Procedure Meldplicht Datalekken

1 Inleiding

De procedure zoals hieronder wordt beschreven is pragmatisch van aard. Het doel is om, indien een informatiebeveiligingsincident of datalek zich voordoet, deze te registreren, te volgen, vast te stellen of het een data-lek is, deze te isoleren, en te herstellen zodat er weer sprake is van een normale werkbare situatie.

1.1 Achtergrond

De meldplicht datalekken, welke actief (verplicht) is geworden op 01-01-2016, is opgenomen in de Wet bescherming persoonsgegevens en brengt wettelijke verplichtingen met zich mee wanneer er zich informatiebeveiligingsincidenten voordoen die de beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens in gevaar brengen. Denk hierbij ongeautoriseerde wijzigingen van persoonsgegevens of het kwijtraken van persoonsgegevens zonder een back-up.

1.2 Wettelijk kader

De wet vereist dat de organisatie ernstige datalekken onverwijld meldt aan de Autoriteit Persoonsgegevens (AP). In de praktijk betekent dit: binnen 2 werkdagen na constatering. Daarnaast geldt als eis dat alle betrokkenen (lees: de burger of burgers) worden geïnformeerd wanneer een datalek voor hem/haar (waarschijnlijk) ongunstige gevolgen heeft. Het is dus niet zo dat elk datalek moet worden gemeld, maar dat voor ieder datalek wel een deugdelijke afweging nodig is in de vorm van een privacy impactanalyse (PIA). Zo kan het dus gebeuren dat een datalek wel moet worden gemeld aan het AP, maar niet aan betrokkenen, omdat hun persoonsgegevens onbegrijpelijk (door versleuteling) of ontoegankelijk zijn voor degenen die geen recht hebben op inzage in deze gegevens.

1.3 Uitbesteding

Tenzij er andere afspraken zijn gemaakt omtrent het eigenaarschap van data bij uitbesteding van werkprocessen, blijft Werkplein Fivelingo verantwoordelijk voor het melden van een datalek. Met alle bewerkers worden afspraken gemaakt over de gestelde eisen op het gebied van informatiebeveiliging en over het onmiddellijk melden van beveiligingsproblemen aan de security officer van Werkplein Fivelingo.

1.4 Achtergrond in de BIG

Het beheer van informatiebeveiligingsincidenten is naast bewustwording en business continuïteit een van de belangrijkste aandachtsgebieden die onder de baseline informatiebeveiliging (BIG) valt.

1.5 Gevolgen bij onjuist handelen in geval van datalek

Indien Werkplein Fivelingo verzuimt of tekortschiet kan de directeur en het bestuur hoofdelijk aansprakelijk worden gesteld in het geval van een datalek. De hoogte van de boete bedraagt €820.000.

2. Procedure

2.1 Inleiding

Elke medewerker moet alert zijn op bedreigingen met betrekking tot informatiebeveiliging en is verplicht om elk beveiligingsincident dat hij/zij ontdekt of vermoedt te melden.

Voorbeelden van beveiligingsincidenten zijn:

- Verlies of diefstal van waardepapier (paspoorten, rijbewijzen), dossier, usb-stick, tablet of andere gegevensdragers
- Niet naleven van beleid of richtlijnen
- Inbreuk op fysieke beveiligingsvoorzieningen
- Toegangsovertredingen
- Opzettelijk foutief handelen (fraude, diefstal)
- Beschadigen of vernielen van (kritische) apparatuur
- Virusbesmetting als gevolg van het aanklikken van een onbetrouwbare bijlage
- Onbevoegd inzien van vertrouwelijke informatie
- Onbedoelde openbaarmaking van vertrouwelijke informatie
- Geen gescreend personeel
- Illegale licenties
- Illegaal kopiëren van gegevens
- Email met onversleutelde vertrouwelijke informatie
- Kenbaar maken van of onzorgvuldig omgaan met wachtwoorden

Maar ook cyberaanvallen zoals een ddos, computerhacking of besmetting met ransomware, of het technische falen van apparatuur, stroomuitval, wateroverlast en dergelijke zijn aan te merken als incidenten.

Voorbeelden datalekken zijn

- een kwijtgeraakte USB-stick met persoonsgegevens,
- een gestolen laptop of
- een inbraak in een databestand door een hacker.

Het proces om datalekken te melden bestaat uit een aantal te doorlopen processtappen die voor elk incident gelijk zijn. De verschillen zitten voornamelijk in de details (inhoud).

2.2 Meld intern en prioriteer

De Security Officer registreert alle incidentmeldingen en de omvang ervan ten behoeve van rapportagedoeleinden.

2.3 Mobiliseer Incidententeam

Voor deze procedure wordt voorgesteld om een lid van het MT, een ICT-medewerker/lid van de hostende partij en de Security Officer de vaste kern van het datateam te laten zijn. Indien het incidententeam wordt gemobiliseerd moeten de leden van dit team zich initieel zodanig vrijmaken dat zij zich volledig op deze werkzaamheden kunnen richten. In overleg met de Security Officer kan de inzet van het team na verloop van tijd weer afgeschaald worden.

De vaste kern van het incidententeam wordt gemobiliseerd als:

1. een incident is afgegeven met een hoge of kritische impact

2. een dergelijke melding rechtstreeks bij een van de vaste leden binnenkomt.
3. de hostende partij een technisch incident zelf heeft opgepakt en technisch afhandelt.

De vaste kern van het incidententeam beoordeelt direct (in geval van punt 3 gelijktijdig of achteraf) de aard en omvang van het incident en stelt vast of het incident ook daadwerkelijk heeft plaatsgevonden, bijvoorbeeld door contact op te nemen met systeembeheer of de melder van het incident. Daarbij maakt de vaste kern van het incidententeam gebruik van een checklist (zie bijlage) om snel inzicht te krijgen in:

- de aard en omvang van het incident,
- welke teamleden aanvullend opgenomen moeten worden in het incidententeam en
- welke instanties geïnformeerd moeten worden over het incident (IBD, CBP, AP etc). (datalekken dienen binnen 2 dagen te worden gemeld)

In deze fase bepaalt het incidententeam (met inhoudelijke ondersteuning van de Security Officer) of de organisatie moet melden aan alleen het AP/CBP of aan het AP/CBP en de betrokkenen. Indien nodig vraagt men advies bij de afdeling juridische zaken of bij een externe adviseur die gespecialiseerd is in privacywetgeving. In essentie wordt bepaald of er op enige manier een risico is ontstaan voor de verwerking van persoonsgegevens.

2.3.1 Gevolgen voor eigen organisatie

De Security Officer bepaalt samen met de andere leden van het incidententeam wat de gevolgen zijn voor Werkplein Fivelingo. Hiermee wordt bedoeld: welke vervolgacties zijn noodzakelijk om het datalek volgens de eisen van de meldplicht datalekken af te handelen. Een datalek kan leiden tot reputatieschade en mogelijk schadeclaims indien het lek verwijtbaar is en betrokkenen schade hebben geleden. Immers Werkplein Fivelingo is verplicht te melden aan betrokkenen en dit kan leiden tot lokale en mogelijk landelijke bekendheid.

Werkplein Fivelingo moet inzicht krijgen:

- of wel of niet gemeld moet worden aan alleen CBP of CBP en betrokkenen,
- in de juridische gevolgen voor schadeclaims of boetes,
- in de te verwachten kosten en dekking van deze kosten (denk aan verzekeringspolissen of
- indienen van schadeclaims indien een bewerker de schade heeft veroorzaakt).
- in de afhandeling (nazorg) van een datalek naar betrokkenen,
- in de communicatie-aanpak om reputatieschade zo beperkt mogelijk te houden.

Het incidententeam is belast met het beperken van verdere schade als gevolg van het incident, het blokkeren of verwijderen van de oorzaak, het vaststellen van de schade en de zorg voor het veiligstellen van bewijsmateriaal. Van elk incident dat via het incidententeam loopt vindt dossiervorming plaats.

Het incidententeam bepaalt welke acties noodzakelijk zijn en neemt bij twijfel contact op voor advies met de helpdesk van het IBD. Voor elk te behandelen incident via het incidententeam geldt dat teamleden hierover niet mogen praten met anderen buiten het team totdat daarvoor toestemming is gegeven door de Security Officer. Dit om zoveel mogelijk ruis in de communicatie te voorkomen.

De security officer onderhoudt het contact met de directeur en het bestuur van Werkplein Fivelingo over de stand van zaken betreffende het incident.

2.4 Beperk schade en elimineer oorzaak

Er wordt zo snel mogelijk gestart met het indammen van de schade door het incident te blokkeren, te verwijderen en de impact voor verdere blootstelling te verminderen. Dit kunnen zowel activiteiten zijn vanuit de techniek als vanuit de organisatie.

Het incidententeam bepaalt in samenspraak met het verantwoordelijke afdelingshoofd en de afdeling communicatie de (interne en externe) communicatiestrategie die de afdeling communicatie verder uitwerkt.

Voor het veiligstellen en verzamelen van bewijslast kan eventueel externe expertise nodig zijn.

Indien sprake is van (mogelijke) inbreuk op de beveiliging van persoonsgegevens behoort een ernstig datalek onverwijld te worden gemeld bij het AP/CBP en eventueel aan betrokkenen. De Security Officer ziet er op toe dat dit traject conform de daarvoor geldende procedure wordt afgehandeld.
Het incidententeam bepaalt aan de hand van de aard van het incident en in overleg met de juridische afdeling of aangifte bij de politie gedaan moet worden (strafrechtelijk onderzoek).

2.5 Herstel oude situatie

Na het indammen van de schade en het verwijderen van het incident is zo spoedig mogelijk herstel naar de oude situatie nodig. Bij bedrijfsprocessen die (deels) gestopt zijn als gevolg van een incident vindt op een gecontroleerde wijze een herstart plaats. Eventueel verlies van data wordt gereconstrueerd bijvoorbeeld aan de hand van een recovery procedure en/of brondocumenten (opnieuw invoeren). Het herstarten van een bedrijfsproces geschiedt in nauw overleg met het verantwoordelijke afdelingshoofd.

In overleg met het verantwoordelijke afdelingshoofd vindt communicatie naar de organisatie plaats over het herstel en eventuele gevolgen ervan.

In geval een medewerker van Werkplein Fivelingo betrokken is bij de oorzaak van een beveiligingsincident door nalatig of kwaadwillend gedrag en daarvoor het nodige bewijsmateriaal is veiliggesteld, wordt een medewerker van P & O ingeschakeld en eventueel aangifte gedaan bij de politie en/of te handelen conform de sancties paragraaf zoals beschreven in het "beleid bij oneigenlijk gebruik en misbruik van persoonsgegevens'. De gevolgen hiervan voor de betrokken medewerker kunnen leiden tot disciplinaire maatregelen, strafrechtelijk onderzoek en/of tot ontslag. Voor betrokkenheid van een externe medewerker geldt eenzelfde procedure.

Afbeelding 1: Processchema melding datalekken