Jaarrapportage Informatieveiligheid

2021

Hessel Bremer - Chief Information Security Officer (CISO)

Deventer, Olst-Wijhe en Raalte: samen staan we sterker.

Jaarrapportage 2021

Voor u ligt de Jaarrapportage Informatieveiligheid 2021 van de Chief Information Security Officer (CISO) van de gemeenten Deventer, Olst-Wijhe en Raalte. Hierin is inzichtelijk gemaakt op welke wijze DOWR in 2021 invulling heeft gegeven aan informatieveiligheid als topprioriteit zoals is vastgelegd in de i-visie 2018-2022.
In algemene zin kan worden gesteld dat de DOWR-gemeenten qua informatiebeveiliging het afgelopen jaar weer de (be-)nodigde, geplande en ongeplande, stappen hebben moeten zetten om de digitale weerbaarheid van onze gemeenten op het gewenste beveiligingsniveau te houden. Ook zijn onze gemeenten wederom geconfronteerd met de nodige cyberdreigingen en hebben wij weer kunnen leren van incidenten die zich elders in het land voordeden of waar DOWR zelf mee werd geconfronteerd.

1 Dreigingsbeeld 2020-2022

Het jaar 2021 stond voor het tweede jaar in het teken van de pandemie COVID-19. Het jaar kenmerkte zich door opeenvolgende lockdowns en aanvullende maatregelen om de epidemie maatschappelijk onder controle te krijgen. Dit met onbedoelde neveneffecten tot gevolg waaronder thuiswerken. Want ook dit jaar werkten we grotendeels vanuit huis. En zagen we opnieuw wereldwijd een toename van het aantal cyberincidenten.

Voor elk van deze incidenten geldt dat de 'lessons learned' zijn geëvalueerd en gespiegeld op de DOWR-organisatie om te beoordelen wat de impact zou zijn geweest als wij getroffen worden.
Zo is eerder dit jaar de hack Hof van Twente door DOWR-I Security uitgebreid geanalyseerd en bevindingen ter lering breed gedeeld en besproken in de DOWR-gemeenten.

2 Ketenpartners en risico's

Gedurende het afgelopen jaar ontvingen wij van de Informatiebeveiligingsdienst (IBD) en het Nationaal Cyber Security Centrum (NCSC van het NCTV) maandelijks updates op het gebied van informatiebeveiliging en cybersecurity, bijvoorbeeld over digitale dreigingen.

Opmerkelijk is te noemen dat digitale aanvallen op of door middel van ketenpartners zijn waargenomen, waaronder ook het Apache Log4j incident van eind vorig jaar. Dit incident kenmerkte zich door een kwetsbaarheid waarmee het risico ontstond dat toegang tot onze informatiesystemen verkregen kon worden, met daarbij een cruciale rol voor (Cloud-)leveranciers. Op dit moment zijn diverse (landelijke) evaluaties gestart en kunnen wij de verbetermaatregelen (lessons learned) binnenkort tegemoet zien. De verbetermaatregelen worden geëvalueerd en waar nodig doorgevoerd.

Dit incident heeft duidelijk gemaakt dat de dienstverlening met onze leveranciers en samenwerkende externe partners aandacht verdient met betrekking tot de contractuele borging, afspraken over beschikbaarheid en serviceverlening bij verstoringen.

Om vroegtijdig de risico's inzichtelijk te krijgen in relatie tot leveranciers is het van belang dat vroegtijdig een risicoanalyse conform de BIO (BBN Baselinetoets) wordt uitgevoerd. Wij noemen dit ook wel 'security by design'.

Onlangs heeft het Directieberaad DOWR ingestemd met de implementatie van het risicoanalyseproces. Er wordt een plan van aanpak uitgewerkt om dit risicoanalyseproces gestructureerd in DOWR te implementeren.

3 Ontwikkelingen informatiebeveiliging DOWR

3.1 Samenwerking informatiebeveiliging en privacy

De samenwerking tussen de vakspecialisten van privacy en informatieveiligheid is dit jaar geëffectueerd en er zijn al mooie resultaten behaald waarover u onderstaand meer kunt lezen. Ook komende jaren zal deze samenwerking waar mogelijk verstevigd worden met als doel de betrouwbaarheid van informatie te waarborgen op een zo efficiënt mogelijke wijze voor de DOWR-gemeenten. Daarbij staat bescherming van zowel persoonsgegevens als andere gegevens van onze inwoners, medewerkers, de gemeenten en ondernemers centraal.

3.2 Resolutie digitale veiligheid (VNG)

Op 12 februari 2021 heeft de VNG in een Buitengewone Algemene Ledenvergadering de 'Resolutie Digitale Veiligheid: kerntaak voor gemeenten' unaniem aangenomen. Alle gemeenten in Nederland gaan meer prioriteit geven aan de beveiliging van hun digitale systemen in de vorm van meer aandacht, meer tijd en meer geld. Binnen de DOWR-gemeenten is informatiebeveiliging al enkele jaren Topprioriteit, hetgeen zich heeft vertaald in de huidige mate van digitale weerbaarheid.

3.3 Cybercrisisplan

Ook dit jaar zijn er serieuze stappen gezet en is een eerste opzet gemaakt van het Cybercrisisplan DOWR. Een cybercrisis oefenen heeft enkel zin als er een plan aanwezig is, zodat een gerichte oefening voorbereid kan worden met betrokkenen.

In oktober 2021 vond een eerste verkennende sessie (kick-off) plaats met de drie burgemeesters van de DOWR-gemeenten, ICT-management, de ISO en de CISO. Een eerste conceptversie is opgemaakt en uitgelijnd met de bestaande crisisorganisatie OOV. In het eerste kwartaal 2022 volgt verdere afstemming van dit plan met de Gemeentesecretarissen en Directeuren en worden achtereenvolgens een Tabletop (digitale simulatie), een bestuurlijke cybercrisisoefening (in DOWR-verband) en een realistische cyberoefening in de regio (veiligheidsregio IJsselland) voorbereid.

3.4 Nanolearning

Volgens het jaarplan is in 2021 de Nanolearning tool geïmplementeerd. De tool geeft medewerkers driewekelijks een korte minitraining per e-mail op het gebied van privacybescherming en informatiebeveiliging. Deze is specifiek bedoeld om een generieke basis voor bewustwording binnen de DOWR-gemeenten te bewerkstelligen. Ook is de tool dermate flexibel dat content waar nodig kan worden aangepast of gespecificeerd. Of dat onderwerpen toegevoegd

kunnen worden, bijvoorbeeld als gevolg van een recent incident. Naast deze tool worden jaarlijks aanvullende bewustwordingsacties voorbereid om waar nodig nog beter en gerichter op het gewenste bewustwordingsniveau te komen.

3.4 Naris ontwikkeling managementtool voor informatie-veiligheid en risicobeheersing (ISMS/GRC)

In 2021 is de management tool ISMS/GRC (Information Security Management Systeem verder geïmplementeerd. En is in samenwerking met DOWR-I en de leverancier de risicomodule ontwikkeld. Deze module is in het leven geroepen om de beheersmaatregelen van de risico's te monitoren. De proceseigenaar zelf heeft hier inzage in en kan verbeteringen melden. Ook is de audit module/compliance in gebruik genomen. De complete DigiD/Suwinet audit is hierin geïmplementeerd en de auditor kan hier zijn bevindingen en aanbevelingen in opnemen. Dit is een belangrijke stap waarmee het omvangrijke auditproces verder is geautomatiseerd.

3.5 IRPA-tool live

De integrale risico- en privacy-analyse (IRPA) tool is ontwikkeld en geïntroduceerd door de IBD. De tool heeft als doel om analyses op het gebied van privacy en informatiebeveiliging gemakkelijk, professioneel en eenduidig te kunnen uitvoeren. Bij DOWR maakt de tool onderdeel uit van het risicoanalyseproces van informatiebeveiliging en zorgt ervoor dat duidelijk wordt, welke passende analyse en maatregelen nodig zijn om verder geïmplementeerd te worden. De tool wordt enkel als hulpmiddel gebruikt en de resultaten worden vastgelegd in onze ISMS/GRC-tool.

4 Audits

4.1 ENSIA

EENSIA helpt gemeenten in één keer verantwoording af te leggen (BRP, DigiD, BAG, BGT, BRO, WOZ en Suwinet) over informatieveiligheid gebaseerd op de normen die gelden voor de Nederlandse overheid, de BIO. Met ENSIA sluit de verantwoording over informatieveiligheid aan op de planning en control-cyclus van de gemeente.

Gedurende 2021 zijn verschillende personen geïnterviewd en verslagen van de interviews opgesteld. Daarnaast zijn voor de certificering, de gewenste documenten en verantwoordingen opgeleverd aan de belanghebbende partijen. Daarmee hebben de gemeenten Deventer, Olst-Wijhe en Raalte de ENSIA-verantwoording van 2021 met succes afgerond.

Echter, één aandachtspunt staan wij graag even bij stil, namelijk de verantwoording van een specifieke leverancier richting DOWR-gemeenten. Door onderschatting van de leverancier hebben wij alle zeilen bij moeten zetten om afsluiting van onze digitale dienstverlening te voorkomen.

Door adequaat en stevige interventie richting de leverancier hebben wij imagoschade van de drie gemeenten kunnen voorkomen. De leverancier heeft inmiddels beterschap beloofd en is ook bezig om maatregelen te treffen om dit in de toekomst te voorkomen.

4.2 IT-verantwoording jaarrekening

In het kader van de jaarrekeningcontrole 2020 van de (gastheer)gemeente Deventer is er een geactualiseerde IT-audit uitgevoerd. Op dit moment worden de uitkomsten van deze audit geëvalueerd door de betreffende belanghebbenden en zal het rapport binnenkort worden vastgesteld door auditor Deloitte.

4.3 Hardening

Het hardeningsproces richt zich op het veiliger maken van systemen door technische maatregelen. Er vinden doorlopend audits plaats op onze systemen. Ondanks dat er in 2021 grote aantallen nieuwe BIO-controls (beheersmaatregelen) zijn toegevoegd die ook meetelden voor de BIO-compliance (en vervolgens geïmplementeerd moesten worden), is het ons gelukt om de BIO (incl. hardening), eind 2021 weer 100% compliant te krijgen. Het gaat hier specifiek om de technische hardening van onze IT-systemen.

4.4 Pentesten

In 2021 is er een externe pentest uitgevoerd om eventuele kwetsbaarheden op de externe toegang tot de DOWR-infrastructuur te identificeren. Pentest is een afkorting van 'penetration testing'. Bij een pentest kruipen pentesters in de huid van een hacker. Tijdens deze pentest zijn geen directe kwetsbaarheden gevonden, maar wel één bevinding die niet direct exploiteerbaar was. Deze is direct opgelost.

4.5 Samenwerking regio IJsselland

In 2020 is de CISO-kring IJsselland gestart. Aan tafel zitten de CISO's en ISO's van de 11 IJssellandse gemeenten aangevuld met de CISO Provincie Overijssel en medewerking van de Informatiebeveiligingsdienst (IBD) en Veiligheidsregio IJsselland (VRIJ). De CISO-kring zal meerdere keren per jaar bij elkaar komen en wanneer nodig op andere wijze met elkaar communiceren. Doel van het overleg is om de onderlinge samenwerking regionaal te bevorderen en informatie over kritische incidenten met elkaar te delen.

5 Tot slot

Informatiebeveiliging staat inmiddels al meerdere jaren 'op de kaart' binnen de DOWR-gemeenten. Gezien een toename van de digitale dreiging is digitale veiligheid een serieus onderdeel geworden van de huidige bedrijfsvoering en is informatiebeveiliging als risicomanagementproces zelfs een kritische succesfactor om de digitale weerbaarheid van onze gemeenten te verhogen.

Specifiek doel daarbij is te voorkomen dat naast onze eigen organisatie ook de dienstverlening aan inwoners en ondernemers van de gemeenten Deventer, Olst-Wijhe en Raalte de gevolgen hiervan ondervinden. Voorkomen van cyberrisico's (100% beveiligen) kunnen wij helaas niet, maar er wel voor zorgen dat wij de beveiligingsincidenten voldoende en tijdig onder controle krijgen. Een mooie uitdaging voor het komende jaar!

Hessel Bremer
Chief Information Security Officer
Deventer, Olst-Wijhe, Raalte

Februari 2022