Protocol
Beveiligingsincidenten en datalekken

Petrus Canisius College

Vastgesteld juli 2018 (18 6227b)
CDO: 4 juni 2018
MR: 2 juli 2018

Protocol beveiligingsincidenten en datalekken

CDO: 4 juni 2018
MR: 2 juli 2018

Samenvatting

Op grond van de Wet meldplicht datalekken en op grond van de Algemene verordening gegevensbescherming (AVG, 2018) dient het schoolbestuur te beschikken over een protocol beveiligingsincidenten en datalekken. In het bijgaande protocol zijn de stappen beschreven die gevolgd worden indien er sprake is van een (vermoedelijk) beveiligingsincident/datalek.

1. Inleiding

Het voorliggende Protocol informatiebeveiligingsincidenten en datalekken (bron: Kennisnet) sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacybeleid van het Petrus Canisius College (PCC)

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

Dit protocol is van toepassing op de gehele organisatie van het PCC.

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. Bij een beveiligingsincident kan worden gedacht aan het verlies van een USB-stick of papieren documenten met beveiligingsgegevens, diefstal van een laptop of een digitale inbraak door een hacker. Niet ieder beveiligingsincident is een datalek.

- **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.

- **Veroorzaker**; de persoon die het beveiligingsincident heeft veroorzaakt.

2. Wet- en regelgeving datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplicht 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 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 bewerkers aanvullende afspraken over het melden van datalekken. Dit gebeurt onder de Algemene verordening gegevensbescherming (AVG) die op 25 mei 2018 van kracht is geworden middels de verwerkersovereenkomsten.

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 het schoolbestuur. Een leverancier is een bewerker voor de school. Er kan worden afgesproken dat een bewerker **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 datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

3. Werkwijze melden

3.1 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/leerling/ouder e.d.)**; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt. Dit kan uiteraard ook de veroorzaker zijn (degene die bijvoorbeeld een USB-stick is kwijtgeraakt).

2. **Meldpunt (manager IBP (hoofd bestuursbureau PCC) / privacy officer** (kwaliteitsmedewerker PCC)**)**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.

3. **Melder (functionaris gegevensbescherming** (extern ingehuurd door het PCC, tot medio 2018 hoofd bestuursbureau PCC)**)**: degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.

4. **Technicus (information security officer** (ICT-coördinator PCC)**)**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

3.2 De zeven stappen

1. **Ontdekken / melden beveiligingsincident**
   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 het meldpunt via ibp@pcc.nu

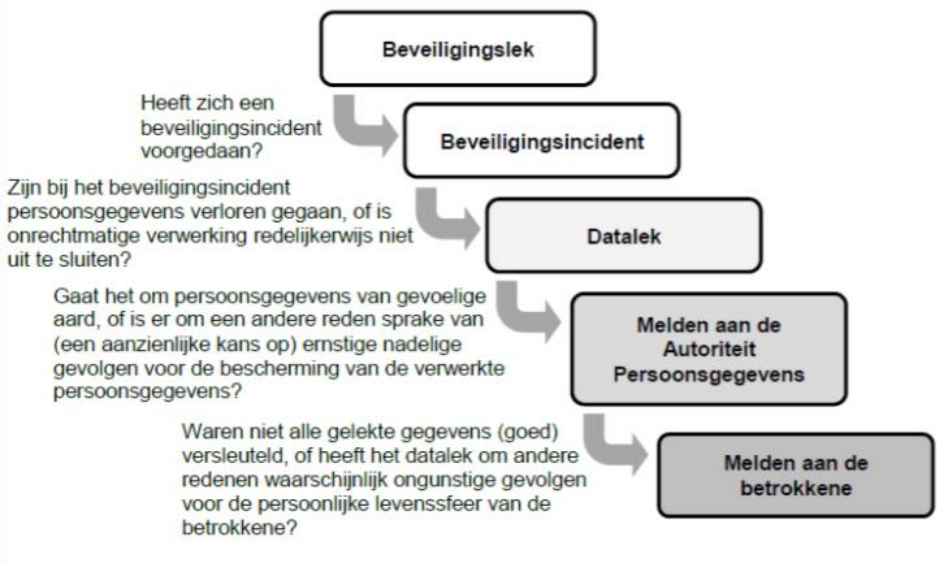
2. **Inventariseren (binnen 24 uur na de melding van het beveiligingsincident)**
   Het Meldpunt bepaalt of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de Ontdekker en/of de Technicus. De volgende informatie wordt daarna vastgelegd:
   - 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 (binnen 48 uur na de melding van het beveiligingsincident)**
   Wanneer het Meldpunt voldoende informatie heeft verzameld en een datalek vermoedt, dan stuurt hij de Melder een verzoek om de verzamelde informatie te bekijken. De Melder 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 Melder:
   - 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.

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 (laten) verhelpen. De technicus van het PCC 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 Autoriteit Persoonsgegevens (binnen 72 uur na melding beveiligingsincident)**
   Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de Melder dit 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 en (interne) communicatie**
   Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door het Meldpunt. Het Meldpunt verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker, na overleg over de in- en externe communicatie met de voorzitter van het college van bestuur en de stafmedewerker PR & Communicatie.
   De voorzitter van het college van bestuur informeert de Raad van toezicht in geval van een melding aan de Autoriteit Persoonsgegevens.

7. **Informeren betrokkene: medewerker, 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 er

van worden uitgaan dat het lekken van gevoelige aard gelekt gemeld moet worden bij de betrokkenen. Als er echter persoonsgegevens zijn gelekt die zijn beveiligd of versleuteld, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan is het informeren van betrokkenen niet nodig (bijvoorbeeld ingeval van een beveiligde én versleutelde database met gebruikersnamen).

4. Monitoring beveiligingsincidenten en datalekken

Het Meldpunt van het PCC 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.

De voorzitter van het college van bestuur en de Raad van toezicht worden geïnformeerd over de uitkomsten van de analyse.

5. Afhandeling beveiligingsincident richting veroorzaker

Met of ten aanzien van de veroorzaker van het beveiligingsincident (dit kan ook de ontdekker zijn) worden afspraken gemaakt dan wel maatregelen getroffen om nieuwe beveiligingsincidenten te voorkomen. De afspraken dan wel maatregelen zullen per incident bekeken moeten worden.