Beveiligingsincidenten en datalekken

PROTOCOL

COLOFON

Eigenaar:	Hoofd ICT
Beheerder:	Hoofd ICT
Vaststelling door:	Bestuurder op 3 april 2024
Instemming door:	GMR op 21 maart 2024
Doelgroep:	Medewerkers, ouders, leerlingen en betrokkenen
Publicatie:	Website Trinamiek, op Tri-net verwijzing naar de plek op de website, verwijzing op website van de scholen
Evaluatie:	Tweejaarlijks, opgenomen in ICT / IBP kalender (intern document)
Huidige Privacy Officer:	Privacy Helder, privacy@trinamiek.nl

Inhoud

Inleiding

Doel van deze notitie

Wanneer er sprake is van een mogelijk beveiligingsincident of datalek, moeten er een of meer handelingen worden uitgevoerd. Dit document geeft aan welke handelingen dit zijn en wie deze moeten uitvoeren. Ook bij twijfel is het van belang actie te ondernemen. Dit document is bedoeld voor alle mensen die bij Trinamiek betrokken zijn.

Wil je direct een melding maken, dan kan dat hier. Wil je meer lezen over hoe het melden werkt, lees dan verder.

In dit document leggen we eerst uit wat een beveiligingsincident is en wanneer er sprake is van een datalek. Vervolgens vind je in dit document de stappen die je zelf moet ondernemen en die de organisatie onderneemt wanneer dat nodig is.

Begrippen beveiligingsincident en datalek

Wat is een beveiligingsincident

Een beveiligingsincident is een fout of een lek in een systeem dat gebruikt wordt of in een proces. Door deze fout of lek kan een systeem bijvoorbeeld niet meer betrouwbaar of beschikbaar zijn. Een beveiligingsincident is niet altijd meteen een datalek. We spreken van een beveiligingsincident als bij een fout of lek geen persoonsgegevens betrokken zijn. Als bijvoorbeeld een laptop zoek raakt, maar de toegang ertoe door beveiliging niet mogelijk is, spreken we van een beveiligingsincident.

Voorbeelden van beveiligingsincidenten

- Besmettingen met virussen en/of malware;
- Diefstal / verlies van versleutelde laptop;
- Het delen van wachtwoorden;
- Gevoelige bedrijfsinformatie, zoals bijvoorbeeld budgetten beschikbaar voor aanbestedingen, zijn terechtgekomen bij mogelijke inschrijvers.

Wat is een datalek

Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is, waarbij de oorzaak een inbreuk op de beveiliging van deze gegevens is. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens door zo'n inbreuk valt onder een datalek.

[bron: https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/wat-is-een-datalek, opgehaald op 25 januari 2024, 14:22 uur.]

Voorbeelden van datalekken

- Een verkeerd verzonden e-mail, of een e-mail met de ontvangers in het aan- of cc-veld in plaats van het bcc-veld, zodat ontvangers elkaars e-mailadres zien;
- Het verlies van een (zakelijke) mobiele telefoon of laptop met gevaar op lekken van persoonsgegevens;
- Een verkeerd verzonden of bezorgde brief;
- Verlies of diefstal van een usb-stick met persoonsgegevens;
- Persoonsgegevens die worden verwerkt of ingezien door een medewerker die daar geen bevoegdheid voor heeft;
- Papieren met bijvoorbeeld toetsresultaten die op een printer/kopieerapparaat blijven liggen;
- Brand in de serverruimte en geen back-up beschikbaar, waardoor persoonsgegevens verloren gaan;
- Toevoegen: pc niet locken en ingelogd staan in diverse systemen met persoonsgegevens.

Wat te doen bij een (mogelijk) beveiligingsincident of datalek

Ga direct naar de website van Trinamiek / Over Trinamiek / Regelingen. Daar vind je het Protocol beveiligingsincidenten en datalekken. Vul het meldformulier in. Het is belangrijk dit zo snel mogelijk te doen en met zo veel mogelijk details. De Privacy Officer (zie pagina 1 van dit protocol) zal het vervolgproces begeleiden en jou op de hoogte houden. In het volgende hoofdstuk kan je de stappen lezen.

Wat gebeurt er na een melding

Stap 1: Meld elk mogelijk datalek meteen bij het de Privacy Officer

Zodra je als medewerker, ouder of leerling een mogelijk beveiligingsincident of datalek ontdekt, moet deze dit onmiddellijk melden bij de Privacy Officer middels het protocol Beveiligingsincidenten en Datalekken. Dit kan door het invullen van het meldformulier of door te bellen naar de de Privacy Officer (PO). Hier is haast bij, want hoe korter een incident duurt, hoe minder schade er meestal veroorzaakt wordt. Ook is snelheid nodig, want bij ernstige datalekken is het nodig dat we deze binnen 72 uur melden bij de Autoriteit Persoonsgegevens. Door snel te melden, kunnen we snel onderzoeken wat er aan de hand is en welke maatregelen we moeten nemen.

Stap 2: De Privacy Officer stelt vast of er sprake is van een datalek

De Privacy Officer gaat onder meer na of er wel of niet persoonsgegevens betrokken zijn bij het vermeende datalek. Zijn er wel persoons- of bedrijfskritische gegevens betrokken, dan beoordeelt de Privacy Officer of er daadwerkelijk sprake is geweest van een inbreuk. Hierbij wordt gebruikgemaakt van het stroomschema uit bijlage 1. Als er geen persoonsgegevens betrokken zijn, dan geeft de PO het mogelijke beveiligingsincident door aan de afdeling ICT voor de verdere afhandeling. Als er wel persoonsgegevens bij betrokken zijn, dan beoordeelt

de PO of en evt hoe de getroffen personen geïnformeerd moeten worden. De PO overlegt hierover ook met de organisatie.

Stap 3: De Privacy Officer verzamelt gegevens en legt ze vast in het register

Als de Privacy Officer heeft vastgesteld dat er inderdaad sprake is van een beveiligingsincident of een datalek, dan registreert zij dat in het Register Beveiligingsincidenten en Datalekken.

Stap 4: De Privacy Officer stelt vast of het datalek moet worden gemeld

Bij een datalek moeten we ook vaststellen of het een zodanig ernstig datalek is dat we de Authoriteit Persoongegevens (AP) moeten informeren. Dat moet in ieder geval binnen 72 uur na het ontdekken van het datalek, ook als op dat moment nog niet alle gevraagde gegevens voorhanden zijn. Voor het doen van een melding maakt het niet uit of het datalek veroorzaakt is door een fout of door overmacht. Indien een datalek bij de AP moet worden gemeld dan zal de Functionaris Gegevensbescherming (FG) de melding verzorgen. Voor hulp bij het beoordelen van dit datalek maakt de Privacy Officer gebruik van het stroomdiagram uit bijlage 2.

Stap 5: Verplichtingen na melding bij AP

Wanneer een datalek serieuze nadelige gevolgen heeft voor het privéleven van de personen in kwestie, moet er niet alleen een melding worden gedaan aan de AP, maar moeten ook de personen van wie de gegevens zijn gelekt op de hoogte worden gebracht.
Serieuze nadelige gevolgen zijn bijvoorbeeld:

- identiteitsfraude
- discriminstie
- reputatieschade

Wanneer er bijzondere persoonsgegevens zijn gelekt, dan moet dit in principe altijd gemeld worden aan de getroffen personen. Een melding aan de getroffen personen is niet nodig als de gegevens onleesbaar zijn door versleuteling of als de gegevens op afstand kunnen worden gewist van bijvoorbeeld een gestolen laptop. Daarbij moet het wel zeker zijn dat niemand deze gegevens heeft ingezien. De PO helpt bij het beoordelen hiervan aan de hand van het stroomdiagram uit bijlage 3.

Stap 6: Leg de genomen maatregelen vast

Nadat er duidelijkheid is over de oorzaak en gevolgen van het beveiligingsincident of datalek, zorgt de Privacy Officer ervoor dat we zo snel mogelijk de genomen maatregelen vastleggen in het Register Beveiligingsincidenten en Datalekken. Zo kunnen we later zien welke incidenten zijn voorgevallen en wat we daarmee hebben gedaan. Ook kunnen we zo toekomstige incidenten zoveel mogelijk voorkomen.

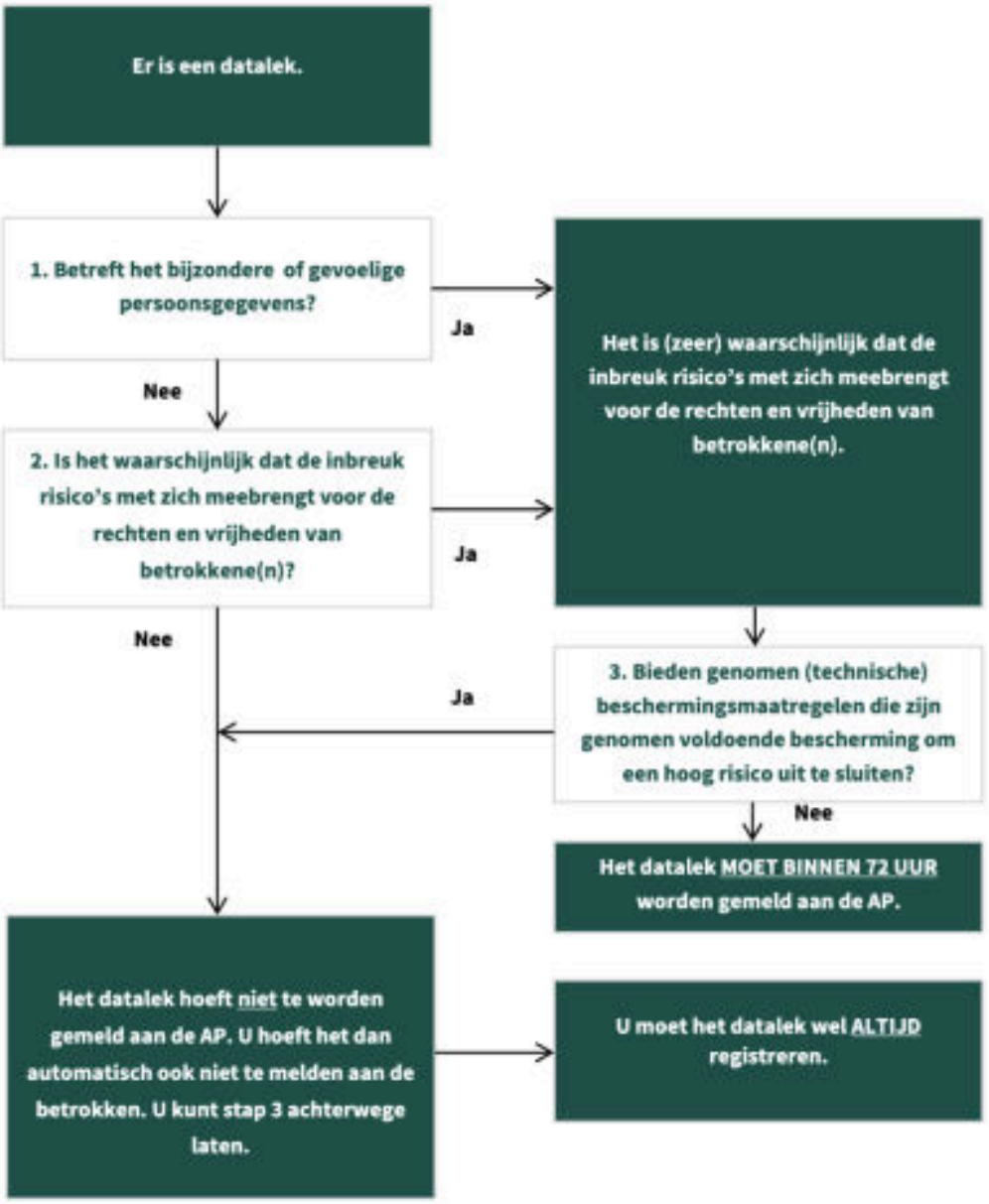
Stap 7: Evalueer regelmatig de maatregelen

Ook nemen we waar mogelijk maatregelen om te voorkomen dat een vergelijkbaar datalek zich in de toekomst opnieuw voordoet. Daarom evalueren we jaarlijks de beveiligingsincidenten en datalekken, met de genomen en voorgenomen maatregelen. De opbrengsten van de evaluatie leggen we ook vast in het Register Incidenten en Datalekken.

Bijlagen

Bijlage 1: Is er sprake van een datalek?

Bijlage 2: Moet het datalek bij de AP worden gemeld?



Bijlage 3: Moet het datalek aan de betrokkenen worden gemeld?