Secura
A BUREAU VERITAS COMPANY

Digitaal Forensisch Onderzoek

Criminelen gebruiken steeds vaker computers om misdrijven te plegen. Als bedrijf kunt u daarvan het slachtoffer worden waarbij de gevolgen vaak lastig te voorspellen zijn. Soms is het slechts een vermoeden van een misdrijf en moet worden vastgesteld of er daadwerkelijk een incident heeft plaatsgevonden.

In veel gevallen is een digitaal forensisch onderzoek nodig om vast te stellen wat er is gebeurd. Bijvoorbeeld als u een datalek vermoedt, of een hack van buitenaf. Maar ook om te onderzoeken of intellectueel eigendom is ontvreemd of wanneer een medewerker verdacht wordt van het lekken van bedrijfsgeheimen.

Secura is geregistreerd als Particulier Onderzoeksbureau bij het ministerie van Justitie en Veiligheid en heeft medewerkers die gekwalificeerd particulier digitaal onderzoeker zijn. Hierdoor is Secura in staat om rapportages en bescheiden af te geven die gebruikt kunnen worden in juridische procedures.

Wat is Digitaal Forensisch Onderzoek?

Vrijwel alle organisaties zijn tegenwoordig afhankelijk van informatietechnologie (IT). Door deze ontwikkelingen ontstaan potentieel kwetsbare systemen die vaak ook nog met elkaar in verbinding staan en daardoor nieuwe risico's met zich mee brengen. Net als in de fysieke wereld is het belangrijk deze digitale wereld te beschermen tegen ongeoorloofd gebruik en maatregelen te nemen om vast te kunnen stellen wat er bij een bepaald systeem gebeurd is. Digitaal forensisch onderzoek is het vakgebied dat zich bezighoudt met het opsporen en reconstrueren van incidenten in digitale systemen.

Digitaal onderzoek is essentieel om te kunnen leren van incidenten die zich hebben voorgedaan en incidenten in de toekomst te voorkomen. Gebruikers van informatiesystemen laten namelijk digitale sporen achter wanneer ze de systemen gebruiken - of het nu gaat om computersystemen, smartphones, mobiele telefoons, tablets of netwerken. Er zijn digitale forensische tools en technieken beschikbaar voor het veiligstellen en analyseren van digitaal bewijsmateriaal. Digitale forensische tools en technieken kunnen ook worden gebruikt om bijvoorbeeld verloren bestanden te herstellen of om interne systemen te monitoren.

Digitaal forensisch onderzoek wordt voornamelijk gebruikt voor onderzoeken die zijn gericht op juridische of wetshandhavingskwesties die mogelijk of waarschijnlijk voor de rechter zullen eindigen; vandaar de nadruk op juridische aanvaardbaarheid. Digitaal bewijs is uiterst vluchtig en kan gemakkelijk verloren gaan of worden aangepast bij onzorgvuldig handelen. Het is dus nodig om digitaal bewijsmateriaal te bewaren en te behandelen op een manier die ervoor zorgt dat het niet wordt vervormd of vernietigd.

Digitaal forensisch onderzoek is een vakgebied dat nog in ontwikkeling is. Het kan worden gedefinieerd als het gebruik van computer- en informatiesysteemkennis, in combinatie met juridische kennis, om op een juridisch aanvaardbare manier digitaal bewijsmateriaal dat is verkregen, verwerkt en opgeslagen op een wettelijk aanvaardbare manier te analyseren.

Welke soorten Digitaal Forensisch Onderzoek zijn mogelijk?

Secura biedt een aantal vormen van digitaal forensisch onderzoek. Afhankelijk van de casus zal worden bepaald welke vormen het meest geschikt zijn. Daarnaast kunnen ook adviestrajecten worden uitgevoerd, bijvoorbeeld om te kijken hoe goed een organisatie is voorbereid op een eventueel incident. Hieronder worden de meest gangbare onderzoeksmethodes toegelicht.

DIGITAAL FORENSISCH SPORENONDERZOEK

Secura beschikt over de benodigde expertise om digitaal forensisch sporenonderzoek uit te voeren op een wijd scala aan apparatuur, van laptops tot werkstations en telefoons.

Een digitaal forensisch sporenonderzoek kan uitsluitsel geven over de onderstaande situaties:

- Is ongeoorloofde toegang tot mijn systemen verkregen?
- Hebben zich ongeoorloofde activiteiten voorgedaan in mijn organisatie?
- Zijn gevoelige gegevens weggesluisd of anderszins verkregen tijdens een security incident?
- Is gebruik gemaakt van specifieke kwetsbaarheden in software of systemen, en hoe is dat gedaan?

Dit soort onderzoeken worden ook wel post-mortems genoemd, omdat na het incident moet worden vastgesteld wat er is gebeurd. Met behulp van specialistische software is Secura in staat om verdachte activiteiten in kaart te brengen zoals:

- In kaart brengen van verdachte activiteiten door middel van analyse op verschillende systeembronnen;
- Uitgevoerde (malafide) programma's;
- Geopende bestanden;
- Bezochte websites;
- Succesvolle/niet-succesvolle loginpogingen;
- Aangesloten USB-apparatuur zoals datadragers.

Tijdens het forensisch onderzoek wordt uitvoerig contact onderhouden met de opdrachtgevers van het onderzoek. Na oplevering van het rapport vindt een debrief plaats; in de debrief wordt gefocust op een korte samenvatting van het onderzoek en relevante aanbevelingen zodat vergelijkbare incidenten wellicht in de toekomst kunnen worden voorkomen.

ONDERZOEK MOBIELE APPARATEN

Smartphones en tablets zijn niet meer weg te denken uit het dagelijks leven en worden gebruikt voor verschillende zakelijke toepassingen. Secura heeft de mogelijkheden om dergelijke apparaten grondig te onderzoeken en verschillende sporen te analyseren. Hierbij valt te denken aan:

- Het uitlezen van de belgeschiedenis;
- Geïnstalleerde apps;
- Recent gebruikte WiFi netwerken;
- Gekoppelde apparatuur via Bluetooth;
- Bezochte webpagina's;
- Het uitlezen van beschikbare mail- en agendasporen;
- Ontvangen berichten waaronder SMS, WhatsApp en soortgelijke chat-diensten.

Het is hierbij wel van belang dat het apparaat kan worden ontsloten: moderne telefoons en tablets kunnen niet zonder meer worden onderzocht op alle aspecten als deze niet is ontsloten.

E-MAILONDERZOEK

Het onderzoeken van e-mail van een medewerker kan deel uitmaken van het digitaal forensisch onderzoek. Met behulp van gespecialiseerde software is Secura in staat om (verwijderde) mails inclusief bijlages inzichtelijk te maken en de communicatie met verschillende partijen in kaart te brengen. Soms kan dit middel ook worden gebruikt om vast te stellen of bijvoorbeeld malware via e-mail is verspreid.

ONDERZOEK CLOUD-OMGEVINGEN AWS & AZURE

Het gebruik van cloud-diensten zoals Amazon Web Services (AWS) en Microsoft Azure wordt steeds meer gemeengoed in zakelijke IT-infrastructuren. Secura is in staat om forensische onderzoeken ook op dergelijke omgevingen uit te voeren. Hierbij valt te denken aan het onderzoeken van virtual machines en de bijbehorende logging van verschillende AWS en Azure diensten.

FORENSIC READINESS

Forensic Readiness geeft aan in hoeverre een organisatie in staat is digitaal bewijs te verzamelen, bewaren, beschermen en analyseren zodat het effectief gebruikt kan worden bij beveiligingsonderzoeken, beantwoording van vragen van toezichthouders, interne juridische kwesties of in de rechtszaal. Hierbij wordt gekeken of en welke vormen van logging en monitoring wordt gebruikt, en of dit afdoende is. In een of meer workshops zal Secura diverse scenario's en bedreigingen doorlopen, om samen met uw technische experts en beheerders te analyseren of uw organisatie klaar is om een incident goed te kunnen onderzoeken. Dit is een belangrijke component van cyberweerbaarheid, omdat het ook het herstelvermogen na een digitale aanval sterk kan vergroten.

De workshop kan uitgevoerd worden in een of meer dagdelen en zal de verschillende fases van een forensisch incident behandelen, waaronder detectie, analyse, indamming en hersteloperaties. Het wordt aangeraden om een workshop bij te wonen met hetzelfde team dat ingeschakeld zal/gaat worden bij een echt incident. Na de workshop worden opgemerkte aandachtspunten verwerkt in een rapportage.

De aanpak van Secura voor een succesvol onderzoek

ONZE ONDERZOEKSAANPAK

Binnen digitaal forensisch onderzoeken volgt Secura een gefaseerde aanpak met ruimte voor verschillende testmethodieken die afhankelijk zijn van het doel, de te onderzoeken omgeving (architectuur, platform, applicatie enz.), branche vereisten of zelfs regelgeving per land.

Dit zorgt voor een professionele aanpak van projecten waarbij wij nauwgezet en methodisch het security vraagstuk onderzoeken. Dit helpt om volledig en nauwkeurig te zijn en geeft zekerheid dat de juiste zaken onderzocht zijn en kwetsbaarheden gevonden worden.

Voor een succesvol onderzoek is het van belang dat Secura toegang krijgt tot de benodigde bronnen. Indien het onderzoek daar aanleiding toe geeft kan het gewenste aantal bronnen groter worden, waarvoor contact zal worden opgenomen met de opdrachtgever voordat Secura deze bronnen gaat onderzoeken. Uiteraard zal er tijdens het onderzoek altijd nauw contact zijn om de voortgang van het onderzoek te bespreken.

Secura zal voorafgaand aan een forensisch onderzoek een plan van aanpak opstellen, waar de opdrachtgever akkoord op dient te geven. Als het plan van aanpak door de opdrachtgever goedgekeurd is en de vereiste toestemming gegeven is, begint het daadwerkelijke onderzoek. Na afloop van het onderzoek volgt een schriftelijke rapportage met de bevindingen zoals tijdlijnen en bewijsvoering.

Belangrijk om te noemen is dat Secura in haar onderzoeken beperkt is door de mate waarin logging en sporen beschikbaar zijn op de te onderzoeken gegevensdragers. Het komt voor dat tijdens een onderzoek moet worden vastgesteld dat er reeds eerder sporen zijn gewist of verloren zijn gegaan. Er kunnen dan ook geen garanties worden gegeven over het al dan niet definitief kunnen vaststellen wat er is gebeurd. Verder is het belangrijk om te weten dat Secura geen Incident Response (IR) activiteiten ontplooit waarbij een actieve aanval wordt bestreden.

STAPPENPLAN EN FASERING MET ACTIVITEITEN

Het digitaal forensisch onderzoek van Secura bestaat uit de volgende zeven fases:

VOORBEREIDING	In de eerste fase van een forensisch onderzoek wordt een onderzoeksomgeving (crime lab) opgezet. Onder de onderzoeksomgeving vallen de infrastructuur, hardware, software, het logboek en handelingsprotocollen, zoals vaststellen wie eindverantwoordelijk is. In deze fase vindt ook het vooronderzoek plaats en wordt het plan van aanpak opgesteld. Hierin wordt vastgesteld wat er wordt onderzocht, wat de hoofdvraag- en deelvragen zijn en of er hypotheses kunnen worden opgesteld. Uiteraard altijd in overleg met de opdrachtgever.
VERWERVING	In deze fase van het forensisch onderzoek wordt de onderzoeksdata verkregen of veiliggesteld. Dit wordt meestal gedaan door middel van `Imaging'. Het veiligstellen van onderzoeksdata wordt beschreven en toestemming zal worden vastgelegd in een verklaring. Alle verdere onderzoeksactiviteiten worden op deze forensische kopieën uitgevoerd. De originele gegevensdragers blijven onaangeroerd.
VERWERKING	De processtappen Verwerking en Analyse kunnen simultaan plaatsvinden. In deze fases wordt data geïdentificeerd, worden bestandstypes herkend, worden bestanden ontsleuteld en indien mogelijk zullen bestanden worden `ontdubbeld'.
ANALYSE	Tijdens een forensisch onderzoek is het gebruikelijk een tijdlijn op te stellen. Door middel van een tijdlijn wordt een overzicht opgesteld waarmee mogelijke verbanden worden gelegd tussen uitgevoerde acties. Tijd en datum zijn de meest kritieke onderdelen in forensisch proces. Daartoe zal data in gespecialiseerde software worden geïndexeerd om sneller te worden geanalyseerd. Hieruit zal een tijdlijn van gebeurtenissen worden opgesteld (zoals bijvoorbeeld wie wanneer was ingelogd op het systeem, wanneer welke programma's zijn opgestart, wanneer welke websites zijn bezocht etc.).
VERIFICATIE	Tijdens de verificatie-fase zal worden geverifieerd of vermeend bewijs ook daadwerkelijk als bewijs te gebruiken is. Data moet terug te redeneren zijn naar de bron en worden gekoppeld aan een verdachte of verdachte activiteit. In deze stap worden de conclusies uit de analyse gevalideerd.
PRESENTATIE	In deze fase zal het rapport worden gedeeld en kunnen bevindingen worden gepresenteerd. Eventuele verklaringen van getuigen zullen in deze fase worden besproken. Indien er inderdaad sprake is van een mogelijk misdrijf, worden bevindingen opgesteld die gebruikt kunnen worden in een strafrechtelijk onderzoek.
ARCHIVERING	In de laatste fase van het forensisch proces zal archivering plaatsvinden. Onderzoeksdata, bewijs, software en hardware kunnen worden opgeslagen. Wanneer inderdaad een strafrechtelijk onderzoek zal plaatsvinden, dan moet de beschikbaarheid van deze informatie voldoen aan de wetgeving.

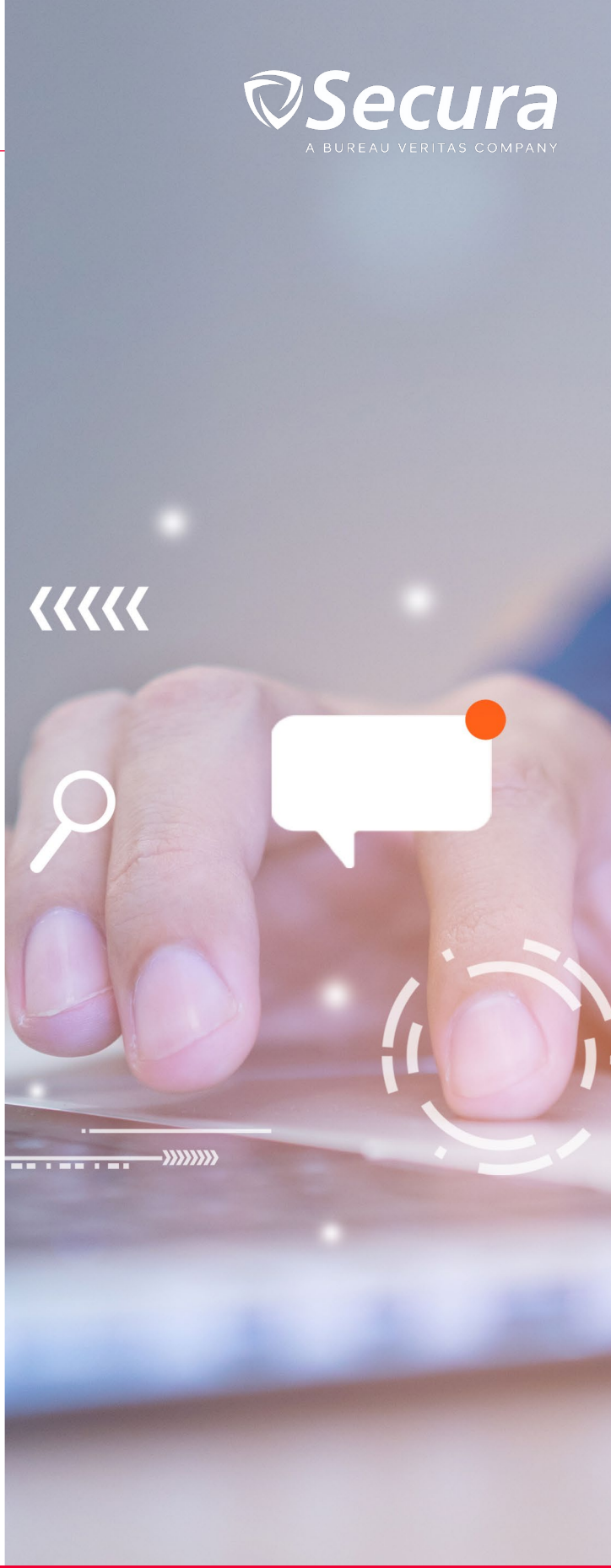
Juridische en vaktechnische kaders

Secura voldoet bij het uitvoeren van al haar opdrachten aan de geldende juridische kaders. Voor forensische onderzoeken zijn daarbij vooral de AVG en de wet computercriminaliteit van belang. Dit betekent onder meer dat geen illegale methodes kunnen worden gebruikt voor het verkrijgen van bewijs, zoals het hacken van online accounts, zonder dat de eigenaar van deze accounts daarvoor toestemming heeft verleend. Het betekent ook dat voor het onderzoek niet-relevante persoonsgegevens zullen worden geanonimiseerd in de rapportages.

Secura heeft een securitymanagementproces dat is gecertificeerd volgens de ISO27001 standaard. Het onderzoekslab van Secura is gecertificeerd volgens de ISO17025 standaard. De kwaliteitsprocessen van Secura zijn gecertificeerd volgens de ISO9001 norm.

Hoe kan Secura helpen?

Heeft u interesse in het uitvoeren van een digitaal forensisch onderzoek of heeft u vragen over wat wij hierin kunnen betekenen voor u? Wij helpen u graag verder! Bel ons op 088 888 3100 of stuur een mail naar: info@secura.com.



Secura
A BUREAU VERITAS COMPANY

Interesse?

Neem contact op:

Volg ons:

+31 88 888 31 00
info@secura.com
secura.com

BUREAU VERITAS 1828
BUREAU VERITAS
Shaping a World of Trust