provincie limburg

Provinciale Staten

Clustercode	OI	**Uw kenmerk**	-
Ons kenmerk	DOC-00764108	**Maastricht**	8 april 2025
Bijlage(n)	-	**Verzonden**	8 april 2025

Onderwerp
Mededeling portefeuillehouder inzake informatieveiligheid 2024

Geachte Staten,

Zoals te doen gebruikelijk informeren wij uw Staten jaarlijks over de belangrijkste ontwikkelingen en uitgevoerde werkzaamheden op het gebied van informatiebeveiliging van het voorgaande jaar. In navolging van onze mededeling portefeuillehouder van 3-7-2018 (2018/43409) is dit daarmee het 7de opeenvolgende jaar dat uw Staten op deze wijze door ons worden geïnformeerd. Het spreekt voor zich dat wij, indien daar aanleiding voor is, u ook tussentijds zullen informeren over belangrijke ontwikkelingen op dit gebied. Informatiebeveiliging is en blijft een actueel thema, getuige publicaties[1] als: *“Amersfoort erkent dat het gelekte persoonsgegevens te lang bewaard”, “Politie getroffen door datalek: namen alle medewerkers buitgemaakt”, “Nationaal Cyber Security Centrum monitort wereldwijde computerstoring, “Vliegverkeer op Eindhoven Airport platgelegd door netwerkstoring”, “Defensie, Tweede Kamer, Kustwacht en DigiD getroffen door computerstoring”, “GVB verwijdert oplaadautomaten wegens einde support van pinsoftware”, “Smartphoneverbod kabinet vooral te maken met risico op insider threat”, “Maandag geen onderwijs op TU Eindhoven wegens cyberaanval”.*

Het is daarom essentieel om als organisatie waakzaam te blijven op het gebied van informatiebeveiliging en maatregelen te nemen om mogelijke *risico’s* tot een minimum te beperken. Maatregelen die de Provincie Limburg in dit kader neemt, lopen uiteen van de inzet van geavanceerde detectiesoftware tot het verhogen van het informatiebeveiligingsbewustzijn van de medewerkers en van een deugdelijke backup-procedure tot de aanschaf van betrouwbare software. Ook wordt nauw samengewerkt met de andere provincies en worden in IPO-verband gezamenlijke organisatorische stappen gezet, die er in resulteren dat de provincies een betere informatiepositie krijgen over mogelijke (cyber-)dreigingen op dit gebied.

[1] Bron: security.nl

Limburglaan 10
6229 GA Maastricht

Postbus 5700
6202 MA Maastricht

+31 43 389 99 99
www.limburg.nl

De Provincie Limburg volgt de actuele ontwikkelingen op dit gebied en speelt daar op in. Waar nodig wordt opgeschaald in termen van informatiebeveiliging. Dat neemt niet weg dat er altijd een risico blijft bestaan dat ook wij te maken krijgen met cybercriminaliteit en ongeautoriseerde toegang tot gegevens. Immers de wereld van de cybercriminelen innoveert continu en loopt daarmee vaak één stap vóór op de fabrikanten van informatiebeveiligingsoplossingen en andere toepassingen die door de Provincie gebruikt worden.

In 2024 uitgevoerde werkzaamheden i.h.k.v. van informatieveiligheid

Bewustwording informatieveiligheid
De Provincie Limburg heeft in 2018 een programma opgestart dat zich richtte op het vergroten van het bewustzijn inzake het informatieveilig handelen van onze medewerkers. In 2023 is een vervolgprogramma opgestart (ARDA) dat aan iedereen die gebruik maakt van de infrastructuur van Provincie Limburg beschikbaar wordt gesteld. Dit betreft de interne en externe medewerkers, organisaties gehuisvest binnen het Gouvernement en gebruik makend van de ICT-infrastructuur van de Provincie (Omgevingsdienst Zuid Limburg en RIEC Limburg), leden van Gedeputeerde Staten en de leden van Provinciale Staten inclusief burgercommissieleden. Het huidige programma bestaat uit een aantal interventies die 2-maandelijks digitaal aan alle deelnemers beschikbaar worden gesteld. Van alle deelnemers heeft in 2024 ongeveer 71% aan één of meerdere interventies deelgenomen.
Dit programma is een maatregel die valt onder de verplichte training i-bewustzijn, zoals opgenomen onder artikel 7.2.2.2 van de voor overheden verplicht gestelde Baseline Informatieveiligheid Overheid (hierna: BIO[2]).

Gebruik moderne internetstandaarden
Door het gebruik van moderne en betrouwbare internetstandaarden wordt het internet voor iedereen toegankelijker, veiliger en betrouwbaarder. Continu worden aan de hand van de algemeen geaccepteerde Nederlandse controlewebsite internet.nl de websites (domeinen) waar de Provincie Limburg de geregistreerde eigenaar van is getoetst aan de richtlijnen en internetstandaarden van Forum Standaardisatie. Daar waar nodig en mogelijk worden websites aangepast aan de voorgestelde standaarden. De Provincie Limburg stuurt actief op hoge scores op deze controlewebsites en hanteert hierbij het principe “comply or explain”.

Pentest
De Provincie Limburg laat jaarlijks door een extern bureau middels de inzet van ethische hackers een penetratietest (pentest) uitvoeren, teneinde de infrastructuur van Provincie Limburg of delen hiervan door te lichten op mogelijke kwetsbaarheden. In dit kader heeft in Q1 van 2024 een beveiligingsonderzoek van medewerkerslaptops plaatsgevonden. Dit onderzoek leverde een beperkt aantal bevindingen op, die geleid hebben tot enkele aanpassingen van de inrichting van de laptops van de Provincie Limburg.

[2] De Baseline Informatieveiligheid Overheid is een set van uniforme richtlijnen en maatregelen voor informatiebeveiliging binnen de Nederlandse overheid. Het doel is om de beschikbaarheid, integriteit en vertrouwelijkheid van overheidsinformatie te waarborgen.

Omwille van het voorkomen van mogelijk misbruik van kwetsbaarheden worden geen uitspraken gedaan omtrent de aard van de bevindingen uit dit soort onderzoeken.
In 2024 heeft tevens een pilot (onderzoek) plaatsgevonden naar het “aanvalsoppervlak” (zg. attack surface) van de Provincie Limburg. Dit onderzoek richtte zich op het actief zoeken op het zg. dark web[3] naar dreigingsinformatie specifiek gericht op de Provincie Limburg, dan wel op gehackte gebruikersaccounts van de Provincie Limburg.

DigiD audit
Binnen de Provincie Limburg wordt DigiD gebruikt voor de digitale ondertekening (authenticatie) van aanvraagformulieren voor subsidies en voor de toegang tot het subsidieportaal. In 2024 is in verband met deze aansluiting op DigiD door een externe auditor een (verplicht) beveiligingsassessment uitgevoerd. In deze audit is vastgesteld dat de Provincie Limburg voldoet aan de beveiligingseisen die door Logius[4] gesteld worden aan het gebruik van DigiD.
In opdracht van PS is een systeem ontwikkeld dat het uitvoeren van een correctief bindend referendum ondersteund, hierin is eveneens een DigiD-koppeling gerealiseerd. Voor dit systeem is in 2024 een pre-audit uitgevoerd. Vanaf 2025 zal ook deze DigiD-koppeling opgenomen worden in de reguliere DigiD-auditcyclus.

Gebruik geavanceerde signaleringssoftware
De Provincie Limburg heeft sinds 2019 geavanceerde signaleringssoftware in gebruik om zowel kwetsbaarheden te identificeren als om incidenten met mogelijk kwaadaardige software vroegtijdig te weren. In 2024 is het gebruik van deze software verder uitgebreid. Dit heeft geleid tot een sterke integratie van de signaleringsfunctionaliteit binnen de werkprocessen van de beheerorganisatie. Daarnaast is de samenwerking met het externe Security Operations Center (SOC[5]), dat de Provincie ondersteunt met 24/7 monitoring en incidentanalyses, verder geïntensiveerd.

Spamfilter
Over 2024 zijn bijna 3 miljoen externe e-mails ontvangen. Door het centrale spamfilter zijn hiervan ruim 1 miljoen verdachte e-mails automatisch geblokkeerd en verwijderd, waardoor deze niet bij de geadresseerde provinciale medewerkers werden afgeleverd. Dit is ongeveer 33% van de totale hoeveelheid in 2024 ontvangen externe e-mails. Daarnaast zijn in 2024 een kleine 300 e-mails automatisch geblokkeerd en verwijderd, omdat deze een virus bevatten.

[3] Het Dark web, soms ook ‘darknet’ genoemd, is een onderdeel van het wereldwijde web dat onzichtbaar is voor zoekmachines als Google en Bing. Het is een kleine verzameling van anonieme en versleutelde websites waar je niet op kunt komen via je normale browser. Op het dark web is vrijwel geen toezicht of censuur.

[4] Logius is de dienst digitale overheid en onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Logius biedt voorzieningen en standaarden die alle overheidsorganisaties gebruiken in hun digitale dienstverlening.

[5] Een Security Operations Center (SOC) is verantwoordelijk voor het beschermen van een organisatie tegen cyberdreigingen. SOC-analisten monitoren hierbij 24 uur per dag het netwerk van een organisatie en onderzoeken mogelijke beveiligingsincidenten.

Privileged Access Management (PAM)
In 2023 is een begin gemaakt met de uitrol van een Privileged Acces Management[6] oplossing binnen de Provincie Limburg. In 2024 is de uitrol van deze oplossing voor externe gebruikersaccounts met speciale rechten (veelal externe beheerders van hard- en/of softwaretoepassingen) afgerond. Hierdoor wordt de toegang van deze specifieke gebruikers tot applicaties en onderdelen van de provinciale ICT-infrastructuur beter beveiligd en gemonitord.

Firewall/netwerkoptimalisatie
In 2024 is het netwerk van de Provincie Limburg in compartimenten verdeeld, teneinde de beveiliging van het netwerk verder te verbeteren. De resultaten van deze werkzaamheden zullen in 2025 aan de hand van een uitgebreide pentest gecontroleerd worden.

Update ISO-norm naar ISO27001:2022
In 2024 zijn de voorbereidingen gestart voor de implementatie van de ISO27001-norm versie 2022. Dit is een update van de norm die tot nu toe binnen de Provincie Limburg als leidraad is gehanteerd voor de inrichting van onze informatiebeveiligingsorganisatie. Dit betekent dat nieuwe normelementen worden geïmplementeerd en dat oude normelementen die nog steeds actueel zijn verder worden aangescherpt conform de bevindingen uit 2023. Dit maakt onderdeel uit van het continu verbeteren zoals in de ISO-norm en -werkwijze is opgenomen.

CISO als dedicated functie
De Concern Information Security Officer (CISO) was tot medio 2024 als rol belegd bij een senior O&I adviseur. Vooruitlopend op de pensionering in 2025 van de zittende CISO en in het licht van het toenemend belang van beleid en sturing op het gebied van informatiebeveiliging, is binnen de provinciale organisatie in 2024 een dedicated CISO-functie gecreëerd. Deze nieuwe functie is in oktober 2024 ingevuld, waardoor een warme overdracht van taken en werkzaamheden van de vorige naar de huidige CISO heeft kunnen plaatsvinden. De functie van CISO blijft gepositioneerd binnen het cluster Organisatie & Informatie, echter de CISO kan gevraagd en ongevraagd onafhankelijk adviseren aan directie en bestuur.

Interprovinciaal informatieknooppunt informatiebeveiliging
Als onderdeel van de stappen die gezet worden om te komen tot een interprovinciaal informatieknooppunt informatiebeveiliging bestaat er sinds 2023 het interprovinciale ISAC[7]. Het ISAC is een samenwerkingsverband waarbinnen provincies informatie delen over cybersecurity en gevoelige en vertrouwelijke informatie over incidenten, dreigingen, kwetsbaarheden en maatregelen tussen de deelnemers van de provincies worden uitgewisseld. Hierdoor helpen provincies elkaar zich beter te beschermen tegen cyberaanvallen en het minimaliseren van mogelijke gevolgen ervan. Het ISAC is ook in 2024 een aantal keer bij elkaar gekomen.

---

[6] Privileged Access Management is een beveiligingsmethode die beheert en controleert hoe geprivilegieerde accounts — met hoge toegangsrechten tot systemen en gevoelige data — worden gebruikt. PAM minimaliseert het risico op misbruik door toegang te beperken, sessies te monitoren en wachtwoorden veilig op te slaan. Hiermee wordt de kans op interne en externe beveiligingsincidenten verkleind.

[7] ISAC: Information Sharing and Analysis Centre

Daarnaast is er op interprovinciaal niveau het CIBO (Centraal Informatie Beveiligingsoverleg), waarin de CISO's van alle 12 provincies en BIJ12 vertegenwoordigd zijn. Dit overleg vindt tweewekelijks plaats en speelt een cruciale rol in het versterken van informatieveiligheid, één van de speerpunten binnen de Nederlandse Digitalisering Strategie (NDS) die in mei a.s. wordt gepubliceerd. Het CIBO fungeert als een belangrijk platform voor interprovinciale kennisdeling en coördinatie rondom cybersecurity.

Om te komen tot een volwaardig interprovinciaal cybersecurity informatieknooppunt heeft het IPO-bestuur in 2023 besloten om als gezamenlijke provincies aan te sluiten bij het bestaande CSIRT[8] van het NCSC[9]. Uit een evaluatie bleek echter dat het NCSC niet beschikt over voldoende capaciteit en sectorspecifieke kennis om de provincies effectief te ondersteunen. Dit heeft geleid tot beperkte voortgang in de aansluiting van de provincies op het CSIRT. Om toch stappen vooruit te zetten en de regie te behouden, zullen de provincies in IPO-verband vanaf 2025 samenwerken om een specifiek interprovinciaal Security Operations Center (SOC) op te richten. Dit SOC wordt afgestemd op de unieke behoeften van de provincies en vult de lacunes op die het NCSC niet kan invullen. Daarnaast zal het SOC complementair zijn aan de bestaande signaleringssoftware die door de provincie wordt ingezet.
Onder toezicht van het IPO zal voor dit project een Europese aanbesteding worden uitgevoerd om een passende partner te selecteren. Het doel is een solide infrastructuur voor informatieveiligheid te realiseren die de provincies helpt bij het adequaat beschermen tegen cyberdreigingen.

Beveiligingsincidenten in 2024

Gemelde incidenten
In het jaar 2024 zijn door de helpdesk 209 meldingen geregistreerd die te maken met informatiebeveiliging. Het grootste deel van deze meldingen heeft betrekking op spam of phishing e-mails die medewerkers hebben ontvangen. Deze meldingen (incidenten) zijn afgehandeld en hebben voor zover bekend niet geleid tot productieverlies of schade. Bij 5 meldingen was sprake van verlies of diefstal van een provinciale laptop en/of provinciale smartphone.
Op basis van de geregistreerde incidenten worden aanscherpingen doorgevoerd in de maatregelen, teneinde een herhaling van deze incidenten in de toekomst zoveel mogelijk te voorkomen en mogelijke gevolgen hiervan te beperken.

Incidenten endpoint security
Sinds 2019 wordt bij een externe partij een dienst afgenomen waarbij de verschillende zg. endpoints (bijvoorbeeld laptops) in het netwerk van Provincie Limburg automatisch worden gescreend en in het geval van beveiligingsdreigingen direct worden uitgeschakeld. In het jaar 2023 ging het om 327 meldingen, waarvan 36 (11%) aangemerkt werden als kwaadaardig. Deze 36 gevallen zijn direct geïsoleerd en hebben niet geleid tot enige schade.

Datalekken
In 2024 zijn 18 meldingen van een datalek opgenomen in het interne register datalekken van de Provincie Limburg. Hiervan zijn 2 datalekken gemeld bij de AP (Autoriteit Persoonsgegevens).

[8] CSIRT: Computer/Cyber Security Incident Response team

[9] NCSC: National Cyber Security Center

De afweging om een datalek wel of niet te melden aan de AP vindt conform het vastgestelde protocol ‘Datalekken’ plaats aan de hand van de ENSIA-methodiek.

Financiële middelen die in 2024 zijn ingezet ten behoeve van informatiebeveiliging

In 2024 zijn circa € 160.000 aan kosten geboekt op informatiebeveiliging. De gemaakte kosten van de in deze mededeling portefeuillehouder opgenomen activiteiten maken hier deel van uit.

Verwachte ontwikkelingen in 2025

Pentest
Begin 2025 heeft reeds een pentest plaatsgevonden, waarbij de netwerksegmentatie (zie Firewall/netwerkoptimalisatie) van de Provincie Limburg het onderwerp van onderzoek was. Het gaat hierbij om het testen van interne scheiding van netwerkcomponenten alsmede het reviewen van de gekozen opzet.
Tevens zal in 2025 zal het onderzoek van het “aanvalsoppervlak” (zg. attack surface) van de Provincie Limburg gecontinueerd worden. Onderdeel van deze permanente scan is het actief zoeken op het zg. dark web naar dreigingsinformatie specifiek gericht op de Provincie Limburg, dan wel op gehackte gebruikersaccounts van de Provincie Limburg.

De Tweede Kamer heeft eind 2024 voor een motie gestemd die de regering verzoekt om overheidsbreed toe te werken naar een uniforme aanpak voor het geven van pentestopdrachten zodat op uniforme en transparante wijze bewezen kan worden dat aan de verplichtingen omtrent informatiebeveiliging is voldaan. De Provincie is voornemens zich te conformeren aan deze aanpak, zodra deze voldoende duidelijk c.q. vastgesteld is.

Privileged Access Management (PAM)
In 2025 zal de uitrol van deze oplossing voor interne gebruikersaccounts met speciale rechten (eigen beheerders van hard- en/of softwaretoepassingen) afgerond worden.

Update BIO naar BIO2.0
Van de BIO wordt in 2025 een nieuwe versie verwacht. De implementatie hiervan binnen de Provincie Limburg zal gestart worden op het moment dat de nieuwe versie beschikbaar komt.

Platform Informatiebeveiliging
Begin 2025 gaan we werken met een nieuw intern informatiebeveiligingsplatform, met daarin een brede afspiegeling van de organisatie, dat risicogericht gaat sturen op het treffen van maatregelen en gaat zorgen voor een sterkere verankering van informatiebeveiliging binnen de bestaande provinciale i-governance. Onderdeel van de beoogde PDCA-cyclus is, conform de ISO27001-norm en -werkwijze, het door dit platform periodiek uitvoeren van risicoanalyses.

Cyberbeveiligingswet en de NIS2-richtlijn
Omdat ontwikkelingen als COVID-19, de Oekraïne-oorlog, geopolitieke veranderingen, cyberdreigingen en de gevolgen van klimaatverandering de veiligheid van onze maatschappij en economie steeds meer onder druk zetten, is er sinds 2020 vanuit de Europese Unie aan de Network and Information Security (NIS2) directive gewerkt. Deze is inmiddels vastgesteld door de Europese Unie en is bedoeld om de cyberbeveiliging en de weerbaarheid van essentiële diensten in alle EU-lidstaten te verbeteren. De NIS2 vergroot de reikwijdte van de eerste richtlijn door meer sectoren te omvatten, waaronder de sector Overheid. Daarnaast hanteert de nieuwe richtlijn strengere beveiligingsnormen en meldingsvereisten voor incidenten. De komst van de NIS2-richtlijn moet bijdragen aan meer Europese harmonisatie en een hoger niveau van cybersecurity bij bedrijven en organisaties en wordt momenteel naar Nederlandse wetgeving vertaald.

De NIS2-richtlijn brengt voor overheden, waaronder ook provincies, enkele nieuwe verplichtingen met zich mee:

- Zorgplicht
  De richtlijn bevat een zorgplicht die organisaties verplicht om zelf een risicobeoordeling uit te voeren. Op basis daarvan nemen zij passende maatregelen om hun diensten zoveel mogelijk te waarborgen en de gebruikte informatie te beschermen. Deze werkwijze maakt deel uit van de werkwijze die in het kader van de ISO27001-norm wordt geïmplementeerd.
- Meldplicht
  De richtlijn schrijft voor dat organisaties incidenten die de verlening van de essentiële dienst sterk (kunnen) verstoren binnen 24 uur bij de toezichthouder moeten melden. Een cyberincident moet ook bij het Computer Security Incident Response Team (CSIRT) van het NCSC gemeld worden. Dit team kan vervolgens hulp- en bijstand leveren. Factoren die een incident meldingswaardig maken, zijn bijvoorbeeld het aantal personen dat door de verstoring is geraakt, de tijdsduur van een verstoring en de mogelijke financiële verliezen die hiermee gepaard zijn gegaan.
- Toezicht
  Organisaties die onder de richtlijn vallen, komen ook onder toezicht te staan. De NIS2-richtlijn schrijft voor dat een onafhankelijk toezichthouder (buiten eventueel interbestuurlijk toezicht) naar de naleving van de verplichtingen uit de richtlijn kijkt, zoals de zorg- en meldplicht. De Rijksinspectie Digitale Infrastructuur (RDI)[10] zal de toezichthouder voor de sector Overheid worden, waarbij de verwachting is dat de RDI toezicht gaat houden op het hele stelsel van informatieveiligheid voor de overheid op basis van systeemtoezicht.

Vanaf 17 oktober 2024 moeten decentrale overheden voldoen aan de NIS2. In 2025 zal deze richtlijn verder uitgewerkt worden in Nederlandse wetgeving, de Cyberbeveiligingswet (Cbw). De verwachte ingangsdatum van deze wet is 17 oktober 2025, de impact van de invoeren van de Cbw is echter dermate groot dat overheden meer tijd nodig hebben voor de implementatie ervan.

In IPO-verband, als onderdeel van de interprovinciale digitaliseringsagenda, wordt het komend jaar samengewerkt aan de implementatie van deze richtlijn en de wet om er voor te zorgen dat provincies en het IPO gaan voldoen aan de eisen van de richtlijnen en de wet.

[10] De Rijksinspectie Digitale Infrastructuur (RDI) is een Nederlandse overheidsorganisatie die verantwoordelijk is voor het toezicht op de Nederlandse digitale infrastructuur. De organisatie is onderdeel van het ministerie van Economische Zaken.

DOSA (Digitale Open Strategische Autonomie)
Dit is een agenda van het ministerie van Economische Zaken gericht op het versterken van digitale onafhankelijkheid en innovatie in Nederland en Europa. Het doel is om minder afhankelijk te zijn van niet-EU-landen en buitenlandse technologieën, met aandacht voor veiligheid, concurrentiekracht en publieke waarden. Belangrijke prioriteiten zijn onder andere kritieke grondstoffen, open source software, AI, halfgeleiders en cybersecurity.
Zowel DOSA als de NDS richten zich op het versterken van een robuuste en toekomstbestendige digitale infrastructuur en het vergroten van digitale autonomie in Nederland. Het thema “Versterken digitale weerbaarheid en digitale autonomie” zal naar verwachting opgenomen worden in de ambitie om de Rijksoverheid, provincies, gemeenten, waterschappen en publieke dienstverleners als één overheid samen te gaan werken en te versnellen.
Voor de Provincie Limburg betekent dit alles o.a. dat we zeer terughoudend zullen zijn bij het gebruik van (nieuwe) clouddiensten van Amerikaanse ‘big tech’ bedrijven en in voorkomende gevallen bijbehorende risico’s (en maatregelen) in kaart zullen brengen. Binnen dit thema wordt niet alleen interprovinciaal onder regie van het IPO door de provincies samen opgetrokken, maar zal ook de interbestuurlijke samenwerking worden versterkt.

Monitor informatieveiligheid
In 2025 wordt verder ingezet op het monitoren van dreigingen op het gebied van informatiebeveiliging, zodat tijdig kan worden ingegrepen.

Wij zullen uw Staten blijven informeren over de voortgang van de hier opgenomen ontwikkelingen.

Gedeputeerde Staten van Limburg
namens dezen,

S.H.M. Satijn