Daten vor Gericht

Um tatsächliche oder nur angenommene Straftaten im digitalen Bereich eines Unternehmens aufzuklären, muss auch der Admin kräftig mithelfen. Doch was muss er speichern und rausgeben? Christian Solmecke

© Maksim Kabakou, 123RF

In Unternehmen finden mittlerweile die meisten Straftaten oder Pflichtverletzungen einen Niederschlag in digitaler Form. Da stellt sich sogleich die Frage, welche Daten ein Unternehmen speichern darf und muss, um diese später eventuell als Beweis in ein Verfahren einzubringen. Die Administratoren des Unternehmens dürfte zudem interessieren, inwieweit sie dazu verpflichtet sind, am konkreten Übermitteln der Beweise mitzuwirken.

Geschäftsunterlagen sichern

Das Gesetz verpflichtet Unternehmer dazu, bestimmte Geschäftsunterlagen aufzubewahren. Das Handels- und Steuerrecht hält dazu an, manche Geschäftsdaten bis zu zehn Jahre zu speichern. In anderen Bereichen finden sich ähnliche Vorschriften, die aber in der Praxis weniger ins Gewicht fallen.

Die steuerrechtliche Aufbewahrungspflicht regelt überwiegend der Paragraf 147 der Abgabenordnung. Diese Pflicht erstreckt sich unter anderem auf Inventare, Jahresabschlüsse, Bilanzen und den Austausch von Handels- und Geschäftsbriefen – im Grunde auf alle Unterlagen, die beim Besteuern eine Bedeutung besitzen. Für bestimmte Berufe oder Tätigkeiten schließt das noch weitere Unterlagen ein. Beispielsweise regelt das Handelsgesetzbuch, dass Bewachungsbetriebe Auftragsbücher führen müssen.

In vielen Unternehmen besteht die Schwierigkeit nun darin, ihre Unterlagen in die richtige Kategorie einzuordnen. Ein Geschäftsbrief liegt zum Beispiel nicht vor, wenn der Austausch mit einem Geschäftspartner letztlich nicht in einem Geschäftsabschluss mündet. Werbeprospekte haben ebenfalls keinen Geschäftsbriefcharakter.

Unter Geschäftsbriefen sind selbstverständlich auch Mails zu verstehen. Die Anhänge der E-Mails müssen Unternehmen aber nur dann ebenfalls speichern, wenn die einzelne Nachricht für sich genommen unverständlich bleibt oder nur unzureichende Informationen enthält.

Zu Sicherheitszwecken und auch, um das Surfverhalten der Arbeitnehmer zu überwachen, speichern viele Unternehmen die besuchten URLs ihrer Arbeitnehmer und die dabei verwendeten IP-Adressen. Sie nutzen dazu so genannte Webtracking -Tools. Das Speichern dieser Daten kann helfen, denn nicht selten lassen sich Softwareprobleme oder ein Datenmissbrauch beziehungsweise -verlust auf ein rechtswidriges Verhalten der Arbeitnehmer zurückführen. Der Arbeitgeber haftet schließlich nach §130 des Ordnungswidrigkeitengesetzes, wenn er seine Mitarbeiter nicht hinreichend überwacht und so Rechtsverstöße ermöglicht.

Speichern von URLs und IP-Adressen

Eine Antwort auf die Frage, ob ein Unternehmen URLs und IP-Adressen speichern darf, geben die datenschutzrechtlichen Vorschriften im Telekommunikationsgesetz (TKG), im Telemediengesetz (TMG) und im Bundesdatenschutzgesetz (BDSG). Erlaubt es der Arbeitgeber seinen Arbeitnehmern, den Firmencomputer privat zu nutzen, qualifiziert das Gesetz in der Regel den Arbeitgeber als Telekommunikationsanbieter. Er darf somit grundsätzlich Daten speichern, die ihm dabei helfen, Störungen oder Fehler im System zu erkennen, einzugrenzen oder zu beseitigen.

Das schließt aber nicht das Verfolgen von URLs und IP-Adressen ein. Der Grund: Das Speichern dieser Daten hilft nicht Fehler und Störungen zu unterbinden oder vorzeitig zu erkennen, da es den Zugriff zu keinem Zeitpunkt verhindert. Arbeitgeber müssen hier vorsichtig sein: Das nur präventive Speichern von IP-Adressen und URLs ist nicht erlaubt,

das TKG deckt es auch nicht. Das gleiche Prinzip gilt im TMG. Auch hier muss zum Zeitpunkt des Speicherns ein konkreter Tatverdacht bestehen, der es zulässig macht, Daten aufzubewahren.

Lediglich das BDSG erlaubt präventives Speichern. Paragraf 32 sieht vor, dass ein Unternehmen personenbezogene Daten, zu denen auch die IP-Adressen zählen, unter Umständen vorhalten darf. Die sind gegeben, wenn die Daten für eine Entscheidung notwendig sind, die ein Beschäftigungsverhältnis begründet, umsetzt oder beendet. Wer zum Beispiel während der Arbeit das Internet vertragswidrig nutzt, verletzt seine arbeitsvertraglichen Pflichten. Das präventive Speichern der Daten ist hier also für das Beschäftigungsverhältnis relevant.

Der Speichernde muss jedoch den Grundsatz der Datensparsamkeit und Datenvermeidung beachten. Er darf immer nur die erforderlichen Daten speichern. Ein Unternehmen muss generell zwischen dem objektiven Interesse des Arbeitgebers, das sich auf sein Recht am eingerichteten und ausgeübten Gewerbebetrieb erstreckt, und dem Persönlichkeitsrecht des Arbeitnehmers abwägen.

Das Grundrecht auf informationelle Selbstbestimmung spielt dabei eine große Rolle als eine Ausprägung des allgemeinen Persönlichkeitsrechts. Personenbezogene Daten darf ein Unternehmen nach §32 BDSG auch erheben, verarbeiten oder nutzen, wenn ein konkreter Straftatverdacht vorliegt.

Das Speichern personenbezogener Daten ist nach §4 BDSG immer nur dann zulässig, wenn der Betroffene eingewilligt hat. Dafür muss er sich im Klaren darüber sein, welche konkreten Daten das Unternehmen zu welchem Zweck erhebt. Das Problem besteht häufig darin, dass Gerichte diese Einwilligung im Nachhinein für unzulässig erklären. In so einem Fall darf das Unternehmen die Daten nicht auswerten und sie im Verfahren als Beweis heranziehen.

Speicherformen

Manche Daten muss ein Unternehmen im Original aufbewahren, Rechnungen und Handels- und Geschäftsbriefe dürfen jedoch auf Bild- oder Datenträgern vorliegen. Wichtig ist nur, dass die Unterlagen während der gesamten Aufbewahrungszeit lesbar bleiben. Admins müssen darauf achten, dass sie auf die Datenträger oder das Format, in dem sie die Daten abspeichern, auch nach Jahren noch uneingeschränkt zugreifen können. Beim Aufbewahren verschlüsselter E-Mails müssen sie dafür sorgen, dass der Verschlüsselungscode dem Unternehmen jederzeit zur Verfügung steht (Abbildung 1).

Admins als Zeugen

Weil Unternehmen zunehmend digital speichern, bekommt die Zeugenpflicht des Administrators bei der Beweissicherung in einem Strafverfahren eine besondere Bedeutung. Strafverfolger vernehmen Admins in Ermittlungsverfahren häufig direkt bei der Durchsuchung vor Ort als Zeuge. Dies ist im Strafverfahren rechtlich grundsätzlich möglich.

Es stellt sich die Frage, inwiefern der Admin als Zeuge verpflichtet ist, die gespeicherten Daten herauszusuchen und aufzubereiten. Im Grundsatz sind sich Rechtsprechung und Juristen einig: Der Admin muss lediglich das preisgeben, was er durch seine tägliche Arbeit an Wissen erlangt hat. Dazu gehören die Art und Weise, wie die Soft- und Hardware konfiguriert ist, die Art und Weise der Datensicherung und Informationen über Sicherungsmechanismen oder sonstige Zugangsberechtigungen.

Die Strafverfolger können den Admin in seiner Stellung als Zeugen nicht zwingen die Daten nach bestimmten Kriterien zu sortieren oder auszuwerten. Es gehört nicht zu den Aufgaben eines Zeugen, das Sichern und Auswerten der vorgefundenen Beweismittel zu erleichtern. Er ist lediglich verpflichtet über sein Wissen und seine Wahrnehmungen Auskunft zu geben. Selbstverständlich darf er jedoch freiwillig seine Hilfe anbieten.

Zur Herausgabe ist er erst verpflichtet, wenn die Staatsanwaltschaft auf Grundlage einer weiteren Norm einen Herausgabeanspruch geltend macht (§95 der Strafprozessordnung). Die Verpflichtung zur Herausgabe geht aber auch hier nicht so weit, dass der Admin die Daten herausgeben und auswerten muss. Die Strafverfolger dürfen im Einzelfall eine Kopie einzelner Daten verlangen, wenn sie damit einen weiter gehenden Eingriff in die Rechte des Betroffenen vermeiden.

Fazit

Ein Unternehmen muss beim Speichern von Daten diverse gesetzliche Regelungen beachten, die hier klare Grenzen vorsehen. Im Rahmen eines Strafverfahrens muss ein Admin als Zeuge sein Wissen preis- und gegebenenfalls die gespeicherten Datensätze herausgeben. Zum Auswerten der Daten kann ihn allerdings niemand verpflichten. *(kki)*

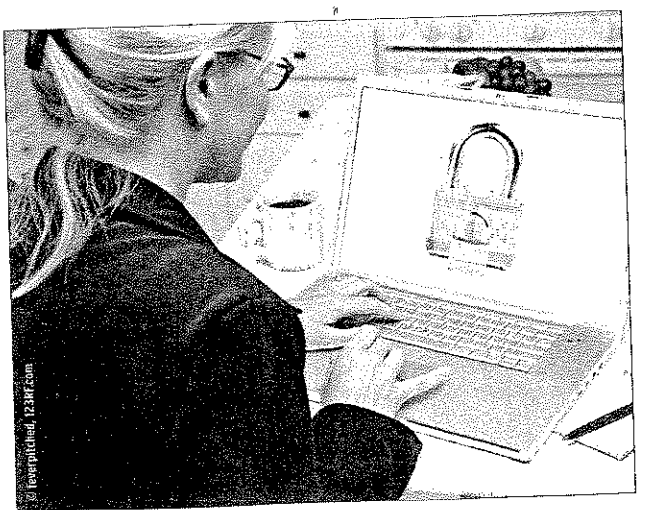

Abbildung 1: Mit verschlüsselten Daten kann ein Gericht in der Regel wenig anfangen, der Admin muss daher den Schlüssel sicher aufbewahren.

Der Autor

Die Kölner Kanzlei Wilde Beuger Solmecke hat sich auf die Beratung der IT- und Onlinebranche spezialisiert. Rechtsanwalt Christian Solmecke (40) hat in den vergangenen Jahren den Bereich IT-und E-Commerce stetig ausgebaut und betreut Medienschaffende und Web-2.0-Plattformen. Daneben ist er Geschäftsführer des Deutschen Instituts für Kommunikation und Recht im Internet (DIKRI) an der Cologne Business School [http://www.dikri.de].