Digitaal forensische expertise
met een scherp randje

Forensisch e-mail onderzoek

Forensisch e-mail onderzoek omvat het systematisch analyseren van e-mailberichten, metadata headers en bijlagen om digitaal bewijs te verzamelen voor juridische procedures of interne onderzoeken en besluitvorming.

Dit onderzoek richt zich op het identificeren van fraude, phishing, datalekken, vervalsing of ongeautoriseerde communicatie. Hiervoor wordt gebruik gemaakt van digitale forensische technieken om de herkomst, integriteit en authenticiteit van e-mails vast te stellen.

Belang van forensisch e-mail onderzoek

Tot op de dag van vandaag is e-mail het meest gebruikte communicatie medium voor elektronische zakelijke correspondentie. Het is echter ook een van de meest kwetsbare communicatie media waarbij relatief kleine gebeurtenissen snel kunnen escaleren tot calamiteiten met ingrijpende gevolgen. Denk hierbij aan een gecompromitteerde IT infrastructuur, fraude, cyberaanvallen, interne bedrijfsconflicten en grensoverschrijdend gedrag, diefstal van intellectueel eigendom, malware infecties of de beruchte business email compromise.

Doelstelling

De primaire doelstelling van een forensisch e-mail onderzoek is het identificeren en veiligstellen van bewijsmateriaal uit e-mail gerelateerde communicatie. De bevindingen kunnen vervolgens als digitaal bewijsmateriaal worden gebruikt ter ondersteuning bij een juridische procedure of intern onderzoek en besluitvorming.

Aanpak van een forensisch e-mail onderzoek

De aanpak van een forensisch e-mail onderzoek verschilt in essentie niet met die van andere digitaal forensische onderzoeken. Een forensisch e-mail onderzoek kan als een enigszins bijzonder onderzoek worden aangemerkt omdat externe organisaties die bepaalde e-mail gerelateerde informatie beheren bijna altijd een rol spelen.

Ieder onderzoek begint daarom met een intake gesprek. Hierbij worden de onderzoeksvraag en de voor het onderzoek benodigde aard en omvang van elektronisch opgeslagen informatie vastgesteld. Met name waar deze informatie zich fysiek bevindt en hoe deze met behoud van forensische integriteit kan worden geacquireerd en veiliggesteld.

Toepassingsgebieden forensisch e-mail onderzoek

Er zijn diverse toepassingsgebieden voor een forensisch e-mail onderzoek.
Een aantal veel voorkomende zijn:

1. ***Fraudeonderzoek.*** Het identificeren en analyseren van e-mail correspondentie en bijbehorende metadata bij indicaties van ondermeer financiële- en / of verzekeringsfraude, werknemersmisbruik van tijd of middelen. Het traceren en terugverkrijgen van ontvreemde bedrijfsmiddelen en financiële middelen zijn andere voorbeelden.
2. ***Cybercriminaliteit.*** Het vaststellen van de oorzaak van datalekken en beveiligingsinbreuken op de IT infrastructuur, welke zijn veroorzaakt door phishing, hacking of malware verspreiding via e-mail. Het uniek identificeren van de hiervoor verantwoordelijke personen en organisaties behoort hier ook toe.
3. ***Interne bedrijfsconflicten en HR kwesties.*** Inhoudelijke analyse van e-mailcorrespondentie in geval van arbeidsconflicten, grensoverschrijdend gedrag van medewerkers of nalevingskwesties. Hieronder valt ook het onderzoeken van claims inzake ongepaste communicatie, zoals pesten, discriminatie en intimidatie op de werkvloer.
4. ***Diefstal van intellectueel eigendom.*** Het identificeren van het lekken van bedrijfsgeheimen of diefstal van vertrouwelijke informatie en intellectueel eigendom welke via e-mail correspondentie heeft plaatsgevonden.
5. ***Compliance audits.*** Verificatie van e-mailcommunicatie met betrekking tot naleving van opgelegde gedragsregels en reglementen. Bijvoorbeeld binnen de financiële sector of de gezondheidszorg, waar communicatie strikt gereguleerd is.
6. ***Juridische geschillen.*** Hieronder valt het identificeren en veiligstellen van bewijs in het kader van civiele rechtszaken of strafrechtelijke vervolging. E-mail correspondentie gerelateerde informatie kan worden gebruikt voor het bewijzen of weerleggen van claims inzake contractbreuk, laster, schending van een concurrentiebeding en overige juridische kwesties zoals conflictresolutie.
7. ***Herstel van verloren of verwijderde e-mail correspondentie.*** Dit omvat het herstellen van e-mail correspondentie en belangrijke zakelijke documenten welke opzettelijk of per ongeluk verloren zijn gegaan of vernietigd.
8. ***Tijdlijn reconstructie.*** Het opbouwen van een tijdlijn op basis van e-mail correspondentie gerelateerde gebeurtenissen is essentieel in zowel juridische processen als bij interne bedrijfsonderzoeken naar aanleiding van incidenten en conflictsituaties.
9. ***Vaststellen van authenticiteit.*** Dit omvat het vaststellen of e-mail berichten authentiek zijn en niet tussentijds zijn gewijzigd, gemanipuleerd of vervalst. Dit is vooral belangrijk in situaties waarbij er twijfels bestaan over de integriteit of intentie van de correspondentie.
10. ***Analyse van gedrag en intenties.*** Inhoudelijk onderzoek van e-mail correspondentie kan helpen om het gedrag en de intenties achter bepaalde correspondentie (beter) te begrijpen. Dit kan met name relevant zijn in gevallen van fraude, intimidatie, maar ook afpersing en oplichting of ander ongepast gedrag.

Het onderzoek zelf bestaat uit de volgende fases:

1. ***Acquisitie en veiligstellen van e-mail gerelateerde communicatie.*** Relevante e-mail gerelateerde correspondentie wordt geacquireerd op forensisch verantwoorde wijze en voorzien van zogenoemde chain of custody documentatie. Van de verkregen dataset worden één of meerdere werkkopieën gemaakt waarbij het origineel veilig wordt bewaard bij de opdrachtgever, advocaat, notaris of betrokken deurwaarder.

2. De forensische integriteit van de dataset wordt gewaarborgd door de toepassing van cryptografische algoritmes waardoor altijd kan worden geverifieerd en aangetoond dat er met een exacte bit voor bit gelijkwaardige dataset als het origineel wordt gewerkt.

3. ***Bewerking van de dataset.*** Deze fase betreft het gereedmaken van de geacquireerde dataset voor analyse. Hieronder valt het inzichtelijk maken van de metadata van e-mail communicatie zoals de headers maar ook eventuele bijlagen. Op bijlagen die bestaan uit gescande documenten wordt optical character recognition (OCR) toegepast zodat ook deze bijlagen doorzoekbaar worden middels zoektermen. Andere voorbeelden zijn het vertalen van e-mail correspondentie in eventuele vreemde talen en het waar mogelijk ongedaan maken van middels encryptie beveiligde e-mail correspondentie.

4. ***Analyse fase.*** De activiteiten in deze fase zijn sterk afhankelijk van de onderzoeksvraag en informatiebehoefte. Enkele voorbeelden die in deze fase worden uitgevoerd zijn inhoudsanalyse, metadata onderzoek, authenticiteit vaststelling, tijdlijn reconstructie, wie correspondeert met wie, herstel van correspondentie die verloren is gegaan, patroon- en zoekwoord analyse, malware analyse, etc. Eventueel kan koppeling van e-mail correspondentie artefacten aan andere digitale bewijzen plaatsvinden.

Wat levert een forensisch e-mail onderzoek op

Elk forensisch e-mail onderzoek wordt afgesloten met een presentatie- en rapportage fase. In deze fase worden alle onderzoekshandelingen, observaties en bevindingen gedocumenteerd en vastgelegd in een gedetailleerd rapport. Hierbij staat de juridische admissibiliteit van het verkregen bewijs en bevindingen voorop.

De bevindingen van het onderzoek worden persoonlijk besproken met de opdrachtgever en eventueel voorzien van aanbevelingen voor mogelijke vervolgstappen.

Bij afronding van het onderzoek wordt al het verzamelde bewijsmateriaal middels de chain of custody documentatie formeel overgedragen aan de opdrachtgever of rechtshandhavingsinstanties. Dit is afhankelijk van de aard en doelstelling van het onderzoek.

212 DIGITAAL FORENSISCH ONDERZOEK BV

NIEUWE GRACHT 3
2011 NB, HAARLEM
NEDERLAND