INFORMATIE
BEVEILIGINGS
DIENST

DIGITAAL FORENSISCH ONDERZOEK

Een van de producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN**
VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document
Digitaal Forensisch Onderzoek (DFO)

Versienummer
1.0

Versiedatum
December 2017

Versiebeheer
Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Met dank aan
De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Versie	Datum	Opmerkingen
1.0	13-12-2017	Eerste versie

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE BEVEILIGINGS DIENST

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN** VERENIGING VAN NEDERLANDSE GEMEENTEN

Leeswijzer

Dit product maakt onderdeel uit van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Doel
Dit product bevat een handreiking en beleid rondom Digitaal Forensisch Onderzoek.

Doelgroep
Dit document is van belang voor het management van de gemeente, de systeemeigenaren, applicatiebeheerders en de ICT-afdeling.

Relatie met overige producten

- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
  - Strategische variant van de Baseline Informatiebeveiliging voor Gemeenten
  - Tactische variant van de Baseline Informatiebeveiliging voor Gemeenten
- Informatiebeveiligingsbeleid van de gemeente

Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

Maatregel 13.2.1.1: procedures voor rapportage
Maatregel 13.2.2.1: beoordelen van beveiligingsmeldingen
Maatregel 13.2.3.1: vervolgprocedure beveiligingsincident

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Inhoudsopgave

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

1 Inleiding

Digitaal forensisch onderzoek, ofwel digitaal sporenonderzoek, is het verzamelen en analyseren van gegevens uit digitale systemen (hard- en software). Het gaat hierbij o.a. over gegevens ten aanzien van toegang en gebruik.

Na een informatiebeveiligingsincident is het om meerdere redenen belangrijk om vast te stellen wat er precies is gebeurd en wat de aanleiding is geweest. Indien een incident te maken heeft met persoonsgegevens, is onderzoek zelfs wettelijk verplicht in het kader van de meldplicht datalekken.

Belangrijke vragen bij een incident zijn:

- Hoe kon dit gebeuren?
- Hoe lang is dit aan de hand geweest?
- Om welke systemen en welke gegevens gaat het?

Digitaal forensisch onderzoek helpt bij het vinden van antwoorden op deze vragen en is ook een belangrijke voorwaarde voor het doen van aangifte en input voor een goede crisiscommunicatie.

De indeling van dit document is als volgt:
Hoofdstuk 2: Wat is digitaal forensisch onderzoek
Hoofdstuk 3: Het forensisch onderzoeksproces voor gemeenten
Hoofdstuk 4: Wanneer specialistische hulp inschakelen
Hoofdstuk 5: Het documenteren
Hoofdstuk 6: bijlages en checklist

1.1 Doel van dit document

Het doel van dit document is om een inzicht te geven wat een Digitaal Forensisch Onderzoek inhoudt met de bijkomende procedures en beleid. Het geeft een overzicht van mogelijke aanleidingen om een forensisch onderzoek te starten en wat er dan al zou moeten gebeuren in de eerste momenten nadat er een forensisch onderzoek is gestart. Ook geeft dit document een overzicht wat er moet gebeuren om tijdens een forensisch onderzoek op een ordentelijke manier bewijs te verzamelen zodat dit later tijdens een eventuele rechtszaak gebruikt kan worden.

Digitaal forensisch onderzoek kan gaan over een aantal onderwerpen, bijvoorbeeld:

1. Incident response
2. Digitale recherche
3. Malware analyse
4. Integriteitsonderzoek
5. Onderzoek in het kader van de openbaarheid van bestuur.

Met behulp van forensische software kunnen eventuele documenten automatisch doorzocht worden en eventueel automatisch worden geanonimiseerd.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

1.2 Raakvlakken

- Incident management en response beleid
- ISMS[1]
- Procedure mobiele gegevensdragers[2]
- Back-up en restore standaard
- Logging beleid
- Hardening beleid[3]
- Datalekkenbeleid[4]

1.3 Aanwijzing voor gebruik

Deze handreiking is qua opzet geschreven om informatiebeveiligingsmaatregelen met betrekking tot forensisch onderzoek uit te werken en daarbij handreikingen te geven voor eigen procedures. Deze handreiking is geen volledige procesbeschrijving.

De BIG raakt forensisch onderzoek in paragraaf 13.2 het volgende over forensisch onderzoek.

De volgende beveiligingsmaatregelen komen hier aan bod:

13.2.1.1 Er zijn procedures voor rapportage van gebeurtenissen en escalatie. Alle medewerkers behoren op de hoogte te zijn van deze procedures.

13.2.2.1 De informatie verkregen uit het beoordelen van beveiligingsmeldingen wordt geëvalueerd met als doel beheersmaatregelen te verbeteren (PDCA Cyclus).

13.2.3.1 Voor een vervolgprocedure naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

[1] Zie de handreiking ISMS van de IBD: https://www.ibdgemeenten.nl/downloads/?id=2286
[2] Zie de handreiking Mobiele Gegevensdragers van de IBD: https://www.ibdgemeenten.nl/downloads/?id=366
[3] Zie de handreiking hardening-beleid voor gemeenten https://www.ibdgemeenten.nl/downloads/?id=460
[4] Zie leaflet Meldplicht datalekken https://www.ibdgemeenten.nl/downloads/?id=3390

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Rol IBD

Tijdens een forensisch onderzoek kunnen na een incident, aanval of hack zogenaamde IoC's (Indicator of Compromise)[5] ontdekt worden. Een IoC is informatie die kan helpen bij het identificeren van malafide gedrag op een systeem of binnen een netwerk welke een bedreiging kan vormen voor de informatieveiligheid. Naast dat deze informatie belangrijk is voor het interne onderzoek kan het ook andere gemeenten helpen dezelfde dreiging af te weren en te voorkomen. Het delen van deze threat intelligence (TI)[6] is daarom erg belangrijk. Let op, niet alle informatie kan gedeeld worden i.v.m. privacyaspecten. Ga hier zorgvuldig mee om.

De IBD is het centrale schakelpunt voor gemeenten m.b.t. TI. Samen met het NCSC en andere CERT's verzamelen we actuele dreigingsinformatie die voor gemeenten relevant is. Als er tijdens forensisch onderzoek dergelijke informatie bekend raakt, heeft het de voorkeur dit te delen met de IBD voor de veiligheid van andere gemeenten.

[5] Zie de factsheet Indicators of Compromise van het NCSC: https://www.ncsc.nl/actueel/factsheets/factsheet-indicators-of-compromise.html
[6] Zie de factsheet Threat Intelligence van de IBD: https://www.ibdgemeenten.nl/downloads/?id=4622

2 Digitaal Forensisch onderzoek

2.1 Introductie

Het doen van (forensisch) incidenten onderzoek is specialistisch werk. Gemeenten zijn vaak niet toegerust om dit type onderzoek te doen. Het kan daarom verstandig zijn om bijvoorbeeld voordat sprake is van een incident contact en/of afspraken te maken met een specialistisch bedrijf het geval dat deze kennis nodig is. Op de IBD-Community kunnen gemeenten kennis en ervaringen uitwisselen over forensische onderzoeksbedrijven.

Bij veel dingen die we doen, laten we sporen na en dit kunnen ook digitale sporen zijn. Van het versturen van een e-mail, het bezoeken van een website, het binnengaan van een kantoor met een pasje tot het printen van een document, zijn voorbeelden van activiteiten waarbij digitale sporen ontstaan.

Het kan voorkomen dat na een incident[7] deze sporen onderzocht moeten worden. Bij zo'n onderzoek speelt subsidiariteit en proportionaliteit een rol. Subsidiariteit betekent dat bij keuze uit verschillende onderzoeksmiddelen het lichtste middel gekozen moet worden, bijvoorbeeld: eerst onderzoeken met wie iemand e-mailt en als dat geen eenduidig beeld oproept dan pas de inhoud van de e-mails bekijken. En proportionaliteit geeft aan dat het gebruikte middel in relatie moet staat tot het doel. Immers, een onderzoek kan behoorlijk inbreuk maken op iemands zijn of haar persoonlijke levenssfeer zijn. Zo'n onderzoek kan zelfs leiden tot een ontslag en strafrechtelijke vervolging.

Een werkgever mag niet zomaar de (privé) e-mails of internetverkeer van een werknemer afluisteren. Een werknemer mag ervan uit gaan dat hij, ook op zijn werk, een privésfeer heeft[8]. Daarom mag er niet zomaar alle digitale sporen onderzocht worden, bijvoorbeeld privé e-mails mogen niet betrokken worden bij een onderzoek, behalve als er sprake is van een strafbaar feit. Zo'n onderzoek wordt dan uitgevoerd door het Openbaar Ministerie.

2.2 Wat is digitaal bewijsmateriaal

In tegenstelling tot tastbare zaken zijn digitale gegevens vluchtig en kwetsbaar. Ze kunnen eenvoudig worden beschadigd, vernietigd en gemanipuleerd. Digitale gegevens hebben nog een eigenschap, ze kunnen ook makkelijk worden gekopieerd. Digitale gegevens worden verkregen met een digitaal forensisch onderzoek van een apparaat dat op de een of andere manier betrokken is bij een digitaal incident, maar niet elk onderzoek is een forensisch onderzoek. Het is pas een forensisch onderzoek op het moment dat er een vermoeden bestaat van een incident. Dat digitaal forensisch onderzoek gebeurt op basis van een hypothese van een incident om vast te stellen of die hypothese klopt. Digitaal bewijsmateriaal is een digitaal object met betrouwbare informatie die een zaak kan ondersteunen, verkregen door digitaal forensisch onderzoek.

[7] Zie ook incidentmanagement en response beleid: https://www.ibdgemeenten.nl/downloads/?id=3412
[8] Zie uitspraak rechter met referenties naar wetsartikelen: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2014:2751

2.3 Soorten onderzoek

Er zijn verschillende soorten digitaal forensisch onderzoek en het is noodzakelijk om te verschillen en overeenkomsten hiervan de begrijpen.

Persoonsgericht integriteitsonderzoek - Vinden plaats na overtreding van integriteitsregels, gemeentelijk beleid en andere gemeentelijke regels.

Denk bijvoorbeeld aan integriteitsonderzoeken, onderzoeken of gegevens rechtmatig zijn ingezien, maar ook het onderzoeken van een digitaal incident.

Binnengemeentelijke digitaal forensisch onderzoek kan leiden tot de tweede vorm van digitaal forensisch onderzoek te weten:

Strafrechtelijke onderzoeken – deze vindt plaats na overtreding van de wordt en uitgevoerd door de Politie.

Het feit dat deze onderzoeken elkaar kunnen opvolgen betekent dat het volgen van bepaalde regels vanaf het allereerste begin noodzakelijk is. Als verantwoordelijke voor het afhandelen van het incident zou je taak dan kunnen bestaan uit het zeker stellen van digitaal bewijsmateriaal (voorkomen dat het wordt vernietigd of gewijzigd)

Er zijn ook andere vormen van onderzoek naast de organisatie of strafrechtelijke onderzoeken, namelijk:

Malware onderzoek

Met malware onderzoek[9] wordt hier bedoeld dat het gedrag van malware wordt onderzocht na een incident. Malware onderzoek kan interessant zijn in het geval er schade is ontstaan door mogelijk incorrect handelen van personen. Malware onderzoek vergt redelijk specialistische kennis en gereedschappen, zoals een onderzoek omgeving en tooling om veilig malware te kunnen onderzoeken. Gemeenten zijn hier minder voor ingericht. Het is ook mogelijk om malware te verzenden naar speciale onderzoekssites[10]. Als de malware al eens onderzocht is, dan volgt doorgaans een antwoord met de bijzonderheden van deze malware.

Als zo'n onderzoekssite de malware nog niet kent, is het gewenst om toch het gedrag van malware te laten onderzoeken om zekerheid te geven over wat er wel of niet is gebeurd (bijvoorbeeld het verzenden van bestanden met persoonsgegevens). Als de gemeente daarover zekerheid wil hebben dan is het verstandig om een gespecialiseerd bedrijf in de arm te nemen of advies in te winnen bij de IBD. Let wel op dat voor zo'n onderzoek een SMART onderzoeksvraag gesteld wordt, en dat tevens een budget plafond aangegeven wordt (= scope). Zonder budgetplafond kan malware onderzoek prijzig worden.

[9] Zie ook https://www.sans.org/reading-room/whitepapers/malicious/malware-analysis-introduction-2103
[10] Bijvoorbeeld: https://www.virustotal.com/nl/

Incident onderzoek

Incident onderzoek is typisch iets wat zou kunnen gebeuren binnen een gemeente. Er treden nou eenmaal incidenten op, en om deze incidenten te onderzoeken is een vorm van digitaal (forensisch) onderzoek nodig. Want elk incident zou potentieel onderzoek kunnen worden en als er sprake is van onderzoek moet dat via een systematische en objectieve methode gebeuren. Denk hierbij aan het onderzoeken van bijvoorbeeld systemen, diverse soorten logbestanden en overige bestanden en computergeheugens. Dit onderzoek richt zich op het opsporen van besmettingshaarden en de gevolgen van de aanval, om herstel mogelijk te maken. Bij dit incident onderzoek is men tevens bezig met het verzamelen van digitaal forensisch bewijsmateriaal dat later gebruikt zou kunnen worden bij een aangifte. Dit maakt dat het correct documenteren van een onderzoek na een incident goed vereist is.

Een incident response-actie[11] bestaat uit de volgende stappen:

- Identificatie (hebben we een incident);
- Schade indamming (insluiting en beperking);
- Remediatie en herstel;
- Kennisgeving;
- Rapportage en evaluatie;

Digitale recherche

Betreft het onderzoek het digitaal onderzoeken van bijvoorbeeld een apparaat, een harddisk, een telefoon, dan heeft dit al gauw iets weg van digitaal rechercheren in het kader van een mogelijk strafrechtelijk onderzoek. Het is dan verstandig om specialistische hulp te vragen van een expert. Er zijn een aantal soorten specialistisch onderzoek die ook van pas kunnen komen bij malware onderzoek en incident onderzoek.

- Digitaal Forensisch Onderzoek met speciale tooling. Het gaat hier over het hebben van tooling kennis, welke tooling waarvoor gebruikt kan worden en hoe deze tooling inzet kan worden. Denk aan tools zoals SIFT[12] om snel door grote hoeveelheden bestanden te zoeken, DEFT[13] is een Linux distributie speciaal voor forensisch onderzoek, FTK[14] en ADIA[15] als forensische toolkits.
- Forensisch onderzoek van harddisks. Dit vereist diepgaande kennis van alle mogelijke soorten opslagmedia, bestandssystemen en structuren, tooling en mogelijkheden en onmogelijkheden. Denk hier bijvoorbeeld ook aan het terughalen van bestanden en diskpartities.
- Forensisch onderzoek van besturingssystemen, bijvoorbeeld Windows of Linux Dit vereist diepgaande kennis van deze besturingssystemen, de benodigde tooling, de logging, het netwerk en hoe bijvoorbeeld met wachtwoorden wordt omgegaan. Het is doorgaans iets waar je specialistische kennis van het betreffende besturingssysteem voor nodig hebt.
- Netwerk forensisch onderzoeken. Met deze onderzoeken wordt hier bedoeld het opvangen, opnemen en analyseren van netwerkverkeer. Dat kan ongericht (sleepnet) en gericht (bijvoorbeeld sniffen van specifiek netwerkverkeer of een specifiek IP-adres). Hiervoor moet er ook goede kennis zijn van tooling en technieken, het OSI model, netwerk protocollen en

[11] Zie ook https://www.ibdgemeenten.nl/downloads/?id=3412
[12] https://sift-tool.org/
[13] http://www.deftlinux.net/
[14] http://accessdata.com/products-services/forensic-toolkit-ftk
[15] http://www.cert.org/digital-intelligence/tools/

poorten en soorten aanvallen. Onder netwerk monitoring zou je ook netwerk security monitoring kunnen vatten, dan neigt het naar Intrusion Detection Systemen (IDS) en diverse soorten firewalls, zoals Next Generation Firewall (NGF). Binnen netwerken worden ook logbestanden geproduceerd en ook die logbestanden bevatten forensische aanwijzingen, deze kunnen ook weer gebruikt worden voor security information and event management (SIEM).

- Mobiele apparaten onderzoeken. Huidige mobiele apparaten hebben bijna net zoveel mogelijkheden als personal computers en zijn een bron van vele soorten bestanden waaronder logbestanden. Dit vereist kennis van mobiele apparaten, netwerktechnologie, besturingssystemen, opslagmogelijkheden en tooling. Uitdagingen zijn hier bijvoorbeeld al de verschillende soorten aansluitingen. Met mobiele apparaten is veel mogelijk, ook dat wat een forensisch onderzoeker liever niet wil (om er twee te noemen: apparaat encryptie, wissen op afstand). Dit vereist extra maatregelen om te borgen dat het onderzoek goed kan worden uitgevoerd, zoals beschreven in het NIST document 'Guidelines on Mobile Device Forensics[16]'
- Applicatie onderzoek. Applicatie onderzoek kan gaan over webapplicaties, gewone applicaties, email en verschillende vormen van onderzoeken zoals penetratietesten.

[16] Zie hiervoor: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

3 Het digitaal forensisch proces voor gemeenten

3.1 Beleidsuitgangspunten omtrent digitaal forensisch onderzoek

Binnen een gemeente is het van belang beleid te hebben omtrent Digitaal Forensisch Onderzoek. Het doel van dit beleid is duidelijke regels neer te leggen die in relatie staan tot Digitaal Forensisch Onderzoek. Dit beleid zou moeten beschrijven wanneer er een forensisch onderzoek gestart gaat worden en door wie deze zal worden uitgevoerd. Ook mogelijke afspraken met externe gespecialiseerde bedrijven kunnen hierin opgenomen worden.

Het starten van een forensisch onderzoek is altijd afhankelijk van de classificatie van een incident. Een forensisch onderzoek kan bijvoorbeeld gestart worden naar aanleiding van een integriteitsonderzoek of naar aanleiding van een incident.

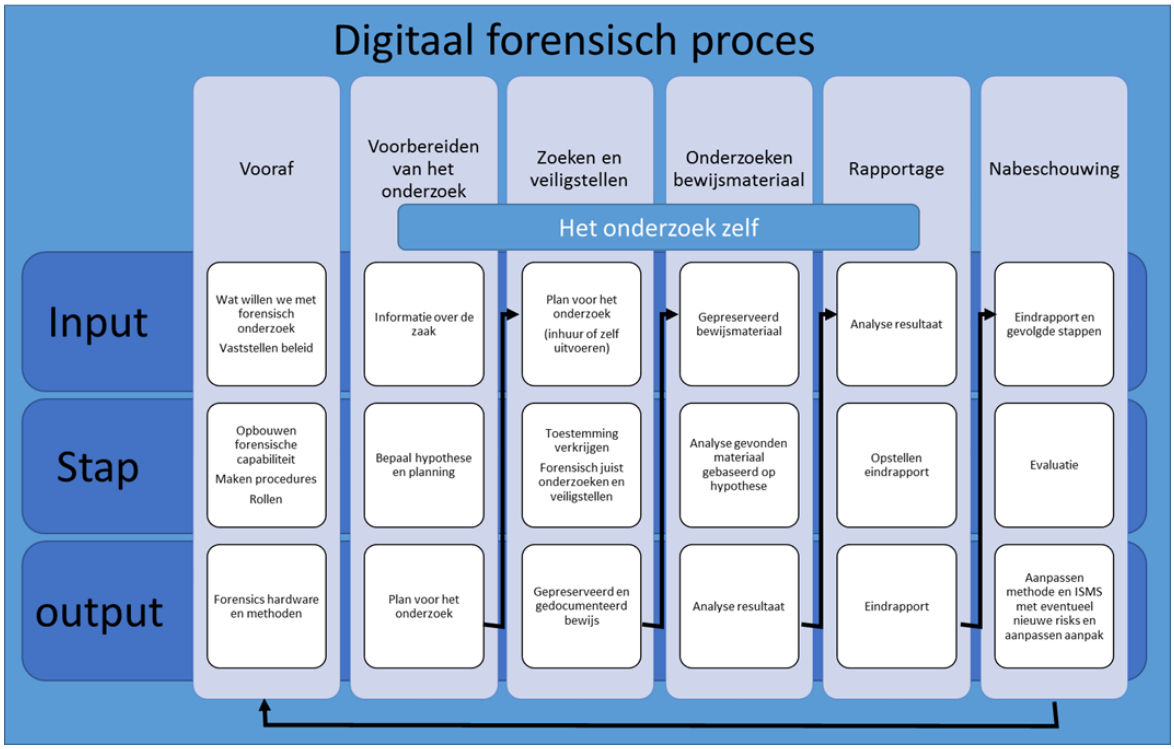
Omdat het uitvoeren van een Digitaal Forensisch Onderzoek (DFO) specialistisch werk is, is het aan te raden die delen die buiten de kennis en kunde van de gemeente liggen uit te laten voeren door specialistisch bedrijf.

Na het opstellen en vaststellen van het gemeentelijk digitaal forensisch beleid moet er ook worden nagedacht over rollen en werkprocessen en procedures. Procedures kunnen conform het hieronder genoemde model uitgewerkt worden. Er moet ook aan procedures gedacht worden voor het melden van en omgaan met incidenten, het verlenen van toegang tot ruimtes en informatiesystemen en hoe om te gaan met bewijsmateriaal.

3.2 Digitaal forensisch onderzoeken is een proces

Voor het doen van digitaal forensisch onderzoek of een onderzoekt van een incident, het volgen van een stappenplan is belangrijk. Het volgen van een proces en de kennis van de onderzoeker bepalen in hoge mate het resultaat en succes van het onderzoek. Het stappenplan heeft ook in zich dat het een checklist is, zodat men geen stappen vergeet of verkeerd uitvoert. De output van het onderzoek kan weer gebruikt worden om het proces te verbeteren, en risico logboek aan te vullen, het ISMS te verbeteren, et cetera et cetera.

Het volgende model zou er gebruikt kunnen gebruiken als voorbeeld van digitaal forensisch proces:



Naast het hebben van beleid en procedures is het ook verstandig om minimaal 1 keer per jaar de procedures te oefenen en waar nodig bij te stellen en te actualiseren. Denk daarbij aan:

- Zijn de contactpersonen nog hetzelfde?
- Zijn er personele dan wel rol wijzigingen?
- Zijn de telefoonnummers nog hetzelfde?
- Zijn er (ICT) ontwikkelingen geweest die een verandering van de processen noodzakelijk maken?

Er zijn vaak een aantal partijen betrokken bij een digitaal forensisch onderzoek. Het is van belang om van tevoren te beschrijven wat de rollen van de verschillende functionarissen zijn.

Een opzet qua rolverdeling ziet er als volgt uit:

- Het managementteam/ senior management is verantwoordelijk voor het onderzoek. Deze wijst 1 persoon aan als incident manager en bepaald de prioriteit van het onderzoek.
- HR draagt zorg voor de communicatie naar de werknemer(s) die wordt/worden onderzocht en interne communicatie.
- Fysieke beveiliging zet het gebied af waar het onderzoek wordt verricht.
- De juridische afdeling ondersteund de incident manager over de mogelijkheden en onmogelijkheden tijdens en na het onderzoek.
- Er wordt een auditor aangewezen die monitort en documenteert hoe er met het fysieke en digitale bewijs wordt omgegaan.
- De ICT-afdeling ondersteund het onderzoek door het verzamelen van bewijs.
- De persvoorlichter/woordvoerder doet de externe communicatie.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Wat als de politie de digitale data van de gemeente vordert?

Het kan voorkomen dat de politie in het kader van een strafrechtelijk onderzoek digitale data vordert van bij de gemeenten. Op het moment dat dit een legitieme vordering is, is een spoedige en soepele afhandeling verstandig.

Als eerste zal moeten worden onderzocht over welke digitale data de vordering gaat. Er mag alleen die digitale data worden overgedragen aan de politie die genoemd staan in de vordering. Bij het overdragen van andere of meer digitale data kan er onbedoeld data van andere personen worden meegegeven, en dat mag niet.

Ten tweede zal de ICT-afdeling tezamen met de politie moeten kijken waar de gevorderde data zich bevindt: is dat bijvoorbeeld op een netwerkschijf, op een mobiele drager en/of op de harde schrijf op de werkplek van de medewerker? Uiteindelijk is de digitale rechercheur van de politie verantwoordelijk voor het op een correcte manier verkrijgen van de digitale data.

3.3 Voorbereiden van het onderzoek

Bij de voorbereiding van een onderzoek komen er een aantal W-vragen voorbij die beantwoord moeten worden:

1) Wie: Wie is de incidentmanager? Is er al een zaaknummer of naam aan het incident of onderzoekgegeven? Gaan we het zelf onderzoeken of gaan we het laten onderzoeken? Wie is de onderzoeksleider.
2) Wat: Wat is er gebeurd?
3) Wanneer: Moet het onderzoek nu gedaan worden of kan het ook morgen, wat is te prioriteren?
4) Waar: Waar moet er een incident worden onderzocht?
5) Waarom: Is het een open of gesloten onderzoek? Is het een gemeentelijk of strafrechtelijk onderzoek.
6) Hoe: Zijn er al zaken bekend of er bijvoorbeeld specifieke hardware en software betrokken zijn. Hoeveel werk wordt er geschat?

Alle begin is moeilijk en welk type onderzoek er ook gedaan gaat worden, begint het met de juiste dingen doen. Bij digitaal forensisch onderzoek is er vaak geen tweede kans. Denk aan apparaten uitzetten terwijl ze aan hadden moeten blijven en omgekeerd.

De eerste stap altijd dat bewijsmateriaal of situatie op de juiste manier bevroren wordt. Bedenk ook dat het vaak anderen zijn die het eerste bij een incident zijn of het opmerken, bijvoorbeeld systeembeheerders. Systeembeheerders moeten worden getraind om vanaf het begin de juiste dingen te doen en weten wie ze moeten opschakelen voor het onderzoek.

- Stel alle elektronische apparaten veilig, met inbegrip van persoonlijke apparaten.
- Voorkom dat onbevoegden toegang krijgen tot een elektronisch apparaat.
- Weiger alle hulp van onbevoegden.
- Verwijder iedereen uit het gebied waar het bewijs wordt verzameld.
- Zorg dat de status van het elektronisch device behouden blijft. Als het uit is, laat het uit - Als het aan is, laat het aan.
- (Mobiele) devices kunnen ook benaderd worden vanaf afstand. Zo kan een gebruiker gegevens wissen/manipuleren. Door devices te compartimenteren kan dit worden voorkomen.
- Het is van belang een “image” te maken van de digitale data. Een “image” is anders dan een copy van de data, omdat images ge-hashte waarmerken heeft zodat het zeker is dat de data hetzelfde is als het origineel.

- ‘Werkplekonderzoek’ van de betrokken ambtenaar, om zo ook gemeentelijke datadragers en wachtwoorden te achterhalen.

Als het niet direct zichtbaar om strafbare zaken gaat, betreft het meestal in eerste instantie een digitaal incident onderzoek. Zorg voor instemming van senior management binnen de gemeente, bijvoorbeeld de CISO. Bedenk ook dat als een onderzoek gestart wordt naar een persoon of met persoonsgegevens dat hier soms andere regels voor gelden. Zo moet de Ondernemingsraad eerst de kaders vaststellen onder welke omstandigheden er überhaupt afgeluisterd mag worden. Pas nadat de kaders zijn vastgesteld mag er een verzoek worden neergelegd bij de OR tot afluisteren. Er mag niet zomaar in iemands persoonlijke levenssfeer ingebroken worden zonder een hele goede reden. Er kunnen ook specifieke regels omtrent integriteit zijn binnen de gemeente. Dit zou dan ook bekend moeten zijn bij het inrichten van de forensische mogelijkheden, zoals beschreven in de vorige paragraaf.

Er kunnen meerdere personen betrokken zijn bij een incident en het komt voor dat een forensisch onderzoeker maar een klein radertje is in het geheel. Als er bijvoorbeeld nog een aanval gaande is, neem als voorbeeld een ransomware aanval, dan kan het gebeuren dat er gefocust wordt op het behoud van onderzoeksmateriaal terwijl dat juist beschadigd wordt bij het tegengaan van verdere schade.

In deze fase moet tevens begonnen worden met het documenteren van alle acties.

3.4 Zoeken en veiligstellen

In deze fase wordt op basis van het plan gestart met het verzamelen van digitaal sporen materiaal.

In de vorige fase is al grofweg bepaald wat er verzameld moet worden. Het is belangrijk om te beseffen dat niet altijd alles kan en mag (vanwege de wet of beperkingen van bijvoorbeeld logging). Maak aantekeningen, label informatie en maak als dat nodig is overzichtsschetsen en of foto's. Zie voor meer details de checklist in de bijlage van dit document. Zorg voor deugdelijke verpakking en transport als dat nodig is.

3.5 Onderzoeken

Analyse van het materiaal dat in de vorige fase is gevonden moet worden veiliggesteld, verpakt en gelabeld. Het is zaak dat het oorspronkelijk materiaal niet wordt veranderd en de integriteit behouden blijft. Alle activiteiten met bewijsmateriaal moeten worden vastgelegd en het moet achteraf bekend zijn wie wat wanneer gedaan heeft. Bedenk dat als materiaal moet worden geanalyseerd dat dit gebeurt vanaf een kopie en nooit vanaf het origineel. Deze kopie van het materiaal moet aantoonbaar een juiste integere kopie zijn, dus er moeten ook hashes worden gemaakt om dit aan te kunnen tonen. Deze hashes worden ook gebruikt om aan te tonen dat het oorspronkelijk materiaal niet is veranderd.

Het forensisch onderzoek wordt vervolgens uitgevoerd volgens planning en volgens de initiële gedachtegang over wat gebeurd zou kunnen zijn (de hypothese). Hierbij moet dan bedacht worden waar je het bewijs zou kunnen vinden en welke tools uit je gereedschapskist hiervoor nodig zijn. Bedenk ook dat het soms om veel data kan gaan, schakel hierbij hulp in als dat nodig is.

Alle gevolgde stappen en resultaten moeten worden vastgelegd.

3.6 Privacy en privé data

Iedereen heeft recht op privacy. Computers bevatten naast zakelijke data ook vaak persoonlijke data, zoals vakantiefoto's of privé e-mails. Vaak heeft de persoonlijke data geen betrekking op een incident of het onderzoek, deze data mag dan ook niet betrokken worden in het onderzoek ingevolge de Wet bescherming persoonsgegevens/ Algemene verordening gegevensbescherming.

Het is van belang dat er tijdens het onderzoek alleen gericht gezocht wordt naar de relevante data. Maar hoe kan er vastgesteld worden dat het gaat om privacygevoelige data zonder deze eerst te lezen?

Hierbij kan gebruikt worden van het subsidiareitsbeginsel, de zogenaamde privacy piramide.
De piramide omvat de volgende zes niveaus (van hoog naar laag):

1. Inhoud
2. Scan op taal (d.w.z. het invoeren van zoektermen)
3. Scan op plaatjes
4. Onderwerp regels
5. Attachments
6. Volume

Op basis van het subsidiariteitsbeginsel zal de onderzoeker moeten zoeken om een zo laag mogelijk niveau in de piramide te gebruiken om de privacy daarmee zo minimaal mogelijk te schaden. Een forensisch specialist of een jurist kan helpen bij het vaststellen van het correcte niveau van onderzoek.

Normenkade en grenzen aan dataonderzoek:

Bij een concreet vermoeden van een integriteitsschending staat dataonderzoek toe (uitspraak Centrale Raad als basis). Wat zijn de grenzen:

- Wanneer is er sprake van computervredebreuk (138a Sr.), bijvoorbeeld als het gaat om een webbased e-mailaccount, of benadering data opgeslagen in de cloud
- Wanneer is sprake van zaakbeschadiging (wanneer bewust computergegevens gemanipuleerd worden, 350a Sr)
- Wat te doen als een bestand redelijkerwijs aangemerkt kan worden als "privé" (uitspraak Europees Hof: "reasonable expection of privacy")? Bij een vermoeden dat via bijvoorbeeld privé e-mailverkeer digitale data is 'gelekt', dan kan het na een goede overweging in privé geoormerkte data worden bekekenen. Dit dient wel in de verschillende rapportages terug te komen.

3.7 Toepassing van hoor- en wederhoor

Tijdens het onderzoek wordt er informatie verzameld en geanalyseerd. Uit deze analyses kunnen voorlopige conclusies worden getrokken. Het is van belang, dat als het gaat om een organisatiegericht onderzoek, de persoon om wie het gaat de gelegenheid krijgt om op de bevindingen te reageren. Door de verdachte te laten reageren wordt de kans op foutieve conclusies geminimaliseerd.

Bijvoorbeeld in het geval van het toeschrijven van handelingen aan iemand, maar hij/zij ontkent dit, dan kan dit aanleiding zijn om verder onderzoek te gaan verrichten.

3.8 Rapportage

Een forensisch onderzoek of incidentonderzoek moet worden afgesloten met een rapport. Het is verstandig om per onderzoeksitem en iedere onderzoeksstap korte rapportages te maken en die dan later deel gaan uitmaken van een groter eindrapport.

Bedenk bij het schrijven van het rapport voor wie het bestemd is, welk doel het rapport heeft en wat de boodschap moet zijn. Geef feiten chronologisch weer en vermeld ook hoe dingen geconstateerd zijn. Maak een presentatie en presenteer de resultaten.

In de rapportage moet minimaal staan de beantwoording op een aantal W-vragen:

- Wie is er aangetroffen? Wie waren in de ruimte tijdens en na het incident? Wie zijn er bij betrokken?
- Wat: wat is er gebeurd? Wat is er aangetroffen?
- Wanneer gebeurde het incident?
- Waarom gebeurde het?
- Hoe: Zijn er al zaken bekend over of er specifieke hardware en software betrokken is.

3.9 Afronding/ nazorg

Na opleveren van het rapport is het belangrijk om terug te kijken in een evaluatie. Mogelijk kan of mag niet alles openbaar zijn omdat het bijvoorbeeld gaat om privacygevoelige gegevens, maar het is toch zaak om dan oog te hebben voor aandachtspunten om bijvoorbeeld het proces aan te scherpen.

De evaluatie kan de volgende uitkomsten hebben:

- Aandachtspunten
- Input voor een risico logboek
- Input voor het ISMS
- Input voor aanvullende te nemen maatregelen
- Input voor Threat Intelligence, zie voor meer informatie de IBD 'Factsheet Threat Intelligence (TI) binnen uw gemeente[17].
- Input voor het doen van een melding en/of aangifte

[17] https://www.ibdgemeenten.nl/downloads/factsheet-threat-intelligence-ti-binnen-gemeente/

4 Wanneer specialistische hulp inschakelen

Het kan nodig zijn om specialistische hulp in te schakelen, dat kan om verschillende redenen:

- Het ontbreekt aan kennis en kunde om zelf onderzoek te doen.
- Het kost te veel tijd om het zelf goed te doen.
- Wanneer men niet verder komt.
- Wanneer gegevens zijn ontvreemd, encrypted en/of gewijzigd.

Het is raadzaam om in ieder geval een lijst te maken waarin is opgenomen welke partijen in welk geval inschakelt moeten worden, zodat men dit niet op het moment zelf moet uitzoeken. Hierbij kan gedacht worden om al met een aantal partijen gesprekken te hebben gevoerd zodat het bekend is welke mogelijkheden de partijen bieden en wat de mogelijke kosten zijn.

Ook kunnen er dan al afspraken gemaakt worden op welk moment de zo'n partij ingeschakeld kan worden en welke handelingen zij verwachten van een gemeente.

4.1 Wat kunnen gemeentes doen zonder specialisatische hulp

De eerste momenten na een incident zijn de belangrijkste. Het is cruciaal om vlak na een incident de betrokken omgeving en hardware veilig te stellen (zie checklist in hoofdstuk 6).

Het veiligstellen van de omgeving en hardware is iets dat een gemeente zelf kan doen.

Om een na een incident de omgeving en hardware te kunnen veiligstellen zal er een plan klaar moeten liggen. Ook zal er bijv. 1 keer per jaar geoefend moeten worden en zal op basis van de leerpunten tijdens de oefening het plan bijgesteld moeten worden.

In dit plan staat in ieder geval:
- Wie de incident manager is.
- Hoe de prioriteit van het incident wordt vastgesteld.
- Wie er als eerste reageert.
- Hoe de vaststelling om welke elektronische apparaten gaat het en wie er bij betrokken.
- Wie de interne en externe communicatie doet.

Omdat de eerste momenten na een incident de belangrijkste zijn is het aan te raden om een 'eerste reactie toolkit' te maken, deze toolkit bevat onder andere:
- Een handleiding hoe elektronische bewijsstukken te verzamelen en te bewaren.
- Afspraken die gemaakt zijn met (externe) partijen over hoe te handelen.
- Hoe in eerste instantie interviews af te nemen.
- Hoe het plaats delict te beschrijven.
- Hoe de omgeving veilig te stellen.
- Welke checklijsten er nagegaan moeten worden.
- Een lijst met veel gemaakte fouten.

4.2 Wanneer naar de politie gaan?

Het is niet zwartwit wanneer men de politie moet inschakelen, maar in ieder geval bij vermoeden van strafrechtelijke feiten.

In overleg met de politie zal worden vastgesteld hoe verder te handelen. Het kan dus voorkomen dat de politie het onderzoek overneemt.

5 Documentatie

Eén van de sleutels tot deugdelijk digitaal forensisch onderzoek is documentatie.

- Een zaak dient te worden ondersteund door bewijsstukken waarbij duidelijk is hoe dit bewijs is ontstaan en hoe er mee is omgegaan. Documenteer dus alles.
- Bewijs mag in principe nooit worden veranderd, alle veranderingen aan bewijs moeten worden gedocumenteerd.
- Achteraf moet de integriteit en authenticiteit van het originele uitgangsmateriaal kunnen worden aangetoond door aan te geven welke tools zijn gebruikt, waar en wanneer de gegevens zijn veilig gesteld en welke hashes daarvan gemaakt zijn. Gebruik liefst SHA-1 of beter nog SHA-256 hashes.
- Wanneer er met apparatuur wordt gewerkt waar gegevens vanaf worden gehaald, zoals een computer dan moet de datum en tijd van de computer worden genoteerd ten opzichte van de geldende datum en tijd. Dit helpt bij het later kunnen koppelen van bijvoorbeeld logging bestanden van verschillende systemen als er tijdsverschillen zijn.

Veranderlijk bewijs

Helaas, digitale rechercheurs vinden zelden de perfecte digitale plaats delict. Het komt voor dat een aanvaller doelbewust bewijsmateriaal vernietigt door het verwijderen van logs, verwijderen of overschrijven van gegevens of het versleutelen van gegevens.

Het komt ook voor dat je niet als eerste op de plaats delict aankomt, er kan dus al van alles met digitaal bewijs gebeurd zijn, tot onbedoeld vernietigen aan toe. Iedere beïnvloeding of verandering van bewijs tussen de tijd van de actie en het moment van veiligstellen van het bewijs moet hierbij in acht genomen worden.

Dit verschijnsel is niet uniek voor digitale recherche of digitaal onderzoek het komt ook voor in de niet digitale omgeving. Veranderlijk bewijs is met name een punt van zorg bij malware-incidenten, bewijs bevindt zich in het geheugen van computers en kan makkelijk worden gewist. Digitaal forensisch onderzoekers zullen rekening moeten houden met het feit dat digitale sporen veranderlijk kunnen zijn en ook makkelijk gewist kunnen worden. Dit kan overigens ook betekenen dat het resultaat van een onderzoek in twijfel kan worden getrokken.

5.1 Toelaatbaarheid van bewijs voor de rechtbank

Er zijn in Nederland bij civiele rechtszaken geen regels die bepalen wanneer bewijs toelaatbaar en/of bruikbaar is. Een rechter mag alles gebruiken om waarheidsvinding te doen. Ofwel, nergens staat vast hoe logbestanden er uit moeten zien noch hoe er na een incident gehandeld moet worden.

Ook hoeft een rechter niet te onderzoeken of bewijs vervalst is of niet, het gaat er om of het aannemelijk is of niet, behalve als er aanwijzingen zijn dat bewijs vervalst dan wel gemanipuleerd is. De rechter kan wel besluiten om minder waarde aan bewijs toe te kennen op het moment dat er een vermoeden bestaat van manipulatie. Daarom is het verstandig om latere discussies te voorkomen goed te beschrijven hoe er aan bepaald bewijs te gekomen.

Verder zijn er geen 'forensische normen' over hoe er bijvoorbeeld omgegaan moet worden met bewijsstukken. Ook wordt illegaal verkregen bewijs toegelaten bij een civiele rechtszaak of strafzaak, immers de rechter is op zoek naar de waarheid.

6 Bijlages, checklists

Dit hoofdstuk is een handreiking over hoe mogelijk te handelen in bepaalde situatie. Deze lijsten zijn zeker niet compleet en zullen moeten worden aangepast per situatie en omgeving.

6.1 De directe omgeving

Werkbeschrijvingen: Wanneer apparatuur aan staat, deze aan laten. Wanneer het uit staat, niet aanzetten.

Als een PC uitgeschakeld is:

• Stel het gebied (bijv. afsluitbare kantoorruimte) veilig waar de PC is geplaatst
• Laat printers en/of faxmachines prints/uitdraaien afronden
• Laat geen personen toe in de nabijheid van de computers en stroomvoorziening
• Zet, onder geen enkele voorwaarde, de PC aan
• Controleer of de PC daadwerkelijk uit staat, sommige screensavers geven een zwart beeld, maar de schijf- en monitor LEDs branden.
• Denk eraan dat sommige laptops inschakelen als je de klep opendoet
• Verwijder de batterij uit de laptop
• Verwijder de stroomtoevoer en andere gekoppelde apparaten, een PC die ogenschijnlijk uit staat, kan in sleep-mode staan waardoor via de netwerkkaart, op afstand bewijsmateriaal kan worden gewijzigd.
• Label en fotografeer alle componenten binnen de situatie, indien geen foto camera beschikbaar, maak dan een tekening
• Label poorten en kabels zodat de PC op later tijdstip weer kan worden opgebouwd
• Verwijder het apparaat voorzichtig en noteer unieke kenmerken, de kast, toetsenbord etc. hebben allen eigen nummers.
• Wees zeker dat alle apparaten en onderdelen op de juiste manier van labels zijn voorzien, indien dit niet goed gebeurt, kunnen de stukken geweigerd worden door de forensisch onderzoekers.
• Zoek binnen het gebied naar agenda's, dagboeken, notitieblokken of andere stukken waar wachtwoorden op genoteerd kunnen staan.
• Vraag eventueel gebruikers of er wachtwoorden zijn en noteer waar deze toegang tot verlenen en wat de wachtwoorden zijn.
• Maak gedetailleerde aantekeningen van alle handelingen die worden verricht gerelateerd aan de apparatuur

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Als een PC ingeschakeld is

• Stel het gebied (bijv. kantoorruimte) veilig waar de PC is geplaatst en neem als verantwoordelijke de controle
• Laat printers en/of faxmachines prints/uitdraaien afronden
• Laat geen personen toe in de nabijheid van de computers en stroomvoorziening
• Verwijder de aansluiting met een modem indien aanwezig
• Als de PC aan een netwerk (lijkt) is aangesloten, vraag advies aan de eindverantwoordelijke of een forensisch specialist
• Neem onder geen voorwaarde advies aan van de gebruiker/eigenaar van de computer
• Label en fotografeer alle componenten binnen de situatie, indien geen fotocamera beschikbaar, maak dan een tekening
• Label poorten en kabels zodat de PC op later tijdstip weer kan worden opgebouwd
• Verwijder alle kabelverbindingen die van de computer lopen naar andere aansluitingen, het zij in de muur of vloer, het zij een apparaat.
• Verwijder het apparaat voorzichtig en noteer unieke kenmerken, de kast, toetsenbord etc. hebben allen eigen nummers.
• Neem de tijd om de apparaten te laten afkoelen voordat deze worden verwijderd
• Zoek binnen het gebied naar agenda's, dagboeken, notitieblokken of andere stukken waar wachtwoorden op genoteerd kunnen staan.
• Overweeg om bij de gebruiker wachtwoorden te vragen, indien verstrekt, noteer deze accuraat
• Maak gedetailleerde aantekeningen van alle handelingen die worden verricht gerelateerd aan de apparatuur
• Leg vast door middel van een foto, screenshot, of notities wat er in beeld is op de monitor
• Raak het toetsenbord niet aan en klik niet met de muis. Indien een screensaver of leeg scherm op de monitor is te zien, laat de eindverantwoordelijke beslissen of een muisknop voldoende is het beeld te activeren en of dit gewenst is. Indien de screensaver met een wachtwoord is beveiligd, probeer dit te achterhalen en noteer dit. Leg, onder deze omstandigheden, de tijd en de activiteit van de muis vast.
• Als er geen specialist aanwezig is, verwijder dan de stroomtoevoer uit de achterzijde van de PC, zonder programma's af te sluiten of andere handelingen op het scherm te verrichten. Bij het verwijderen van de stroomtoevoer, altijd de stekker uit de computer trekken en nooit de stekker uit de muur trekken. Dit voorkomt dat er data naar de harde schijf wordt geschreven indien er een Ups is aangesloten.
• Bedenk: met het uitzetten van de PC kunnen kleine hoeveelheden bewijsmateriaal onherstelbaar worden beschadigd, echter het nog aanwezige bewijsmateriaal wordt bewaard en geaccepteerd als bewijs.

Wat valt allemaal onder Digitaal Forensisch Onderzoek:

Hardware zoals:
• De computerkast
• Beeldscherm, Muis en toetsenbord
• Kabels
• Voeding
• Draadloze netwerkkaarten
• Digitale camera's

Datadragers zoals:
• Externe harde schijven
• Dongels
• Back-up tapes
• Cd's en Dvd's
• Harde schijven niet verbonden aan de computer
• Geheugen stick (USB) en geheugen kaart ((Micro)SD)

De data op schijven is van groot belang, hierin zijn mogelijk sporen terug te vinden. Data is niet alleen de bestanden die te zien zin, maar verborgen en verwijderde bestanden zijn vaak nog belangrijker.

Ter ondersteuning van het onderzoek van de apparatuur, stel veilig:
• Handleidingen van de computer en software
• Alles wat wachtwoorden zou kunnen bevatten

Ter vergelijking van gemaakte prints stel veilig:
• Printers
• Gemaakte prints
• Indien nodig, print papier voor vergelijkend forensisch onderzoek

Tenslotte nog een aantal tips:
• Apparatuur alleen opslaan onder normale omstandigheden qua temperatuur en vochtigheid
• Houdt rekening met de levensduur van batterijen op het moederbord, CMOS informatie kan verloren gaan

6.2 De ICT-afdeling en gegevens terughalen

Tijdens een forensisch onderzoek speelt de ICT-afdeling een belangrijke rol. Zij hebben toegang tot gegevens, zoals log- en auditfiles. Ook kunnen zij gegevens terughalen van backups[18]. Deze gegevens kunnen tijdens het onderzoek een rol gaan spelen als bewijs. Daarom is het van belang dat er op regelmatige basis backups worden gemaakt en er wordt geoefend om deze terug te zetten.

Om tijdens een forensisch onderzoek te kunnen nagaan wat er is gebeurd is het van belang dat de systemen en applicaties zo zijn geconfigureerd dat deze:

- Auditinggegevens[19] verzamelen
- De auditgegevens worden doorgestuurd naar een veilige centrale auditserver
- Alle gelukt en mislukt authenticatiepogingen worden bijgehouden

Verder is het verstandig om in een lijst of database de hashwaardes van belangrijke documenten en applicaties bij te houden. Als deze documenten of applicaties onverwachts veranderen dan kan dit worden gedetecteerd door middel van een integriteitscheck applicatie.

De Internet Service Provider (ISP) houdt vaak logfiles bij van internetverkeer. Deze logfiles kunnen nuttig zijn tijdens een onderzoek. Het is verstandig om te inventariseren of en welke logfiles de ISP verzamelt en of u deze mag gebruiken voor het onderzoek.

[18] Zie ook aanwijzing back-up en recovery: https://www.ibdgemeenten.nl/downloads/?id=468
[19] Zie ook aanwijzing logging: https://www.ibdgemeenten.nl/downloads/?id=446

Bijlage: Voorbeeld beleid gemeente

Beleidsuitgangspunten forensisch onderzoek gemeente

Ten behoeve van de beveiliging van informatie is er beleid voor digitaal forensisch onderzoek (DFO). Het doel van dit beleid is om er voor te zorgen dat DFO dusdanig wordt ingericht dat het resultaat van DFO onderzoeken inhoudelijk juist worden uitgevoerd

De gemeente <naam gemeente> hanteert de volgende beleidsuitgangspunten en deze zijn ontleend aan de BIG en aanvullend op het algemene beveiligingsbeleid van de gemeente:

1. De gemeente gebruikt Digitaal Forensisch Onderzoek voor het onderzoeken van:
    1.1. Persoonsgericht integriteitsonderzoek, zoals
        1.1.1. Overtreding van integriteitsregels,
        1.1.2. Overtreding van gemeentelijk beleid en andere gemeentelijke regels.
    1.2. Digitaal Incidentonderzoek
2. Een Digitaal Forensisch Onderzoek zal subsidiair en proportioneel worden uitgevoerd.

Aldus vastgesteld door burgemeester en wethouders van *[gemeente]* op *[datum]*

[Naam. Functie] [Naam. Functie]

_____ _____

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE BEVEILIGINGS DIENST

INFORMATIEBEVEILIGINGSDIENST
V00R GEMEENTEN (IBD)

NASSAULAAN 12
2514 JS DEN HAAG

POSTBUS 30435
2500 GK DEN HAAG

HELPDESK 070 373 80 11
ALGEMEEN 070 373 80 08
FAX 070 363 56 82

INFO@IBDGEMEENTEN.NL
WWW.IBDGEMEENTEN.NL

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN**
VERENIGING VAN NEDERLANDSE GEMEENTEN