COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/datenklau-nichts-leichter-als-das,1904227

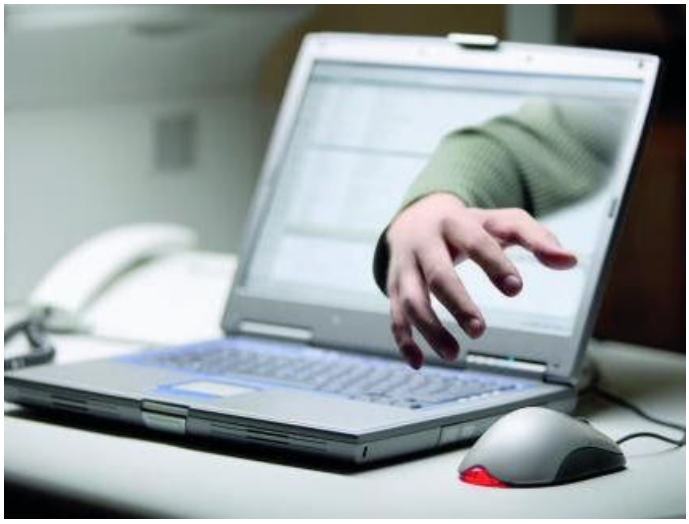
Acht Tipps zum Schutz Ihrer Unternehmensinformationen

Datenklau - nichts leichter als das

Datum: 01.09.2009
Autor(en): Thomas Pelkmann

Der Datenklau nimmt zu - nicht nur durch Angreifer von außen, sondern zunehmend auch durch unzufriedene Mitarbeiter des eigenen Unternehmens. Wir zeigen Ihnen, wie Sie sich wirksam davor schützen.

Der Ruf des Fürstentums Liechtenstein hat böse gelitten, seit im Februar 2008 bekannt wurde, dass die Bankdaten vieler hundert ausländischer Kunden gestohlen und an bundesdeutsche Behörden verkauft wurden. Bei den 15 Banken Liechtensteins brachen seitdem die Kundenanlagen um 29,5 Prozent ein, wie der jüngst vorgelegte Jahresbericht des Liechtensteiner Bankenverbandes (LBV) dokumentiert. Das Kundenvermögen betrug zum 31. Dezember 2008 demnach rund 121 Milliarden Schweizer Franken (76 Milliarden Euro) und war damit um 50,6 Milliarden Franken geringer als Ende 2007.



Der Datenklau in Unternehmen nimmt zu. Dabei droht Gefahr nicht nur von außen. Auch die eigenen Mitarbeiter können wertvolle Informationen entwenden.

Die Gefahr ausgespäht zu werden, droht nicht nur von externen Datendieben, die sich unbefugten Zugang zu Firmennetzen verschaffen. Es sind in vielen Fällen die eigenen Mitarbeiter, die vertrauliche Informationen aus dem Unternehmen schmuggeln, um ihrem Arbeitgeber zu schaden oder mit den Daten Geld zu verdienen. So haben beispielsweise die Wirtschaftsprüfer von KPMG in der **e-Crime Survey 2009**[1] herausgefunden, dass vor allem entlassene IT-Fachkräfte zum Sicherheitsrisiko werden können.

Als größtes Problem nannten die mehr als 300 befragten Sicherheitsbeauftragten den Diebstahl von Kunden- oder Mitarbeiterdaten. Am zweithäufigsten befürchten sie, dass Entlassene ihr Wissen um Schwachstellen der firmeneigenen Systeme ausnutzen könnten. Diebstahl geistigen Eigentums oder wichtiger Geschäftsdaten war das an dritter Stelle genannte mögliche Delikt ehemaliger Kollegen.

Das Sicherheitsunternehmen **Cyber-Ark**[2] wiederum fand in einer Umfrage heraus, dass mehr als ein Drittel aller IT-Mitarbeiter potentielle Schnüffler seien. Ein erhebliches Sicherheitsrisiko gehe dabei von privilegierten Accounts aus, wie Administratoren sie besitzen: In der Regel sind die Passwörter dieser bevorzugt behandelten Benutzer der Generalschlüssel zu allen unternehmenskritischen Datenbeständen.

Auf dem Wunschzettel der Datendiebe ganz oben stehen der Cyber-Ark-Umfrage zufolge M&A-Pläne, die etwa 47 Prozent der Befragten entwenden würden. Knapp dahinter: F&E-Informationen mit einer Anhängerschaft von 46 Prozent der IT-Mitarbeiter. Besonders beliebt sind zudem die Passwörter des CEO, bei dem ebenfalls 46 Prozent gerne zugreifen würden.

Für das Bekämpfen dieses Datendiebstahls hat sich in den vergangenen Jahren der Begriff **Data Loss Prevention (DLP)**[3] durchgesetzt. - Produkte und Lösungen, die den unautorisierten Abfluss von Informationen verhindern sollen. Aber auch jenseits solcher Lösungen gibt es Verhaltensmaßnahmen für Unternehmen, die den Datenklau verhindern helfen. Der Sicherheitsspezialist **Websense**[4] hat daher die folgenden Tipps zum Schutz vor Datenlecks veröffentlicht.

So schützen Sie Ihre Firmendaten

1 Definieren Sie Regeln für die IT-Security

Jedes Unternehmen braucht eine schriftlich fixierte und an alle Mitarbeiter kommunizierte IT-Sicherheitsstrategie. Sie enthält sämtliche Vorschriften und Regeln, wie sensible Daten intern und mit Kunden, Lieferanten und Geschäftspartnern ausgetauscht werden dürfen. Ohne verpflichtende und zentral überwachte Sicherheitsregeln geht es nicht. Die Security-Vorschriften umfassen interne Anordnungen, aber auch branchenweite Regeln und die gültigen Datenschutzgesetze.

2 Klassifizieren Sie Ihre Unternehmensdaten

Möchten Sie in Ihrem Unternehmen eine Lösung zum Schutz vor Datenverlusten einführen, müssen Sie zunächst einmal die vorhandenen Daten ermitteln und klassifizieren. Dabei legen Sie fest, welche Informationen allgemein zugänglich, welche vertraulich und welche streng geheim sind. Dazu kommt eine Dokumentation der Geschäftsprozesse, in denen sensible Daten zum Einsatz kommen. Für die Kontrolle der Einhaltung von Sicherheitsmaßnahmen ist dieser Punkt unerlässlich.

3 Spüren Sie sicherheitsrelevante Daten auf

Wer weiß, wo sich im Unternehmen besonders sensible Daten befinden, kann dann auch Maßnahmen ergreifen, um sie optimal zu schützen. Denn nur in den seltensten Fällen verbleiben die vertraulichen Daten gut abgeschirmt im Rechenzentrum. Vertrauliche Kundeninformationen, Konstruktionspläne, Basisdaten für Preiskalkulationen oder Ausschreibungsunterlagen werden per E-Mail verschickt oder sind auf den Notebooks der Außendienstmitarbeiter zugänglich - manchmal unverschlüsselt und ohne sicheres Passwort.

4 Schulen Sie Ihre Mitarbeiter regelmäßig

Ergänzend zu allen technischen IT-Security-Maßnahmen der Datenklassifikation und zu den schriftlich formulierten Sicherheitsregeln ist es unabdingbar, dass Unternehmen ihre Mitarbeiter regelmäßig schulen und deren Sensibilität beim Umgang mit vertraulichen Daten schärfen. An konkreten Beispielen aus der betrieblichen Praxis lässt sich leicht aufzeigen, welche Gefahren beim leichtsinnigen Umgang mit sensiblen Informationen drohen.

5 Bewerten Sie die Risiken eines Datenverlusts

Untersuchen Sie, wie wahrscheinlich das Eintreten eines bestimmten Schadens ist und welche Auswirkungen dieser Schaden hätte. Die Risikoanalyse liefert Ihnen entscheidende Informationen, um festzustellen, wo im Unternehmen Sie ansetzen sollten und wie sich die gravierendsten Lücken am schnellsten schließen lassen.

6 Regeln Sie den Zugriff auf vertrauliche Daten

Aus der Klassifikation der Daten leiten sich die Zugriffsrechte für Benutzergruppen ab. Über Arbeitsanweisungen definiert der Sicherheitsbeauftragte eines Unternehmens, wer in welchen Geschäftsprozessen befugt ist, bestimmte Daten zu erstellen und zu ändern. Aus der Kombination Klassifikation und Geschäftsprozesse können Sie dann über Verzeichnisdienste, etwa Microsoft Active Directory, regeln, wer vertrauliche Daten an einen bestimmten Kreis von Adressaten verschicken darf. Damit verhindern Sie in Ihrem Unternehmen, dass sensible Informationen unkontrolliert das firmeneigene Netz verlassen.

7 Überwachen Sie die Kommunikationswege

Wichtig ist, die Kommunikationswege genau zu kennen und zu überwachen, auf denen vertrauliche Daten das Unternehmen verlassen können. Neben E-Mail und Instant Messaging betrifft dies auch den Export einzelner Dateien oder gar Teile der Kundendatenbank via USB-Stick oder anderen mobilen Speichermedien. Dazu können Sie Anwendungen einrichten, die kontrollieren, wer, was, wohin und wie verschickt. Die Möglichkeiten der inhalts- und benutzerbasierten Kontrolle ergeben sich aus den Zugriffsregeln, wie sie der IT-Sicherheitsbeauftragte definiert hat.

8 Verschlüsseln Sie Ihren Datenverkehr

Alle vertraulichen Informationen dürfen das Unternehmen nur geschützt verlassen. Im idealen Fall gibt es eine automatische Verschlüsselung des Datenverkehrs. Falls nicht, sollte Sie so etwas dringend einführen. Die Verschlüsselung ist ein wichtiger Baustein in einer wirksamen DLP-Lösung. Wer dann versehentlich oder absichtlich sensible Daten unverschlüsselt per E-Mail-Anhang zu versenden versucht, wird vom System auf das Fehlverhalten hingewiesen und hat die Möglichkeit, die Aktion zu stoppen.

Links im Artikel:

[1] **http://www.e-crimecongress.org/ecrime2009/documents/e-CrimeSurvey2009_AKJ_KPMG%281%29.pdf**
[2] **http://www.cyber-ark.com/**
[3] **http://de.wikipedia.org/wiki/Data_Loss_Prevention**
[4] **http://www.websense.com/content/Regional/Germany/Home.aspx**
