt of gemitigeerd kan worden, bepaalt het tempo waarop digitalisering zich verder kan ontwikkelen. Connectiviteit op het internet in combinatie met adequate informatiebeveiliging is daarmee een maker of kraker voor verdere digitalisering. Permanente aandacht voor beveiliging is daarom een must.

Inspiratie door de achterstand

Door allerlei incidenten op mondiale schaal – onder andere de recente digitale actie tegen filmmaker Sony, waar Noord-Korea voor verantwoordelijk wordt gehouden – is het besef dat digitalisering de samenleving ook kwetsbaar maakt, inmiddels goed doorgedrongen.
Maar waar kritische infrastructuur zoals gas, licht en water bewaakt worden, en waar fysieke- en monetaire infrastructuren extra beveiligd worden, blijft de beveiliging van digitale infrasructuren een zorgenkindje. Daar zijn drie belangrijke oorzaken voor.
De eerste is dat de digitale omgeving zo enorm is uitgebreid dat controle steeds lastiger wordt. Connectiviteit is goed, maar de omvang van de te beveiligen omgeving is aanzienlijk groter geworden en groeit dag in dag uit. Vergelijk het met de fysieke wereld. De beveiliging van een gebouw met een duidelijke in- en uitgang is te overzien, terwijl het beveiligen van een grote manifestatie als zeer complex wordt beschouwd. De mate waarin een individu of organisatie controle heeft over de omgeving bepaalt de complexiteit van de beveiliging. Wordt die controle minder of verdwijnt die zelfs helemaal, dan neemt de complexiteit exponentieel toe, tot op het niveau dat een individu of organisatie de complexiteit niet meer kan bevatten. Met de technologische ontwikkeling als cloudcomputing, big data, mobiele toegang, de versmelting van het privé- en zakelijke leven en de internationalisering, neemt de complexiteit met grote sprongen toe.
Ten tweede leidt de huidige digitalisering tot druk op de bedrijfseconomische indicatoren *(zie Informatie, december 2014)* en neemt de druk op vernieuwing van IT in gelijke mate toe. IT-organisaties hebben minder budget, maar moeten daarmee wél de vernieuwing in de business én de complexe informatiebeveiliging en privacy-gerelateerde onderwerpen in goede banen leiden:

Thingfullness

Het Internet of Everything (IoE) combineert in feite 'person-to-person (P2P)'-, 'machine-to-machine (M2M)'- en 'machine-to-person (M2P)'-communicatie en introduceert pas echt het big data- tijdperk. Elke mens, elk proces, elke organisatie en elk apparaat – groot of klein, complex of eenvoudig – krijgt een IP-adres en wordt een sensor of node op het netwerk. Elke node is in staat informatie uit te wisselen met duizelingwekkende snelheid. Het verandert de manier waarop we leren, werken, spelen, communiceren, veilig zijn, oud worden, gezond blijven en liefhebben.
Het opvangen, analyseren en interpreteren van die enorme hoeveelheid informatie leidt tot nieuwe (business)mogelijkheden, zoals: efficiënter energieverbruik, betere woonomstandigheden, minder CO2-uitstoot, een gezonder leven of meer veiligheid. De noodzaak, of vraag, naar deze ontwikkeling zal vanuit een maatschappelijk en economisch besef enorm zijn en onomkeerbaar.
Gartner voorspelt dat het Internet of Everything in 2020 in totaal 26 miljard verbonden apparaten telt. Netwerkleverancier Cisco gaat nog een stap verder en voorspelt dat volgend jaar al 25 miljard apparaten verbonden zullen zijn. Voor 2020 voorspelt Cisco een totaal van 50 miljard verbonden apparaten.
Vrijwel alle bekende marktonderzoekers zien gigantische economische kansen en nieuwe markten opkomen. Om dit enigszins te begrijpen is het van belang om enkele macro-economische trends te beschouwen. Het Internet of Everything representeert een zeer waardevolle markt waarin:

- 3 miljard 'abonnees' 24/7 informatie willen ontvangen, bereid zijn daarvoor te betalen, en daarmee hun levensstandaard verhogen en hun persoonlijke veiligheid verbeteren. In een volwassen markt heeft elke consument tussen de 5 à 10 aangesloten apparaten;
- 1,5 miljard 'smart cars' verbonden zijn met internet en voor een grotere gebruiksdichtheid en veiligheid zorgen;
- 3 miljard 'smart meters' voor gas, licht en water, gigantische hoeveelheden data verzamelen en via het internet afleveren ten behoeve van data-analyse.

De positieve impact, die het IoE kan hebben op de maatschappij als geheel, kan alleen maar worden geborgd zodra de infrastructuur toegankelijk, beschikbaar, betaalbaar, veilig, interoperabel, veerkrachtig en stabiel blijft.

méér doen met minder. Tegelijkertijd zien CIO's dat zodra de ontwikkelingen aan de businessziide niet vlot genoeg gaan, de business inventief genoeg is om beschikbare services van internet zoals Dropbox, Evernote of iCloud te gaan gebruiken. Ook dit introduceert weer nieuwe risico's en valkuilen.
De derde en laatste oorzaak wordt meer geïnitieerd vanuit het domein van het Internet of Everything. In dit hypermoderne domein convergeren traditionele fabrikanten naar fabrikanten met een IP-adres. Technologisch is dat niet moeilijk, maar vanuit het oogpunt van informatiebeveiliging en privacywetgeving is het enorm complicerend. Onder meer omdat de partijen met wie men 'linkt' niet native zijn, onder andere jurisprudentie vallen en daarmee een risico voor de informatiebeveiliging vormen.
Wat hiervan de consequenties zijn laat zich wellicht helder illustreren door ontwikkelingen in de automobielindustrie. Autofabrikanten zijn thuis in fysieke omgevingen en hebben zich sterk ontwikkeld in de richting van design, veiligheid, vermogen en verbruik. Met name op het terrein van fysieke veiligheid zet de automobielindustrie al decennialang de toon. Maar door de ontwikkeling van de zelfrijdende auto moeten zij hun denken nu formeren rondom de veiligheid van passagiers in een digitale context, wat voor hen een heel nieuw aandachtsgebied is.

Dat overkomt ons niet

Als ontwikkelingen zo snel gaan en overduidelijk is wat de richting is, dan lijkt het aannemelijk dat elke overheidsinstelling, elke ondernemer en elke burger op voorhand adequate maatregelen neemt. Helaas zien we in de praktijk, zowel bij het mkb als bij grote organisaties, dat informatiebeveiliging en bescherming van privacy dikwijls geen prioriteit hebben. "Dat overkomt ons toch niet", blijft de meest gehoorde reactie op de vraag of een onderneming voldoende beschermd is tegen inbreuken op de informatie-infrastructuur. Bestuurders en directieleden van organisaties zijn vaak van mening dat de ICT-beveiliging afdoende is. Er is immers flink geïnvesteerd in technische middelen zoals firewalls, intrusion detection en accessmanagement. Daarnaast denkt men vaak dat ze niet interessant genoeg zijn of dat ze niets te verbergen hebben.
De virtuele risico's worden door ondernemers nog zwaar onderschat, terwijl de praktijk van alledag uitwijst dat elke onderneming – groot of klein, rijk of arm, privaat of publiek – doelwit is van cyberactiviteit. De belangrijkste reden daarvoor is dat hackers vanuit een netwerkgedachte naar hun doel toewerken. Hun doel ligt misschien niet bij de onderneming zelf, maar de onderneming kan wel op de weg náár het doel van de hacker liggen. Kortom, een onderneming kan zelf het doelwit zijn omdat de onderneming van waarde is voor de hacker. Een onderneming kan ook, onbedoeld, onderdeel gaan uitmaken van een botnet en daarmee de virtuele infrastructuur vormen voor eventuele criminele activiteiten. Daarnaast kan elke onderneming, zeker wanneer men actief is in een interessante branche, middels social engineering het doel van de hacker dichterbij brengen.
De vraag is dus niet óf bedrijven en organisaties doelwit worden van cybercriminaliteit, maar wat de organisatie gedaan heeft om de consequentie voor de bedrijfscontinuïteit en bescherming van de privacygevoelige gegevens te waarborgen.

Tot slot

De gevolgen van cybercrime kunnen groot zijn. Verlies van klantinformatie of personeelsgegevens, geheime product- en procesontwerpen, octrooien, het in verkeerde handen komen van betaalkaartgegevens, schade aan het IT-netwerk, derving van online inkomsten, aansprakelijkheidsclaims en reputatieschade. Het zijn reële risico's die door veel ondernemers en publieke bestuurders nog worden onderschat.
De afgelopen paar jaar is gebleken dat overheden, bedrijven, burgers en kennisinstituten wel veel inspanningen leveren om informatie te beveiligen, maar dat de werkelijke ontwikkelingen en doorbraken achterblijven. Indicatoren wijzen enerzijds uit dat allerlei organisaties en instellingen juist daardoor een steeds groter ongemak voelen bij het gebruik van het internet, maar anderzijds dat zij er steeds méér gebruik van maken.
In de praktijk blijkt dat de onbekendheid en onwetendheid van directies, toezichthouders en financiers hieraan debet is. Dat heeft vooral te maken met het beperkte begrip van technologie en digitalisering. Daarnaast blijkt dat directies in veel gevallen onwetend zijn van het aantal cyberaanvallen of beveiligingsincidenten omdat de ICT-verantwoordelijken de aanvallen gewoon niet melden.
Ook blijkt dat organisaties die slachtoffer van cybercriminaliteit zijn geworden hier tot nu toe zo weinig mogelijk ruchtbaarheid aan geven vanwege mogelijke reputatieschade.
Dat leidt ertoe dat directies en toezichthouders nog op traditionele indicatoren sturen en niet de juiste vragen over informatiebeveiliging stellen. Een boardroom die beseft dat 70 procent van de waarde van de onderneming afhankelijk is van informatie, en weet dat die informatie wellicht niet afdoende beveiligd is, zal andere vragen gaan stellen en op andere indicatoren gaan sturen. De conclusie is dat om de ontwikkelingen ter zake te stimuleren dat de bewustwording bij directeur-grootaandeelhouders, directies, toezichthouders, financiers en bestuurders van publieke diensten sterk moet toenemen.

Met dank aan: R. van den Vossen, Cyco en Asim Jahan (voorzitter Ngi-NGN Special Interest Group Informatiebeveiliging).

Huub Stiekema (hstiekema@interimpoint.nl) is adviseur strategisch management, medeoprichter van MKB Cyber Advies Nederland en voorzitter van de Ngi-NGN Special Interest Group Digitale Transformatie. MKB Cyber Advies Nederland adviseert mkb-directies, toezichthouders en financiers van mkb-ondernemingen op het gebied van informatiebeveiliging en bedrijfscontinuïteit.

Meldplicht

Door het geschetste maatschappelijk belang heeft de wetgever ook niet stilgezeten. Vorig jaar werd een wetsvoorstel ingediend voor de Wet bescherming persoonsgegevens (Wbp) en de Telecommunicatiewet. De wijziging betreft een invoering van een meldplicht voor datalekken van privacygevoelige gegevens. Een verandering die met ingang van 2015 van toepassing is. Daarmee krijgt het College bescherming persoonsgegevens (CBP) zelfstandig de bevoegdheid een bestuurlijke boete op te leggen bij overtreding van regels van maximaal 450.000 euro. In het concept van de Europese verordening worden zelfs boetes genoemd die kunnen oplopen tot 5 procent van de wereldwijde omzet van de onderneming. Deze meldplicht en verordeningen zullen een hele nieuwe fase inluiden in de bewustwording van cyberrisico's en gevolgschade. Door deze meldplicht zal aan veel meer incidenten ruchtbaarheid moeten worden gegeven om de digitale snelweg voor iedereen open te houden: veilig, waakzaam en veerkrachtig.