212

Digitaal forensische expertise met een scherp randje

Digitaal forensisch onderzoek

Digitaal forensisch onderzoek richt zich op het identificeren, veiligstellen en analyseren van elektronisch opgeslagen informatie om hieruit met specialistische forensische methodieken digitaal bewijsmateriaal te verkrijgen.

Elektronisch opgeslagen informatie

Elektronisch opgeslagen informatie bevindt zich onder meer in computersystemen en mobiele apparaten, maar ook binnen zogenaamde clouddiensten. In feite in (bijna) alles met een stekker of batterij.

Meer concrete voorbeelden van elektronisch opgeslagen informatie zijn chat berichten, e-mail correspondentie, inloggegevens, foto bestanden en GPS locatie gegevens. Ook voertuigen, elektronische fietsen, koelkasten, koffiezetapparaten en bankpassen bevatten elektronisch opgeslagen informatie.

Doelstelling

De belangrijkste doelstelling van een digitaal forensisch onderzoek is het verkrijgen van digitaal bewijsmateriaal voor toepassing binnen de context van een juridische procedure of intern onderzoek.

Toepassingsgebieden

1. ***Rechtszaken en juridische geschillen.*** Hierbij wordt digitaal bewijsmateriaal verkregen voor gebruik in civiele of strafrechtelijke procedures. Dit is veruit het meest voorkomende toepassingsgebied van digitaal forensisch onderzoek.
2. ***Cybercriminaliteit.*** Dit is een onderzoek naar hacking, malware, phishing en andere vormen van digitale criminaliteit waarbij computersystemen of netwerken zijn gebruikt dan wel aangetast.
3. ***Fraudeonderzoek.*** Dit omvat het verkrijgen van bewijsmateriaal van bijvoorbeeld financiële fraude, identiteitsfraude, contractbreuk, verduistering, diefstal van intellectueel eigendom of vervalsing van digitale documenten.
4. ***Datalekken en privacy-inbreuken.*** Onderzoek naar de oorsprong en omvang van datalekken en de identificatie van de personen of organisaties die verantwoordelijk zijn voor ongeautoriseerde toegang tot confidentiële of gevoelige informatie.
5. ***Kwesties inzake werknemers.*** Omvat onderzoeken binnen organisaties naar bijvoorbeeld ongeautoriseerde toegang tot bedrijfsgegevens, arbeidsconflicten, belangenverstrengeling of schending van bedrijfsbeleid en gedragsregels door werknemers.
6. ***Incident response.*** Dit is een onderzoek gericht op het detecteren, analyseren en beheersen van veiligheidsincidenten in digitale systemen. Belangrijke doelstellingen zijn het verzamelen van bewijsmateriaal voor nader forensisch onderzoek, het herstellen van beschadigde systemen en voorkoming van verdere schade. Het achterhalen van de oorzaak van het veiligheidsincident valt hier ook onder.

Soorten digitaal forensisch onderzoek

1. ***Onderzoek aan computersystemen.*** Dit omvat het onderzoeken van computers in de breedste zin van het woord. Denk bij dit type onderzoek aan bijvoorbeeld het herstel van opzettelijk verwijderde of verborgen bestanden en het maken van tijdslijnen van gebeurtenissen. Dat laatste met de doelstelling om gedetailleerd inzicht te verkrijgen in wat er precies is gebeurd met een bepaald computer systeem. Andere voorbeelden zijn het inzichtelijk maken van bepaalde internetactiviteiten zoals ingevoerde zoektermen in zoekmachines, de kopieer geschiedenis van bestanden, het analyseren van inloggegevens en webbrowser gebruik.

2. ***Onderzoek aan mobiele apparaten.*** Betreft het onderzoeken van ondermeer smartphones, tablets en de zogenaamde wearables zoals smart watches. Dit type onderzoek richt zich veelal op de analyse van chat berichten, de bel-geschiedenis, locatiegegevens en het gebruik van bepaalde software applicaties.

3. ***Netwerk forensisch onderzoek.*** Onderzoekt netwerkverkeer en -communicatie om sporen van cyberaanvallen, datalekken of ongeoorloofde toegang te identificeren.

4. ***Onderzoek aan clouddiensten.*** Richt zich op het onderzoeken van elektronisch opgeslagen informatie in cloud-omgevingen. Het gebruik van clouddiensten is de afgelopen jaren sterk toegenomen. Daarmee is ook de hoeveelheid data die niet meer fysiek binnen de eigen organisatie wordt opgeslagen toegenomen.

5. ***Malware forensisch onderzoek.*** Omvat de analyse van mogelijk schadelijke software (malware). Dit type onderzoek wordt met name uitgevoerd om de functionaliteit ervan te kunnen begrijpen, welke systemen het heeft geïnfecteerd en welke schade het heeft veroorzaakt.

6. ***Electronic discovery.*** Electronic discovery ook wel e-discovery genoemd is een onderzoek dat zich richt op het identificeren van specifieke relevante data binnen grote hoeveelheden elektronisch opgeslagen informatie. Bij een e-discovery onderzoek ligt de focus op informatie die relatief eenvoudig te ontsluiten is. Denk hierbij aan grote hoeveelheden e-mail correspondentie en bijlagen, agenda's, fotobestanden, digitale contracten en documenten of stukken uit financiële administraties. De nadruk bij e-discovery ligt op het efficiënt toegankelijk maken en ordenen van deze informatie, meestal voor analyse door externe professionals zoals accountants of juristen.

Wat levert digitaal forensisch onderzoek op

Een digitaal forensisch onderzoek levert bewijsmateriaal op dat kan worden gebruikt bij juridische procedures of intern onderzoek.

Het resultaat bestaat ondermeer uit een gedetailleerd rapport met bevindingen. Dit wordt opgesteld op basis van de uitgevoerde technische analyses en documentatie van de bewijsketen, de zogenaamde chain of custody. Dat laatste is essentieel voor het waarborgen van de forensische integriteit en daarmee de juridische toelaatbaarheid van het verkregen bewijs.

Een digitaal forensisch onderzoek kan de positie van een partij bij een juridisch conflict of geschil verbeteren en zelfs doorslaggevend beïnvloeden.

212 DIGITAAL FORENSISCH ONDERZOEK BV

NIEUWE GRACHT 3
2011 NB, HAARLEM
NEDERLAND