Procedure melding datalekken

Algemeen

Ingangsdatum:	25 mei 2018
Versie:	1.4
Opgesteld door:	Gert Staal, directeur-bestuurder
Gewijzigd op:	8 maart 2021
Ondertekening:	

Inleiding

Dit document geeft een beschrijving van verschillende rollen en fases omtrent de afhandeling van beveiligingsincidenten en datalekken.

Standaardprocedure meldplicht datalekken

Het proces gaat uit van drie rollen en zes fases. Een belangrijk uitgangspunt is dat het proces ertoe moet leiden dat alle relevante feiten goed worden vastgelegd gedurende de afwikkeling van een beveiligingsincident/mogelijk datalek. Voor het vastleggen van deze feiten bevat de Toolkit het document Meldplicht datalekken: sjabloon.

Beveiligingsincident of datalek?

Een datalek is een beveiligingsincident waarbij persoonsgegevens verloren zijn gegaan, waarbij de persoonsgegevens onrechtmatig verwerkt zijn of wanneer het niet redelijkerwijs uitgesloten kan één van deze mogelijkheden plaats heeft gevonden. Indien dit niet het geval is, is het dus een beveiligingsincident. Wanneer de organisatie tot de conclusie komt dat het om een datalek gaat, moet worden bepaald of er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens. Afhankelijk daarvan moet het datalek gemeld worden aan de Autoriteit Persoonsgegevens (hierna: AP), of niet.

Standaardprocedure meldplicht datalekken: rolverdeling

Om de juiste informatie tijdig op de juiste plek te krijgen, is het van belang om de voor de afhandeling van een beveiligingsincident en dus een mogelijk datalek, de relevante rollen en verantwoordelijkheden vast te stellen. De proceseigenaar is de manager bedrijfsvoering.

Wij onderscheiden drie rollen:

Rol	*Uitleg*	*Voorbeeld*
Ontdekker	Degene die het beveiligingsincident en mogelijk datalek op het spoor komt, vaak ook degene die (in eerste instantie) over de meeste informatie beschikt.	Vrijwilliger
Technicus	Degene die, indien het datalek een technische oorzaak heeft (wat vaak het geval zal zijn), maatregelen kan nemen zodat het lek 'gedicht' wordt.	N.v.t.
Melder	Degene die belast is met het vergaren van de relevante informatie om op basis daarvan een melding te kunnen doen aan de AP en eventueel aan getroffen klanten.	Functionaris gegevensbescherming

De hierboven beschreven rollen hebben ieder hun eigen verantwoordelijkheden. Hierna worden deze kort omschreven.

Ontdekker

De ontdekker is degene die een beveiligingsincident/mogelijk datalek signaleert en daarover rapporteert bij de melder binnen organisatie waarvoor hij of zij werkzaam is. Omdat de ontdekker aanvankelijk het dichtst op het mogelijke datalek zit, zal hij of zij vaak over nuttige informatie beschikken. Voorbeelden van ontdekkers zijn onder meer:

- Een systeembeheerder die een gat in de beveiliging van een systeem met persoonsgegevens op het spoor komt.
- Een callcentermedewerker die van een klant te horen krijgt dat deze via een klantportaal ook inzage heeft in de persoonsgegevens van een andere klant.
- De medewerker die tot de ontdekking komt dat hij of zij een zakelijke laptop met daarop een omvangrijk klantenbestand in de trein heeft laten liggen.

Het is zaak dat de ontdekker wordt aangespoord om juiste en volledige informatie aan de melder te verstrekken zodat geen kostbare tijd verloren gaat. Zorg dat hiervoor een duidelijke procedure is ingericht.

Over het moment van ontdekken valt te discussiëren. Is het redelijk om van bijvoorbeeld de klantenservice medewerker te verwachten dat deze kan inschatten wanneer het incident een meldplichtig datalek is? Vaak zal dat niet het geval zijn. Of ontdek je de meldplichtigheid pas wanneer het beveiligingsincident wordt beoordeeld door bijvoorbeeld een privacyfunctionaris, die gericht een inschatting kan maken of er persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt en de impact daarvan. Gelukkig biedt de wet nog wel enige mogelijkheid tot het verrichten van onderzoek nadat het beveiligingsincident ontdekt is voordat dit gemeld moet worden, als het een datalek blijkt te zijn. Zo stelt de wet dat een datalek onverwijld gemeld moet worden en hier is door de AP invulling aan gegeven. Zij stelt dat onverwijld betekent binnen 72 uur na het ontdekken. Het is dus zaak dat iedere medewerker binnen de organisatie bekend is met het fenomeen datalek en dat medewerkers ook weten wat er van hen wordt verwacht wanneer ze ermee geconfronteerd worden.

Naast de ontdekker binnen de organisatie kan er ook sprake zijn van een situatie waarbij de ontdekker een persoon is buiten de organisatie zoals bijvoorbeeld een leverancier. In die gevallen is het nog belangrijker voor de organisatie die de rol van verwerkingsverantwoordelijke heeft om ervoor te zorgen dat de (sub)verwerker in de rol van ontdekker weet wat er van hem of haar verwacht wordt. Om dit risico af te kunnen dekken is het aan te raden strikte bepalingen omtrent datalekken en de afhandeling ervan op te nemen in de verwerkersovereenkomst.

Inzet technicus

De technicus is degene die de melder kan helpen met:

- De beantwoording van de vraag welke typen persoonsgegevens gelekt zijn.
- De beantwoording van de vraag wanneer het datalek heeft plaatsgevonden (incl. inzage in of analyse van logfiles).
- De beantwoording van de vraag of de data beveiligd is door bijvoorbeeld versleuteling of anderszins onbegrijpelijk is gemaakt voor derden en op welke wijze dit is gerealiseerd.
- Het repareren van het datalek.
- Voor overige technische vragen.

De melder moet aan de hand van de informatie die hij of zij van de ontdekker ontvangt, snel kunnen vaststellen of er een technicus betrokken moet worden bij de afhandeling van het datalek. Dit zou bijvoorbeeld kunnen door een overzicht op te stellen van de aanwezige systemen en de daarbij behorende technicus. Verder is het aan te raden ook de in dit systeem aanwezige persoonsgegevens

te vermelden, zodat de melder hierop kan anticiperen.

Melder
De melder is de spin in het web van de (formele) afhandeling van het beveiligingsincident en het mogelijke datalek; het is de medewerker die alle benodigde informatie verzamelt of vaststelt. Aan de hand hiervan bepaalt hij of zij of gemeld moet worden aan de AP of niet. En zo ja, of eveneens aan de betrokkenen gemeld moet worden dat zijn of haar persoonsgegevens zijn gelekt. De melder is ook degene die deze melding bij de AP daadwerkelijk doet en zorgt voor archivering van de melding.

Deze rollen sluiten elkaar niet uit: de ontdekker, maar vooral de technicus en melder kunnen, zeker in een kleine organisatie, één en dezelfde persoon zijn. De rol van ontdekker zal niet van tevoren toegewezen kunnen worden aan een medewerker. Deze rol kiest de medewerker in plaats van andersom, aangezien vrijwel iedere medewerker een datalek zou kunnen ontdekken. De rollen van de technicus en melder kunnen vaak wel op voorhand worden toegewezen en dit is ook aan te raden. Bij kleine bedrijven zal de rol van de technicus bij één medewerker of een kleine groep medewerkers berusten. In grote organisaties zal per systeem of groep systemen één technicus aangewezen moeten worden. De melder zal een coördinerende rol gaan spelen in de afhandeling van een beveiligingsincident of mogelijk datalek.

Standaardprocedure meldplicht datalekken: zes fases
In de afhandeling van een beveiligingsincident en mogelijk datalek kunnen zes fases worden onderscheiden. Deze fases zijn niet per se strikt van elkaar gescheiden en de volgorde staat – uitzonderingen daargelaten - evenmin vast. De fases zijn:

1. Ontdekken;
2. Inventariseren;
3. Kwalificeren;
4. Repareren;
5. Melden;
6. Archiveren.

1. Ontdekken
Iemand moet een beveiligingsincident en daarmee een mogelijk datalek op het spoor komen: de ontdekker. De ontdekker is waarschijnlijk goed in staat om een aantal relevante feiten aan de melder mee te delen. Dit is een belangrijk moment in afhandeling van het beveiligingsincident of mogelijk datalek. De ontdekker moet dan wel weten welke informatie er van hem of haar verlangd wordt. Welke feiten over het datalek aan melder gerapporteerd moeten worden, moet dus op voorhand vaststaan.

Daarmee wordt voorkomen dat de melder op een later moment voor ontbrekende informatie weer te rade moet gaan bij de ontdekker. De organisatie zal eveneens een modaliteit zoals een incidentenmeldingentool of een vast e-mailadres moeten voorschrijven. Zodat de meldingen op één centraal punt binnenkomen.

Het is voor de ontdekker doorgaans lastig om in te schatten of het door hem ontdekte beveiligingsincident een datalek is. Daarom is het aan te raden om een ruime marge te nemen en ieder beveiligingsincident door ontdekker als (mogelijk) datalek te laten rapporteren. Of er daadwerkelijk sprake is van een meldplichtig datalek, zal worden bepaald door de melder aan de hand van een beslissingsschema datalekken. In de bijlage van dit document is een voorbeeld gegeven voor een dergelijk beslissingsschema.

Het is wenselijk dat, voor zover mogelijk, de hierna genoemde informatie door de ontdekker wordt

verstrekt aan de melder. Dit kan worden aangevuld door de technicus en de melder zelf. De vraag over de verantwoordelijkheid moet bijvoorbeeld doorgaans door de melder worden beantwoord. Wanneer de organisatie bij alle incidenten een dergelijk formulier hanteert, ontstaat er uniformiteit in de afhandeling van een beveiligingsincident of mogelijk datalek. Het gaat om de volgende informatie:

- De samenvatting van het incident.
- Het aantal betrokkenen en van wie zijn de persoonsgegevens gelekt.
- Een omschrijving van de groep betrokkenen (klanten, medewerkers, etc.).
- Welke persoonsgegevens gelekt zijn (NAW-gegevens, IBAN, bijzondere of gevoelige gegevens, etc.).
- Of de eigen organisatie als verwerkingsverantwoordelijke of verwerker aan te merken is.
- Wanneer het datalek is ontstaan.
- Wat de oorzaak is van het datalek.
- Welke technische en/of organisatorische maatregelen er getroffen zijn om het datalek te dichten, en/of in de toekomst te kunnen voorkomen.

2. Inventariseren

Naast de gegevens die melder ontvangt van ontdekker, zal het in sommige gevallen nodig zijn om aanvullende informatie omtrent het datalek te verzamelen. Deze informatie is nodig om af te wegen of er wel of geen verplichting is tot het melden van het datalek bij de AP en eventueel bij de betrokkenen. Het grootste gedeelte van de nog ontbrekende informatie zal van technische aard zijn. De melder zal bij de technicus te rade moeten gaan voor deze informatie. Zoals hiervoor vermeld, is het dan ook aan te raden om het bovenstaande schema uit te zetten bij de technicus. Op die manier kan de technicus aanvullen waar relevant en/of noodzakelijk.

Wanneer contact gelegd wordt met de technicus in kwestie, zal deze direct de opdracht moeten krijgen om het beveiligingsincident/mogelijk datalek te (laten) repareren. De technicus zal de melder op de hoogte moeten houden van de ontwikkelingen hieromtrent.
De melder zal in het beheersysteem een nieuwe case aan moeten maken en alle informatie over het beveiligingsincident/datalek hierin moeten opnemen. Het schema is daarmee ook een goed uitgangspunt om zoveel mogelijk informatie direct tot je beschikking te hebben.

3. Kwalificeren

Wanneer de feiten zijn verzameld, kan de melder bepalen of het beveiligingsincident een datalek is en of het gemeld moet worden aan de AP en eventueel aan de betrokkenen. Dit gebeurt aan de hand van het beslissingsschema datalekken. De uitkomst van deze kwalificatie moet eveneens in het beheersysteem worden opgenomen. In de bijlage staat een voorbeeld van een dergelijk beslisschema.

4. Repareren

Onafhankelijk van de uitkomst van fase 3, zullen er maatregelen getroffen moeten worden om het beveiligingsincident/mogelijk datalek te dichten en ook eventueel te voorkomen in de toekomst. Dit gebeurt door de technicus. De technicus moet de melder op de hoogte houden van de vooruitgang. Dit kunnen initiële maatregelen zijn om de directe impact te kunnen beperken, zoals het tijdelijk blokkeren van een klantportaal wanneer er in het klantportaal gegevens zichtbaar zijn van een andere klant. Daarnaast moet er ook gewerkt worden aan structurele maatregelen zodat een dergelijk beveiligingsincident/mogelijk datalek onder gelijkblijvende omstandigheden zich in de toekomst niet nogmaals voordoet.

5. Melden

Indien het datalek onder de meldplicht valt, zal het moeten worden gemeld. De meldplicht is

tweeledig: naast dat gemeld moet worden aan de AP, moet onder voorwaarden ook aan de betrokkenen gemeld worden. De melder heeft reeds onder stap 3 bepaald of en aan wie gemeld moet worden. De melder is ook degene die belast is met het daadwerkelijk doen van de melding. Het afschrift van de gedane melding, het meldingsnummer en de ontvangstbevestiging moeten in het beheersysteem worden ondergebracht.

6. Archiveren
Wanneer de zaak is afgerond, moet het één en ander worden gearchiveerd. De meeste informatie is reeds in het beheersysteem ondergebracht.

Beheersysteem
Van belang is dat alle informatie over een beveiligingsincident en/of mogelijk datalek, op een centrale plek wordt vastgelegd. Bijvoorbeeld in wat hierboven steeds met de term beheersysteem is aangeduid (het meldingsregister).

Deze vastlegging dient twee doelen:
- De melder houdt overzicht over de lopende zaken. Er zijn nogal wat variabelen bij de afhandeling van een datalek. Zeker wanneer er mee dan één datalek tegelijk is, is het van belang om overzicht te kunnen houden.
- Incidenten die onder het begrip datalek vallen, dienen te worden gedocumenteerd. De AP mag de documentatie van datalekken opvragen om naleving van de privacyverordening te controleren.

Zoals reeds vermeld is, zijn de bovenstaande zes fases niet statisch. Sterker nog: het is heel belangrijk om de volgorde niet strikt te volgen. Het is een leidraad om weer te geven waar in ieder geval bij stil moet worden gestaan. De fases 1 tot en met 4 lopen eigenlijk meestal tegelijkertijd.

Bijlage: **voorbeeld beslisschema datalekken**