Link meldloket datalekken AP: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

Puntsgewijs crisisplan datalek SV Nucleus

Functionaris Gegevensbescherming 2020-2021: Joulyssa Wolff

Secretaris 2020-2021: Esmee van den Berg

Met expliciete dank aan Nick Tijsterman, Larissa Rosbach, Menno Sieval en Inge van Veen.

Processtappen	**Activiteit**	**Verantwoordelijke persoon**
1. Er wordt een (mogelijk) datalek ontdekt	- Maak direct intern melding van (mogelijke) datalek - Informeer de verantwoordelijke Contactpersoon	Medewerker die het ontdekt
2. Beoordeel het datalek	- Onderzoek het beveiligingsincident - Onderzoek of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden - Beoordeel wie of welke afdelingen binnen de organisatie hierbij betrokken zijn - Beoordeel of er een verwerker betrokken is bij het incident. Zo ja dan dient deze bij het proces betrokken te worden	Bestuurslid die contactpersoon is van commissie waar binnen het datalek heeft plaatsgevonden Functionaris Gegevensbescherming
3. Bestrijdt het datalek	- Stop het datalek als het nog kan - Neem andere maatregelen om het datalek en de daaruit voortvloeiende schade te beperken - Leg de acties van de genomen maatregelen vast in het dossier	Bestuurslid die contactpersoon is van commissie waar binnen het datalek heeft plaatsgevonden Functionaris Gegevensbescherming
4.Vaststellen impact datalek	- Onderzoek het datalek en de gevolgen daarvan - Onderzoek de aard van de gegevens die gelekt zijn. Bijv. gezondheidsgegevens, wachtwoorden, gegevens over financiële situatie of die kunnen leiden tot stigmatisering/misbruik - Onderzoek de omvang van de gelekte gegevens - Beoordeel welke impact het lek kan hebben op de betrokken personen - Stel vast wat de nadelige gevolgen kunnen zijn	Bestuurslid die contactpersoon is van commissie waar binnen het datalek heeft plaatsgevonden Functionaris Gegevensbescherming De overige bestuursleden
5. Vaststellen Meld en Herstelaanpak	- Bepaal aanpak/informeren AP - Bepaal aanpak/informeren betrokkenen - Bepaal acties voor nazorg betrokkenen - Bepaal acties voor belang van de organisatie - Bepaal acties voor verbetering beveiliging	Bestuurslid die contactpersoon is van commissie waar binnen het datalek heeft plaatsgevonden Functionaris Gegevensbescherming De overige bestuursleden
6. Melden AP*	- Indien besloten wordt om AP te informeren dan moet dat binnen 72 uur - Melding via de website van het AP	Bestuurslid die contactpersoon is van commissie waar binnen het datalek heeft plaatsgevonden Functionaris Gegevensbescherming

7. Melden betrokkenen**	- Melding via bijvoorbeeld brief - Meedelen wat er is gebeurd, welke persoonsgegevens getroffen zijn en wat de mogelijke gevolgen van het datalek kunnen zijn. - Informeren over de maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen	Secretaris Functionaris Gegevensbescherming Bestuurslid die contactpersoon is van commissie waar binnen het datalek heeft plaatsgevonden
8. Uitvoeren herstelwerkzaamheden	- Herstel het datalek - Verbeteren van de beveiliging - Lever nazorg aan de betrokkenen	Bestuur Commissie waar lek heeft plaatsgevonden
9. Optimaliseer het beveiligings- en het Datalek proces	- Registreer, evalueer en verbeter de beveiliging en het proces inzake melding datalekken	Bestuur Commissie waar lek heeft plaatsgevonden

* Melding aan de Autoriteit persoonsgegevens kan alleen achterwege blijven indien het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Of hiervan sprake is hangt mede af van de aard en omvang van de gelekte persoonsgegevens. Indien bijvoorbeeld uitsluitend de adresgegevens zijn gelekt van een kleine groep betrokkenen, dan is het onwaarschijnlijk dat er sprake is van een hoog risico. Dat is wellicht anders indien de adresgegevens in combinatie met het lidmaatschap van de patiënten of cliëntenorganisatie zijn gelekt. Het lidmaatschap van de organisatie kan gezien worden als een gevoelig gegeven en de leden van de organisatie kunnen wellicht behoren tot een kwetsbare groep, die extra bescherming nodig heeft. Bij de afweging van het risico voor de rechten en vrijheden van de betrokkenen zal altijd de Functionaris Gegevensbescherming betrokken moeten worden.

** Indien het datalek waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen veroorzaakt, moet het datalek ook aan de betrokkenen gemeld worden. Het risico zal bijvoorbeeld moeten worden beoordeeld aan de hand van de aard en de hoeveelheid van de gelekte gegevens. Als er persoonsgegevens van gevoelige aard (bijv. gezondheidsgegevens) gelekt zijn, zal het lek in ieder geval gemeld moeten worden aan de betrokkenen. Bij de afweging van het risico voor de rechten en vrijheden van de betrokkenen zal altijd de Functionaris Gegevensbescherming betrokken moeten worden.

Uitgebreid crisisplan datalek SV Nucleus

Stap 1: Inventariseer & beperk

Op het moment dat een (mogelijk) datalek u ter ore komt, is het belangrijk om inzicht te krijgen in de aard en omvang van het incident. Vragen die in deze fase centraal staan zijn: wat is de aard van de gegevens waarop inbreuk is gemaakt, is er sprake van verlies of onrechtmatige verwerking van deze gegevens en kunnen de primaire bedrijfsprocessen normaal doorgang vinden?
In veel gevallen is het raadzaam om bij een online datalek meteen technische en procedurele maatregelen te treffen om het huidige lek zo snel mogelijk te stoppen. Dit kan betekenen dat uw internetkoppelingen en digitale dienstverlening moeten worden stilgelegd (ook al blijkt dit wellicht achteraf een te zwaar middel te zijn geweest).
Neem in deze inventarisatiefase tevens mee welke mogelijkheden er zijn voor verder onderzoek. Denk hierbij aan het veiligstellen van specifieke logbestanden of systemen voor verder onderzoek.
Een belangrijk juridisch aspect is of u de verantwoordelijke of 'slechts' de bewerker van de data bent. In de bewerkersovereenkomst is vaak vastgelegd dat de bewerker een bepaalde tijd heeft om het datalek bij de verantwoordelijke te melden. De tijd die de bewerker nodig heeft om onderzoek te doen en het lek te melden bij de verantwoordelijke wordt ook van de 72 uur afgetrokken die de verantwoordelijke heeft om het lek bij de Autoriteit Persoonsgegevens te melden.
De korte responstijd vraagt bij een dergelijk incident tot snelle actie. Het is daarom van belang dat op voorhand een incident response plan en crisisplan gedefinieerd zijn en dat deze plannen worden gevolgd (zodat relevante personen en procedures niet ten tijde van het datalek geïdentificeerd hoeven te worden). Zorg er ook zo snel mogelijk voor dat technische en juridische expertise (intern of extern) beschikbaar zijn om met spoed ondersteuning te leveren indien nodig.

Stap 2: Consulteer & onderzoek

Nadat u de eerste acties heeft uitgezet is het zaak om met uw in- en externe cyber- en forensisch specialisten, juristen en verzekeringsadviseur in gesprek te gaan. Welke impact heeft het datalek, wat zijn de benodigde juridische en onderzoek-stappen en wat zijn de langetermijnoplossingen om herhaling te voorkomen?
Zorg er vervolgens voor dat u, voor zover mogelijk, de details van het lek onderzoekt. Is het bijvoorbeeld mogelijk om op basis van de beschikbare sporen vast te stellen welke gegevens naar welke partijen zijn gelekt en door wie? Voer om symptoombestrijding te voorkomen een 'root cause'-analyse uit om de oorzaak van het incident vast te stellen.
Ook als blijkt dat zaken maar beperkt aangetoond kunnen worden, wilt u hiervan op de hoogte zijn. Dit vormt namelijk belangrijke input voor juridische en communicatieve vervolgstappen en ook voor de bepaling van technische organisatorische maatregelen ter voorkoming van soortgelijke incidenten in de toekomst.

Stap 3: Communiceer

Zorg dat in uw incident response plan procedureel vastgelegd is wanneer en door wie de melding aan de Autoriteit Persoonsgegevens is gedaan. Er geldt een meldingsplicht wanneer het datalek gevoelige persoonsgegevens betreft of tot nadelige gevolgen voor de betrokkenen kan leiden. Afhankelijk van de ernst van de zaak en de gevolgen voor de betrokkenen dient ook melding aan de betrokkenen zelf plaats te vinden. Consulteer uw functionaris gegevensbescherming indien u van uw incident response plan afwijkt.
Daarnaast is het van belang om te bepalen of bredere communicatie wenselijk is, denk bijvoorbeeld aan een persbericht. Dit kan helpen om zelf de regie te houden over het beeld dat de buitenwereld van uw organisatie en het onderhavige incident heeft.

Stap 4: Verbeter & leer

Wanneer de eerste maatregelen ter beperking van het incident met succes zijn genomen, en het incident is onderzocht, is het tijd om de focus op de lange termijn te leggen.
Denk na over aanvullende technische maatregelen zoals monitoring of verscherpte toegangsbeveiliging om herhaling te voorkomen. Denk ook na over aanvullende organisatorische maatregelen zoals gedragsprogramma's, trainingen en aangepaste procedures om bewustwording van medewerkers naar een hoger niveau te tillen.
Ten slotte, gebruik het incident ook om de werking van het incident response plan te toetsen en waar nodig aan te scherpen.
Hierboven is één van de scenario's geschetst betreffende de wijze waarop onze 'cyber response'-specialisten op dagelijkse basis klanten bijstaan in het samenspel met verzekeraars, advocaten en toezichthouders, met als doel de organisatie zo spoedig mogelijk van crisis terug naar 'business as usual' te begeleiden. Hierbij helpen zij klanten zowel om de organisatie zo optimaal mogelijk voor te bereiden op het moment dat de alarmbellen afgaan, als gedurende het moment van de alarmbellen zelf.

Bron: geraadpleegd 5-3-19
https://home.kpmg/nl/nl/home/social/2017/08/een-mogelijk-datalek-welke-stappen-moet-ik-nemen.html