

# Informationslecks - eine wachsende Herausforderung

*Videokameras, gelegentliche Checks von Fahrzeugen und Zugangsschranken gehören beim Werkschutz zum Standard. Wo der Verlust unternehmenskritischer Daten zu grossen wirtschaftlichen Schäden führen kann, sind Lösungen unerlässlich, die vergleichbare Sicherheitsstandards auch im IT-Umfeld etablieren.*

FRANK BRANDENBURG

**F**ür die physische Sicherheit im Unternehmen ist der Sicherheitsdienst zuständig. Seine Aufgabe: Gefahren und Schaden abwehren. Seine Hilfsmittel sind Alarmanlagen, Brandmelder und Bewegungssensoren. Darüber hinaus müssen sich Besucher bei ihrer Ankunft anmelden und erhalten einen temporären Ausweis, den sie bei Verlassen des Gebäudes wieder abgeben. Die Fahrzeuge von Fremdfirmen werden bei der Ein- und Ausfahrt registriert, und auch die Mitarbeiter müssen sich beim Betreten des Gebäudes mit

einer elektronischen Kennkarte ausweisen. Physisch ist das Firmengelände sehr gut gesichert.

Im digitalen Zeitalter hat sich einiges geändert. Früh haben Unternehmen die Vorteile des Internets erkannt und damit begonnen, diese für sich zu nutzen. Folglich gibt es heute kaum noch sensible Firmendaten, die nicht digital gespeichert sind und über das Internet mit Geschäftspartnern ausgetauscht werden. Umso wichtiger erscheint es jetzt, diese Informationen besser zu schützen. Kundendaten,

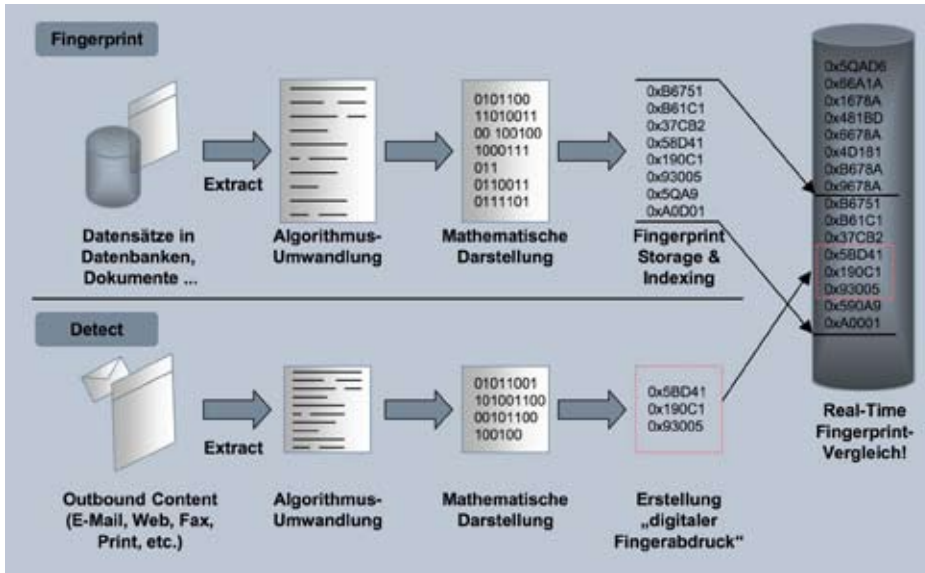
Verträge, Angebote oder Konstruktionspläne aus der Forschung und Entwicklung finden sich zuhauf in den Datenbanken und auf den File-Servern von Unternehmen.

## **Informationslecks: eine wachsende Herausforderung**

Beim Datenschutz hat sich in den letzten Jahren viel getan, wenn auch noch nicht genug. Die gute Nachricht vorweg: Fast jedes Unternehmen nutzt heute Virenschutzsoftware, Firewalls und Zugangskontrollen in Form von Passwörtern oder



Quelle: istockphoto



Um die Datenstruktur von Files zu analysieren, verwendet die Websense Data Security Suite eine Serie von Algorithmen. Der daraus entstehende digitale Fingerabdruck erlaubt eine akkurate Identifikation von Informationen. Quelle: Websense

## Essential Information Protection



Eine mehrstufige, integrierte Data-Loss-Prevention-Lösung schützt Unternehmen vom Gateway bis zu den Endgeräten. Quelle: Websense

Tokens, um sich vor Angriffen von aussen zu schützen. Die schlechte Nachricht: Ihre Wirkung reicht nicht aus. Dass solche Angriffe häufig unbemerkt stattfinden, sollte Anlass genug sein, die digitale Integrität von Prozessen und Systemen zu hinterfragen.

Das gilt beispielsweise für vertrauliche Unterlagen und Dokumente, die Firmen früher im Tresor aufbewahrten. Sie werden heute oft nur unzureichend mit Passwörtern gesichert auf File-Servern gespeichert. Versehentlich verschickt jemand das falsche Dokument per Attachment. In anderen Fällen ergänzen Outlook oder Notes automatisch die E-Mail-Adresse und aus Unachtsamkeit haben die vertraulichen Geschäftsunterlagen den falschen Empfänger erreicht. Wird der Irrtum sofort bemerkt, hält sich der Schaden in Grenzen. Landen die wichtigen Daten jedoch in den falschen Händen, kann daraus

sehr schnell ein wirtschaftlicher Nachteil entstehen.

Bisher wurde primär kontrolliert, was von aussen ins Unternehmen kommt. Künftig wird man sich mindesten ebenso intensiv darum kümmern müssen, welche Daten auf welchen Kommunikationskanälen das Unternehmen verlassen. Das Thema lautet hier Data Loss Prevention (DLP). Als einfache Faustregel gilt: Schützenswert ist immer das, was einem Risiko ausgesetzt ist. Nach dieser Maxime handelt jedes Unternehmen. Die Bewertung des Risikos und die Sicherheitsmassnahmen zu Minderung der Risiken – etwa als Folge von Industriespionage oder Datenverlusten durch gestohlene Notebooks – sind die zentralen Kriterien für eine durchgängige, ganzheitliche End-to-End-Security.

Dazu wird ein vollständig integriertes Sicherheitskonzept benötigt, das alle po-

tenziellen Angriffspunkte und Schwachstellen in den Bereichen Web Security, Messaging Security und Data Security berücksichtigt. Das reicht vom Internetzugang über den E-Mail-Verkehr einschliesslich der damit transportierten Attachments bis den auf den auf internen und mobilen Speichermedien vorhandenen Daten. In dem Zusammenhang dürfen natürlich auch die rechtlichen Anforderungen an den Datenschutz nicht vergessen werden. Zu nennen sind branchenabhängige sowie allgemein gültige Richtlinien zu Compliance und Risikomanagement.

Am Rande bemerkt befassen sich auch Marktforscher wie IDC mit den hier angesprochenen Themen. IDC zufolge benötigen Unternehmen einen ganzheitlichen und integrierten Ansatz für Internet Security, um den Bedrohungen aus dem Web wirksam begegnen zu können; IDC bezeichnet dies als «Web Security Ecosystem». Namentlich erwähnt IDC die drei Bereiche Web 2.0, Blended Malware (eine Kombination aus E-Mail, Trojanern und Ausnutzung bekannter und unbekannter Sicherheitslücken) sowie die Risiken einer unerlaubten Weitergabe unternehmenskritischer Daten (Data Loss Prevention).

## Essential Information Protection

Bei der IT-Sicherheit im engeren Sinn geht es um Integrität, Vertraulichkeit und Verfügbarkeit von Daten. Analog zum physikalischen Werkschutz sind viele Unternehmen auch im digitalen Umfeld sehr stark auf Systeme zur Zugangskontrolle fokussiert. Ist der User einmal authentifiziert, gibt es bislang aber nur wenige Einschränkungen, wie mit den vorhandenen Daten umzugehen ist. Hier setzt das Konzept des Essential Information Protection an.

Bei Essential Information Protection geht es unter anderem um eine abgestufte, aber dennoch vollständig integrierte Verteidigung gegen Bedrohungen jeder Art. Am Beginn steht eine Risikobewertung. Vereinfacht ausgedrückt untersuchen Unternehmen, wie wahrscheinlich das Eintreten eines bestimmten Schadens ist und welche Auswirkungen der Schaden hätte. Die Risikoanalyse liefert wertvolle Informationen, um festzustellen, wo im Unternehmen anzusetzen ist.

An Massnahmen für einen sicheren Internetzugang kommt niemand vorbei. Firewall, Virenschutz auf den Servern und den Endgeräten sowie ein möglichst effektiver Spamfilter gehören zu den Mindestanforderungen. Dazu kommen auch Content-Filter-Lösungen. Sie ermöglichen Unternehmen, sehr flexible Richtlinien zum Zugriff auf Webseiten zu definieren. Solche Vorgaben können sich auf Kategorien wie Rassismus, Kinderpornografie, Waffen etc. beziehen sowie auf bestimmte Dateitypen und Protokolle, die ein Risiko für das Netzwerk und die PCs darstellen, z. B. Trojaner, Malware und Würmer.

