GGI-Veilig/Perceel 3: Forensische dienstverlening

Datum: maart 2021

1. Forensische dienstverlening bij security incidenten

Inzet van forensische expertise heeft tot doel om na een opgetreden security incident, waarvan de oorzaak niet evident is dan wel naar verwachting moeilijk te bepalen is:

1) te achterhalen welke kwetsbaarheid in de ICT-infrastructuur/dienstverlening en/of welk (opzettelijk) menselijk handelen of nalaten daarvan de oorzaak is geweest waardoor het security incident heeft kunnen optreden;
2) te bepalen wat de impact (“schade”) technisch, functioneel en bestuurlijk is (geweest) van het opgetreden security incident en
3) te adviseren welke maatregelen genomen kunnen worden ter opheffing van de achterliggende oorzaak en zo de ICT-infrastructuur en de IV-dienstverlening weerbaarder te maken.

De gewenste reactiesnelheid om het forensisch onderzoek naar de oorzaak te doen plaatsvinden is afhankelijk van de aard en het type van het security incident dat heeft plaatsgevonden. Voor de beeldvorming zijn in de bijlage in het kort een aantal scenario’s uitgeschreven om de verschillende behoeften bij gemeenten te schetsen.

2. GGI-Veilig en forensische dienstverlening

Bij de aanbesteding GGI-Veilig is bij het perceel 3 “Expertise diensten” onder andere het expertise gebied “forensics” aanbesteed. Alle gemeenten kunnen deze dienst binnen de daartoe afgesloten raamovereenkomst afnemen.

3. Verwerven van forensische dienstverlening

Een gemeente kan, via het Servicecentrum Gemeenten, de forensische dienstverlening via een minicompetitie op twee manieren verwerven: als enkelvoudige opdracht of als abonnement.
De leveringsvorm “enkelvoudige opdracht” is niet geschikt als een gemeente in spoedeisende situaties direct wil kunnen handelen. Dit omdat ingeval van een enkelvoudige opdracht het enkele dagen (bij spoedaanvraag) tot enkele weken kan duren voordat de expertise beschikbaar en inzetbaar is. Daarom wordt vanuit VNG Realisatie sterk aanbevolen om deze dienst op korte termijn als abonnement af te nemen, voor alle in de bijlage beschreven scenario’s. Bij een spoedeisende situatie is het immers van belang om direct handelend te kunnen optreden; eerst vrijwel direct met mitigerende maatregelen en spoedig daarna met forensisch onderzoek. Bij de abonnementsvorm kan een gemeente altijd direct contact hebben en korte reactie/inzet-tijden voor de start van forensisch onderzoek overeenkomen, bijvoorbeeld binnen 24 uur of binnen 8 uur. De voordelen zijn: 1 aanspreekpunt, snelle response, gekende kosten en gegarandeerde capaciteit.

Meer informatie hierover is te verkrijgen bij Servicecentrum Gemeenten via één van de implementatieadviseurs GGI-Veilig. U kunt daartoe een mail sturen naar ggi@vng.nl of bellen naar Servicecentrum Gemeenten (070-250 14 14).

Bijlage: GGI-Veilig/Perceel 3: varianten forensisch onderzoek

In deze bijlage is een aantal korte beschrijvingen opgenomen van de verschillende varianten op forensisch onderzoek met onderaan in de tabel de bij een scenario behorende gewenste reactiesnelheid.

Scenario 1: Hackers actief op interne netwerk - SPOED
Bij de gemeente zijn diverse aanwijzingen dat er hackers actief zijn (geweest) op het interne netwerk. Er zijn meerdere systemen versleuteld middels gijzelsoftware, er zijn onverklaarbare administrator accounts, systeembeheer kan de servers niet meer benaderen. De gemeente heeft een crisisteam samengesteld of is hier mee bezig.

Het is noodzakelijk dat meerdere ICT Security specialisten met diverse disciplines zo spoedig mogelijk op locatie van de gemeente komen om de situatie te managen en te analyseren.
Deze specialisten dienen zowel tijdens, maar ook buiten kantooruren beschikbaar te zijn binnen een kort tijdbestek. 24/7 binnen enkele uren op locatie en telefonisch direct eerste stappen die een gemeente al kan treffen voor de komst van de specialisten.

In het incident response team dienen ook ervaren medewerkers te zitten die eerder grotere beveiligingsincidenten hebben gemanaged, bij voorkeur ook in het gemeentelijk domein.
Veel gemeenten hebben geen ervaring met een groter cyberincident. De specialisten dienen niet alleen onderzoekers of techneuten te zijn, maar moeten het beveiligingsincident ook kunnen managen, communiceren met de afdeling communicatie en deel kunnen nemen aan het crisisteam van de gemeente. In sommige situaties dient de leiding genomen te worden over het onderzoek vanuit expertise en ervaring.

Scenario 2: Malware op server (DMZ)
Bij de gemeente is een enkele server (DMZ) besmet geraakt met malware of er zijn sporen van een hacker aanwezig. De gemeente heeft de server geïsoleerd, maar is zelf niet in staat om uit te zoeken in hoeverre een hacker verder toegang heeft gehad tot andere systemen van de gemeente. Ook is niet duidelijk welke data er mogelijk door hacker zijn ingezien of buit gemaakt. De gemeente heeft geen crisisteam; de CISO en de afdeling ICT handelen zelf het incident af.

Het is noodzakelijk dat enkele ICT Security specialisten naar de locatie van de gemeente komen om de situatie te onderzoeken en te analyseren. Deze specialisten dienen voornamelijk overdag tijdens kantooruren beschikbaar te zijn, maar in enkele gevallen is het ook wenselijk dat onderzoek al in het weekend plaatsvindt. De specialisten zijn vooral technisch en goed in digitaal onderzoek. Wenselijk dat de volgende dag onderzoek gedaan kan worden.

Scenario 3: Gecompromitteerd account
Deels gelijk aan scenario 2. Bij de gemeente is een account gecompromitteerd. De gemeente heeft het account geïsoleerd, maar is zelf niet in staat om uit te zoeken in hoeverre een hacker verder toegang heeft gehad tot andere accounts of systemen van de gemeente.
Ook is niet duidelijk welke data er mogelijk door de hacker zijn ingezien of buit gemaakt. De gemeente heeft geen crisisteam; de CISO en de afdeling ICT handelen zelf het incident af.

Afhankelijk van de situatie dienen enkele ICT Security specialisten naar de locatie van de gemeente te komen of in een Cloud omgeving de situatie te onderzoeken en te analyseren. Deze specialisten dienen voornamelijk overdag tijdens kantooruren beschikbaar te zijn, maar in enkele gevallen is het ook wenselijk dat onderzoek al in het weekend plaatsvindt. De specialisten zijn vooral technisch en goed in digitaal onderzoek. Wenselijk dat de volgende dag onderzoek gedaan kan worden.

Scenario 4: Onderzoek naar medewerker
Er dient digitaal forensisch onderzoek gedaan te worden naar een medewerker. Het onderzoek is goedgekeurd door bevoegd gezag. De gemeente heeft geen crisisteam; leidinggevende, de CISO en de afdeling ICT handelen zelf het onderzoek af.

Afhankelijk van de situatie dienen enkele ICT Security specialisten naar de locatie van de gemeente te komen of in een Cloud omgeving de situatie te onderzoeken en te analyseren. Deze specialisten dienen overdag tijdens kantooruren beschikbaar te zijn. De specialisten zijn technisch en goed in digitaal onderzoek, maar ook goed bekend met wetgeving. Het onderzoek dient door een organisatie uitgevoerd te worden met de juiste certificering en vergunning. De onderzoeken hebben geen spoed.

Totaaloverzicht

	Scenario 1	Scenario 2	Scenario 3	Scenario 4
Soort Forensisch Onderzoek	Incident Response	Compromis onderzoek	Forensisch onderzoek	Fraudeonderzoek Integriteitsonderzoek
Skills	Incidentmanagement Grote hacks Gemeentelijke organisatie Crisismanagement Ervaren techneuten	Ervaren techneuten Goed in digitaal onderzoek	Goed in digitaal onderzoek Optioneel: Cloud	Kennis wetgeving Goed in digitaal onderzoek
Aanbevolen Responsetijd	Zelfde dag 24/7 *(= binnen 8 uur)*	Volgende dag *(= binnen 24 uur)*	*Volgende dag (=binnen 2/3 werkdagen)*	Week
Certificaat	Optioneel	Optioneel	Optioneel	Ja