Wim Kweekel, Justus de Bruijn (redactie)

Digitale trends

Hoe als bedrijf om te gaan met de digitale revolutie

- Hoe tegen trends aan te kijken
- De trends
- Ethische en juridische beschouwingen

Kweekel / RGO-Academy

12 Strategische bescherming met business-resilience

Rick Strijbos

Dat de digitalisering steeds verder voortschrijdt en een transformatie van ongekende omvang meebrengt, is helder. En gelukkig begrijpen steeds meer bestuurders dat de security van deze digitalisering steeds belangrijker wordt. Maar wat is dat eigenlijk: security? Deskundigen kunnen u helder uitleggen wat het verschil is tussen IT-security (IT-beveiliging) en information-security. Terwijl de ene persoon onder business-continuity eigenlijk slechts IT-continuity verstaat, begrijpt de ander daarbij ook de complete supplychain-continuity. Als we al deze disciplines effectief en efficiënt in willen zetten, is een integrale aanpak nodig, waarbij ook risico- en crisismanagement goed zijn ingericht. Dat noemen we *business-resilience* (handelend vermogen in kritische omstandigheden).

Wat kunnen bestuurders bereiken door goed richting te geven aan business-resilience? Welke risico's worden hiermee geminimaliseerd en welke kansen optimaal benut? En het belangrijkst: wat is de invloed op de blijvende toegevoegde waarde voor de organisatie? En was u daar al niet toe verplicht op basis van de Corporate Governancecode?

Van weerbaarheid tot business-resilience

We kennen meerdere vormen van weerbaarheid. Zo is psychologische veerkracht het vermogen om mentaal of emotioneel om te gaan met een crisis of om snel terug te keren naar de status van voor de crisis. De digitale resilience van een IT-omgeving is het vermogen om een acceptabel serviceniveau

voor normaal gebruik te bieden en te behouden. Ook bij storingen en andere uitdagingen. Organizational-resilience (ISO 22316:2017) is het vermogen van een organisatie om te absorberen en zich aan te passen aan een veranderende omgeving. Het Security and Continuity (SECO) Institute heeft een aantal disciplines samengebracht in wat zij noemen: Business Resilience.

Daarbij is business-resilience het vermogen van een organisatie om te anticiperen, zich voor te bereiden, te detecteren, te reageren op en zich aan te passen aan substantiële veranderingen en plotselinge verstoringen. Doel is om te overleven en voorspoed te bereiken door managementsystemen te integreren die deze veerkracht bieden en mogelijkheden te ontwikkelen voor een effectieve response op risico's. Hierdoor worden de belangen van de stakeholders optimaal beschermd en de capaciteiten van de organisatie hersteld.

Twee voorbeelden van waar het goed fout ging

Wellicht dat de paragraaftitel u op het verkeerde been zet. Want veel mensen die actief zijn in het securitywerkveld hebben het vooral over wat er mis kan gaan. Of mis is gegaan. En bij de twee voorbeelden die hierna volgen is er veel misgegaan. Maar ook veel goed. En daarvan kunnen we het meeste leren.

Maersk

In 2017 kwam APM Terminals, onderdeel van transportgigant Maersk, volledig tot stilstand door malware (NotPetya). Alle computers bleken besmet en waren geblokkeerd door deze cyberaanval. Het hele bedrijfsproces kwam stil te liggen. Maersk moest het complete IT-systeem (4000 nieuwe servers, 45.000 nieuwe pc's en 2500 applicaties!) volledig opnieuw opbouwen. De kosten: 300 miljoen dollar. Natuurlijk zijn veel (IT-security)deskundigen achteraf kritisch geweest over het patchmanagement en de onvoldoende netwerksegmentering. Allemaal waar. Maar de organisatie valt ook te prijzen omdat zij in tien dagen tijd, door rigoureuze beslissingen, alles vanaf de grond weer heeft opgebouwd. Normaal gesproken duurt zoiets in deze omvang minimaal een halfjaar.

Ging dit voorbeeld nu over alleen IT-security, of ging het over business-resilience? Hoe overleefde APM Terminals deze ramp? De voldoende financiële slagkracht om de grootschalige investeringen in de geheel nieuwe IT-om-

geving direct te kunnen doen, heeft zeker geholpen. Ook dat is veerkracht. En wat te denken van hun hands-on-cultuur. Aanpakken! Resilience is zoveel meer dan alleen IT-security...

Maastricht University

Eind 2019 kregen aanvallers toegang tot het universiteitsnetwerk van de Universiteit Maastricht (UM). Zij versleutelden bestanden op allerlei systemen met ransomware, waardoor systemen, functionaliteiten en programma's voor zowel studenten als medewerkers niet beschikbaar waren. Achteraf bleken de hackers al twee maanden actief in het netwerk. Een maand na de infectie was de universiteit zo goed als helemaal hersteld. De universiteit zag zich gedwongen om de hackers 30 bitcoin te betalen voor het ontsleutelen van de bestanden. Op dat moment was dat 200.000 euro.

Doordat UM de geleerde lessen van de ransomware-aanval via een symposium openbaar maakte, kunnen we nu van tevoren afwegen of we wel of niet toegeven aan dit soort chantagepraktijken. Het is natuurlijk maatschappelijk wenselijk om te zeggen dat je nooit zult toegeven aan chantage, want dat maakt dit soort ransomwareaanvallen een lucratieve business voor criminelen. Maar je zult als organisatie maar voor de afweging staan. Dan helpt het om een plan B gereed te hebben.

De kracht benutten

Business-resilience is meer dan het samenvoegen van wat security- en continuity-disciplines. Het is van belang dat een organisatie zich op strategisch niveau realiseert waarom en wat tegen wat beschermd moet worden. Want welke risico's moeten we in kaart gebracht hebben en hoe verhouden deze zich onderling? Het uitgangspunt is dus riskmanagement als geheel te behandelen waardoor de diverse risico's in perspectief komen te staan. Daarbij is information-security het deelgebied dat zich bezighoudt met 'information-risk'. Deze discipline geeft richting aan IT-security die de technische bedreigingen onder haar hoede heeft. Privacyfunctionarissen hebben vaak de 'compliance & reputation-risk' in hun scope. Met natuurlijk de dwarsverbanden met information-security.

De business-continuity-specialisten houden zich bezig met 'continuity-risk'. Sterk afhankelijk van de aard van een onderneming gaat dit over

het vermogen om de kritisch geprioriteerde activiteiten en processen voort te zetten op vooraf bepaalde, acceptabele niveaus. In de digitale transformatie zijn organisaties steeds sterker afhankelijk van technologie, waardoor de connectie met information-risk-onderwerpen bepalend is of wordt voor goed BCM-beleid. Wat is het plan B om de continuïteit van het businessproces weer zoveel mogelijk te herstellen? Wellicht zelfs tijdelijk zonder (bepaalde) IT-systemen.

Ten slotte zorgt goed crisismanagement voor het beschermen van een 'stakeholder value risk', wanneer het ergens misgaat. Je voorbereiden op het onbekende, zorg voor de mens en goede communicatie intern en extern kunnen een organisatie laten overleven.

De professionals die werkzaam zijn in deze disciplines zullen veel effectiever en efficiënter kunnen functioneren, terwijl zij nog steeds in staat zijn om onafhankelijk te werken en hun onpartijdigheid te behouden voor die zaken waarvoor dit vereist is. Wanneer deze risicogebieden zo verweven zijn, dan is het een heldere lijn om ook de visie, budgettering en aansturing aan te passen. Dit vraagt om de juiste plek in de organisatie, te beginnen op strategisch niveau.

Survival of the fittest

Hoe cruciaal het werk van IT'ers is in de digitale transformatie, hebben we kunnen ervaren tijdens de coronacrisis. Veel processen konden doorlopen doordat we digitaal verbonden zijn. Maar deze verbindingen hebben bandbreedte nodig, net zoals stabiliteit en veiligheid. Het werk van de technische mensen die dit verzorgen, maakt hun inzet even cruciaal als bijvoorbeeld die van de handen aan het bed.

Informatietechnologie wordt vaak vergeleken met nutsvoorzieningen zoals water en stroom. Alleen gaat die vergelijking niet helemaal op. Wel wat betreft belangrijkheid. Maar deze technologie is veel complexer en heeft een grote impact op bijna alle andere processen in een organisatie en de samenleving. En een crisis kan de start zijn van grote veranderingen.

Crises zorgen ervoor dat we op een heel andere manier naar de inrichting van ons werk gaan kijken. Zoals Winston Churchill al zei: 'Never waste a good crisis.' Wanneer je erdoor transformeert zul je zegevieren. Als je apathisch blijft hangen, zul je ten onder gaan.

Adviezen

Een business-resilience-aanpak geeft een aantal voor de hand liggende voordelen: een geïntegreerd beleid en gemeenschappelijke doelen en doelstellingen, minder versnippering, meer consistentie en coördinatie en minder verwarring. Dus uiteindelijk biedt het de standaard synergievoordelen in tijd- en kostenbesparing.

Maar er zijn nog veel belangrijkere voordelen: je toont innovatief leiderschap door vanuit een holistisch dreigingsbewustzijn een optimale risicorespons te creëren.

Hierdoor wordt je merkwaarde en reputatie beschermd en verbeterd. En dit is goed voor de aandeelhouders, partners, klanten en leveranciers. Ook toezichthouders zullen dit waarderen. Ga dus voor een verbeterde integriteit en kwaliteit van uw aanbod. Het zal u helpen overleven.

- Maak één persoon eindverantwoordelijk voor uw business-resilience. Deze persoon geeft richting aan iedereen in riskmanagement, information-security, privacy, business-continuity-management en crisismanagement bij hun gezamenlijke doel: het beschermen van de bezittingen en belangen van de organisatie.

- Bepaal waar deze persoon in de organisatie het beste gepositioneerd kan worden: op C-level of direct rapporterend aan een specifieke C-level-functionaris. Afhankelijk van de omvang en structuur van de organisatie vervangt deze persoon de CISO, BCM-manager en crisismanager of stuurt deze direct aan.

- Het is belangrijk om de werkzaamheden van de professionals die werkzaam zijn binnen business-resilience optimaal te integreren, terwijl zij nog steeds in staat moeten zijn om onafhankelijk te werken en hun onpartijdigheid moeten kunnen behouden voor die zaken waarvoor dit vereist is.

- Investeer in kennis en kunde in de diverse geledingen in de organisatie. Op strategisch, tactisch en operationeel managementniveau. En ja, ook bij de informatie- en IT-technologie.

Digitale trends

Hoe als bedrijf om te gaan met de digitale revolutie

Momenteel vinden er vele veranderingen plaats. Zoveel zelfs dat wetenschappers als Robbert Dijkgraaf zich openlijk hebben afgevraagd of wij deze veranderingen wel aan kunnen. Nu zijn veranderingen uiteraard niet nieuw. Wat wel nieuw is dat de meeste veranderingen digitaal plaats vinden en met elkaar verbonden worden. Met alle bijbehorende voor- en nadelen. Dit heeft effect op de maatschappij, individuen en organisaties.

In dit boek komen een aantal zaken aan de orde:

- 5G
- Internet of things
- Kwantumcomputers
- Big data
- Het gebruik van platforms
- Blockchain
- Kunstmatige intelligentie
- Augmented en virtual reality
- 3D printing

Ingegaan wordt op de vraag hoe deze trends zijn te beoordelen en op een aantal relevante aspecten (zoals security, ethiek en wetgeving).

Ook en vooral wordt er stil gestaan hoe de relevante trends in de eigen bedrijfsvoering en (niet te vergeten) bij de eigen klanten zijn toe te passen.

Het boek is tot stand gekomen met in totaal 12 auteurs.
Stuk voor stuk gerenomeerde specialisten in hun vak.

Praktische pocketserie

In de Praktische pocketserie van de Kweekel/RGO-Academy verschijnen delen over concrete problemen waar managers in de praktijk tegenaan lopen. Elke editie beschrijft een concrete aanpak aangevuld met tips uit de praktijk en verwijzingen naar praktische tools op het internet.

Elk deel helpt je bij jouw ontwikkeling op het gebied van het behalen van betere resultaten. Of het nu gaat om je werk beter uit te voeren, efficiënter te werken of door beter te delegeren en het werk goed door anderen uit te laten voeren

RGO Academy