provincie limburg

Provinciale Staten
van Limburg

Cluster	OI	**Behandeld**	P.L.J. Deben
Ons kenmerk	DOC-00443398	**Telefoon**	+31 6 11 59 19 00
Uw kenmerk	-	**Maastricht**	28 maart 2023
Bijlage(n)	-	**Verzonden**	28 maart 2023

Onderwerp
Mededeling portefeuillehouder rapportage informatieveiligheid 2022

Geachte Staten,

Zoals te doen gebruikelijk informeren wij uw Staten jaarlijks in Q1 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 5e 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. Het onderwerp informatiebeveiliging is actueler dan ooit, getuige publicaties[1] als: *“Ransomware-aanval kost moederbedrijf Makro tientallen miljoenen euro's*”, *“Ransomware-aanval kostte lerse gezondheidszorg al 80 miljoen euro”, “Antwerpen kampt door cyberaanval met grootschalige uitval dienstverlening”, “Nederlandse gemeenten melden driehonderd cyberincidenten per jaar”, “Nederlandse windmolens konden door ransomware-aanval niet proefdraaien”, “Datalek gemeente Veenendaal door technische handeling softwareleverancier”*.

Het blijkt dat het essentieel is 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.

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

[1] Bron: security.nl

Limburglaan 10
6229 GA Maastricht

Postbus 5700
6202 MA Maastricht

+ 31 43 389 99 99
www.limburg.nl

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 voor op de fabrikanten van informatiebeveiligingsoplossingen.

In 2022 uitgevoerde werkzaamheden i.h.k.v. van informatieveiligheid

Herhaalonderzoek Zuidelijke Rekenkamer
In 2022 heeft de Zuidelijke Rekenkamer (ZRK) een vervolgonderzoek gedaan op het onderzoek informatieveiligheid van 2018. De ZRK heeft geconstateerd dat de toenemende aandacht van de Provincie Limburg voor informatieveiligheid is voortgezet, de inspanningen zijn geïntensiveerd en te nemen maatregelen zijn gerichter gekozen, vastgesteld en voortvarender geïmplementeerd. Verder zijn periodiek de voorgenomen penetratietesten uitgevoerd. De bevindingen daarvan laten een duidelijke verbetering zien ten opzichte van het eerdere onderzoek uit 2019. Daarnaast is het bewustwordingsprogramma voortgezet dat in 2022 werd afgerond en zijn PS jaarlijks actief en uitgebreid geïnformeerd over de uitvoering. Anderzijds constateert de ZRK ook dat de Provincie Limburg er nog niet in geslaagd was om al gereed te zijn voor een eventuele certificering tegen de ISO27001-norm.
Zoals ook in onze bestuurlijke reactie van 5 juli 2022 aangegeven, passen de door de ZRK gedane aanbevelingen naadloos binnen onze eigen plannen en zijn deze dan ook overgenomen. In uw commissie FEB van 7 oktober 2022 is het rapport van de ZRK inzake informatieveiligheid aan de orde geweest. Tijdens deze behandeling is toegezegd een informerende sessie over o.a. informatiebeveiliging voor PS te organiseren (toezegging 9170). Een mededeling portefeuillehouder n.a.v. behandeling van het ZRK-rapport in commissie FEB van 7 oktober 2002 is op 8 november 2022 aan u verzonden.

Informatiebeveiligingsbeleid
Als onderdeel van de implementatie van de ISO27001-norm is in 2022 het beleid informatieveiligheid herijkt. Dit beleid is door de directie in juli 2022 vastgesteld. Dit beleid is, conform de eisen, via de website van Provincie Limburg in te zien[2].

Onderzoek cyberweerbaarheid
Medio 2022 heeft een extern onderzoek naar de cyberweerbaarheid van de Provincie Limburg plaatsgevonden. Dit onderzoek bestond uit 2 delen. Het eerste deel had betrekking op het beoordelen van de reeds door de Provincie Limburg getroffen maatregelen in relatie tot de geïnventariseerde risico's. Als basis voor dit onderzoek werd genomen de controls en methodiek zoals deze door het CIS[3] worden gehanteerd. De conclusie van dit gedeelte van het onderzoek was dat de maatregelen die genomen zijn op het gebied van informatiebeveiliging in relatie tot de geïnventariseerde risico's over het algemeen voldoende waren, waarbij op sommige onderdelen nog ruimte voor verbetering was. Het tweede deel van het onderzoek had betrekking op de beheersing van een calamiteit als gevolg van een cyberincident. Uit dit onderzoek kwam naar voren dat op dit onderdeel nog stappen gezet dienen te worden om op het gewenste volwassenheidsniveau te komen. De uit dit onderzoek voortkomende verbeteracties, die overigens grotendeels organisatorisch van aard zijn, worden in 2023 opgepakt.
Tijdens de toegezegde en nog te plannen informerende sessie voor PS-leden over o.a. informatiebeveiliging kan in een vertrouwelijke setting meer informatie over de gedane aanbevelingen verstrekt worden.

---

[2] Zie: https://www.limburg.nl/algemeen/privacy-0/

[3] Center for Internet Security: een non-profitorganisatie annex gemeenschap verantwoordelijk voor het onderhoud van wereldwijd erkende "best practices" voor het beveiligen van IT-systemen en gegevens.

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. Hiertoe zijn alle personen die gebruik maken van de infrastructuur van Provincie Limburg uitgenodigd deel te nemen aan een serious game. De afgelopen jaren zijn hier 5 rondes mee gespeeld, waarbij de medewerkers in elke spelronde een aantal vragen dienden te beantwoorden op het gebied van informatiebeveiliging, privacy en fysieke beveiliging. In 2022 is deze serious game voor het laatst gespeeld. In 2023 wordt een nieuw meerjarig vervolgprogramma opgestart dat meer en verschillende interventies gedurende het jaar met zich meebrengt.

Beveiligde e-mail
Naast de technische standaarden m.b.t. het ontvangen en versturen van provinciale e-mails conform de richtlijnen van Forum Standaardisatie[4] wordt gebruik gemaakt van het versleutelen van email en (grote) bijlagen. Het Forum Standaardisatie toetst periodiek in hoeverre de technische standaarden worden gebruikt bij de emailvoorzieningen en de websites van (overheids)organisaties. Via de website internet.nl kan eenieder deze toets uitvoeren. De Provincie Limburg stuurt actief op een 100% score.

Gebruik geavanceerde signaleringssoftware
Het gebruik van de door de Provincie Limburg in 2019 aangeschafte geavanceerde signaleringssoftware om enerzijds inzicht te verkrijgen in kwetsbaarheden en anderzijds incidenten met potentieel kwaadaardige software in de kiem te smoren, is ook in 2022 verder toegenomen. Dit betreft zowel de inbedding van de signaleringsfunctie binnen de werkprocessen van de beheerorganisatie als de samenwerking met het externe SOC[5], dat de Provincie Limburg op dit gebied ondersteunt.

ISO27001/BIO
In 2020 is binnen de Provincie Limburg gestart met de voorbereiding op de implementatie van de ISO27001-norm, met de Baseline Informatiebeveiliging Overheid als referentiekader voor de te nemen maatregelen. In de loop van 2021 is e.e.a. verder geformaliseerd en is hiervoor een plan van aanpak opgesteld en door de directie goedgekeurd. Hierna is voor dit traject een intern project opgestart, dat opgenomen is in het uitvoeringsprogramma van het in 2021 door GS vastgestelde Strategisch Informatiebeleid Limburg 2021-2024. Als onderdeel van de implementatie van ISO27001 is in 2022 de toepassing die het ISMS[6] (Information Security Management System) ondersteunt verder ingericht en in gebruik genomen.
Nadat eerder voor alle provincies een 0-meting van de ISO27001-norm heeft plaatsgevonden, is in 2021 voor alle provincies een 1-meting uitgevoerd. Provincie Limburg heeft deze meting herhaald in september 2022 en in februari 2023. Het beeld dat uit deze meting naar voren komt is dat de Provincie Limburg eind 2022 nagenoeg klaar was voor certificering. De directie zal in 2023 een besluit nemen over een daadwerkelijke certificering.

[4] Forum Standaardisatie is onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en toetst en adviseert aan publieke organisaties over het gebruik van open standaarden.

[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.

[6] ISMS (Information Security Management Systeem) is een set aan procedures voor het beheersen van de informatieveiligheid.

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 controlewebsites internet.nl[7] en basisbeveiliging.nl[8], de websites (domeinen) waar de Provincie Limburg de geregistreerde eigenaar van is beoordeeld en daar waar nodig en mogelijk, aangepast aan de voorgestelde standaarden. De Provincie Limburg stuurt actief op hoge scores op deze controlewebsites en hanteert hierbij het principe “comply or explain”.

DigiD audit
In 2022 is in verband met de aansluiting op DigiD een beveiligingsassessment uitgevoerd door een externe auditor. Binnen de Provincie Limburg wordt DigiD gebruikt voor de digitale ondertekening (authenticatie) van aanvraagformulieren voor subsidies, voor de toegang tot het subsidieportaal en voor een mogelijk correctief bindend referendum. In de audit is vastgesteld dat de Provincie Limburg voldoet aan de beveiligingseisen die door Logius[9] gesteld worden aan het gebruik van DigiD.

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 door te lichten op mogelijke kwetsbaarheden. In dit kader heeft in Q1 van 2022 een zgn. black- en greybox test plaatsgevonden. Dit onderzoek leverde een beperkt aantal bevindingen op die geleid hebben tot enkele aanpassingen binnen de ICT-infrastructuur van de Provincie Limburg. Omwille van het voorkomen van mogelijk misbruik van kwetsbaarheden wordt geen uitspraak gedaan omtrent de aard van de bevindingen uit dit onderzoek. Inmiddels heeft ook in 2023 reeds een Pentest plaatsgevonden.

Interprovinciaal informatieknooppunt informatiebeveiliging
Als onderdeel van de stappen die gezet worden om te komen tot een interprovinciaal informatieknooppunt informatiebeveiliging heeft de voorbereiding voor de oprichting van het ISAC[10] plaatsgevonden. Dit heeft geleid tot de formele start per 31 januari 2023. Het ISAC is een formele samenwerking tussen alle 12 provincies en BIJ12 waarbij informatie over cybersecurity en gevoelige en vertrouwelijke informatie over incidenten, dreigingen, kwetsbaarheden en maatregelen wordt uitgewisseld. Onderdeel van een ISAC is ook een netwerk van ICT- en cybersecurityspecialisten. Door samen te werken en ervaringen te delen kan gezamenlijk opgetrokken worden bij incidenten die de sector treffen. Ook zullen kosten lager uitvallen door van elkaar te leren en maatregelen te treffen.
Dit geeft de provincies in zijn algemeenheid, en de Provincie Limburg in het bijzonder, een betere informatiepositie bij het treffen van maatregelen tegen mogelijke risico’s en draagt op die manier bij tot het verder versterken van onze informatiebeveiliging en het bevorderen van de horizontale samenwerking met andere provincies.

---

[7] Dit is een initiatief van het Platform Internetstandaarden, een samenwerkingsverband van partijen uit de Internetgemeenschap en de Nederlandse overheid. Op internet.nl kan eenvoudig getest worden of de website, e-mail en internetverbinding van een organisatie gebruik maken wel moderne, betrouwbare Internetstandaarden.

[8] Om bij overheden de veiligheid op internet te vergroten is de website basisbeveiliging.nl ontwikkeld, een geografische kaart die met stoplichtkleuren aangeeft of de website en externe netwerkdiensten van lokale overheden qua online veiligheid op orde zijn.

[9] 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.

[10] ISAC: Information Sharing and Analysis Centre

Govroam
In 2022 zijn verdere acties ondernomen ten aanzien van het draadloze netwerk in het Gouvernement in combinatie met de dienst “Govroam”. Govroam stelt overheidsorganisaties zoals gemeenten, provincies, ministeries, waterschappen, ZBO’s, etc. in staat hun elektronische netwerken (zoals wifi) op een veilige manier met elkaar te delen. Hierdoor krijgen medewerkers op iedere deelnemende locatie eenvoudig, veilig en draadloos toegang tot de digitale services, e-mail en data van de eigen organisatie. Zo wordt het eenvoudig, vertrouwd én veilig op afstand werken binnen de overheid bevorderd. Govroam maakt gebruik van standaarden zoals certificaten en toegangsprotocollen.

Spamfilter
Over 2022 zijn ruim 8.2 miljoen externe e-mails ontvangen. Door het centrale spamfilter zijn hiervan ongeveer 6.3 miljoen verdachte e-mails automatisch geblokkeerd en verwijderd, waardoor deze niet bij de geadresseerde provinciale medewerkers werden afgeleverd. Dit is ongeveer 80% van de totale hoeveelheid in 2022 ontvangen externe e-mails. Daarnaast zijn in 2022 ongeveer 6.000 e-mails automatisch geblokkeerd en verwijderd, omdat deze een virus bevatten.

Privileged Access Management
In 2022 is gestart met de implementatie van een wachtwoordmanagementtool. Middels deze tool worden wachtwoorden voor beheerders en systeemaccounts automatisch beheerd en beschermd. Tevens biedt deze tool mogelijkheden voor het wijzigen van gebruikerswachtwoorden (selfservice) en biedt het voorzieningen voor het tijdelijk en veilig verstrekken van toegang aan externe leveranciers tot onderdelen van de ict-infrastructuur van de Provincie Limburg. In 2023 wordt de implementatie van deze tool afgerond.

Firewall/netwerkoptimalisatie
In 2022 zijn we gestart met een proefsegmentatie van het netwerk in het Gouvernement. Na een succesvolle testperiode wordt dit traject in 2023 volledig uitgerold.

Beveiligingsincidenten

Gemelde incidenten
In het jaar 2022 zijn door de helpdesk ongeveer 100 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. 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 zgn. endpoints (bijvoorbeeld laptops) in het netwerk van Provincie Limburg automatisch worden gescreend en in het geval van beveiligingsdreigingen, deze direct worden uitgeschakeld. In het jaar 2022 ging het om ruim 320 meldingen, waarvan geen aangemerkt werd als kwaadaardig. In veel situaties blijken meldingen achteraf niet kwaadaardig of schadelijk te zijn. Dit noemen we zg. “false positives”.

Datalekken
In 2022 zijn 5 meldingen van een datalek opgenomen in het interne register datalekken van de Provincie Limburg. Hiervan zijn geen datalekken gemeld bij de AP (Autoriteit Persoonsgegevens). De afweging om een datalek wel of niet te melden aan de AP vindt plaats aan de hand van de ENISA-methodiek, conform het vastgestelde protocol datalekken.

Financiële middelen die in 2022 zijn ingezet t.b.v. informatiebeveiliging

In 2022 zijn afgerond € 300.000 aan kosten geboekt op informatiebeveiliging. De gemaakte kosten van de in deze mededeling portefeuillehouder opgenomen activiteiten maken hier deel van uit.

Verwachte ontwikkelingen in 2023

Informerende sessie voor PS over o.a. informatiebeveiliging
Op 7-10-2022 is n.a.v. de behandeling van het ZRK-rapport in de commissie FEB aan PS toegezegd een informerende sessie te organiseren over o.a. informatiebeveiliging (toezegging 9170). In afstemming met de Griffie wordt momenteel een geschikte datum voor deze sessie gezocht.

ISO27001
De implementatie van de ISO27001-norm binnen Provincie Limburg is in 2022 voor het grootste deel afgerond. Een aantal beschreven en getroffen maatregelen zal echter in 2023 nog verder aangescherpt dienen te worden. Dit maakt onderdeel uit van het continu verbeteren zoals dit ook in de ISO-norm is opgenomen.

Resultaten extern onderzoek cyberweerbaarheid
Uit het in 2022 uitgevoerde externe onderzoek naar de cyberweerbarheid van de Provincie Limburg komen enkele voornamelijk organisatorische aanbevelingen naar voren, die ook tijdens de implementatie van de ISO27001-norm zijn opgemerkt. Deze aanbevelingen zullen in de loop van 2023 verder opgepakt worden en leveren daarmee niet alleen een bijdrage aan het vergroten van de cyberweerbaarheid van de Provincie Limburg, maar ook aan de afronding van de implementatie van de ISO27001-norm binnen Provincie Limburg.

Interprovinciaal informatieknooppunt informatiebeveiliging
Interprovinciaal wordt in 2023 verder invulling gegeven aan de rol die het ISAC krijgt binnen de interprovinciale samenwerking op het gebied van informatieveiligheid. In 2023 zal tevens duidelijk worden welke invulling gegeven wordt aan het beoogde informatieknooppunt informatiebeveiliging. Aan de hand van een businesscase zal de interprovinciale besluitvorming hieromtrent worden voorbereid.

GovGuest
In 2022 is in het kader van de beveiliging van het draadloze netwerk in het Gouvernement onderzocht of de Govroam-technologie kon worden ingezet voor het veilig verlenen van internettoegang aan gasten. In opvolging van dit onderzoek wordt Govguest in 2023 geïmplementeerd.

Pentest
In 2023 is reeds een pentest op de infrastructuur van Provincie Limburg uitgevoerd. Later dit jaar zal

bekeken worden in hoeverre een pentest of vergelijkbaar kan worden uitgevoerd op enkele belangrijke SAAS-toepassingen[11] die in gebruik zijn bij Provincie Limburg.

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

Gedeputeerde Staten van Limburg
namens dezen,

A.G.M. Roest

[11] SAAS staat voor Software As A Service. Hierbij wordt een toepassing, zoals bijvoorbeeld een HRM-systeem, als een dienst afgenomen. De hard- en software wordt in dat geval door de leverancier beheerd, waarbij deze ook zorgdraagt voor de beveiliging van het systeem.