Experts in Training & Conferences
an informa business

whitepaper

Wet meldplicht datalekken

Wanneer en aan wie melden?
Zijn boetes te voorkomen?

WEBWERELD CUSTOM

Wet meldplicht datalekken

Wanneer en aan wie melden? Zijn boetes te voorkomen?

Eind juni is de wet meldplicht datalekken aangenomen. Organisaties zijn nu in bepaalde situaties verplicht om datalekken te melden. Verzwijgen en hopen dat het allemaal wel overwaait is zeer onverstandig. Voorheen werden geen boetes uitgedeeld bij beveiligingslekken, maar met de nieuwe wet kunnen torenhoge boetes worden opgelegd. Wat verandert er allemaal en wat betekent dit voor organisaties?

De nieuwe wet meldplicht datalekken is geen zelfstandige wet, maar een wijziging van de Wet bescherming persoonsgegevens (Wbp). Daar is een nieuw kernartikel aan toegevoegd, artikel 34a. Dit artikel treedt op 1 januari 2016 in werking. De meldplicht datalekken loopt vooruit op een meldplicht datalekken die ook wordt opgenomen in de Europese Privacy Verordening (EPV). Over de EPV wordt op Europees niveau nog onderhandeld maar de verwachting is dat die nog dit jaar wordt aangenomen, waarbij waarschijnlijk een overgangsperiode van twee jaar zal worden gehanteerd. Maar de Nederlandse wetgever wilde de EPV niet afwachten en voert een meldplicht datalekken alvast nationaal in.

Boetes

Met de gewijzigde Wbp kan toezichthouder Cbp (College bescherming persoonsgegevens) hoge boetes opleggen tot maximaal 810.000 euro. Niet alleen in geval van een datalek, maar ook bij andere schendingen van de Wbp. Voorheen kon het Cbp hiervoor geen boetes opleggen. De naam van toezichthouder Cbp verandert met de wetswijziging overigens in Autoriteit Persoonsgegevens (AP) om het gezag en het toezichthoudende karakter van dat orgaan te benadrukken.

.. de boetebevoegdheid bij schending van de privacy oplopen tot maximaal honderd miljoen euro ..

Zodra de EPV van kracht wordt, kan de boetebevoegdheid bij schending van de privacy oplopen tot maximaal honderd miljoen euro, of vijf procent van de wereldwijde omzet. Dat zijn omvangrijke boetes die vergelijkbaar zijn met de boetes in het mededingingsrecht, zoals bij kartelafspraken en bij de bouwfraude. Alle reden dus voor organisaties om er alles aan te doen om datalekken en misbruik van persoonsgegevens te voorkomen.

Wanneer meldplicht

De definitie van een datalek waarvoor de meldplicht geldt, is helaas wat onduidelijk aangegeven en op meerdere manieren te interpreteren. Het staat geformuleerd als een inbreuk op de beveiliging, waarbij een aanmerkelijke kans bestaat op nadelige gevolgen voor betrokkenen. Dit betekent dat elk beveiligingsincident waarbij persoonsgegevens misbruikt kunnen worden, in potentie een datalek is dat gemeld moet worden.

Denk aan een hack, een medewerker die per ongeluk of door social engineering gevoelige data naar buiten stuurt, of iemand die al dan niet tegen betaling opzettelijk data naar buiten brengt. Denk ook aan verlies van een laptop, tablet, smartphone, usb-stick of andere gegevensdrager met daarop niet-encrypted data. Er hoeft niet eens misbruik van de gegevens gemaakt te worden. Alleen al het feit dat er een inbreuk is, is voldoende om het te kwalificeren als een datalek waarvoor de meldplicht geldt.

Toezichthouder en betrokkenen

Wanneer en aan wie datalekken gemeld moeten worden, is momenteel ook nog lastig te zeggen.

De wettelijke definities zijn op meerdere manieren te interpreteren. Ook wanneer boetes worden uitgedeeld en hoe hoog deze zullen zijn is nog onduidelijk. Het Cbp zal zijn boetebeleid de komende tijd dan ook nog moeten verduidelijken. Wat de meldplicht betreft gaat het in ieder geval om twee losse verplichtingen: een meldplicht aan de toezichthouder en een meldplicht aan betrokkenen.

Een datalek moet onverwijld aan de toezichthouder gemeld worden als er een aanmerkelijke kans bestaat op nadelige gevolgen. Melden aan betrokkenen is pas verplicht als het waarschijnlijk is dat de persoonlijke levenssfeer benadeeld wordt. Melding aan de toezichthouder moet altijd als eerste gebeuren. Verder zijn er twee uitzonderingen opgenomen in de wet. De meldplicht geldt namelijk niet voor organisaties in de telecomsector en de financiële sector, omdat voor deze sectoren op grond van specifieke regelgeving al een meldplicht geldt.

Communicatiestrategie

In de wet staat ook vermeld hoe de melding van een datalek eruit hoort te zien. Zo moet de organisatie aangeven wat er gebeurd is, welke maatregelen getroffen zijn en wat de verwachte nadelige gevolgen zijn voor betrokkenen. Verder moet de organisatie verbetermaatregelen voorstellen en aangeven hoe betrokkenen geïnformeerd worden. Dit laatste kan variëren van een gericht telefoontje naar een individu, tot een landelijke mediacampagne.

Het vraagt veel van organisaties om dit proces goed te waarborgen. Want hoe licht je alle betrokkenen in als een bestand met een miljoen klantgegevens is kwijtgeraakt? Doe je dat per SMS, e-mail, of misschien zelfs per brief? Is een landelijke campagne of een advertentie in de krant nodig? Wie is de woordvoerder? Welke informatie breng je naar buiten? Het is essentieel dat organisaties hierop zijn voorbereid, hun draaiboeken hebben klaarliggen en dat bekend is welke functionarissen nodig zijn. De communicatiestrategie moet vooraf bepaald zijn. De meldtermijnen zijn te kort om pas met deze processen te beginnen zodra er een datalek is.

Impactanalyse en risicomanagement

Om datalekken, schade en boetes te voorkomen, is het van belang dat organisaties hun systemen, applicaties en gegevensstromen in kaart brengen. Wat doen ze met persoonsgegevens en is alles wel adequaat beveiligd? Dat kan nog best een klus zijn. Bij grote ondernemingen draait het immers al snel om honderden en soms duizenden applicaties. Hiermee dwingt de wet organisaties aan risicomanagement te doen en meer aandacht te besteden aan het thema privacy.

De IT-architectuur moet meer privacy by design worden. Met goede data governance en de nadruk op dataminimalisatie. Om de risico's in kaart te brengen is een impactanalyse nodig. In de nieuwe wetgeving wordt dit een PIA genoemd, een Privacy Impact Assessment. Dit begint met een nulmeting voor de organisatie, de huidige stand van zaken waarin alle tekortkomingen in het stelsel van beheersmaatregelen aan het licht komen. Op grond daarvan kunnen vervolgens passende beheersmaatregelen getroffen worden.

Het draait niet alleen om het juist inrichten van systemen. Ook bewustzijn en gedrag van medewerkers speelt een grote rol bij het voorkomen van datalekken. Want er kan bijvoorbeeld wel beleid zijn om sterke wachtwoorden te gebruiken, maar als het de cultuur is om die wachtwoorden overal te laten rondslingeren, heeft dat beleid weinig zin. Gedrag staat los van techniek. Training van medewerkers is een continu proces. Het is nodig op alle niveaus, van werkvloer tot aan de directie. Want een organisatie is tegenwoordig in potentie nog maar één muisklik verwijderd van een datalek.

Bewerkers

Vooral bij grotere bedrijven wordt veel gebruik gemaakt van de cloud, outsourcing,

toeleveranciers en ondersteunende partijen. Deze organisaties moeten zowel hun civiele als hun privacy overeenkomsten goed nalopen, om te bepalen of ze nog wel toereikend zijn gezien de wetswijziging. De wet zegt namelijk dat een bewerker, dat is een externe partij die niet hiërarchisch ondergeschikt is aan de verantwoordelijke, verantwoordelijk is voor de beveiliging van persoonsgegevens en daarom de melding moet doen bij een inbreuk op de beveiliging.

Vooral bij de grote publieke cloud service-providers kun je er als organisatie niet voor kiezen om ze bewerker te maken. Dus moet vooraf worden uitgezocht hoe het met de verantwoordelijkheden zit als er een datalek ontstaat en wie boeteplichtig is, dan wel bij wie regres zou kunnen worden gehaald in geval van een opgelegde boete of in geval van schade.

Schade voorkomen bij een datalek

De gevolgen van een datalek kunnen sterk geminimaliseerd worden door ervoor te zorgen dat alle data beveiligd wordt opgeslagen. Bijvoorbeeld via encryptie. Want het nieuwe wetsartikel bepaalt dat organisaties een datalek niet hoeven te melden als de data onleesbaar is voor een onbevoegde derde. Door encryptie te gebruiken kan een organisatie in voldoende mate aantonen dat melden aan toezichthouder en betrokkenen niet nodig is, ondanks dat er sprake is van een datalek.

Stel bijvoorbeeld alleen encrypted usb-sticks met toegangscode of biometrische-controle beschikbaar aan medewerkers. Beveilig mobiele apparaten zodat ze onbruikbaar zijn bij verlies of diefstal. Bij Bring Your Own Device (BYOD) ligt dit lastiger, omdat medewerkers eigen apparaten ook zakelijk gebruiken. Het is aan de organisatie hierin een keuze te maken. BYOD verbieden is aan te raden als het risico groot is, zoals bij medische en financiële organisaties. In dat geval zou aan medewerkers altijd een zakelijk mobiel apparaat aangeboden worden. Een andere optie is BYOD aan strikte gebruiksregels te koppelen en medewerkers eventueel te verplichten hun apparatuur te laten monitoren door de werkgever. Een sterk onderschat veiligheidsrisico is het meelezen door onbevoegden op openbare plekken zoals in het openbaar vervoer of in flexibele kantooromgevingen. Een privacy-filter op het beeldscherm van mobiele apparaten is vaak al een simpele maar doeltreffende bescherming.

Er is al met al heel veel waar je aan moet denken om de risico's te minimaliseren. In ieder geval dienen organisaties zich goed voor te bereiden op deze nieuwe wetgeving.

De benodigde maatregelen op een rij

- geef voorlichting aan medewerkers over hoe om te gaan met persoonsgegevens;
- faciliteer medewerkers in een veilige omgang met persoonsgegevens door zakelijke devices aan te bieden, private cloud oplossingen, privacy filters en/of encrypted gegevensdragers;
- zorg voor richtlijnen of gedragscodes waarin is vastgelegd wat het gewenste gedrag is en gedrag waartegen zal worden opgetreden;
- richt preventief een meldproces in, inclusief een communicatiestrategie en train de verantwoordelijke medewerkers in het doorlopen van dit proces;
- zorg voor standaard encrypted dataverkeer en dataopslag;
- controleer bestaande ICT- en/of bewerkersovereenkomsten op passendheid met de nieuwe regelgeving;
- zorg voor systemen en applicaties die voldoen aan het privacy-by-design en privacy-by-default principe;
- zorg voor het uitvoeren van een privacy impact assessment en bed de resultaten hiervan in je risk control framework in.