Kapteynstraat 1, SBIC - Building suite 220 / 2201 BB Noordwijk

info@cyberveilignederland.nl
www.cyberveilignederland.nl

KvK 71802525

Commissie Digitale Zaken

Noordwijk, 11 mei 2026
Ref.: PA901-251105

Betreft: Schriftelijke inbreng Cyberveilig Nederland over rondetafel Cyberveiligheid

Geachte leden van de commissie Digitale Zaken,

Niemand wil ermee te maken krijgen: een cyberincident waarbij persoonlijke gegevens worden gestolen. Helaas neemt dit soort diefstal toe doordat bij ransomware aanvallen ook steeds vaker sprake is van data-exfiltratie (datalekken),[1] waarbij persoonlijke gegevens van klanten of medewerkers buit worden gemaakt met (de dreiging tot) publicatie van deze gegevens.

Van Ransomware naar data-exfiltratie: een toename van datalekken

Clinical Diagnostics, de gemeente Epe, Rituals, Basic Fit en Odido zijn enkele recente voorbeelden die het nieuws hebben gehaald omdat er sprake was van data-exfiltratie. Na een relatief rustig 2023 en 2024, zien we in 2025 en 2026 een scherpe stijging in het aantal datalekken door accountovernames en gestolen authenticatiegegevens in Nederland.[2] De gevolgen zijn vaak niet direct zichtbaar, maar wel groot voor 'secundaire slachtoffers'[3], burgers wiens data op straat ligt. Gestolen NAW-gegevens, salarisstroken en identiteitsbewijzen vormen de basis voor identiteitsfraude en jarenlange onzekerheid.

Om beter grip te krijgen op de toename van dit fenomeen en in te zetten op betere preventie hiervan heeft Cyberveilig Nederland drie concrete oproepen aan de commissie Digitale Zaken opgenomen in dit position paper.

Oproep: *Cyberveilig Nederland vraagt de commissie om de publieke organisaties, waaronder de AP, NCSC, politie, AIVD en toezichthouders, in samenwerking met het cybersecurity bedrijfsleven en de onderzoekswereld, verder te onderzoeken naar de oorzaken van deze toename en verschuiving van ransomware naar datalekken. De geopolitieke situatie, de inzet van AI en de*

[1] Vanuit project Melissa is hier een whitepaper over geschreven: https://cyberveilignederland.nl/upload/userfiles/files/VCNL_Whitepaper_Exfiltratie_v3_0_Web.pdf
[2] https://www.ncsc.nl/nieuws/jaarbeeld-ransomware-2025
[3] Vanuit project Melissa is hier een handreiking over geschreven: https://cyberveilignederland.nl/actueel/persbericht-samenwerkingsverband-melissa-publiceert-best-practices-secundair-slachtofferschap

verder vercommercialisering van cybercriminelen zijn enkele aanwijzingen die verder uitgezocht dienen te worden om dit fenomeen beter te duiden en tot beter handelingsperspectief te komen.

Governance in het voorkomen van datalekken

Rondom de aanpak en het voorkomen van datalekken zijn een hoeveelheid aan organisaties betrokken:

- **NCSC** en de **AIVD** helpen door het geven van inzicht in de dreigingen en het geven van beveiligingsadviezen.
- **NCSC** heeft, straks onder de Cyberbeveiligingswet (Cbw), de CSIRT-taak. Daarnaast notificeert het NCSC organisaties die kwetsbaar zijn voor mogelijk misbruik van hun systemen.
- **Autoriteit Persoonsgevens (AP)** heeft een controlerende en toezichthoudende taak of organisaties zich aan de privacywet (AVG) houden, onderzoeken datalekken en kunnen ingrijpen met waarschuwingen of boetes als wetten worden overtreden.
- Toezichthouders als de **Rijksinspectie Digitale Infrastructuur (RDI)** en **Inspectie Leefomgeving en Transport (ILT)** krijgen straks onder de Cbw, handvaten om te zorgen dat de basis hygiëne van organisaties op orde is[4] om (de impact van) incidenten te voorkomen.
- **De Politie** en het **Openbaar Ministerie** hebben een rol in het aanpakken van criminelen die datalekken veroorzaken, verhandelen of inzetten voor eigen (crimineel) gewin. Daarnaast notificeert de politie indien mogelijk en zet zij ook steeds meer in op preventieve maatregelen.
- **Cybersecurity bedrijven** leveren diensten aan organisaties die moeten voorkomen dat incidenten ontstaan of staan organisaties bij wanneer een incident heeft plaatsgevonden.

Oproep: *De huidige fragmentatie belemmert een effectieve aanpak. Cyberveilig Nederland vraagt de commissie om zich in te zetten dat er een betere informatie-uitwisseling op gang komt. Zo zou data van de AP over datalekken breder gedeeld kunnen worden met het NCSC, Cbw-toezichthouders en de cybersecuritysector om goede inzichten te krijgen en handelingsperspectief te bieden die datalekken voorkomen. Structurele deelname bij bestaande samenwerkingsverbanden (zoals Project Melissa of programma Cyclotron) is nodig om de informatiepositie in de breedte te versterken.*

Zorgplicht verantwoordelijkheden

Om de impact van incidenten te beperken en data-exfiltatie te voorkomen, moet elke schakel in de keten zijn rol pakken. Zo hebben organisaties een eigen (zorg)plicht om hun basis op orde hebben. Denk hierbij aan:

[4] Zie artikel 21.2 van de NIS2 waarin deze zijn uitgewerkt.

- basishygiëne maatregelen als netwerksegmentatie, tweefactor authenticatie en monitoring van het netwerkverkeer;
- het toepassen van data-minimalisatie. Wat je niet hebt, kan ook niet gestolen worden. Deze data-minimalisatie zou ook een onderdeel moeten zijn van de risico-gebaseerde benadering. Deze gaat vaak over cybersecurity-maatregelen en te weinig over de bescherming van persoonsgegevens.
- regie op (externe) IT-partners. Vaak is de basishygiëne bij externe IT-partners belegd, zeker bij MKB-bedrijven. Heldere afspraken over verantwoordelijkheden, genomen maatregelen en wie wat doet bij een incident is noodzakelijk.

Oproep: *De Cyberbeveiligingswet ziet toe op een aantal maatregelen die vallen onder de zorgplicht. Veel van deze maatregelen voorkomen datalekken. Zorg dat de toezichthouders voldoende mens en mankracht hebben om goed toezicht te houden bij implementatie van de Cbw. Bij invoering van de AVG hebben we geleerd dat de AP dit onvoldoende had. Meteen actief en daadkrachtig optreden is wenselijk om Cbw-entiteiten die cybersecurity nog onvoldoende serieus nemen, en daarmee het risico op datalekken laten toenemen, de juiste maatregelen te laten nemen. Hierbij is het van belang dat het lekken van persoonsgegevens wordt meegenomen in de risico gebaseerde aanpak.*

Daarnaast krijgt het NCSC er bij implementatie van de Cbw een grote taak bij als nationale CSIRT. Het blijft belangrijk dat het NCSC, naast deze wettelijke taak, ook het niet vitale bedrijfsleven van adviezen en handelingsperspectief te blijven voorzien. Houdt het NCSC hierop scherp.

Aanpak secundair slachtofferschap

Helaas valt het niet altijd te voorkomen dat datalekken plaatsvinden. Echter burgers en organisaties die hiervan slachtoffer worden, weten vaak niet waar ze terecht kunnen met hun vragen. Cyberveilig Nederland vraagt de commissie:

- Te zorgen dat er een goed toegankelijk en herkenbaar loket is voor secundaire slachtoffers van datalekken. De Fraudehelpdesk vervult deze rol in de praktijk al voor burgers en (kleine) ondernemers die vragen hebben over wat te doen na een datalek. Gezien de groeiende impact en complexiteit is het van belang om deze functie te versterken, met voldoende structurele middelen en een helder mandaat, zodat slachtoffers tijdig en adequaat ondersteund kunnen worden;
- De drempel te verhogen dat secundaire slachtoffers ook te maken krijgen met identiteitsfraude. Onderzoek hiertoe de mogelijkheden met het Bureau Krediet Registratie (BKR);
- Start een bewustwordingscampagne over de eigen, individuele rol in dataverspreiding, bij voorkeur vanuit Europa. Moeten we al onze gegevens echt delen met alle social media

platformen of omdat een organisatie daar om vraagt? Doen we zelf voldoende om onze eigen gegevens te beschermen of geven we het ook te gemakkelijk weg? Een bewustwordingscampagne kan hierin helpen.

Cyberveilig Nederland staat klaar om samen met u, de overheid, toezichthouders en andere betrokken organisaties de noodzakelijke stappen te zetten. Nu is het moment om de digitale weerbaarheid van Nederland structureel te verankeren en burgers en bedrijven te beschermen tegen datalekken en de impact van incidenten te verkleinen.