Datalek of beveiligingsincident: zorg dat je voorbereid bent!

Uit cijfers blijkt dat 94% van de Nederlanders zich wel eens zorgen maakt over de bescherming van en/of omgang met zijn of haar persoonsgegevens[i]. Datalekken zijn op dit moment een van de grootste cyberbedreigingen. Ook organisaties merken deze groei en doen er van alles aan om datalekken zoveel mogelijk te voorkomen. Ondanks alle inspanningen is een datalek nooit helemaal uit te sluiten. In deze factsheet maken wij u wegwijs in de wereld van beveiligingsincidenten en datalekken en hoe hiermee om te gaan.

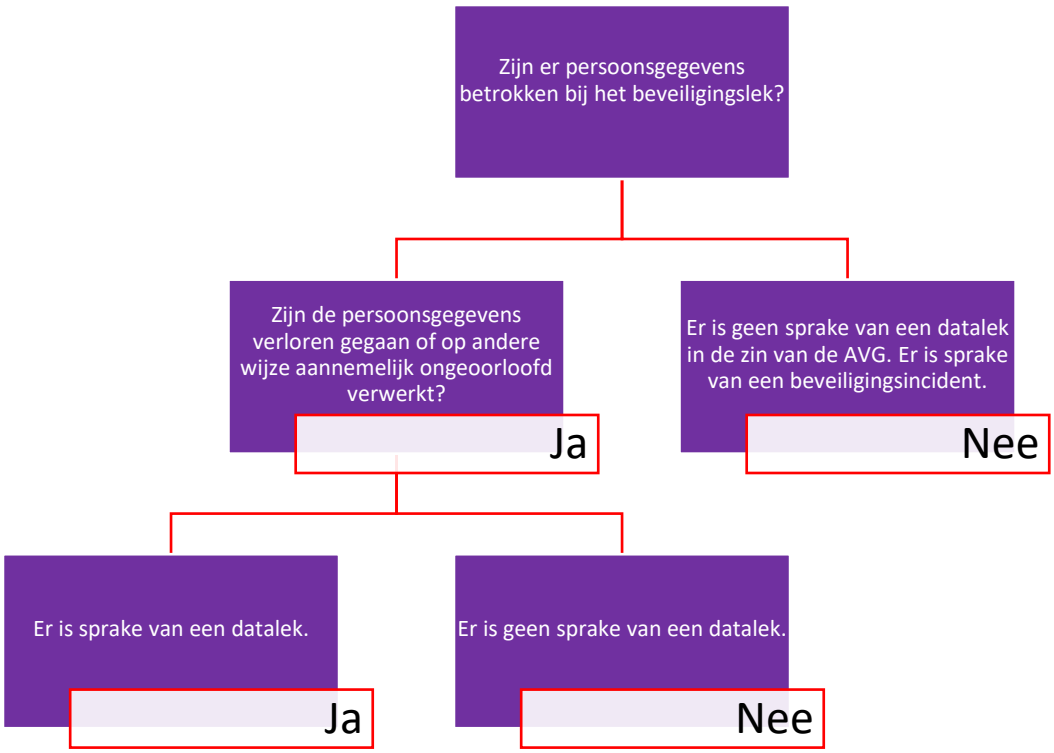
Inleiding

In de Algemene Verordening Gegevensbescherming (AVG) zijn geen definities opgenomen van beveiligingsincidenten en datalekken. Het is daarom lastig om een duidelijke en eenduidige omschrijving van deze termen te geven. Er moet gekeken worden naar een "inbreuk in verband met persoonsgegevens" leert art. 4 lid 12 AVG ons. Een inbreuk wordt vervolgens omschreven als: "*Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.*"[ii] De Autoriteit Persoonsgegevens (AP) gaat ook van deze definitie uit en stelt dat er drie categorieën van beveiligingsincidenten en datalekken te onderscheiden zijn:

- *Inbreuk op de vertrouwelijkheid*
  Wanneer er sprake is van een onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens.
- *Inbreuk op de integriteit*
  Wanneer er sprake is van een onbevoegde of onopzettelijke wijziging van persoonsgegevens.
- *Inbreuk op de beschikbaarheid*
  Wanneer er sprake is van een onbevoegd of onopzettelijk verlies van toegang tot, of vernietiging van, persoonsgegevens.

Classificeren datalek

Het volgende schema kan helpen om te bepalen of er sprake is van een beveiligingsincident of datalek:



Het verschil tussen een beveiligingsincident en een datalek ligt in het feit dat er bij een datalek persoonsgegevens verloren zijn gegaan of dat een onrechtmatige verwerking redelijkerwijs niet is uit te sluiten. Het verschil met een beveiligingsincident is dat daar geen persoonsgegevens bij betrokken zijn. Een datalek is dan ook altijd een beveiligingsincident. Dit geldt andersom niet. Het is belangrijk om het verschil tussen beide begrippen helder te hebben, omdat een beveiligingsincident niet onder de wettelijke meldplicht bij de AP en/of betrokkenen valt waar dit wel geldt voor een datalek.

Voorbeelden van een datalek
Een datalek kan op verschillende manieren plaatsvinden. Bij een datalek wordt veelal gedacht aan het verliezen van digitale informatie of het gehackt zijn door hackers, maar dit hoeft niet zo te zijn. Een datalek kan ook offline gebeuren en het gevaar zit in een klein hoekje. Een aantal voorbeelden van een offline datalek zijn:

- Vertrouwelijke documenten die niet in een papiervernietiger worden gedeponeerd maar in een normale (papier)bak;
- Het laten liggen van documenten op je bureau;
- Je tas verliezen in de trein met daarin mappen met informatie;
- Het versturen van een (medisch) dossier naar een onjuist adres;
- Het plakken van post-its met vertrouwelijke informatie op je beeldscherm als geheugensteuntje.

Echter, de meeste datalekken ontstaan digitaal:

- Verlies van een USB-stick of laptop met niet-versleutelde persoonsgegevens;
- Een cyberaanval waarbij persoonsgegevens zijn buitgemaakt;
- Persoonsgegevens die naar een verkeerde mailinglijst worden gestuurd, waardoor de ontvangers onbedoeld toegang krijgen tot persoonsgegevens;
- Een verwerker die persoonsgegevens verwerkt zonder daarvoor de juiste beschermingsmaatregelen te nemen;
- Het verzenden van een e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden;
- Het gebruik van onveilige software waardoor gegevens niet beveiligd worden;
- Het klikken op phishingmails;
- Het niet beschikbaar zijn van kritieke applicaties zoals een elektronisch patiëntdossier.

Deze voorbeelden zijn niet limitatief dus wanneer u vermoedt dat er *wellicht* een datalek heeft plaatsgevonden, meldt dit dan onmiddellijk intern bij het juiste meldpunt en volg het interne stappenplan of eventueel het stappenplan zoals wij hieronder weergeven.

Artikel 33 en artikel 34 AVG hebben betrekking op het melden van een inbreuk in verband met persoonsgegevens. De eisen uit deze artikelen komen terug bij een aantal van de hieronder genoemde stappen en zullen daar worden toegelicht.

Datalekken: Facts & Figures
De AP heeft aan de hand van alle datalekmeldingen die in 2019 zijn ontvangen de volgende cijfers gepubliceerd:

- Aantal meldingen: 26.956.
- Stijging totaal aantal meldingen ten opzichte van het jaar ervoor: 29%.
- Stijging meldingen hacking & malware ten opzichte van het jaar ervoor: 25%.
- Sector met de meest gemelde datalekken: financiële sector.[iii]

De cijfers vertellen aan de ene kant een duidelijk verhaal maar aan de andere kant kunnen deze zonder achtergrondinformatie

ook een vertekend beeld geven. De stijging van het aantal meldingen is knip en klaar; 2019 steekt vooralsnog met kop en schouders uit boven andere jaren als het aankomt op het totaal aantal meldingen. Het aantal meldingen wat de AP ontvangt is echter redelijk hetzelfde; 67% van de meldingen gaat namelijk over verkeerd verstuurde of verkeerd afgegeven persoonsgegevens. Als je dit vergelijkt met 3% van de meldingen over hacking, malware en/of phishing lijkt het dus te gaan om een groot aantal eenvoudigere/minder 'heftige' meldingen.

Als het om hacking, malware en/of phishing gaat is de AP erg duidelijk: meldt dit altijd direct bij de AP. Deze datalekken leveren de hoogste risico's op voor betrokkenen omdat hackers vaak gerichte aanvallen uitvoeren en op die manier zeer specifieke persoonsgegevens bemachtigen. Deze kunnen ze weer gebruiken om andere vormen van aanvallen uit te voeren. Het is zaak dat de risico's voor betrokkenen niet worden onderschat. Daarnaast is het in veel gevallen alleen te achterhalen wat er precies gebeurd is en hoe de aanval gestopt kan worden door een digitaal forensisch onderzoek te starten en hier een gespecialiseerde partij voor in te schakelen. Hierdoor is het lastig voor een organisatie om op eigen houtje tot een juiste oplossing te komen en zal ook de AP direct moeten worden geïnformeerd. De melding aan de AP kan ook een voorlopige melding zijn en altijd op een later moment worden aangevuld.

Grote malware aanvallen hebben we recent gezien bij de TU Delft en Universiteit Utrecht. Beide waren het slachtoffer van een ransomware aanval waarbij persoonsgegevens buit zijn gemaakt.[iv] Volgens de TU Delft zou het gaan om 60.000 alumni. Het is in deze zaak voor te stellen dat de gestolen gegevens misbruikt zullen worden voor phishing of bijvoorbeeld spam mail.[v]

De financiële- en zorgsector zijn gezamenlijk goed voor bijna 60% (respectievelijk 30% en 28%) van alle bij de AP gemelde datalekken. Door de grote hoeveelheid persoonsgegevens die daar op dagelijkse basis verwerkt worden, is het niet gek dat deze twee sectoren het overgrote deel van de datalekmeldingen vertegenwoordigen.

Tot slot is het interessant om te zien dat meer dan de helft van alle datalekmeldingen (64%) betrekking heeft op maar één persoon. Verder heeft 92% van alle meldingen betrekking op maximaal 100 personen. Slechts een heel klein aandeel van de meldingen (1%) gaat over meer dan 5000 personen.

Uit bovenstaande cijfers kunnen we concluderen dat organisaties (potentiële) datalekken vaak in de gaten hebben, maar dat ze deze soms ook te voorbarig gemeld worden. Wanneer een datalek wel of niet meldplichtig is bij de AP zullen we hieronder uitleggen.

Te volgen stappen
Welke stappen dient uw organisatie te nemen in geval van een datalek:

1) <u>Intern melden</u>
   Op het moment dat er binnen de organisatie een vermoeden is van een datalek dient deze te allen tijde direct en zonder vertraging te worden gemeld bij het eerste aanspreekpunt binnen de organisatie, bijvoorbeeld:
   - Functionaris Gegevensbescherming (FG);
   - Privacycontactpersoon;
   - De directie.

   Zorg dat er een beknopte maar heldere beschrijving gegeven kan worden van het datalek en het vermoeden op welk moment deze is ontstaan. Dit helpt het aanspreekpunt

een eerste inschatting te maken van de ernst van het potentiële datalek.

2) Inventariseren
De aangewezen partij(en) binnen de organisatie bepalen aan de hand van de melding of ze over voldoende informatie beschikken om een juiste (risico)inschatting te kunnen maken. De volgende informatie moet minimaal beschikbaar zijn:
   - Een samenvatting van het datalek;
   - De (mogelijke) oorzaak;
   - Een uiteenzetting van de situatie;
   - Datum en tijd van het ontdekken en van het plaatsvinden van het datalek;
   - De aard van het datalek (inbreuk op vertrouwelijkheid, integriteit of beschikbaarheid);
   - De betrokkenen;
   - Het aantal betrokkenen;
   - Persoonsgegevens;
   - Hoeveelheid persoonsgegevens;
   - Aanwezigheid van bijzondere persoonsgegevens;
   - Zijn er andere organisaties betrokken bij het datalek;
   - Zijn er vooraf technische- en/of organisatorische maatregelen genomen om een dergelijk datalek tegen te gaan.

3) Beoordelen
Vervolgens bepalen de aangewezen partij(en) binnen de organisatie aan de hand van de eerder ingewonnen informatie of er een melding aan de AP en/of betrokkenen is vereist. De volgende informatie wordt meegenomen in het besluit:
   - Wat zijn de (mogelijke) gevolgen voor de persoonlijke levenssfeer van de betrokkenen?
   - Wordt het datalek aan de AP gemeld? Is het antwoord nee, zorg dan voor een uitgebreide onderbouwing.
   - Wordt het datalek aan de betrokkenen gemeld? Is het antwoord nee, zorg dan voor een uitgebreide onderbouwing.
   - Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

Voor het bepalen of er een melding gedaan dient te worden bij de AP is het van belang dat er een risico inschatting is gemaakt. Op het moment dat er een kans is op een risico/er een risico is vastgesteld op de rechten en vrijheden van betrokkenen zal er binnen 72 uur een melding bij de AP gedaan moeten worden. De AP acht de volgende factoren van belang voor een objectieve risico inschatting:
   - De aard van de inbreuk;
   - De aard, gevoeligheid en omvang van de persoonsgegevens;
   - Gemak waarmee de personen kunnen worden geïdentificeerd;
   - Ernst van de gevolgen voor personen;
   - Bijzondere kenmerken van de persoon;
   - Bijzondere kenmerken van uw organisatie;
   - Het aantal getroffen personen.

Betrokkenen dienen te worden geïnformeerd op het moment dat het om een hoog risico gaat. Een datalek

brengt een hoog risico met zich mee wanneer het kan leiden tot lichamelijke, materiële of immateriële schade voor de betrokken personen. Het is niet altijd nodig om een datalek te melden aan de AP of betrokkenen. Daar is in de volgende gevallen sprake van:

- **Melden aan de AP niet verplicht:**

  1) U heeft voordat het datalek plaatsvond passende maatregelen getroffen. Hierdoor zijn de gelekte persoonsgegevens onbegrijpelijk voor onbevoegden. Bijvoorbeeld doordat de gegevens goed zijn versleuteld of vervangen door een hashwaarde.

  Let op, deze uitzondering geldt alleen als:
  - De gegevens nog volledig intact zijn.
  - U nog steeds de volledige controle over de gegevens heeft.
  - De sleutel die voor de encryptie of voor de hashing is gebruikt geen gevaar heeft gelopen bij het datalek en deze ook met de beschikbare technologie niet vindbaar is voor onbevoegden

  2) Zijn de persoonsgegevens verzonden aan een verkeerde maar betrouwbare ontvanger? Dan betekent dit mogelijk dat het niet langer waarschijnlijk is dat het datalek een risico oplevert. In dat geval hoeft u het datalek niet te melden aan de AP of getroffen personen.

- Melden aan betrokkenen niet verplicht:

1) U heeft voordat het datalek plaatsvond passende maatregelen getroffen. Hierdoor zijn de gelekte persoonsgegevens onbegrijpelijk voor onbevoegden. Bijvoorbeeld doordat de gegevens goed zijn versleuteld of vervangen door een hashwaarde.[vi]

2) U heeft, onmiddellijk nadat het datalek plaatsvond, maatregelen getroffen. Het hoge risico voor de rechten en vrijheden van betrokkenen zal zich hierdoor waarschijnlijk niet meer voordoen. Bijvoorbeeld wanneer u de persoon die toegang tot de persoonsgegevens heeft gehad onmiddellijk heeft geïdentificeerd en u actie heeft ondernomen voordat die persoon iets met de persoonsgegevens kon doen.[vii]

3) De gerichte mededeling aan iedere betrokkene zou een onevenredige inspanning vragen. Het gaat bijvoorbeeld om een grote groep van betrokkenen waarvan niet direct (recente) contactgegevens beschikbaar zijn. Er dient dan wel naar andere oplossingen gekeken te worden, bijvoorbeeld het doen van een openbare mededeling op de website van de organisatie.[viii]

4) Daarnaast noemt de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) een aantal gevallen waarin u

een melding aan betrokkenen achterwege mag laten:
- Wanneer dat noodzakelijk en evenredig is om een zwaarwegend belang te waarborgen. Zoals de nationale of openbare veiligheid of de bescherming van de privacy van anderen, bijvoorbeeld wanneer kinderen een hulpvraag hebben gedaan zonder dat hun ouders dat weten.
- Is uw organisatie een financiële onderneming als bedoeld in de Wet op het financieel toezicht (Wft)? Dan geldt de meldplicht aan de betrokken personen niet voor u. Wel geldt de meldplicht aan de AP.

De AP heeft op haar website enkele voorbeelden van het wel/niet melden van datalekken gepresenteerd:

- Als gevolg van een cyberaanval zijn de medische dossiers in een ziekenhuis gedurende 30 uur niet beschikbaar. In dit geval is het ziekenhuis verplicht om aan de AP te melden dat de inbreuk een hoog risico kan inhouden voor het welzijn en de patiënt. Ook moet deze inbreuk gemeld worden aan de getroffen personen.[ix]
- Een verwerkingsverantwoordelijke heeft een back-up van een archief van persoonsgegevens op een USB-stick opgeslagen die wordt gestolen tijdens een inbraak. Dit hoeft niet te worden gemeld aan de AP of betrokkenen zolang de gegevens zijn versleuteld met een geavanceerd algoritme, er back-ups van de gegevens zijn, de unieke sleutel niet is gecompromitteerd en de gegevens tijdig kunnen worden hersteld. Indien er op een later moment wel een compromittering plaatsvindt, moet de inbreuk wel worden gemeld.[x]
- Persoonsgegevens van een groot aantal studenten worden per ongeluk naar de verkeerde mailinglijst gestuurd. Het betreft een lijst met meer dan 1000 ontvangers. Deze inbreuk dient aan de AP te worden gemeld. Daarnaast dient de inbreuk aan personen gemeld te worden, afhankelijk van de omvang en het type persoonsgegevens en de ernst van de mogelijke gevolgen.[xi]

4) <u>Herstellen</u>
Bij een datalek met een technisch aspect dient altijd de ICT-afdeling ingeschakeld te worden om te achterhalen wat de oorzaak is geweest. Zij zullen op dat moment de oorzaak moeten verhelpen. Het is belangrijk dat er wordt vastgelegd wat de technische en organisatorische maatregelen zijn om het datalek te herstellen en een verder of volgend datalek te voorkomen.

Het is belangrijk om de gevolgen van het datalek nadat deze is ontdekt zoveel mogelijk in te dammen. Ten eerste is het van belang om het datalek zo spoedig mogelijk te beëindigen indien deze nog bestaat. Verder is het van belang maatregelen te nemen om de negatieve gevolgen te beperken.[xii] Voorbeelden van maatregelen die genomen kunnen

worden, zijn een gepubliceerd bestand offline halen, een verkeerde ontvanger vragen om een bevestiging dat hij/zij de persoonsgegevens uit een e-mail of brief heeft vernietigd of het blokkeren van een account van een medewerker.

5) Melden bij de Autoriteit Persoonsgegevens

In stap 3 wordt er bepaald of er een melding gedaan moet worden bij de AP. Is dit het geval? Zorg dan dat de in stap 2 verzamelde informatie gebruikt wordt om zonder onredelijke vertraging, maar in ieder geval binnen 72 uur na het ontdekken van het datalek deze te melden.[xiii] In het geval u als verwerker kennis heeft genomen van een datalek dan dient u dit zonder onredelijke vertraging bij de verwerkingsverantwoordelijke te melden.[xiv] Controleer in de verwerkersovereenkomst die is overeengekomen of de gemaakte afspraken en verplichtingen zijn nageleefd. Als verwerkingsverantwoordelijke blijf je verantwoordelijk voor het maken van een melding richting de AP.
Het doel van de meldplicht aan de AP is het voorkomen van datalekken en indien deze zich toch voordoen, de gevolgen ervan voor de betrokkenen zoveel mogelijk beperken.[xv]

Ondanks dat een melding bij de AP redelijk eenvoudig te doen is door het volgen van de vragenlijst moet er wel voldaan worden aan de eisen van art. 33 lid 3 AVG. Dit artikel stelt een aantal eisen aan wat er tenminste in een melding moet staan:[xvi]

a) de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
b) de naam en de contactgegevens van de FG of een ander contactpunt waar meer informatie kan worden verkregen;
c) de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
d) de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomende gevallen, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Het is gelukkig niet verplicht om in eerste instantie meteen een definitieve melding te maken. Omdat het achterhalen van alle verschillende informatie een complex en tijdrovend proces kan zijn, is het volgens de wet en volgens de AP mogelijk om eerst een voorlopige melding te maken. Deze melding kan gezien worden als een vooraankondiging van het datalek en de notie dat de organisatie bezig is met het oplossen en achterhalen van alles omtrent een dergelijk datalek.[xvii]

Als er ten onrechte geen melding wordt gemaakt van een datalek kan dit een bestuurlijke boete tot gevolg hebben van de AP. Dit was het geval

bij Uber. Uber kreeg een bestuurlijke boete van €600.000 opgelegd van de Nederlandse toezichthouder vanwege het te laat melden van een datalek.[xviii] Onbevoegden hadden toegang tot persoonsgegevens van 57 miljoen Uberklanten wereldwijd, waaronder 174.000 Nederlandse gebruikers. De AP oordeelde dat het Uber-concern het datalek te laat had gemeld en tevens de betrokkenen niet binnen 72 uur na het ontdekken van het datalek had geïnformeerd.

6) Betrokkenen Informeren
Op het moment dat er sprake is van een datalek dat leidt tot een hoog risico voor betrokkenen, dienen deze betrokkenen geïnformeerd te worden. Anders gezegd wanneer het waarschijnlijk is dat er ongunstige gevolgen zullen zijn voor de persoonlijke levenssfeer van betrokkenen.[xix] In welke gevallen er sprake is van een hoog risico datalek hebben we gezien in stap 3.

De melding naar betrokkenen is anders dan die naar de AP in die zin dat het in een duidelijke en eenvoudige taal dient te zijn. Daarnaast zal het tenminste de aard van de inbreuk en de in art. 33 lid 3 sub b-d AVG bedoelde gegevens en maatregelen moeten bevatten.[xx] Het is aan te raden om in ieder geval een korte beschrijving te geven van wat er is gebeurd, wat de waarschijnlijke gevolgen zijn, de genomen of nog te nemen maatregelen, wat de betrokkene zelf kan doen, de overweging om al dan niet aan de AP te melden en de contactgegevens van het Privacy Office of de FG voor het stellen van vragen.[xxi] Hoewel de AVG hier niets over regelt, is het aan te raden om de betrokkenen altijd schriftelijk te informeren over het datalek zodat deze melding aantoonbaar gemaakt kan worden.

7) Evalueer, rapporteer en documenteer
Neem tot slot het datalek op in je datalekregister of een logboek, dit geldt voor zowel gemelde als niet-gemelde beveiligingsincidenten of datalekken.[xxii] In het laatste geval dient gemotiveerd te worden vastgelegd waarom er niet is gemeld. Verder dienen ten minste de feiten van de inbreuk in verband met persoonsgegevens, de gevolgen daarvan, de genomen corrigerende maatregelen, de actiehouder en monitoring opgenomen te worden. Spreek intern af met welke frequentie dergelijke taken worden gemonitord. Het register of logboek dient als naslagwerk voor de organisatie en als verantwoording en bewijs naar de AP toe. Het is het advies om per beveiligingsincident of datalek een registratie in het register of logboek bij te houden waarin alle handelingen opgenomen zijn die na het constateren van het incident zijn genomen. Om het register of logboek zo compleet mogelijk te maken dient het exacte tijdstip van de handelingen geregistreerd te worden naast alles wat hierboven al genoemd is.

Toepassing in de praktijk
De aanpak van datalekken begint met het opstellen van een goede interne procedure datalekken. Het doel van een datalekprocedure is het vastleggen van de stappen die gezet moeten worden om een datalek in kaart te brengen.[xxiii] Belangrijk is dat er binnen de organisatie een aantal personen verantwoordelijk zijn voor de beoordeling en afhandeling van datalekken. Vaak zijn dit de Privacy Officer(s) en de FG (indien aanwezig), zij maken deel uit van het ‘Incident Response

Team' dat bestaat uit onder meer IT, communicatie en een verantwoordelijke vanuit het bestuur. Daarnaast dient er een intern meldpunt te zijn waar datalekken gemeld kunnen worden. Dit kan bijvoorbeeld in de vorm van een vast contactpunt (e-mailadres) of bij een team. Zowel voor medewerkers als voor eventuele verwerkers is bekendheid van dit interne meldpunt belangrijk. Zij dienen bekend te zijn met hoe en waar een beveiligingsincident gemeld kan worden. Om de melding zo eenvoudig en soepel mogelijk te laten verlopen doe je er als organisatie verstandig aan om een vragenlijst op te stellen voor melders van een incident. Hierin kunnen vragen opgenomen worden zoals bijvoorbeeld de aard van het incident, het geschatte moment van ontstaan van het incident en het aantal betrokkenen. Hoe eenvoudiger en praktisch werkbaarder de procedure is, des te groter de kans is dat deze binnen de organisatie wordt opgevolgd.

Wat kost een datalek?[xxiv]

De kosten van een datalek verschillen uiteraard van geval tot geval en zijn afhankelijk van een aantal factoren:

- Het aantal betrokken records;
- De duur van het datalek;
- Verlies van het vertrouwen van klanten.

Volgens een studie uitgevoerd in 2019 door IBM zijn de gemiddelde kosten van een datalek 3,92 miljoen dollar. Dit is een optelsom van een grootte van gemiddeld 25,575 records, 150 dollar aan kosten per record en een gemiddeld duur van 279 dagen voordat het datalek volledig is ontdekt en gestopt. Met dergelijke bedragen is het niet meer dan logisch dat bedrijven veel zouden kunnen en moeten investeren in een juiste preventieve datalek huishouding die periodiek getest wordt door de gehele organisatie (zie ook art. 24 lid 1 AVG).

Dit zie je overigens terug in de cijfers die IBM heeft gepubliceerd. Organisatie met een actief en professioneel 'incident response team' en die regelmatig tests uitvoeren, kunnen volgens IBM gemiddeld 1,23 miljoen dollar per datalek besparen in vergelijking met organisaties die dit niet doen.

Daarnaast komt IBM met nog een aantal interessante conclusies in zijn rapport:

- Kwaadaardige aanvallen vormen tegenwoordig het grootste deel (51%) van alle datalekken en kosten een organisatie over het algemeen ook 27% meer dan datalekken veroorzaakt door een menselijke fout en 37% meer dan die veroorzaakt dor een systeemfout.
- Kleinere bedrijven worden over het algemeen harder geraakt als er gekeken wordt naar de kosten per werknemer. Ondanks dat datalekken bij grotere bedrijven vaak stukken hoger zijn, zijn door de grote hoeveelheid werknemers de uiteindelijke kosten per werknemer vaak veel lager dan bij kleinere bedrijven. Het gaat in veel gevallen om een paar duizend euro per werknemer. Het is daarom ook aan te raden om als kleine organisatie te investeren in een goede datalekprocedure.
- De kans dat zich bij uw organisatie een datalek voordoet is de afgelopen jaren gestaag gestegen. Van 22,6% in 2014, 27,9% in 2018 naar uiteindelijk 29,6% in 2019. Hieruit blijkt dat organisaties datalekken steeds beter leren te herkennen.

IBM baseert bovenstaande gegevens op een studie van 507 bedrijven waarbij ze 3.211 individuen hebben geïnterviewd.

Conclusie

Het is duidelijk dat er tegenwoordig meer aandacht is voor datalekken, niet alleen vanuit organisaties en de AP, maar ook vanuit het publiek en zelfs kwaadwillende. Wij willen daarom aanraden om de mogelijkheid op een datalek niet te onderschatten. Voorkomen is beter dan genezen. Vanuit Legal2Practice willen we graag de volgende tips geven ter voorkoming van datalekken:[xxv] [xxvi]

- Stimuleer veilige methoden om data te delen;
- Zorg voor encryptie van persoonsgegevens om te voorkomen dat persoonsgegevens gelezen kunnen worden door derden;
- Stel BCC in als standaardoptie in het e-mailprogramma van de organisatie zodat de kans kleiner wordt dat een medewerker de e-mailadressen van een groepsmail zichtbaar maakt;
- Houd de software waarmee gewerkt wordt actueel;[xxvii]
- Creëer awareness bij medewerkers zodat zij weten hoe ze moeten handelen indien er een datalek plaatsvindt;
- Organiseer een interne opschoonactie waarbij e-mails of bestanden die niet meer nodig zijn worden verwijderd;[xxviii]
- Draag zorg voor het inrichten van een proces omtrent datalekken om te zorgen dat bij ontdekking van een datalek tijdig en doeltreffend gehandeld wordt;
- Creëer een veilige omgeving voor het melden van een datalek;
- Leg een register van datalekken aan en vermeld daarin ook de niet gemelde datalekken/beveiligingsincidenten inclusief motivering;
- Laat het datalekregister en/of de procedure omtrent datalekken jaarlijks beoordelen door een (externe) FG of auditor.

Wij hopen dat we u met deze factsheet wegwijs hebben kunnen maken in de wereld van datalekken en beveiligingsincidenten. Heeft u naar aanleiding van deze factsheet vragen of heeft u hulp nodig bij een datalek? Legal2Practice kan u bijvoorbeeld helpen met het beoordelen of er een datalek heeft plaatsgevonden, een datalekprocedure voor u inrichten, de communicatie naar betrokkenen verzorgen of begeleiden en het beoordelen van het datalekregister.

Gezonde groet,

Legal2Practice B.V.

+31 (0) 26 848 3118

info@legal2practice.nl

Geraadpleegde bronnen

[i] Autoriteit Persoonsgegevens, 'Nederland maakt zich zorgen over privacy', *Autoriteit Persoonsgegevens* 28 januari 2019.
[ii] Art. 4 lid 12 AVG.
[iii] Autoriteit Persoonsgegeven, 'Meldplicht Datalekken: facts & figures Overzicht feiten en cijfers 2019'.
[iv] 'A. Monterie, 'TU Delft en UU roepen Blackbaud op matje na datalek', 11 augustus 2020.
[v] J. Jonnkers, 'Universiteiten van Delft en Utrecht getroffen door datalek', 11 augustus 2020.
[vi] Art. 34 lid 3 sub a AVG.
[vii] Art. 34 lid 3 sub b AVG.
[viii] Art. 34 lid 3 sub c AVG.
[ix]Autoriteit Persoonsgegevens, 'Voorbeeldlijst wel/niet melden datalek', juni 2019.
[x] Idem.
[xi] Idem.
[xii] Autoriteit Persoonsgegevens, 'Acties bij datalekken'.
[xiii] Art. 33 lid 1 AVG.
[xiv] Art. 33 lid 2 AVG.
[xv] *Kamerstukken II* 2012/13, 33662, 3.
[xvi] Art. 33 lid 3 AVG.
[xvii] Art. 33 lid 4 AVG.
[xviii] Autoriteit Persoonsgegevens, 'AP legt Uber boete op voor te laat melden datalek', 27 november 2018.
[xix] CIP, 'De meldplicht datalekken', *CIP* 26 januari 2016.
[xx] Art. 34 lid 2 AVG.
[xxi] Autoriteit Persoonsgegevens, 'Welke informatie moet ik de betrokken personen geven bij een datalek?'.
[xxii] Art. 33 lid 5 AVG.
[xxiii] M. Hennekens, 'Help, een datalek! Hoe stel ik een procedure op?', *Hekkelman* 13 september 2019.
[xxiv] IBM Security, 'Cost of a Data Breach Report', 2019, Poneman.
[xxv] Informatiebeveiligingsdienst, 'Meldplicht Datalekken', *IBD* 4 september 2019.
[xxvi] Autoriteit Persoonsgegevens, 'Acties bij datalekken'.
[xxvii] Idem.
[xxviii] Idem.