enable
Magazin für Unternehmer

FINANCIAL TIMES DEUTSCHLAND

NOVEMBER 2011

SCHWERPUNKT

GRÜNDER INITIATIVE
enable 2 start

NAHTKAMPF

Nach zwei Pleiten ist der Nähmaschinenbauer Pfaff wieder quicklebendig – als Spezialist für die Industrie

DU KOMMST HIER NICHT REIN

Gegen Hackerattacken sichern sich viele Firmen ab. Gegen Datenmissbrauch durch die eigenen Mitarbeiter nur die wenigsten. Ein gefährlicher Fehler

Text: ALMUT KASPAR und CLAUS HORNUNG

So viel Ehrlichkeit ist selten. Man habe finanzielle Probleme, räumte die Firma Häffel in einer E-Mail an ihre wichtigsten Geschäftspartner und Kreditgeber ein. Möglicherweise könne es zu Verzögerungen beim Bezahlen von Außenständen und Kreditraten kommen. Absender: der Geschäftsführer des Gebäudereinigungs- und Bewachungsunternehmens.

Die Information verbreitete sich schnell, bald tuschelte die ganze Stadt über die Schwierigkeiten der Firma Häffel, die in Wirklichkeit anders heißt. Das war der Anfang vom Ende: Kunden stellten die Zusammenarbeit ein, Geschäftspartner sprangen ab, schließlich musste das Unternehmen Insolvenz anmelden.

Was die Verbreiter des Gerüchts nicht wussten: Das Unternehmen war in Wirklichkeit kerngesund, die Behauptungen über angebliche Zahlungsschwierigkeiten waren frei erfunden. Die E-Mails aus der Geschäftsführung waren gefälscht.

DEN WAHREN ABSENDER ermittelte Mark Semmler, Chef der Firma Antago, die Firmen bei Suche nach Lecks in ihren IT-Systemen hilft. Semmler, ein ehemaliger Hacker, fand heraus, dass die Mails aus Rache verschickt worden waren – vom ehemaligen Prokuristen der Firma. Der war kurz zuvor fristlos entlassen worden, weil er Geld in die eigene Tasche gesteckt hatte. Offensichtlich hatte anschließend niemand daran gedacht, seinen Zugang zum firmeninteren E-Mail-System zu sperren.

Semmler wundert das nicht. Er weiß: Die meisten Angriffe auf die IT von Unternehmen kommen aus den eigenen Reihen. Einer Studie der Wirtschaftsprüfungsgesellschaft KPMG zufolge werden mehr als 60 Prozent aller IT-Delikte in deutschen Unternehmen von den eigenen Mitarbeitern begangen (siehe Grafik).

Nicht immer handeln die Täter vorsätzlich wie im Fall des rachsüchtigen Prokuristen. Auch pure Sorglosigkeit kann große Schäden verursachen. Wenn Firmen ihn als Sicherheitsberater engagieren, lässt Semmler beim Gang durch die Flure gern mal einen USB-Stick fallen, auffallend markiert mit der Beschriftung „FKK-Urlaub 2011“. Seine Erfolgsquote liege sehr hoch, sagt Semmler: „Irgendjemand steckt den Stick immer in einen der Firmencomputer – und installiert damit ein Schadprogramm, mit dem ich Zugriff auf den Rechner bekomme.“

AUSGEBREMST
Sollen vertrauliche Daten gesichert werden, müssen Unternehmen klar regeln, welcher Mitarbeiter auf welche Dateien Zugriff hat

Ebenso leicht können sensible Firmendaten durch unaufmerksam versandte E-Mails in die falschen Hände gelangen. „Jedem passiert es einmal, dass er versehentlich eine Nachricht an den falschen Empfänger schickt“, sagt Katrin Böhme, Referentin für IT-Sicherheit im Mittelstand bei der Initiative „Deutschland sicher im Netz“ (DisN). „Darum sollte es Standard in Unternehmen sein, vertrauliche Daten in Anhängen zu speichern und diese durch eine Verschlüsselungssoftware zu schützen.“ Zu den gängigsten Herstellern zählen etwa Sophos, McAfee oder Symantec.

Tetra Images/Your Photo Today

Die größte Gefahr aber droht durch Mitarbeiter, die auch nach ihrem Ausscheiden noch auf Firmendaten zugreifen können. Oder die eine Zugangsberechtigung für Daten erhalten haben, die nichts mit ihrer Arbeit zu tun haben. „Das Problem ist, dass oft niemand weiß, wer innerhalb der Firma Zugriff auf welche Daten hat“, sagt Stephan Brack, Geschäftsführer der Berliner Firma Protected Networks. „Wenn ein neuer Mitarbeiter kommt, heißt es einfach: Gib dem mal die gleichen Rechte wie der Frau Meier, die das vorher gemacht hat – nur war Frau Meier mal Vorstandssekretärin und hatte deshalb auch Zugriff auf die Finanzdaten.“ Für Brack ist diese Laxheit nicht nachzuvollziehen. „Wenn Büroschlüssel verteilt werden, muss ja auch jeder dreimal unterschreiben.“

PROTECTED NETWORKS hat darum die Software 8Man entwickelt, mit der Unternehmen ihr Berechtigungsmanagement organisieren können. 8Man scannt Zugriffsmöglichkeiten auf Dateien und Laufwerke und stellt sie in Grafiken dar. „Damit können wir Führungskräften zeigen, wer auf was Zugriff hat und ob derjenige dazu berechtigt ist.“ Das Ergebnis sei oft erstaunlich. Immer wieder stellt Brack fest, dass Unternehmen sensible Daten auf Jedermann-Konten speichern, auf die alle im Betrieb Zugriff haben. „Dann reicht es, wenn Externe einen einzigen Mitarbeiter beeinflussen oder gar bestechen, um Daten nach außen zu geben.“

„Ein durchdachtes Berechtigungskonzept ist das A und O“, sagt Gerhard Kongehl, Professor für Datensicherheit an der Fachhochschule Ulm. „Unternehmen müssen mit technischen Mitteln dafür sorgen, dass diese Berechtigungen auch eingehalten werden.“ Dazu gehörten personenbezogene Zugangscodes, die zeitlich befristet sind. Zeitarbeiter sollten einen Chip erhalten, mit dem sie sich in bestimmte Rechner mit klar definierten Rechten einloggen können, empfiehlt Kongehl. „Und dass nur innerhalb der Zeit, in der sie in der Firma beschäftigt sind.“ Nach dem Ausscheiden der Zeitarbeiter werden die Chips deaktiviert. Diese können zudem so programmiert werden, dass man auch im Nachhinein nachvollziehen kann, wer wann an welchem Rechner gearbeitet hat. „So kommt man rachsüchtigen Mitarbeitern auf die Spur, denen gekündigt wurde und die dafür wertvolles Datenmaterial mitgehen lassen.“

DICHTMACHEN – SO SCHÜTZEN SIE IHRE DATEN

SICHERHEITSSTRATEGIE Jedes Unternehmen sollte wissen, wo wichtige Informationen gespeichert sind und ein Risikoregister mit Bedrohungsszenarien erstellen. Datensicherheitsprogramme müssen regelmäßig auf ihre Effektivität überprüft werden.

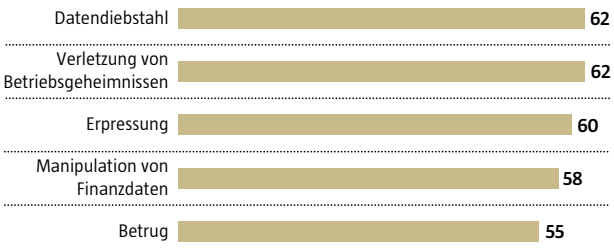
AUFKLÄRUNG Beschäftigte sollten in Schulungen dafür sensibilisiert werden, wo es Gefahren gibt und wie sie ausgeschaltet werden können. Wichtig ist, den Mitarbeitern mit Beispielfällen klar zu machen, wie wertvoll firmeninterne Daten sind.

BERECHTIGUNGSMANAGEMENT Jeder Angestellte darf nur Zugriff auf Daten haben, die er wirklich braucht. Die Berechtigungen müssen von den Abteilungsleitern regelmäßig überprüft werden.

VERSCHLÜSSELUNG Vertrauliche Informationen und Kundendaten sollten prinzipiell nur verschlüsselt abgespeichert und übertragen werden. Das gilt auch für Notebooks, Tablets oder Smartphones und für das Versenden von E-Mails.

Der Feind in meinem Haus

Anteil der Mitarbeiter an Computerstraftaten in Unternehmen, Angaben in %*



* Umfrage unter 125 deutschen Unternehmen, die bereits Opfer von Computerkriminalität geworden sind

FTD/ws; Quelle: KMPG 2010

> Oft herrscht das Denken vor: Bei uns ist ja noch nichts passiert
> KATRIN BÖHME, DISN

Ein häufiger Fehler von Unternehmen sei, neuen Mitarbeitern pauschal Zugriffsrechte einzuräumen, sagt DisN-Referentin Böhme. „Die beste Methode ist, erst einmal gar keine Rechte einzurichten, und sie dann nach Bedarf zu erteilen.“

Doch was nützen solche Vorgehensweisen, wenn es niemanden gibt, der die Kriterien festlegt und entscheidet, wann welcher Mitarbeiter in welche Kategorie fällt? „IT-Sicherheit ist Chefsache“, sagt Böhme, „das kann man nicht auf den IT-Leiter abschieben. Schließlich haftet der Geschäftsführer im Schadensfall mit.“ Das Bewusstsein über diese Gefahren sei im Mittelstand oft nicht stark ausgeprägt, so Böhme. „Bei vielen herrscht das Denken vor: Bei uns ist ja noch nichts passiert.“

Ein gefährliches Denken. Denn wenn tatsächlich etwas passiert, können Unternehmen dies kaum geheim halten. Denn seit 2009 gibt es den Paragrafen 42a des Bundesdatenschutzgesetzes. Der schreibt vor, dass Unternehmen umgehend die Aufsichtsbehörde informieren müssen, sobald vertrauliche Daten in die Öffentlichkeit gelangen. Ebenso alle von der Panne Betroffenen, beispielsweise Kunden. Sind diese nicht direkt zu erreichen, wird der Imageschaden noch größer. Dann ist das Unternehmen verpflichtet, halbseitige Anzeigen in mindestens zwei überregionalen Tageszeitungen zu schalten.

UM DAS RISIKOBEWUSSTSEIN im Mittelstand zu fördern, haben DisN und Bundeswirtschaftsministerium eine Internet-Seite eingerichtet (www.it-sicherheit-in-der-wirtschaft.de), auf der sich Unternehmer informieren können, wie sie ihre Daten am besten vor unbefugten Zugriffen sichern.

Sicherheitsberater Semmler empfiehlt Firmen, sich für eine Risikoanalyse an den Grundschutznormen des Bundesamts für Sicherheit oder der ISO-Norm 27001 zu orientieren. Das bedeute nicht gleich, eine teuere und zeitaufwendige ISO-Zertifizierung anzustreben. „Für kleine und mittlere Betriebe mit ein paar hundert Mitarbeitern reicht es, einzelne Punkte umzusetzen. Dafür reichen schon fünf bis zehn Arbeitstage.“ Ein überschaubarer Aufwand im Vergleich zu einer Insolvenz. □