INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Data Leak Prevention

E-Mails überwachen – oder doch nicht?

von Bernd Reder
CRN.de, 06.07.2010

Oft sind es E-Mails, über die Mitarbeiter absichtlich oder aus Versehen interne Informationen aus einem Unternehmen hinausschaffen. Kein Wunder, dass Unternehmen solche Vorfälle durch eine strikte Kontrolle und interne Vereinbarungen unterbinden möchten. Doch der Gesetzgeber setzt solchen Aktionen enge Grenzen.

E-Mails überwachen – ja oder nein? Vor dieser Frage stehen Firmen und Behörden, die den Abfluss wichtiger Informationen über diesen Kommunikationskanal verhindern möchten. Statistiken des Data-Leak-Prevention-Spezialisten Info Watch belegen, dass der Schutz der Unternehmens-E-Mails normalerweise der erste Schritt ist, um ein effizientes System zum Schutz von Unternehmensdaten zu schaffen.

Dabei sind zwei Fragen zu klären:

- Wie kann Software zur Analyse von vertraulichen Daten in der E-Mail-Korrespondenz und auf Workstations von Benutzern verwendet werden, ohne gegen geltendes Recht zu verstoßen?
- Wie können die Ergebnisse als Beweis einer widerrechtlichen Aktivität von Mitarbeitern verwendet werden?

Ansatz 1: Keine privaten E-Mails

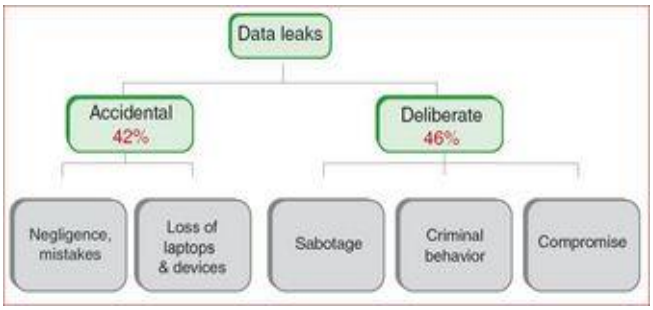
Eine Möglichkeit besteht darin, dass ein neuer Mitarbeiter eine Vereinbarung mit dem Unternehmen unterzeichnet. Das Dokument enthält die Liste der vertraulichen Informationen, auf die der Mitarbeiter im Rahmen seiner Tätigkeit zugreifen, die er aber keinesfalls weitergeben darf.

Ein weiterer Bestandteil der Vereinbarung ist, dass der Mitarbeiter über die mögliche Verwendung von technischen Kontrollmaßnahmen im Unternehmen in Kenntnis gesetzt wird. Es wird festgelegt, dass der Mitarbeiter Computer und Kommunikationskanäle zur Erfüllung seiner Arbeitsverpflichtungen erhält.

Er verpflichtet sich jedoch, keine privaten E-Mails zu senden oder empfangen oder Dokumente mit persönlichem Inhalt auf seinem Arbeitsplatzrechner zu speichern. In diesem Fall darf der IT-Sicherheitsbeauftragte alle E-Mails des Mitarbeiters einsehen – vorausgesetzt, sie enthalten keine persönlichen Informationen.

Auch Arbeitgeber auf dünnem Eis

Und genau hier liegt das Problem: Denn was tun, wenn der Mitarbeiter gegen diese Vorgaben verstößt? Er verletzt in diesem Fall die Vereinbarung mit seinem Arbeitgeber und kann dafür zur Verantwortung gezogen werden – bis hin zur fristlosen Entlassung.



Doch auch der IT-Sicherheitsbeauftragte bewegt sich in einem solchen Fall auf dünnem Eis. Denn er verstößt gegen die Regelungen zum Schutz der Privatsphäre und des Briefgeheimnisses, wenn er auf persönliche Daten des betreffenden Mitarbeiters zugreift – auch dann, wenn der die Informationen gegen Weisung auf seinem Rechner lagert.

Die Kontrolle stellt eine strafbare Handlung dar, die mit Geldbußen oder mit Freiheitsentzug geahndet werden kann.

Ansatz 2: Arbeitnehmer lässt E-Mail-Überwachung zu

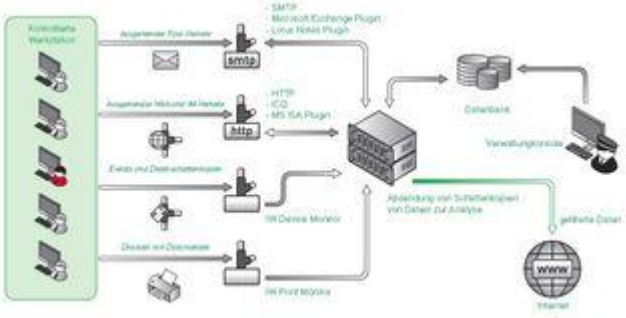
Häufig praktiziert wird ein zweiter Ansatz: Der Mitarbeiter erhält zum einen die Aufstellung mit den vertraulichen Dokumenten, die das Unternehmen nicht verlassen dürfen. Zum anderen ermächtigt er das Unternehmen, speziell den Chief Security Officer, seine E-Mails und die Inhalte auf seiner Workstation auf vertrauliche Daten hin zu untersuchen.

Der CSO erhält somit das Recht, die elektronische Korrespondenz des Mitarbeiters zu lesen, allerdings nur zu dem Zweck, Verstöße gegen die Sicherheitsregeln zu verhindern oder nachzuweisen.

Allerdings vertritt die Mehrzahl der Rechtsexperten die Auffassung, dass eine solche Vereinbarung einen unzulässigen Eingriff in die Grundrechte eines Mitarbeiters darstellt und somit nichtig ist. Kommt es zu einem Verfahren vor einem Arbeitsgericht, kann sich der Arbeitgeber nicht auf entsprechende Abmachungen berufen.

Ansatz 3: Software kontrolliert E-Mails

Keine rechtlichen Bedenken der genannten Art gibt es jedoch, wenn eine Software die Überwachung von Informationen übernimmt. In diesem Fall werden weder Persönlichkeitsrechte noch das Briefgeheimnis verletzt, natürlich vorausgesetzt, der Überwachungsvorgang läuft ohne Zutun des IT-Fachpersonals ab.



Dazu ein Beispiel: Das Analysesystem hat einen Anhang im Postausgang eines E-Mail-Postfachs ermittelt, der verdächtige Daten

enthält.

Handelt es sich um einen Vorgang mit kriminellem Hintergrund (Kinderpornografie, Drogen- oder Waffenhandel et cetera), sind Polizei und Staatsanwaltschaft zu informieren. Diese dürfen die E-Mails oder Inhalte auf dem Rechner des Verdächtigen ohne Einwilligung des Besitzers oder Benutzers einsehen.

Kontrolle im Beisein von Vorgesetzten

Stellt Vorfall »nur« einen Verstoß gegen die Arbeitsvereinbarung dar, hat der Sicherheitsbeauftragte das Recht, das Dokument oder die E-Mail mit Einwilligung des Mitarbeiters einsehen. Dem Mitarbeiter wird in diesem Fall angeboten, dem Sicherheitsbeauftragten den Inhalt der E-Mail oder des Dokuments in Beisein seines Vorgesetzten zu zeigen.

Außerdem hat der Mitarbeiter das Recht, die Anwesenheit eines Betriebsrats während der Inspektion zu verlangen.

Natürlich kann ein Mitarbeiter auch ein Veto gegen die Kontrolle seines Betriebsrechners und der darauf befindlichen Informationen einlegen. Das jedoch kann zu einer Neubewertung des Vorfalls führen.

Schlimmstenfalls wird der Sicherheitsbeauftragte die Weigerung als Eingeständnis werten, dass der betreffende Mitarbeiter gegen die Weisung des Unternehmens gehandelt oder gegen Gesetze verstoßen hat. In diesem Fall ist es denkbar, dass die Polizei zur Untersuchung des Falles hinzu gezogen wird. Diese kann, wie erwähnt, auch ohne Zustimmung des Mitarbeiters dessen Rechner und E-Mail-Postfächer untersuchen.

Der Autor: Rustem Khayretdinov ist Deputy Chief Executive Officer der russischen IT-Sicherheitsfirma Info Watch.

http://www.crn.de/security/artikel-84472.html