KoutersVanderMeer
bureau voor prestatieverbetering

FM.NL
FINANCIEEL MANAGEMENT

Een praktische oplossing voor uw meldplicht datalekken

In vier stappen het lek gedicht!

De redactie - 18 okt 2016

In het bedrijfsleven bestaat onrust over de nieuwe Meldplicht Datalekken mede ingegeven door de dreiging van een hoge boete of reputatieschade. In dit artikel presenteren twee experts een praktische oplossing voor het op bestendige wijze inrichten van de Meldplicht Datalekken. Een oplossing die aansluit bij de huidige bedrijfsvoering van organisaties en inzicht geeft in aanwezige risico's en de wijze waarop deze beheerst kunnen worden.

Door Dennis Stabel en Ad Meeuwesen

Wat is er aan de hand?

Vooruitlopend op de nieuwe Europese Verordening Gegevensbescherming, die in mei 2018 van kracht wordt, is in Nederland per 1 januari 2016 de meldplicht datalekken in werking getreden. Het verplicht melden van bepaalde type datalekken is sindsdien geregeld in de Wet Bescherming Persoonsgegevens (WBP). Met de meldplicht datalekken beoogt de

regering de gevolgen van een datalek voor de betrokkenen zoveel mogelijk te beperken en hiermee een bijdrage te leveren aan het behoud van vertrouwen in de omgang met persoonsgegevens.

De verantwoordelijkheid om adequate maatregelen te treffen ter beveiliging van persoonsgegevens is van alle tijden. Als deze verantwoordelijkheid niet serieus wordt genomen, neemt de kans op beveiligingsincidenten toe. Bepaalde typen beveiligingsincidenten zijn ook te kwalificeren als datalek. De verantwoordelijke van de persoonsgegevens zal deze dan in de meeste gevallen moeten melden. Dit betekent niet alleen een melding doen bij de toezichthouder, de Autoriteit Persoonsgegevens (AP), maar mogelijk ook de betrokkene informeren.

Deze meldplicht geldt voor alle organisaties die persoonsgegevens verwerken, zowel in de private als publieke sector. Als er geen melding wordt gemaakt van een datalek kan dit leiden tot een door de AP op te leggen bestuurlijk boete van €820.000,- of 10% van de jaaromzet pér overtreding.

Wij constateren dat in het bedrijfsleven onrust bestaat voor de nieuwe verplichting mede ingegeven door de dreiging van de hoge boete of, waarschijnlijk nog erger, reputatieschade. Organisaties zijn zoekende wat de nieuwe regelgeving precies voor hen betekent en op welke wijze ze de nieuwe verplichtingen in hun bedrijfsvoering kunnen implementeren. En het liefst dan wel op een zodanige manier dat niet alles binnen het bedrijf ‘overhoop’ gehaald moet worden, maar aansluiting gezocht kan worden bij huidige bedrijfsprocessen.

In dit artikel presenteren wij een praktische oplossing voor het op bestendige wijze inrichten van de meldplicht datalekken binnen uw organisatie. Een oplossing die aansluit bij de huidige bedrijfsvoering van

organisaties én die in korte tijd inzicht geeft in aanwezige risico's en de wijze waarop deze beheerst kunnen worden. Hiermee hopen we goede handvatten aan te reiken en het onrustige gevoel weg te nemen.

In vier stappen naar controle op drie aandachtsgebieden

De Wet Bescherming Persoonsgegevens inclusief de meldplicht datalekken is voor vrijwel alle profit en non-profit organisaties van toepassing. Denk bijvoorbeeld aan de personeels- en salarisadministratie als typische voorbeelden van persoonsregistraties binnen het bedrijf. Daarnaast kan het verwerken van persoonsgegevens onderdeel uitmaken van de dienstverlening. Voorbeelden hiervan zijn payrolling, callcenters, uitzendbureaus en feitelijk alle dienstverlening aan consumenten. Ook zijn 'indirecte' voorbeelden te bedenken, zoals organisaties die IT-diensten verlenen: het hosten van een IT-infrastructuur of het aanbieden van software in een hosted omgeving (Software as a Service).

Het onderscheid in de directe en de indirecte relatie met de verwerking van persoonsgegevens wordt in de wet aangeduid als de verantwoordelijke organisatie voor de persoonsgegevens en organisatie(s) die als (sub-)bewerker van persoonsgegevens optreden. In de praktijk maakt het echter geen verschil of de organisatie verantwoordelijke of bewerker van de persoonsgegevens is. Dezelfde voorwaarden en verplichtingen zijn van toepassing. Het enige, belangrijke verschil sinds 1 januari 2016 zit in de partij die melding van het datalek moet maken.

Ongeacht de omvang van de organisatie en de aard van de dienstverlening wordt dus elke organisatie 'geraakt' door de meldplicht datalekken. Om de zaken goed te organiseren en te voldoen aan de eisen die worden gesteld om datalekken te herkennen en te melden, onderkennen wij voor elke organisatie de volgende drie aandachtsgebieden:

1. organisatie en procedure rondom datalekken;

2. risicobeeld van de organisatie;
3. bewustzijn vergroten en vasthouden.

Het op een goede wijze inregelen van deze aandachtsgebieden leidt tot het voorkomen van boetes en reputatieschade. Daarnaast biedt het ook de mogelijkheid een onderscheidende positie ten opzichte van concurrenten in te nemen.

Per aandachtsgebied zijn er vier relevante stappen die op continue wijze doorlopen moeten worden om uiteindelijk op een duurzame wijze in control te zijn op het gebied van datalekken. Meer specifiek: om (potentiële) datalekken te voorkomen, te signaleren en/of te herstellen, alsook het voldoen aan de verplichtingen die de meldplicht met zich meebrengt. Deze vier stappen zijn: analyseren, ontwerpen, implementeren en leren.

	Organisatie en procedure	Risicobeeld	Bewustzijn
analyseren	analyse huidige organisatie en procedure	wat is er beschreven over risicobeeld	wat is er beschikbaar op gebied van bewustzijn
ontwerpen	ontwerpen/opzetten inrichting van organisatie en procedure (aanhaken op bestaande structuren)	ontwerpen/opzetten van het huidige risicobeeld: inventariseren typen/omvang registraties, niveau technische beveiliging, juridische tekortkomingen	ontwerpen/opzetten communicatieplan (intern en extern) en opleidingsplan
implementeren	inrichten organisatie en procedure door oa opzet overlegstructuren, inrichting tooling en rapportages	keuzes maken op basis van het risicobeeld ter verbetering beheersing: verhogen technische beveiliging, uniformeren en verbeteren juridische kaders	uitvoeren communicatieplan en trainingen
leren	analyseren beveiligings- en datalekken en afhandeling hiervan, indien nodig bijstellen ontwerp organisatie en procedure	periodiek herevalueren van risicobeeld en bijstellen verbeteracties	periodiek datalek-test of organisatie 'staat' en betrokkenen procedure kennen en correct toepassen; periodiek terugkoppeling beveiligingslekken en datalekken met afhandeling teneinde een lerende organisatie te creëren

Drie aandachtsgebieden en vier relevante stappen

Organisatie en procedure rondom datalekken

Van een datalek is sprake als zich een beveiligingsincident heeft voorgedaan én persoonsgegevens verloren zijn gegaan of onrechtmatige

verwerking van persoonsgegevens niet is uit te sluiten. Beveiligingsincidenten worden bij voorkeur geïdentificeerd en afgewikkeld binnen de huidige (security) incident procedure van de organisatie. De identificatie, registratie, analyse en (eventuele) melding van (mogelijke) datalekken wordt vervolgens als integraal onderdeel van de incident procedure opgenomen. Hierbij is het eenduidig beleggen van verantwoordelijkheden en het betrekken van de juiste kennis binnen de organisatie van cruciaal belang om een goede afweging te maken of én wanneer een (mogelijk) datalek wordt gemeld. In het algemeen is bestuurlijke betrokkenheid, alsook de betrokkenheid van IT-(security)specialisten onontbeerlijk.

Het besluit om over te gaan tot het melden van een (mogelijk) datalek verdient speciale aandacht. Belangrijk hierbij is de rol die de organisatie speelt ten aanzien van de verwerking van de persoonsgegevens waar het beveiligingsincident betrekking op heeft: verantwoordelijke dan wel bewerker.

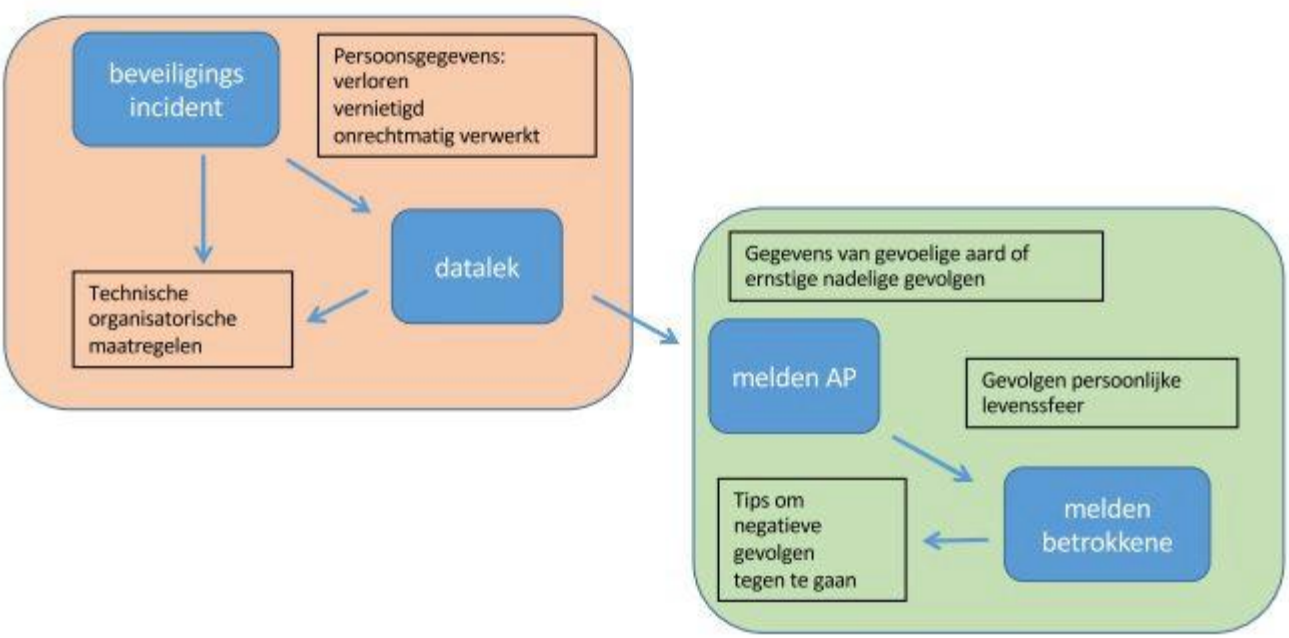
Situatie 1: Organisatie is verantwoordelijke van de persoonsgegevens. In dit geval dient de organisatie zelf de beslissing te nemen of het datalek gemeld gaat worden aan de AP en/of betrokkene(n).

Situatie 2: Organisatie is bewerker van de persoonsgegevens. In dit geval dient de verantwoordelijke (meestal de klant/opdrachtgever) geïnformeerd te worden door de organisatie over het feit dat er sprake is van een (mogelijk) datalek. Vervolgens dient de klant het besluit te nemen of het datalek gemeld moet worden aan de AP en/of betrokkene(n).

Overigens geldt dat wanneer de verantwoordelijke van oordeel is dat een datalek gemeld moet worden, dit binnen 72 uur na ontdekking van het datalek dient te gebeuren aan de AP. In het geval ook besloten wordt dat

de betrokkene(n) geïnformeerd moet worden dan dient dit onverwijld te gebeuren. Dit betekent gelijktijdig of direct na de melding aan de Autoriteit Persoonsgegevens.

Voor de beoordeling of sprake is van een datalek en de besluitvorming om over te gaan tot het maken van een melding hanteren wij de afwegingen die zijn opgenomen in onderstaande afbeelding.



Besluitvorming melding datalek

De volgende beslissingen moeten worden gemaakt:
1. de beslissing of sprake is van een datalek, en
2. de beslissing of overgegaan moet worden tot het maken van melding aan de Autoriteit Persoonsgegevens en/of betrokkene. In geval de organisatie als bewerker optreedt moet gemeld worden aan de klant (verantwoordelijke).

Elke organisatie dient het besluitvormingsproces concreet uit te werken in het ontwerp van haar organisatie en procedures rondom de meldplicht datalekken. In veel voorkomende gevallen wordt de coördinatie van

het gehele besluitvormingsproces belegd bij een security officer of daarvoor aangewezen privacy officer. Belangrijk bij de coördinatie van dit proces betreft het bewaken van de tijdslijnen en het vastleggen van het incident, inclusief het gehele beoordelingsproces.

Voor het vastleggen kan gebruik gemaakt van een incident registratie tool. Een dergelijke tool helpt ook bij het vastleggen en inzichtelijk maken van de doorlooptijd na ontdekking van het beveiligingslek. Immers, gelet op de termijn van 72 uur zal voor een 'bewerker' de melding aan de klant relatief snel moeten plaatsvinden. In de praktijk zien wij dat hiervoor veelal een termijn van 24 uur wordt gehanteerd. Dergelijke afspraken worden normaliter in een zogenaamde bewerkersovereenkomst vastgelegd. Dit vergt een goed ingerichte organisatie en duidelijke procedures.

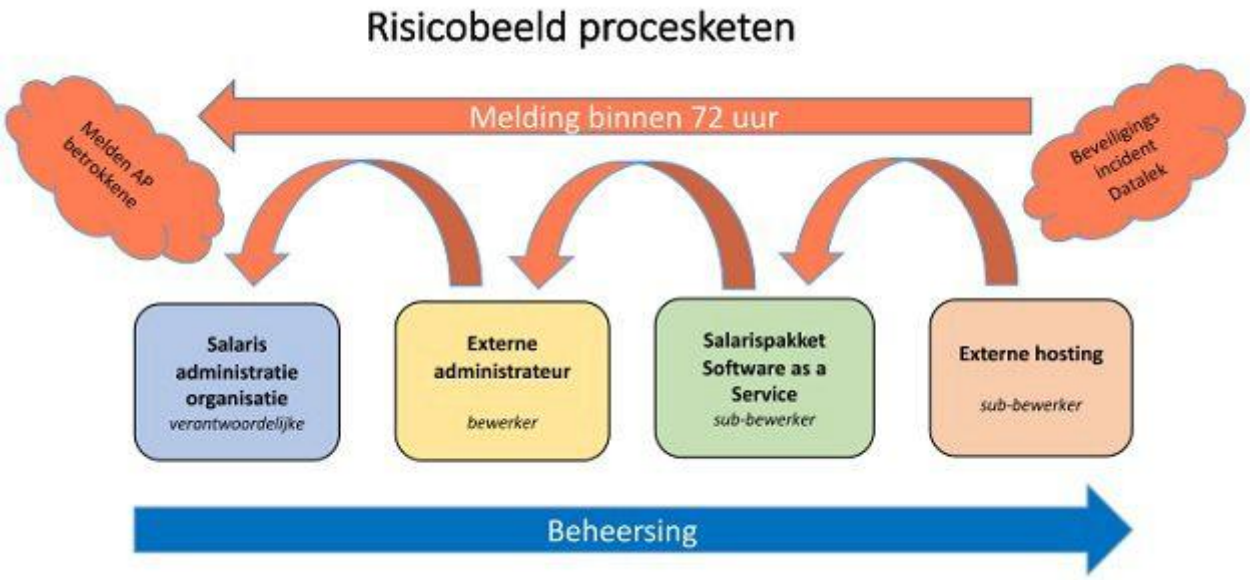
Belangrijk is dat de organisatie periodiek analyses doet naar de oorzaak van gesignaleerde beveiligingsincidenten en datalekken en hierop beoordeeld of zaken binnen de bedrijfsvoering en/of procedures aanscherpt moeten worden. Op deze wijze ontstaat een doorlopende leercyclus.

Verkrijgen risicobeeld van de organisatie

Organisaties hebben veelal geen zicht op de privacy risico's waaraan zij zijn blootgesteld. Simpelweg omdat men het technisch beveiligingsniveau rondom haar persoonsregistraties niet inzichtelijk heeft. Een belangrijke oorzaak hiervan ligt in de vlucht die Cloud Computing heeft genomen. Dit betreft in feite het uitbesteden van (fysieke) IT-infrastructuren en het verwerken van softwaretoepassingen, alsook het technisch en/of functioneel beheer van deze IT-omgevingen.

Daarnaast is een toename van de lengte en complexiteit van procesketens duidelijk zichtbaar. Denk hierbij aan het uitbesteden van de

salarisadministratie, waarbij de administrateur op haar beurt gebruik maakt van een salarispakket dat afgenomen wordt als Software-as-a-Service, terwijl de aanbieder van de SaaS-oplossing gebruikt maakt van IT-hosting diensten van een daartoe gespecialiseerde organisatie. Het gevolg is dat de organisatie veelal geen volledig beeld heeft van de registraties die onder haar (bewerkers)verantwoordelijkheid vallen. Laat staan dat men zicht heeft op de beveiligingsrisico's rondom deze persoonsregistraties.

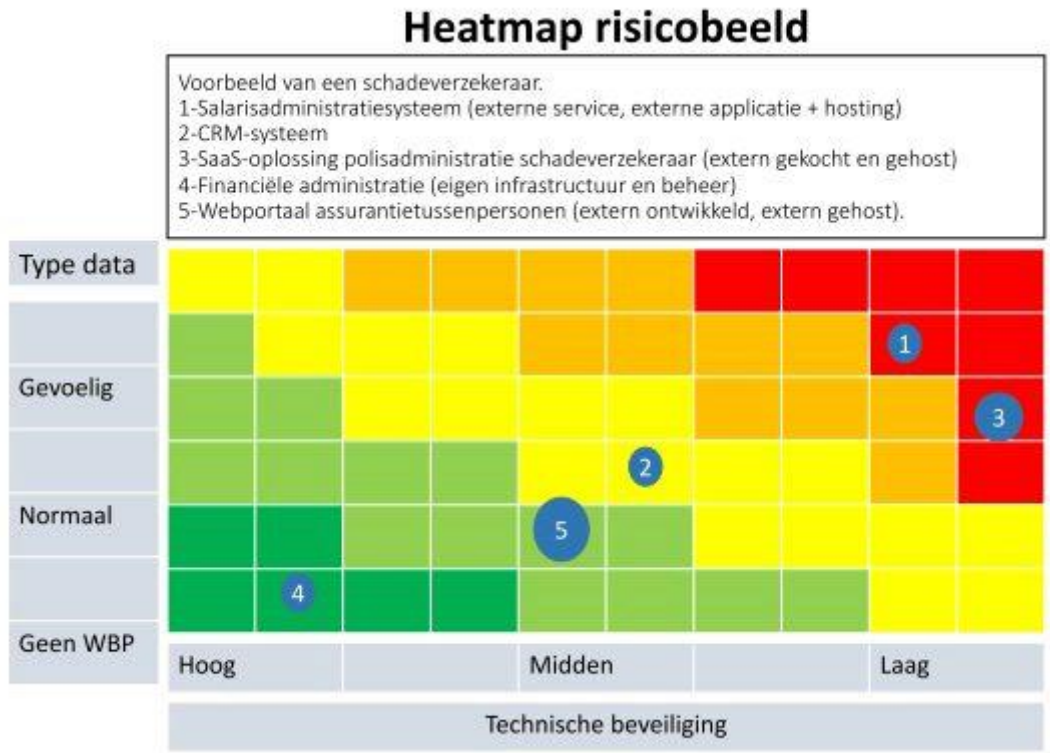


Risicobeeld procesketen

Voor het verkrijgen van het risicobeeld van een organisatie is het nodig een inventarisatie van de aanwezige persoonsregistraties te maken, zowel binnen als buiten de organisatie. Tevens dient de omvang en impact van deze registraties inzichtelijk te worden gemaakt. Denk hierbij aan het aantal personen die zijn opgenomen, alsook welke soorten van gegevens verwerkt worden: geen WBP-gegevens, normale persoonsgegevens of gevoelige persoonsgegevens.

Zodra inzicht in de aanwezige registraties is verkregen, is het van belang per registratie het niveau van de technische beveiliging in kaart te brengen. Dimensies die daarbij worden onderkend zijn beveiliging van de applicatie,

infrastructuur en de data (persoonsgegevens). Ook de eventuele juridisch tekortkomingen in contracten, SLA's en bewerkersovereenkomsten zijn van invloed op het risicobeeld. Met de verkregen informatie wordt een 'heatmap' gecreëerd van de risico's ten aanzien van de aanwezige persoonsregistraties.



Heatmap risicobeeld

Het verkregen risicobeeld geeft de organisatie een instrument om risico's, maar ook risico afwegingen bespreekbaar en visueel te maken. De organisatie heeft in één oogopslag inzicht in haar risico's en kan daardoor gerichter besluiten welke risico's wel en welke niet acceptabel zijn, alsook waar aanvullende (beheersings)maatregelen nodig zijn. Denk hierbij aan het implementeren van specifieke beveiligingsmaatregelen om het beveiligingsniveau te verhogen. Een ander voorbeeld betreft het op orde brengen van bewerkersovereenkomsten in lijn met wettelijke verplichtingen omtrent de meldplicht datalekken.

Ook voor dit aandachtsgebied geldt dat op een reguliere basis het risicobeeld opnieuw moet worden opgemaakt. Hiermee kan beoordeeld worden of maatregelen het gewenste effect hebben en of er mogelijk andere risico's zijn ontstaan.

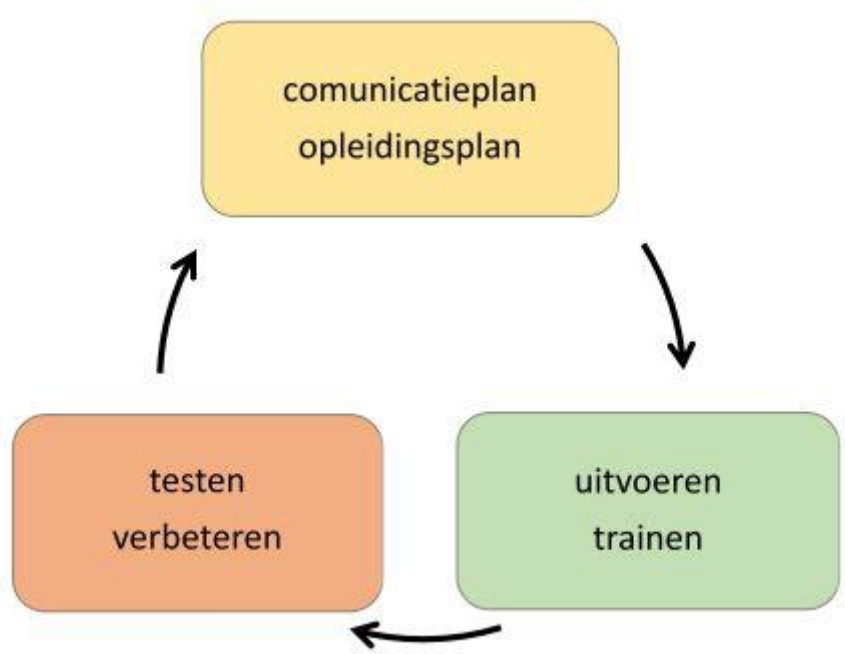
Bewustzijn vergroten en vasthouden binnen de organisatie

Net als bij informatiebeveiliging is 'de mens' ook bij het voldoen aan de meldplicht datalekken in feite de zwakste schakel. Het creëren van bewustzijn bij alle medewerkers van de organisatie is dan ook van cruciaal belang. Het bewustzijn is gericht op diverse aspecten met betrekking tot beveiligingsincidenten en datalekken, onder andere: preventie, detectie, melden en herstel. Hiertoe moeten de medewerkers kennis hebben van de organisatie en procedures die zijn ingericht. Van belang is dat deze aspecten voortdurend aandacht krijgen binnen een organisatie en dat de organisatie leert van de incidenten die zich voor doen en de risico's van datalekken daarbij. Uiteindelijk is bewustzijn slechts de eerste stap: bewust blijven is de grootste uitdaging.

Ook dient er aandacht te zijn voor het vergroten van het bewustzijn bij de ketenpartners van de organisatie. Zoals geschetst maken zij een onlosmakelijk deel uit van het verwerkingsproces. Bij ketenpartners kunnen zich ook beveiligingsincidenten voordoen waarvoor de organisatie zelf de verantwoordelijkheid draagt.

Om een groter bewustzijn binnen de organisatie te realiseren is het belangrijk aandacht te besteden aan opleiding en communicatie. Een effectief middel dat ingezet kan worden betreft een zogenaamde datalektest die periodiek uitgevoerd wordt. Bij een dergelijke test wordt een fictief datalek in de organisatie gecreëerd. Hiermee wordt vervolgens getest of de organisatie op orde is en medewerkers de procedure kennen en goed toepassen.

Een ander effectief middel is actieve terugkoppeling aan de organisatie over de afwikkeling van gemelde beveiligingsincidenten en de herstel- en verbeteracties die zijn uitgevoerd naar aanleiding van eventuele datalekken die zich hebben voorgedaan.



Bewustzijn vergroten

Conclusie

De beveiliging van persoonsgegevens is geen nieuw thema, echter door de meldplicht datalekken krijgt het hernieuwde aandacht. Voor het in control komen op de verplichtingen om datalekken te melden hebben wij drie aandachtsgebieden beschreven: organisatie en procedure, risicobeeld en bewustzijn. Indien hierbij de vier beschreven stappen, analyseren - ontwerpen – implementeren – leren, worden doorlopen kan een organisatie haar privacy risico’s bestendig en duurzaam beheersen.

Elke organisatie in Nederland die te maken heeft met persoonsgegevens zal hier, los van de vraag of de organisatie verantwoordelijke of bewerker is, invulling aan moeten geven. De uitdaging is om het op een zodanige wijze

in te regelen dat het aansluit bij bestaande procedures en processen. Wordt dit op een goede manier gedaan dan kan sprake zijn een verhoogd beheersingsniveau en onderscheidend vermogen ten opzichte van concurrenten.

Auteurs: *Dennis Stabel.(dennis.stabel@koutersvandermeer.nl) is partner bij KoutersVanderMeer, Bureau voor Prestatieverbetering. Dennis heeft zich de afgelopen jaren binnen diverse organisaties ingezet voor het oplossen van audit- en assurancevraagstukken.*

Ad Meeuwesen (ad.meeuwesen@koutersvandermeer.nl) is als adviseur verbonden aan KoutersVanderMeer. Ad houdt zich bezig met compliance en privacy-advisering, juridisch advies en IT gerelateerde procesverbeteringen.