Capgemini Consulting

Geen digitalisering zonder digitale veiligheid

Digitale transformatie van samenleving en economie

De digitale transformatie van onze maatschappij biedt enorme perspectieven voor de toekomst en is de motor achter de huidige economie. De snelheid van de digitale ontwikkelingen en de mate waarin deze door de maatschappij zijn omarmd, leiden tot vergaande afhankelijkheid van digitale innovaties en dwingt iedereen om mee te gaan in het digitale transformatieproces.

Voor bedrijven en instellingen betreft deze digitale transformatie onder andere het digitaliseren van bedrijfsprocessen. Dit staat internationaal hoog op de agenda, blijkt uit een onderzoek dat Capgemini Consulting en MIT uitvoeren[1]. Mobiele diensten, sociale media, tablets, analytics (big data) en embedded software zijn belangrijke technologische ontwikkelingen die met een ongekende snelheid worden omarmd door zowel organisaties als klanten. De wijze waarop organisaties omgaan met deze digitale transformatie (en de daarmee gepaard gaande digitale risico's) hangt af van twee elementen: de digitale intensiteit (wat) en het transformatiestijl (hoe). Uit het onderzoek van Capgemini Consulting en MIT blijkt dat organisaties (publiek en privaat) zijn in te delen in vier typen: Beginners, Fashionistas, Conservatieven en Digirati.

De druk om te digitaliseren is groot en de wens komt voort uit klanten, het eigen personeel en de concurrentie. Investeringsbeslissingen worden echter veelal vanuit een economische argumentatie genomen zonder veel oog te hebben voor de risico's[2].

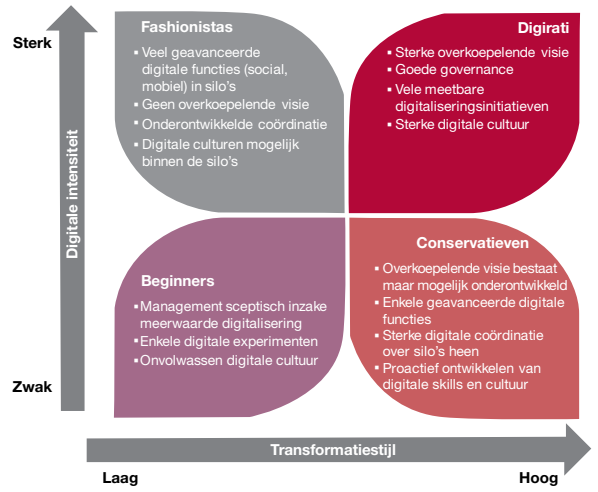
Digitale veiligheid is een randvoorwaarde voor digitalisering

De digitale transformatie kan alleen maar duurzaam plaatsvinden indien digitale veiligheid simultaan hieraan wordt georganiseerd. De digitale ontwikkelingen geven naast vele mogelijkheden en kansen, namelijk ook ruimte voor kwetsbaarheden en misbruik. Veel informatie die we opslaan,

[1] Digital Transformation Review N° 02, January 2012; Capgemini Consulting, MIT Center for Digital Business.

[2] Bauer J.M.; Eeten M; "Introduction to the economics of Cyber Security", Communications & Strategies, N° 81.Business.

Figuur 1: Vier typen 'digitalen'



verwerken of uitwisselen of (denken te) verwijderen, heeft door de toegenomen afhankelijkheid steeds meer waarde. De sterke gebondenheid met de hedendaagse digitale ontwikkelingen dringt diep door in ons dagelijks leven. Denk maar aan het gebruik van online bankieren of het gebruik van de ov-chipkaart. Dit zijn digitale omgevingen waarin uw financiële en persoonsgegevens zijn opgeslagen. De gehele samenleving kan niet meer zonder goed functionerende en veilige ICT-systemen. Storingen (in bijvoorbeeld het betalingsnetwerk) zorgen voor een grote impact in onze maatschappij. Zowel organisaties als individuele gebruikers vertrouwen op de veiligheid en werkzaamheid van digitale systemen. Of in woorden van de Europeese Commissie: *"The more we depend on the internet – the more we depend on its security."*[3]

De combinatie van afhankelijkheid, hoge waarde en kwetsbaarheid, trekt kwaadwillende personen. Gedreven door nieuwsgierigheid, persoonlijk gewin, activisme, landsbelang of gewoon voor de kick, kunnen zij veel materiële en immateriële schade veroorzaken. De weinige harde cijfers die er zijn ten aanzien van cybercrime, digitale spionage, hacktivisme, cyberwarfare en cyberterrorisme, laten een stijging zien van digitaal misbruik. Het Cybersecuritybeeld Nederland 2012 geeft aan dat cybercrime en digitale spionage net als vorig jaar de grootste dreiging vormen voor overheden, bedrijven en burgers. Hacktivisten, technisch falen en andere niet-opzettelijke incidenten zijn dat in mindere mate.[4] Banken rapporteren al enkele jaren stijgende cijfers over schade bij internetbankieren.[5]

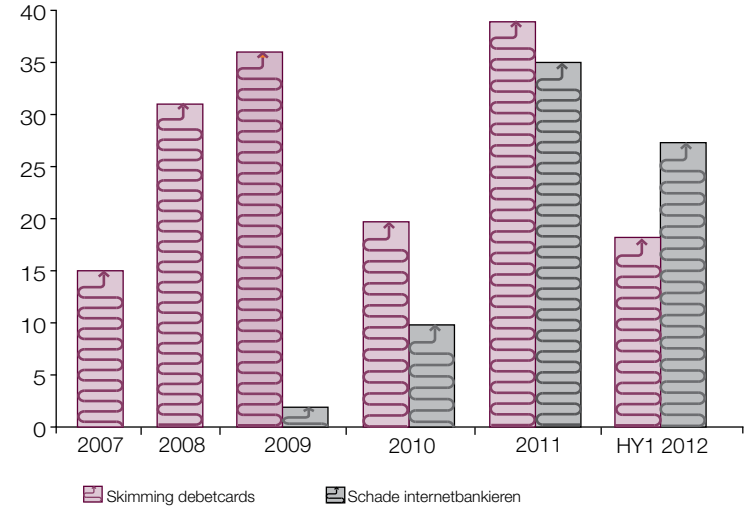
Digitale dreigingen moeten serieus en op alle niveaus in de organisatie worden opgepakt. Digitale dreigingen vormen een relatief nieuwe dimensie van een breed scala aan dreigingen die de organisatie dient te mitigeren. Het vormt daarmee een aanvulling op de set van veiligheidsrisico's van een organisatie. Digitale veiligheid is een normale randvoorwaarde voor de continuïteit van de organisatie en moet onderdeel van een integrale veiligheidsbenadering. Organisaties kunnen digitale veiligheid niet langer onderschatten en zullen hun verantwoordelijkheid moeten nemen. Maar hoe moet de invulling van digitale veiligheid eruit zien en welke nieuwe inzichten zijn daarbij belangrijk?

[3] Eurocommissioner Neelie Kroes, The Digital Agenda two years on: is Europe well-placed?, 12 June 2012 (press release).

[4] Nationaal Cyber Security Centrum. (2011) Cybersecuritybeeld Nederland CSBN-2. Den Haag: Ministerie van Veiligheid en Justitie.

[5] http://www.nvb.nl/home-nederlands/nieuws/nieuwsberichten/fraude-internetbankieren-stijgt-eerste-half-jaar-met-14_.html

Figuur 2: Gerapporteerde schade v.a. 2007 t/m eerste half jaar 2012 in miljoenen euro's (bron: zie voetnoot 5 op vorige pagina)



De nieuwe wereld: ga ervan uit dat u wordt gehackt

De traditionele benadering van informatiebeveiliging, waarbij aan de buitenkant van de organisatie (vuur-) muren werden opgetrokken om het kwaad buiten te houden, is niet meer houdbaar. Medewerkers maken immers gebruik van internet, sociale media, mobiele apparaten, tablets, werken ook thuis of brengen hun eigen apparatuur mee naar kantoor[6]. Digitale buitengrenzen van de organisatie vervagen en de kwetsbaarheid voor dreigingen verhoogt. Het bewust of onbewust verspreiden van virussen en andere malware, onvoldoende beveiligde websites en webapplicaties, toegangsbeveiliging die eenvoudig is te omzeilen, niet bijgewerkte software, het gebruik van mobiele apparaten, het gebruik van big data en de effecten daarvan zijn zaken waar iedere organisatie zich tegen moet bewapenen. Of er wordt toegestaan dat een leverancier onderhoud pleegt en een besmette laptop aan uw netwerk aansluit, of iemand plugt een USB-stick met een virus in tijdens een presentatie.

Organisaties zullen bij de planning en maatregelen er vanuit moeten gaan dat hun digitale muren doordringbaar zijn, zelfs als de kritische netwerken niet direct met het internet verbonden zijn. Ook afzonderlijke onderdelen van de ICT-omgeving kunnen kwetsbaarheden bevatten en alleen al door de toenemende complexiteit van ICT-systemen en de manier waarop zij in verbinding staan met andere systemen en mensen ontstaat kwetsbaarheid.[7] Dat een organisatie gehackt kan worden, betekent dat het accent van de veiligheidsmaatregelen verschuift van het steeds hoger maken van de digitale muren (weerbaarheid) naar de capaciteit veerkrachtig ('resilient') op te kunnen treden. Detectie van, en de respons op incidenten ('recovery') moeten worden georganiseerd. Om de hinder voor klanten en het eigen bedrijfsproces te minimaliseren, is aandacht nodig voor het herstellend vermogen en continuïteitsmanagement.

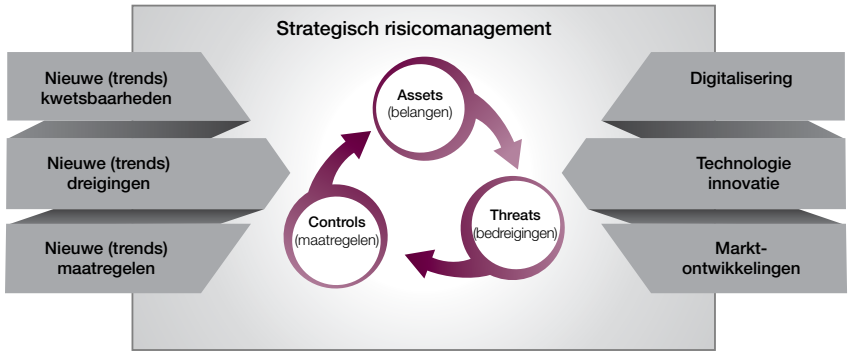
Als hogere muren niet voldoende zijn, wordt het beveiligen van kleinere delen binnen de muren relevanter. Dergelijke 'defense in depth' zorgt ervoor dat een aanvaller die eenmaal binnen is niet overal door kan dringen. Dit kan bijvoorbeeld worden gerealiseerd door delen van het netwerk in verschillende, afgescheiden netwerken (zonering) of door afzonderlijke ICT-systemen zwaarder te beveiligen dan de rest van de omgeving waarin ze staan. Daarnaast kan de beveiliging nog dieper: op het niveau van de data zelf.[8]

[6] Nationaal Cyber Security Centrum. (2011) Cybersecuritybeeld Nederland CSBN-2. Den Haag: Ministerie van Veiligheid en Justitie.

[7] Weijnen, M., Bruijne, M.de; "Complexiteit: de nieuwe realiteit van vitale infrastructuren", 3 april 2012.

[8] Jericho Forum® Data Protection; https://www2.opengroup.org/ogsys/catalog/W12C

Figuur 3: Strategisch risicomanagement in het kader van cyber security



Digitale veiligheid is onderdeel van strategisch risicomanagement

De weerbaarheid kan worden vergroot door zowel aan de binnenkant van de organisatie als aan de poort te monitoren. Echter het is van groot belang dat men ook op de hoogte blijft van ontwikkelingen buiten de organisatie, zoals: in hoeverre heeft de digitale buitenwereld impact op de organisatie? Is er bijvoorbeeld sprake van malware die cruciale elementen uit de ICT tot doelwit heeft? Is de organisatie op de hoogte van hoe er over haar wordt gesproken op (underground) fora? Geeft de informatie op social media inzicht in op handen zijnde aanvallen? Zijn er bij vergelijkbare partijen aanvallen geweest waar organisaties van kunnen leren? Loont het om te investeren in cyber threat intelligence, wanneer digitale belangen (heel) groot zijn? Cyber threat intelligence versterkt het omgevingsbewustzijn (ook wel 'situational awareness') en kan ervoor zorgen dat de organisatie meer tijd krijgt om zich voor te bereiden op een incident.

Aanvullend is versterking van het omgevingsbewustzijn over de digitale wereld ook nodig op senior management niveau. Digitale onveiligheid raakt namelijk belangrijke 'assets' van de organisatie, zoals bijvoorbeeld geld, intellectueel eigendom, continuïteit van processen, gegevens van klanten, en imago. Voor de boardroom moet daarom duidelijk zijn welke risico's de organisatie loopt en welke maatregelen nodig en gerechtvaardigd zijn op basis van de kritieke assets. Een cyber dashboard voor senior management helpt om een goed beeld te krijgen en te houden en daarmee met de juiste informatie sturing te geven, als onderdeel van het totale strategisch risicomanagement. Dit geldt ook voor het nationaal niveau. Het cyber dashboard is geen technisch dashboard, maar een vertaling van digitale trends (zowel positief als negatief) naar actuele en voor de organisatie kritische parameters. Dit voorkomt een focus op incidenten.

Een integrale aanpak zoekt synergie met andere vakgebieden

Cybersecurity is vanwege het belang van ICT voor de organisatie bij uitstek een onderwerp voor de boardroom. Er zijn namelijk genoeg organisaties waarbij uitval van ICT (of de elektriciteit die de ICT draaiende houdt) zal betekenen dat veel werk stil komt te vallen. Denk aan webwinkels of banken, maar ook transport, de elektriciteitsvoorziening of administratieve processen bij overheden en bedrijven. Zo zijn er genoeg voorbeelden waaruit die afhankelijkheid ook blijkt.

Door gericht aan de buiten- en binnenkant van uw organisatie te investeren in beveiliging (defense in depth), kunt u beter balanceren tussen de mate van veiligheid en de kosten die daarmee samenhangen. Wat is het risico in termen van kans en impact en wat is daartoe een gerechtvaardigde investering? U kunt efficiënter beveiligen wanneer u het opschalen van een hoger beveiligingsniveau weet te beperken tot die onderdelen die dat ook echt nodig hebben.

Kortom:

- Ga ervan uit dat u wordt gehackt;
- accepteer uw kwetsbaarheid;
- focus op 'resilience' en 'recovery';
- pas uw beveiligingsniveau aan op kleinere extra gevoelige onderdelen;
- investeer in cyber threat analysis;
- geef senior management een middel, zoals een cyber dashboard, waarmee ze kunnen sturen.

In de praktijk blijkt de aandacht voor digitale veiligheid echter minder groot te zijn, dan je zou verwachten9. Zoals gezegd vormen digitale dreigingen een aanvulling op de bestaande veiligheidsrisico's van een organisatie. Cyberrisico's moeten onderdeel zijn van het cyclische proces van strategisch risicomanagement, waarbij periodiek belangen (assets), dreigingen en risico's en maatregelen (controls) worden geëvalueerd. Cyberrisico's zijn daarbij slechts één dimensie waar de organisatie rekening mee moet houden. Een integrale aanpak kijkt ook naar dreigingen en kwetsbaarheden vanuit andere dimensies zoals fysieke verstoring (moedwillig of 'acts of God' c.q. security en safety), milieu-risico's, arborisico's en eventueel financiële risico's. Alleen al daarom is een integrale aanpak nodig, waarbij gestreefd wordt naar synergie en samenwerking met disciplines zoals hr, finance, communications, legal en strategy. Alleen door deze integrale aanpak kan de bestuurder 'in control' zijn over de veiligheid in de organisatie. De uitdaging voor een organisatie is er om doormiddel van de juiste maatregelen mix in de dimensies 'mens', 'technologie' en 'organisatie' de belangen te beschermen. Onderstaande figuur geeft een overzicht van de samenhang om als organisatie 'in control' te zijn.

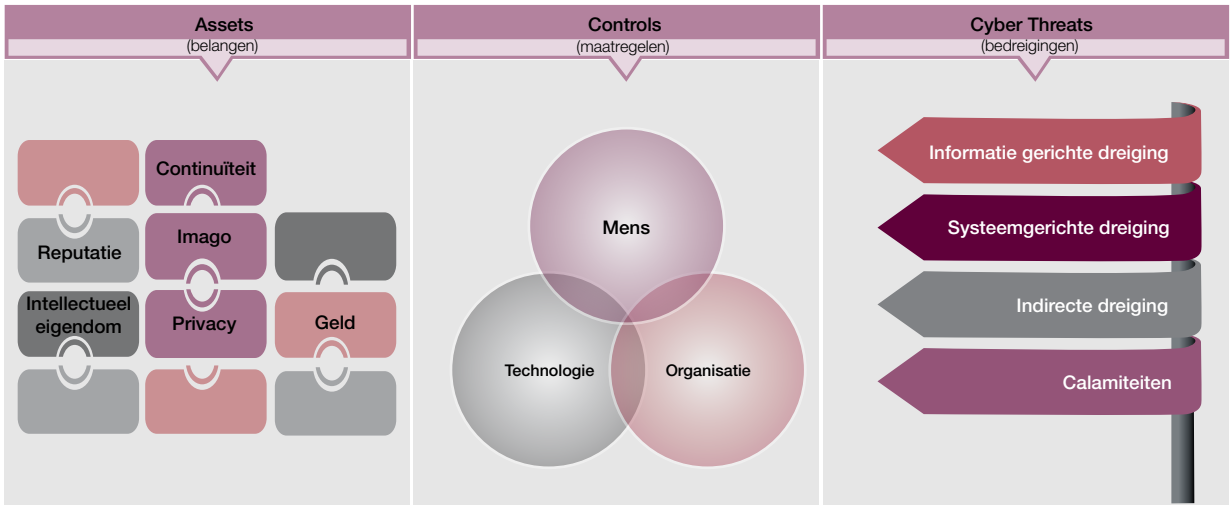
Cybersecurity is mensenwerk

Hoe technisch 'cyber' ook lijkt, cybersecurity omvat veel meer dan technologie. Juist de mens en de organisatie zijn belangrijke dimensies voor een veilige digitale omgeving. In elk van deze drie dimensies, bevinden zich kwetsbaarheden, maar ook mogelijkheden om de schade te voorkomen of te beperken (maatregelen).

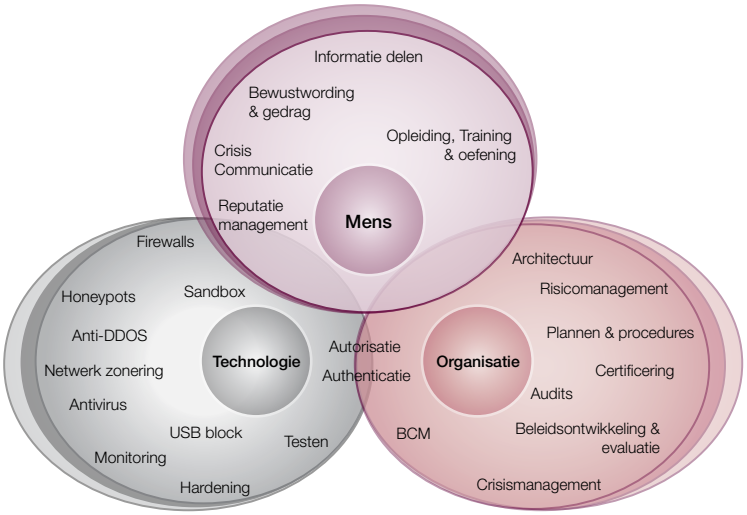
Technologische maatregelen voor het beveiligen van waardevolle assets in de organisatie zoals hardware, netwerken, besturingssystemen, administratieve bedrijfssystemen, industriële procescontrolesystemen (ICS of PCS) en webapplicaties, is een noodzakelijke stap. Het is daarom goed te blijven investeren in klassieke informatiebeveiligingsmaatregelen zoals bijvoorbeeld: firewalls, netwerk beveiliging, identity and accesmanagement, monitoring.

Organisatorische maatregelen in de vorm van een beveiligingsbeleid, koppeling aan de organisatiedoelstellingen, financiering, crisismanagement, wet- en regelgeving en eigen richtlijnen en de inrichting van bedrijfsprocessen is essentieel voor cybersecurity en zorgt voor een volwassen en veerkrachtige organisatie die snel weer een normale situatie kan creëren.

Figuur 4: Integrale benadering



Figuur 5: De drie dimensies van cybersecurity met voorbeelden van controls



In veel opzichten staat echter de mens centraal en wordt deze ook vaak de 'zwakste schakel' genoemd. Maatregelen in de dimensie mens zijn gericht op bewustwording, gedrag en informatie uitwisseling. Versterking van het omgevingsbewustzijn over zowel de cyberdreigingen als de ontwikkelingen in de digitale wereld is noodzakelijk op alle niveaus in de organisatie (strategisch, tactisch en operationeel). Op elk niveau zijn verschillende maatregelen aan te grijpen. Awareness staat of valt dus met de implementatie van maatregelen op alle drie de lagen in de organisatie.

De mens kan vanuit drie rollen te maken krijgen met cybersecurity. Als gebruiker, als besluitvormer en/of zijn adviseur en als expert.

- De medewerker/gebruiker (ook thuis): is hij voldoende op de hoogte van de risico's die hij zelf loopt en in staat om maatregelen te treffen om bijvoorbeeld besmetting met een computervirus te voorkomen of te verwijderen? Houdt hij zich aan de spelregels? Bij deze groep zijn bewustwording (of awareness) en basiskennis van dreigingen belangrijk.

- De besluitvormer en diens adviseurs: is deze doelgroep voldoende geïnformeerd over incidenten en strategische risico's? Is deze doelgroep in staat om bij incidenten effectief te sturen op herstel? Hoe kan op een effectieve manier worden samengewerkt met ketenpartners, branchegenoten en de overheid? Bewustwording, externe samenwerking en een goede vertaalslag van en naar cyber experts zijn van belang.

- De cyber specialist/expert: zijn er kwalitatief en kwantitatief voldoende 'mensen achter de knoppen'? Hoe werken zij samen met de rest van de organisatie in de koude en warme fase (normale gang van zaken en incidenten)? Onder andere capaciteit, motivatie, opleiding, wijze van aansturing en diepgaande kennis zijn van belang.

‘No digital transformation without digital security’

Digitale ontwikkelingen in onze maatschappij dwingt iedereen om mee te gaan in het digitale transformatieproces. Investeren in digitale vooruitgang betekent ook investeren in digitale veiligheid, anders kan de continuïteit van de organisatie niet meer gegarandeerd worden. Gezien de grote potentiële impact van digitale dreigingen is versterking van veerkracht nodig om na incidenten schade voor de eigen organisatie en derden te beperken en terug te veren naar de normale bedrijfsvoering.

Alleen een integrale aanpak waarbij synergie en samenwerking ontstaat met verschillende disciplines in de bedrijfsvoering helpt de bestuurder in control te zijn over de veiligheid van de organisatie. Cybersecurity is hierbij meer dan techniek alleen en ‘de mens’ heeft een sleutelrol in het vergroten van de veiligheid.

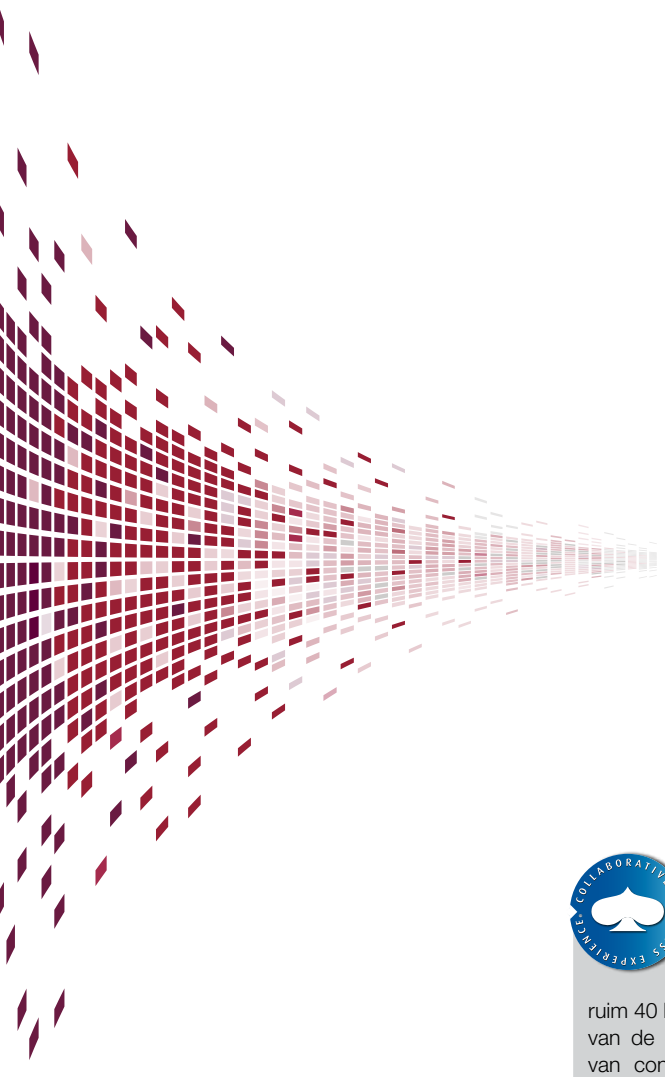
Versterking van het omgevingsbewust-zijn over de digitale wereld op senior management niveau is echter essentieel. Digitale veiligheid moet onderdeel zijn van strategisch risicomanage-ment, wanneer digitale middelen belangrijk zijn voor uw organisatie. Het is een ‘gewone’ randvoorwaarde voor de bedrijfsvoering, net als mensen, geld en kennis. Door cyber threat intelligence en een sturingsinstrument in de vorm van een cyber dashboard krijgen bestuurders meer zicht en grip op digitale veiligheid.

“No digital transformation without digital security!”

Erik Hoorweg
Vice President
Tel. +31 615 030869
erik.hoorweg@capgemini.com

Roeland de Koning
Principal Consultant
Tel. +31 622 206055
roeland.de.koning@capgemini.com

Capgemini Consulting



Over Capgemini

Met meer dan 145.000 mensen in ruim 40 landen is Capgemini wereldwijd een van de meest vooraanstaande aanbieders van consulting-, technology- en outsourcingdiensten. In 2014 rapporteerde Capgemini Group een omzet van 10,571 miljard euro. Samen met zijn klanten creëert en realiseert Capgemini resultaatgerichte business- en technology-oplossingen, toegesneden op de klantbehoefte. Als een cultureel diverse organisatie heeft Capgemini zijn eigen onderscheidende manier van werken, de Collaborative Business Experience™. Hierbij maakt Capgemini gebruik van het wereldwijde leveringsmodel Rightshore®.

Capgemini Consulting is de wereldwijde organisatie van de Capgemini Group voor transformatie- en strategisch advies, en is gespecialiseerd in het adviseren en begeleiden van ondernemingen bij belangrijke transformaties: van innovatieve strategieën tot strategie-implementatie, waarbij resultaten constant in het vizier worden gehouden. De nieuwe digitale economie veroorzaakt aanzienlijke tumult en creëert kansen. Om de bijbehorende digitale transformatie in goede banen te leiden werkt ons wereldwijde team van meer dan 3600 getalenteerde consultants samen met toonaangevende ondernemingen en overheden. We putten hierbij uit ons inzicht in de digitale economie en ons leiderschap in bedrijfstransformaties en organisatorische veranderingen.

Kijk voor meer informatie op:
www.nl.capgemini-consulting.com

Rightshore® is een handelsmerk van Capgemini

Capgemini Consulting
Postbus 2575 - 3500 GN Utrecht
Tel. +31 30 689 18 50
E-mail: capgeminiconsulting.nl@capgemini.com
www.nl.capgemini-consulting.com