INTERNATIONAL SECURITY PARTNERS

EEN DATALEK IS ZO GEBEURD

Met de nieuwe privacywet AVG (25 mei 2018) bent u als ondernemer eindverantwoordelijk voor de bescherming van privacy gevoelige informatie van uw medewerkers en relaties. Elke onderneming is uniek, wij kijken graag samen met u welke maatregelen het beste passen binnen uw organisatie. Werknemers, opdrachtgevers en andere relaties moeten er op kunnen vertrouwen dat hun privacy gevoelige informatie bij u veilig is, zegt de wet.

Hoe u deze verplichting uitvoert en welke maatregelen u neemt laat de wetgever over aan u. Het enige wat de wetgever er over zegt is dat u 'passende maatregelen dient te nemen'. In het geval dat privacy gevoelige informatie ongewenst in verkeerde handen komt wordt er gesproken over een datalek waarvan u verplicht bent melding te maken bij de Autoriteit Persoonsgegevens.

IN 2018 ONTVING DE AUTORITEIT PERSOONSGEGEVENS 20.881 MELDING VAN DATALEKKEN.

Dit is een bijna een verdubbeling ten opzichte van 2017 waarin 10.009 en een verviervoudiging ten opzichte van 2016 waarin 5.617 meldingen werden genoteerd (Bron: Autoriteit Persoonsgegevens)

Ingeval van een datalek kan u dat een forse boete opleveren van de Autoriteit Persoonsgegevens en mogelijk tot reputatieschade leiden.

DATALEK TENGEVOLGE VAN ONDERSCHATTING

In onze praktijk zien wij dat bedrijven voornamelijk investeren in technische maatregelen en desgevraagd hun eigen kwetsbaarheid, als het gaat om de kans en effecten van een datalek, ernstig onderschatten. Dit blijkt uit de cyber risicoanalyses die we hebben uitgevoerd in opdracht van verzekeraars bij meer dan tweehonderd ondernemingen. Uit deze risicoanalyses blijkt dat veel ondernemingen geen objectief en goed beeld hebben bij wat privacy gevoelige informatie is en wat risico's en gevolgen zijn indien die in verkeerde handen terecht komt. Uit diezelfde analyses blijkt ook dat vele ondernemingen niet helder in beeld hebben hoe kwetsbaar zij zijn voor een cyber incident. Oorzaak hiervan is veelal bedrijfsblindheid. Daarbij constateren we dat er door ondernemers zwaar geleund wordt op hun externe IT partner en/of systeembeheerder en niet goed op de hoogte zijn van hoe de beveiliging van hun eigen IT infrastructuur is georganiseerd.
Wij constateren dat de organisatorische maatregelen veelal te wensen overlaten en er weinig wordt geïnvesteerd in het creëren van cyber awareness onder medewerkers.
Dat technische maatregelen een datalek niet voorkomen blijkt wel uit de praktijk.

DE MENS EN BEDRIJFSBLINDHEID

Een medewerker van een marketingbureau besluit om s 'avonds thuis zijn werk af te maken. Onderweg naar huis stopt hij nog even bij de supermarkt voor zijn avondeten. Hooguit 5-10 minuten is deze medewerker in de winkel geweest maar dit was lang genoeg om de laptop uit zijn auto te stelen. Deze laptop bevatte twee miljoen persoonsgegevens welke in vertrouwen door hun relaties zijn overgedragen aan het marketingbureau. Deze liggen nu op straat voor de hoogste bieder.
In bovenstaand voorbeeld was sprake van een zeer betrokken en loyale medewerker. Wellicht als gevolg van bedrijfsblindheid in combinatie met onvoldoende risico bewustzijn heeft dit incident kunnen plaats vinden. Voor de medewerker was het allemaal data op zijn laptop, voor de cybercriminelen is dit goud.

DE MENS EN ORGANISATORISCHE MAATREGELEN

Onze klant maakt gebruik van een glazenwassersbedrijf. Op een dag worden de glazen binnen gewassen. Eén van de glazenwassers laat een USB stick rondslingeren en verlaat vervolgens het pand. Een medewerker vindt de USB stick en wil deze terug brengen bij de eigenaar. Zij steekt de USB stick in de computer en het volledige bedrijfsnetwerk ligt een halve dag later plat. De USB stick was geïnfecteerd met een slim virus die niet door de virusscanners werd gedetecteerd.
Dit voorbeeld toont aan hoe een onschuldige en goedbedoelde actie van een medewerker tot grote gevolgen kan leiden. In dit voorbeeld moesten extra kosten worden gemaakt om het virus te verwijderen en is de getroffen onderneming een groot aantal uren lamgelegd.

UW DATA BESCHERMEN

Uw informatie moet beveiligd worden, door de juiste beveiliging voorkomt u dat gevoelige informatie in de verkeerde handen komt. Data beschermt u door technische en organisatorische maatregelen te nemen, International Security Partners kan u hierbij ondersteunen.
Enkele oplossingen die International Security partners u kan bieden:

- Awareness trainingen (klassikaal of middels E-Learning)
- Mystery Guest (op locatie of van afstand)
- Cyber Risico Analyse
- Informatiebeveiligingsaudit
- Het opstellen van een informatiebeveiligingsbeleid

International Security Partners is de crisis management partner van MS Amlin op het gebied van cyberincidenten. Samen met gerenommeerde partners vormen wij het MS Amlin First Response Team. Het MS Amlin First Response Team staat 24/7 voor haar klanten klaar met onder meer crisismanagement, juridisch advies, IT ondersteuning, forensisch onderzoek en crisiscommunicatie. Deze nationale én internationale dienstverlening is erop gericht om risico's te beperken en te beheersen.