Protocol informatiebeveiligingsincidenten

Bron
Kennisnet

Bewerkt door:

K. Knoester

Versie	Status	Datum	Auteur	Omschrijving
1.0	Concept	25-3-2019	K. Knoester (model Kennisnet en aangepast naar CBS De Hoeksteen)	

Vastgesteld door CBS De Hoeksteen:

Versie	Datum	Naam	Functie
			MR (instemming)
			Voorzitter bes (vaststelling)

Inhoud

Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het InformatieBeveiligings- en Privacy beleid (IBP-beleid) van Vereniging tot Stichting en Instandhouding van Scholen met de Bijbel voor Basisonderwijs te Ooltgensplaat (hierna: CBS De Hoeksteen).

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 CBS De Hoeksteen als geheel en geldt voor al haar medewerkers.

Gebruikte termen:

- **Beveiligingsincident**: een beveiligingsincident is een gebeurtenis die er voor 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.

Wet- en regelgeving datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd, opgevolgd door de Algemene Verordening Gegevensbescherming (effectief per 25 mei 2018). 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 je leerlingadministratie of 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 maken 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. Neem in geval van twijfel contact op met de directeur of de veiligheidsverantwoordelijke (zie hierna).

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. 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 schoolbestuur. Dat moet wel worden afgesproken, anders zal de verantwoordelijke zelf de melding moeten doen.

Als er een ernstig datalek is (zie hierna), moet daarvan binnen 72 uur na ontdekking van het lek melding worden gedaan bij de Autoriteit Persoonsgegevens.

Afspraken met leveranciers

Het schoolbestuur moet als verantwoordelijke voor de persoonsgegevens afspraken maken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. Spreek af:

- Hoe informeer je elkaar over datalekken, en zorg 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.

Maak schriftelijke afspraken met uw verwerker(s) over datalekken. Hiervoor kan gebruik worden gemaakt van de model verwerkersovereenkomst die hoort bij het convenant “Digitale onderwijsmiddelen en privacy” (www.privacyconvenant.nl).

Werkwijze

Uitgangssituatie

- Er is een actueel InformatieBeveiligings- en Privacy beleid;
- Er is een actuele gedragscode InformatieBeveiliging en Privacy.

De drie rollen

Er zijn tenminste drie 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 (de IBP-verantwoordelijke of de Functionaris Gegevensbescherming):** de persoon waar alle beveiligingsincidenten worden gemeld en worden geanalyseerd. De rol van het Meldpunt wordt binnen CBS De Hoeksteen vervult door het IBP-team. Bij afwezigheid van de IBP-verantwoordelijke zal hij worden vervangen door de Functionaris Gegevensbescherming om te waarborgen dat er tijdig actie wordt ondernomen.
3. **Technicus (applicatiebeheerder, ict-coördinator of ICT-leverancier)**: 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 via het Meldingsformulier Informatiebeveiligingsincident bij de directeur (Karel Knoester, k.knoester@hoeksteen-ooltgensplaat.nl) of bij diens afwezigheid bij de adjunct-directeur (Jan-Willem van de Werken, j.vandewerken@hoeksteen-ooltgensplaat.nl). Zij vormen samen het zogenaamde IBP-team.

2. **Inventariseren**
   Het meldpunt bepaalt vervolgens of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de Ontdekker en/of de Technicus. De volgende informatie wordt daarna in het incidentenregister 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 en locatie 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
     - De mogelijke gevolgen voor de privacy van de betrokkenen

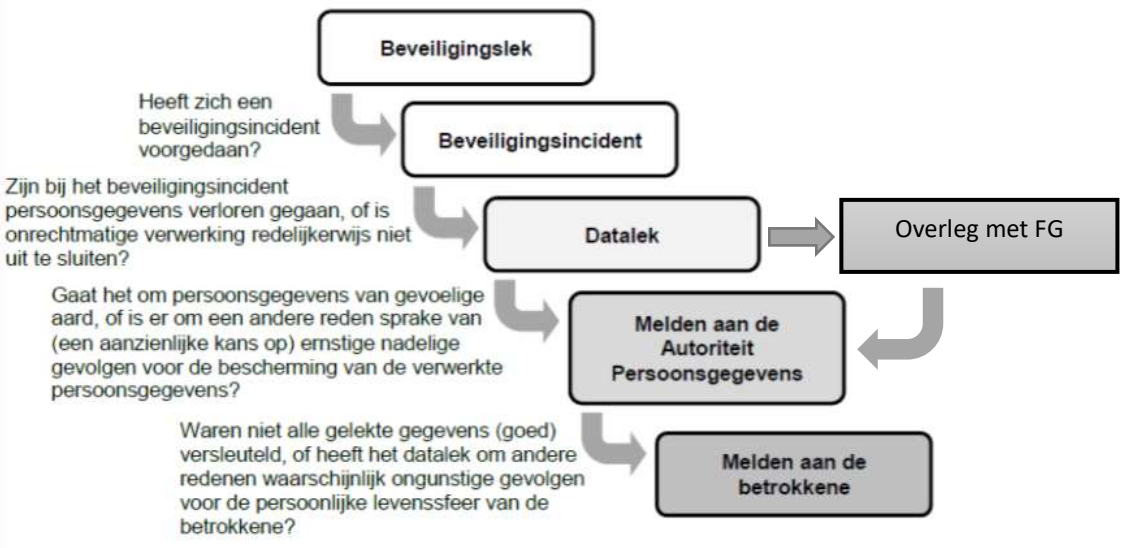
3. Beoordelen

Het Meldpunt (IBP-team) beoordeelt (al dan niet in afstemming met de Ontdekker) de feiten om te bepalen of er sprake is van een datalek. Wanneer het IBP-team voldoende informatie heeft verzameld en een datalek vermoed of constateert, neemt hij hierover contact op met de Functionaris Gegevensbescherming. In overleg met de Functionaris Gegevensbescherming besluit het IBP-team (of bij afwezigheid van een van beiden besluiten zij zelfstandig) of gemeld moet worden aan de Autoriteit Persoonsgegevens en – in dat geval – of ook de betrokkenen moeten worden geïnformeerd.

De informatie welke door het Meldpunt in ieder geval wordt vastgelegd is opgenomen in het incidentregister.

Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek', hou je rekening 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 bijvoorbeeld aan het lekken van een leerling die vaak kinderen pest en daarmee gezien kan worden als notoire pester).
Zie voor een toelichting op de meldplicht de beleidsregels van de Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken_wbp.pdf

De onderstaande beslisboom kan gebruikt worden



4. Repareren

De Technicus wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak - indien mogelijk/van toepassing - (laten) verhelpen. De Technicus rapporteert aan het de veiligheidsverantwoordelijke:

- 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 dan zal de Melder dit binnen 72 uur na ontdekking door de Ontdekker 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://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken. Het schoolbestuur wordt door het Meldpunt zo spoedig mogelijk geïnformeerd indien er een datalek wordt gemeld bij de Autoriteit Persoonsgegevens.

6. **Vastleggen**
   Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door het Meldpunt waarmee het incident is afgesloten. Het Meldpunt informeert de Ontdekker over de afwikkeling van het incident en doet – indien van toepassing – verslag van de genomen maatregelen.

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 bijvoorbeeld medewerkers of leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). In principe kan er van 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.

Monitoring beveiligingsincidenten en datalekken

Het Meldpunt (IBP-team) maakt een keer per jaar een analyse van de meldingen van beveiligingsincidenten en datalekken. In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen. Het Meldpunt (IBP-team) rapporteert aan het schoolbestuur over de uitkomsten van de analyse.

Communicatie

Uitgangspunt is dat het informeren van betrokkenen wordt gedaan door de directeur. In overleg met de directeur kan hiervan in voorkomende gevallen om moverende redenen worden afgeweken.