© iStockphoto

*Warum war B. so gut über Dinge informiert, die er eigentlich nicht hätte wissen dürfen?*

# Der Spion, der von innen kam

**Dr. iur. Michael Alkalay, Leiter Wirtschaftskriminalistik und**
**Prof. Dr. Maurizio Tuccillo, Leiter IT-Forensics, Hochschule Luzern Wirtschaft**

**Vor lauter Fixierung auf Angriffe von aussen wird häufig die Gefahr von «innen» unterschätzt. Dabei haben Manipulationen von «inneren Feinden» in letzter Zeit beträchtliche Schäden angerichtet. Ein Fallbeispiel.**

Angriffe von Hackern, Sabotageaktionen, Daten- und Identitätsdiebstahl bedrohen das Zusammenleben im Cyberspace. Als Normalverbraucher im Internet ist man inzwischen hauptsächlich auf den äusseren Feind fixiert. Die «inneren Feinde» haben aber in letzter Zeit – zumindest in der Schweiz und in Liechtenstein – die grössten Schäden materieller, immaterieller und politischer Art angerichtet. Motivation ist nicht zwingend die Bereicherung, sondern wie die nachstehende wahre Geschichte zeigt, auch der alltägliche «Wahnsinn der Bürointrige»...

**Bestens informiert**

Die Sachlage schien klar zu sein: Geschäftsleitungsmitglied B. war offenbar in der Lage, den Mailverkehr der andern wichtigen Personen im Unternehmen mitzulesen. Nur so liess sich erklären, weshalb er immer bestens informiert war – auch und gerade über Angelegenheiten, die er eigentlich nicht wissen durfte. Damit verschaffte er sich persönliche Vorteile und begann gegen andere zu intrigieren. Bloss, wie bewerkstelligte er diese Überwachung?

Der Verwaltungsrat beginnt, B. genauer auf die Finger zu schauen: Weitere Unregelmässigkeiten kommen ans Licht: Unterlagen verschwinden, Passwörter werden unmotiviert geändert, Datensicherungen lassen sich nicht mehr zurückspielen – und immer zum Vorteil von B. Alles nur Zufälle? Als die Situation zu eskalieren droht, wird B. mit sofortiger Wirkung freigestellt. Doch wenige Tage später fehlen erneut wichtige Unternehmensdaten und eine Wiederherstellung ab den Datensicherungen ist wieder nicht möglich. Der Verdacht einer begangenen Straftat materialisiert sich. Aber wie lautet das Tatvorgehen und wer ist nachweislich der Täter? Hat B. noch Zugriff auf das Computer-Netzwerk? Hat er Helfer innerhalb der Firma? Oder hat er gar sein Ausscheiden von langer Hand geplant und bösartige Automatismen eingebaut?

**Wem kann man noch trauen?**

Die Geschäftsleitung ist hier in der Zwickmühle. Kann sie ihre internen Spezialisten mit der Aufklärung der Vorgänge betrauen? Ist hier sogar ein Komplott ausgeheckt worden? Reichen die Verdachtsmomente für eine Strafklage? Und lohnt sich der Gang vor die Justiz überhaupt? In solchen Fällen wenden sich Unternehmen zuerst an einen Rechtsanwalt, der aufgrund der vorliegenden Sachlage nicht immer den gewünschten Ratschlag erteilen kann. Um rechtliche Aussagen machen zu können, benötigt er den IT-Forensiker.

Dessen Aufgabe ist es, die Vorgänge allein anhand der zurückgelassenen Spuren nachzuzeichnen und zu belegen. Im Bereich der digitalen Daten nicht immer ein leichtes Unterfangen, denn die anfänglich zahlreichen Spuren sind flüchtig, oftmals nur schwer zu deuten und selten zweifelsfrei einer handelnden Person zuzuordnen. Umso wichtiger ist es, dass der IT-Forensiker möglichst zeitnah am Geschehen seine Untersuchungen vornehmen kann, dass er eine möglichst vollständige Datenlage erheben kann und dass die Spurenlage nicht durch die eigenen Nachforschungen oder zwischenzeitlichen Rettungsversuche verschleiert wird.

**Auf Spurensuche**

Die Arbeit des IT-Forensikers beginnt im Allgemeinen mit einer Analyse der IT-Umgebung und dem Ermitteln potenzieller Schwachstellen – technische wie organisatorische. Dies dient insbesondere dazu, plausible Hypothesen über den Hergang des Geschehens aufzustellen. Denn nicht immer erweisen sich die offensichtlichsten Vermutungen auch als die richtigen. Gibt es überhaupt einen Fernzugriff auf das Computernetzwerk, welcher zu den untersuchten Zwecken missbraucht worden sein könnte? Für wen ist dieser Zugriff normalerweise eingerichtet und von wem ist er tatsächlich genutzt worden? Erst wenn sich der IT-Forensiker ein genügend präzises Bild über die Funktionsweise des Systems gemacht hat, wird er in der Lage sein, Belege für oder gegen die aufgestellten Hypothesen zu finden. Das Erheben der Daten ist in den meisten Fällen reine Routinearbeit. Mit der nötigen technischen Ausrüstung gelingt es auch, die Spurenlage unverändert zu konservieren, oftmals die vermeintlich gelöschten Daten wieder herzustellen und – etwas aufwändiger zwar – verschlüsselte Inhalte lesbar zu machen. Doch gilt es aus Hunderten von Puzzleteilchen ein möglichst lückenloses Gesamtbild zu zeichnen. Der Forensiker sucht nach

Korrelationen, Auffälligkeiten oder Unstimmigkeiten. Ein Beispiel: Wie verschiedene Protokollierungen zeigen, verfügte B. zwar über Berechtigungen für einen Fernzugriff, er machte davon aber schon seit längerer Zeit keinen Gebrauch mehr. Hingegen meldete er sich häufig bereits um 6.30 Uhr interaktiv am System an, obschon er nie vor 7.15 Uhr mit seinem Badge das Tor zur Tiefgarage öffnete. Das erste Telefongespräch tätigte er jeweils gegen 7.30 Uhr. War also doch ein interner Helfer im Spiel?
In der Tat: Die Spur der Logins führt an den Arbeitsplatz eines einfachen Mitarbeiters, der mit den Anmeldedaten von B. ausgestattet, die Mailboxen verschiedener Personen in dessen Auftrag ausspioniert und Dokumente zum Verschwinden gebracht hat. Die Systemadministration ist damit entlastet. Zumindest teilweise, denn B. verfügte offenbar über unnötig weitreichende Berechtigungen, die er zudem problemlos an eine andere Person weitergeben konnte.

Und was ist mit den verschwundenen Unternehmensdaten und den fehlenden Datensicherungen? Die Abklärungen zeigen, dass B. die vermissten Daten lokal auf seinem Laptop aufbewahrte anstatt auf dem zentralen Fileserver. Das Datensicherungskonzept berücksichtigte den Laptop von B. überhaupt nicht. Mit dem Verlust des Laptops waren auch die Daten weg. Auch das gibt schlechte Noten für die Systemadministration.

**Nicht auf alle Fragen eine Antwort**

Mit dem Abschlussbericht wird es dem IT-Forensiker in den meisten Fällen gelungen sein, auf einige Fragen Antworten zu liefern. Der Justitiar der Firma wird eine Strafanzeige oder bei einem Schadenfall eine Zivilklage formulieren können. Doch die internen Prozesse müssen danach überprüft werden, und bei der Rekrutierung des neuen Kaders wird die Geschäftsleitung neben Fachwissen und Management Skills vermehrt auf Charakter und Integrität achten müssen.