Bezoekadres
Turfmarkt 147
2511 DP Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

I www.cybersecurityraad.nl
T 070 751 5333 (secretariaat)
E info@cybersecurityraad.nl

Minister van Justitie en Veiligheid
Dhr. prof. mr. F.B.J. Grapperhaus

Datum
11 februari 2020

Onderwerp
CSR Advies
'Meldplicht Datalekken'

Excellentie,

De Cyber Security Raad (hierna de raad) is een nationaal en onafhankelijk strategisch adviesorgaan van het kabinet en het bedrijfsleven (via het kabinet) als het gaat om cybersecurity in Nederland en is samengesteld uit hooggeplaatste vertegenwoordigers uit de publieke, private en wetenschappelijke sector. Door deze unieke samenstelling bekijkt de raad de nationaal strategische cybersecurity-uitdagingen vanuit meerdere invalshoeken en worden gewogen strategische adviezen aan het kabinet en het bedrijfsleven gegeven. Daarbij houdt de raad oog voor de economische kansen die cybersecurity ons land kan bieden.

De raad vraagt uw aandacht voor het volgende.

Nederland kent sinds 1 januari 2016 een meldplicht datalekken. Na de invoering van de Algemene Verordening Gegevensbescherming (AVG) op 25 mei 2018 geldt in de hele Europese Unie dezelfde wet- en regelgeving omtrent gegevensbescherming, waaronder ook een meldplicht datalekken. Dit houdt in dat organisaties verplicht zijn melding te doen van een datalek bij de Autoriteit Persoonsgegevens (AP).

De meldplicht datalekken genereert elk jaar een substantiële hoeveelheid data rondom veiligheidsincidenten waarbij persoonsgegevens zijn betrokken. Nadere analyse van deze informatie kan tot aanbevelingen leiden ter verbetering van de informatiebeveiliging. De AP is bereid deze informatie, uiteraard onder bepaalde voorwaarden, beschikbaar te stellen voor onderzoek. De raad en de AP zijn in nauw overleg tot het advies gekomen om een project uit te voeren om de meerwaarde van het beschikbaar stellen van deze informatie voor onderzoek vast te stellen. Het in overleg opgestelde projectvoorstel is aangehecht als **Bijlage 1**.

Aanleiding

Het advies om datalekmeldingen beschikbaar te stellen voor onderzoek sluit aan op het in september 2019 gepubliceerde rapport van de WRR met als titel 'Voorbereiden op digitale ontwrichting'[1]. In dit rapport wordt opgeroepen tot het breder delen van incidentdata. Ook de meldingen van datalekken bij de AP worden daartoe gerekend.

[1] Adviesrapport 'Voorbereiden op digitale ontwrichting', Wetenschappelijke Raad voor het Regeringsbeleid (WRR), september 2019

Het advies hangt ook samen met een onderzoek dat in opdracht van de raad is uitgevoerd en heeft geresulteerd in het rapport met als titel *Scientific research data breach notification obligation*[2]. In dit rapport wordt gewezen op het belang van het breder beschikbaar stellen van datalekmeldingen. Het onderzoek is in opdracht van de raad uitgevoerd door de Erasmus Universiteit en de Technische Universiteit Delft.

Bijdrage verhoging cyberweerbaarheid door verkrijgen van meerwaarde meld-informatie

Informatie over datalekken vormt een belangrijke bron voor inzicht in de daadwerkelijke effecten van veiligheidsmaatregelen (of het ontbreken daarvan). Beter onderzoek naar de effecten ervan zorgt ervoor dat organisaties beter weten in welke veiligheidsmaatregelen ze moeten investeren. Cyberverzekeringen zullen hierdoor mogelijk meer ingang vinden, waardoor verzekeraars het basisniveau qua veiligheidsmaatregelen kunnen verhogen als onderdeel van de polisvoorwaarden.

De raad vindt informatie-uitwisseling van belang om de cyberweerbaarheid van ons land in het algemeen en organisaties in het bijzonder te verhogen en heeft in juli 2017 hier in het CSR-advies *'Naar een landelijk dekkend stelsel van informatieknooppunten'*[3] bij toenmalige minister van Veiligheid en Justitie op aangedrongen. Het tijdig beschikken over de actuele en betrouwbare informatie is van groot belang voor de digitale weerbaarheid van organisaties in zowel publieke als private sectoren. Het delen en analyseren van informatie maakt het mogelijk om de weerbaarheid van organisaties te vergroten tegen cyberincidenten en/of de schade ervan te beperken. Het is een cruciale randvoorwaarde om de kansen die de digitalisering met zich meebrengt ook daadwerkelijk te kunnen verzilveren, dreigingen het hoofd te bieden, veilig en betrouwbaar zaken te doen en fundamentele rechten en waarden te beschermen.

Creëren van een onderzoeksomgeving voor analyse datalekmeldingen

De raad stelt daarom voor om een project te starten om de meerwaarde te toetsen van het beschikbaar stellen van het bestand met datalekmeldingen aan onderzoekers. Het doel van het project is om vast te stellen welke inzichten rondom privacy en beveiliging van persoonsgegevens kunnen worden afgeleid uit de meldingsdata en/of (en zo ja, onder welke voorwaarden) dit soort analyses structureel kunnen worden uitgevoerd na de projectfase. Meer informatie over de opzet en de randvoorwaarden van het project is opgenomen in **Bijlage 1** van deze brief.

Advies

De raad constateert dat het voor Nederland waardevol is de meerwaarde te bepalen van het breder delen van de informatie uit datalekmeldingen. De mogelijkheid om op deze manier te leren van incidenten is in Nederland vooralsnog niet of nauwelijks aanwezig. Om die reden adviseert de raad het onderzoeksproject, zoals hiervoor beschreven, te starten. Mede met dit project kunnen we onze kansen voor een open, veilig en welvarend digitaal Nederland verzilveren.

---

[2] Report 'Scientific research data breach notification obligation', Michel van Eeten, Bernold Nieuwesteeg, Michael Faure, November 2018

[3] Naar een landelijk dekkend stelsel van informatieknooppunten, advies inzake informatie-uitwisseling met betrekking tot cybersecurity en cybercrime, CSR-advies 2017, nr. 2

In Bijlage 1 is uitgewerkt hoe de onderzoeksomgeving gecreëerd wordt om onderzoek mogelijk te maken. Het project heeft een looptijd van anderhalf jaar. De AP heeft berekend dat voor een adequate uitvoering van het project € 177.000,- benodigd is. Tevens heeft de AP aangegeven zelf niet over dit bedrag te beschikken.

Uitkijkende naar uw reactie verblijven wij,

Namens de Cyber Security Raad,

Hans de Jong
Covoorzitter CSR

Pieter-Jaap Aalbersberg
Covoorzitter CSR

Bijlage 1: Onderzoeksomgeving bestand datalekken

Inleiding

Sinds 2016 geldt in Nederland de meldplicht datalekken. Organisaties moeten een datalek melden aan de Autoriteit Persoonsgegevens (AP), tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor de personen waarvan de gegevens zijn gelekt. Daarnaast moet een datalek worden gemeld aan de getroffen personen wanneer het lek waarschijnlijk een hoog risico voor hen oplevert.

Het aantal meldingen stijgt. In 2017 ontving de AP 10.000 meldingen. In de eerste helft van 2019 ontving de AP al 11.906 meldingen van datalekken. Dat komt neer op ongeveer 2.000 meldingen per maand. Het aantal datalekmeldingen over geheel 2019 zal waarschijnlijk uitkomen op ongeveer 24.000; een stijging van 14 procent ten opzichte van 2018.

Het bestand met daarin de datalekmeldingen bevat interessante informatie. Nadere analyse van de gegevens levert waarschijnlijk inzichten op die bij kunnen dragen aan de verbetering van de cyberveiligheid. Met het oog daarop wil de AP het bestand beschikbaar stellen om onderzoek te kunnen uitvoeren. De AP is daarmee bereid om in te gaan op het verzoek van de raad om een onderzoeksomgeving te realiseren voor de analyse van datalekmeldingen. De aanpak is in dit document opgenomen. Het project vindt plaats onder verantwoordelijkheid van de AP.

De AP publiceert twee keer per jaar een Datalekrapportage. In deze halfjaarlijkse rapportage wordt inzicht geboden in de aard van de meldingen en worden aanbevelingen gedaan gericht op het verbeteren van de beveiliging. In september 2019 was de rapportage specifiek gericht op de zorgsector. Door de datalekmeldingen te delen met onderzoekers is de verwachting dat de halfjaarlijkse datalekrapportages kunnen worden verrijkt. Voor de onderzoekers biedt het project daarnaast de mogelijkheid om vernieuwende onderzoeksvragen te kunnen beantwoorden die helpen bij het veiliger maken van Nederland door de meldingsdata te kunnen analyseren en verrijken met andere datasets.

Doel

De AP realiseert een onderzoeksomgeving met als doel om wetenschappelijke instituten de mogelijkheid te geven om wetenschappelijk of statistisch onderzoek uit te voeren en de gegevens uit het datalekkenbestand te duiden, teneinde te komen tot algemene adviezen en aanbevelingen ter verbetering van de beveiliging van persoonsgegevens.

Bestand bij het Centraal Bureau voor de Statistiek (CBS)

De onderzoeksomgeving krijgt vorm door het bestand met datalekmeldingen beschikbaar te stellen aan het CBS. Hiermee creëert de AP ook de mogelijkheid dat het bestand voor statistische doeleinden gekoppeld kan worden aan andere relevante databestanden waarover het CBS beschikt. Het CBS heeft veel ervaring met de beveiliging van dit soort bestanden en met het regelen van ‘begeleide toegang’ tot de bestanden.

De AP maakt daarover nadere afspraken met het CBS. De dienstverlening vanuit het CBS om externe onderzoekers toegang te geven vindt plaats binnen de zogeheten Remote Access-omgeving[4].

Persoonsgegevens uit het bestand

Persoonsgegevens worden vóór de overdracht aan het CBS door de AP uit het bestand verwijderd. Hierbij gaat het in de eerste plaats om de naam van de contactpersoon bij de organisatie die de melding doet. Daarnaast gaat het incidenteel om andere persoonsgegevens, bijvoorbeeld van de betrokkene(n) waarvan de gegevens gelekt zijn. Ook bedrijfsnamen waaruit een persoonsgegeven kan worden afgeleid, worden verwijderd. Het nummer van de Kamer van Koophandel (KvK) van een bedrijf organisatie wordt wel meegenomen in de database die aan het CBS wordt verstrekt, teneinde koppelingen met andere (statistische) bestanden mogelijk te maken. Het over te dragen bestand bevat daarmee nog persoonsgegevens, met name voor zover het eenmanszaken betreft. De CBS zal vervolgens het KvK-nummer omzetten in een ander nummer voordat zij het bestand beschikbaar stellen in de Remote Access-omgeving. Dit om herleidbaarheid tot personen te verminderen en om vertrouwelijk om te gaan met bedrijfsgegevens.

De datalekmeldingen worden periodiek overgedragen aan het CBS, met een nog nader te bepalen frequentie.

Voorwaarden voor toegang tot het bestand bij CBS (Remote Access omgeving)

Onderzoekers van wetenschappelijke instituten kunnen een projectvoorstel voor onderzoek indienen waarbij ze gebruik kunnen maken van de datalekgegevens, maar eventueel ook van andere gegevens die bij het CBS beschikbaar zijn voor extern onderzoek. De onderzoekers moeten afkomstig zijn van instituten conform de voorwaarden van het CBS. Onderzoekers krijgen desgewenst onder voorwaarden toegang tot de database om een projectvoorstel op te kunnen stellen. Het CBS heeft een aantal criteria geformuleerd voor het uitvoeren van zogeheten microdata-onderzoek, zie https://www.cbs.nl/nl-nl/onze-diensten/maatwerk-en-microdata/microdata-zelf-onderzoek-doen/aanvraag-toegang-microdata.

De volgende criteria zijn relevant voor de onderzoeksomgeving die de AP creëert:

- De instelling beschikt over een geldige machtiging voor toegang tot microdata.
- De microdata worden alleen gebruikt voor doeleinden van statistische aard, dus niet voor administratieve, gerechtelijke of fiscale doeleinden of voor controledoeleinden tegen individuele personen, bedrijven of instellingen.
- Onder andere vanwege de doelbinding die de AVG voorschrijft, dient de instelling een welomschreven projectvoorstel voor onderzoek in (die in het geval van een exploratief onderzoek ook een globaal karakter mag hebben).
- Het is aannemelijk dat tenminste een aanzienlijk deel van de onderzoeksvragen beantwoord kan worden met CBS-microdata.

[4] Het CBS heeft een Remote Access-omgeving. Die omgeving is bedoeld om externe onderzoekers onder voorwaarden toegang te geven tot de data. Daarnaast kent het CBS ook de Aanvullende Statistische Dienstverlening. Het betreft hier door het CBS uitgevoerd onderzoek naar een specifieke onderzoeksvraag. Via deze dienst kan het CBS rapportages opleveren om de halfjaarlijkse datalekrapportages van de AP te verrijken.

- Indien de instelling zelf bestanden inbrengt ter koppeling met CBS-microdata, zijn deze rechtmatig verkregen, mogen de bestanden verstrekt worden aan het CBS en mogen de bestanden gebruikt worden voor onderzoek.

Met de onderzoekers wordt een overeenkomst opgesteld. In de overeenkomst wordt opgenomen dat de onderzoekers vertrouwelijk omgaan met de informatie in het datalekbestand. De overeenkomst bevat strikte geheimhoudingsbepalingen. Ook wordt vastgelegd dat in de uiteindelijke rapportages geen bedrijfsnamen mogen staan. Over de inhoud van de overeenkomst voert de AP nog overleg met het CBS.

CBS: Aanvullende Statistische Dienstverlening

Naast de Remote Access-omgeving onderscheidt het CBS de Aanvullende Statistische Dienstverlening (ASD). Binnen deze lijn voert het CBS in opdracht statistisch onderzoek uit op de database. Deze statistieken hebben – in tegenstelling tot producten die voortkomen uit de Remote Access omgeving - een 'CBS-keurmerk'. Het CBS is verantwoordelijk voor de kwaliteit van de uitkomsten. De AP wil het CBS vragen om aanvullende statistische analyses uit te voeren met als doel om de halfjaarlijkse datalekrapportages te verrijken.

In termen van de AVG is het CBS verwerkingsverantwoordelijke voor deze verwerking van data.

Kosten voor het onderzoek

De kosten voor het statistische werk van het CBS dat wordt uitgevoerd in opdracht van de AP (binnen ASD), moeten worden gefinancierd. De AP heeft deze kosten niet in haar begroting opgenomen.

De benodigde kosten om het bestand geschikt te maken voor het onderzoek binnen de Remote Access-omgeving zijn opgenomen in bijgesloten begroting voor het project. De aanvullende kosten voor het onderzoek binnen de Remote Access-omgeving van het CBS worden gedragen door de instituten die een projectvoorstel indienen. Aan het werken met CBS-microdata zijn kosten verbonden. Het CBS zal op basis van het projectvoorstel specificeren welke kosten aan het onderzoeksproject zijn verbonden. De kosten zijn mede afhankelijk van de vraag of en zo ja welke onderzoeksactiviteiten het CBS moet verrichten voor het specifieke onderzoek.

Onderzoekscommissie datalekmeldingen

We stellen een onderzoekscommissie datalekmeldingen in. Deze commissie richt zich op toetsing van de projectvoorstellen voor onderzoeken die plaatsvinden binnen de Remote Access-omgeving. De commissie volgt voorts het verloop van het onderzoek en beoordeelt het resultaat van het onderzoek. Bij de beoordeling van het voorgenomen onderzoek gaat de commissie na of het onderzoek valt binnen het hiervoor geformuleerde doel, en of het onderzoek volgens het plan wordt uitgevoerd binnen de gestelde randvoorwaarden. De onderzoeken zijn uitdrukkelijk niet gericht op het openbaar maken van de meldingen van datalekken. Eventuele projectvoorstellen op dit punt worden niet geaccepteerd. Projectvoorstellen die tot doel hebben om na te gaan of openbaarmaking toegevoegde waarde zou hebben vallen eveneens buiten de scope. Bij een positief besluit van de commissie krijgen de onderzoekers toegang tot de dataset binnen de Remote Access-omgeving voor het uitvoeren van het onderzoek.

In de commissie nemen zitting: een vertegenwoordiger van de AP (voorzitter), een vertegenwoordiger van de raad en een vertegenwoordiger van het CBS. Een medewerker van de AP draagt zorg voor het secretariaat.

Publicatie van de resultaten

De resultaten van de onderzoeken worden openbaar gemaakt. De AP heeft het recht om de resultaten eerst te publiceren via de datalekrapportage die de AP twee keer per jaar uitbrengt. Als het om fundamenteel wetenschappelijk onderzoek gaat, wordt ermee rekening gehouden dat eerste publicatie mogelijk via andere wegen plaatsvindt. Hier zal in goed overleg met de commissie een oplossing voor worden gevonden, rekening houdend met de belangen van de AP om resultaten in de datalekrapportages mee te nemen en de belangen van de onderzoekers om tot wetenschappelijke publicatie van onderzoeksresultaten te kunnen komen. Na publicatie van de resultaten in de datalekrapportage kunnen de resultaten van het onderzoek – met bronvermelding – ook via andere wegen door de onderzoekers worden verspreid. De commissie beoordeelt of publicatie in de datalekrapportage, gelet op de aard van het onderzoek, in de rede ligt. Bij de beoordeling van het projectvoorstel, dus bij de start van het project, worden hierover afspraken gemaakt. De rapportages die uit het onderzoek voortkomen zullen geen bedrijfsnamen of uniek identificerende kenmerken van bedrijven/organisaties bevatten. De openbare resultaten zullen nooit herleidbaar zijn naar een bedrijf. Onderzoeken dragen bij aan verbeterde generieke inzichten over informatiebeveiliging en leiden tot adviezen ter verbetering van systemen. Naming & shaming is niet aan de orde. De rapportages bevatten evenmin uitspraken die tot personen herleidbaar zijn.

Evaluatie

Het project heeft een looptijd van anderhalf jaar. Het project start op het moment dat de data beschikbaar komen via de Remote Access-omgeving voor het indienen van projectvoorstellen. Na afloop van het project vindt een evaluatie plaats. De evaluatie wordt voorbereid door de AP in nauw overleg met de raad. De evaluatie heeft tot doel om te bepalen of we een structurele setting kunnen creëren voor de onderzoeksomgeving.

Kosten

Het project wordt onder verantwoordelijkheid van de AP uitgevoerd. De AP heeft berekend dat voor een adequate uitvoering van het project € 177.000,- benodigd is. Tevens heeft de AP aangegeven zelf niet over dit bedrag te beschikken. Het bedrag is als volgt opgebouwd:

Kosten AP: Bestand gereedmaken voor overdracht (het opschonen van persoonsgegevens) en het voeren van het secretariaat voor de in te stellen onderzoekscommissie.	€ 50.000,- (1)
Kosten CBS: Bestand beschikbaar maken voor de RA-omgeving; gericht op halfjaarlijkse beschikbaarstelling (12.000). Inclusief verwerken en koppelen aangeleverde basisgegevens (3 x 6.000).	€ 30.000,- (2)
Kosten CBS: Eerste proeflevering (4.000), opleveren halfjaarlijks basisrapport voor het verrijken van de Datalekrapportage (3 x 6.000), verdiepende rapportage gericht op specifieke onderzoeksvragen AP (3 x 25.000).	€ 97.000,-
Totaal benodigde financiering	**€ 177.000,-**

(1)
Deze kosten zijn nog exclusief de kosten om ook de algemene beschrijvingen uit het datalekbestand geschikt te maken voor een export. Aan het externe bureau dat het datalekbestand in beheer heeft (VISMA) is gevraagd een offerte op te stellen om ook deze velden geschikt te maken voor een export. In deze velden wordt het datalek verder toegelicht (kwalitatieve beschrijvingen). Dat kan voor onderzoekers interessante informatie opleveren. De offerte hiervoor is aangevraagd, maar de exacte kosten zijn nog niet bekend. De AP zal deze kosten voor haar rekening nemen.

(2)
Uitgegaan wordt van halfjaarlijkse leveringen aan het CBS.