GGI-Veilig

De 3 percelen uitgelegd

KPN Security

Burgers en ondernemers weten de digitale overheid steeds beter te vinden. Dat geldt helaas ook voor cybercriminelen. Steeds meer gemeenten hebben dan ook al eens te maken gehad met bijvoorbeeld malware, ransomware of andere pogingen om de dienstverlening te verstoren. Om het voor gemeenten zo eenvoudig en efficiënt mogelijk te maken hun digitale weerbaarheid te vergroten heeft VNG Realisatie GGI-Veilig ontwikkeld. GGI-Veilig is onderdeel van de Gemeentelijke Gemeenschappelijke Infrastructuur en biedt actieve netwerk monitoring om dataverkeer op het eigen bedrijfsnetwerk te bewaken. Naast monitoring biedt GGI een robuust scala aan security producten en diensten waarmee ook uw gemeente haar digitale weerbaarbaarheid kan verhogen.

Inkoop voordeel en kwaliteitsgarantie
De oplossingen van GGI-veilig worden in drie percelen aangeboden door leveranciers die allemaal voldoen aan de strikte eisen gesteld door het IBD. Als deelnemende gemeente bespaart u zo op uw aanbestedingskosten en bent u ervan verzekerd dat de geboden oplossingen blijvend voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). Tot slot draagt GGI-Veilig bij aan een betere kennisdeling tussen gemeenten en leveranciers waardoor er collectief wordt gewerkt aan een betere digitale weerbaarheid.

Perceel 1:
MONITORING EN DETECTIE MET SIEM/SOC-DIENSTVERLENING

Cybercriminelen zijn constant op zoek naar zwakke plekken in netwerken. Deze zwakke plekken kunnen technisch van aard zijn, maar kunnen ook ontstaan door – veelal onbedoelde - gebruikers of configuratiefouten. Daarom is het belangrijk dat u te allen tijde zicht heeft op verdachte activiteiten rondom en in uw netwerk en applicatie landschap.

Gemeentelijke netwerken worden daarbij steeds complexer. Uw applicaties en data bevinden zich allang niet meer alleen binnen uw bedrijfsnetwerk maar ook in de cloud - denk aan de SaaS applicaties waar uw gemeente gebruik van maakt, de ontwikkeling van de GGI-cloud en de data die u uitwisselt met de Generieke Digitale Infrastructuur (GDI).
De BIO stelt dan ook hoge eisen aan de detectie- en monitoring oplossingen waarmee u direct op de hoogte bent van verdachte activiteiten, zowel binnen uw eigen infrastructuur als daarbuiten. Deze oplossingen worden aangeboden als SIEM/SOC-dienstverlening in perceel 1.

Met SIEM/SOC-diensten bent u altijd direct op de hoogte van uw actuele security en compliance status. Daarmee verkleint u de kans dat de beschikbaarheid en integriteit van uw informatiesystemen in gevaar komen.

Wat biedt KPN Security?
KPN Security is binnen perceel 1 de enige aanbieder en we beseffen ons dat dat een grote verantwoordelijkheid met zich mee brengt. Onze SIEM/SOC-dienstverlening wordt aangeboden als een managed security service en dat maakt ons als Managed Security Service Provider (MSSP) verantwoordelijk voor:

- De inrichting en beveiliging van uw centrale SIEM/SOC-dienstverlening
- Het verzorgen van trainingen en opleidingen met betrekking tot het gebruik van het SIEM-systeem en de SOC-diensten
- De koppeling van de SIEM/SOC-dienstverlening met de securityoplossingen uit perceel 2
- Het tijdig signaleren en inzichtelijk maken van security en compliance risico's zodat u in staat bent om de beschikbaarheid en integriteit van uw dienstverlening te beschermen

Alle security informatie en incidenten worden gecorreleerd en geanalyseerd. Op basis van deze analyses kunnen onze securityconsultants u adviseren over mitigerende maatregelen. Nota bene; de uitvoering van deze maatregelen wordt gedekt met security oplossingen in perceel 2.

Toekomstvaste security oplossingen voor een veilige gemeente
Om de gemeente en de gemeenschappelijke infrastructuur adequaat te bewaken, is het belangrijk dat er een compleet beeld bestaat van het dreigingslandschap. Vanuit onze positie als provider zijn we onderdeel van de Vitale Infrastructuur van Nederland en gesterkt door ons eigen SOC – waardoor we kunnen putten uit hoogwaardige bronnen aan dreigingsinformatie. De generieke security intelligence en benchmark-data die we hieruit opdoen, delen we via onze samenwerkingsverbanden met het Nationaal Cyber Security Center zodat we Nederland veilig houden, nu en in de toekomst.

Aanpak, werkwijze en doorlooptijd
De SIEM/SOC-dienstverlening die we aanbieden in het GGI-portfolio kent vier niveaus: Start, Basis, Medium en Optimaal. In niveau 'Start' monitort u de meest invloedrijke logbronnen voor uw inkomend en uitgaand verkeer. In niveau 'Optimaal' monitort u uw complete infrastructuur inclusief bedrijfskritische applicaties. Vanaf niveau 'Medium' voldoet u met een aantal specifieke controls aan de BIO vereisten. De ervaring leert dat voor niveau 'Optimaal' de doorlooptijd kan oplopen tot meer dan één jaar. Dit is uiteraard afhankelijk van uw vastgestelde security volwassenheidsniveau. We adviseren u dan ook om op tijd te beginnen zodat u anticipeert op de wettelijke verankering van de BIO.

Ongeacht het niveau richten we de dienstverlening altijd in aan de hand van een gefaseerde en cyclische aanpak. Daarin onderscheiden we drie fases:

1. Initiatie
In deze fase vindt een technische inventarisatie van de infrastructuur plaats die de basis vormt voor een technisch ontwerp. Dit is het uitgangspunt voor de configuratie van de benodigde beveiligde koppelingen van uw netwerk met ons SOC. Aan het eind van deze fase hebben we - in samenwerking met uw IT-medewerkers - de technische en organisatorische randvoorwaarden voor SOC/SIEM diensten geïmplementeerd.

2. Opstart
In deze fase vinden de eerste testen plaats, gevolgd door een akkoord voor een go-live. Ook stellen we de ondersteunings- en nazorgprocessen vast. Denk hierbij aan het inrichten van de servicedesk, het instellen van algemene rapportages en het optimaliseren van configuratie-instellingen van de dienstverlening. Aan het eind van deze fase kan de SIEM/SOC-dienst in gebruik worden genomen door uw gemeente.

3. Oplevering
Na oplevering actualiseren we de SIEM/SOC-dienstverlening continu. Dat doen we onder andere door in de monitoringsresultaten de zogenaamde false positives en false negatives terug te dringen. Ook kijken we samen met de deelnemende gemeenten hoe we de opvolging van incidenten en mitigatie van risico's kunnen optimaliseren. Zo is uw gemeente continu verzekerd van tijdige en juiste signalering van beveiligingsrisico's

Perceel 2: AANVULLENDE SECURITYSERVICES

Hackers en cybercriminelen innoveren hun aanvalstechnieken continu. Dat betekent dat uw IT-infrastructuur 24x7 beschermt moet zijn met bewezen technologie dat altijd up-to-date is. Deze oplossingen kunt u afnemen in perceel 2 van GGI-Veilig.

Perceel 2 biedt producten en diensten die uw netwerk, applicaties en data beschermen tegen ongeautoriseerde toegang en ervoor zorgen dat ook mobiele apparaten (end points) veilig kunnen worden gebruikt. Hieronder vallen ook oplossingen die actief cyberaanvallen blokkeren, zoals de activatie van malware of DDoS aanvallen. Deze middelen vormen samen het digitale hang- en sluitwerk van uw IT-infrastructuur en zijn nodig om te voldoen aan de BIO.

Wat biedt KPN Security?
Een overzicht van onze security oplossingen;
- Cloud Access Security Broker: verzorgt veilige toegang tot en data-uitwisseling met clouddiensten.
- DDI Services: beveiligt en beheert netwerktechnologieën als DNS, DHCP en IP-adresmanagement.
- Firewall: beschermt het gemeentenetwerk tegen hackpogingen.
- Micro Segmentation Firewall: deelt het gemeentenetwerk op in meerdere van elkaar afgeschermde zones.
- Web Application Firewall: beschermt webapplicaties tegen hackpogingen.
- Mail filtering: verschoont het e-mailverkeer van spam en phishingmails.
- Advanced Threat Protection (ATP): biedt bescherming tegen geavanceerde hackpogingen en malwareaanvallen.
- Endpoint protection: beschermt endpoints (laptops, servers, smartphones, et cetera) tegen malware.
- Anti-DDoS: beschermt het netwerk en servers tegen DDoS-aanvallen.
- Intrustion Detection & Prevention (IDP): beschermt en detecteert cyberaanvallen waarbij hackers proberen het netwerk binnen te dringen.
- Enterprise Mobility Management (EMM): technologie, processen en regels voor de beveiliging en het beheer van de mobiele devices.
- VPN Management Site: beveiligt VPN-verbindingen voor bijvoorbeeld het faciliteren van veilige thuiswerkplekken.
- DLP-services: diensten en technologieën die de kans op datalekken en datadiefstal verkleinen.
- Vulnerabilitymanagementservices: detecteert en verhelpt (waar mogelijk) kwetsbaarheden in de IT-infrastructuur.

Aanpak en werkwijze
Na gunning bestaat het vervolgtraject uit drie fasen:

1. Intake
Onze securityconsultants brengen uw huidige infrastructuur in kaart om uw security risico's te bepalen. Aan de hand hiervan adviseren onze consultants over uw security prioriteiten. Hierna volgt een impactanalyse. Deze analyse brengt de gevolgen van de nieuwe securitymiddelen voor mensen, processen en techniek in kaart. Daarbij adviseren we wat de impact op de organisatie is en wat de randvoorwaarden voor een succesvolle implementatie zijn.

2. Kick-off
In deze fase vertalen we het implementatieplan naar een realistische planning en kijken we naar de benodigde samenstelling en leveringsvorm van oplossingen (via managed dienstverlening, fysieke hardware of via een virtual appliance). Tijdens deze fase bestellen we ook alle benodigde licenties, hardware en support. Ten slotte zorgen wij voor een eventuele opschaling van de organisatorische capaciteit.

3. Implementatie
Voorafgaand aan de implementatie stellen we samen met u een stuurgroep samen. De samenstelling wordt op maat samengesteld en bestaat uit KPN security consultants en relevante gemeentefunctionarissen. Deze stuurgroep is op strategisch niveau verantwoordelijk voor het project. Tijdens de implementatie loopt de stuurgroep zes fases door; initiatie, technisch ontwerp, functioneel ontwerp, voorbereiding migratie, migratie en als laatste nazorg. De projectmanager bespreekt wekelijks de voortgang met de stuurgroep, bewaakt de planning en borgt dat de impact op uw gemeente zo klein mogelijk blijft.

Perceel 3:
SECURITY-CONSULTANCY

Cybersecurity is een complex vakgebied. Van security-monitoring en pentesting tot het voldoen aan wet- en regelgeving, elk onderdeel vereist specifieke expertise. Het werven en behouden van security-experts is dan ook voor veel gemeenten een zorg. En dat terwijl de beveiliging van uw netwerk en data één van de belangrijkste randvoorwaarden is voor het succes van uw digitale dienstverlening.

Security oplossingen in lijn met uw digitale agenda
De digitale ambities van gemeenten verschillen, afhankelijk van het zwaartepunt van de dienstverlening. Daarmee kunnen security prioriteiten ook verschillen, nu en in de toekomst. Voor uw gemeente is het belangrijk om te weten welke security oplossingen nu prioriteit hebben om snel te voldoen aan de BIO, - maar ook welke nieuwe security eisen er ontstaan op basis van uw toekomstige ambities.
Perceel 3 biedt u de mogelijkheid securityspecialisten in te huren die u helpen om binnen perceel 1 en 2 de juiste prioriteiten te stellen, zodat u niet alleen op korte termijn maar ook in de toekomst voldoet aan de BIO. Zo kunt u zonder zorgen, veilig uw dienstverlening innoveren.

Wat biedt KPN Security?
KPN Security zorgt ervoor dat er altijd voldoende kennis en kunde beschikbaar is voor VNG en deelnemende gemeenten. Zo maken we jaarlijks een bezettingsplan op basis van de huidige trends en de verwachte marktvraag. Daarbij toetsen we vier keer per jaar of deze capaciteit nog voldoet aan de vraag zodat we op tijd extra consultants kunnen werven indien nodig. Hierdoor bent u ervan verzekerd dat wij altijd over voldoende expertise en capaciteit beschikken.

Aanpak en werkwijze
1. Efficiënt en snel matchingproces
KPN Security verwerkt aanvragen volgens een bewezen matchingproces. Hiermee kunnen we snel bepalen welke expertise en ervaring u nodig heeft en welke security consultant past bij uw gemeente. U mag verwachten dat wij binnen een week de benodigde expertise voor u kunnen opschakelen.

2. Waarborgen kwaliteit en continuïteit
Na het matchingproces maakt de deliverymanager van KPN Security met uw gemeente en de security consultant afspraken over de werkwijze en de beoogde resultaten. Continuïteit is daarbij een belangrijk uitgangspunt. In deze gesprekken gaan we na of de professional naar tevredenheid functioneert en of uw doelstellingen binnen de planning gehaald kunnen worden.

3. Continu verbeteren dienstverlening – uw mening telt.
KPN Security is altijd op zoek naar nieuwe manieren om onze dienstverlening te verbeteren. Zo nemen onze experts deel aan nationale en internationale security congressen zoals Black Hat en DEFCON en stimuleren we het delen van kennis. Daarnaast realiseren we ons dat uw mening leidend is, daarom zullen we u met enige regelmaat vragen om onze dienstverlening te beoordelen. Op basis van alle interne en externe feedback krijgen we inzicht in de benodigde verbeterpunten.

Waarom KPN?
1. Complete en ervaren securityleverancier
KPN Security is een van de meest complete en ervaren security leveranciers van Nederland. Ons portfolio biedt dan ook gecertificeerde oplossingen voor al uw security behoeftes – zowel binnen de maatstaven van de BIO als daarbuiten. Zo bent u met KPN Security verzekerd van een efficiënt en centraal aanspreekpunt voor al uw securitydiensten.

2. Focus op mensen, processen en techniek
Voor KPN Security gaat veiligheid en risicomanagement verder dan technologie. Wij hanteren een alomvattende benadering op basis van drie domeinen: mensen, processen en techniek.
Daarbij kijken we goed naar overeenkomsten en verschillen tussen gemeenten. Gemeenten hebben in eerste instantie een vergelijkbare security behoefte, maar deze verschilt toch afzonderlijk op basis van het zwaartepunt van de dienstverlening en de digitale ambities van een gemeente. We hechten daarbij veel waarde aan een goed samenwerkingsverband op basis van verdiend vertrouwen.

3. Flexibele managed security services
De ontwikkeling van digitale netwerken vraagt om flexibele en schaalbare security oplossingen die uw applicaties en data beschermen ongeacht waar deze zich bevinden, - in uw eigen netwerk of in de cloud. Afhankelijk van uw specifieke security behoefte stellen we een pakket aan producten en diensten samen die u uiteraard als managed service bij ons kunt afnemen; u heeft dan geen omkijken meer naar de beveiliging van uw dienst-verlening. Die verantwoordelijkheid draagt KPN Security voor u.

4. Altijd verzekerd van de meest geavanceerde beveiliging
Cybercriminaliteit is altijd in ontwikkeling. Daarom werken wij vanuit ons eigen innovatielab dagelijks aan nieuwe oplossingen en gaan onze specialisten regelmatig op training. Daarbij zorgen we dat uw data in veilige handen is en blijft conform Nederlandse wet- en regelgeving

Meer informatie
Meer weten over onze producten en diensten rondom GGI-Veilig?
Neem contact op met **kpnsecurity@kpn.com**

KPN Security