



#### Wohngebäudeversicherung

HUK24 Wohngebäudeversicherung: Sicherer Schutz, niedrige Beiträge!  
[www.HUK24.de](http://www.HUK24.de)

#### It Security

Identity Management, Zugriffsschutz Verschlüsselung und Skalierbarkeit.  
[www.oracle.com/de/mittelstand](http://www.oracle.com/de/mittelstand)

## Sicherheit vor der Gefahr von innen

Datum:21.08.2008

Autor(en):Michael Thieroff

URL: <http://www.pcwelt.de/176072>



**Nach außen hin sind die meisten Unternehmen vor Betriebsespionage geschützt. Doch an Spione in den eigenen Reihen denken die wenigsten Firmenchefs. Dabei ist es relativ einfach, Maßnahmen dagegen zu ergreifen.**

Fast ein Fünftel der deutschen Unternehmen hatten in der Vergangenheit wirtschaftliche Schäden durch Spionage zu beklagen. Zu diesem Ergebnis kommt eine Studie der Firma Corporate Trust aus München. Der entstandene Schaden für die deutsche Wirtschaft geht dabei in die Milliarden. Der Fokus liegt bei der Spionageabwehr in Unternehmen hauptsächlich auf Hackerangriffe von außen.

Doch was, wenn ein Maulwurf in der eigenen Firma sitzt? Der so genannte "Informationsabfluss" durch eigene Mitarbeiter, wie es im Fachjargon heißt, liegt bei über 20 Prozent der geschädigten Firmen. Meist werden technische Innovationen oder das Know-how von Produktionsabläufen weiter gegeben. Doch auch Kundendaten werden von Mitarbeitern gerne mitgenommen, wenn sie etwa den Job wechseln wollen.

### Nicht alles unter Verschluss

Doch was kann man gegen Spionage im Inneren tun? Firewalls nutzen nur für die Sicherheit nach außen. Und das Wegschließen von sensiblen Daten nützt auch nur begrenzt. Schließlich sollen die Mitarbeiter ja effektiv arbeiten können. Christian Schaaf, Geschäftsführer von **Corporate Trust**<sup>1</sup>, rät zur Sensibilisierung der Mitarbeiter. "Häufig wird nach einem Informationsabfluss durch interne Täter festgestellt, dass es vereinzelt kleine Hinweise gab. Diese kleinen Puzzlestücke wurden aber nirgends zusammen geführt, weil die Mitarbeiter zu dem Thema gar nicht sensibilisiert waren. Ihnen war nicht bewusst, dass speziell dieser Hinweis wichtig sein könnte", erklärt Schaaf.

IT-Vverantwortliche sollten sich erst einmal den Status quo anschauen. "Anhand einer Risikomatrix für das Unternehmen sollte definiert werden, welche Bereiche überhaupt sensibel sind", sagt Schaaf. Meist seien das nur zehn bis 15 Prozent aller Informationen des Unternehmens, die so genannten Kronjuwelen. Gibt es bereits Sicherheitsstrategien, kann man unter Umständen darauf aufbauen. Ist noch keine Strategie im Unternehmen vorhanden, sollte man schnell reagieren. Es sollte eine Risiko- und Schwachstellenanalyse für diese sensiblen Bereiche geben, welche "Leaks" es gibt und wie hoch die Anfälligkeit ist. Christian Schaaf: "Das Endergebnis sollten klare Empfehlungen zur Beseitigung der Schwachstellen und damit eine Risikominimierung sein."

### Welche Daten für welchen Mitarbeiter?

Je sensibler der Bereich, umso "vertrauenswürdiger" sollte der Mitarbeiter sein. "Unternehmen sollten gewisse Einstufungen vornehmen, wer an höchst vertrauliche Informationen kommen kann und darf", sagt Schaaf. Was ein wenig nach Geheimdienst klingt, kann im Alltag sehr nützlich sein und in manchen Fällen sogar ein Unternehmen vor dem Ruin bewahren. Der Sicherheitsexperte rät, die Abstufung der Informationen und Dokumente von "offen" über "vertraulich" bis zu "streng vertraulich" oder auch "geheim" einzustufen, je nachdem in welchem Bereich ein Unternehmen tätig ist.

Christian Schaaf rät auf jeden Fall, Bewerber zu überprüfen: "Ausschlaggebend für die Intensität der Überprüfung sollte die Vertraulichkeit der zu besetzenden Position sein. Die Maßnahmen können dabei von der Überprüfung der vorgelegten Zeugnisse auf Echtheit, über Anrufe bei früheren Arbeitgebern bis hin zu Schufa-Auskunft, polizeilichem Führungszeugnis oder einem Background-Check durch Sicherheitsspezialisten reichen." Das gelte auch für Mitarbeiter, die schon länger im Unternehmen tätig sind und auf eine sensible Position versetzt werden sollen.

Überprüft werden sollte aber auch externes Personal. So üben etwa Reinigungskräfte ihre Tätigkeit nach Büroschluss aus und sind damit "ohne Aufsicht". "Hier sollte man schon genau wissen, wer unter Umständen freien Zugriff auf herumliegende Dokumente hat oder sich Zutritt in sensible Bereiche verschaffen kann", sagt Schaaf.

## Unsicherheitsfaktor Mensch

Steht das Sicherheitskonzept, sind alle Rechte vergeben und wichtige Dokumente unter Verschluss, muss noch das größte Sicherheitsrisiko beseitigt werden: der Mensch. Natürlich soll das nicht heißen, dass alle Mitarbeiter entlassen werden müssen. Vielmehr muss Sicherheit im Unternehmen gelebt werden. Die besten Mechanismen zum Schutz vor Spionage können nicht greifen,

wenn die Sicherheitsphilosophie den Mitarbeitern nicht nahe gebracht wird. Sicherheitsexperte Christian Schaaf warnt davor, Maßnahmen "von oben nach unten durchzudrücken". "Die Sensibilisierung der Mitarbeiter leistet hier einen wesentlichen Beitrag." So müssen die Mitarbeiter unbedingt ein Verständnis dafür entwickeln, warum es wichtig ist, mit sensiblen Informationen aufmerksam umzugehen.

### Geheime Daten auf dem iPod

Doch was, wenn ein Spion aus den eigenen Reihen Firmengeheimnisse per Webmailer verschickt? Admins sollten per URL-Filter entsprechende Adressen sperren. Dann wird es schwieriger, geheime Daten auf den iPod zu kopieren oder eine DVD zu brennen. Man könnte entsprechende Geräte in der Firma verbieten. Diese Methode dürfte allerdings in den wenigsten Bereichen durchführbar sein. Zweckmäßig ist es, die entsprechenden Ports zu sperren und keine CD- oder DVD-Brenner in die Arbeitsplatzrechner einzubauen.

Wer eine Datei mitnehmen möchte, muss diese entweder beim Sicherheitsbeauftragten abholen oder braucht eine hohe Sicherheitseinstufung. Christian Schaaf rät dazu, sensible Informationen besonders zu schützen: "Bei den Zugängen zu den 'Kronjuwelen' eines Unternehmens sollte darüber nachgedacht werden, ob diese Informationen nur auf Stand-alone-Geräten verarbeitet werden oder ob es eine Abtrennung nach außen gibt, also kein Zugang ins Internet."

### Menschliches Versagen

Sind alle Sicherheitsmechanismen ausgeschöpft, ist man allerdings immer noch nicht vor menschlichem Versagen gefeit. So kann der Mitarbeiter noch so vertrauenswürdig sein, wenn er sich einen Datenträger mit wichtigen Dokumenten stehlen lässt oder verliert, kann trotz der Sicherheitsrichtlinien großer Schaden entstehen. In solch einem Fall hilft eine so genannte Zweiwege-Authentifizierung. Damit man an die Daten herankommt reicht nicht allein ein Passwort. Bei jedem Aufruf einer so gesicherten Datei muss eine Transaktionsnummer (TAN), ähnlich wie beim Online-Banking, eingegeben werden. Fehlt dem Datendieb das Passwort oder die TAN, kann er mit den Daten nichts anfangen.

### Sicherer USB-Stick



Eine andere Möglichkeit besteht darin, Daten gleich auf einen sicheren USB-Stick zu kopieren und unterwegs nur mit dem Stick zu arbeiten. Die Firma Corsair bietet etwa einen USB-Stick an, der mit einem Codeschloss versehen ist. Wird der Stick abgezogen, sperrt er sich automatisch. Nach dem Einstecken gibt er Daten nur nach richtiger Eingabe der PIN frei.

### Restrisiko bleibt

Dateifreigaben, Background-Checks und USB-Dongles schützen wertvolle und geheime Firmendaten. Die wichtigste Voraussetzung für effektive Sicherheit im Firmennetzwerk ist, dass die Sicherheitsphilosophie von allen Mitarbeitern gelebt wird. Nur dadurch kann sichergestellt werden, dass auch kleinere Lecks sofort aufgedeckt und an den Sicherheitsverantwortlichen weiter gemeldet werden. Geschäftsführung und Mitarbeiter müssen sich im Klaren sein, dass an der Sicherheit der Unternehmensdaten unter Umständen das Wohl und die Existenz des Unternehmens hängt.

### Links im Artikel:

<sup>1</sup> <http://www.corporate-trust.de/>

---

IDG Magazine Media GmbH  
Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Magazine Media GmbH. DPA-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass in PC-WELT unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von PC-WELT aus gelinkt wird, übernimmt die IDG Magazine Media GmbH keine Verantwortung.