Advies Programma Beveiliging

Versie: 1.2
Status: Definitief
Auteur: Nyree Glaap, Werner Vissers

Bestandsnaam: Advies Programma Beveiliging

Documenthistorie

Revisies

Versie	Status	Datum	Wijzigingen
0.1	Concept	07-01-2022	1e opzet
0.2	Concept	11-01-2022	Interne review
0.3	Concept	21-02-2022	Review DT
1.0	Definitief	28-02-2022	
1.1	1e review	15-03-2022	Kosten nu incl. formatie
1.2	Definitief	07-04-2022	Aanvulling Advies op verzoek van Ciso's en I-adviseurs

Goedkeuring

Dit document behoeft de volgende goedkeuringen:

Versie	Datum goedkeuring	Naam	Functie	Paraaf
1.0	01-03-2022	DT iRvN		
1.2	07-04-2022	Henk De Groot	Manager I&A Beheer	
1.2	07-04-2022	Werner Vissers	Manager ICT-Beheer	

Distributie

Dit document is verstuurd aan:

Versie	Datum verzending	Naam
0.2	11-02-2022	DT iRvN
1.0	02-03-2022	Hoofden Bedrijfsvoering RvN
1.2	07-04-2022	Hoofden Bedrijfsvoering RvN
1.2	04-05-2022	Portefeuillehouders ICT Rijk van Nijmegen

Inhoudsopgave

1 Voorwoord

Versie 1.0 van dit document is besproken en toegelicht met hoofden Bedrijfsvoering, CISO's en i-adviseurs. Op basis van die gesprekken is een formeel advies door de CISO's geformuleerd aan de hoofden bedrijfsvoering en hebben de i-adviseurs in gestemd met dit advies. Het advies luidt als volgt:

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.

Op basis van dit advies is versie 1.0 aangepast naar dit document, versie 1.2, en zijn de projecten Pentesten en Assetmanagement toegevoegd aan scenario "De Gulden Middenweg".

Verder adviseren CISO's en i-adviseurs dat de gekozen oplossing flexibel moet zijn om toekomstige ontwikkelingen niet in de weg te staan. Zij zien het voorstel als een mooie stap om het veiligheidsniveau te vergroten maar dat het niet moet blijven bij een eenmalige acties. In hun advies wordt meegegeven dan er gezamenlijk moet worden opgetrokken om het toekomstperspectief te bewaken en waar nodig bij te stellen. Genoemd worden dan:

- Zero Trust model (nabije toekomst), een model voor informatiebeveiliging waarbij 'niets of niemand vertrouwd wordt' en 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 on premise 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) afstaat. 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 t.a.v. 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 (bijvoorbeeld EternalBlue, Stuxnet). Meer wantrouwen veroorzaakt meer spionage-software en meer aanvallen.

iRvN onderstreept deze aandachtspunten en wil graag actief participeren in het CISO-overleg om deze punten te bespreken. Vanuit DT iRvN zal de manager ICT-Beheer aansluiten bij dit overleg, indien dit gewenst is.

2 Inleiding

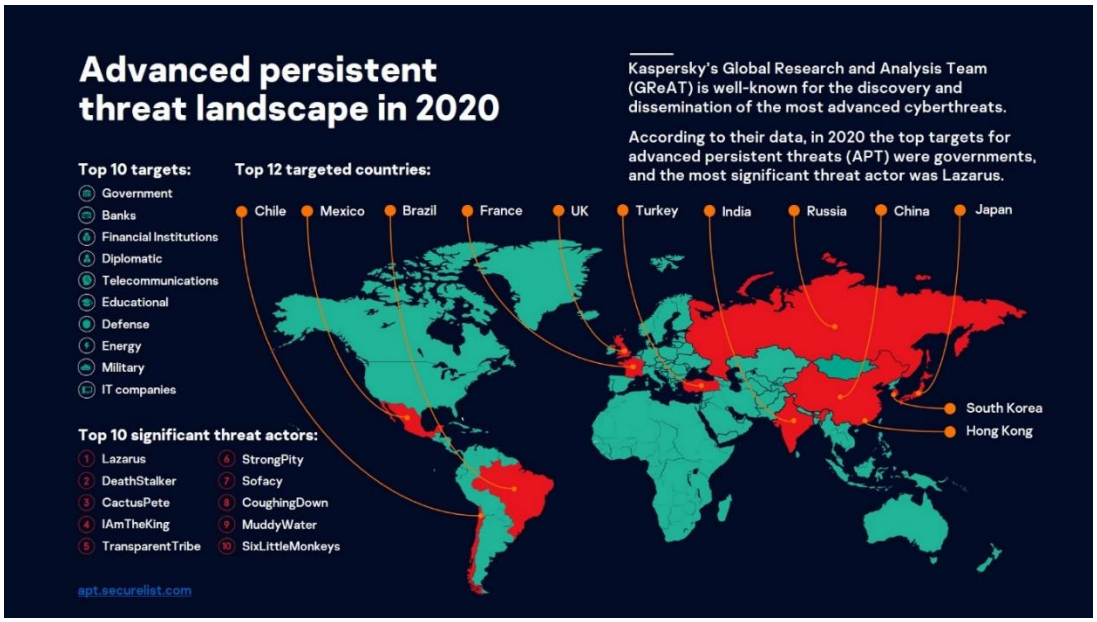
2.1 Situatieschets

Binnen iRvN bestaat veel aandacht voor (informatie)beveiliging. iRvN heeft de ambitie om weerbaarder te zijn tegen moderne ransomware-aanvallen en het stelen van data door kwaadwillenden. iRvN beschikt echter nog niet over voldoende technische middelen om een doelgerichte aanpak op dit gebied te realiseren. De weerbaarheid van iRvN blijft daarom achter bij het actuele iRvN- en gemeente-specifieke dreigingsbeeld. Het doel van iRvN is dan ook om de weerbaarheid in lijn te brengen met het actuele dreigingsbeeld. Deze handelswijze zorgt ervoor dat iRvN over het vermogen beschikt om zowel organisatorisch (CSIRT[1]-RVN,), als technisch inhoudelijk, adequaat en doelmatig te handelen bij alle voorkomende cyberincidenten en -crises.

Het dreigingslandschap van de (lokale) overheid is de afgelopen jaren sterk veranderd in omvang en volwassenheid. Kwaadwillenden werken georganiseerd, internationaal en op hoog technisch niveau. De methodes en technieken welke hierbij worden aangewend staan inmiddels op gelijke voet met die van statelijke actoren. Daarnaast valt hierbij op dat aanvallers niet alleen gericht overheidsorganisaties aanvallen maar ook in hoge mate via ketenpartners bij overheden proberen binnen te dringen. In de onlangs ontvangen brief van Jan van Zanen (voorzitter VNG) wordt hier op basis van de digitale agenda Veiligheid aan gerefereerd.

Het doel van de aanvallers is steevast hetzelfde: financieel gewin. Middels afpersing en het middels versleuteling van gegevens “op slot” houden van de omgeving proberen aanvallers overheden te dwingen tot betaling. Geconstateerd moet worden dat zodra versleuteling succesvol heeft plaatsgevonden, dit tot grote disruptie of zelfs totale uitval van de dienstverlening kan leiden. Deze aanvallen staan ook wel bekend als de zogenaamde ransomware-aanvallan. Dit type van aanval blijft voor de aanvallers uiterst lucratief zolang organisaties de basis v.w.b. cyberhygiëne niet op orde hebben.

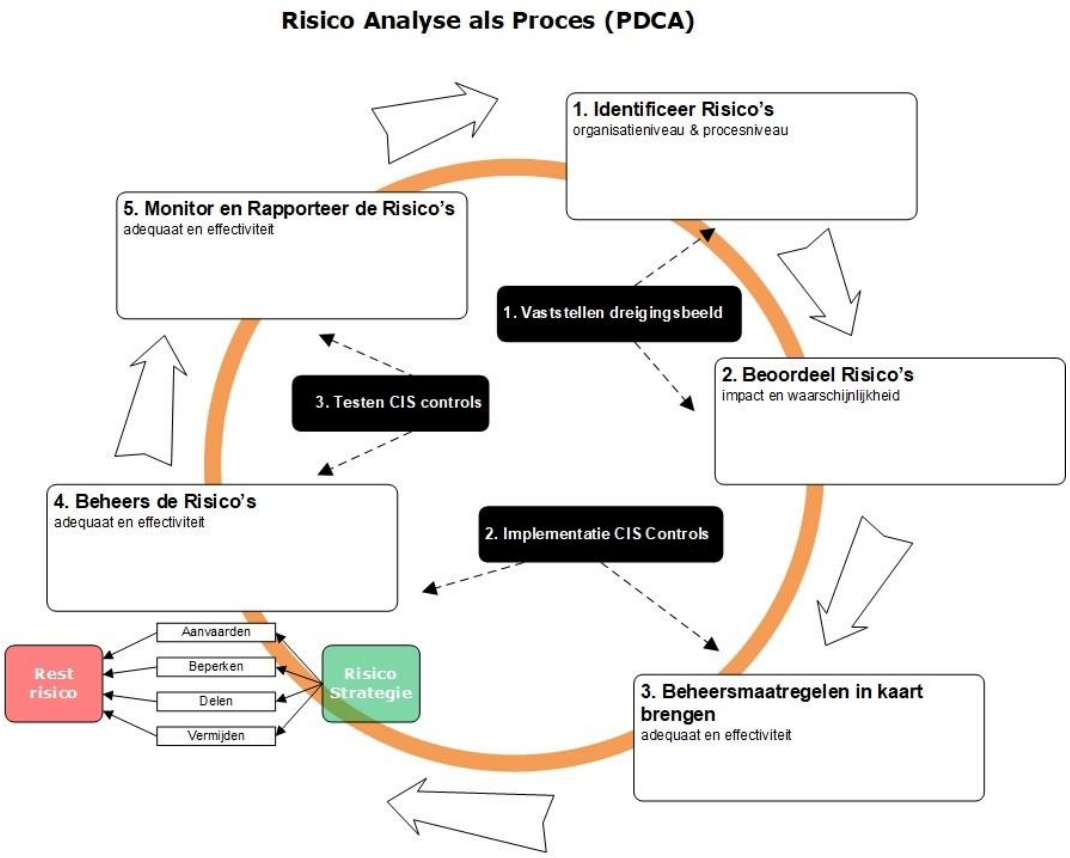
Voorbeelden van succesvolle aanvallen bij vergelijkbare organisaties als iRvN zijn de afgelopen jaren meermaals voorbijgekomen: Universiteit Maastricht, Hof van Twente.



Bron: https://www.businesswire.com/

[1] Cyber Security Incident Response Team

Om het actuele- en specifiek op iRvN gerichte dreigingslandschap in kaart te brengen is i.s.m. Hunt & Hackett een Gap-analyse uitgevoerd. De analyse is uitgevoerd m.b.v. “threat modelling”-methodiek. Mogelijke risico’s welke ontstaan vanuit actuele dreigingen worden hiermee concreet gemaakt en stellen iRvN in staat om de juiste beveiligingsmaatregelen te implementeren. De relatie kwetsbaarheid – dreiging – risico – maatregel worden hierdoor inzichtelijk (plaat IBD).



Een korte samenvatting hierover wordt in hoofdstuk 2 van de Gap-analyse toegelicht.

De uiteindelijke doelstelling van deze exercitie was het opstellen van dit advies en het starten van een regionaal beveiligingsprogramma voor de gezamenlijke IT-infrastructuur om de weerbaarheid tegen, met name ransomware-aanvallen, te vergroten.

3 Onderzoek

3.1 Gap-analyse

Bij de start van de GAP-analyse heeft iRvN samen met Hunt & Hackett inzichtelijk gemaakt welke beveiligingsmaatregelen reeds geïmplementeerd zijn binnen de diverse onderdelen/deelnemers van iRvN.
Deze maatregelen zijn vervolgens vergeleken met de algemeen geaccepteerde standaard op dit gebied: de CIS-implementatiegroepen[2] (link). Ook is hierbij gekeken naar de te monitoren databronnen. De individuele CIS-maatregelen zijn door H&H middels een eigen ontwikkeld “threat & diagnostic”-systeem gekoppeld aan het actuele iRvN-dreigingsbeeld welke op haar beurt is gekoppeld aan de handelswijze (TTP - link) van de voor iRvN relevante aanvalsgroepen (APT - link).

Om het minimale en/of het optimale niveau van beveiligingsmaatregelen te kunnen vaststellen, zijn de volgende analyses samengebracht:

- De uitkomsten van de analyse welke is uitgevoerd met het H&H “threat diagnostic”-systeem;
- Het risico-acceptatieniveau van de organisatie (risicomijdend);
- De eventueel van toepassing zijnde normenkaders (e.g. CIS, NIST, ENISA, BIO, ISO27001-2).

Het optimale securityniveau is hierna vertaald naar;

(1) de benodigde preventiemaatregelen, inclusief eerste set van aanbevelingen;
(2) de benodigde databronnen, t.b.v. juiste detectie van relevantie aanvalsmethodes en;
(3) response maatregelen en/of 'capabilities' als een aanvaller (toch) iRvN succesvol weet te compromitteren.

Hierbij is hoofdzakelijk gebruik gemaakt van de CIS-implementatiegroepen welke waar nodig gekoppeld kunnen worden aan beveiligingsmaatregelen uit andere normenkaders zoals de BIO, NIST en ISO27001.

De geïdentificeerde 'GAPs' zijn hierna vertaald naar concrete projecten. Elk van deze projecten dekt één of meerdere ontbrekende, of nog niet volledig geïmplementeerde beveiligingsmaatregelen af. Elk individueel project kent een prioriteit, investering en doorlooptijd en is op het gebied van uitvoering en implementatie afgestemd op de reeds beschikbare technologie- en (security)-architectuur van iRvN.

3.2 Resultaten

Huidige beveiligingsniveau

Het beveiligingsniveau is onderverdeeld in 3 aandachtsgebieden, namelijk:

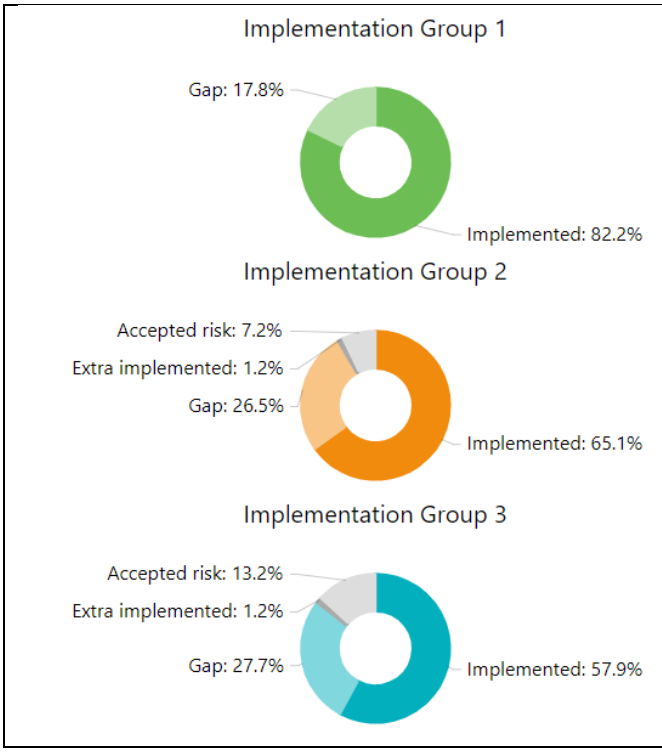
(1) Basis Hygiëne (CIS-maatregelgroep 1)
De ondergrens aan niet-organisatie specifieke beveiligingsmaatregelen welke minimaal moeten zijn geïmplementeerd, zoals: multifactorauthenticatie, autorisatieprocedures, controle op kwetsbaarheden etc.
(2) Reactieve maatregelen (CIS-maatregelgroep 2)
Beveiligingsmaatregelen die de IT-organisatie ondersteunen bij het beheren en beveiligen

[2] CIS: Center for Internet Security is een non-profit organisatie die wereldwijd erkende “best practices” opstelt voor het beveiligen van IT-systemen en data.

van de IT-infrastructuur en het managen en beschermen van de infrastructuur zoals: SIEM-SOC[3], endpoint protectie[4], honeypots[5] etc.

(3) Proactieve maatregelen (CIS-maatregelgroep 3)
Dit zijn beveiligingsmaatregelen waarbij handmatig en actief op zoek wordt gegaan naar kwetsbaarheden in de IT-infrastructuur, activiteiten op het gebied van pentesten[6], applicatiebeveiliging, red teaming[7], etc..

Beveiligingsniveau 3 realiseert een hoger (cyber)volwassenheidsniveau dan beveiligingsniveau 1, maar is qua implementatie afhankelijk van Beveiligingsniveau 1 en 2. Een 100%-score op beveiligingsniveau 3 is daarom alleen mogelijk als er ook een 100%-score is op de niveaus 1 en 2.



De basis hygiëne bij iRvN is redelijk goed op orde. De GAP is slechts 17.8% en is op basis van de huidige effort en financiële middelen goed te sluiten.

De GAP voor niveau 2 is groter maar niet onoverbrugbaar. Hier bevinden zich echter wel de grote projecten in zoals implementatie van een SIEM-oplossing.

Bij de preventiemaatregelen zitten we op 57,9% geïmplementeerd. Een logisch gevolg, aangezien de GAP op niveau 2 eerst noodzakelijke aandacht vraagt.

Conclusie van de GAP-analyse is: We doen het niet slecht, maar er is nog veel winst te behalen.

GAP per niveau

De volgende bevinden zijn voor de basis-hygiëne gevonden:

- Er is onvoldoende aandacht voor het monitoren van kwetsbaarheden. Dit is een gevolg van onvoldoende zicht op de iRvN-infrastructuur, d.w.z. het is niet gedetailleerd inzichtelijk wat zich afspeelt binnen de iRvN-infrastructuur.

[3] SOC staat voor Security Operation Center. Een SOC richt zich op het monitoren van dreigingen en de kwalificatie van incidenten. Om dit te bereiken, gebruiken analisten een tool genaamd “SIEM”, Security Information Management System. Een SIEM integreert software die wordt gebruikt om bedrijfsinfrastructuren te bewaken. Analisten configureren een set correlatieregels volgens het aanbevolen security beleid om mogelijke bedreigingen te detecteren

[4] Endpoint protectie: het proces om een computernetwerk te beschermen zodat de functie van de systemen op het netwerk en de privacy van de informatie niet kan worden aangetast door externe bedreigingen en inbraak

[5] Een honeypot is een computer of een keten van computers die applicaties en data bevatten om hackers te lokken. Het is speciaal opgezet om kwaadwillende hackers aan te pakken en ze in de val te laten lopen

[6] Pentest is een afkorting van ‘penetration testing’. Bij een Pentest gaan legale (ethische) hackers op realistische wijze systemen onderzoeken

[7] Red Teaming is het uit laten voeren van een georganiseerde aanval op een digitale omgeving

    - *Voor het jaar 2022 is de grootste uitdaging inmiddels ondervangen met een jaarcontract met Hunt&Hackett voor het monitoren van onze server- en citrixomgeving middels een EDR[8]-oplossing*
- EDR, maar ook SIEM-SOC, behoren tegenwoordig echt in de standaardinrichting te zijn opgenomen. Traditionele middelen, zoals firewalls en antivirusproducten bieden minimale weerstand tegen huidige dreigingen.
- Het ontbreken van auditlogbestanden waardoor deze niet worden verwerkt en gecontroleerd.
- Achterstallig beheer en onderhoud van de netwerkcomponenten in de infrastructuur. Infrastructurele componenten die verder van het primaire gemeentelijke proces afstaan, staan voor wat betreft urgentie en het installeren van patches en updates op een lager niveau dan bijvoorbeeld een update van een werkplekapparaat of een primaire procesapplicatie.

Vanuit de meer reactieve toepassingen zijn de volgende GAP's geconstateerd:

- Incomplete inventarisatie en beheersing van systemen, ook wel assetmanagement genoemd. iRvN maakt geen gebruik van geautomatiseerd assetmanagement waardoor het handwerk blijft. Dat zorgt voor tekortkomingen.
- Onvoldoende inventarisatie en beheer van software. iRvN heeft afgelopen jaren veel gedaan aan inventarisatie van de software van de primaire processen (regio-breed), maar veel ontbreekt nog. Ook zijn relaties tussen software niet altijd duidelijk (ketenafhankelijkheid). Ook hier geldt dat handwerk zorgt voor tekortkomingen.
- Onvoldoende maatregelen ter verbetering van e-mail- en webbrowserbeveiligingen.
    - *Inmiddels is er een E5-module voor Office365 aangeschaft om dit te verbeteren n.a.v. het Log4j-cyberincident van december 2021. De kosten hiervan zijn opgenomen in de in document genoemde scenario's.*
- Onvoldoende beveiliging inzake malware.
    - *De aangeschafte E5-module lost een gedeelte van het probleem op en met name de EDR-oplossing voor 2022 zorgt voor een adequate dekking van de risico's.*
- Er is geen formeel vastgesteld data-recovery beleid inzake ransomware.
  iRvN is verantwoordelijk voor de technische component en zal in 2022 een aanbestedingstraject starten voor storage en backup waar extra aandacht is voor ransomware-dreiging. Verwacht wordt dat de gezamenlijke Ciso's met tactische beleidsvoorstellen gaan komen zodat beide componenten kunnen worden volbracht.
- Er is geen security awareness-programma voor iRvN-medewerkers, behalve voor de medewerkers die een rol hebben binnen het CSIRT.
  iRvN is per 1 april 2021 begonnen met een CSIRT en de implementatie van de daarbij behorende procedures. Aanvullende activiteiten zijn nodig om weerbaarder te worden.
- Er is geen formeel beleid inzake beheer en omgang met serviceproviders. Iedere organisatie werkt op een eigen manier. De BIO stelt hiervoor kaders- en richtlijnen maar geen concrete voorstellen.
- Er is geen penetratietestprogramma waardoor kritische kwetsbaarheden onopgemerkt kunnen blijven.
  Middels het 1-jarig contract met de EDR-oplossing Carbon Black wordt het serverpark gescand op kwetsbaarheden. Dit is echter een reactieve oplossing. Een penetratietest heeft een breder kader en kan ook een preventief karakter bevatten.

Aan de preventieve kant is reeds een aantal maatregelen genomen zoals bijvoorbeeld het oprichten van een CSIRT. Met als kanttekening dat een aantal van deze preventieve maatregelen nog niet volledig zijn geïmplementeerd:

[8] EDR software (Endpoint Detection en Response) monitort terminals (computers, tablets, mobiele telefoons, enz.)

- Onvoldoende scheiding tussen de verschillende servernetwerken (datacenter-segmentatie), virtuele werkplek en de rest van de infrastructuur ter voorkoming van kruisbesmetting.
- Er is geen Role Based Access Management beleid (RBAC - Rechtenstructuur op basis van rollen).
  Dit traject dient samen met de gemeenten te worden opgepakt.
- Er is onvoldoende scheiding tussen de beheeromgeving en de Kantoorautomatiseringsomgeving van beheerders.
- Er zijn geen cyclische penetratietesten en dus ook geen plan-do-check-act cyclus voor securitymaatregelen.

4 Scenario's

Bij onderstaande scenario's wordt uitgegaan van de huidige iRvN ICT-infrastructuur. De omvang en diversiteit van de ICT-infrastructuur is van invloed op benodigde middelen om de GAP in lijn te brengen met het gewenste beveiligingsniveau. Hoe meer de infrastructuur in volume toeneemt (bijv. aantallen servers en medewerkers) des te meer middelen (licenties, ondersteuning) er nodig zijn om de resultaten te behalen. Dit geldt ook voor de diversiteit: meer platformen (cloud, software, koppelingen) betekent meer "smaken" aan middelen om het gewenste beveiligingsniveau te handhaven.

Vanzelfsprekend heeft dit zijn weerslag op de kosten. Waar leveranciers en fabrikanten vroeger rekenden in voornamelijk eenmalige investeringen aangevuld met een relatief klein bedrag t.b.v. ondersteuning, zijn deze verdienmodellen tegenwoordig omgedraaid: de structurele kosten nemen toe en investeringen (eenmalige kosten) nemen af.

De bestaande iRvN IT-infrastructuur concentreert zich voornamelijk in de on-premise datacenters, welke m.n. sinds de Covid19-crisis wordt aangevuld met Microsoft Office365 cloud-omgevingen. De belangrijkste kengetallen van de IT-infrastructuuromgeving zijn:

- 4.800 eindgebruikers;
- 800 servers (on-premise serverpark);
- 400 VDI-werkplekken[9];
- c.a. 10.000 fysieke werkplekken[10];
- 3 Microsoft Office365 cloudplatformen.

Bij de uitwerking van de scenario's worden niet alleen keuzes gemaakt m.b.t. te implementeren maatregelen om het beveiligingsniveau in lijn te brengen met het dreigingsbeeld maar ook binnen welke onderdelen van de ICT-infrastructuur deze maatregelen worden geïmplementeerd. De minimale variant zal zich bijv. minder of zelfs niet focussen op de werkplekken van de eindgebruikers, waar bij de maximale variant dit wel in de volle breedte wordt meegenomen.

Begrotingstechnisch wordt een inschatting van de verwachte extra materiele exploitatiekosten én de uitbreiding van de formatie (personele kosten) gegeven. Een gedetailleerde begroting is op dit moment nog niet mogelijk aangezien de oplossingen aanbestedingsplichting zijn en een bundeling van oplossingen een prijsvoordeel zou kunnen opleveren. In het uiteindelijke programmaplan zal de aanbesteding een essentieel onderdeel worden.

Bij de projecten worden projectnummers genoemd die gekoppeld zijn aan de projecten beschreven in de GAP-analyse uitgevoerd door Hunt & Hackett.

4.1 Minimale variant

Het scenario 'minimaal' realiseert de ondergrens v.w.b. maatregelen t.a.v. een generiek dreigingsniveau (niet organisatiespecifiek). Dit zijn, zoals eerder beschreven, de maatregelen waarop de laatste jaren flink is gehamerd door o.a. Rijksoverheid, IBD en het NCSC[11]. Het niet-implementeren van deze maatregelen zal met grote zekerheid leiden tot een compromittatie van de iRvN-

[9] VDI, Virtual Desktop Infrastructure (VDI) is een virtualisatieoplossing die virtuele machines gebruikt om virtuele desktops aan te bieden en te beheren. VDI hosts desktopomgevingen op een gecentraliseerde server en implementeert deze op aanvraag voor eindgebruikers. In ons geval wordt hiervoor Citrix gebruikt.

[10] Onder werkplekken vallen, desktops, laptops, tablets en smartphones. Al deze apparatuur wordt gebruikt in de primaire processen van de gemeenten.

[11] Nationaal Cyber Security Centre

infrastructuur. Vanuit de GAP-analyse bezien wordt hierbij gerefereerd aan de set van maatregelen beschreven in CIS-implementatiegroep 1.

Dit scenario creëert een eerste defensieve ring binnen de infrastructuur van iRvN. Echter is de reikwijdte beperkt (interne serverpark) en ligt de focus binnen dit scenario nagenoeg volledig op detectie en niet op preventie. Bij een aanval is men dus altijd 'te laat' maar door detectie kan de schade mogelijkerwijs worden beperkt. Dit laatste is sterk afhankelijk van het type aanval en de gebruikte aanvalsmethoden (TTP) en de mogelijkheden van de kwaadwillende (APT).

Om iRvN en aangesloten gemeenten naar het minimale beveiligingsniveau te brengen is het noodzakelijk om, naast de reeds geïmplementeerde beveiligingsmaatregelen, onderstaande projecten/activiteiten te starten en succesvol tot uitvoering te brengen:

- Herstructuring van de Active Directory (project 1)
- Implementatie endpoint security d.m.v. een EDR-oplossing (project 4)
- Het scheiden van Beheer- en KA-accounts incl. de fysieke werkplek (project 17)
- Volledige implementatie DMARC[12] (project 19)
- Mailbeveiliging ter voorkoming van malafide bestanden (project 20)

Deze minimale variant heeft de volgende begrotingstechnische gevolgen:

- Materiële kosten €500.000,- per jaar
- Personele kosten 1 formatieplaats schaal 9 = €65.000 per jaar

4.2 Maximale variant

Het scenario op basis van de maximale variant gaat uit van volledige implementatie van beveiligingsmaatregelen uit de scenario's minimaal en álle aanvullende, voornamelijk op preventie gerichte, beveiligingsmaatregelen. Hiermee wordt compromittatie in zijn uiterste vorm getracht te voorkomen. Meer dan bij deze vorm van implementatie kan nauwelijks gedaan worden.

Dit implementatieniveau zorgt voor een maximale reikwijdte en zorgt voor meer defensieve ringen. Bijvoorbeeld: endpoint security (EDR) wordt binnen dit scenario niet alleen toegepast binnen de Citrix-omgeving maar ook op de fysieke werkplek en telefoon van de eindgebruiker.

Om dit beveiligingsniveau te bereiken zijn de volgende projecten/activiteiten benodigd:

- Herstructurering van de Active Directory (project 1)
- Implementatie endpoint security binnen de gehele infrastructuur d.m.v. een EDR-oplossing (project 4)
- Het scheiden van beheer- en KA-accounts incl. de fysieke werkplek (project 17)
- Volledige implementatie DMARC (project 19)
- Mailbeveiliging ter voorkoming van malafide bestanden (project 20)
- Implementatie SIEM-SOC dienstverlening (project 3,5,6)
- Implementatie Intune[13]-beveiliging (project 10)
- Definiëren baseline configuraties (project 13)
- Applicatie- en OS (operating system)-patching (project 18)
- Segmentatie datacenter (project 22)
- Ontwikkeling pentestprogramma (project 7)

[12] DMARC (Domain-based Message Authentication, Reporting and Conformance) is een e-mailverificatiesysteem dat de domeinen van de organisatie beschermt tegen spoofing, phishing en andere cyberaanvallen

[13] Middels Microsoft Intune is het mogelijk om alle apparaten van een organisatie te beheren via een cloudservice. Het is mogelijk om een specifiek beleid te configureren om toepassingen te beheren

- Activatie disk-encryptie op alle endpoints (servers, laptops etc.)
- Pentest huidige backup-oplossing (project 21)
- Bewustwording creëren en onboarding programma nieuwe medewerkers (project 8, 23)
- Uitwerking en implementatie assetmanagement (project 28)
- Implementatie van DLP[14] (project 11)
- Implementatie van RBAC[15] (project 16)

Naast projecten die we als iRvN zelfstandig kunnen uitvoeren is er een tweetal trajecten waar ook directe betrokkenheid vereist is vanuit de Gemeenten, namelijk:

- Identity & access management (IAM)
- Werkplekinrichting voor de eindgebruikers

Deze maximale variant heeft de volgende financiële gevolgen:

- Materiële kosten €1,0mln en 1,3 mln per jaar
- Personele kosten 2 formatieplaatsen schaal 10 = €150.000 per jaar

4.3 De Gulden Middenweg

Tussen maximaal en minimaal zit een middenweg. Hierbij worden de projecten uit scenario 'minimaal' aangevuld met overige projecten. Scenario 'de gulden middenweg' realiseert "de basis op orde" en zet een extra stap in richting van preventie- en detectiemogelijkheden. Om dit te realiseren wordt met name gekeken naar de maatregelen welke zijn beschreven in de CIS-implementatiegroep 2.

Daarnaast wordt de reikwijdte van dit scenario binnen de infrastructuur van iRvN vergroot t.o.v. de minimale variant. Dat wil zeggen dat de defensieve ring welke in scenario 'minimaal' gelegd wordt rond het serverpark, aangevuld wordt met extra ringen (bijv. werkplekbeveiliging). Hierdoor worden ook de monitoring en detectiemogelijkheden vergroot, waardoor een aanval in een vroeger stadium kan worden gedetecteerd, maar ook kan worden gekoppeld aan een zogenaamde geautomatiseerde reactie.

- Herstructurering van de Active Directory (project 1)
- Implementatie endpoint security binnen de server- en VDI-omgeving d.m.v. een EDR-oplossing (project 4)
- Het scheiden van beheer- en KA-accounts incl. de fysieke werkplek (project 17)
- Volledige implementatie DMARC (project 19)
- Mailbeveiliging ter voorkoming van malafide bestanden (project 20)
- Implementatie SIEM-SOC dienstverlening (project 3,5,6)
- Implementatie Intune-beveiliging (project 10)
- Definiëren baseline configuraties (project 13)
- Applicatie- en OS patching (project 18)
- Segmentatie van het datacenter (project 22)
- Ontwikkeling pentestprogramma (project 7)

Op basis van het advies van de Ciso's en I-adviseurs worden het volgende toegevoegd:

- Structureel pentesten door externe partijen (project 7 en 21)
- Implementatie van assetmanagement (project 28)

[14] Data Loss Prevention

[15] Role-Based Access Control

Deze gulden middenweg variant heeft de volgende begrotingstechnische gevolgen:

- Materiële kosten €800.00 per jaar
- Personele kosten 1 formatieplaatsen schaal 10 = €85.500 per jaar

Samengevat:

Maatregel	**min**	**mid**	**max**
Herstructurering van de Active Directory (project 1)	X	X	X
Implementatie endpoint security binnen de gehele infrastructuur d.m.v. een EDR-oplossing (project 4)	X	X	X
Het scheiden van beheer- en KA-accounts incl. de fysieke werkplek (project 17)	X	X	X
Volledige implementatie DMARC (project 19)	X	X	X
Mailbeveiliging ter voorkoming van malafide bestanden (project 20)	X	X	X
Implementatie SIEM-SOC dienstverlening (project 3,5,6)		X	X
Implementatie Intune-beveiliging (project 10)		X	X
Definiëren baseline configuraties (project 13)		X	X
Applicatie- en OS patching (project 18)		X	X
Segmentatie datacenter (project 22)		X	X
Ontwikkeling pentestprogramma (project 7)		X	X
Activatie diskencryptie op alle endpoints (servers, laptops etc.)			X
Pentest huidige backup oplossing (project 21)		X	X
Bewustwording creëren en onboarding programma nieuwe medewerkers (project 8, 23)			X
Uitwerking en implementatie assetmanagement (project 28)		X	X
Implementatie van DLP (project 11)			X
Implementatie van RBAC (project 16)			X
Materiële jaarlijkse kosten (x 1000)	500	800	1.300
Personele jaarlijkse kosten (x 1000)	70	85,5	140

5 Advies

5.1 Advies iRvN

iRvN adviseert de deelnemers om akkoord te geven op het scenario van “De Gulden Middenweg” en het opstarten van het gezamenlijke traject inzake Identity & Access Management (IAM). Voor de laatste zal een separaat voorstel worden gemaakt. De verwachte exploitatiekosten zijn reeds opgenomen in het advies.

5.2 Uitgangspunten programma

Tijdens de GAP-analyse is ook een aantal zaken besproken dat vooral meer betrekking heeft op de taken en verantwoordelijkheden die bij de gemeenten zijn gebleven. Dit advies beperkt zich tot de taken en verantwoordelijkheden die bij de iRvN belegd zijn. Het gaat dan ook vooral om infrastructurele maatregelen. Overige maatregelen horen in eerste instantie thuis bij het Ciso-overleg waar iRvN aan deelneemt.
De volgende randvoorwaarden worden gesteld:

- Eindverantwoordelijke voor het programma is iRvN. iRvN zal tijdens het kwartaaloverleg met de hoofdenbedrijfsvoering de collega’s informeren over de voortgang.
- Opdrachtgever is directeur iRvN, opdrachtnemer is een nog aan te stellen programmamanager.
- Het structurele budget voor het programma en de beheerfase wordt additioneel toegevoegd aan de begroting van iRvN. Er wordt in het beveiligingsprogramma geen rekening gehouden met positieve resultaten op de overige infrastructurele onderdelen.
- Het betreft een programma van 3 jaar dat elk jaar herijkt zal worden op basis van de ontwikkelingen op security gebied.
- Programma betreft alleen maatregelen op infrastructurele componenten, procedures etc. die onder verantwoordelijkheid van iRvN vallen. Saas-oplossingen, hostingafspraken ect. die onder verantwoordelijkheid vallen van de deelnemende partijen worden niet opgenomen in dit programma.
- In het realiseren van de projecten dient ICT-Beheer een actieve bijdrage te leveren.
- Buiten scope valt de VMC/RTC-omgeving. Deze omgeving wordt volledig door VMC beheerd met uitzondering van de kantoorwerkplekken.

5.3 Organisatie

Ten tijde van het programma zijn de volgende functies en rollen van belang:

Functie	**Rol**	**Toelichting**
Manager ICT-Beheer	Opdrachtgever	Manager ICT-Beheer is eindverantwoordelijk voor het beheer, onderhoud en doorontwikkeling van de infrastructuur. Beveiliging op deze infrastructuur valt onder zijn verantwoordelijkheid
Hoofden Bedrijfsvoering	Stakeholders	Vormen te samen het opdrachtgeversplatform richting iRvN en zijn verantwoordelijk voor de ICT-budgetten van hun organisatie.
Coördinatoren ICT-Beheer	Leverancier	Leveren mankracht en dragen bij een vlekkeloze inbeheername
Programmamanager	Programmamanager	Verantwoordelijk voor de aansturing van het Programma
Security Officer	Stakeholder	Verantwoordelijk voor de kwaliteitsborging
Ciso’s	Klankbordgroep	Mede verantwoordelijk voor de invoering van o.a. de BIO voor hun organisatie.

5.4 Exploitatiebegroting

Op basis van de projecten in scenario “De Gulden Middenweg” hebben we een inschatting gemaakt van de exploitatiekosten per oplossing. De initiële kosten worden opgesteld bij het programmaplan waarbij het uitgangspunt is dat iRvN deze kosten in eerste instantie op zich zal nemen vanuit het inhuurbudget en de investeringsbegroting.

Project	**Geschatte exploitatiekosten**
EDR	€ 150.000
SOAR	€ 25.000
24x7 detection en response	€ 40.000
Threathunting	€ 40.000
Beveiligingsadvies	€ 4.000
SIEM/SOC	€ 250.000
Mailbeveiliging	€ 80.000
identity & Accesmanagement	€ 60.000
Monitoring netwerk	€ 45.000
Honeypots	€ 6.000
Pentesten	€ 65.000
Assetmanagement	€ 35.000
Formatieplaats (schaal 10)	€85.500
	€ 885.500

De groei van de exploitatie zal geleidelijk zijn, namelijk:

1. 2022 € 300.000,-
2. 2023 € 675.000,-
3. 2024 € 750.000,-
4. 2025 € 885.500.-

De kosten voor de bijdragen per Gemeente wordt op basis van het eindbedrag uitgebreid met:

Gemeente	**Jaarlijke bijdrage Incl. formatie**
Nijmegen	€ 480.000,00
WDW	€ 117.000,00
Berg en DAL	€ 58.500,00
WBRN	€ 67.000,00
ODRN	€ 45.500,00
Beuningen	€ 63.000,00
Heumen	€ 36.000,00
Mook & Middelaar	€ 18.500,00
	€ 885.500,00

5.5 Het traject

Om te komen tot een gerealiseerd beveiligingsprogramma wordt, na akkoord, het volgende traject geadviseerd:

1. Collectief Collegevoorstel
2. Akkoord Colleges
3. Werven Programmamanager
4. Programmaplan opstellen
5. Goedkeuring programmaplan
6. Europese aanbesteding
7. Projectplannen opstellen
8. Projecten uitvoeren, implementeren en in beheer nemen
9. Afronding