DATA RISK MANAGEMENT

De hoeveelheid bedrijfsdata neemt exponentieel toe. Zo ook het aantal locaties en leveranciers die data voor u in beheer hebben. Door de grote hoeveelheid data is het voor vele organisaties onoverzichtelijk waar de data staat en hoe dat werkelijk is beschermd. De omvang en complexiteit van data vormt een extra dimensie die beteugeld moet worden om grip te krijgen op de beveiliging ervan. Zonder overzicht en goede bescherming van die data loopt de organisatie een groot risico. Tot nu toe zijn we nog niet verder gekomen dan checklists en heatmaps met getallen tussen 0 en 10 voorzien van stoplichtkleuren. In dit artikel neem ik u mee in de wereld van risicomanagement gericht op data, zoals de nieuwe versie van ISO27001:2013 specifiek van ons vraagt.

De inhoudsopgave van de internationale informatiebeveiliging standaard ISO27001:2013 beschrijft in grote lijnen waaraan een managementsysteem voor informatiebeveiliging moet voldoen. Een belangrijke verbetering ten opzicht van de vorige versie (ISO27001:2005) is de verbijzondering van de risicomethodiek die gericht moet zijn op de data. Maar hoe ziet dat Data Risico Management eruit? Vele organisaties worstelen met een data risico-analyses. De toenemende hoeveelheid data, de complexiteit van de verschillende beveiliging-standaarden, de administratieve lasten van checklists, project security reviews en de technische details met nietszeggende 'heatmaps' maken het in de praktijk onmogelijk voor het hoger management informatiebeveiliging op een normale manier aan te sturen. Nog maar te zwijgen van de adviseurs die bijna weten hoe je informatiebeveiliging moet implementeren. De kunst is om maatregelen optimaal af te stemmen op basis van je data risico's, zodat je niet een risico van een dubbeltje met een maatregel van een kwartje verzekerd. Tevens is het vereenvoudigen van informatiebeveiliging een kritische succesfactor, waarbij wel recht wordt gedaan aan de complexiteit van deze risico's. Bedrijven doen wel van alles aan beveiliging, maar de samenhang is zoek. Een één-dimensionale beveiligingsmaatregel om USB-poort af te sluiten op de bedrijfslaptop is weinig effectief als je vervolgens via Dropbox, Gmail en WeTransfer de data thuis op een USB-stick zet. Er is zoveel data, dat bedrijven door de bomen het bos niet meer zien wat ze moeten beschermen. Data Risico Management is de "missing link" die bedrijven nodig hebben om beveiligingsmaatregelen in balans te krijgen met een acceptabel bedrijfsrisico.

De speld in de berg van data

Om te beginnen moet je focus aanbrengen in de grote hoeveelheid data. Alles analyseren is met deze grote hoeveelheden data gewoon niet meer mogelijk. Een logische focus in deze grote hoeveelheid data, is de data van Mission Critical Applications (MCA). MCA ondersteunen namelijk de belangrijkste bedrijfsprocessen en vormen een bedrijfsrisico als het mis gaat. In de regel hebben MCA's een hoofdgebruiker die verantwoordelijk is voor de productiedata. Echter, bij audits blijkt dat productiedata wordt gekopieerd naar andere omgevingen en de nieuwe "data eigenaar" niet wordt benoemd. Dit eigenaarschap is wel nodig. Als de data namelijk wordt verplaatst, veranderen vaak de beveiligingsomstandigheden. Het is daarom van belang om alle databronnen van een MCA

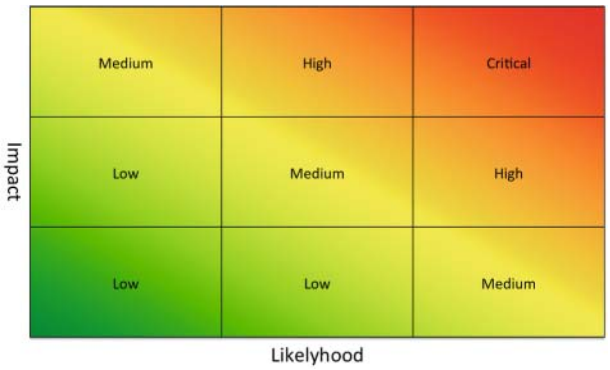
in kaart te brengen, inclusief de bijbehorende data eigenaar. Het risico neemt ook exponentieel toe naarmate de hoeveelheid (vertrouwelijke) data toeneemt. Een databron met alle patiëntgegevens op straat heeft veel meer impact dan een enkel papieren dossier. Een andere reden om alle databronnen van een MCA in kaart te brengen, is dat hackers in de praktijk ook liever de achterdeur gebruiken. Denk aan incidenten met bijvoorbeeld Cheaptickets (testomgeving) en Diginotar (via kantoornetwerk naar productie).

Voorbeeld: Een Cliënt Volg Systeem heeft een productiesysteem bij een ISO27001-gecertificeerde hosting partner in Almere, een dagelijkse back up-procedure van de databron met patiënt- en/of medewerkergegevens in de cloud (VS) en een datawarehouse in India. Dezelfde data valt in dit voorbeeld onder verschillende wetgeving, kent verschillende beveiligingsniveau's en het data eigenaarschap is versnipperd. Om dit goed aan te sturen, is een specifieke vorm van risicomanagement nodig.

Risico = Kans x Impact

Risicomanagement is traditioneel kans maal impact. Kans neemt toe als er iets van waarde te halen is en de impact is groter naarmate de organisatie groeit. Context en reputatie spelen daarom een belangrijke factor om de waarde van data risico's in te schatten. Een hoog risico voor een lokale bloemist is nu eenmaal anders dan een hoog risico voor een nationale bank. Het uitdrukken van impact in geld is handiger dan de traditionele indeling "High, Medium en Low". Systemen die namelijk allebei geclassificeerd zijn als 'High', zijn bij de vergelijking gelijk, maar blijken in de praktijk toch een verschillend risicoprofiel te hebben. De impact wordt ingeschat op basis van een schadepost die deze data kan veroorzaken.

De impact wordt uitgedrukt in een realistische schadepost op basis van termen uit de informatiebeveiliging, te weten: beschikbaarheid, integriteit, beschikbaarheid en non-compliance. De maximale schade als alle data uit een databron op straat komt te liggen (Confidentiality), de kosten



Risico heatmap

van een foute beslissing als de data niet juist blijkt te zijn (Integrity), de waarde als data voor maximaal aantal dagen niet beschikbaar is (Availability) en tot slot het niet voldoen aan wetgeving waardoor ik een boete kan krijgen (Non-compliance). De hoogste waarde bepaalt voor deze specifieke MCA de waarde van alle hoge risicoklassen – C,I,A,N – uitgedrukt in geld.

Het Ponemon Instituut heeft op basis van bekende incidenten onderzoek gedaan naar de gemiddelde kosten van een security incident. Deze schade komt internationaal neer op 150 euro per record. Dit bedrag biedt een uitgangspunt voor het bepalen van risico schade op basis van aantal records. Dit schadebedrag heb ik getoetst op incidenten die ik zelf ken, maar ook bij verzekeraars. Het is mijn conclusie dat dit schadebedrag per record naar beneden wordt bijgesteld bij organisaties met een lokale of nationale reputatie. Hierdoor krijg je een realistische inschatting van de werkelijke risico's.

Soms kan ik slechts één High-waarde vaststellen, soms twee en soms allemaal. De impact van deze data is daarom de hoogste waarde van deze vier categorieën (C,I,A,N) en geldt voor alle databronnen die gekoppeld zijn aan deze MCA. De andere risicoklassen Medium en Low worden hiervan afgeleid

Gerco Kanbier is directeur van Trust in People - the information protection company. Hij is te bereiken via gerco.kanbier@trustinpeople.com.

met respectievelijk 50% en 10% van de 'High'.
De kans is gekoppeld aan het aantal ISO27002-maatregelen die deels of niet genomen zijn rond de databron. In deze methodiek starten we dus niet met een dreigingenanalyse, maar starten met een mogelijke maatregel uit ISO27002 die een specifiek risico scenario afdekt. Het niet nemen van een individuele maatregel introduceert een kans dat het op dit punt fout kan gaan. Tegelijkertijd kunnen genomen maatregelen reeds preventief en/of overlappend zijn. Meer maatregelen, hoe kleiner de kans. Minder maatregelen vergroot andersom de kans op incidenten. De hypothese is dan wel dat een "databron" 100% veilig is als alle ISO27002-maatregelen zijn toegepast. Deze hypothese is natuurlijk niet waar, maar wel praktisch toepasbaar en goed bruikbaar als stuurinformatie. Beide grootheden - kans en impact - zijn op deze manier objectief meetbaar en kwantificeerbaar. Als een andere beveiligingsspecialist een inschatting doet, dan zal dat vergelijkbare resultaten opleveren. Dit in tegenstelling tot die risicospecialisten die zich bezig houden met wiskundige kansberekeningen.

Maatregelen (ISO27002)	Toegepast?	Auto Classificatie (C,I,A,N)	Scenario	Schade
Organisatie [Video bewaking]	JA	2C	Aanwezigheid of handeling kan ontkend worden bij onderzoek naar gestolen waar	€1.312.500
Organisatie [Security awareness training voor medewerkers]	NEE	3C	Medewerkers zijn een makkelijk prooi voor social engineer en/of phishing aanvallen	€262.500
Organisatie [Geheimhoudingsverklaring medewerkers]	DEELS	1C	Leverancier of medewerker lekt informatie naar derden	€2.625.000
Organisatie [Functiescheiding]	JA	1C	Gebruiker heeft teveel toegang tot vertrouwelijke informatie	€2.625.000
Organisatie [Uitwijklocatie]	NEE	1A	bij een ramp is er geen alternatieve locatie	€2.625.000
Organisatie [Informatiebeveiligings functionaris is aangesteld]	JA	2N	data eigenaarschap is niet goed belegd en bestuur is daarmee aansprakelijk	€1.312.500
Organisatie [Security is staffunctie van directie]	NEE	3N	informatiebeveiliging kan niet goed en/of volledig worden aangestuurd	€262.500
Processen [Data risico analyses worden periodiek uitgevoerd]	JA	2N	ad hoc aanpak laat echte risico's ongemoeid	€1.312.500
..	..	..	..	..

Risico's per databron in balans

Per databron wordt in kaart gebracht welke ISO27002-maatregelen wel, niet en/of deels genomen zijn. Het management heeft in een oogopslag een gewogen beeld van de huidige informatiebeveiliging per databron. Het management krijgt daarnaast een overzicht met begrijpelijke scenario's die nu nog als rest risico mogelijk zijn. Zo kan het management zelf quickwins definiëren en risico's accepteren op basis van integrale samenhang. Zie het voorbeeld in tabel

Heatmap

Als alle belangrijke databronnen geregistreerd, geanalyseerd en beoordeeld zijn, dan is het belangrijk voor het management een overzicht te krijgen waar de grootste risico's liggen, de zogenaamde 'heatmap'. Het management wil een beoordeling van het geheel. Alle risico's onder een bepaald platfond (bijvoorbeeld 1 miljoen euro), worden volgens beleid niet met hoger management besproken. Boven dat plafond wordt door de directie bekeken welke maatregelen extra genomen moeten worden dan wel als geheel geaccepteerd worden als rest risico. Met een heatmap krijgt het management een goed beeld of de standaard security architectuur over de linie goed is geïmplementeerd. Gemiddeld zijn er x maatregelen per databron genomen, waardoor afwijkingen goed zichtbaar zijn voor het management. De impact is uitgedrukt in geld, waardoor onderlinge risicoverschillen tussen MCA's en databronnen in een oogopslag zichtbaar worden. Zo kan het management besluiten gericht op een specifieke databron maatregelen te nemen (bijvoorbeeld een quick win), of een project te definiëren die de beveiliging van alle systemen verbeterd (bijvoorbeeld de centralisatie van logging).
Met bovenstaande managementinformatie kan het management ook haar bestuurlijke verantwoordelijkheid waarmaken. Het wordt duidelijk welke risico's acceptabel zijn en welke niet.

Statement of Applicability

Tot slot beschrijf ik de relatie tussen Data Risico Management, ISO27001, ISMS en het Statement of Applicability (SOA). Ongecertificeerde bedrijven hebben nog nooit gehoord van een Statement of Applicability. Dit is een document noodzakelijk voor een ISO27001-certificering met onder andere een beschrijving van de scope, de security incidenten en laatste audit findings. Maar belangrijkste onderdeel voor klanten, auditors en management is de vastlegging welke data risico's zijn geaccepteerd. Data Risico Management (DRM) is daarom een onmisbare schakel bij de uitvoering van informatiebeveiliging. De ISO27001 beschrijft een management systeem gericht op informatiebeveiliging (ISMS). Andere ISO-normen worden momenteel herschreven, waarbij elke norm onderscheid wordt gemaakt tussen het management systeem en de maatregelen. Hierdoor kunnen bedrijven in de toekomst makkelijker verschillende normen naast elkaar implementeren zonder verschillende managementsystemen aan te schaffen.

DRM

De afkorting van Data Risico Management, DRM, roept onder vakgenoten vraagtekens op. DRM staat namelijk ook voor Digital Rights Management. Tevens heeft Data Risico Management hetzelfde doel als Informatie Risk Management (IRM). Toch heb ik gekozen voor een andere naamgeving, omdat de methodiek gericht is op de DATA en een geheel andere aanpak heeft dan de bestaande risico methoden. In navolging van Enterprise Risk Management (ERM) wat zich op de enterprise richt, Operational Risk Management(ORM) op de operatie en Credit Risk Management (CRM) op de kredieten, richt Data Risk Management zich specifiek op de data.