

Leer

Vraag

Ontmoet

Lees

Doe

Handleiding Meterkastkaart

Procedure datalekken en
beveiligingsincidenten

VOB202311V0.1



Inhoud

Inhoud	1
Inleiding	2
Aan de slag	2
Definities	2
Noodzakelijk	3
1. Eén contactpunt	3
2. Vermoed je een datalek of beveiligingsincident? Direct bellen!	3
3. Het belang van de juiste CSIRT-medewerkers... ..	3
4. Formeer een crisisteam	4
5. Denk vooraf na over keuzes die je in geval van een incident zult moeten maken.....	5
6. Welke organisaties moeten gebeld worden?	5
Borging	6
Sterk aan te bevelen.....	6
Achtergrondinformatie	6

Inleiding

De bescherming van persoonsgegevens is een belangrijk onderwerp voor elke organisatie die met vertrouwelijke informatie werkt. Dit geldt ook voor openbare bibliotheken, die allerlei persoonlijke gegevens van hun klanten en bezoekers verwerken.

Een ernstig datalek of beveiligingsincident (verder: een *incident*) kan niet alleen de reputatie van de bibliotheek schaden, maar ook ernstig nadelige gevolgen hebben voor de privacy van onze medewerkers, klanten en bezoekers.

Het is daarom essentieel dat de bibliotheek een procedure heeft voor het omgaan met incidenten. In deze handleiding wordt stap voor stap toegelicht hoe een effectieve procedure voor het melden en afhandelen van datalekken kan worden opgezet en ingevoerd in een openbare bibliotheek.

Deze handleiding is bedoeld voor alle bibliotheken. Ook als je (van) alles hebt uitbesteed. In dat geval is het wenselijk om de meterkastkaart en deze handleiding met jouw externe partij te bespreken. Leg de afspraken uit dat gesprek goed vast en werk de meterkastkaart bij.

Feedback van jullie kan leiden tot een verbeterde volgende versie (huidig: versie 0.1). Mail daarom jullie suggesties graag naar vereniging@debibliotheken.nl.

Aan de slag

Dit stuk bevat een set aan maatregelen die de bibliotheek voorafgaand kan treffen, om zo beter voorbereid te zijn wanneer zich een ernstig incident voordoet. Deze maatregelen zijn algemeen ingestoken, maar óf en hoe een maatregel wordt ingevoerd is maatwerk. Het hangt bijvoorbeeld samen met mogelijke andere beveiligingsmaatregelen die de bibliotheek al heeft getroffen om de impact van een incident te beperken.

De maatregelen zijn verdeeld in categorieën die de mate van belang aanduiden. *Als noodzakelijk* (pagina 2) beschouwen we als noodzakelijk voor elke bibliotheekorganisatie. De andere maatregelen beschouwen we als maatwerk-keuzes die voor elke organisatie anders kunnen uitpakken.

Definities

Incident: Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatieverwerkende systemen in gevaar is of kan komen. Let op: het betreft dus niet persé (alleen) persoonsgegevens als het om een beveiligingsincident gaat

CSIRT (computer security incident response team) medewerker: Beschikbaarheid en roosteren zijn belangrijk; één CSIRT medewerker heeft dienst in het service-window. Bij een kleine bibliotheek is de IT manager/coördinator min of meer automatisch ook CSIRT-medewerker.

CSIRT: team: Dit is een centraal team van deskundigen dat zich richt op het aanpakken van IT-beveiligingsincidenten, zoals datalekken en cyberaanvallen. Een CSIRT team biedt zowel reactieve als preventieve beveiligingsmaatregelen. Op dit moment is er géén centrale CSIRT organisatie voor de gehele bibliotheekbranche ingericht.

Noodzakelijk

1. Eén contactpunt

Er moet een centraal telefoonnummer en e-mailadres bestaan waar beveiligingsincidenten gemeld kunnen worden en waar informatie naar gestuurd kan worden.

Denk aan bijv. security@debibliotheeknaam.nl, en een telefoonnummer dat kan worden doorgeschakeld naar de dienstdoende CSIRT-medewerker.

Over het CSIRT-telefoonnummer. Je wil voorkomen dat iemand die een datalek wil melden, eerst moet uitvinden wie er dienst heeft en dan nog eens het bijbehorende nummer moet opzoeken.

De mailbox moet te openen zijn voor de collega's die incidenten behandelen, en met de CSIRT-medewerker(s) moeten afspraken gemaakt worden over bereikbaarheid.

2. Vermoed je een datalek of beveiligingsincident? Direct bellen!

Bij alle medewerkers moet bekend zijn dat het CSIRT-telefoonnummer gebeld moet worden in geval van een incident. Dus niet via e-mail, en ook niet iemand anders bellen of mailen.

Deze werkwijze kan eenvoudig gedeeld worden (1) via een regelmatig terugkerend bericht op het intranet, (2) bij de onboarding-procedure voor nieuwe medewerkers, en (3) met een stickertje op elke laptop en telefoon dat kan worden bedrukt met bijvoorbeeld deze tekst:

Vermoed je een datalek of beveiligingsincident? Bel direct het CSIRT op.....

Stuur aanvullende informatie naar security@debibliotheeknaam.nl.

3. Het belang van de juiste CSIRT-medewerkers...

Wanneer een incident direct op de juiste plek gemeld wordt, is het van belang om de melding goed op te volgen.

De melding wordt in behandeling genomen door de dienstdoende CSIRT-medewerker. Het aantal CSIRT-medewerkers dat past bij de organisatie varieert met de grootte van de organisatie, maar bestaat – ook bij kleine bibliotheken - altijd uit ten minste 2 personen. Zo kan ook bezetting gerealiseerd worden tijdens vakanties, ziekte en roostervrije dagen.

Elke CSIRT-medewerker heeft voldoende kennis van ICT, zodat snel een inschatting gemaakt kan worden van de aard en omvang van het incident. Idealiter heeft de CSIRT-medewerker ook deze kennis en vaardigheden: beveiligingstechnologieën, bekendheid met verschillende soorten dreigingen (malware, phishing, DDoS, social engineering), inzicht in methoden en technieken van aanvallers, sterke communicatieve vaardigheden, analytische vaardigheden, vermogen om te werken onder druk en snel te reageren, is bereid om zichzelf op de hoogte te houden van de nieuwste ontwikkelingen over al het bovenstaande.

Verder is het van belang om afspraken te maken over de bereikbaarheid en beschikbaarheid van het CSIRT-team. Bijvoorbeeld: van 7:00-23:00 op werkdagen en 9:00 - 18:00u in weekends.

Dit betekent dat voor de CSIRT-medewerkers een rooster opgesteld wordt, waarin deze beschikbaarheid wordt geregeld.

Maak met CSIRT-medewerkers onder andere afspraken over de verwachting rond:

- Moet de CSIRT-medewerker volledig nuchter zijn tijdens beschikbaarheidsdienst? Mogelijk aansluiten bij bestaande afspraken met IT-collega's.

- De afspraken bij ziekte en verlof: belt de zieke of verlofnemende CSIRT-medewerker zelf naar een collega om de dienst over te nemen, of wordt het gemeld bij een coördinator die het overnemen van de dienst regelt?

Het is aan te bevelen om de bereikbaarheid van CSIRT-medewerkers af en toe te controleren, om te bewaken dat een incident daadwerkelijk snel in behandeling genomen kan worden.

4. Formeer een crisisteam

Wanneer zich een ernstig incident voordoet (bijv. een ransomware aanval) blijkt het goed om vooraf een crisisteam ingericht te hebben. Een crisisteam is erop gericht om het ernstige incident met prioriteit boven de reguliere bedrijfsvoering te onderzoeken, risico's te mitigeren, en daarover te rapporteren en communiceren.

Het crisisteam bevat de volgende rollen:

- **Regievoerder/crisismanager:** is verantwoordelijk voor het sturen van het proces rond het cyberincident. Voorzitter van het crisisteam. De regievoerder stelt (in overleg) acties en deadlines vast, en monitort dit. Organiseert de overlegmomenten. Zorgt dat de juiste info op de juiste plek komt. Dit moet een persoon zijn met helicopterview, communicatief vaardig, besluitvaardig, recht-door-zee, bij voorkeur een interne collega i.v.m. bekendheid van de organisatie en de mensen, niet de ICT functionaris); door de directeur van tevoren aangewezen. Het kan ook de directeur zelf zijn.
- **ICT functionaris (CIO/CISO/I(C)T manager):** onderzoek en analyse van het incident, forensische sporen van Politie veiligstellen (zie <https://www.politie.nl/binaries/content/assets/politie/nieuws/2022/juni/brochure-stappenplan-cybercrime.pdf>). Los het incident op en beperk / herstel de schade. Zorgt voor een op de crisis aangepaste rolverdeling in het ICT team, waarbij de ICT functionaris zich primair kan bezighouden met de crisis. Bewaakt (ook in deze fase) de systemen van andere dreigingen. Betreft de forensische hulplijn. Informeert KB, betrokken leveranciers. Is een expert met veel kennis van de ICT omgeving van de bibliotheek, beveiligingsmaatregelen van de bibliotheek, en dreigingen. Zie de vaardigheden genoemd bij de CSIRT-medewerker onder 3.
- **Privacy functionaris (privacy officer of functionaris gegevensbescherming):** de privacy functionaris brengt de risico's en maatregelen die verband houden met de privacywetten in kaart, onderzoekt en adviseert over de meldplicht aan de AP en aan betrokkenen. Betreft en informeert de Politie, cyberverzekeraar, juridische hulplijn en de Autoriteit Persoonsgegevens. Adviseert over gegevensbeschermingskwesaties vanuit de risico's voor betrokkenen.
- **Finance functionaris:** Verantwoordelijk voor het beschikbaar maken van middelen en in kaart brengen van kosten die gemoeid zijn met het cyberincident. In verband met de operationele kosten die acties met zich meenemen, maar denk ook aan kaarttegoeden van leden/bezoekers.
- **Publieke dienstverlening functionaris (omvat Frontoffice en klantenservice):** verantwoordelijk voor aan de crisis aangepaste dienstverlening, inclusief de hiervoor benodigde facilitaire voorzieningen (in afstemming met de manager facilitaire diensten). Zorgt ook voor een centraal contactpunt voor klanten/bezoekers/leden, met voldoende bezetting (bijv. telefonisch en e-mail) – of outsourcing.
- **Marketing/communicatie functionaris:** Verantwoordelijk voor interne en externe communicatie, zodat allen over de actuele stand en de gevolgen van het cyberincident geïnformeerd zijn. Communicatie intern aan alle (groepen) medewerkers, en extern aan stakeholders, bezoekers en leden. Besteedt waar noodzakelijk communicatie intern uit, bijvoorbeeld aan educatiemedewerkers voor dBos-scholen. Bijvoorbeeld aan HRM wanneer 'hun' data of systemen betrokken zijn, bijvoorbeeld aan publieke dienstverlening medewerkers wanneer het dienstenaanbod moet veranderen. Ook een secundaire website, en social media hebben aandacht nodig.
- **Directeur:** interne brede communicatie over wat speelt, bekrachtigt besluiten, informeert gemeente, RvT, VOB, verantwoordelijken van de inwonende instellingen (in MFA), en zijn overige netwerk.

- **Support functionaris:** Documenteert het verloop, en geeft algemene ondersteuning aan het crisisteam. Verslaglegging/documenteren, vastleggen van overwegingen en besluiten, acties vastleggen met deadline en eigenaar, tijdlijn in kaart brengen (ook vóór het incident) – en vastleggen hiervan, catering, praktische organisatie: vergaderruimtes / facilitair / schermen. Rapportage en evaluatie organiseren.

Met bepaalde medewerkers moeten afspraken gemaakt worden over beschikbaarheid (op aanwijzing van het crisisteam) ook buiten kantoor tijden en bijvoorbeeld op het vakantieadres.

Procedures van het CSIRT en crisisteam worden op verschillende plekken (ook fysiek) opgeslagen zodat de beschikbaarheid in geval van een incident niet afhankelijk is van de beschikbaarheid van een systeem.

Punt van aandacht. De ICT functionaris heeft vermoedelijk de handen zo vol dat alle minder urgente zaken en kwesties die door anderen kunnen worden opgelost respectievelijk worden uitgesteld of door een ander worden uitgevoerd.

5. Denk vooraf na over keuzes die je in geval van een incident zult moeten maken

- Gaan we in onderhandeling met een hackersgroep?
- Zijn we bereid losgeld te betalen?
- Welke hulplijnen hebben we?
- Belang van openhouden van de bibliotheek versus adequate afhandeling en bescherming gegevens?

6. Welke organisaties moeten gebeld worden?

Bij een ernstig incident moet een aantal partijen worden betrokken of ingelicht, deze staan op de Meterkastkaart. Vul de contactgegevens daar in.

- Er zijn externe hulplijnen georganiseerd die in geval van een crisis extra support kunnen leveren, bijvoorbeeld op het gebied van informatiebeveiliging en privacy.
- Zorg dat een contactenlijst met telefoonnummers van voornamelijk stakeholders en sleutelfiguren / collega's beschikbaar is buiten het eigen systeem, zodat de beschikbaarheid van deze gegevens niet afhangt van één of enkele kritische systemen.
- Informeer ICT medewerkers (ook extern, wanneer zij direct betrokken zijn) over het bestaan van de meterkastkaart, en leg uit wanneer dit 'opgestart' wordt.
- Organiseer dat je snel een secundaire website kunt openen en maken bij een andere leverancier. Eventueel roep je de hulp in van de VOB, om crisiscommunicatie aan leden/gebruikers te kunnen voeren.
- Forensische hulplijn, bijv. Fox IT, EyeSecurity, je cyberverzekeraar, je eigen kantoorautomatisering leverancier. Zorg wel dat je van tevoren afspraken met die partijen gemaakt hebt.
- Juridische hulplijn, bijvoorbeeld een gespecialiseerde jurist van Dirkzwager, of via de gemeente.
- Bereid voor welke organisaties mogelijk geïnformeerd moeten worden. Denk aan: MFA organisaties, overige organisaties die in huis komen bijvoorbeeld vrijwilligersorganisaties, en instrueer wanneer nodig de betreffende collega's over welke boodschap dan verstrekt moet worden.
- De autoriteit persoonsgegevens (AP) moet niet als hulplijn beschouwd worden, er kan wel een meldplicht ontstaan bij de AP. Binnen 72 uur na kennisname van een datalek moet de verwerkingsverantwoordelijke het datalek melden.
- Zorg voor mandatering van de juiste personen, zodat bij eventuele afwezigheid van bepaalde functionarissen ook effectief gehandeld kan worden.

- Er is een secundair communicatiekanaal beschikbaar dat onafhankelijk opereert van de systemen van de bibliotheek. Bijvoorbeeld met privé-e-mailadressen en telefoonnummers. Zorg dat een groep voor (enkel) het crisisteam bestaat waarin communicatie mogelijk is in bijvoorbeeld Signal. Zorg ook voor een alternatief beeldbellen tool.
- Gebruik een veilig communicatiekanaal zoals Signal bij communicatie in de groep. Alleen als er geen reactie in de groep komt bel je. Dat kan via Signal maar ook via de reguliere telefoonnummers.

Borging

- Jaarlijkse check van Signal installaties op betrokken telefoons van medewerkers
- Actualiseer de meterkastkaart
- Actualiseer de medewerkerslijst en bewaar die naast de meterkastkaart

Om een cyberincident te voorkomen is het belangrijk om alles technisch op orde te hebben en te zorgen voor een goede awareness onder de medewerkers.

Sterk aan te bevelen

- Er is een verwerkingsregister dat volledig, juist en actueel is.
- De werking van de procedure en de bereikbaarheid van het CSIRT wordt regelmatig (ten minste jaarlijks) getoetst.
- Zorg dat de mailbox waarin datalekken gemeld kunnen worden voldoende vaak gelezen wordt, zodat snel gehandeld kan worden indien nodig.
- Organiseer regelmatig een cyberoefening.
- Test eens in de praktijk of back-ups kunnen leiden tot een succesvol herstel en vervolgens herstart van de operatie (restore test). Test ook of de back-ups daadwerkelijk immutable zijn. Zorg er ook voor dat de bewaartermijn van de back-ups voldoende ruim is.

Achtergrondinformatie

[Samen tegen cybercrime, Stappenplan voor IT-specialisten \(politie.nl\)](#)

[infographic-cybercrimes-ransomware.pdf \(politie.nl\)](#)

[Cybercrime | politie.nl](#)

[Home | Nationaal Cyber Security Centrum \(ncsc.nl\)](#)

[Home - Informatiebeveiligingsdienst](#)

[Home | Digital Trust Center \(Min. van EZK\)](#)

[Home - Digitale Overheid](#)

[Home | Autoriteit Persoonsgegevens](#)

[Informatiebeveiliging | AIVD](#)

[Home NL - cip-overheid](#)

VOB202311V0.1