VNG Realisatie

INFORMATIE BEVEILIGINGS DIENST

Monitoring & Response

Visie

Gemeenten hebben in algemene zin onvoldoende adequate voorzieningen voor netwerkmonitoring. Dat past in het beeld dat gemeenten stappen zetten op het vlak van informatiebeveiliging, maar dat er meer nodig is. De basis is kortgezegd niet op orde. Hacks, malware, ongeautoriseerde toegang en overige digitale narigheid worden niet of te laat opgemerkt. Met grote schade tot gevolg.

Wat is het knelpunt?

Het blijkt dat gemeenten inmiddels – mits de wil van management en het bestuur er is - zelf goed in staat zijn om dergelijke laagdrempelige diensten in te kopen of te implementeren. Dat blijkt wel uit hoe snel een gehackte organisatie dat inricht.

Het kan zijn dat er situaties zijn waarbij er wel de wil van management en bestuur is om monitoring in te kopen, maar dat er een gebrek is aan inkoopcapaciteit. Die signalen hebben we bij de IBD niet. Wel hebben we signalen dat management en bestuur – gegeven de knellende financiële situatie – keuzes moeten maken en dan onvoldoende overtuigd zijn van de noodzaak van monitoring. Dat wil zeggen; totdat ze zelf getroffen worden door een incident.

Gemeenten hebben behoefte aan laagdrempelige, onderhoudsarme voorzieningen tegen lage kosten.

Deze voorzieningen blijken in de afgelopen paar jaar op de markt te zijn gekomen, mede naar aanleiding van incidenten als de hack bij Hof van Twente. Dit staat in contrast met de situatie van 3 tot 4 jaar geleden waarbij dergelijke diensten complex om in te zetten waren, er was toen gespecialiseerd personeel nodig om de meldingen te kunnen duiden en opvolging te kunnen organiseren.

Randvoorwaarden:

Snelheid

Snelheid is van het grootste belang. Gemeenten hebben de afgelopen jaren niet de verwachte en noodzakelijke vlucht naar voren gemaakt m.b.t. monitoring & response. Dreigingen zijn de afgelopen jaren ernstiger geworden en incidenten kunnen enorme impact op gemeenten hebben. In de afgelopen twee jaar ondersteunde de IBD bij een aantal grote incidenten met een schade van enkele tonnen tot enkele miljoenen.

De IBD ziet bij elk van deze voorbeelden dat deze hadden kunnen worden opgemerkt en gestopt met standaard detectieregels uit iedere willekeurige oplossing. Detectie voorkomt per direct schade en impact. Daarom liever een snelle standaard oplossing dan een lang implementatie/aanbestedingstraject op maat. Start liever nog vandaag dan morgen.

Eenvoud

Start zo eenvoudig mogelijk. Veel leveranciers/dienstverleners hebben inmiddels een standaard oplossing/dienstverlening die ook voor gemeenten prima voldoet als basis. De IBD ziet in de praktijk dat een dergelijke oplossing doorgaans met relatief weinig inspanning op korte termijn is te realiseren. Uitbreiden kan altijd later nog. De IBD beschouwt Monitoring & Response inmiddels als een onderdeel van de basis op orde voor informatiebeveiliging.

In het IBD dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2023/ 2024 staat ransomware als grootste dreiging genoemd. Criminelen maken voor de uitrol van ransomware gebruik van bekende technieken en methoden. Die zijn goed te detecteren.

Gemeenten hebben behoefte aan een M&R dienst die actuele indicatoren detecteert. Het is gebruikelijk dat er een ruime hoeveelheid detectieregels standaard beschikbaar is en dat er met regelmaat door leveranciers nieuwe detectieregels worden toegevoegd om nieuwe dreigingen te kunnen detecteren.

Managed Service

Neem M&R af als managed service. Bij voorkeur op basis van de eenvoudige richtlijnen van de IBD. Bij de meeste gemeenten is geen kennis en capaciteit aanwezig om een eigen SOC in te richten, tooling te beheren en de analyses uit te voeren. Op korte termijn is deze kennis ook niet te verwachten. Leveranciers van managed oplossingen hebben de juiste kennis al in huis.

80–20 regel

Deze aanpak zal naar schatting passend zijn voor zo'n 80% van de Nederlandse gemeenten. De IBD richt zich met deze hulpmiddelen voornamelijk op de genoemde 80%. De andere 20% heeft een andere behoefte, of meer kennis en capaciteit in huis. (Bijvoorbeeld de G4). Deze groep kan uiteraard contact opnemen met de IBD voor passend advies en ondersteuning.

Informatie & Downloads

Kijk op **https://www.informatiebeveiligingsdienst.nl** voor meer informatie.