De opmars van smartphones, cloud computing en sociale media leidt tot een continue toename van allerlei digitale sporen. Deze kunnen worden ingezet in forensisch onderzoek. Tegelijkertijd ontstaan er nieuwe vormen van digitale criminaliteit. Hans Henseler van de Hogeschool Leiden en Magnet Forensics vertelt over de ontwikkelingen, uitdagingen en kansen van e-Discovery.

tekst Lynsey Dubbeld

E-Discovery:

Trends en toekomst van digitale opsporing

In de komende tien jaar gaat er meer gebeuren dan in de afgelopen dertig jaar. Het is een veelgehoorde stelling van ICT-deskundigen. Is dat overdreven? “Ontwikkelingen zoals *artificial intelligence* (AI), *augmented reality* (AR) en het *internet of things* (IoT) gaan ervoor zorgen dat de computer steeds verder doordringt tot in de haarvaten van de samenleving”, zegt *Hans Henseler*, lector aan de Hogeschool Leiden en directeur van het Canadese bedrijf Magnet Forensics, dat software voor digitaal forensisch onderzoek ontwikkelt. “Ongemerkt gaan we overal digitale techniek bij gebruiken en versmelt cyberspace steeds meer met onze dagelijkse werkelijkheid.”

Ontwikkelingen in bijvoorbeeld *personal assistants* en spraakherkenning maken het steeds makkelijker om de computer te bedienen, zonder dat er een toetsen-

bord, muis of *swipe screen* aan te pas komen. “Kunstmatige intelligentie maakt ons werk en onze levens simpeler: een zoekvraag hoef je straks niet eens op een apparaat in te typen, maar kan je simpelweg uitspreken. Dankzij het *internet of things* neemt de beschikbaarheid van slimme systemen in hoog tempo toe. In huis en op kantoor maar ook in de stad.” Henseler noemt als voorbeelden de slimme thermostaat, de slimme afvalbak en 5G-wifi.

De trends in *artifcial intelligence*, *augmented reality* en het *internet of things*, die Henseler in zijn lectorale rede van 2017 uitgebreid beschrijft, hangen nauw samen met de opkomst van sociale media, de smartphone en de cloud – en vooral ook met de combinatie daarvan. “Door sociale media en bijvoorbeeld gezichtsherkenning zijn de data op onze mobiele telefoon nu veel persoonlijker dan pakweg twintig jaar geleden. Daarmee zijn de digitale sporen die we achterlaten ook veranderd en lijkt onze digitale voetafdruk steeds meer op de sporen die forensisch onderzoek traditiegetrouw gebruikt, zoals DNA en vingerafdrukken.”

REVOLUTIONAIRE ONTWIKKELINGEN

Aan het lectoraat Digital Forensics & E-Discovery van de Hogeschool Leiden houdt Henseler zich bezig met onderzoek en onderwijs op het gebied van digitale forensische opsporing. Traditioneel was e-Discovery, dat zich bezighoudt met het ontdekken van verbanden en patronen in grote hoeveelheden elektronische bestanden en e-mails, vooral gericht op het analyseren van documenten om te achterhalen wie wat wist en wanneer. Nu is het ook mogelijk om bijvoorbeeld locaties en interacties te achterhalen. Politie, opsporingsdiensten en bedrijven kunnen de *big data* gebruiken voor onderzoek en opsporing.

‘De versmelting tussen de digitale en fysieke wereld brengt ook nieuwe vormen van criminaliteit met zich mee’

AI, AR en het IoT zijn volgens Henseler onomkeerbare ontwikkelingen die een belangrijke rol spelen in de revolutie in digitaal bewijs die zich de komende jaren zal voortzetten. Tegelijkertijd brengt de versmelting tussen de digitale en fysieke wereld ook nieuwe vormen van criminaliteit mee. “Bij computercriminaliteit dachten we tot voor kort vooral aan hackers. Maar tegenwoordig hoef je helemaal geen ICT-expert te zijn – of zelfs maar te kunnen programmeren – om online een misdaad te kunnen plegen. Oplichters en chanteurs weten mensen te verleiden om geld aan hen over te maken en traditionele criminaliteit zoals identiteitsdiefstal verplaatst zich naar internet. Criminelen zijn altijd op zoek naar de makkelijkste manieren om geld te krijgen, zonder daarbij een groot risico te lopen. Dan is het interessant om ongemerkt vanaf een

Wie is Hans Henseler?

Hans Henseler is sinds 2016 lector aan de Hogeschool Leiden. Daarnaast is hij Director Digital Evidence Review bij het Canadese bedrijf Magnet Forensics, dat software voor digitaal forensisch onderzoek ontwikkelt. Hij is ook lid van het College van het Nederlands Register van Gerechtelijk Deskundigen en voorzitter van de Board of Directors van DFRWS, het platform dat onderzoekers, technologie-ontwikkelaars en opsporingsdiensten samenbrengt om digitaal forensisch onderzoek verder te brengen.

Henseler studeerde Informatica aan de TU Delft en promoveerde in 1992 aan de Universiteit van Maastricht op een onderzoek naar artificiële neurale netwerken. Hij stond vervolgens aan de basis van de afdeling Forensisch Computer Onderzoek van het NFI, waar hij onder andere methoden ontwikkelde om elektronische zakagenda’s van criminelen uit te lezen. Daarna werkte hij bij bedrijven als ZyLAB, PWC en Fox-IT, waar hij zich specialiseerde in e-Discovery.

computer te handelen, zonder dat je je ergens op straat hoeft te vertonen."

OPLOSSINGEN EN TOOLS

Het goede nieuws: tegen het licht van de razendsnelle digitale ontwikkelingen worden ook nieuwe oplossingen en tools ontwikkeld. "Er bestaat steeds betere software om digitale sporen in telefoons op te zoeken. Er zijn ook AI-toepassingen om digitale informatie, zoals e-mails, anoniem en automatisch door te lichten zodat spanningen binnen een organisatie tijdig kunnen worden gedetecteerd", geeft Henseler als voorbeelden.

In het IoT Forensic Lab, gevestigd op de campus van The Hague Security Delta (HSD) in Den Haag, doet Henseler samen met studenten en docenten onderzoek naar onder andere het slim zoeken van informatie in open bronnen. Dat levert inzichten op die ook voor particuliere opsporingsbureaus relevant zijn. Link-analyse met behulp van kunstmatige intelligentie maakt het mogelijk om een sociaal netwerk in kaart te brengen op basis van een breed scala aan data. Daarmee kunnen bovendien visualisaties worden gemaakt die helpen om significante patronen te herkennen en onverwachte verbanden te leggen. Daarnaast kan kunstmatige intelligentie alternatieve scenario's aandragen en daarmee tunnelvisie voorkomen.

Hans Henseler adviseert securitymanagers om goed op de hoogte te zijn van de informatie die de organisatie in huis heeft en de locaties waar de data zich bevindt.

UITDAGINGEN EN KANSEN

Hoewel het onderzoek naar *digital forensics* en e-Discovery in volle gang is – en de markt in toenemende mate met slimme tools komt – kent de dagelijkse praktijk de nodige uitdagingen. Henseler: "Je kunt mensen steeds beter online volgen. Maar dan moet je wel weten welke informatie bruikbaar is, hoe je die verantwoord verzamelt, hoe je links legt met andere bronnen en hoe je grote hoeveelheden data analyseert." Andere uitdagingen hebben te maken met de technische ontwikkelingen in smartphones. Het veiligstellen van informatie uit smartphones is lastig en de beschikbare analysetools zijn niet toepasbaar op alle apps die momenteel in gebruik zijn.

Henseler ziet volop kansen om e-Discovery in te zetten voor bijvoorbeeld *information governance*. "Tools voor e-Discovery kunnen uitstekend helpen bij het lokaliseren van privacygevoelige data in de IT-infrastructuren van bedrijven en overheden. E-specialisten brengen dan het informatielandschap van een organisatie in kaart om persoonsgegevens te lokaliseren." Deze inventarisatie is een eerste stap op weg naar de inrichting van de *information governance*. In essentie komt dat neer op het beheren van de informatiewaardeketen, de keten van informatieprocessen, die ervoor zorgt dat informatie vindbaar, beschikbaar en toegankelijk blijft.

Henseler adviseert securitymanagers om goed op de hoogte te zijn van de informatie die de organisatie in huis heeft en de locaties waar de data zich bevindt. Vervolgens kan worden vastgesteld of dat de geëigende plek is. "Ook informatiebeheer en digitale archivering zijn hierbij belangrijk. Heb je alle informatie nog wel nodig? Hebben we voldoende grip op de levenscyclus van gegevens? Veel bedrijven hadden vroeger *records management*, specialisten die oude papieren ophaalden en bewaarden of vernietigden. Voor digitale informatie hebben we dat soort processen vaak nog niet." Met de komst van de Algemene Verordening Gegevensbescherming (AVG) is dit vraagstuk urgenter dan ooit. "Persoonsgevoelige informatie mag je niet eindeloos opslaan. Bovendien kan het kostbaar zijn om gegevens te bewaren en neemt het risico van datalekken toe. In het huidige digitale tijdperk heeft securitymanagement meer dan ooit te maken met verantwoord informatiebeheer." ■

Lynsey Dubbeld is communicatieadviseur, contentstrateeg, trendanalist en copywriter