CYBERSPRINT
BREAKTHROUGH SECURITY

WHITEPAPER

BIO EN GGI-VEILIG

MET ATTACK SURFACE MANAGEMENT

www.cybersprint.com // info@cybersprint.com // +31 70 22 12 892

BIO EN GGI-VEILIG MET ATTACK SURFACE MANAGEMENT

CONTEXT

De Baseline Informatiebeveiliging Overheid (BIO) is nu ongeveer anderhalf jaar van kracht. Het biedt gemeenten, het Rijk, waterschappen en provincies de handvatten om het niveau van hun Information Security Management System (ISMS) te peilen en verbeteren.

Het doel van een ISMS is onder andere het continu beoordelen van welke beveiligingsmaatregelen passend en effectief zijn en deze indien nodig bij te stellen. Het legt de basis voor andere beveiligingsmaatregelen binnen een gemeente, en dient daarom voor langere tijd effectief te zijn en onderhouden te worden.

Dat onderhouden kan weer aan de hand van verschillende processen. In het kader van de Digitale Agenda 2020 heeft de Vereniging van Nederlandse Gemeenten (VNG) de Gemeentelijke Gemeenschappelijke Infrastructuur (GGI) gerealiseerd. De GGI zorgt voor een veilige infrastructuur tussen de gemeenten en andere overheden. Eén van de onderdelen hierin is de GGI-Veilig module. Het is bedoeld voor de operationele informatiebeveiliging, en geeft een systeem voor de toetsing van de ‘volwassenheid digitale weerbaarheid’ (VDW) van gemeenten.

Dit paper legt uit hoe de toetsing van de GGI-Veilig VDW is opgebouwd. Daarnaast legt het een link tussen specifieke aspecten uit de module, en hoe deze structureel verbeterd kunnen worden met behulp van Attack Surface Management.

GGI-VEILIG VDW

De overheidssector heeft de laatste jaren een stroomversnelling van digitalisering meegemaakt. De decentralisatie van taken van het Rijk[1] zorgt voor grotere verantwoordelijkheden voor gemeenten. Dienstverlening en onderlinge samenwerking gebeurt steeds meer digitaal, zowel tussen gemeentes, als via leveranciers en ketenpartners. Deze ontwikkelingen zorgen op hun beurt weer voor strengere wet- en regelgeving om de informatiebeveiliging en privacy-waarborging te kunnen reguleren.

Op deze manier wordt de noodzaak voor efficiënte informatiebeveiliging van meerdere kanten gedreven, los van de dreiging van cybercriminaliteit. Hoe beter een (gemeentelijke) organisatie de beveiliging op orde heeft, des te kleiner is de kans dat het een doelwit wordt. Daarnaast is het IT team significant minder tijd kwijt met het detecteren van mogelijk besmette systemen in het geval er toch een (malware) aanval plaatsvindt — een scenario waarin handelingssnelheid bovenaan staat.

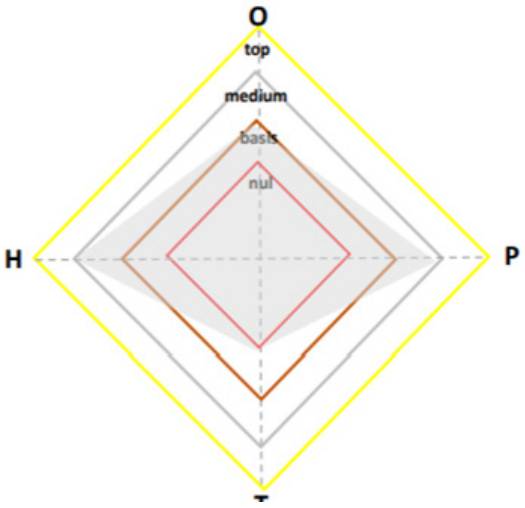
Het baat dus een hoge ‘volwassenheid digitale weerbaarheid’ te hebben. Maar hoe is dit te meten? Hiervoor bestaat het onderstaande model uit de VGN realisatie[2], waarin de volwassenheid op vier assen is onderverdeeld.

O = organisatie

H = personeel

P = processen

T = techniek



Per kwadrant kan er vervolgens aangegeven worden op welk niveau de beveiliging zich bevindt, uitgedrukt in nul tot top. Zo kan een gemeente een GGI-Veilig VDW score hebben van bijvoorbeeld

O - basis

H - medium

P - medium

T - nul.

Vanuit het perspectief van digitale veiligheid zijn voor alle assen maatregelen te treffen om de gemeentelijke organisatie te beschermen. Echter, voor dit paper wordt de aandacht geschonken aan de Technische aspecten, en hoe deze te indexeren en verbeteren zijn met behulp van een overkoepelende oplossing: Attack Surface Management. Tevens wordt belicht hoe het verbeteren van de Technische aspecten ook meetbare voordelen heeft voor andere kwadranten.

KWADRANTSCORES

Om tot een niveau per kwadrant te komen, zijn er richtlijnen gesteld op basis van vier factoren. Per factor kan een gemeente weer nul, basis, medium, of top scoren. Dit wordt toegekend aan de hand van meerdere eigenschappen en de procesindeling binnen de organisatie. Zo wordt er voor de kwadrant Techniek gekeken in hoeverre een gemeente beschikt over een proces voor:

- T1 = Centraal ISM;
- T2 = Compliancy en ICT configuratiebeheer;
- T3 = Incidentmelding en -monitoring;
- T4 = Geautomatiseerde incident detectie.

Samen genomen vormt dit de overkoepelende score voor het gehele kwadrant.

Om een hoge score voor het kwadrant Techniek te behalen — en dus aan de opgelegde standaard van de BIO te voldoen — moeten de procesmatige en technische aspecten in orde zijn. Hieruit volgt automatisch

	NUL	BASIS	MEDIUM	TOP
T1	Geen (centraal) ISM. Documentatie wordt los bewaard.	Er is een ISM systeem, waarvan de CISO de beheerder is. Het systeem wordt niet meegenomen in het jaarlijkse beveiligingsbeleid.	Portefeuillehouder is eigenaar van het ISM systeem, en de CISO de beheerder. Het systeem wordt actief gebruikt in het jaarlijkse beveiligingsbeleid.	Alles in Medium + de werking van het ISM wordt periodiek geëvalueerd voor continue verbetering.
T2	Geen ICT configuratiebeer en compliancy vindt niet plaats.	Er is een ICT configuratie systeem. Compliancy is voldoende betrouwbaar op moment van toetsing.	Het ICT configuratiesysteem wordt gebruikt voor het bijhouden van meerdere facetten, zoals wijzigingen, certificaten, en autoriteit beheer. De compliancy data geeft een betrouwbaar beeld.	Alles in Medium + compliancy meeting gebeurt op 'live' data en gegevens vormen een extra controle voor configuratiebeheer.
T3	Geen incidentmelding en -monitoring	Er bestaat een systeem voor melding en monitoring waarin een audit trail wordt vastgesteld.	Het incidentmelding en -monitoring systeem legt een geheel audit trail vast en is deel van het ISM systeem.	Alles in Medium + effectievere toetsing en verbetering van mitigatie processen.
T4	Geen geautomatiseerde incident detectie	Er is een systeem voor de collectie en analyse van logdata voor reactieve incident detectie.	De organisatie beschikt over een SIEM voor analyse en pro- en reactieve incident detectie, en vulnerability scanning. SIEM is gekoppeld aan bestuurlijke processen.	Alles in Medium + periodieke evaluatie en verantwoording met een proces van continue verbetering.

de vraag: Hoe kan de organisatie dit zo efficiënt mogelijk bereiken? Er bestaan losse oplossingen en tools om de individuele processen in te richten, maar dit is vaak veeleisend qua kosten en de benodigde werkuren, of lastig te integreren met andere oplossingen. Daar komt bij dat de snel veranderende digitale omgevingen van gemeenten en de toenemende rol van de keten van leveranciers en derde partijen zorgen voor een complexer system, wat lastig in één overzicht te bevatten is.

Door een ander perspectief te hanteren is het echter mogelijk met één methode inzichten te creëren voor alle vier de eigenschappen die hierboven staan genoemd. Er is een plek waar al deze factoren samensmelten: De digitale ontwikkelingen; de noodzaak om aan de regelgeving te voldoen; en het kunnen voorkomen van digitale aanvallen — allen komen ze samen in het digitale aanvalsoppervlak van de gemeente. Attack Surface Management (ASM) biedt een methode om dit in kaart te brengen en te managen.

HOE IS ATTACK SURFACE MANAGEMENT TOEPASBAAR?

Een aanvalsoppervlak is de totale som van open en aan het internet gekoppelde assets, met de bijkomende risico's die een hacker kan gebruiken voor een digitale aanval. Pas wanneer het aanvalsoppervlak volledig is gedetecteerd en geïnventariseerd heeft een IT team inzicht in zaken zoals:

- welke assets eigendom zijn van de gemeente;
- waar de zwakke plekken zitten;
- hoe de risico's het beste gemanaged kunnen worden;
- welke software in gebruik is en waar die draait;
- welke derde partijen bij de gemeente zijn aangesloten;
- welke governance / compliance processen verbeterd kunnen worden;
- wie verantwoordelijk is voor welke omgevingen;
- of de CMDB volledig is en hoe deze het beste gemanaged kan worden;
- welke omgevingen beter getest moeten worden.

De methode is te gebruiken om alle vier de toetsings-eigenschappen binnen het Techniek kwadrant te meten en optimaliseren. De toepassing wordt hieronder per onderdeel uitgelicht.

T1. CENTRAAL ISM

Er bestaat een sturende wisselwerking tussen Attack Surface Management (ASM) en het gebruik van het Information Security Management (System). Het ISMS is een verzameling van processen die samen zorgen voor de sturing van totale informatiebeveiliging. Op deze manier kan richting worden gegeven aan security en kunnen onderdelen van de IT volgens bepaalde standaarden blijven functioneren. De governance en strategische draagkracht van het ISMS heeft invloed op de indeling van de digitale assets. Tegelijkertijd kunnen deze assets perspectief bieden over hoe het ISMS functioneert.

Het Attack Surface Management platform van Cybersprint vindt de digitale assets van de organisatie op een geautomatiseerde manier, met behulp van een veelvoud aan tools en plugins, aangevuld met het gebruik van kunstmatige intelligentie en de input van analisten. Het

sterke aan deze methode is dat er van buitenaf naar het aanvalsoppervlak wordt gekeken, zonder een vooraf opgelegd kader. Hierdoor worden blinde vlekken voorkomen en heeft de gemeente een realistisch beeld van het eigen aanvalsoppervlak - inclusief de aangesloten leverancierskeketen.

ASM biedt de juiste inzichten in het totale aanvalsoppervlak, waardoor de link gelegd kan worden naar de sturing van de achterliggende processen. Doordat ASM een overzicht geeft van de risico's worden de sterke en zwakke punten zichtbaar. Wanneer er meer van een specifiek type risico wordt gevonden, of bijvoorbeeld gecentreerd in één bepaald stuk van de digitale omgeving, is dit een indicatie om ook naar de desbetreffende ISMS processen te kijken. Zijn deze nog wel toereikend? En waar kunnen ze verbeterd worden voor de langere termijn? Daarnaast wordt duidelijk welke ISMS-onderdelen juist goed functioneren, als er op deze gebieden weinig (grote) risico's worden gevonden. Deze processen kunnen dienen als ISM best practices.

Zo biedt ASM input voor de priorisering van het ISMS op lange termijn, voor een continue verbetering van de strategische en governance processen van de informatiebeveiliging. Wat werkt goed, wat werkt minder goed, en wat moet nog worden toegevoegd?

Met inzicht in de digitale assets en risico's rijst de vraag wie eigenaar is van de assets. Dit is niet altijd goed belegd binnen organisaties. Op papier kan iemand verantwoordelijk zijn voor een asset, maar voelt hij/zij zich ook eigenaar? En daarmee dus ook eigenaar van de eventuele security kwetsbaarheid en risico? Bovendien: wat wordt er gedaan met assets die nog aan niemand toebedeeld zijn? ASM geeft de inzichten om eigenaarschap te kunnen bepalen — expliciet op basis van data en volledig rapporteerbaar.

Het toekennen van eigenaarschap en verantwoordelijkheden is fundamenteel voor de borging van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Hiermee zet een organisatie de stap naar niveaus medium en top. Wanneer ook dit duidelijk is, dan is het vervolgens mogelijk om de verantwoordelijke functionarissen, bijvoorbeeld op basis van

T2. COMPLIANCY EN ICT BEHEER

Wanneer inzichtelijk is welke digitale assets kwetsbaarheden bevatten en welke risico's daarbij horen, kan er prioriteit gegeven worden aan de meest kritieke systemen, en bijvoorbeeld een change management proces gestart worden.

Het ASM platform verzamelt continu relevante en actuele data over de assets (denk hierbij ook aan informatie over de geldigheid van certificaten) en vormt daarmee een goede bron voor het onderhoud van de CMDB.

Daarnaast beschikt een gemeente altijd over een actueel en volledig overzicht van haar assets in de CMDB door een integratie tussen het ASM platform en de CMDB. Hierin wordt de status (waaronder de reeds genomen technische security maatregelen) en de security kwetsbaarheden en risico's (inclusief risicoclassificatie) allemaal meegenomen.

Kortom, CISO's hebben hiermee te allen tijde een betrouwbaar beeld van de werkelijkheid en verkleinen meetbaar het online aanvalsoppervlak van hun organisatie, na doorvoeren van de benodigde mitigerende maatregelen. De verkregen data uit het ASM platform is na meerdere scans en detectiemethoden zo relevant en actiegericht als mogelijk.

Tevens vormt de data, verwerkt in het ASM-platform, de basis voor het opzetten van periodieke penetratietesten of technische security assessments. Deze asset en vulnerability data kan de gemeente gebruiken om de exacte scope, doelstellingen en aanpak van specifieke onderzoeken te bepalen.

T3. INCIDENTMELDING EN -MONITORING

Het melden, afhandelen en monitoren van kwetsbaarheden en risico's zit verwoven in het volledige IT beveiligingsproces. Zowel automatisch gevonden risico's, als meldingen vanuit de volledige organisatie moeten een plek krijgen in het systeem. Het accuraat bijhouden en het inrichten van een systeem voor deze stappen heet het audit trail.

Het vastleggen van een audit trail brengt de organisatie van Nul naar Basis. De voorwaarde voor de volgende stap is het verwerken van dit audit trail in het ISM. Het ASM platform van Cybersprint maakt deze automatische vastlegging en monitoring mogelijk door risico's over tijd

te kunnen waarnemen. Daarnaast kunnen de resultaten en efficiëntie van de gebruikte tooling en bestaande processen waargenomen worden. Dit faciliteert de stap naar het niveau Top, door de verkregen data en inzichten te gebruiken in periodieke evaluaties en verbeteringen. Dit is in veel gevallen tevens toepasbaar op IT processen in de gehele gemeentelijke organisatie. Zodoende dient het als input voor de overige kwadranten, met name voor Processen en Organisatie.

T4.

GEAUTOMATISEERDE INCIDENT DETECTIE

Een belangrijk onderdeel van cyber security is het hebben van actuele dreigings-informatie en het tijdig kunnen signaleren van beveiliging incidenten en events. Niet alleen het security incident managementproces is belangrijk na een succesvolle cyberaanval, maar ook de real-time alarmering op het moment van een incident of event zelf[3]

Het gebruik en integratie van Cybersprints ASM platform met de SIEM of SOC van de gemeente is hierin een belangrijk hulpmiddel naar een score van Medium en Top. Het komt (te) vaak voor dat een IT Security team op de hoogte wordt gesteld van een incident, maar hier nog niet direct op kan acteren omdat de besmette systemen eerst in kaart gebracht moeten worden. Dit komt vooral voor bij incidenten via de leverancierskeketen, zoals met de Citrix en Microsoft Exchange kwetsbaarheden in 2019 en 2020-2021.

Wanneer in het SIEM / SOC eerst gezocht moet worden naar de desbetreffende software en de gekoppelde data, neemt dat kostbare tijd in beslag. Tijd die beter besteed kan worden met het patchen en hardening van de systemen.

Door gebruik van het ASM platform is deze informatie altijd beschikbaar. Tevens kan er door slimme en personaliseerbare filteropties direct een lijst van gemeenschappelijke assets gemaakt worden, en over tijd gemonitord worden. Dit vergroot de effectiviteit van het SIEM / SOC aanzienlijk.

MET ASM NAAR BIO-CONFORM

Ter conclusie: door gebruik te maken van de handvatten van de GGI-Veilig VDW, kan een gemeentelijke organisatie dus op een georganiseerde wijze voldoen aan de doelstellingen van de BIO. Attack Surface Management biedt hierin één centrale oplossing om de verschillende facetten binnen deze richtlijnen te ordenen, monitoren, en verbeteren.

Een voorbeeld van een gemeente die dit proces al langer doorloopt is de gemeente Den Haag. In de afgelopen 10 jaar is er veel aandacht geschonken aan het opzetten en verbeteren van de digitale veiligheid, innovatie en transparantie op dit vlak.

Voor een directe link van de theorie naar de praktijk hebben wij de gemeente geïnterviewd. Hierin legt Information Security Manager Peter van Eijk uit hoe de gemeente deze groei heeft gemaakt - van de eerste stappen naar de toekomstige projecten. Ook hier heeft het Attack Surface Management platform van Cybersprint een rol in gespeeld.

Lees het interview hier.

BRONNEN

1. https://www.rijksoverheid.nl/onderwerpen/gemeenten/decentralisatie-van-overheidstaken-naar-gemeenten#:~:text=Gemeenten%20zijn%20sinds%202015%20verantwoordelijk,Dit%20heet%20ook%20wel%20decentralisatie.
2. https://www.vngrealisatie.nl/sites/default/files/2018-06/GGI-Veilig%20VDW%20_0.pdf
3. Eenvoudiger en veiliger digitaal dienstverlenen GGI-Veilig / Volwassenheidsmodel Digitale Weerbaarheid, juni 2018
4. https://www.cybersprint.com/blog/controlling-risks-at-the-municipality-of-the-hague

MEER WETEN?

CONTACT ROBERT GEBHARDT

+31 6 39 84 04 11
r.gebhardt@cybersprint.com

ABOUT CYBERSPRINT

Cybersprint maps the attack surface of organisations and brands. We offer full visibility using continuous and automated digital asset discovery. Our zero-scope approach provides an outside-in perspective, eliminating blind spots.

Assets are individually scanned for a multitude of risk types. These insights empower cybersecurity professionals to prioritise the mitigation of vulnerabilities. Our integrated AI correlates dozens of data sources and uses a multitude of scanners, making risk relevant.

Cybersprint's SaaS platform allows organisations to manage and monitor risks with customisable filters and alerts, integrated into existing processes. Detect and prevent threats such as phishing, brand abuse, data theft and more.

Visit www.cybersprint.com