Introductie Forensisch IT-onderzoek

Paul Bakker en Matthijs van der Wel

Iedere organisatie krijgt vroeg of laat eens te maken met een verdenking, een delict of een vermoeden dat een delict plaats heeft gevonden. Hierbij kun je denken aan fraude, diefstal, bedrijfsspionage of bedreigingen en beledigingen van een werknemer. Bij deze activiteiten laat een dader vaak (ongewild) sporen na. Een forensisch onderzoeker gebruikt deze sporen om de daders op te sporen of de precieze toedracht te achterhalen. Steeds vaker zijn deze sporen ook digitale sporen. Het onderzoeken van digitale sporen is specialistisch werk en vergt een andere aanpak dan het onderzoeken van 'traditionele sporen'. Voor een mogelijke rechtsgang moet een onderzoek op een grondige en rechtsgeldige manier plaatsvinden. Om die reden is het verstandig dat organisaties bij delicten een forensisch IT-onderzoeker inzetten. Dit artikel geeft een kijkje in de wereld van het forensisch onderzoek en behandelt enkele belangrijke kenmerken van forensisch IT onderzoek.

ir. P.J. Bakker CISSP CISA is Chief Technical Officer Crypto bij Fox-IT en heeft in het verleden veel forensische onderzoeken uitgevoerd en forensische software ontwikkeld.
M. van der Wel MBA CISSP CISA RON was tot voorkort Business Unit Manager van de Business Unit Forensics & Audits bij Fox-IT en is nu verantwoordelijk voor de internationale sales.

Forensisch IT-onderzoek

Bij veel handelingen die we dagelijks verrichten laten we gewone en digitale sporen na. De digitale sporen ontstaan bijvoorbeeld al door het versturen van een e-mailbericht, het maken of verwijderen van een bestand, het ontvangen van een SMS-bericht of het gebruiken van een pasje om toegang te krijgen tot een pand. Voor forensische onderzoeksdoeleinden kunnen deze digitale sporen erg belangrijk zijn. Een digitaal sporenonderzoek beperkt zich niet alleen tot een voornamelijk digitaal uitgevoerd delict, zoals bijvoorbeeld het hacken van een server. Het is ook zeer goed bruikbaar bij 'traditionele delicten' zoals fraude en diefstal. Mede door de toenemende hoeveelheid ICT-hulpmiddelen die we gebruiken, zijn bij fraude- en diefstalzaken vaak ook digitale sporen aanwezig. Het is dan ook niet meer dan begrijpelijk dat digitaal sporenonderzoek een steeds belangrijker onderdeel vormt van een forensisch onderzoek.

Naast het zoeken naar achtergelaten sporen is het in een digitaal onderzoek ook mogelijk om te zorgen dat toekomstige sporen kunnen worden onderzocht. Een voorbeeld hiervan is het gedurende een periode vastleggen van e-mailverkeer, Internetgebruik en alle handelingen die op een werkstation plaatsvinden.

Kort gezegd is forensisch IT onderzoek dus een specialisatie van forensisch onderzoek waar de focus voornamelijk ligt op het analyseren van digitale sporen van een al dan niet digitaal uitgevoerd delict.

Eigen onderzoek

Veel grote organisaties voeren van oudsher zelf onderzoeken uit en vinden dat zij ook een forensisch IT onderzoek kunnen uitvoeren. Het waarnemen van deze 'nieuwe' sporen is volgens hen namelijk niet erg ingewikkeld: het plaatje staat op de harde schijf of niet. Het e-mail bericht is verzonden door de medewerker of niet.

Toch is het belangrijk om deze keuze goed te overwegen. Hoewel een onderzoek grotendeels bestaat uit het verzamelen van sporen en bewijzen, is het vaak wel de bedoeling deze sporen en bewijzen te gebruiken in bijvoorbeeld een ontslagprocedure. Om rechtsgeldig te zijn, moet een dergelijk onderzoek ook volgens de juiste procedures uitgevoerd worden en 'reproduceerbaar' zijn.

Helaas komt het toch nog voor dat een gedeelte van de

sporen en bewijzen niet in de rechtszaal bruikbaar is, doordat een systeembeheerder of beveiligingsmedewerker zelf al onderzoek uitgevoerd heeft op een verdacht systeem. Doordat er wijzigingen op het systeem hebben plaatsgevonden, is het moeilijk nog een goede analyse uit te voeren.

Een betrokkene mag daarbij juridisch gezien altijd een contra-expertise laten uitvoeren. Als in de contra-expertise niet met hetzelfde bronmateriaal gewerkt kan worden, kan niet meer worden vastgesteld dat het bewijsmateriaal origineel en dus niet geprepareerd is.

Een andere reden om niet zelf als organisatie het forensisch onderzoek te doen, is dat het vanuit onafhankelijkheidsoogpunt niet altijd gewenst is dat collega's de handelingen van een collega-medewerker onderzoeken.

Particulier recherchebureau

Bij gegronde verdenkingen heeft iedere organisatie zelf het recht om een gericht onderzoek uit te voeren, maar mag dat recht ook overdragen aan een particulier recherchebureau.

Een particulier recherchebureau mag niets méér onderzoeken dan de organisatie zelf mag doen; het onderzoekt uitsluitend de eigen middelen van de organisatie. Het gaat hier dus om de (IT) middelen die daadwerkelijk in eigendom zijn van de organisatie. Als een medewerker bijvoorbeeld zijn privé USB-stick gebruikt voor bedrijfsdoeleinden, mag een organisatie deze USB-stick niet zonder meer betrekken in het onderzoek. Een uitzondering is als er sprake is van een wettelijk strafbaar feit. Dit onderzoek wordt dan uitgevoerd door het Openbaar Ministerie.

Om te garanderen dat een onderzoek door een particulier recherchebureau aan bepaalde normen voldoet, stelt het Ministerie van Justitie eisen aan bedrijven die een vergunning Particulier Recherchebureau willen verkrijgen. Deze eisen houden onder andere in dat alle medewerkers een antecedentenonderzoek moeten ondergaan en het officieel erkende diploma 'Particulier Onderzoeker' moeten hebben gehaald.

Ook worden eisen gesteld aan wanneer en op welke wijze een onderzoek plaatsvindt. Zo moet er een gegronde verdenking zijn, moet het onderzoek gericht plaatsvinden en spelen de begrippen subsidiariteit en proportionaliteit een rol. Subsidiariteit betekent dat als je de keuze hebt uit verschillende onderzoeksmiddelen, je het lichtste middel in moet zetten. Proportionaliteit geeft aan dat het gebruikte middel in relatie moet staan tot het doel. Aan beide voorwaarden moet in een forensisch onderzoek altijd zijn voldaan.

We zullen deze voorwaarden aan de hand van een voorbeeld toelichten. Als een organisatie een werknemer verdenkt van het via e-mail verhandelen van illegale films dan zal de organisatie dit nader willen onderzoeken. Dit kan bijvoorbeeld door alle IT middelen van de organisatie, inclusief USB-sticks, mailboxen en bestanden van alle werknemers, te doorzoeken op illegale software, audio en video. Dit voldoet dit niet aan de voorwaarden van subsidiariteit en proportionaliteit en de eis om een zo gericht mogelijk onderzoek te doen. De verdenking gaat immers maar over één werknemer en slechts over videomateriaal. Om aan de voorwaarde van proportionaliteit te voldoen zal het onderzoek zich moeten beperken tot de verdachte werknemer. Om te voldoen aan de voorwaarde van subsidiariteit is het daarnaast nodig het onderzoek te beperken tot door de medewerker gebruikte IT middelen. Hierbij is het onderzoek zo gericht mogelijk uitgevoerd.

Naast de eisen van het Ministerie van Justitie stelt het College Bescherming Persoonsgegevens (CBP) eveneens eisen aan particuliere recherchebureaus. Een particulier recherchebureau moet een openbare melding doen over de methodes die zij hanteert en het CBP geeft hierover haar goedkeuring. Tenslotte is er nog een aantal wettelijke regels en bepalingen die van belang zijn bij de uitvoering van een onderzoek door een particulier recherchebureau, zoals het instemmingsrecht en de geheimhoudingsplicht van de ondernemingsraad en de Wet Bescherming Persoonsgegevens, waarin ook een informatieplicht naar de betrokkenen staat.

Onafhankelijkheid en objectiviteit

Een van de eisen die aan de onderzoeker en het bedrijf worden gesteld is dat deze aan 'objectieve waarheidsvinding' doet. Objectieve waarheidsvinding houdt in dat de onderzoekers niet uitsluitend zoeken naar mogelijk belastende sporen, maar juist ook naar ontlastende sporen of alternatieve verklaringen. Het uitvoeren van 'hoor en wederhoor' zorgt dat een onderzoek ook andere mogelijke verklaringen meeneemt.

Deze objectieve waarheidsvinding is ook terug te vinden in de omgang met de opgestelde eindrapportage. De betrokkene heeft altijd recht op inzage in het conceptrapport en heeft het recht deze van commentaar te voorzien.

Daarnaast kan iedereen die met een onderzoeksrapport wordt geconfronteerd, een contra-expertise laten uitvoeren. Dit is de reden waarom het op de juiste wijze veiligstellen

van de sporen cruciaal is. Hiervoor worden tijdens het veiligstellen van digitale sporen zogenaamde 'hashwaardes' berekend om later vast te kunnen stellen dat deze onveranderd zijn gebleven. Daarnaast is het vastleggen van een 'chain of custody' zeer belangrijk. Deze chain of custody geeft informatie over alle handelingen die uitgevoerd zijn op veiliggestelde informatie. De hashwaardes en de chain of custody geven een contra-onderzoeker de mogelijkheid om te controleren of deze hetzelfde bronmateriaal onderzoekt en om vast te stellen wie toegang heeft gehad tot het bronmateriaal. Het recherchebureau is verantwoordelijk voor het correct en volledig vastleggen van deze chain of custody.
In de praktijk komt het soms voor dat onderzoekers tijdens een onderzoek 'geprepareerd' bewijsmateriaal tegenkomen. Geprepareerd bewijsmateriaal is bewust aangepast of toegevoegd om het onderzoek een bepaalde kant op te sturen. Een voorbeeld hiervan is het plaatsen van een compromitterende foto op een harde schijf. Door kritisch te kijken naar elk gevonden 'bewijs' is het mogelijk om geprepareerde sporen te herkennen.

Een ander instrument wat nog eens extra bijdraagt aan de objectieve waarheidsvinding is het 'schaduwonderzoeken'. Deze extra onderzoekers verifiëren het resultaat van de hoofdonderzoekers door met een andere onderzoeksmethode dezelfde gegevens nogmaals te onderzoeken.

Overzicht stappen

Hoewel ieder onderzoek anders is en haar eigen probleemstelling heeft, is het mogelijk een algemene beschrijving van de verschillende onderdelen van een forensisch onderzoek te geven. De stappen beschrijven een forensisch onderzoek vanuit de optiek van een organisatie die een recherchebureau inschakelt. De doorlooptijd van een dergelijk onderzoek kan variëren van een aantal dagen tot enkele weken.

Stap 1: Voorbereiding

Voordat een particulier recherchebureau een forensisch (IT) onderzoek kan beginnen zijn een intakegesprek en een schriftelijk plan van aanpak nodig.

In het intakegesprek met de opdrachtgever achterhaalt de hoofdonderzoeker de doelstelling van het onderzoek en beoordeelt hij of een onderzoek ook daadwerkelijk gerechtvaardigd is. Een onderzoek is slechts gerechtvaardigd als inderdaad sprake is van gegronde verdenkingen, proportionaliteit en subsidiariteit. Het gesprek dient ook als basis om te bepalen op welke locaties men het beste kan zoeken naar mogelijke sporen.

Naar aanleiding van het intakegesprek stelt de hoofdonderzoeker een plan van aanpak op. Hierin staat de situatie beschreven, evenals de onderzoeksvragen, en een voorstel voor de wijze van uitvoering van het onderzoek. Hierin staat ook beschreven welke partijen de verschillende onderzoeksactiviteiten uitvoeren of ondersteunen. Bij grotere organisaties zijn vaak de IT afdeling, de Security afdeling en de interne Audit afdeling betrokken bij een forensisch onderzoek. Het plan van aanpak eindigt met een inschatting van de inzet en een planning voor de uitvoering van de verschillende activiteiten.

Stap 2: Veiligstellen gegevens

Een van de belangrijkste onderdelen van een forensisch onderzoek is het adequaat en spoedig veiligstellen van de verschillende sporen die aanwezig zijn op een 'plaats veiligheidsinbreuk'. Dit hoeft zich niet te beperken tot digitale sporen, maar kan ook een scala aan niet-digitale sporen behelzen. Het is echter wel zaak tijdig te beginnen met het veiligstellen van eventuele sporen om het verdwijnen of overschrijven hiervan te voorkomen (denk bijvoorbeeld aan overschrijven van logbestanden) of omdat het, naarmate de tijd vordert, moeilijker is om bepaalde sporen in verband te brengen met een natuurlijke persoon.

Bij het veiligstellen van digitale sporen is het noodzakelijk dat men rekening houdt met het specifieke karakter van digitale gegevens. Digitale sporen zijn namelijk eenvoudiger manipuleerbaar dan traditionele sporen. Een groot voordeel van digitale sporen is dat het vaak mogelijk is een identieke kopie te maken van het spoor, iets dat met traditionele sporen vaak niet goed mogelijk is. Hiervoor zijn standaard digitale kopieermethodes echter niet toereikend. Een forensische kopie van bijvoorbeeld een harde schijf bestaat uit een volledige kopie van alle informatie op de schijf en niet slechts de voor de gebruiker zichtbare bestanden. Een forensische kopie bevat bijvoorbeeld ook alle gewiste bestanden, niet gebruikte ruimtes en besturingssysteeminformatie. Deze kunnen namelijk veel belangrijke en relevante informatie voor het onderzoek bevatten.

Het veiligstellen van digitale sporen is specialistisch werk. Zo is het onder andere nodig om over de forensische kopieën zogenaamde hashwaardes te berekenen om in de toekomst altijd te kunnen controleren of het oorspronkelijke bronmateriaal niet gewijzigd of beschadigd is. Hiervoor maakt men gebruik van speciale apparatuur waarmee het mogelijk is snel, volledig en op meerdere manieren mogelijke sporen en gegevensdragers veilig te stellen. Een voorbeeld hiervan is het maken van een forensische kopie van een harde schijf uit een PC of laptop of het maken van een kopie van de gegevens uit een mobiele telefoon. In sommige speciale gevallen is het zelfs nodig om gegevens veilig te stellen uit een systeem dat nog 'aan' staat en niet 'uit' kan.

Stap 3: Analyse

Voordat de verzamelde digitale informatie in een onderzoek bruikbaar is, wordt deze doorzoekbaar gemaakt en geïndexeerd. Met behulp van steekwoordenlijsten is het mogelijk snel en doeltreffend in deze grote hoeveelheden data te zoeken. De doorzochte data bestaat niet alleen uit de zichtbare bestanden op harde schijven, maar ook uit informatie

die onder de oppervlakte verborgen ligt, zoals verwijderde bestanden of de niet gebruikte ruimte aan het eind van elk bestand. Forensische apparatuur en software kunnen deze verborgen informatie zichtbaar maken voor de onderzoekers.

De onderzoeker onderzoekt de aangetroffen sporen en interpreteert deze in de gestelde context. Hierna is het zaak om de sporen aan natuurlijke personen te koppelen en waar nodig tijdlijnen op te stellen om een beeld te krijgen van de volgtijdelijkheid van specifieke sporen. De onderzoeker kan zo een helder beeld vormen van het gevonden bewijsmateriaal door het recherche-onderzoek en de juiste relatie tussen en interpretatie van de sporen.

Om te illustreren dat de interpretatie en een tijdlijn van sporen belangrijk zijn, geven we het volgende voorbeeld. Binnen een organisatie is een e-mail verstuurd die een leidinggevende beledigt en bedreigt. De e-mail is anoniem verstuurd met een webmail account. Na onderzoek van het e-mailbericht en de logfiles, lijkt de e-mail verstuurd te zijn vanaf een specifieke vaste werkplek binnen het bedrijf. Hiermee is dus impliciet een medewerker aangewezen. Bij de ondervraging ontkent de medewerker alles en beweert dat iemand anders de e-mail vanaf zijn plek gestuurd moet hebben terwijl hij afwezig was. Het is dus van belang in het onderzoek ook daadwerkelijk aannemelijk te maken of deze medewerker ook op dit tijdstip op deze werkplek aanwezig was. Het onderzoeksteam onderzoekt hiervoor de PC en stelt vast dat het surfgedrag op de PC is gewist. Het onderzoeksteam weet deze historie bestanden terug te halen. De analyse laat vervolgens zien dat vlak voor en na de verstuurde e-mail ook gebruik is gemaakt van de privé-webmail van de medewerker. Hierdoor is het aannemelijk te maken dat de medewerker ook zelf de anonieme e-mail heeft verstuurd.

Stap 4: Rapportage

Ieder forensisch onderzoek eindigt met een onderzoeksrapportage. De onderzoeksrapportage schetst de situatie en geeft antwoord op de onderzoeksvraag. Verder staan in de rapportage de Stukken van Overtuiging: Het verzamelde 'bewijsmateriaal' waarop onderzoek heeft plaatsgevonden. De rapportage vervolgt met de uitkomsten van het onderzoek en de conclusies en aanbevelingen. In dit laatste hoofdstuk staat tevens het antwoord op de gestelde onderzoeksvraag. Het kan ook voorkomen dat het nodig is de onderzoeksrapportage in de rechtbank te presenteren om de rechtsgang te ondersteunen. Hierbij is de forensische onderzoeker dan getuige-deskundige in de rechtbank.

Forensische softwaretools

Aangezien digitale gegevensdragers veel meer gegevens/informatie bevatten dan mensen handmatig kunnen bekijken binnen redelijke tijd is het gebruik van een verzameling van forensische softwaretools onvermijdelijk. Deze forensische tools maken het mogelijk om de enorme hoeveelheid digitale gegevens snel en effectief te doorzoeken en te interpreteren.

Het is ondanks de vele goede tools niet mogelijk om volledig op deze tools te vertrouwen. Een goed voorbeeld is het bestaan van de 'Metasploit Anti-forensics' toolkit. Deze set open source applicaties is juist bedoeld om de standaard forensische tools om de tuin leiden door valse sporen toe te voegen en echte sporen te verbergen of te wissen. Het is daarom belangrijk te weten hoe de resultaten van een bepaalde tool te interpreteren zijn, welke waarde hieraan verbonden kan worden en wat de beperkingen zijn. Ook hier is het gebruik van een schaduwonderzoek een goede vorm van kwaliteitsborging.

Ook al zijn er veel commerciële en open source tools te verkrijgen, het komt vaak voor dat een onderzoek een uniek aspect heeft dat de bestaande tools niet kunnen afhandelen. Het komt dus regelmatig voor dat speciale forensische software specifiek voor een onderzoek wordt ontwikkeld. Bijvoorbeeld de ontwikkeling van software om honderden Outlook e-mailboxen geautomatiseerd te kunnen doorzoeken op een lijst met trefwoorden of het analyseren van logfiles van speciaal ontwikkelde applicaties, zoals de software van pinterminals.

Ondanks dat tools vaak de basis vormen van een onderzoek, staat in de rechtszaal de validiteit van de gebruikte tools niet vaak ter discussie. De gebruikte tool is vaak niet erg interessant, omdat het gaat om de getrokken conclusies en of de resultaten objectief valideerbaar zijn. Een goede mogelijkheid om te bewijzen dat de tools goed hebben gewerkt is als schaduwonderzoekers met andere tools – onafhankelijk van het eerdere onderzoek – met dezelfde conclusie komen.

Conclusie

Dit artikel heeft een kijkje gegeven in de wereld van het forensisch onderzoek. Iedere organisatie heeft vroeg of laat eens te maken met delicten, verdenkingen of vermoedens. Een forensisch onderzoek kan duidelijkheid bieden over de toedracht, mogelijke motieven, daders en hulpmiddelen. Wij hebben uitgelegd dat het doen van een forensisch onderzoek anders is dan een 'gewoon' onderzoek. Om een forensisch onderzoek rechtsgeldig te kunnen gebruiken, is een degelijke uitvoering noodzakelijk en kan een particulier rechercheburo een rol spelen. Een goed en rechtsgeldig forensisch onderzoek volgt nauwgezette processtappen en is gebonden aan richtlijnen en moet worden uitgevoerd door forensisch deskundigen.
En dat is nodig om bewijs echt als hard bewijs te kunnen gebruiken in de rechtzaal. De aanschaf van specialistische tools maakt nog geen goede forensisch IT onderzoeker. Dit is een (nieuw) vakgebied waarbij kennis, kunde en ervaring van essentieel belang zijn.