ADVANCED BUSINESS IMPACT ANALYSIS (DEEL 2)

Verbeterd risico-management door gerichte impactbepaling

Alle bedrijven lopen risico's, waardoor er een kans bestaat dat bedrijven hun verplichtingen naar hun stakeholders - zoals klanten of aandeelhouders - niet meer kunnen nakomen en daardoor zelf schade leiden. Het is dus van vitaal belang dat bedrijven de relevante risico's identificeren en vervolgens managen. De stap in het risicomanagementproces waarin de impact van een bepaalde dreiging op het behalen van business doelstellingen wordt bepaald is de Business Impact Analysis (BIA). Aan de BIA zoals die tegenwoordig in de meeste organisaties wordt uitgevoerd kan nog veel verbeterd worden. Dat is de conclusie van een aantal interviews en een expertsessie met verscheidene information-security-consultants met meerjarige ervaring in het ondersteunen van organisaties met het uitvoeren van BIA's. De geconstateerde tekortkomingen resulteren in mogelijk onjuist ingeschatte impacts van cyberdreigingen, met het gevaar dat enerzijds werkelijk relevante risico's over het hoofd worden gezien en anderzijds het risico wordt gelopen om te investeren in onnodige veiligheidsmaatregelen.

In deel 2 van dit artikel de geconstateerde onvolkomenheden besproken.. Deze maand zullen we een aantal mogelijke verbeterpunten bespreken voor zowel de korte, als de wat langere termijn.

Geconstateerde tekortkomingen

In het artikel van vorige maand zijn enkele tekortkomingen geïdentificeerd van het BIA-proces zoals dat nu in het bedrijfsleven wordt uitgevoerd. De tekortkoningen zijn divers. Zo is er bij degenen die de BIA uitvoeren vaak te weinig zicht op de belangen van hogere of aanpalende organisatieniveaus, met het gevolg dat belangrijke risicoscenario's over het hoofd worden gezien. Daarnaast worden dimensies als reikwijdte en tijdsduur van een incident vaak achterwege gelaten en leidt het vaststellen van een worst-case-scenario tot ambiguïteit. Tot slot is het bepalen van de impact van incidenten niet eenvoudig. Niet alleen door het ontbreken van data, maar ook door het feit dat er vaak een discrepantie bestaat tussen de scope van de verantwoordelijke persoon en de impactsoort, denk aan een IT-specialist die moet beoordelen wat de impact is van een data-breach op de aandeelhouderswaarde van een onderneming.

Door deze tekortkomingen, resulterend in onjuist ingeschatte impacts van cyberdreigingen, loopt men het risico dat enerzijds werkelijk relevante risico's niet in beschouwing worden genomen. Anderzijds loopt men het risico om te investeren in onnodige maatregelen. De praktijk is vaak dat de BIA als proces wordt doorlopen omdat dat onderdeel is van een ISO-standaard. Met de resultaten wordt echter niet gedaan wat ermee gedaan zou moeten worden. Het is duidelijk dat een andere aanpak nodig is. Bepaalde verbeteringen kunnen daarbij al op korte termijn worden doorgevoerd. Andere hebben meer tijd nodig.

Korte-termijn-verbeteringen

De BIA dient uitgevoerd te worden op verschillende organisatie-niveaus. De BIA-vragen dienen dan ook specifiek voor elk organisatieniveau (scope) gedefinieerd te zijn. In eerste instantie zou een dergelijke gelaagdheid bereikt kunnen worden door een voorselectie van bestaande vragen te maken, waarbij rekening gehouden wordt met relevantie van de vragen voor het specifieke organisatieniveau. Sluiten de vragen goed aan bij de doelstellingen van de verantwoordelijke manager? Bij alle vragen zou aangegeven moeten worden door wie, en op welk organisatieniveau ze dienen te worden beantwoord. Vragen over verlies van vertrouwen door de financiële wereld of over impact op de beurskoers zijn typisch de vragen waarover een directie zich zou moeten uitspreken. Ziehier het gedachtengoed van de Networked Risk Management methodiek, waarover later meer. Ook zou impact beter ingeschat kunnen worden als de karakteristieken van incidenten duidelijker zouden zijn omschreven. Tijdsduur en reikwijdte zijn daarbij belangrijke elementen. Bijvoorbeeld de omvang en tijdsduur van hacking van systemen om de impact hiervan op de vertrouwelijkheid van informatie gerichter te kunnen inschatten. Ook de karakteristieken van de dienst - waar in de life-cycle, kritieke dienst of niet – moeten en kunnen beter omschreven worden. Door dit te doen kan al op korte termijn een betere BIA worden uitgevoerd, met meer zeggingskracht. De tekortkomingen op het gebied van het beantwoorden van vragen, kunnen ook deels op korte termijn worden weggenomen. Door een voorselectie te maken van generieke vragen op basis van bedrijfskenmerken, wordt bereikt dat de BIA beter aansluit op de behoeftes van een specifiek bedrijf. Niet alle impact categorieën zijn immers even relevant voor verschillende bedrijven. Zo is bijvoorbeeld aandeelhouders-waarde alleen relevant voor aan de beurs genoteerde bedrijven. Ook kunnen verschillende impact types in mindere of meerdere mate relevant zijn voor een specifiek bedrijf. Het kwantificeren van impact gaat gemakkelijker indien degenen die bij het uitvoeren van de BIA betrokken zijn, gewapend worden met manieren om de impact van verschillende scenario's op hun bedrijfsvoering te bepalen. Als men bijvoorbeeld over relevante data zou beschikken kan de impact realistischer worden bepaald. Dit kan bewerkstelligd worden door voor bepaalde type impacts - bijvoorbeeld verlies van klanten, reputatieschade - te inventariseren welke data er bestaat en welke databronnen er nog nodig zijn om enige kwantificatie van impacts te faciliteren, al is het op het niveau van ordegrootte. Dan pas kunnen overwogen business cases rondom te treffen maatregelen opgesteld worden, en kan een doordacht besluit genomen worden over risico-acceptatie.

Lange-termijn-verbeteringen

Voor het verbeteren van sommige geconstateerde tekortkomingen van de BIA - zoals bijvoorbeeld tekortkomingen gerelateerd aan scope-bepaling, of tekortkomingen door gebrekkige aansluiting van vragen op de doelstellingen de scope-verantwoordelijke - is een tijdspanne van enkele jaren

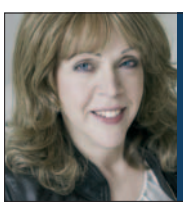
Milena Janic promoveerde aan de Technische Universiteit Delft, op het gebied van performance van informatie- en communicatienetwerken en diensten. Zij werkt als consultant en onderzoekster bij de expertisegroep Information Security van TNO. Haar focus ligt op onderzoek en consultancy op het gebied van risicomanagement, identity- en access-management en privacygerelateerde vraagstukken.

nodig. Op lange termijn is een omslag vereist in de manier waarop risicomanagement wordt gedaan: een paradigm shift. Onlangs heeft TNO een Networked Risk Management (NRM)-methodiek ontwikkeld en aangedragen, die de onvolkomenheden van ISO 31000 en 27005 adresseert en daarmee een aantal geconstateerde onvolkomenheden van het traditionele risicomanagement aanpakt. Één van de belangrijke aanvullingen die NRM introduceert is definitie en gebruik van het begrip "scope". Daar waar ISO-standaarden ervan uitgaan dat de scope duidelijk is, blijkt dat in de praktijk geenszins het geval te zijn. Om een voorbeeld te geven: vaak bestaat onduidelijkheid over wie waarvoor verantwoordelijk is, met als gevolg dat de besluitvorming rond de daaraan gerelateerde risico's ontbreekt. Daarom wordt de scope in NRM helder gedefinieerd als zijnde de ruimte waarbinnen een manager verantwoordelijk is om een aantal verplichtingen na te komen. Zo zijn voor de scope van een Raad van Bestuur hun verplichtingen aan aandeelhouders of overheid relevant. Ook een werkproces kan als scope gedefinieerd worden, als de verplichtingen (requirements) van dat proces duidelijk geïdentificeerd zijn, en een manager voor het nakomen van deze verplichtingen verantwoordelijk is. Ook kan een manager verplichtingen aan zichzelf definiëren die nodig zijn om zijn eigen business-doelen te halen. Gezonde bedrijfsvoering houdt dan in dat de verplichtingen aan derden en aan zichzelf worden nagekomen.

Verder worden in NRM risico's uitgesplitst in verplichtings- en verwachtingsrisico's. Een verplichtingsrisico is een risico van het niet kunnen nakomen van een verplichting. Naast verplichtingsrisico's worden ook verwachtingsrisico's geïdentificeerd. Een manager is voor het waarmaken van zijn verplichtingen doorgaans ook afhankelijk van anderen. Deze afhankelijkheden uiten zich in verwachtingen die een manager heeft van andere scopes om zijn doelstellingen te halen. Het belang van een gegeven verwachting wordt bepaald door de mate waarin het vervullen ervan bijdraagt aan het nakomen van verplichtingen. Als een manager een verwachting heeft van een andere scope, dan bestaat verwachtingsrisico uit de mate waarin die verwachting niet ingevuld wordt of gaat worden. De BIA is in NRM de inventarisatie van verplichtingen en de bijbehorende impacts voor een scope. De schade wordt bepaald die een manager verwacht te lijden bij het niet nakomen van een verplichting, en dat is niets anders dan de impact van het niet nakomen van de verplichting. De uiteindelijke BIA-lijst zal alle verplichtingen bevatten waarvan de impact voor de scope en verantwoordelijke manager onacceptabel hoog is. Van elk van deze verplichtingen is vastgelegd tegenover welke partij deze geldt. Tevens is de impact ingeschat van het niet nakomen van de verplichting. Om deze verplichtingen af te dekken, wordt vastgesteld hoe deze verplichtingen worden waargemaakt en worden de bijbehorende verwachtingen gedefinieerd, die een manager heeft aan zichzelf of aan anderen. De geïdentificeerde verwachtingen die een manager aan derden heeft, worden verplichtingen in de scopes waar deze derde partijen voor verantwoordelijk zijn. Kortom: vanuit de NRM-gedachte heeft het uitvoeren van de BIA betrekking op het inventariseren van verplichtingen en het bepalen van de schade die resulteert als de verplichting niet wordt nagekomen. NRM vult de huidige risicomanagement-methodes op een aantal vlakken aan, zoals onder andere de definitie en het gebruik van "scope". Hiermee is een groot aantal tekortkomingen uit de vorige sectie, geadresseerd. Echter, ook hier geldt dat het nodig zal zijn dat de scope-verantwoordelijke de impact van het niet kunnen nakomen van verplichtingen, kan inschatten.

Conclusies

Het bepalen van de impact die een bepaalde dreiging kan hebben op de business is een belangrijk onderdeel van risicomanagement. De stap in het risicomanagementproces waarin deze impact wordt bepaald is de Business Impact Analysis (BIA). Aan de BIA zoals die tegenwoordig in de meeste organisaties wordt uitgevoerd kan nog veel verbeterd worden. In dit artikel hebben we een aantal mogelijke verbeterpunten voorgesteld, zowel op korte als wat langere termijn. Zo vinden we dat er op korte termijn al veel kan gewonnen worden door bijvoorbeeld de BIA beter te laten aansluiten bij de organisatieniveaus waarvoor deze wordt uitgevoerd. Voor andere geconstateerde tekortkomingen is een omslag nodig in de manier waarop risicomanagement wordt gedaan: een paradigm shift. Het denken in verplichtingen en verwachtingen is het gedachtengoed van Networked Risk Management (NRM), een door TNO ontwikkelde methodiek, die in dit artikel nader is toegelicht. Vanuit de NRM-gedachte heeft het uitvoeren van de BIA betrekking op het inventariseren van relevante verplichtingen en het bepalen van de schade die resulteert als een bepaalde verplichting niet wordt nagekomen. Wij geloven dat door in ieder geval de tekortkomingen aan te pakken die op korte termijn kunnen worden opgelost, een organisatie zich beter kan wapenen tegen huidige en toekomstige security-dreigingen.



Eldine Verweij is als kwantitatief bedrijfseconoom afgestudeerd aan de Erasmus Universiteit Rotterdam en werkt als consultant en onderzoekster bij de expertisegroep Strategic Business Analysis van TNO. Haar focus ligt op onderzoek en consultancy met betrekking tot de economics van cybersecurity en kosteneffectiviteitsafwegingen binnen de informatiebeveiliging.