

Aufklärung durch „IT-Forensic“

Sebastian Erdmann,

General Manager, Corporate Integrity Solutions GmbH, erdmann@corporate-integrity.de

Ob Betrug, Unterschlagung, Bilanzfälschung oder Diebstahl von Betriebs- und Geschäftsgeheimnissen im Unternehmen: bei Unregelmäßigkeiten und Wirtschaftsdelikten ist es wichtig, schnell und entschlossen zu handeln. Gerade bei Wirtschaftskriminalität kommt es darauf an, alle Maßnahmen zur Aufklärung, dem Krisenmanagement und der juristischen Betreuung gezielt aufeinander abzustimmen und dafür zu sorgen, dass alle Beweise, Unterlagen und Daten gesichert und gerichtsverwertbar dokumentiert werden.

I. Aufklärung

Viele Unternehmen schützen sich vor Computerangriffen und wirtschaftskriminellen Handlungen von außen. Täter sitzen aber häufig auch im Unternehmen selber. Leider werden bisher zu wenig präventive Maßnahmen getroffen, um Wirtschaftskriminalität zu verhindern und dadurch Schäden zu vermeiden. Teilweise argumentieren Unternehmen, man könne sowieso nicht alles verhindern. Daher wartet man, bis ein Schadensfall eintritt, um erst dann Geld in die Aufklärung zu investieren. Dies kann Unternehmen teuer zu stehen kommen. Wenn Informationen erst mal das Unternehmen verlassen haben, ist es sehr schwer, den Schaden wieder zu beheben.

Eine forensische Untersuchung kann nur dann erfolgreich verlaufen, wenn Beweise und Spuren noch nachvollziehbar sind. Daher ist es erforderlich, im Vorfeld entsprechende Datensicherungen und Protokolle zu erstellen, um Beweise für eine Straftat sichern zu können. Oft wird Wirtschaftskriminalität nicht sofort erkannt. Somit kann eine Untersuchung teilweise erst Wochen, Monate oder sogar Jahre später stattfinden. Sind dann die Beweise bereits vernichtet oder im Falle von elektronischen Daten be-

reits gelöscht und überschrieben, ist es unter Umständen nicht mehr möglich, die Straftat nachzuweisen.

II. Fallbeispiel

Ein leitender Angestellter eines mittelständischen Unternehmens kündigt seinen Arbeitsvertrag und wechselt zur Konkurrenz. Einige Tage später verlassen weitere Mitarbeiter das Unternehmen. Einer der größten Kunden kündigt an, künftig ebenfalls mit der Konkurrenz zusammen zu arbeiten.

Liegt in diesem Fall unlauterer Wettbewerb vor und haben die Mitarbeiter Betriebs- und Geschäftsgeheimnisse an die Konkurrenz verraten? Wie hoch ist der entstandene Schaden für das betroffene Unternehmen? Und hätte das verhindert werden können?

Rechtliche Vorgaben

Bei einem wirksamen Verbot der privaten Nutzung der elektronischen Kommunikationssysteme eines Unternehmens finden weder das Bundesdatenschutzgesetz (BDSG) noch das Telekommunikationsgesetz (TKG) auf die in den unternehmenseigenen IT-Systemen gespeicherten Kommunikationsdaten Anwendung. Die elektronische Kommunikation innerhalb des Unternehmens wird dann nämlich als geschäftlich betrachtet. Auf diese

Daten und Informationen hat der Arbeitgeber grundsätzlich ein weitgehendes Zugriffsrecht. Lediglich eine Kontrolle, die einer so genannten Vollüberwachung nahe kommt, würde gegen das allgemeine Persönlichkeitsrecht der Arbeitnehmer verstoßen und wäre unzulässig.

Wird hingegen den Arbeitnehmern (Dritten) die private Nutzung der elektronischen Kommunikationssysteme erlaubt oder nicht ausdrücklich untersagt, so muss der Arbeitgeber die Beschränkungen des BDSG bei personenbezogenen Daten auch bei der Kommunikation der Arbeitnehmer anfallenden Daten beachten. Personenbezogene Daten darf der Arbeitgeber nur dann erheben, verarbeiten oder nutzen, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene zuvor eingewilligt hat. Das BDSG erlaubt die Nutzung der Daten unter anderem dann, wenn der Arbeitgeber ein den Interessen des Arbeitnehmers überwiegendes Interesse an der Nutzung hat. Dies kann unter Umständen bei einem konkreten Verdacht auf Wirtschaftskriminalität der Fall sein.

Ist die private Nutzung der elektronischen Telekommunikationssysteme erlaubt, ist der Arbeitgeber zudem Dienstanbieter von Telekommunikationsleistungen im Sinne des TKG und hat daher das Fernmeldegeheimnis zu wahren. Deshalb be-

nötigt man in diesem Fall für eine rechtmäßige Untersuchung der auf den unternehmenseigenen IT-Systemen gespeicherten Kommunikationsdaten neben dem berechtigten Interesse des Arbeitgebers und einem konkreten Anfangsverdacht zudem noch eine formelle Rechtfertigung oder einen Entschuldigungsgrund.

Ablauf der Untersuchung

Die „IT-Forensic“ analysiert verdächtige Vorfälle in IT-Systemen und wertet digitale Spuren und Massendaten aus. Die erste Maßnahme besteht darin, die IT-Umgebung zu erheben und zu identifizieren, auf welche Daten zugegriffen werden kann. Im Anschluss werden dann unverzüglich die relevanten Daten forensisch gesichert, d.h. es wird eine exakte Kopie der zu untersuchenden Datenträger erstellt, um Veränderungen an den Daten zu verhindern und die Gerichtsverwertbarkeit sicherzustellen.

Da es bei Diebstahl von Betriebs- und Geschäftsgeheimnissen sowie bei unlauterem Wettbewerb hauptsächlich um eine Auswertung von Kommunikationsdaten (E-Mails, Telefongespräche, SMS, etc.) geht, sollte die Analyse neben Rechnern, PDAs und Handys der Zielpersonen, auch die Backups der E-Mails und Telefonprotokolle umfassen.

Mit Hilfe geeigneter forensischer Software können auch große Datenmengen schnell nach Schlagwörtern und Beziehungen zueinander durchsucht werden. Vorteil einer solchen Analyse ist, dass neben den normalen Dateien und E-Mails auch gelöschte und teilweise überschriebene Daten mit untersucht werden können.

Untersuchungsergebnisse

Bei der IT-forensischen Untersuchung des Fallbeispiels wurden auf dem Computer des Mitarbeiters gelöschte Anschreiben wiederhergestellt, in denen er Mitarbeiter da-

zu aufforderte ebenfalls den Arbeitgeber zu wechseln. In diversen E-Mails mit dem Konkurrenzunternehmen vereinbarte der Mitarbeiter die Konditionen, unter denen ein Wechsel stattfinden sollte. Dazu gehörte auch die Übernahme von diversen Kunden.

Durch Betriebsvereinbarungen bzw. in den Arbeitsverträgen war die Nutzung des Internets und E-Mail für private Zwecke untersagt. Durch diese unternehmensinternen Regelungen war eine IT-forensische Untersuchung möglich, so dass die Beweise für einen unlauteren Wettbewerb und den Verrat von Betriebs- und Geschäftsgeheimnissen gesammelt werden konnten.

III. Fazit

Unternehmen sind daher gut beraten, bereits präventive Maßnahmen zu treffen, um Schäden durch wirtschaftskriminelle Delikte abzuwenden. Tritt dennoch ein Notfall ein, ist der finanzielle Schaden deutlich geringer. Zudem wird die Aufklärung des Sachverhalts erheblich erleichtert. Führungskräfte sollten sich die folgenden Fragen stellen, um zu erkennen, ob in ihrem Unternehmen Präventionsmaßnahmen ergriffen wurden:

- Kann ein Mitarbeiter der Forschungs- und Entwicklungsabteilung (oder anderer sensibler Abteilungen) mit einem USB-Speicherstick oder per E-Mail Geschäftsgeheimnisse aus dem Unternehmen heraustragen?
- Ist sichergestellt, dass meine Kundendatei nicht kopiert wird und das Unternehmen verlässt?
- Werden E-Mails regelmäßig gesichert und können gelöschte E-Mails wieder hergestellt werden?
- Werden Laptops in Ihrem Unternehmen verschlüsselt?

- Dürfen Sie im Verdachtsfall auf Mitarbeiter - E-Mails zugreifen?
- Werden WLAN Anschlüsse geblockt?
- Ist die Benutzung von USB Geräten limitiert?

Damit diese Fragen nicht unbeantwortet bleiben, sollten im Vorfeld bereits die technischen und juristischen Weichen gestellt werden. Dies dient nicht nur der besseren Aufklärung im Ernstfall, sondern auch zur Abschreckung durch Kontrollen.