Procedure voor het afhandelen van datalekken

3 februari 2016

Wie een mogelijk datalek ontdekt, zal snel onderzoek moeten doen en mogelijk ook meldingen moeten doen aan de overheid en getroffen personen.

Medewerkers van de Universiteit Twente moeten het datalek zo snel mogelijk melden via cert@utwente.nl of Servicedesk ICT (LISA) servicedesk-ict@utwente.nl tel. 5577.

Medewerkers van de ICT Servicedesk zijn ook alert op mogelijke datalekken zoals: verlies van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker en melden beveiligingslekken via e-mail aan cert@utwente.nl. In urgente gevallen wordt de dienstdoende CERT-UT medewerker gebeld.

CERT-UT registreert iedere melding in het AIRT (Application for Computer Security Incident Response) systeem. Dit is een workflow applicatie waarmee CERT-UT de beveiligingsinbreuken en incidenten bijhoudt. CERT-UT neemt daarna contact op met de melder voor aanvullende gegevens over de melding.

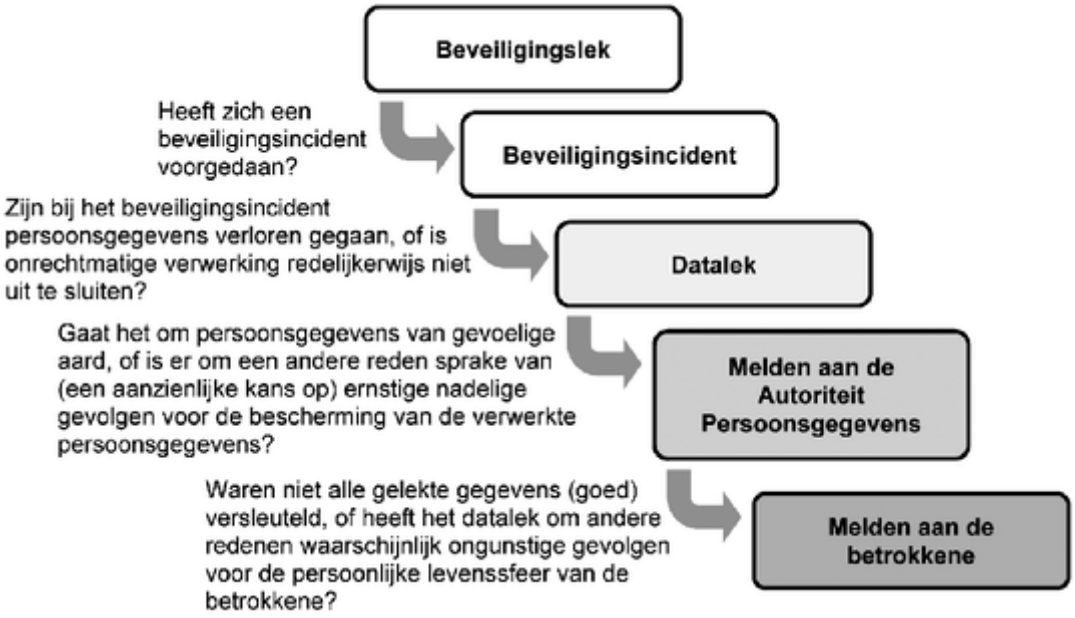
Door de dienstdoende CERT-UT medewerker wordt een eerste analyse gedaan. Als het om persoonsgegevens gaat, dan wordt het incident bij de Security manager (LISA), Functionaris Gegevensbescherming (FG) en Privacy Contactpersoon (PCP) van de eenheid gemeld. Het security incident krijgt een typeaanduiding zodat het herkenbaar is als privacy incident. CERT-UT verzorgt de afhandeling van het security incident, waarbij bewijsmateriaal of informatie voor het afhandelen van het datalek in een veilige omgeving wordt bewaard. De Security manager zorgt voor afhandeling van het privacy incident.

De security manager (LISA) maakt samen met de FG en de PCP een afweging of het incident gemeld moet worden aan de Autoriteit Persoonsgegevens, en eventueel daarnaast ook aan de betrokkene. Indien de conclusie is dat het incident moet worden gemeld aan de Autoriteit Persoonsgegevens (AP) dan wordt door de security manager eerst contact opgenomen met de secretaris van de universiteit alvorens de melding te doen.

Meldingen bij de AP worden gedaan door de security manager (LISA), waarbij tegelijk de status in AIRT wordt aangepast. Het zo nodig informeren van de betrokken personen wordt gedaan door de PCP.

Wanneer melden?

Voor een gedetailleerde beschrijving van de afweging of een melding gedaan moet worden zie Beleidsregels van de Autoriteit Persoonsgegevens. Het onderstaande schema geeft in het kort deze afwegingen weer.



Datalek

Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Een voorbeeld van een beveiligingsincident is het kwijtraken van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker.

Maar niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als onrechtmatige verwerking van de persoonsgegevens redelijkerwijs niet kan worden uitgesloten.

Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. Daarvoor geldt geen meldingsplicht aan de Autoriteit Persoonsgegevens.

Melden aan de Autoriteit Persoonsgegevens

Niet ieder datalek hoeft te worden gemeld aan de Autoriteit Persoonsgegevens. Volgens de wet moet een melding gedaan worden aan de Autoriteit Persoonsgegevens als het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

De Wet Bescherming Persoonsgegevens gebruikt een brede definitie van persoonsgegevens. Elk gegeven dat herleidbaar is tot een natuurlijk persoon, is een persoonsgegeven. Dit betreft namen, adressen, kentekens, telefoonnummers, IP-nummers, email-adressen, biometrische kenmerken, een combinaties van specifieke voorkeuren.

Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is over het algemeen een melding noodzakelijk. Persoonsgegevens van gevoelige aard zijn bijvoorbeeld:

Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp
Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

Gegevens over de financiële of economische situatie van de betrokkene
Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.

(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.

Gebruikersnamen, wachtwoorden en andere inloggegevens
De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.

Gegevens die kunnen worden misbruikt voor (identiteits)fraude
Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn).

Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie er persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. Maar let op: als de aard van de gelekte gegevens daar aanleiding toe geeft is het zelfs mogelijk dat een datalek moet worden gemeld waarbij de persoonsgegevens van slechts één persoon betrokken zijn.

De melding moet worden gedaan zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek. Op de website van de Autoriteit Persoonsgegevens is voor dit doel een webformulier beschikbaar. Via dit webformulier kan de melding later nog worden aangevuld of ingetrokken.

Melden aan betrokkenen

Als een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens, dan betekent dit niet automatisch dat dit datalek ook moet worden gemeld aan de betrokkene. De wet geeft hiervoor als richtlijn dat het datalek moet worden gemeld aan de betrokkene als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

De wet schrijft voor dat de melding aan de betrokkene onverwijld moet worden gedaan, zodat de betrokkene naar aanleiding van de melding maatregelen kan nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder de betrokkene daarover geïnformeerd is, hoe eerder deze in actie kan komen.

Als er passende technische beschermingsmaatregelen zijn genomen (zoals encryptie en hashing), waardoor de persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kan de melding aan de betrokkene achterwege blijven.

Vervolgstappen

Zodra de melding aan de Autoriteit Persoonsgegevens en aan de betrokkenen is gedaan, is voldaan aan de meldplicht en zal de security manager het privacy incident afsluiten.

Indien nodig zal CERT-UT verder onderzoek te doen naar oorzaken en om de beveiliging aan te scherpen. Pas als dit afgehandeld is zal CERT-UT het security incident afsluiten.

Security managers houden een register bij van alle gemelde datalekken en de actuele status daarvan.

Rapportage

Rapportage over datalekken wordt meegenomen in de securitykwartaalrapportage die maandelijks door de Security manager van LISA wordt opgesteld.