Informatiebeveiligings-incidenten en datalekken

Bestuur

scholengemeenschap voor
vmbo
havo
atheneum
gymnasium

school voor
praktijkonderwijs

Bezoekadres:
Stationslaan 17
9503 CA Stadskanaal

Postadres:
Postbus 137
9500 AC Stadskanaal

0599 - 631122
stt@ubboemmius.nl

Inhoudsopgave

INFORMATIEBEVEILIGINGS-INCIDENTEN EN DATALEKKEN 1

1. INLEIDING 2
GEBRUIKTE TERMEN 3

2. WET- EN REGELGEVING DATALEKKEN 4
AFSPRAKEN MET LEVERANCIERS 4

3. WERKWIJZE 5
UITGANGSSITUATIE 5
DE VIER ROLLEN 5
DE ZEVEN STAPPEN 5

4. MONITORING BEVEILIGINGSINCIDENTEN EN DATALEKKEN 7

Dit protocol is door het bevoegd gezag vastgesteld op 27 juni 2018, na instemming van de GMR op 25 juni 2018.

1. Inleiding

Geregeld lezen we in de media dat gegevens van werknemers, studenten, leerlingen of patiënten letterlijk op straat liggen; dossiers die worden aangeboden als oud papier, een gestolen smartphone of een verloren USB-stick. Als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben spreken we van een datalek. Het risico op datalekken wordt steeds groter omdat onze persoonsgegevens in steeds meer databanken en/of op dragers zijn opgeslagen.

Een datalek kan nadelige gevolgen hebben voor de persoonlijke levenssfeer van betrokkenen, doordat de weggelekte gegevens oneigenlijk gebruikt kunnen worden. Identiteitsfraude is hiervan een voorbeeld maar ook kan gedacht worden aan ongewenste profilering of doorbreking van bewust gekozen anonimiteit.

Op 1 januari 2016 is de Wet meldplicht datalekken in werking getreden. Het doel van deze Wet is: *"het voorkomen van datalekken ten gevolge van doorbreking van beveiligingsmaatregelen en als deze zich toch voordoen, de gevolgen ervan voor de betrokkenen zoveel mogelijk te beperken".*

De Algemene Verordening Gegevensbescherming (Europese wetgeving die is ingegaan op 25 mei 2018) heeft de privacywetgeving aangescherpt. Dit protocol sluit aan bij de uitgangspunten in het Informatiebeveiligings- en privacybeleid van de stichting Ubbo Emmius, dat mede is gebaseerd op de genoemde AVG.

Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het voorkomen van beveiligingsincidenten en datalekken.

Dit protocol is van toepassing op de gehele organisatie van de stichting Ubbo Emmius, zoals vermeld in het IBP en al haar medewerkers.

Gebruikte termen

- *Beveiligingsincident*: een beveiligingsincident is een gebeurtenis die ervoor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- *Informatievoorziening*: het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
- *Datalek*: een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- *Betrokkene*: de persoon van wie de persoonsgegevens zijn gelekt.

2. Wet- en regelgeving datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplichting melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Het nalaten van deze melding kan leiden tot een fikse boete. De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt, bijvoorbeeld in de leerlingenadministratie of bij digitale leermiddelen. Als de school gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school, dan moet de school met deze verwerkers aanvullende afspraken over het melden van datalekken.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten is dat persoonsgegevens verloren zijn gegaan. Er is persoonlijke informatie 'gelekt'. Een klassiek voorbeeld van een datalek is een hack waarbij een database met persoonsgegevens is gestolen. Maar het verliezen van een usb-stick met daarop de adresgegevens van klas 3b, is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het CvB. Een leverancier is een verwerker voor de school. Er kan worden afgesproken dat een verwerker *namens* de verantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van het CvB. Dat moet wel worden afgesproken, anders zal de verantwoordelijke zelf de melding moeten doen.

Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

Afspraken met leveranciers

Het CvB maakte als verantwoordelijke voor de persoonsgegevens afspraken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. Er zijn afspraken gemaakt over:

- Hoe informeer je elkaar over datalekken en zorg je ook voor bereikbaarheid tijdens bijvoorbeeld het weekend en vakanties.
- Wie doet de melding bij de Autoriteit Persoonsgegevens.
- Welke informatie/gegevens de verwerker moet geven bij een datalek.
- Welke informatie nodig is voor het doen van een melding en dat je elkaar informeert over de melding (maak afspraken dat je een kopie van de melding krijgt of doorstuurt).
- De tijd waarbinnen de verwerkers de gegevens moet aanleveren.
- Wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is.

Voor de afspraken met de verwerker(s) over datalekken wordt gebruik gemaakt van de model verwerkersovereenkomst die hoort bij het convenant "Digitale onderwijsmiddelen en privacy" (www.privacyconvenant.nl).

3. Werkwijze

Uitgangssituatie

- Er is een actueel informatiebeveiligings- en privacy beleid;
- Er is een actueel document betreffende het aanvaardbaar gebruik van bedrijfsmiddelen en/of gedragscode ict en internetgebruik.

Beide documenten zijn te vinden op het UbboNet.

De vier rollen

Er zijn tenminste vier rollen die onderscheiden moeten worden om een beveiligingsincident en/of datalek succesvol af te handelen:

1. *Ontdekker (medewerker):* degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. *Meldpunt (servicedesk):* een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. *Melder (functionaris gegevensbescherming):* degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. *Security officer/ict):* degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

De zeven stappen

1. ONTDEKKEN

De Ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij de locatiedirecteur, stafdirecteur, hoofd ICT of de bestuurder.

2. INVENTARISEREN

De security officer (hoofd ICT) bepaalt of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de Ontdekker en/of de afdeling ICT. De volgende informatie wordt daarna vastgelegd:

- Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
- Datum/periode van het beveiligingsincident
- Aard van het beveiligingsincident
- Wanneer van toepassing (bij een datalek):
  - Omschrijving van de groep betrokkenen
  - Aantal betrokkenen
  - Type persoonsgegevens in kwestie
  - Worden de gegevens binnen een keten gedeeld

3. BEOORDELEN

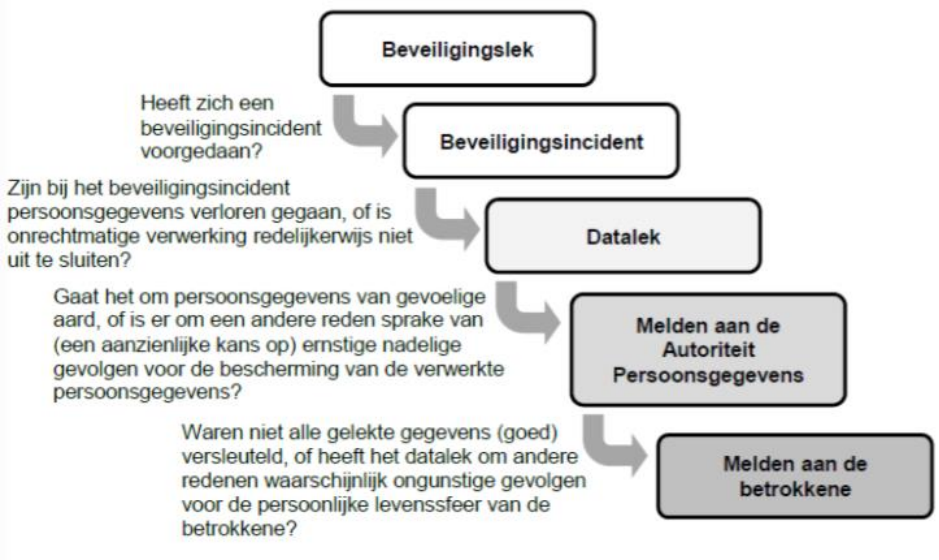
Wanneer de security officer voldoende informatie heeft verzameld, en een datalek vermoedt, stuurt deze de manager IBP een verzoek om de verzamelde informatie te bekijken. Deze brengt dit in het Bestuurstafoverleg (BSO). BSO beoordeelt de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is. De volgende informatie wordt vastgelegd door de manager IBP:

- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
- Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
- Wordt het datalek aan betrokkenen gemeld? Waarom niet?
- Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek', wordt rekening gehouden met het *type* gegevens en met de *hoeveelheid* gegevens. Indien het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, moet er gemeld worden.

Van die ernstige nadelige gevolgen of de kans op ernstige nadelige gevolgen is bijvoorbeeld sprake wanneer er heel veel gegevens van een betrokkene of gegevens van heel veel betrokkenen gelekt zijn maar ook wanneer de gelekte gegevens "gevoelig" zijn zoals bijvoorbeeld bijzondere persoonsgegevens over gezondheid, over de financiële of economische situatie van de betrokkene, of als de gegevens kunnen leiden tot stigmatisering van de betrokkene (denk aan het lekken van een leerling die vaak kinderen pest en daarmee gezien kan worden als notoire pester).

De onderstaande beslisboom kan gebruikt worden



4. **REPAREREN**
   De Technicus (hoofd ICT) wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus van de stichting Ubbo Emmius legt onderstaande vast:
   - Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voorgaande voor zover de oorzaak bekend is.
   - Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Hoe zijn de gegevens onbegrijpelijk gemaakt (versleuteld)?

5. **MELDEN**
   Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de manager IBP dit binnen twee werkdagen doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij het meldloket datalekken: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0.

6. **VASTLEGGEN**
   Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de manager IBP, waarmee het incident is afgesloten. De manager IBP verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker.

7. **INFORMEREN BETROKKENE: LEERLING EN/OF ZIJN OUDERS**
   Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers, leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). In principe kan ervan worden uitgaan dat het lekken van gevoelige aard gelekt gemeld moet worden bij de betrokkenen. Let op: als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat toch niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

4. Monitoring beveiligingsincidenten en datalekken

De manager IBP maakt twee keer per jaar een analyse van de meldingen van beveiligingsincidenten en datalekken in samenwerking met de functionaris gegevensbescherming.

In de analyse wordt ingegaan op eventuele structurele ontwikkelingen en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.

Het schoolbestuur wordt geïnformeerd over de uitkomsten van de analyse.