Hoe omgaan met secundair slachtofferschap als je organisatie getroffen is door datadiefstal

Inleiding

Niemand wil ermee te maken krijgen: een cyberincident in je organisatie waarbij persoonlijke gegevens van medewerkers worden gestolen. Denk bijvoorbeeld aan NAW-gegevens, telefoonnummers, kopieën van identiteitsbewijzen, informatie over iemands gezondheid, of gegevens over het salaris.

Helaas komen dit soort datadiefstallen steeds vaker voor.[1] Het kan zijn dat deze zonder directe gevolgen blijven voor de medewerkers en als er gevolgen zijn, zijn ze vaak niet direct zichtbaar. De gestolen data kunnen verhandeld worden op de (digitale) zwarte markt en daarna ingezet worden voor frauduleuze activiteiten. Een voorbeeld is WhatsApp-fraude (hulpvraagfraude), waarbij buitgemaakte mobiele telefoonnummers misbruikt worden om mensen te misleiden en verleiden om geld over te maken naar iemand die zich weet voor te doen als een bekende. Een ander voorbeeld is dat criminelen persoonlijke gegevens kunnen misbruiken voor identiteitsfraude door er bijvoorbeeld kredieten mee af te sluiten, omdat zij in het bezit zijn van een gestolen kopie van een geldig identiteitsbewijs.

Deze vorm van slachtofferschap wordt ook wel secundair slachtofferschap genoemd, omdat de slachtoffers betrokken zijn bij een bedrijf dat primair slachtoffer is geworden van datadiefstal en deze betrokkenen er dus in tweede instantie mee te maken krijgen. Secundair slachtofferschap kan grote gevolgen hebben voor slachtoffers, zowel financieel als emotioneel. (Mogelijke) identiteitsfraude kan grote impact hebben op iemands gevoel van veiligheid.

Organisaties die te maken hebben met datadiefstal van gegevens van hun medewerkers kunnen maatregelen treffen om secundair slachtofferschap te voorkomen of te beperken. Ook begeleiden zij soms medewerkers die hiermee in de praktijk te maken krijgen als zij daadwerkelijk slachtoffer worden. In dit document hebben wij enkele adviezen en maatregelen uit de dagelijkse praktijk op een rij gezet. Ook maken we inzichtelijk wat organisaties kunnen doen om het risico op datadiefstal en secundair slachtofferschap van hun medewerkers in de toekomst te voorkomen.

Voor een aantal van de adviezen geldt dat timing belangrijk is. Als bijvoorbeeld na een datadiefstal onduidelijk is of kwaadwillenden nog toegang hebben tot het netwerk van de organisatie, kunnen zij kennis nemen van getroffen maatregelen of opnieuw een datadiefstal plegen. Het is daarom aan te raden om vervolgstappen goed af te stemmen met juristen én met degenen die technisch onderzoek uitvoeren naar een incident zodat de juiste timing kan worden bepaald.

Hoe dit document te gebruiken

Dit document richt zich primair op organisaties die te maken hebben (gehad) met datadiefstal en wiens medewerkers het risico lopen op secundair slachtofferschap. In dit document geven we adviezen die gebruikt kunnen worden tijdens verschillende fasen van het afhandelen van zo'n datadiefstal:

1. Wat communiceer je naar medewerkers?
2. Hoe voorkom je dat medewerkers slachtoffer worden van identiteitsfraude?
3. Hoe begeleid je medewerkers die (alsnog) slachtoffer zijn geworden?
4. Wat kan je doen om schade door datadiefstal (in de toekomst) te beperken?

Iedere organisatie maakt zijn eigen keuzes bij het afhandelen van cyberincidenten. De adviezen in dit document kunnen als leidraad worden gebruikt om een eigen aanpak mee vorm te geven.

Tot slot merken we op dat niet alleen medewerkers, maar ook andere bij een organisatie betrokken natuurlijke personen geraakt kunnen worden door een datadiefstal, denk aan samenwerkingspartners of klanten als dit consumenten zijn. Veel van de adviezen in dit document zijn ook voor hen relevant.

[1] In 2023 zijn er 1313 datalekken gemeld bij de AP die zijn ontstaan door hacking/malware/phishing. Een deel hiervan gaat over datadiefstal zoals bedoeld in dit document - https://www.autoriteitpersoonsgegevens.nl/uploads/2024-04/Rapportage%20datalekken%202023.pdf

1. Communicatie over datadiefstal van persoonlijke gegevens

Medewerkers van een organisatie kunnen na een datadiefstal bezorgd zijn dat hun gegevens misbruikt zouden kunnen worden. Het is goed om dit als realiteit onder ogen te zien. Het is niet te zeggen of het gebeurt, maar het helpt om hier in de communicatie naar medewerkers realistisch over te zijn zonder hen te angstig te maken. Het hóéft niet te gebeuren, maar het kán wel. Medewerkers reageren hier over het algemeen erg verschillend op. Sommige medewerkers gaan over tot de orde van de dag, maar anderen kunnen zich hier erg zorgen over maken. Het is goed om hier oog voor te hebben en medewerkers bij dit soort zorgen ondersteuning en handelingsperspectief te bieden, ofwel vanuit de eigen organisatie, ofwel via doorverwijzing naar externe ondersteuning, zoals Slachtofferhulp Nederland en Centraal Meldpunt Identiteitsfraude (CMI, zie relevante informatiebronnen).

Het is belangrijk om na een datadiefstal slachtoffers transparant te informeren over welke data (mogelijk) van hen gestolen zijn. Wees daarbij zo compleet mogelijk, zodat zij bij een eventueel gebruik van hun data door kwaadwillenden niet worden verrast. Denk aan NAW-gegevens, kopieën van identiteitsbewijzen, salarisinformatie, ziekteverzuiminformatie, herstelplannen, etc. Geef openheid van zaken en vertel wat je wel en niet weet, wat er nog wordt onderzocht en wat niet kan worden uitgesloten.

Overweeg verder om de volgende onderwerpen in deze communicatie mee te nemen:

- Welke actie(s) de organisatie onderneemt en welke de medewerkers en/of klanten kunnen ondernemen om de impact van de datadiefstal op het individu te minimaliseren.
- Dat de organisatie zelf op sporen van identiteitsdiefstal monitort (als dat het geval is).
- Dat de organisatie melding heeft gemaakt bij de Autoriteit Persoonsgegevens en andere relevante instanties om ervoor te zorgen dat alle wettelijke vereisten worden nageleefd.

Vervolgens is het van belang om toe te lichten hoe de gestolen gegevens eventueel misbruikt kunnen worden zodat medewerkers inzicht krijgen in de kans dat zo'n situatie optreedt en de effecten ervan als het daadwerkelijk gebeurt. Cybersecuritydienstverleners kunnen hier eventueel ondersteuning bieden met concrete voorbeelden uit de praktijk. In elk geval is het goed als medewerkers alert zijn op de volgende zaken, nadat hun data is gestolen:

- Phishing-berichten met besmette links of bijlagen.
- Hulpvraagfraude: verzoeken om aan (zogenaamde) bekenden onverwachts plotseling een grote geldsom over te maken.
- Onduidelijke afschrijvingen op de eigen bankrekening of creditcard.
- Brieven of e-mails waarin wordt bevestigd dat iemand een krediet heeft afgesloten terwijl de medewerker dat niet zelf heeft geïnitieerd.

Tot slot is het belangrijk om de medewerkers een concreet handelingskader te bieden. Leg dus niet alleen uit wat ze kunnen verwachten (bijvoorbeeld een phishing-bericht), maar ook hóe ze daar het beste op kunnen reageren (bijvoorbeeld checken van URL van een link voordat je erop klikt). Zo biedt je een concreet handelingspersectief en bied je een medewerker houvast.

Zorg dat werknemers toegang krijgen tot een betrouwbaar, makkelijk vindbaar en bereikbaar informatiekanaal waar ze vragen kunnen stellen en actuele informatie voorhanden is over de datadiefstal, de gevolgen ervan en hoe ze er het beste mee kunnen omgaan. Ook kan via dit kanaal voorlichting worden gegeven over identiteitsfraude. Op de website van het CMI is informatie beschikbaar die hierbij gebruikt kan worden. Het CMI kan zelf ook tips aan medewerkers geven om identiteitsfraude te voorkomen en advies geven en ondersteuning bieden wanneer er daadwerkelijke sprake is van identiteitsdiefstal.

2. Verkleinen van risico's van secundair slachtofferschap

Organisaties kunnen na een diefstal additionele ondersteuning bieden aan hun medewerkers om het risico van secundair slachtofferschap te beperken. Dit is vooral van belang bij de meest gevoelige gestolen informatie zoals een kopie van identiteitsbewijzen. Kijk altijd of u naast de algemene ondersteuning aan al uw medewerkers bijzondere aandacht moet geven aan specifieke medewerkers, bijvoorbeeld omdat zij persoonlijk extra kwetsbaar zijn, of een bijzondere positie binnen uw organisatie bekleden die kan zorgen voor extra kwetsbaarheid.

IDENTITEITSBEWIJZEN VERVANGEN

Als er digitale kopieën van persoonlijke identiteitsbewijzen (zoals Europese identiteitskaarten en paspoorten) zijn gestolen, dan is een verstandige maatregel om het identiteitsbewijs te (laten) vervangen door nieuwe en de oude ongeldig te laten verklaren door de gemeente. Dit wordt dan opgenomen in het VIS (Verificatie Identificatie Systeem). Meerdere organisaties, waaronder financiële instellingen, raadplegen dit systeem om te kijken of een document nog geldig is. Daarnaast staat na zo'n melding het document ook als ongeldig te boek in de Basis Registratie Personen (BRP). Verder is het mogelijk om een melding te maken bij de politie. Dat helpt de politie bij hun onderzoek als zij deze gegevens tegenkomen.

Het is goed om dit aan de getroffen medewerkers te adviseren en uitleg te geven hoe zij dit moeten regelen. Het is prettig voor medewerkers als zij een stappenplan van de organisatie ontvangen over hoe zij nieuwe identiteitsbewijzen kunnen aanvragen en hun oude ongeldig kunnen laten verklaren. In elk geval kan verwezen worden naar de website van de Rijksoverheid (zie relevante informatiebronnen). Ook kan een organisatie ervoor kiezen om de vervanging van identiteitsbewijzen geheel of gedeeltelijk aan de medewerker te vergoeden.

TOEGANGSPASSEN VERVANGEN

Als ook de gegevens van de toegangspassen zijn ontvreemd, is het niet ondenkbaar dat kwaadwillenden deze willen gebruiken in een poging om toegang te krijgen tot uw pand(en). Als dat een reëel risico is, dan is het verstandig om de toegangspassen te vernieuwen.

WIJZIGEN VAN WACHTWOORDEN

Als de wachtwoorden van medewerkers onderdeel zijn van een datadiefstal is het verstandig om deze voor iedereen te resetten. Wijs medewerkers er in dit geval op dat zij een risico lopen als het wachtwoord dat zij binnen de organisatie gebruiken ook door hen op andere plekken wordt gebruikt. Adviseer werknemers in dat geval om ook hun wachtwoorden bij belangrijke online (privé)accounts te wijzigen. Geef richtlijnen voor het maken van sterke unieke wachtwoorden, het aanzetten van multifactor-authenticatie en het gebruik van wachtwoordmanagers.

MONITOREN VAN MOGELIJKE FRAUDE

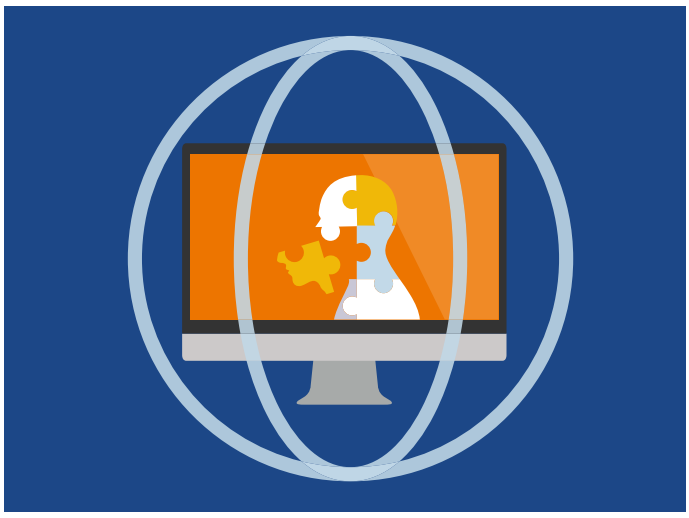
Spoor werknemers aan om in de periode na een datadiefstal enkele maanden hun bankrekeningen en BKR-registraties regelmatig te controleren op verdachte transacties en/of registraties. Geef toelichting hoe ze dit kunnen doen. Bied eventueel de mogelijkheid aan voor medewerkers om kosteloos voor hen te monitoren op sporen van identiteitsdiefstal.

MEDEWERKERS WIJZEN OP WAT ER OVER HEN TE VINDEN IS OP INTERNET

Tegenwoordig maken veel mensen gebruik van sociale media, zowel privé (bijvoorbeeld Instagram, Facebook of Snapchat), maar ook zakelijk (bijvoorbeeld LinkedIn). Op het moment dat kwaadwillenden beschikken over persoonlijke informatie die zij willen misbruiken, kunnen zij via social media de missende puzzelstukjes soms invullen waarmee het makkelijk wordt om identiteitsfraude te plegen. Het is daarom goed om medewerkers door deze bril opnieuw te laten kijken naar de informatie die zij zelf beschikbaar maken op het Internet.

Elementen waar medewerkers op kunnen letten zijn:

- Welke persoonlijke informatie is vrijelijk via de profielen beschikbaar? Denk aan: mobiele telefoonnummers, e-mailadressen of zelfs NAW-gegevens.
- Wat post een medewerker over zijn persoonlijke leven door middel van visuele media zoals foto's en filmpjes? Bijvoorbeeld foto's van iemands interieur, kinderen, huisdieren, vakanties, etc.
- Is voor iedereen alles in de profielen zichtbaar? Bij de meeste sociale media kan je instellen wie de informatie mag bekijken. Hoe opener een medewerker is, hoe meer informatie beschikbaar is voor kwaadwillenden om te gebruiken.
- Medewerkers zouden zelf kunnen uitzoeken wat er precies vindbaar is door anoniem op internet hun eigen profielen te bezoeken.



3. Begeleiden van medewerkers die slachtoffer zijn geworden

En dan gebeurt het (alsnog): één of meer van uw medewerkers krijgen persoonlijk te maken met kwaadwillenden die de bij u gestolen data misbruiken. Het is voor medewerkers fijn als u dan ook klaar staat om hen te ondersteunen. Richt een meldpunt in waar uw medewerkers een melding kunnen doen van een verdachte situatie danwel vastgesteld misbruik van de gestolen persoonsgegevens. Zorg dat u bij een melding klaarstaat met professionele ondersteuning, of weet hoe u die zelf kunt inschakelen.

Stimuleer medewerkers om een melding bij u te maken. Zo krijgt u zelf ook zicht op de omvang van het misbruik en kunt u de informatie uit de meldingen gebruiken om andere medewerkers te waarschuwen voor specifiek misbruik.

In het meldpunt is het verstandig om in elk geval de volgende zaken mee te nemen:

1. Indien er sprake is van identiteitsfraude, dan kan de medewerker een melding doen bij het Centraal Meldpunt Identiteitsfraude (CMI) van de overheid. Na een melding neemt een medewerker van het CMI contact op met de melder om advies te geven en betrekt waar nodig ketenpartners zoals de Belastingdienst, politie of de Rijksdienst Wegverkeer (RDW).
2. Maak onderscheid tussen praktische en emotionele begeleiding. Maak een draaiboek als bepaalde vormen van misbruik vaker voorkomen zodat vergelijkbare situaties op dezelfde manier worden begeleid. Zorg dat helder is welke hulproutes beschikbaar zijn, zowel voor praktische als emotionele begeleiding.
3. Communiceer naar getroffen medewerkers welke stappen zij verder nog kunnen nemen als blijkt dat zij vaker dan incidenteel worden geraakt. Denk aan een melding maken bij specifieke instanties, zoals het doen van aangifte bij de politie, een melding maken bij de Fraudehelpdesk, contact opnemen met financiële instanties om additionele ondersteuning te vragen, het veranderen van e-mailadressen en telefoonnummers.
4. Mogelijk wil een medewerker aangifte doen bij de politie. Zorg dat informatie over hoe dat in zijn werk gaat voor de medewerker beschikbaar is.
5. Als er sprake is van hulpvraagfraude via WhatsApp, kan een medewerker het telefoonnummer in WhatsApp rapporteren en daarna blokkeren.
6. Het faciliteren van juridische bijstand.

Bij al deze zaken is het goed om na te denken hoe lang deze ondersteuning aan medewerkers moet worden geboden en ook hoe om te gaan met ex-medewerkers die slachtoffer worden nadat ze uit dienst zijn getreden.

4. Beperken van schade door datadiefstal

Er valt veel te zeggen over goede beveiliging in het algemeen. Digitale veiligheid is in veel gevallen bovendien maatwerk dus in algemene zin is het lastig om hierover zonder context een goed advies te geven. Desalniettemin zijn er wel een aantal algemene principes die kunnen helpen om schade als gevolg van datadiefstal te beperken.

ZICHT OP DE DATA VAN EEN ORGANISATIE

In de praktijk blijken veel organisaties te worstelen met het beheer van de data met persoonsgegevens. Het is belangrijk om in elk geval te identificeren welke informatie in een organisatie aanwezig is en waar deze is opgeslagen, bijvoorbeeld:

- Gedeelde mappen op file servers
- Publieke cloudopslag providers (bijvoorbeeld Microsoft SharePoint)
- Back-up locaties
- Mailboxen van werknemers

Welke data is opgeslagen op welke locatie verandert veelal met de tijd. Het is daarom belangrijk om periodiek te checken of deze nog actueel is. Ook kan worden overwogen om af en toe assessments uit te voeren om vast te stellen of gevoelige data niet per ongeluk op de verkeerde plek zijn opgeslagen.

DATAMINIMALISATIE

Data die er niet zijn, kunnen ook niet worden gestolen. Een open deur zo lijkt het, maar het komt helaas vaak voor dat er veel meer gegevens aanwezig zijn dan strikt noodzakelijk is. Mogelijke maatregelen voor dataminimalisatie zijn:

- Verwijderen van data die niet meer nodig zijn en waarvoor de bewaartermijnen zijn verstreken. Het komt bijvoorbeeld voor dat medewerkers die niet meer in dienst zijn ook nog secundair slachtoffer worden.
- Het offline archiveren van data die niet dagdagelijks nodig zijn.
- Het offline halen van informatie die online beschikbaar is gemaakt.

EXTRA BESCHERMING VAN DE DATA

Niet alle medewerkers hebben te allen tijde toegang nodig tot persoonlijke gegevens (of andere bedrijfsgevoelige informatie). Mogelijke maatregelen voor extra bescherming zijn:

- Het beperken van toegang tot data tot alleen die medewerkers die er toegang toe nodig hebben. Denk na over het opslaan van de data en op welke plekken dat gebeurt. Het komt regelmatig voor dat kopieën van identiteitsbewijzen en gevoelige data op een FileShare staan voor veel medewerkers toegankelijk is. Er kan ook netwerksegmentatie overwogen worden om informatie beter af te schermen voor medewerkers die er geen toegang toe nodig hebben.
- Het realiseren van een extra toegangscontrole voor toegang tot data.
- Het toepassen van encryptie bij gevoelige data. Sommige data, zoals kopieën van identiteitsbewijzen, moeten weliswaar bewaard worden, maar worden dagdagelijks niet of nauwelijks gebruikt. Door ze versleuteld op te slaan, is het voor kwaadwillenden moeilijker om er toegang toe te krijgen.
- Kopieën van identiteitsbewijzen kunnen door de organisatie van een watermerk worden voorzien. In zo'n watermerk kan bijvoorbeeld de naam van de organisatie en een datum worden opgenomen. Hierdoor is zo'n kopie minder bruikbaar om fraude mee te plegen. Ook kunnen delen van de bewijzen die niet nodig zijn voor de vastlegging worden zwartgelakt. Dit kan een medewerker met de KopieID-app van de overheid zelf doen.
- Er kan maskering op specifieke gegevens worden toegepast op gevoelige data waarmee gewerkt wordt zoals creditcard- en bankrekeninggegevens (voorbeeld: *******8561).
- Het gebruiken van Data Loss Prevention (DLP) tools om te bewaken dat informatie de organisatie niet ongeautoriseerd verlaat. Specialisten kunnen ondersteunen bij advies en implementatie van dit soort tools. Bij gebruik van dit soort tools moeten de data in een organisatie veelal goed geclassificeerd zijn opgeslagen. In veel gevallen is dat een oplossing die een significante investering vraagt om adequaat in te richten en te onderhouden.
- Met behulp van netwerk monitoring kan alarm worden geslagen als onverwachts grote hoeveelheden data in korte tijd de systemen van een organisatie verlaten.
- Met behulp van zogeheten "canary files" kan alarm worden geslagen bij het uitlezen van mappen met gevoelige data. Canary files zijn bestanden waaraan alarmeringen zijn gekoppeld op het moment van uitlezen. Deze bestanden dienen geplaatst te worden in mappen met gevoelige gegevens.

VOORBEREIDING OP EEN INCIDENT MET DATAVERLIES

Het is altijd goed om voorbereid te zijn op het moment dat er iets mis kan gaan. Daarom is het verstandig om vast na te denken over een plan van hoe om te gaan met een datadiefstal. Neem in dit plan in elk geval op welke processen bij een incident moeten worden doorlopen, wie daarbij betrokken moeten worden (intern en extern) en wat de communicatiestrategie zou moeten zijn. Eventueel kunnen er ook al templates voor de communicatie worden voorbereid zodat in geval van nood snel kan worden geschakeld. Neem in het plan ook mee dat tijdens een incident in een logboek wordt vastgelegd welke stappen zijn genomen. Dat is prettig als er vragen komen, maar ook om later lessen uit te trekken.

Relevante informatiebronnen

Centraal Meldpunt Identiteitsfraude (CMI)	https://www.rvig.nl/cmi
Rijksdienst voor Identiteitsgegevens (RVIG)	https://www.rvig.nl/
Slachtofferhulp Nederland	https://www.slachtofferhulp.nl/
Informatie over vervangen van identiteitsbewijzen	https://www.rijksoverheid.nl/onderwerpen/paspoort-en-identiteitskaart/vraag-en-antwoord/wat-moet-ik-doen-als-ik-mijn-paspoort-of-identiteitskaart-kwijt-ben https://www.rijksoverheid.nl/onderwerpen/paspoort-en-identiteitskaart/vraag-en-antwoord/waar-en-hoe-kan-ik-een-paspoort-of-identiteitskaart-aanvragen

Colofon

Auteur:
Petra Oldengarm[2]

Jaar van uitgave:
2025

Vormgeving en lay-out:
Cooler Media BV

Dit is een gezamenlijke uitgave van het project Melissa, een samenwerking in het kader van het bestrijden van ransomware tussen Cyberveilig Nederland, Nationaal Cyber Security Centrum, Openbaar Ministerie, Politie, Computest, Data Expert, Deloitte, ESET, Eye Security, Fox-IT, Kennedy Van der Laan, NFIR, Northwave, Tesorion en Trellix

Contactgegevens
E-mail: info@cyberveilignederland.nl
Telefoon: 088 - 118 25 10

[2] Directeur Cyberveilig Nederland