Forensische Spurensicherung: Fehler bei internen Untersuchungen können teuer werden

Dieser Artikel befasst sich mit häufigen Fehlern bei internen Untersuchungen. Ziel ist es, diese dem Leser aufzuzeigen, damit sie bei einer eigenen Untersuchung vermieden werden können. Der Autor arbeitet selbst seit 8 Jahren im Bereich der Computerforensik und Ediscovery und hat in diesen Jahren etliche „aufregende" Sicherungen von elektronischen Beweisen miterlebt – sogar bis zur Androhung von körperlicher Gewalt durch den Betriebsrat eines untersuchten Unternehmens.

Interne Untersuchungen & VerSanG

Die meisten Probleme und unerfreulichen Überraschungen lassen sich durch professionelle Planung, Durchführung und Knowhow vermeiden oder zumindest entschärfen. Gerade im Hinblick auf den neuen Referentenentwurf des Verbandssanktionsgesetzes wird die professionelle Durchführung von internen Untersuchungen immer wichtiger. Der vorgeschlagene Strafrahmen liegt, wie beim Kartellrecht, bei bis zu 10% des Jahresumsatzes eines Unternehmens. Eine Minderung ist durch frühzeitige und vollständige Kooperation mit den Behörden möglich. Es kann sich also finanziell erheblich lohnen, gut auf eine interne Untersuchung vorbereitet zu sein.
Die rechtliche Einschätzung soll jedoch nicht Teil dieses Beitrages sein, hierfür sind die Kollegen in Anwaltskanzleien zuständig.

Häufige Fehler bei internen Untersuchungen

1. Zu spät anfangen
Die Dauer einer Datensicherung ist nicht zu unterschätzen. Besonders bei Archivdaten können Wochen bis Monate vergehen, bis die Daten eines einzelnen Mitarbeiters kopiert sind. Dasselbe gilt bei ausgeprägter Homeoffice-Kultur oder mehreren Standorten. Hinzu kommt zusätzliche Zeit für Aufbereitung, Durchsuchung und Sichtung. Daher ist es für Unternehmen vorteilhaft, die Verfügbarkeit aller Datenquellen zu kennen. Die Unternehmens-IT und ein Computer-Forensik-Anbieter sollten frühzeitig involviert werden, um im Verdachtsfall schnell und umfassend reagieren zu können.

2. Unzureichend Daten sichern
Am Anfang einer Untersuchung weiß man selten genau, wann und bei wem ein Compliance-Verstoß vorliegt – bestenfalls gibt es Hinweise. Daher gilt zunächst: Sichern, sichern, sichern. Denn vielleicht werden bestimmte Verdächtige durch neue Erkenntnisse erst später in die Untersuchung einbezogen. Wichtige Indizien auf deren Geräten könnten dann bereits gelöscht worden sein.
Will man aufgrund mangelnder Beweislast einige Daten zunächst nicht in die Untersuchung mit einbeziehen, können diese – verschlüsselt und in Beweismitteltüten eingeschweißt – an einem sicheren Ort im Unternehmen verwahrt werden. Speicherplatz kostet heute wenig – Daten zu verlieren kann hingegen sehr teuer werden.

3. Daten kopieren
Eine forensische Sicherung unterscheidet sich von einer gewöhnlichen Kopie durch die zusätzliche Sicherung aller Metadaten, dem elektronischen Fingerabdruck einer Datei. Wird eine Datei beispielsweise kopiert und daraufhin erneut abgespeichert, trägt die Kopie ein anderes Erstelldatum. Derartige elektronische Informationen können aber ein wichtiges Beweismittel sein, deren Veränderung nicht nur den Beweis verändert, sondern zudem die Validität aller anderen Meta-Daten (Autor, zuletzt geöffnet, gedruckt, versandt, kopiert) in Frage stellt.
Bei großen Datenmengen, Laptop- und Handysicherungen ist es sinnvoll, einen IT-Forensiker hinzuzuziehen, der bei der Identifizierung und Sammlung relevanter Daten hilft und als Sachverständiger vor Gericht auftreten kann.

4. Gelöschte Daten übersehen
Besonderes Augenmerk gilt mutwillig oder versehentlich gelöschten Daten. Denn wer den Papierkorb leert, gibt lediglich den belegten Speicherplatz für ein erneutes Überschreiben frei. Die frei gegebenen Bereiche und damit auch die darin enthaltenen Daten werden jedoch mit den richtigen forensischen Tools – hier seien EnCase und FTK Imager als zwei der gängigsten genannt – wiederherstellbar. Mit dem erhaltenen „Full Image" kann so jederzeit auf den IST-Zustand zum Zeitpunkt der Datensammlung zurückgegriffen werden.

5. Suchen in Outlook
Die Suchfunktion von Outlook oder anderen E-Mail-Programmen zum Auffinden bestimmter Informationen liefert äußerst unvollständige Ergebnisse. So zeigt Outlook nur eine begrenzte Anzahl von Ergebnissen an und auch nur die Daten, die aktuell auf dem System verfügbar sind und ignoriert Dokumente, die nicht identifizierbar sind, z.B. vom System bereits archivierte Nachrichten, gescannte Anhänge oder Bilder.

Fazit

Forensische Datensicherungen sind komplex, zeitaufwändig und benötigen erhebliches Wissen, um erfolgreich durchgeführt werden zu können. Es geht nicht nur um den Inhalt der Daten, sondern auch um eine gerichtsfeste Beweismittelsicherung. Dazu gehören Metadaten und eine lückenlose Beweismittelkette, erstellt durch ausgebildete Experten. Je früher mit der professionellen Planung begonnen wird, desto weniger Fehler geschehen. Und desto besser können sich Unternehmen und Kanzleien auf die Ergebnisse der Untersuchung vorbereiten.

Hinweis zum Autor:

Daniel Heinrichs
arbeitet bei KLDiscovery im Bereich der Computerforensik und Ediscovery und betreut in seiner Rolle als Business Development Manager Unternehmen und Kanzleien in Deutschland, Österreich und der Schweiz. Herr Heinrichs hat einen Abschluss als Master in Business Management.