Vereniging Beveiligingsprofessionals Nederland

Meldplicht Datalekken

Vereniging Beveiligingsprofessionals Nederland

Versie	: 0.2 concept
Auteur	: Peter Meijer
Datum	: december 2017

Inleiding

Dit document beschrijft de verschillende stappen die binnen de VBN genomen worden bij een datalek die valt onder de Meldplicht Datalekken. De Meldplicht Datalekken is een wijziging van de Wet Bescherming Persoonsgegevens en is in werking getreden met ingang van 1 januari 2016. Bij een datalek is er sprake van een inbreuk op de beveiliging van persoonsgegevens (zie bijlage I). De persoonsgegevens zijn dan blootgesteld aan verlies of onrechtmatige verwerking.

Datalekken kunnen ontstaan door:
- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, malware besmetting)
- technisch falen (ICT-storingen)
- menselijk falen (te eenvoudige wachtwoorden/het verstrekken van username/wachtwoord aan collega's en externen)
- calamiteit (brand datacentrum, wateroverlast)
- verloren USB stick of laptop
- verzenden van email met emailadressen van alle geadresseerde
- maar ook het onrechtmatige verwerking van gegevens

Het doel van dit protocol is drieledig:
1) het creëren van een laagdrempelig meldpunt voor betrokkenen
2) het structureel en volgens een vast format registreren en beoordelen van incidenten
3) het periodiek rapporteren aan het bestuur

Melden

Alle datalekken van persoonsgegevens moeten intern worden gemeld en worden gedocumenteerd. Bij de VBN zijn deze werkzaamheden belegd bij de penningmeester. De melding kan door iedere medewerker, lid en bestuurder worden gedaan. De melding kan ook door een externe persoon worden gedaan bij een bestuurder van de VBN. De melding moet direct en telefonisch worden gedaan bij de penningmeester van de VBN. De melding wordt door de penningmeester direct digitaal vastgelegd. Alle wijzigingen en mutaties tijdens het proces worden door de penningmeester, met vermelding van datum en tijdstip, digitaal vastgelegd.

Ten behoeve van de melding legt de penningmeester de volgende gegevens vast:
- naam van de melder
- datum en tijdstip van de melding
- aard van de melding

De melding wordt per omgaande doorgegeven aan de penningmeester. Deze neemt contact op met de melder en vult de gegevens aan:
- aard van de inbreuk
- welke persoonsgegevens vallen onder de melding
- om welke aantal en/of gegevensrecords gaat het
- welke gegevensrecords betreft het (programma/software)
- welke (groepen) personen zijn betrokken bij de melding
- welke maatregelen zijn of worden door de melder getroffen
- welke gevolgen zijn er volgens de melder voor de betrokkenen
- de contactpersoon voor de melding

Eerste analyse

Voor de beoordeling van het incident maakt de penningmeester gebruik van het document *'Beleidsregels Meldplicht Datalekken'* van de Autoriteit Persoonsgegevens (AP). De penningmeester beoordeelt of van de inbreuk 'redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking, waaraan nadelige gevolgen voor de privacy van de betrokkenen zijn verbonden'. Is dit niet het geval, dan vindt alleen registratie van de melding plaats. Is dit wel het geval, dan voert de penningmeester de volgende acties uit:

1. telefonisch informeren van het bestuur;
2. (telefonisch) informeren evt. direct betrokkenen (nader te bepalen binnen VBN);
3. tijdens kantooruren:
- direct telefonisch overleg met het bestuur
- buiten kantoortijden en in het weekend wordt de melding gedaan bij de penningmeester

Bij het niet kunnen bereiken van de penningmeester, wordt de melding gedaan bij de secretaris. Als het mogelijk is wordt een eventueel gewenst overleg uitgesteld tot tijdens kantooruren. Als dit niet mogelijk is wordt zoveel als mogelijk telefonisch en elektronisch overleg gevoerd.

Dagelijks Bestuur / Incident Response Team - IRT

Het IRT wordt bijeengeroepen door de penningmeester of secretaris. Het IRT bespreekt en legt vast:

- de gegevens die door de penningmeester of zijn vervanger zijn vastgelegd bij het aannemen van de melding
- de noodzakelijke vervolgacties m.b.t. het datalek (lek onmiddellijk dichten, toegang tot informatie beperken en tegelijkertijd meer informatie vergaren over de indringer)
- hetgeen gemeld gaat worden bij het AP door de penningmeester (naast aard inbreuk, welke persoonsgegevens, aantal betrokken personen/records)
  - de mogelijke gevolgen voor de betrokkenen
  - de maatregelen die de VBN neemt en/of kan nemen om de schade voor betrokkenen te verkleinen;
  - de maatregelen die betrokkenen kunnen nemen om verdere schade te verkleinen, inclusief de wijze van inlichten hierover
  - contactgegevens voor betrokkenen
- de wijze van afhandeling intern, inclusief communicatie naar melder
- of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden, zoals uit hoofde van wanprestatie (omdat een geheimhoudingsverplichting is geschonden, of in strijd met een contractuele verplichting onvoldoende beveiliging is gerealiseerd) of onrechtmatige daad
- het al dan niet doen van aangifte en vaststellen of sprake is van strafrechtelijke verwijtbaarheid. Dit kan bijvoorbeeld spelen wanneer er sprake is van betrokkenheid vanuit de VBN zelf, een bewerker, of wanneer er onvoldoende maatregelen zijn getroffen om ongeregeldheden te voorkomen. Indien gewenst vindt overleg plaats met de juridisch adviseur
- hetgeen intern gecommuniceerd wordt, op welk moment
- hetgeen extern gecommuniceerd wordt, op welk moment. Er wordt vastgesteld of de pers geïnformeerd moet worden
- of naast het AP ook andere stakeholders geïnformeerd worden
- of er individuen, bedrijven, ketenpartners of andere derden geïnformeerd worden
- op welke wijze er intern wordt gerapporteerd, inclusief actiehouder
- of eventuele schade is gedekt door de verzekeringspolis

Vervolg

De penningmeester rapporteert aan het bestuur de uitkomsten van het overleg, alsmede een actielijst van het IRT. Het bestuur accordeert de uit te voeren activiteiten, zoals vastgesteld door het IRT, of stelt de uit te voeren activiteiten bij. De door het bestuur vastgestelde activiteiten worden uitgevoerd door de penningmeester.

Melding bij de AP

De penningmeester meldt binnen 2 dagen (48 uur. Wettelijk binnen 72 uur) na ontdekking van het incident volgens de aangewezen methode het datalek bij het AP (webformulier AP). In ieder geval zal gemeld worden:

- aard van de inbreuk, waaronder betrokken categorieën, aantal betrokkenen, aantal gegevensrecords
- beschrijving van de te verwachten gevolgen
- getroffen en/of voorgestelde maatregelen
- informatie over te nemen maatregelen door de betrokkene om de nadelige gevolgen te beperken
- contactgegevens voor betrokkene

Ontvangstbevestiging AP

Is er een melding gedaan, dan ontvangt de VBN een ontvangstbevestiging. Bij de meldingen die aanleiding geven tot nadere actie door de AP, zal de AP contact opnemen met de VBN om de herkomst van de melding te verifiëren.

Bijlagen

I - Stroomschema ontdekking incident

Bijlage I – Stroomschema *ontdekking incident*