OPENBAAR ONDERWIJS GRONINGEN

Detectie van beveiligingsincidenten en datalekken

Arnold van den Akker - 1 juli 2016

Bij het gebruiken en beheren van informatie kan van alles misgaan. Alle manieren waarop informatie kwijt kan raken of een onbevoegd iemand de informatie kan inzien, kopiëren, of aanpassen noemen we een **beveiligingslek**. Onze beveiliging is daar niet goed genoeg.

Eigenlijk kennen we twee hoofdcategorieën voor beveiligingslekken:

- Onvolkomenheden in de de manier waarop we omgaan met de techniek waarmee we informatie gebruiken (denk bv. aan applicaties, netwerken, usb-sticks, laptops).
  Voorbeelden zijn het doorgeven/verliezen van accountnamen met wachtwoorden aan onbevoegden, laptops waarop vertrouwelijke gegevens staan ergens onbeheerd zonder toegangsbeveiliging achterlaten of slordig omgaan met een USB-stick met gegevens
- Onvolkomenheden in de manier waarop we die techniek inrichten en beheren.
  Voorbeelden hiervan zijn 'gaten' in de beveiliging van het netwerk (bv. een open poort, of een verouderde virusscanner), beheerdersaccounts met een onveilig wachtwoord, onjuiste autorisatieprofielen gebruiken in applicaties.

Met een beveiligingslek hoeft het niet mis te gaan, het gaat zelfs verbazingwekkend vaak goed. Maar de dreiging dat het mis gaat bestaat. Afhankelijk van het risico en van onze eigen regels en wetgeving moeten we beveiligingslekken 'dichten'.

Bij een beveiligingsincident is er niet uitsluitend sprake van een dreiging van verlies van gegevens of onrechtmatige toegang tot gegevens, of van een tekortkoming in de beveiliging (ook wel aangeduid als een beveiligingslek), maar heeft is een dreiging werkelijkheid geworden of is er door iemand binnen of buiten de organisatie gebruik gemaakt van een beveiligingslek. Daarbij maakt het niet uit of er iets mis is gegaan met gegevens. Wanneer we niet kunnen uitsluiten dat gegevens zijn ingezien, gekopieerd of gewijzigd is er sprake van een beveiligingsincident. Onze gegevens warden immer niet veilig genoeg.

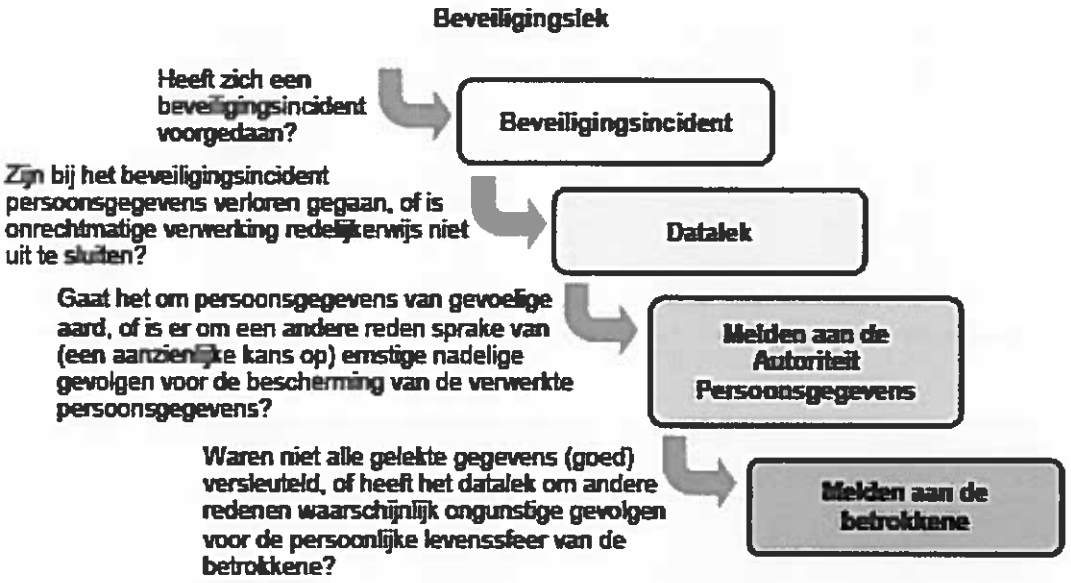
Bij beveiligingsincidenten kan je bijvoorbeeld denken aan:

- een kwijtgeraakte USB-stick of een gestolen laptop;
- een inbraak door een hacker;
- het openbaar worden van inloggegevens op een applicatie of dataopslag
- een malware-besmetting;
- een calamiteit zoals een brand in een datacentrum.

Wanneer hierdoor persoonsgebonden gegevens verloren zijn gegaan of beschikbaar zijn gekomen voor onbevoegden noemen we dit een **datalek**. Persoonsgebonden gegevens zijn alle gegevens die eenduidig tot iemand zijn terug te leiden. Een lijst met alle BSN van examenleerlingen en hun uitslagen van een examen zijn dus persoonsgegevens, ook zonder vermelding van hun namen.

Beveiligingslekken en beveiligingsincidenten willen we natuurlijk zoveel mogelijk voorkomen en , wanneer ze onverhoopt toch optreden, zo snel mogelijk verhelpen. Maar wanneer er persoonsgegevens in gevaar gekomen zijn, en er dus sprake is van een datalek, treed de wetgeving op de privacy in werking. Dat betekent dat we naast onze eigen afhandeling sommige datalekken ook moeten melden bij de nationale 'Autoriteit Persoonsgegevens' en/of bij de personen waar de gegevens betrekking op hebben.

In een schema weergegeven ziet dat er als volgt uit



Bij elke storing of andere incidentmelding moet dus worden beoordeeld of dit een beveiliginsincident betreft. Zo ja, dan moet niet alleen het incident worden verholpen, maat ook het beveiligingslek dat heeft geleid toe het incident gedicht. Wanneer er een beveiligingsincident heeft plaats gevonden moeten we ook bepalen of er sprake is van een datalek. Dit om ook de wettelijke eisen goed af te handelen.

Om te beoordelen of een incident een beveiligingsincident is (en eventueel zelfs een datalek), gebruik je de beslisboom op de volgende pagina.

Heeft het incident te maken met:
- het verlies van gegevens/informatie
  (bijvoorbeeld bestand verwijderd dat nog nodig is ,
- toegang van onbevoegden tot informatie en/of systemen van O2G2
  (bijvoorbeeld een inbraak van een hacker, openbaar worden accountgegevens, teveel rechten toegekend)
- verstoring van de informatievoorziening door oorzaken van buiten invloed van de organisatie
  (bv een virusaanval, malware, kabelbreuk internetaansluiting, brand in datacenter)

→ Neen → Er is GEEN sprake van een beveiligingsincident.
Handel het incident af zoals past bij de aard van het incident.

→ Ja

Er is **WEL** sprake van een beveiligingsincident.
Het incident moet zoveel mogelijk worden verholpen.
Daarnaast moet het incident voldoende worden geanalyseerd zodat maatregelen kunnen worden genomen om herhaling te voorkomen.

→

Is er informatie verloren gegaan of beschikbaar gekomen voor onbevoegden
EN
bevat deze informatie persoonsgebonden gegevens ?

Persoonsgebonden gegevens zijn gegevens die herleidbaar zijn tot een persoon. Denk hierbij aan namen, emailadressen etc. Maar ook zonder de bijbehorende naam verwijzen een adres met een geboortedatum of een BSN naar één bepaald persoon. Dit zijn dus ook persoonsgegevens.

→ Neen → Er is GEEN sprake van een datalek.

→ Ja

Er is **WEL** sprake van een datalek
Elk datalek moet worden gemeld bij de bestuurssecretaris van O2G2
(Functionaris Gegevensbescherming).
Hij zorgt voor verdere afhandeling, inclusief een eventuele melding bij de betrokkenen

→

Bevatten de betreffende persoonsgebonden gegevens gevoelige gegevens?
Gevoelige persoonsgegevens zijn:
- *Bijzondere persoonsgegevens zoals bedoeld in artikel 16 WBP (dit zijn bijvoorbeeld gegevens betreffende religie, levensovertuiging, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van vakvereniging, strafrechtelijke gegevens en of gegevens over onrechtmatig of hinderlijk gedrag)*
- *Gegevens over de financiële of economische situatie van de betrokkene (dit zijn gegevens over bijvoorbeeld salaris, schulden, betalingsgegevens)*
- *Gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene*
  (dit zijn gegevens over bijvoorbeeld verslavingen, prestaties op werk of school of relatieproblemen)

→ Neen → Er hoeft GEEN melding te worden gedaan bij de Autoriteit Persoonsgegevens.

Wel moet het datalek worden onderzocht, en moet herhaling zoveel mogelijk worden voorkomen

- *Gebruikersnamen, wachtwoorden en andere inloggegevens*
- *Gegevens die kunnen worden misbruikt voor (identiteits)fraude (dit gaat bijvoorbeeld om biomedische gegevens, kopieën van identiteitsbewijzen en het BSN)*

→ Ja

Er moet WEL een melding worden gedaan bij de Autoriteit Persoonsgegevens (binnen 72 uur na ontdekken van het datalek).

→

Leiden de Aard en omvang van de gelekte of verloren gegevens tot ernstige nadelige gevolgen voor de betrokkenen

→ Ja →

Er moet WEL melding worden gedaan bij de betrokkenen

→ Neen →

Er hoeft GEEN melding worden gedaan bij de betrokkenen, behalve als de Autoriteit Persoonsgegevens dit alsnog noodzakelijk acht