MEMO

Dit advies is opgesteld door het regionale CISO-overleg en de i-adviseurs hebben zich vervolgens achter dit advies geschaard in hun overleg op 31 maart 2022.

Onderwerp: Gezamenlijke reactie op ''Advies Programma Beveiliging''

Aan:	Hoofden bedrijfsvoering/CIO Rijk van Nijmegen
Van:	CISO-groep Rijk van Nijmegen
CC:	I-regio managers
Datum:	29 maart 2022

Aanleiding

Naar aanleiding van het Advies Programma Beveiliging van iRvN wordt door de Hoofden Bedrijfsvoering/CIO de vraag gesteld aan de CISO`s in de regio of het "gulden middenweg scenario" in het advies de risico`s voldoende beperkt en invulling geeft aan de "must haves". Als CISO's komen we met een gezamenlijke reactie en advies, nadat er afstemming en uitleg heeft plaatsgevonden met iRvN.

Advies

Wij adviseren de hoofden bedrijfsvoering in te stemmen met de voorgestelde investeringen van de iRvN die behoren bij het scenario ''De Gulden Middenweg''. We onderstrepen hierbij dat we een mooie stap in de richting van meer veiligheid zetten. Het is van belang dat er snel begonnen kan worden en dat iedere gemeente meedoet; het geheel is zo sterk als de zwakste schakel.
Additioneel op het scenario ''De Gulden Middenweg'' adviseren we om structurele (externe) pentesten toe te voegen bovenop het geadviseerde scenario en vragen we in dit memo meer aandacht voor assetmanagement en het bredere perspectief waarin de ontwikkelingen plaatsvinden.

Must Haves

De toetsing door Hunt & Hackett heeft plaatsgevonden op basis van de zogenoemde Critical Security Controls (CIS controls). Deze controls gaan voornamelijk op technisch vlak in op waargenomen dreigingen en minder op het aspect van beleid en beheersing. Als CISO's richten wij ons bij het gemeentelijk beveiligingsbeleid voornamelijk op de BIO en aanvullende technische eisen en kaders die auditors stellen (bijv. ISO 27001).
In dit kader hebben we de voorgestelde scenario's tegen het licht gehouden, waarbij we gezamenlijk tot de conclusie komen dat het scenario van de gulden middenweg een ''must'' is om de komende tijd door te ontwikkelen. Als we de projecten zoals in het rapport omschreven spiegelen aan de BIO maatregelen komen we tot eenzelfde conclusie.

Het scenario van de maximale variant bevat verschillende projecten die dienen te gebeuren, maar de vereisten uit de BIO zijn op deze vlakken minder helder en strikt. Zodoende is er binnen de verplichte normen ruimte om een norm in een aangepaste vorm in te vullen. Hierbij worden sommige projecten door iRvN al op een bepaalde manier ingevuld en aan risicobeperking gedaan, echter zo blijkt uit het onderzoek dient hier meer en aantoonbaar aandacht aan te worden besteed.

Zoals in het advies opgenomen adviseren we om structureel (externe) pentesten uit te laten voeren (back-up oplossing inbegrepen) en de resultaten hiervan ook te laten delen met de CISO-groep. Ook vragen wij aandacht voor goed assetmanagement, dit is in onze ogen elementair.

Risico beperking en actualiteit
CIS-controls zijn bedoeld als een set maatregelen waarmee je de basis op orde krijgt. Het antwoord op de vraag naar het beperken van de risico`s is dan ook dat het midden scenario (waarbij de projecten uit het maximale scenario wel uitgevoerd worden maar op een "slankere manier") voldoende is voor de bekende risico`s op dit moment.

Het onderzoek van Hunt & Hackett geeft aan dat de belangrijkste dreiging voor Nederlandse overheidsorganen bestaat uit het gijzelen van data voor losgeld. Dit beeld is gebaseerd op ervaringen uit het verleden en biedt absoluut geen garanties voor de toekomst. Er zal dus zeer regelmatig nagegaan moeten worden of het dreigingsbeeld verschuift. Oftewel door de ontwikkelingen aan de kant van de cybercriminaliteit, dan wel door de ontwikkelingen aan de kant van de gemeenten. Oplossingen en maatregelen zullen 'flexibel' moeten zijn om in te kunnen spelen op actuele dreigingen.

Breder perspectief
Meer dan techniek
Natuurlijk is er meer dan technische maatregelen. Keuzes die gemeenten maken als opdrachtgever hebben effect op de werking van sommige technische maatregelen. Ook keuzes die gemeenten niet maken hebben gevolgen. Het samenspel tussen iRvN en de gemeentelijke deelnemers loopt niet altijd even soepel en ook dit veroorzaakt een risico. In de uitvoering van de projecten zal er goede afstemming moeten plaatsvinden met de deelnemers om te voorkomen dat oplossingen onvoldoende draagvlak hebben.

Van belang is het verder dat gekozen oplossingen schaalbaar, toekomstgericht en toepasbaar zijn voor alle gemeenten en dat individuele gemeentelijke maatregelen die leiden tot een verzwakking van de regionaal gedeelde infrastructuur te allen tijde voorkomen worden. Hiervoor moeten betere regionale afspraken worden gemaakt.

Ontwikkelingen en toekomstperspectief
Zoals eerder aangegeven zullen alle oplossingen flexibel genoeg moeten zijn om nodige ontwikkelingen niet in de weg te staan. Het dreigingsbeeld verandert voortdurend door externe ontwikkelingen (denk aan de oorlog in Oekraïne) of veranderingen in de werkprocessen van de gemeenten (denk aan het thuiswerken i.v.m. Corona). Genomen maatregelen zullen indien nodig aangepast, opgeschaald, afgeschaald, toegevoegd of verwijderd moeten kunnen worden.

De geadviseerde maatregelen betekenen een mooie stap voor het veiligheidsniveau van de regio. Wel is het goed om te realiseren dat er altijd 'meer' gedaan moet worden om voldoende effect te sorteren tegen de toenemende dreiging. Hierbij dienen we rekening te houden met de werkbaarheid maar ook met de financiële aspecten van bepaalde beslissingen. Wel geven we graag nog de volgende toekomstperspectieven en aandachtspunten mee:

- Zero Trust model (nabije toekomst)

Een model voor informatiebeveiliging waarbij alleen toegang verleend wordt aan gebruikers, applicaties en apparatuur die geverifieerd zijn.

- Toenemend gebruik van SaaS

Software as a Service: applicaties worden door een leverancier op internet aangeboden en niet in huis bij iRvN.

- Toename van en betere social engineering, bescherming gericht op phishing en insider threat.

Computer crimineel probeert toegang te krijgen tot de IT omgeving door de gebruiker met trucjes zo ver te krijgen dat hij/zij zijn gegevens (wachtwoord) af staat. Dit kan ook via een werknemer (insider).

- Steeds meer data op steeds meer plekken (SaaS, maar ook koppelingen, ketenafhankelijkheid, controle op leveranciers)

Wij gebruiken gegevens van andere partijen (belastingdienst bijvoorbeeld) anderen gebruiken gegevens van ons (wijkteams). Een fout heeft gevolgen voor velen.

- European Cyber Resilience Act (continuïteit, maar ook als het mis gaat recovery)

Voorstel staat voor Q3 2022 gepland. Doel is gedeelde eisen aan leveranciers tav de weerstand tegen aanvallen zodat de maatschappij minder geraakt wordt door digitale problemen.

- Onstabiele wereld – grondstoffen staan onder druk

Variërend van minder betrouwbare stroomvoorziening tot terugtrekking van beschikbare leveranciers en bronnen binnen Europa. Zie het minder stabiele stroomnet nav de energietransitie en de recente leveringsproblemen

- Politieke instabiliteit

Collateral damage in digitale oorlogsvoering (bijv EternalBlue, Stuxnet). Meer wantrouwen veroorzaakt meer spionage software en meer aanvallen.