Bedrijven zullen steeds vaker zelf onderzoek moeten doen naar frauderende werknemers, omdat het Openbaar Ministerie aan bedrijfsfraude geen of nauwelijks prioriteit geeft. In twee artikelen gaan Marcus Draaisma en Berndt Rif in op het toenemende belang van bewijsbeslag voor de waarheidsvinding.

tekst Marcus Draaisma en Berndt Rif

Bewijsbeslag:

Belangrijk instrument voor waarheidsvinding (1)

Een werknemer wordt verdacht van de schending van zijn of haar geheimhoudingsplicht, diefstal van data of concurrerende activiteiten die bedreigend zijn voor het bedrijf. Laten we het gemakshalve fraude noemen. Om maatregelen te kunnen treffen zal de securitymanager, in afstemming met juristen van de afdeling compliance en integriteit, de verdenking hard moeten maken. Dit vereist zorgvuldig onderzoek om het bewijs van het onbevoegde handelen rond te kunnen krijgen. Vaak begint het onderzoek met het bekijken van camerabeelden, computerbestanden, de aan de werknemer verstrekte laptop of telefoon van de zaak en (externe) servers van het bedrijf.

ZELF ONDERZOEK DOEN

Onderzoek naar data die de werknemer thuis of elders fysiek heeft, al dan niet verstuurd vanaf het werk, of heeft opgeslagen op de privélaptop of telefoon, WhatsApp en sociale media, kan een werkgever niet zomaar (laten) bekijken. Bij de verdachte werknemer thuis of op een andere locatie ligt meestal wel het bewijs van het onrechtmatig handelen van de werknemer of van derden. Met behulp van bewijsbeslag kan dit bewijs worden veiliggesteld en vervolgens worden ingezien. Met de toename van de digitalisering en de mogelijkheid van opslag van grote databestanden, is bewijsbeslag een belangrijk instrument geworden voor de waarheidsvinding.
Bedrijven zullen steeds vaker zelf onderzoek moeten doen naar frauderende werknemers, omdat het Openbaar Ministerie aan bedrijfsfraude geen of nauwelijks prioriteit geeft.

BEWIJSBESLAG EEN STERK WAPEN

De inzet van bewijsbeslag kan het beste worden beschreven aan de hand van praktijkvoorbeelden. Daarbij benoemen we per voorbeeld het probleem dat door bewijsbeslag kan worden opgelost.

Voorbeeld 1: onrechtmatige concurrentie/bedrijfsspionage

Een bedrijfsleider wordt benaderd om voor een concurrent te komen werken, al dan niet met de belofte dat hij een belang in de concurrent krijgt. Aan de bedrijfsleider wordt verzocht belangrijke knowhow en *source*-codes mee te nemen. De bedrijfsleider doet dit in het geheim en slaat alles wat hij kan kopiëren thuis op een harde schijf op. Op enig moment overhandigt hij de gekopieerde informatie aan de concurrent. Dit komt op een gegeven moment uit. Bewijsprobleem: waaruit blijkt dat de bedrijfsleider de data heeft gekopieerd, opgeslagen en aan de concurrent heeft verschaft (en in welke mate)? En wat heeft de concurrent met deze data gedaan?

Voorbeeld 2: niet-ambtelijke omkoping

Een hoofd verkoop van een autoconcern verzorgt voor een inkoper van een groot leasebedrijf een bezoek voor twee naar Monaco en betaalt ook de verbouwing van een badkamer. De inkoper besluit om bij het autoconcern het wagenpark voor 2018 te bestellen en vindt de prijs van de auto's niet zo belangrijk. Bewijsprobleem: waaruit blijkt dat de verkoper de inkoper heeft gefêteerd en de kosten van de verbouwing van diens badkamer heeft betaald en dat dit in relatie stond tot de bestelling van het nieuwe wagenpark?

Bedrijven zullen steeds vaker zelf onderzoek moeten doen naar frauderende werknemers.

Voorbeeld 3: gebruik gegevens van patiënten in strijd met AVG

Zonder toestemming van patiënten en het ziekenhuis heeft een farmaceutisch bedrijf gegevens van 3000 patiënten ontvangen en deze gebruikt om patiënten te benaderen. Bewijsprobleem: van wie heeft het farmaceutisch bedrijf deze patiëntengegevens ontvangen en wie hebben deze vervolgens gebruikt voor andere doeleinden?

In al deze voorbeelden zullen de daders slechts gedeeltelijk sporen hebben nagelaten. Meestal is het zichtbaar dat heel veel bedrijfs- en patiëntendata zijn gekopieerd en op welk tijdstip (behalve als de dader bijvoorbeeld foto's van schermen heeft gemaakt met een eigen camera). Vaak gaat er een tijd overheen voordat het gedupeerde bedrijf bekend is met de dataroof. Dat komt meestal bij toeval aan het licht als de concurrent dan wel het farmaceutisch bedrijf uit voorbeeld 3 met de data aan de haal zijn gegaan; deze data, om zo te zeggen, hebben geheeld. Dan komt het erop aan vast te stellen wie de data heeft gekopieerd en in welke mate daarvan gebruik is gemaakt door on-

Uitvoering van bewijsbeslag moet met militaire precisie gebeuren

bevoegde derden en wie die derden zijn. Een vermoeden van betrokkenheid van (een) werknemer(s) uit het eigen bedrijf ontstaat omdat de betreffende persoon afwijkend en geheimzinnig gedrag vertoont of omdat (een) werknemer(s) ontslag heeft (hebben) genomen en niet verteld wordt wat de nieuwe werkkring wordt. Of door sociale media waar een trouwe klant opeens wordt benaderd door de concurrent met specifieke kennis en deze trouwe klant dit vervolgens doorgeeft aan de directie van het gedupeerde bedrijf.

BEWIJS VEILIGSTELLEN

In een dergelijke situatie zal aannemelijk moeten worden gemaakt dat deze persoon de data heeft gekopi-

→

eerd, heeft bewaard en heeft doorgegeven. Dat bewijs moet worden gezocht in de directe omgeving van deze persoon. Thuis bijvoorbeeld. Of bij de concurrent of farmaceut in de genoemde voorbeelden. Het is daarom belangrijk in een vroeg stadium het bewijs dat vermoedelijk op bepaalde plaatsen aanwezig is, veilig te stellen en zonder dat de betrokken personen hiervan lucht krijgen. Dat kan met behulp van bewijsbeslag op alle gegevensdragers die bij betrokkenen van de spionage aanwezig zijn, waar dan ook. En ook op data die in de cloud zijn opgeslagen.
Wanneer een bewijsbeslag met succes wordt gelegd, betekent dit nog niet dat de data mogen worden ingezien. Daarvoor is aparte toestemming van de rechter nodig op grond van artikel 843a Rv (Wetboek van Burgerlijke Rechtsvordering).

TOESTEMMING VOOR BEWIJSBESLAG

Het mogen leggen van bewijsbeslag gaat met toestemming van de rechter en via een advocaat. Die moet aannemelijk maken dat het bewijsbeslag noodzakelijk en proportioneel is en ook doel zal treffen. Ook dient zo concreet mogelijk te worden aangegeven waarop bewijsbeslag gelegd moet worden. Een verzoek tot beslag op alle data die zich bij een betrokkene bevinden, zou te algemeen en onvoldoende specifiek zijn. Om de rechter goed te informeren, werkt een advocaat nauw samen met professionele bedrijfsrechercheurs, IT-afdelingen en riskmanagers.

Bewijsbeslag is een ingrijpend middel en maakt per definitie inbreuk op iemands persoonlijke levenssfeer en mag geen *shot in the dark* zijn. Een deugdelijk onderbouwd verzoek om bewijsbeslag is essentieel voor een succesvol bewijsbeslag. Voordat men naar de rechter met een verzoek om bewijsbeslag gaat, moet er al onderzocht zijn dat er een gefundeerd vermoeden is dat de betrokken werknemer en betrokken personen (1) onrechtmatig hebben gehandeld (of in strijd met contractuele afspraken), (2) dat onder de in beslag te nemen data waarschijnlijk bewijs is voor dit onrechtmatig handelen en waarschijnlijk aanwezig is op de plekken waar verzocht wordt beslag te leggen en (3) dat dit bewijs niet op een andere manier verkregen kan worden.

Deze fase van waarheidsvinding vraagt nauwe samenwerking tussen bedrijfsrechercheur, advocaat, deurwaarder en IT-deskundige. Allen hebben ervaring met het leggen van bewijsbeslag. Uiteraard wordt een bewijsbeslag in alle vertrouwelijkheid voorbereid. Als men door bedrijfsspionage schade lijdt (wat vaak het geval is) of boetebedingen zijn overtreden, is het verstandig om meteen conservatoir (derden) beslag te leggen op vermogen en bankrekeningen van verdachte werknemers en andere betrokkenen die profiteren van de gestolen data. Daarmee kan ook meteen de oneerlijke concurrentie een gevoelige financiële klap worden gegeven.

HET LEGGEN VAN BEWIJSBESLAG

De uitvoering van een bewijsbeslag moet met militaire precisie gebeuren. Als het beslagverlof van de rechter is verkregen om bewijsbeslag te mogen leggen, komt het aan op goede samenwerking tussen advocaat, deurwaarder, IT-deskundige en de bedrijfsrecherche en/of riskmanager. Met behulp van een gespecialiseerde IT-deskundige legt de deurwaarder beslag op de toegestane plaatsen waar hij gegevensdragers in beslag neemt. Met de IT-deskundige lukt het meestal alle data ter plekke van deze gegevensdragers te kopieren. Daarna worden met behulp van de IT-deskundige als gerechtelijk bewaarder de data veiliggesteld (extern). Of het bewijs dat gezocht wordt tussen deze data te vinden is, weet de beslaglegger nog niet, want daarvoor moet hij aan de rechter inzage vragen (artikel 843a Rv).

De advocaat heeft de leiding over het proces waarvoor bewijsbeslag wordt gelegd. De deurwaarder heeft zijn eigen verantwoordelijkheden. Hij kan tijdens het beslag de data inzien, maar mag daarover geen mededelingen doen aan de advocaat als daarvoor nog geen rechterlijke toestemming is. De IT-deskundige valt onder verantwoordelijkheid van de deurwaarder. Zou de deurwaarder mededelingen doen over hetgeen hij van de beslagen data heeft gezien, dan zullen de beslagenen met succes de rechter kunnen vragen de beslagen op te heffen. Het hoeft geen toelichting dat opnieuw beslag leggen dan kansloos is. ■

In Security Management nummer 12 wordt in deel 2 van dit artikel ingegaan op onder andere de rol van de overige betrokkenen in het proces van bewijsbeslag.

Mr. Marcus Draaisma is advocaat bij Palthe Oberman Advocaten (draaisma@paltheoberman.nl)

Berndt Rif MSc MBA is senior beveiligingsadviseur bij De Nederlandsche Bank (b.rif@dnb.nl)