Security & Privacy
Cyber Risks

VanDoorne Advocaten • Notarissen • Fiscalisten

ZURICH

Privacyrisico's: bescherm uw gegevens!

Datalekken zijn aan de orde van dag. Banken, verzekeraars, zorginstellingen, retailorganisaties, automatiseerders en advocatenkantoren, iedere organisatie kan het overkomen. De gevallen die de pers halen illustreren dat datalekken reëel zijn en een serieuze aanpak vereisen. Organisaties ontkomen er niet aan aandacht te besteden aan de beveiliging van hun gegevens, zeker met het oog op de steeds striktere regelgeving op het gebied van datalekken. Naast het opstellen van een Incident Roadmap is het aan te raden om regelmatig audits uit te voeren en zich te verzekeren tegen de risico's die samenhangen met datalekken en cyberaanvallen.

Mede door de technologische vooruitgang zijn gegevens tegenwoordig eenvoudig en goedkoop beschikbaar. Wereldwijd is ook de mobiliteit van personen toegenomen en worden gegevens op grote schaal doorgegeven, over de landsgrenzen heen. De technologische ontwikkelingen en globalisering hebben ertoe bijgedragen dat het risico op incidenten, zoals datalekken, steeds groter is geworden. Een datalek kan ontstaan door een menselijke fout, systeemfouten of een geavanceerde aanval van buitenaf. Wat de oorzaken van een datalek ook zijn, het feit dat persoonlijke gegevens van klanten, werknemers of patiënten op straat komen te liggen zorgt ervoor dat een organisatie op diverse gebieden schade lijdt. Datalekken duperen de betrokkenen, de reputatie van de organisatie staat op het spel en de bedrijfsactiviteiten kunnen behoorlijk ontwricht raken. Al met al leidt het tot de nodige schade en kosten voor alle betrokken partijen.

praktijkvoorbeeld 1

Een ziekenhuis constateert dat de medische dossiers van tientallen patiënten en hun adresgegevens jarenlang toegankelijk zijn geweest via een server van het ziekenhuis. De gegevens blijken alleen beveiligd te zijn geweest met een eenvoudig te ontcijferen wachtwoord.

praktijkvoorbeeld 2

Een bank blijkt de website onvoldoende te hebben beveiligd. Hackers weten zich toegang te verschaffen tot allerlei persoonlijke gegevens van vermogende klanten, zoals naam, email adressen, creditcards en financiële gegevens. Deze gegevens worden vervolgens openbaar gemaakt.

praktijkvoorbeeld 3

Door een fout van uw interne postverwerking raken tijdens de verzending cd-roms en een USB stick kwijt met daarop de adressen, bankrekeningnummers, burgerservicenummers en de beoordelingen van uw personeel.

Passende beveiliging

Als het gaat om het lekken van persoonsgegevens is de Wet bescherming persoonsgegevens *(Wbp)* van toepassing. Persoonsgegevens zijn allerlei soorten gegevens die herleidbaar zijn tot een natuurlijke persoon, zoals naam, geboortedatum, gezondheidsgegevens of IP adres.

De Wbp vereist dat persoonsgegevens op een passende manier beveiligd worden door technische en organisatorische maatregelen. Van geval tot geval moet gekeken worden wat een passende beveiliging is. Criteria die daarbij een rol spelen zijn de aard van de te beschermen persoonsgegevens, de stand van de techniek, en de kosten van de tenuitvoerlegging.

Omdat deze normen voor de praktijk niet altijd helder zijn, heeft de privacytoezichthouder, het College Bescherming Persoonsgegevens *(CBP)*, onlangs nieuwe richtsnoeren gepubliceerd voor de te nemen beveiligingsmaatregelen. Per 1 maart 2013 zijn deze nieuwe richtsnoeren in werking getreden en hebben de richtlijnen uit 2001 vervangen. Organisaties dienen regelmatig te checken of het beveiligingsbeleid nog steeds up-to-date is en tevens aansluit op de wet- en regelgeving.

Risico-analyse

Als u het vermoeden heeft dat een incident heeft plaatsgevonden, dient u over te gaan tot maatregelen ter detectie van het incident. Het voor handen hebben van een duidelijk crisismanagement plan is op dat moment cruciaal. De ervaring leert dat de eerste 24 uur na een incident meestal de belangrijkste fase is voor 'damage control' en onderzoek.

Indien een incident wordt gesignaleerd, dienen in ieder geval de volgende stappen te worden genomen:

- Identificeer het incident.
- Kwalificeer aard en ernst van incident.
- Informeer onmiddellijk de contactpersoon voor incidenten.
- De contactpersoon dient het Incidententeam in te schakelen.
- Schakel noodvoorzieningen in.
- Informeer het management.
- Draag zorg voor de vertrouwelijke behandeling van het incident.

Meldplicht datalekken

In Nederland bestaat er formeel nog geen algemene verplichting om datalekken te melden. Toch kunnen zich, afhankelijk van de aard van het datalek, omstandigheden voordoen die maken dat een organisatie ook nu al over zal moeten gaan tot het melden van een datalek. De Wbp verplicht organisaties om persoonsgegevens zo zorgvuldig mogelijk te verwerken. Uit deze zorgplicht zou men indirect een meldplicht aan de gedupeerden en de toezichthouder kunnen afleiden.

In navolging van de Europese wetgever kennen we sinds juni 2012 in Nederland in de Telecommunicatiewet wel al de 'smalle meldplicht'. Deze meldplicht houdt in dat op de aanbieders van openbare elektronische communicatiediensten een wettelijke meldplicht rust. Zij moeten lekken van persoonsgegevens melden aan de Onafhankelijke Post en Telecommunicatie Autoriteit *(OPTA)* en aan benadeelde klanten. Inmiddels is de OPTA samengevoegd met de Consumentenautoriteit en de Nederlandse Mededingingsautorite*it (NMa)* tot de Autoriteit Consument en Mark*t (ACM),* zodat de melding aan de ACM moet worden gedaan.

Verder is een wetsvoorstel tot wijziging van de Wbp in de maak, ter invoering van een 'brede meldplicht'. Dit wetsvoorstel beoogt de meldplicht voor datalekken uit te breiden naar iedere organisatie die persoonsgegevens verwerkt en kent daarnaast sanctionerende bevoegdheden. Volgens dit voorstel kunnen de boetes oplopen tot € 200.000,00. Daarmee loopt het voorstel vooruit op de op handen zijnde herziening van de Europese privacyregels. In de nabije toekomst wordt de Europese Privacyrichtlijn uit 1995 vervangen door een Algemene Privacy Verordening. Volgens het voorstel van de Verordening komt er een algemene meldplicht datalekken binnen de EU. Omdat het nog een voorstel is, ligt de inhoud van deze meldplicht nog niet definitief vast. De hoofdlijnen zijn wel al te benoemen. Er wordt een algemene meldplicht geïntroduceerd om datalekken, vermoedelijk binnen 72 uur, aan de bevoegde toezichthoudende autoriteit te melden. Daarnaast dient zo spoedig mogelijk melding plaats te vinden aan gedupeerden. Op niet melden van een datalek staat, volgens het voorstel voor de verordening, de hoogste sanctie: 2% van de wereldwijde jaaromzet van een onderneming. Naar verwachting zal de Verordening rond 2014 definitief zijn vastgesteld. Er zal sprake zijn van een overgangsperiode van twee jaar.

Multinationals

De EU privacyvoorstellen zijn niet alleen van belang voor bedrijven met vestigingen binnen de EU, maar ook als uw organisatie buiten de EU is gevestigd, bijvoorbeeld in de USA of Japan. Als uw organisatie (gratis) producten en diensten levert aan EU burgers, of als uw organisatie hen monitort, bijvoorbeeld door analyse van het koopgedrag, krijgt u straks ook te maken met de nieuwe strengere privacyregels voor datalekken. Bedrijven die buiten de EU gevestigd zijn, zullen in de EU een vertegenwoordiger moeten aanwijzen, die verantwoordelijk wordt voor de naleving van de privacyregels.

Privacy claims

Wanneer een datalek zich voordoet, kan de organisatie hiervoor aansprakelijk worden gehouden. Deze aansprakelijkstelling kan ontstaan doordat een melding is gedaan, of juist niet is gedaan. In de samenleving begint steeds meer het bewustzijn te leven dat individuen organisaties aansprakelijk kunnen houden voor geleden schade in verband met gegevensverwerkingen en -lekken. De gedupeerden kunnen een civielrechtelijke actie starten op basis van onrechtmatige daad. Naast een vergoeding voor de daadwerkelijk geleden (financiële) schade, voorziet de wet in de mogelijkheid om de immateriële schade te vorderen. Het gaat hierbij om een naar billijkheid vast te stellen vergoeding.

De met deze vergoedingen gemoeide bedragen kunnen oplopen al naar gelang de omvang en de aard van de gelekte gegevens en het aantal gedupeerden toeneemt. Naarmate het onderwerp meer in de belangstelling komt, is de kans aanwezig dat meer claims volgen. Als een groot aantal personen door het incident getroffen is, kan het totale schadevergoedingsbedrag oplopen.

Binnen de Wet collectieve afwikkeling massaschade wordt gedupeerden de mogelijkheid geboden om een schadevergoeding algemeen bindend te laten verklaren. Nadat de schadevergoeding algemeen bindend is verklaard, zijn de gemaakte afspraken ook geldig voor partijen die niet bij de onderhandelingen betrokken waren. Organisaties kunnen aldus geconfronteerd worden met grote claims.

praktijkvoorbeeld 1

Een bankinstelling wordt aangeklaagd omdat het bedrijf de gegevens van haar klanten niet goed had beveiligd en de diefstal ervan niet snel genoeg bekend heeft gemaakt.

praktijkvoorbeeld 2

Een online retailer wordt ervan beschuldigd onzorgvuldig omgegaan te zijn met de persoonlijke gegevens van miljoenen gebruikers, waardoor deze openbaar toegankelijk zijn geworden.

Rol van de toezichthouders

Het CBP kan uit eigen beweging of naar aanleiding van een melding een onderzoek instellen naar de naleving van de Wbp. Daarbij kan het CBP zowel proactief als reactief optreden. Voor de uitoefening van zijn bevoegdheden kan het CBP bij organisaties binnentreden, inlichtingen inwinnen en zich de toegang verschaffen tot relevante documenten. Als sprake is van overtreding van de Wbp kan het CBP ook bestuursdwang toepassen. Dat betekent dat het CBP de schending van de Wbp feitelijk ongedaan kan laten maken op kosten van de overtredende organisatie. Tevens kan het CBP een last onder dwangsom opleggen. Dat houdt in dat de organisatie een dwangsom verbeurt totdat voldaan is aan de door het CBP opgelegde verplichting. Het staat het CBP verder vrij om haar bevindingen publiekelijk bekend te maken waardoor de reputatie van de organisatie kan worden aangetast.

Recente voorbeelden tonen aan dat de toezichthouders, zowel binnen als buiten Europa, steeds meer de handen ineen slaan bij de aanpak van privacyovertredingen. Naar verwachting zullen zij vaker gezamenlijk optrekken en zich daarbij toeleggen op toezicht en de handhaving. Als het aan de Europese wetgever ligt, krijgen de toezichthouders ook steeds meer mogelijkheden om boetes op te leggen, variërend van 0,5% tot 2% van de wereldwijde jaaromzet van een onderneming. De boetes dienen daarbij, volgens de voorstellen, proportioneel en afdoende afschrikwekkend te zijn.

Verzekeringsoplossing

Verzekeringstechnisch laten de incidenten rondom datalekken zich indelen in twee soorten:

First Party incidenten. Dat zijn incidenten die verband houden met het eigen gebruik van IT systemen en infrastructuur.

Third Party incidenten. Dit type incidenten heeft ook impact op derden, waaronder klanten en betrokkenen, waarop de gegevens betrekking hebben.

Datalekken kunnen leiden tot kosten en schade die zowel behoren tot de first party als de third party incidenten. Bij deze kosten en schade kan onder meer worden gedacht aan:

- Notificatiekosten (notificatie naar toezichthouder, notificatie naar de klanten). Momenteel geldt deze verplichting voor specifieke branches waarvoor een Europese Richtlijn bestaat voor melding datalekken.
- Herstel van data (als data verloren zijn gegaan, beschadigd zijn geraakt of gecodeerd zijn, dienen deze data hersteld te worden).
- Herstel van het netwerk, herstel van de beveiliging.

- Aansprakelijkheid tegenover derden (het verwerken en bewaren van persoonlijke gegevens dan wel gegevens onder een non-disclosure agreement brengt verplichtingen mee).
- Forensisch onderzoek (onderzoekskosten naar de oorzaken en herstel van het incident).
- Juridisch onderzoek naar de verplichtingen op het moment dat een digitale aanval heeft plaats gevonden (onderzoek naar de verplichtingen tot notificeren, verplichtingen tegenover derden).
- Reputatieschade; op het moment dat bekend is geworden dat een online platform is aangevallen, kan schade ontstaan indien men niet accuraat op het incident reageert (PR bureau, crisismanagement, kosten tot herstel van privacy schendingen).
- Bedrijfsstilstand (door een digitale aanval is de bedrijfswebsite een week offline en mist verzekerde inkomsten).
- Boetes, mits verzekerbaar volgens toepasselijke wetgeving (Europese Ontwerp Verordening spreekt over een boete van 2% van de wereldwijde omzet).
- Afpersing en kosten bij dreiging met cyberaanval.

Het is lastig te voorspellen wanneer en hoe een incident plaatsvindt. Het staat vast dat vrijwel alle organisaties hiermee te maken kunnen krijgen. Het is daarom raadzaam om in de preventieve sfeer stappen te ondernemen om de risico's zoveel mogelijk te minimaliseren. Wij verwijzen u hiertoe naar de Zurich Incident Roadmap. Als onderdeel van de risicobeperkende maatregelen is het mogelijk om de Zurich Security & Privacy verzekering tegen dit soort risico's af te sluiten.

Voor nadere informatie kunt u contact opnemen met:

Erik Wolper / Richard Bakker
Underwriters Security & Privacy
Zurich Insurance Plc, Netherlands Branch

Zurichtoren
Muzenstraat 31
2511 VW DEN HAAG

Tel: 0031 (0)70 418 4108
Email: erik.wolper@zurich.com
richard.bakker@zurich.com

ZURICH®

VanDoorne

Advocaten • Notarissen • Fiscalisten