212

Digitaal forensische expertise met een scherp randje

Bewijsbeslag digitale bescheiden

Bewijsbeslag op digitale bescheiden is een juridische maatregel op basis van een rechterlijk bevel waarmee elektronisch opgeslagen informatie wordt veiliggesteld als bewijsmateriaal in juridische geschillen.

Elektronisch opgeslagen informatie is kwetsbaar en vaak volatiel van aard. Het kan in korte tijd verloren gaan of worden gewijzigd. Zelfs onbedoelde vernietiging is niet ondenkbaar doordat de meeste IT systemen zijn geconfigureerd op een manier waarbij bepaalde (log)bestanden automatisch periodiek worden overschreven. Hierdoor kan belangrijk potentieel bewijsmateriaal verloren gaan. Bewijsbeslag op digitale bescheiden is een juridische maatregel op basis van een rechterlijk bevel. Hierbij wordt elektronisch opgeslagen informatie in beslag genomen en veiliggesteld om te dienen als bewijsmateriaal in een toekomstig of reeds lopend juridisch geschil.

Onder een dergelijk bewijsbeslag vallen onder meer e-mail correspondentie, zakelijke documenten, (digitale) contracten, boekhoudkundige bestanden, sociale media berichten en communicatie, etc. In feite kan iedere vorm van elektronisch opgeslagen informatie onder een bewijsbeslag digitale bescheiden vallen. Zelfs informatie welke in beheer is bij derde partijen zoals financiële instellingen en telecom providers.

Nadat bewijsbeslag is toegekend wordt het uitgevoerd door gerechtelijke instanties (strafrecht) of onder toezicht van een deurwaarder (civiel recht) in samenwerking met een digitaal forensisch deskundige.

Doelstelling van bewijsbeslag op digitale bescheiden

Digitaal bewijsbeslag faciliteert waarheidsvinding door veiligstelling van digitaal bewijsmateriaal. De belangrijkste doelstelling is dat wordt voorkomen dat bewijsmateriaal verloren gaat door overschrijving, vernietiging, wijziging, manipulatie of op andere wijze wordt onttrokken aan de rechtsgang.

Om het risico op vernietiging van bewijsmateriaal te voorkomen dient bewijsbeslag bij voorkeur in een zo vroeg mogelijk stadium plaats te vinden. Het achteraf reconstrueren van data is veelal niet mogelijk.

Aanpak bewijsbeslag op digitale bescheiden

Een bewijsbeslag op digitale bescheiden is strikt gereguleerd middels rechterlijke uitspraak en kan in de regel maar één keer worden uitgevoerd. Meestal zijn er door de rechtbank ook bepaalde restricties opgelegd welke nageleefd dienen te worden.

212 kan het gehele proces van voorbereiding tot uitvoering verzorgen. De aanpak die we hieronder nader toelichten verzekert een systematische en juridisch verantwoorde uitvoering van het bewijsbeslag. De forensische integriteit en bruikbaarheid van het digitale bewijsmateriaal blijven hierdoor gewaarborgd.

Toepassingsgebieden bewijsbeslag digitale bescheiden

Er zijn meerdere toepassingsgebieden voor bewijsbeslag op digitale bescheiden. Een aantal specifieke voorbeelden zijn:

1. ***Civiele juridische procedures.*** Zoals handelsgeschillen, vermeende contractbreuk, diefstal van intellectueel eigendom en schadevorderingen. Bewijsbeslag wordt hier vaak gebruikt om cruciale digitale documenten veilig te stellen.

2. ***Insolventie gerelateerde zaken.*** In geval van faillissement of surseance van betaling kan bewijsbeslag worden ingezet om digitale boekhoudgegevens, facturen en andere financiële bescheiden veilig te stellen. Feitelijk alle bescheiden die inzicht kunnen geven in het beheer van de failliete boedel. Zelfs als deze door derde partijen worden beheerd zoals bijvoorbeeld een accountants- of administratiekantoor.

3. ***Geschillen inzake intellectueel eigendom.*** In geschillen over auteursrechten, patenten, of handelsgeheimen kan bewijsbeslag worden gebruikt om digitale bestanden veilig te stellen die betrekking hebben op het gestolen of betwiste intellectuele eigendom.

4. ***Arbeidsrechtelijke conflicten.*** Denk hierbij aan conflicten tussen werkgevers en werknemers, zoals ontslag op staande voet. Bewijsbeslag op e-mail correspondentie of interne documenten biedt juridische ondersteuning bij het onderbouwen van feiten of juist weerleggen van bepaalde gebeurtenissen en omstandigheden.

5. ***Medische aansprakelijkheid.*** Bijvoorbeeld patiëntendossiers, e-mail correspondentie tussen medisch specialisten en andere relevante digitale gegevens in geval van medische fouten of nalatigheid.

Voorbereiding van het bewijsbeslag

1. ***Analyse van de zaak / kwestie.*** Ieder bewijsbeslag begint met een grondige analyse van de casus om de aard en omvang van de in beslag te nemen digitale bescheiden vast te stellen. Dit omvat ondermeer het identificeren van relevante computer systemen, gegevensdragers en soort elektronisch opgeslagen informatie zoals e-mail (zakelijke) correspondentie, documenten, databases, etc.

2. ***Juridische afstemming.*** Samenspraak met de betreffende juristen is essentieel om ervoor te zorgen dat het bewijsbeslag binnen de wettelijke kaders plaatsvindt. De digitaal forensisch onderzoeker moet niet alleen op de hoogte zijn van de reikwijdte van het gerechtelijk bevel, maar ook van eventuele specifieke vereisten en opgelegde restricties.

   Tevens worden procedures doorgesproken voor het documenteren van de beslaglegging en het waarborgen van de forensische integriteit van de in beslag genomen bescheiden. Dit gebeurt via de chain of custody documentatie. Hierin wordt gedetailleerd vastgelegd welke elektronisch opgeslagen informatie is geacquireerd, op welke wijze en wanneer.

3. ***Technische voorbereiding.*** De onderzoeker bereidt de benodigde hardware en software zoals write blockers voor om het bewijsbeslag uit te voeren. Bewijsbeslagen verschillen onderling sterk qua complexiteit. De acquisitie van de harde schijf van een laptop computer verschilt in alle opzichten met die van een complete storage array van een server infrastructuur.

Uitvoering van het bewijsbeslag

1. ***Acquisitie.*** De digitaal forensisch onderzoeker voert onder supervisie van een deurwaarder het feitelijke bewijsbeslag uit en acquireert de elektronisch opgeslagen informatie conform het vonnis. Dit omvat het feitelijk acquireren van gegevens van elektronische apparaten zoals computers, servers, clouddiensten, mobiele apparaten, etc.

2. ***Forensische integriteit.*** De geacquireerde digitale bescheiden worden onder meer veiliggesteld door toepassing van cryptografische algoritmes om de forensische integriteit te waarborgen. Dit garandeert ook dat de in beslag genomen bescheiden niet tijdens of na de beslaglegging zijn gewijzigd.

3. ***Documentatie en verslaglegging.*** Gedetailleerde documentatie van de beslaglegging is cruciaal. De bij de acquisitie gebruikte methodes en technieken, alsmede de aard, omvang en context van de data zoals tijdstempels en locaties worden nauwkeurig en gedetailleerd gedocumenteerd.

4. ***Opslag en beheer digitale bescheiden.*** Na acquisitie van de in beslag genomen data, wordt deze onder beheer van de deurwaarder gesteld. Een rechterlijk vonnis voor bewijsbeslag digitale bescheiden omvat meestal niet direct ook toestemming voor gebruik of nader onderzoek van deze data. Hiervoor is meestal een separate rechterlijke uitspraak of verlof nodig. Het is dus vaak niet mogelijk om gelijk na het bewijsbeslag een digitaal forensisch onderzoek, eDiscovery of forensisch audio- of e-mail onderzoek op de in beslag genomen data uit te voeren. De in beslag genomen data wordt daarom tot die tijd meestal fysiek bewaard bij de deurwaarder in kwestie.

Wat levert digitaal bewijsbeslag op

Een bewijsbeslag digitale bescheiden levert veiliggesteld bewijsmateriaal op. Hiermee wordt voorkomen dat potentieel bewijsmateriaal wordt overschreven, vernietigd, gemanipuleerd, of onttrokken aan de rechtsgang.

Het faciliteert daarmee waarheidsvinding en waarborgt toegang tot cruciale informatie welke nu of in de toekomst noodzakelijk kan zijn om claims in juridische geschillen te ondersteunen of weerleggen.

Een bewijsbeslag op digitale bescheiden kan de uitkomst van een juridische procedure of geschil doorslaggevend beïnvloeden.

212 DIGITAAL FORENSISCH ONDERZOEK BV

NIEUWE GRACHT 3
2011 NB, HAARLEM
NEDERLAND