Protocol informatiebeveiligingsincidenten en datalekken

mgr. Frencken college

Inhoud

Inleiding 3
Wet- en regelgeving datalekken 3
Afspraken met leveranciers 4
Werkwijze 4
De vier rollen 4
De zeven stappen 4
Monitoring beveiligingsincidenten en datalekken 6

Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacybeleid van het Frencken.

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 het Frencken, zoals vermeld in het IBP-beleid 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.

Wet- en regelgeving datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn wij 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 onze leerlingadministratie of digitale leermiddelen.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten dat persoonsgegevens verloren zijn gegaan. 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 schoolbestuur.

Als er een datalek is, moeten wij het lek binnen 72 uur na ontdekking melden bij de Autoriteit Persoonsgegevens.

Afspraken met leveranciers

Als verantwoordelijke voor de persoonsgegevens hebben wij afspraken gemaakt met leveranciers die persoonsgegevens van ons ontvangen. In de bewerkersovereenkomsten hebben we afspraken over:

- Elkaar informeren over datalekken.
- Wie de melding doet bij de Autoriteit Persoonsgegevens.
- Welke gegevens de bewerker moet geven bij een datalek.
- Dat de bewerker zonder onredelijke vertraging de gegevens levert.
- Wie de communicatie met de gebruikers voor zijn rekening neemt als dat nodig is.

Werkwijze

De vier rollen

Er zijn tenminste vier rollen die wij onderscheiden 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, zijnde meldpuntdatalek@frenckencollege.nl
3. **Melder (functionaris gegevensbescherming)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Technicus (security officer / ict coördinator)**; 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 het meldpunt via meldpuntdatalek@frenckencollege.nl .

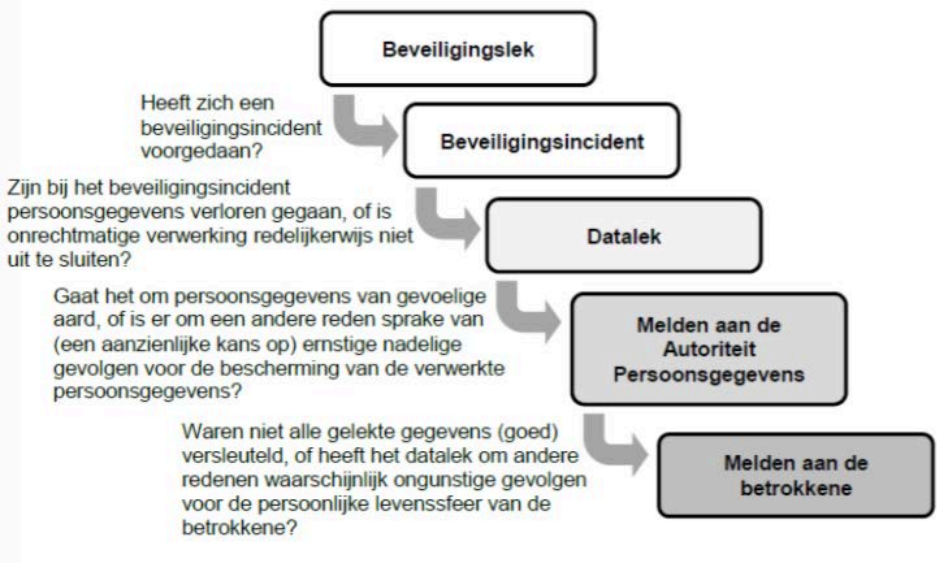
2. **Inventariseren**
   Het meldpunt bepaalt of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de ontdekker en/of de technicus. De volgende informatie wordt daarna vastgelegd:
   - Samenvatting van het beveiligingsincident; wat is 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**
   Wanneer het meldpunt voldoende informatie heeft verzameld en een datalek vermoedt, stuurt deze 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 betrokkene(n) vereist is.
   De volgende informatie wordt vastgelegd door de melder:

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

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, wordt het lek gemeld.
Van 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 hierbij bijvoorbeeld aan het lekken van een leerling die vaak kinderen pest en daarmee gezien kan worden als notoire pester).

De onderstaande beslisboom wordt gebruikt



4. Repareren

De technicus (intern of extern) wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus 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 degene 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 betrokkene(n) dan zal de melder 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.

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 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 melden we het datalek ook aan de betrokkene(n) zelf. Dat kunnen medewerkers, leerlingen (of hun ouders als zij jonger zijn dan 16 jaar) zijn. In principe kan er van worden uitgegaan dat het lekken van gevoelige aard gemeld moet worden bij de betrokkene(n). Als er persoonsgegevens zijn gelekt die zijn beveiligd of versleuteld, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat niet aan betrokkene(n) te worden gemeld.

Monitoring beveiligingsincidenten en datalekken

Het meldpunt van het Frencken 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.

Dit protocol is met instemming van de MR door het bevoegd gezag vastgesteld op 16 april 2018