Protocol Beveiligingsincidenten en datalekken

Oplegger

Besluitvormingsprocedure		
Betrokkene	**Onderdeel**	**Datum**
College van bestuur	Voorlopige vaststelling	15-01-2019
Directieberaad	Ter informatie	22-01-2019
Gemeenschappelijke Medezeggenschapsraad	Ter informatie	12-02-2019
College van Bestuur	Vaststelling	19-02-2019

Toelichting:
Dit document beschrijft de wijze waarop de betrokkenen bij stichting Trinamiek om dienen te gaan met een datalek en/of beveiligingsincident.

Bronn(en):
Dit document is een bewerking van het voorbeelddocument van Kennisnet en op maat gemaakt voor stichting Trinamiek.

Herzien: per maart 2021
Map: AVG
Publicatie: Tri-net (AVG) en website Trinamiek
Verantwoordelijke: Portefeuillehouder AVG
Aandachtspunt: -

Protocol Beveiligingsincidenten en datalekken

Inhoud

Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacy beleid van Stichting Trinamiek.

Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is om de mogelijke gevolgen van beveiligingsincidenten en datalekken te minimaliseren.

Dit protocol is van toepassing op de gehele organisatie van Stichting Trinamiek, zoals vermeld in het privacyreglement.

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.

1. 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. Een datalek is *ernstig* als het waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Het nalaten van deze melding kan leiden tot een fikse boete.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Bijvoorbeeld in de leerlingadministratie of digitale leermiddelen. Als de school gebruik maakt van leveranciers die persoonsgegevens ontvangen van de school, zoals uitgevers of distributeurs, dan moet de school met deze bewerkers aanvullende afspraken over het melden van datalekken maken in de verwerkers overeenkomsten die met deze leveranciers worden afgesloten.

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. 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 groep 3b, is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, het bestuur van stichting Trinamiek. 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 bestuur. Dat moet wel worden afgesproken, anders zal de verantwoordelijke zelf de melding moeten doen.

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

2. Afspraken met leveranciers

Het schoolbestuur moet als verantwoordelijke voor de persoonsgegevens afspraken maken met leveranciers als die persoonsgegevens verwerken. Afspraken over datalekken vallen daar ook onder. Trinamiek spreekt daarom met leveranciers 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 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.

Trinamiek maakt schriftelijke afspraken met haar verwerker(s) over datalekken. Hiervoor wordt gebruikgemaakt van de model verwerkersovereenkomst die hoort bij het convenant “Digitale onderwijsmiddelen en privacy” (www.privacyconvenant.nl).

3. Werkwijze

Uitgangssituatie

- Er is een actueel privacyreglement;
- Er is een actueel document betreffende het aanvaardbaar gebruik van bedrijfsmiddelen onder de noemer ‘Gedragscode IBP’.

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/ouder/leerling)**; degene die het beveiligingsincident of het datalek op het spoor komt en het proces in werking stelt. Ten behoeve van de ontdekker is er voor verschillende groepen een document opgesteld waarin is beschreven hoe wij verwachten dat zij handelen bij het ontdekken van een datalek. Voor leerlingen is dit het document. Voor ouders en medewerkers is dit document opgesteld.
2. **Meldpunt (servicedesk)**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt. De functionaris gegevensbescherming, hoofd ict en bestuurssecretaris maken deel uit van dit meldpunt.
3. **Melder (functionaris gegevensbescherming)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens namens de verwerkingsverantwoordelijke.
4. **Technicus (hoofd ict)**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

4. 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 door het invullen van het eerste gedeelte van het bijbehorende meldingsformulier waar op de website van Trinamiek en de afzonderlijke scholen naar verwezen wordt. Vanuit het meldpunt wordt contact opgenomen met de ontdekker om te bepalen of er daadwerkelijk sprake is van een incident/datalek en om te bepalen wat er eventueel nog nodig is om risico’s verder te beperken of geheel op te heffen. Het meldpunt vult het tweede gedeelte van het formulier in.

2. Inventariseren

Het Meldpunt bepaalt op basis van het ontvangen meldingsformulier of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet het aanvullende vragen uit bij de Ontdekker en/of de Technicus. Het meldpunt vult eventueel aanvullende gegevens aan in het meldingsformulier bij het gedeelte van de Ontdekker (eerste deel van formulier).

3. Beoordelen

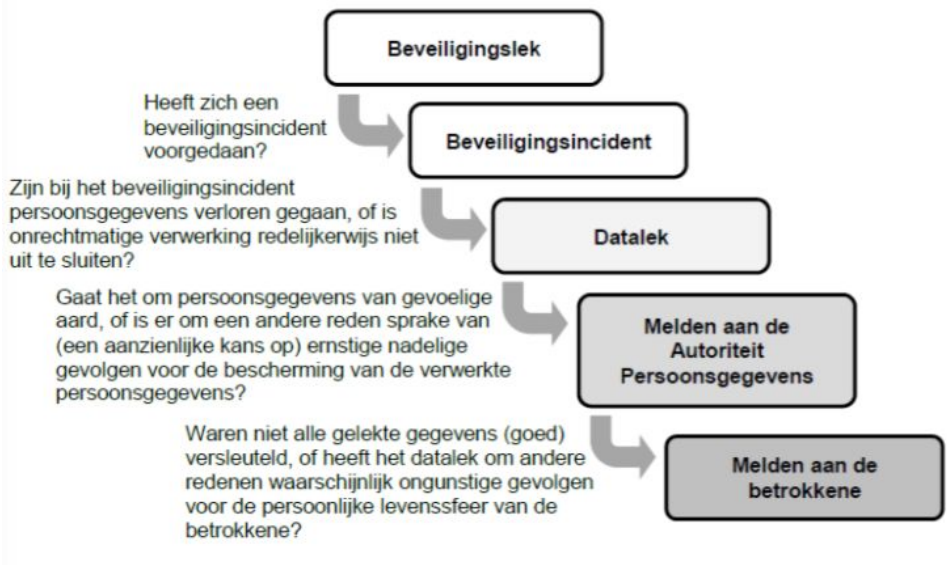
Wanneer het Meldpunt voldoende informatie heeft verzameld, en een datalek vermoedt, stuurt deze de Melder (Functionaris gegevensbescherming) een verzoek om de verzamelde informatie te bekijken. De Melder beoordeelt de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is (dient dan binnen 72 uur na ontdekking van het datalek plaats te vinden).

De volgende informatie wordt vastgelegd door de Melder in het laatste gedeelte van het meldingsformulier:

- 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', houdt de melder 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 aan het lekken van een leerling die vaak andere leerlingen pest en daarmee gezien kan worden als notoire pester).
De onderstaande beslisboom wordt hierbij gebruikt:



4. Repareren

De Technicus wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus van Stichting Trinamiek legt in het (tweede deel van het) meldingsformulier onderstaande vast:

- Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voorgaande voor zover de oorzaak van de inbreuk 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 Melder dit binnen 72 uur na ontdekking van het datalek doen. De Melder informeert de verwerkingsverantwoordelijke (het bestuur) vooraf over de melding. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen zoals in het meldingsformulier vastgelegd. Het lek wordt gemeld bij het meldloket datalekken.

6. Vastleggen

Alle informatie, die in de voorgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door het Meldpunt waarmee het incident is gesloten. Het Meldpunt verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker.

7. Informeren betrokkenen: leerling en/of zijn ouders

Binnen Trinamiek gaan we er vanuit overwegingen van transparantie van uit dat we betrokkene(n) informeren over het lekken van hun persoonsgegevens. Alleen wanneer dit op basis van de wet niet noodzakelijk is en het informeren onevenredig veel onrust kan veroorzaken, zal hier in voorkomende gevallen van worden afgezien. In principe kan ervan worden uitgegaan dat het lekken van persoonsgegevens van gevoelige aard altijd 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. Ook als er al maatregelen zijn genomen waardoor het datalek zich in de toekomst niet meer zal voordoen, hoeven betrokkenen niet te worden geïnformeerd. De afweging om in dergelijke gevallen al dan niet direct te melden aan betrokkenen zal in samenspraak met de functionaris gegevensbescherming worden gemaakt.

5. Monitoring beveiligingsincidenten en datalekken

Het Meldpunt van Stichting Trinamiek 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 bestuur van stichting Trinamiek wordt geïnformeerd over de uitkomsten van de analyse.

6. Overige aandachtspunten

- In bovenstaand protocol is de formele communicatie met de betrokkenen en degenen die vanuit de stichting Trinamiek een officiële rol hebben (zie vier rollen) beschreven. Mochten

er anderen rondom de inbreuk informatie willen of zich op andere wijze in de communicatie mengen (waar onder mogelijkerwijs de pers), dan zal de afdeling communicatie leidend zijn in de omgang met deze derden.
- Een signaal van buiten de organisatie van stichting Trinamiek zal op gelijke wijze worden benaderd als beschreven in dit protocol. Degene die het betreffende lek meldt zal als 'ontdekker' worden beschouwd.
- Indien de aard van de inbreuk de technische en/of organisatorische kwaliteiten binnen de stichting te boven gaat, dan zal externe deskundigheid worden betrokken. Bij een dergelijk besluit zal steeds de verwerkingsverantwoordelijke en de functionaris gegevensbescherming worden betrokken.

Bijlage 1

Instructie medewerkers en ouders voor melden beveiligingsincident

De rol van medewerkers en ouders/verzorgers bij een inbreuk op de veiligheid van persoonsgegevens en privacy

Bij Trinamiek vinden wij de veiligheid van onze computer- en informatiesystemen (internet en bijbehorende hardware en software), persoonsgegevens en privacy erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen en de gegevens kan het voorkomen dat er toch ergens een zwakke plek zit of iets is misgegaan. Als u een zwakke plek (kwetsbaarheid) in één van onze systemen heeft gevonden of denkt dat er ergens onzorgvuldig met persoonsgegevens is omgegaan, dan horen wij dit graag van u. Wij kunnen dan zo snel mogelijk maatregelen treffen om dit op te lossen. Wij willen graag met u samenwerken om de leerlingen, medewerkers en onze systemen beter te kunnen beschermen.

Wij vragen u:

- Uw bevindingen te melden met het meldingsformulier waarnaar op de website van Trinamiek en de afzonderlijke scholen wordt verwezen;
- De zwakke plek niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of (persoons)gegevens van derden in te kijken, te verwijderen of aan te passen;
- De zwakke plek niet met anderen te delen totdat deze is verholpen en alle (vertrouwelijke) gegevens die zijn verkregen via het lek direct na het verhelpen van het lek te wissen;
- Voldoende informatie te geven om het probleem te reproduceren zodat wij het zo snel mogelijk kunnen verhelpen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de zwakke plek voldoende, maar bij complexere problemen kan meer nodig zijn.

Wij zeggen toe dat:

- Wij de melding binnen 1 werkdag in behandeling nemen en binnen 3 werkdagen reageren op uw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing;

- Wij behandelen uw melding vertrouwelijk en zullen uw persoonlijke gegevens niet zonder uw toestemming met derden delen tenzij dat noodzakelijk is om een wettelijke verplichting na te komen. Melden onder een pseudoniem is mogelijk;
- Wij houden u op de hoogte van de voortgang van het verhelpen van de zwakke plek;
- In berichtgeving over het gemelde probleem zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker. Wij streven er naar om alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.