Meldplicht Datalekken en het MKB

Wat houdt de meldplicht in, hoe kun je eraan voldoen en welke technische oplossingen kun je inzetten.

versie Q4 2016-2

Deze whitepaper wordt u aangeboden door SecureMe2.
www.secureme2.eu

Ook kleine bedrijven moeten de mogelijkheid hebben om aan de wet te kunnen voldoen."

Aad van Boven, CEO SecureMe2

Samenvatting

De meldplicht datalekken is sinds 1 januari 2016 in werking getreden. De bedoeling van de aanpassing is om de bescherming van persoonsgegevens te verbeteren.

U bent als organisatie (binnen het bedrijfsleven maar ook binnen de overheid) verplicht melding te maken van beveiligingsincidenten met betrekking tot persoonsgegevens. In bepaalde gevallen is ook een melding verplicht aan personen van wie de gegevens afkomstig zijn.

De publiciteit en mogelijke reputatieschade moeten een preventieve werking opleveren. Om dat verder te versterken is ook de boetebevoegdheid van de toezichthouder uitgebreid. Een boete kan bijvoorbeeld worden opgelegd als de beveiliging niet deugt of als persoonsgegevens onnodig lang worden opgeslagen. Het betreft een bestuurlijke boete van maximaal € 900.000,-- of 10% van de jaaromzet per overtreding bij handelen in strijd met de Wet bescherming persoonsgegevens (Wbp).

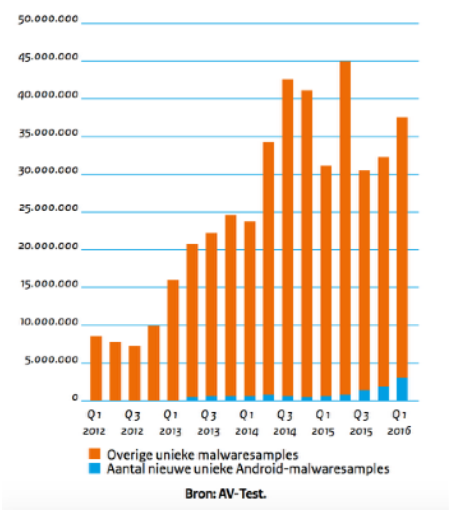
Wat betekent dit voor het MKB ?
Lees er alles over in deze whitepaper.

SecureMe2 levert Compliance en Security dienstverlening voor het MKB. Kijk op www.secureme2.eu voor oplossingen in relatie tot de Meldplicht Datalekken.

“Ransomware is gemeengoed en is nog geavanceerder geworden”

Cybersecurity Beeld 2016

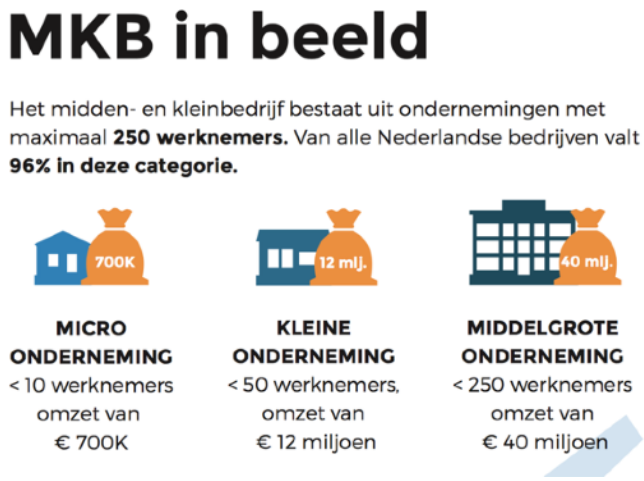
Het MKB en cybersecurity



Het MKB vormt een grote groep bedrijven en is goed voor 61 procent van het bruto binnenlands product. Veel vitale processen zijn onderdeel van een keten, waar bedrijven uit het MKB ook vaak onderdeel van uitmaken. Het MKB is dus niet alleen belangrijk voor de economie, maar ook voor de samenleving. Dit terwijl het MKB een lage weerbaarheid heeft op digitaal gebied. Samen met de groeiende dreiging van beroepscriminelen vormt dit een steeds groter wordend risico voor het economisch belang van Nederland.

Grote bedrijven en organisaties investeerden de afgelopen jaren vrijwel altijd in meer of mindere mate in cybersecuritymaatregelen. Dit geldt niet voor het MKB. Uit onderzoek van Interpolis blijkt dat ondernemers het risico van digitale dreigingen onderschatten. Een derde van de onderzochte bedrijven besteedt niet regelmatig aandacht aan digitale dreigingen. Veel bedrijven in het MKB kunnen zich geen voorstelling maken bij cybercrime. De beschermingsmaatregelen die ze nemen zijn

basaal, zoals het gebruik van virusscanners, firewalls en het versleutelen van wifi-verbindingen. Dit is opvallend, omdat uit onderzoek blijkt dat 74 procent van de bedrijven uit het MKB in grote mate of volledig afhankelijk zegt te zijn van ICT. Hetzelfde onderzoek meldt dat ruim 28 procent van het MKB slachtoffer is geweest van cybercrime.



Het MKB is belangrijk voor Nederland. Veel ketens bevatten bedrijven uit het MKB, zo ook ketens binnen de vitale processen. Qua cybersecuritymaatregelen blijft deze groep achter. Dat betekent een risico voor de vitale processen en daarmee voor de Nederlandse samenleving. Gebruikers stellen impliciet hoge kwaliteitseisen aan digitale dienstverlening. Zonder dat hierover afspraken zijn gemaakt gaan zij ervan uit dat beschikbaarheid, integriteit en vertrouwelijkheid hoog is.

Dienstverleners voelen de noodzaak van ‘goed huisvaderschap’, maar kunnen niet aan alle impliciete verwachtingen voldoen.

Lokaal of in de ‘Cloud’

Veel MKB-bedrijven maken gebruik van clouddiensten voor hun kantoorautomatisering. Daarmee zijn ze voor een groot deel ontzorgd voor hun ICT beheer. Dit brengt wel extra complexiteit voor de Informatie Beveiliging met zich mee. Enerzijds doordat de eigenaar van de data (de MKB’er) altijd verantwoordelijk blijft voor zijn data en dus harde eisen moet stellen aan zijn cloud-dienstverlener, anderzijds doordat zijn lokale apparatuur nog steeds data kan lekken. In het ergste geval zelfs de log-in gegevens van de clouddienst waardoor een mogelijke hacker overal vandaan kan inloggen op de gegevens. Dubbele bescherming is dus noodzakelijk.

Wat is een datalek?

Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident moet u bijvoorbeeld denken aan het kwijtraken van een USB-stick, diefstal van een laptop of aan inbraak door een hacker.

Maar niet ieder beveiligingsincident is tevens een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan of als u onrechtmatige verwerking van de persoonsgegevens redelijkerwijs niet kunt uitsluiten.

Als alleen sprake is van een zwakke plek in de beveiliging spreken we van een beveiligingslek en niet van een datalek. U hoeft dan geen melding te doen aan de Autoriteit Persoonsgegevens.

Wanneer moet je een datalek melden?

Niet elk datalek hoeft te worden gemeld. De wet bepaalt dat ‘ernstige’ datalekken binnen 72 uur bij de toezichthouder gemeld moeten worden. Een lek kan ernstig zijn als het een grote hoeveelheid data betreft (kwantitatief ernstig), maar ook als het om gevoelige gegevens gaat (kwalitatief ernstig). Volg het schema op pagina 11 om te bepalen of u moet melden.

Uitzondering op de Meldplicht

De meldplicht datalekken uit de Wbp is niet van toepassing als de Wbp niet van toepassing is. Dit is bijvoorbeeld het geval als u uitsluitend voor persoonlijke of huishoudelijke doeleinden persoonsgegevens verwerkt.

Wat zijn bijzondere persoonsgegevens?

Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

- **Gegevens over de financiële of economische situatie van de betrokkene**: Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
- **(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene**: Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- **Gebruikersnamen, wachtwoorden en andere inloggegevens**: De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang tot geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- **Gegevens die kunnen worden misbruikt voor (identiteits)fraude** : Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het burgerservicenummer (bsn).

Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal personen van wie er gegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. Maar let op: als de aard van de gelekte gegevens daar aanleiding toe geeft is het mogelijk dat u een datalek moet melden waar de persoonsgegevens van slechts één persoon bij betrokken zijn.

U moet de melding doen zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek. Op de website van de Autoriteit Persoonsgegevens is voor dit doel een online formulier beschikbaar. Via dit formulier kunt u de melding zo nodig aanvullen of intrekken.

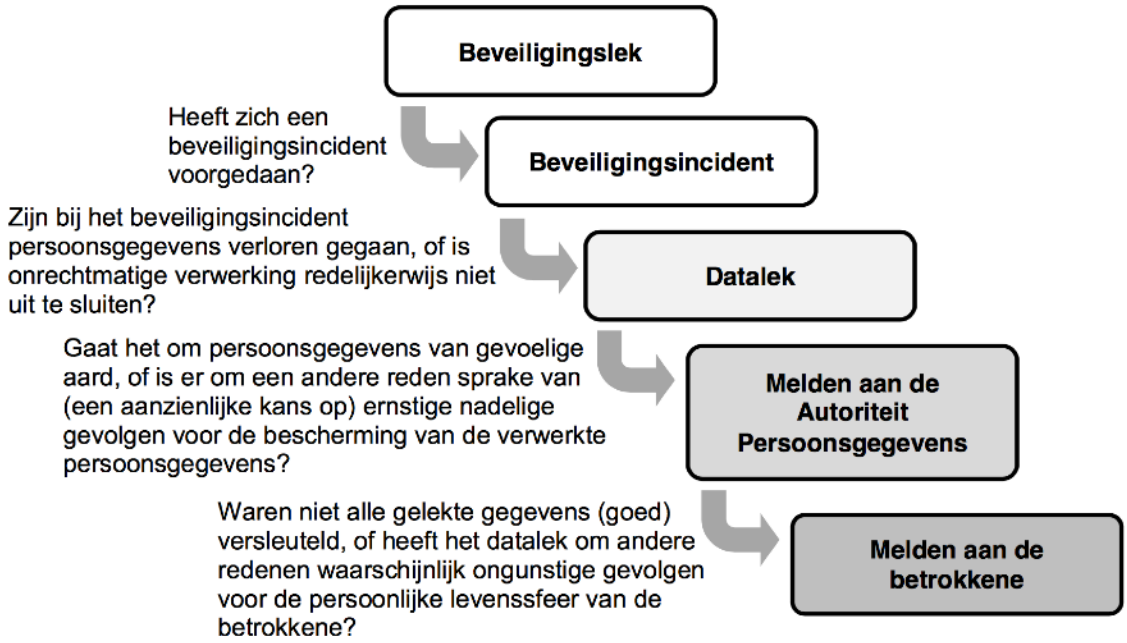
Wanneer moet je een datalek melden aan de getroffen personen?

Indien het datalek waarschijnlijk ongunstige gevolgen heeft voor het privéleven van de personen van wie de gegevens gelekt zijn, dien je - naast de melding aan de toezichthouder - het lek tevens binnen twee werkdagen te melden aan de personen waarvan de gegevens zijn gelekt. Dit zullen in de meeste gevallen klanten zijn. Ongunstige gevolgen zijn bijvoorbeeld:

- Identiteitsfraude
- Discriminatie
- Reputatieschade

Wanneer kwantitatief ernstige gegevens zijn gelekt, is er eigenlijk altijd sprake van een ongunstig gevolg. Dit moet dus ook altijd worden gemeld aan de getroffen personen.

Als u een financiële onderneming drijft zoals bedoeld in de Wet op het financieel toezicht (Wft), dan is de verplichting vanuit de Wbp om datalekken te melden aan de betrokkenen niet op u van toepassing. Als u de betrokkenen informeert, doet u dat op grond van uw zorgplicht vanuit uw financiële onderneming.



Wanneer hoef je een datalek niet te melden?

Een datalek dat aan het criterium van vraag 2 voldoet, moet altijd worden gemeld aan de toezichthouder. Daarbij doet het er niet toe of het lek door een fout is ontstaan of het gevolg is van overmacht. Een datalek hoeft echter niet aan de getroffen personen gemeld te worden wanneer de gelekte persoonsgegevens onleesbaar zijn. Hiervan is bijvoorbeeld sprake wanneer de persoonsgegevens versleuteld zijn of wanneer de gegevens op afstand verwijderd kunnen worden van bijvoorbeeld een gestolen laptop. Je moet er dan wel zeker van zijn dat niemand de gegevens heeft kunnen inzien. Je draagt hiervoor de bewijslast. De beoordeling of een datalek gemeld moet worden aan de toezichthouder en/of de getroffen personen ligt te allen tijde bij jezelf. Als je echter onjuist inschat dat er geen melding nodig is dan kun je dáár ook voor op de vingers getikt worden.

Hoe meld ik een datalek?

U moet de melding doen zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek. Op de website van de Autoriteit Persoonsgegevens is voor dit doel een online formulier beschikbaar. Via dit formulier kunt u de melding zo nodig aanvullen of intrekken.

Welke informatie over een datalek moet je bewaren?

Wanneer je een datalek aan de toezichthouder meldt, dien je een overzicht hiervan in jouw administratie te bewaren. Dit overzicht moet de feiten en gegevens van het lek bevatten. Denk hierbij aan de oorzaak van het lek, het soort gegevens dat gelekt is, het moment waarop het lek is ontdekt en op welke wijze het lek gedicht is. Als je het datalek ook aan de getroffen personen hebt gemeld, is het belangrijk de communicatie hierover te bewaren. Voor het bewaren van de voornoemde gegevens dien je uit te gaan van een minimale bewaartermijn van één jaar.

Wat zijn de gevolgen van de wet?

Bij overtreding van de meldplicht datalekken uit de Wbp kan de Autoriteit Persoonsgegevens een bestuurlijke boete opleggen. Deze bestuurlijke boete bedraagt ten hoogste het bedrag van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht. Dat is per 1 juli 2016 maximaal € 900.000,--. Indien de overtreding niet opzettelijk is begaan en er geen sprake is van ernstig verwijtbare nalatigheid, dan zal de Autoriteit Persoonsgegevens eerst een bindende aanwijzing opleggen voorafgaand aan een eventuele oplegging van een bestuurlijke boete. Bij het opleggen van een bestuurlijke boete houdt de Autoriteit Persoonsgegevens rekening met alle omstandigheden die betrekking hebben op de melding. Een omstandigheid kan bijvoorbeeld zijn dat de gegevens waarover het gaat niet door derden zijn ingezien.

Vaak zal er eerst een waarschuwing gegeven worden, maar de toezichthouder mag besluiten direct een boete op te leggen als je opzettelijk of grof nalatig hebt gehandeld.

Moet een bewerker datalekken melden?

In veel gevallen wordt het verwerken van persoonsgegevens uitbesteed aan een derde partij. Deze derde partij noemt de wet een bewerker. Data kan bijvoorbeeld toegankelijk zijn voor een clouddienstverlener die updates uitvoert op software, opgeslagen zijn bij een hostingprovider, of beschikbaar zijn voor het marketingbedrijf dat e-mails in opdracht van klanten verzendt.

Een bewerker hoeft een datalek niet te melden bij de toezichthouder. Wel moet de bewerker er zorg voor dragen dat haar klanten deze melding tijdig bij de toezichthouder kunnen maken. Er zullen daarom schriftelijke afspraken moeten worden gemaakt waarin wordt vastgelegd op welke wijze de klanten door de bewerker op de hoogte worden gesteld van een datalek. Deze afspraken kunnen worden opgenomen in een (weerbare) bewerkersovereenkomst.

Let op: ben je bewerker en zijn bij een datalek ook gegevens met betrekking tot jouw eigen klantenadministratie gelekt, dan zul je ook zelf melding van het lek moeten maken. Je bent daar dan immers zelf verantwoordelijk voor.

“Het MKB is belangrijk voor de economie,
maar is kwetsbaar op digitaal gebied”

Wat kun je doen om aan de Meldplicht te voldoen?

Eén van de wettelijke verplichtingen is dat je aantoonbaar passende organisatorische en technische maatregelen treft om de persoonsgegevens die je verwerkt te beschermen. De Autoriteit Persoonsgegevens heeft aan de hand van richtsnoeren invulling gegeven aan de elementen waar jouw informatiebeveiliging aan moet voldoen. Dit is geen verplichting, maar het beperkt de kans op hoge boetes en reputatieschade. Het levert ook geen garanties op: elke situatie wordt apart behandeld om te beoordelen of de beveiliging ‘passend’ was.

De Autoriteit Persoonsgegevens heeft meerdere richtsnoeren gepubliceerd. De twee die in dit kader relevant zijn:

1. Richtsnoeren beveiliging van persoonsgegevens
2. Richtsnoeren meldplicht datalekken

Om aan de Wbp te voldoen, uitgaande van de handreiking vanuit de richtsnoeren, zijn de volgende maatregelen nodig:

- **Beleidskader**: het 'wie, wat, waarom' voor jouw informatiebeveiliging.

- **Assessments**: stel vast welke algemene en privacy gerelateerde risico's je loopt.

- **Bewerkersovereenkomst**: inventariseer wie jouw gegevens verwerken en of met deze partijen een bewerkersovereenkomst is gesloten.

- **Non Disclosure Agreement met derden**: sluit met iedere partij waarmee je samenwerkt een NDA af (Non Disclosure Agreement) waarin je persoonsgegevens benoemt.

- **Veiligheidscheck**: controleer hoe bedrijven jouw persoonsgegevens opslaan. Gebeurt dit veilig? Controleer dit uiteraard ook binnen jouw eigen bedrijf. Geven bedrijven aan gecertificeerd te zijn, bijvoorbeeld ISO 27001? Vraag dan naar de scope van deze certificering.

- **Verzekerd**: ga na bij jouw verzekeraar of verzekeringstussenpersoon of je verzekerd bent tegen het lekken van persoonsgegevens (een cyberrisico verzekering).

- **Beveiligingsbewustzijn**: hanteer intern een procedure voor de omgang met en melding van datalekken. De mens is namelijk vaak de zwakste schakel.

- **Fysieke en logische toegangsbeveiliging**: zorg dat alleen bevoegden bij de data kunnen.

- **Security monitoring**: logging, controle en beheer van technische kwetsbaarheden.

- **Databescherming**: validatie op gegevensbewerking en versleuteling van data.

- **Incidentenbeheer**: risico-inschatting, informeren van betrokkenen, evalueren en wanneer er juridische vervolgstappen nodig zijn het bewijsmateriaal verzamelen.

- Beslis **wie** in de organisatie datalekken gaat beoordelen en melden bij de Autoriteit Persoonsgegevens en hoe je de betrokkenen gaat informeren bij een datalek.

- **Controle op naleving**: valideren dat maatregelen ook echt werken.

Deze zaken zijn niet van de ene op de andere dag geregeld. Het vereist een plan op basis van beleid en risicoanalyse waarbij dat plan het meest fundamentele onderdeel van de richtsnoeren is.

Zorg in ieder geval voor zoveel mogelijk passende maatregelen voor uw organisatie. Niets doen is geen optie. Alles doen is vaak te duur. Maak een goede afweging tussen technische en organisatorische maatregelen. Het feit dat u actief bezig bent met deze materie en het goed wilt doen is al van heel veel waarde.

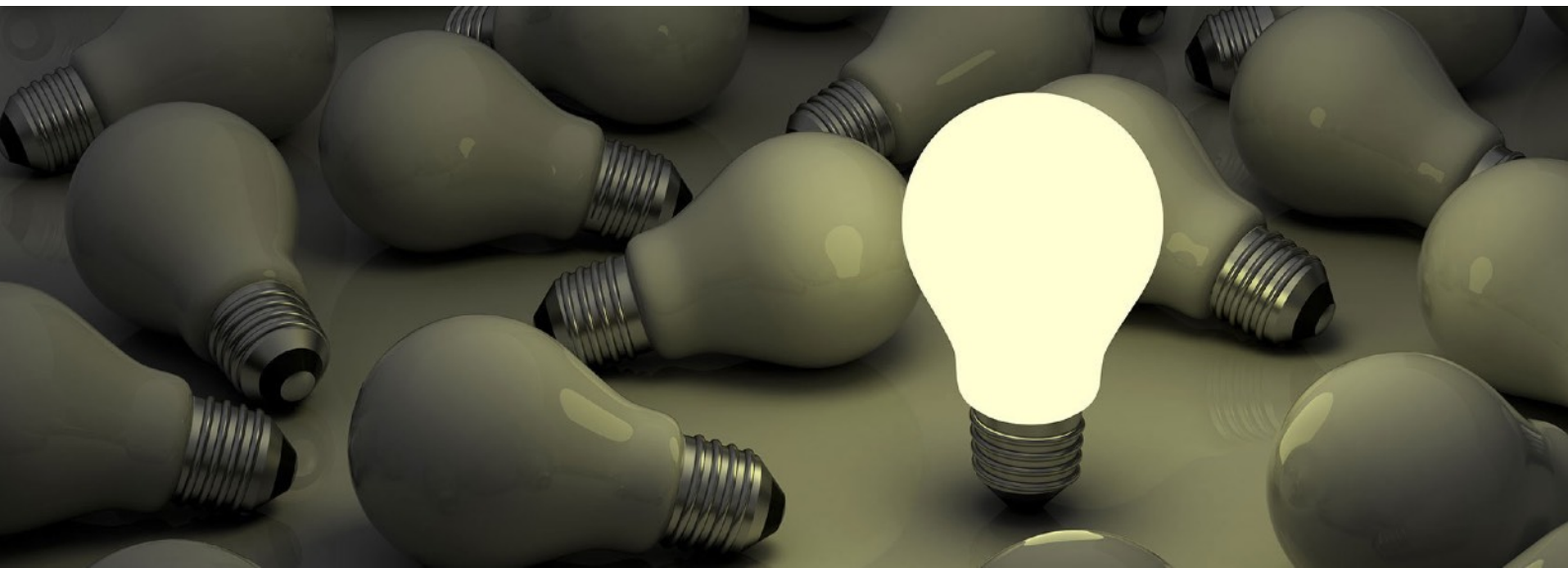
Wat levert dit mij op?

Door aan bovenstaande maatregelen te voldoen, doe je er (aantoonbaar) alles aan om persoonsgegevens te beschermen. En dat is wat de Autoriteit Persoonsgegevens zal valideren. Er zijn geen garanties, want die worden door de Autoriteit Persoonsgegevens zelf op voorhand niet afgegeven.

Maar los van het Wbp zijn dit maatregelen die van toegevoegde waarde zijn. Ze leiden tot inzicht en controle over informatiebeveiliging en daarmee tot volwassenheid en weerbaarheid tegen digitale dreigingen.

Dit dient, naast het voldoen aan de wet, ook andere business doelen:

- **Voorkomen van schade als gevolg van digitale incidenten in brede zin (continuïteits verstoring, reputatieschade)**
- **Goede concurrentiepositie in markten die steeds veeleisender worden ten behoeve van privacy en databescherming**
- **Aantoonbare beveiliging naar klanten en toezichthouders**
- **Sterkere bewustwording van risico's en beveiliging bij management en medewerkers**



7 Tips om ‘In Control’ te zijn

1 Zet technische maatregelen in om een incident zoals een datalek te detecteren. Denk dan aan **monitoring van het uitgaande netwerkverkeer** of aan het beheer van de mobiele apparaten die in gebruik zijn. Zonder dergelijke maatregelen blijft bijvoorbeeld communicatie van een besmette computer met een Command and Control-server van een hacker onopgemerkt.

2 Zorg intern voor **duidelijke procedures** voor het melden van een datalek. Organisaties moeten voorkomen dat medewerkers bijvoorbeeld het kwijtraken van een USB-stick niet doorgeven. De aanwezigheid van een ‘helpdesk’ of vertrouwenspersoon die de meldingen in ontvangst neemt kan de drempel verlagen.

3 Maak helder **wie de melding doorgeeft** richting de Autoriteit Persoonsgegevens. Dit kan een afdelingsmanager zijn, een IT-medewerker die is belast met security, of iemand van de juridische afdeling die goed is ingevoerd in de privacyregelgeving. Misschien heeft u zelfs al een Data Protectie Officer in dienst? De aankomende Europese Privacyverordening stelt deze functie in sommige gevallen verplicht.

4 Uit onderzoek blijkt dat veel organisaties niet bekend zijn met de richtlijnen voor het melden. De beleidsregels meldplicht datalekken die de Autoriteit Persoonsgegevens heeft opgesteld bieden een goed houvast.

5 Zorg dat u weet hoe uw **incident-responseproces** is ingericht. Bij de melding wil de Autoriteit Persoonsgegevens weten welke maatregelen u heeft getroffen om verdere schade te voorkomen, zoals het patchen van kwetsbare systemen of het wijzigen van wachtwoorden.

6 Bereid uw **communicatie** van tevoren goed voor als het gaat om incidenten. Zo moet u niet alleen de getroffenen informeren, maar bijvoorbeeld ook de pers.

7 Twijfel over het wel of niet melden van een incident? **Melden!** De meldplicht voorziet niet in boetes voor onnodige meldingen, maar wel in boetes voor het niet melden van een datalek.

(Bron: KPN bit.ly/29WKKk6)

Technische oplossingen

Er bestaan diverse mogelijkheden om technisch in control te komen over uw data:

- Update uw router/modem met de laatste firmware.
- Installeer alle updates op uw computer en mobiele apparaten.
- Gebruik versleuteling op uw computer, zeker bij een laptop.
- Zet geen gevoelige informatie op USB-sticks. Als dat toch moet dan in ieder geval versleutelen.
- Wees voorzichtig met openen van onbekende e-mail.
- Houd uw anti-virus/anti-malware pakket up-to-date. Het voorkomt niet alle besmettingen maar beter iets dan niets.
- Gebruik de firewall in uw router en op uw computer.
- Zet een pincode op uw mobiele apparaat.
- Gebruik sterke wachtwoorden (minimaal 8 tekens).
- Gebruik minimaal WPA2 voor Wifi verbindingen.
- Gebruik een password manager voor het beheer van uw wachtwoorden.

Ondanks alle bovenstaande maatregelen kan het toch voorkomen dat uw computer of netwerk besmet raakt. Dat is dan alleen nog maar te detecteren op het uitgaande netwerkverkeer.

Tot voor kort was dat alleen maar mogelijk door middel van dure technische oplossingen, vaak voor tienduizenden euro's. SecureMe2 brengt deze oplossing nu naar het MKB.

Bescherm uw klantgegevens tegen misbruik en uw organisatie tegen hoge boetes. SecureMe2, de eerste betaalbare oplossing voor het MKB.

Kijk voor meer informatie op www.secureme2.eu of stuur een e-mail naar info@secureme2.eu