DuD
Datenschutz und Datensicherheit

Beweissicherung bei Computer-Delikten

Dirk Fox

Delikte unter Verwendung von Computern haben in den vergangenen Jahren erheblich zugenommen. Das ist zum Einen zweifellos auf die voranschreitende Durchdringung aller Lebensbereiche mit moderner Informations- und Kommunikationstechnik zurückzuführen. Zum Anderen eröffnen Computer Kriminellen auch gänzlich neue Möglichkeiten, sowohl hinsichtlich der Zielsetzung als auch bei der Tatdurchführung.

Spielen Computersysteme eine Rolle, so sind an die Beweissicherung und die Analyse des Vorfalls oder Tathergangs deutlich andere Anforderungen zu stellen als bei der „klassischen" Forensik. Werden bei der Beweissicherung Fehler gemacht, sind Computer oft nicht nur die einzigen, sondern auch schnell ahnungslose Zeugen. Vor allem bei internen Untersuchungen aufgrund eines Anfangsverdachts werden in betroffenen Unternehmen meist zahlreiche Spuren unwiederbringlich vernichtet. Zwar ist nachvollziehbar, dass ein Verdacht zunächst durch weitere Indizien erhärtet oder ausgeräumt werden soll. Handelt es sich aber bei dem untersuchten Vorfall um einen potentiell großen Schaden oder eine Straftat, kann eine dilettantische Voruntersuchung, bei der Teile der Beweislage vernichtet werden, erhebliche negative Folgen haben.

Analyse

Bei der Vorfallsanalyse an Computersystemen sind vor allem zwei Dinge wesentlich: Die Zuordnung eines Ereignisses zu einer eindeutig bestimmbaren Person und einem eindeutig bestimmbaren Zeitpunkt.

Die Zuordnung eines technischen Vorgangs zu einer bestimmten Person setzt zunächst voraus, dass es eine geeignete Eingrenzung von Zugriffsberechtigungen gibt, durch die einerseits die Anzahl der Verursacher eines protokollierten Vorgangs eingegrenzt und andererseits wirksam verhindert wird, dass ein Verursacher die Berechtigung besitzt, seine im System hinterlassenen Spuren selbst zu löschen oder sie so zu verändern, dass der Vorgang einer anderen Person zugeordnet wird. Ein gutes Berechtigungskonzept orientiert sich daher am „Need-to-Know"-Prinzip: Jeder erhält nur die Berechtigungen, die er tatsächlich benötigt. Jede Zugriffsberechtigung wird darin Person zugeordnet, die sich wiederum vor der Benutzung des Systems durch die Eingabe eines individuellen Passwortes ausweisen müssen. Die Beweissicherung muss daher die im Vorfallszeitraum bestehenden Berechtigungen und die vergebenen Passworte umfassen.

In der Praxis beginnen die Fehler hier häufig lange vor einem Vorfall: Die Berechtigungen sind nicht sinnvoll begrenzt, Zugriffspassworte werden gemeinsam verwendet, zu einfach gewählt, an Kollegen weitergegeben oder aufgeschrieben. Damit ist die Beweiskraft einer solchen Zuordnung begrenzt, sofern sie nicht durch zusätzliche Indizien erhärtet werden kann.

Die Möglichkeit der Zuordnung eines technischen Vorgangs zu einem bestimmten Zeitpunkt hängt ebenfalls von mehreren Voraussetzungen ab. Die beiden wichtigsten: Das zu untersuchende System verfügt über eine genaue und vom Nutzer nicht manipulierbare Systemzeit, und es gibt eine Protokollierung, die von der verdächtigten Person nicht manipuliert werden kann. In vielen Systemen müssen solche Protokollierungen aktiviert und geeignet konfiguriert werden, damit zum Zeitpunkt der Beweissicherung aussagekräftige Protokolleinträge vorliegen.

Die meisten solcher Protokolleinträge unterliegen aus Gründen des Datenschutzes definierten Löschfristen. Daher ist es wesentlich, beim Vorliegen eines Anfangsverdachts die betroffenen Protokolldateien bis zur Klärung zu sichern. Besonders aussagekräftig sind bei den meisten Vorfällen die Informationen, die bei den automatisch erzeugten Zeiteinträgen des Rechnersystems abgelegt werden, wie der Zeitpunkt der Erzeugung und der letzten Änderung eines Dokuments. Aber Vorsicht: Diese „Zeitstempel" können mit geeigneten Tools leicht modifiziert werden; auch mit einer kurzzeitigen Änderung der Systemzeit lassen sich diese Zeitangaben verfälschen, sofern der Benutzer dazu die Berechtigung besitzt. Auch hier hilft Vorsorge: Benutzer sollten nicht die Berechtigung besitzen, Programme auf dem von ihnen genutzten Rechner zu installieren.

In jedem System gibt es außerdem zahlreiche versteckte Protokollierungen, die den meisten Nutzern nicht bekannt sind und mit deren Hilfe Manipulationen von Zeiteinträgen aufgedeckt werden können. Voraussetzung: Der Computer wird nach dem Vorgang nicht einfach weiter genutzt, und es wird auch keine Voruntersuchung direkt am betroffenen System durchgeführt. Denn schon beim Herunterfahren und erneuten Starten des Computers werden zahlreiche wichtige Protokolleinträge unrettbar überschrieben.

Vorgehen

Daher beginnt eine professionelle Beweissicherung mit der Erzeugung zweier Bitidentischer Kopien des Originalsystems – nicht durch einfaches Kopieren der Festplatten, denn dabei werden viele Daten nicht dupliziert. Die anschließende Untersuchung und Beweissicherung erfolgt niemals auf dem Originalsystem, sondern auf einer der beiden System-Kopien mit geeigneten Analyseprogrammen.

Die einzelnen Schritte der Analyse werden dabei akribisch und idealer Weise in Anwesenheit eines Zeugen protokolliert. Zusammen mit der erzeugten zweiten Kopie erlaubt diese Vorgehensweise später, die Beweissicherung zu reproduzieren – ein sehr wichtiger Aspekt, sollte die Korrektheit der gefundenen Spuren in Zweifel gezogen werden. Dabei müssen auch Abweichungen der Systemzeit von einer Referenzzeit festgehalten werden, um später Protokolleinträge von unterschiedlichen Systemen, beispielsweise die Zeitpunkte der Versendung eines Dokuments und dessen Empfang, miteinander in Beziehung setzen zu können.

Aber nicht nur das Vorgehen bei der technischen Analyse eines Systems sollte dokumentiert werden, sondern der gesamte Umgang mit dem betroffenen System: Wer hatte nach Bekanntwerden des Verdachts Zugang zum System? Um Zweifel an der Beweiskraft der Untersuchungsergebnisse auszuräumen, sollte jeder Kontakt mit dem Originalsystem von einer weiteren Person bezeugt und dies schriftlich dokumentiert werden (wer, wo, was, wann).

Vor Gericht hilft es, wenn eine unternehmensinterne Untersuchung nicht von einem eigenen Mitarbeiter, sondern von einem unabhängigen Dritten durchgeführt wurde, der als sachkundiger Zeuge die Vorgehensweise und die Schlüssigkeit der Beweiskette überzeugend bestätigen kann.