



Serie: IT für den Mittelstand

Das firmeneigene Rechnernetz ist selbst manchem Selfmade-Boss nicht immer ganz geheuer. Ist es zu teuer? Zu alt? Zu unsicher? Das neue Impulse Themenspezial "IT für den Mittelstand" bringt alles, was Unternehmer heute in Sachen IT im Kopf haben sollten.

weitere Folgen:

IT-Sicherheit überfordert viele Mittelständler

05.03.2010

Angriff auf das Firmennetz

IT-Sicherheit überfordert viele Mittelständler

Von: Lars Reppesgaard



Jedes elfte Unternehmen wurde bereits Opfer eines Hacker-Angriffs.

© dpa

Den Firmenmitarbeitern, die sich um eine Anlage zum Pasteurisieren von Milch scharten, standen die Haare zu Berge. Ein Erpresser hatte gedroht, die Anlage zu manipulieren. Pünktlich zu dem Zeitpunkt, den er genannt hatte, veränderte sich wie von Geisterhand die Temperatur der Maschine.

Über eine Computerschnittstelle war das Produktionssystem der Firma an das Firmennetz angeschlossen. Zu dem hatte der Erpresser sich einen Zugang gehackt und kontrollierte nun, ob die Firma saubere Milch oder sauren, weißen Brei produzierte. "Die Firmenleitung zahlte. Was sollten die sonst machen?", sagt einer, der mit dem Fall befasst war.

Solche Kriminalfälle werden in Deutschland selten publik. Auch bei diesem Beispiel einer gelungenen Cybererpressung dürfen offiziell weder Mitarbeiter der bayrischen Firma noch die beteiligten Anwälte und Ermittler reden. Das eisige Schweigen rund um das Thema Computerattacken ist ein Grund, warum bei der Absicherung der Rechnerlandschaften im Mittelstand nach wie vor großer Nachholbedarf besteht.

"Bei uns doch nicht"

Dabei sind derartige Attacken weit verbreitet. Jedes elfte Unternehmen wurde bereits Opfer eines Hacker-Angriffs. Das ist ein Ergebnis einer Studie des Netzwerks Elektronischer Geschäftsverkehr (NEG), einer Förderinitiative des Bundesministeriums für Wirtschaft und Technologie. Einer Untersuchung von Symantec zufolge waren sogar drei Viertel aller Unternehmen im letzten Jahr Cyber-Attacken ausgesetzt. 43 Prozent der 2100 befragten Firmen gaben zu, vertrauliche oder unternehmenskritische Daten verloren zu haben.

Trotz solcher Zahlen ist das Thema IT-Sicherheit bei vielen deutschen Mittelständlern nach wie vor ein blinder Fleck. Anders als die großen Konzerne verfügen kleinere Firmen zugegebenermaßen nur selten über dezidierte Sicherheitsabteilungen. Doch das mangelnde Gespür für das Thema ist nicht nur eine Ressourcen- sondern auch eine Einstellungsfrage. Netzsicherheit spielt für viele kleine und mittlere Unternehmen bislang einfach keine Rolle. "Mittelständler haben per se ein weniger ausgeprägtes Sicherheitsbewusstsein, da die Unternehmensphilosophie sehr stark auf einer gewachsenen Vertrauenskultur basiert", sagt Walfried O. Sauer, Chef der Sicherheitsberatung Result Group aus Grünwald bei München. "Dies spiegelt sich vor allem in einer uns gegenüber oft getätigten Aussage: "Bei uns doch nicht...." wieder."

Mehrstufige, professionelle Attacken

Dabei ignorieren viele Unternehmenslenker, dass sie mit ihren innovativen Produkten von einem regionalen Familienbetrieb mittlerweile zu einem international tätigen Marktführer in der jeweiligen

Nische avanciert sind. Der deutsche Mittelstand ist in vielen Bereichen Weltmarktführer und Vorreiter mit Produktinnovationen.

"Da liegt es in der Natur der Sache, dass Mitbewerber versuchen, diesen Wissensvorsprung mit allen Mitteln zu kompensieren", sagt Sauer. "Durch einen verstärkten Wettbewerbsdruck lassen sie sich vermehrt zu grenzwertigen und teilweise illegalen Handlungen hinreißen, um Entwicklungskosten zu sparen, Preislisten oder Kundendaten zu erhalten und so ihre Marktanteile erhöhen."

Zum Thema

IT für den Mittelstand:

Auslagern ist
Verhandlungssache

Energiekosten: Grüne
Technik für den Mittelstand

Das Problem: Zur Absicherung gegen Hacker und Industriespione genügt es heute nicht mehr, Virens Scanner und Firewall zu installieren und sich dann zurückzulehnen. Die Angriffe heutiger Zeit sind nicht mehr einfache Virenangriffe, sondern komplexe mehrstufige Attacken, hinter denen oft professionelle Kriminelle stecken. Mal bringen Cyber-Trickser Unternehmensmitarbeiter mit einfachen Kniffen dazu, Login-Daten und Passwörter zu verraten. Mit einer einfachen E-Mail von einem Absender, der sich "Hans Frederick" nannte, täuschten Cybergangster vor kurzen etwa sieben Manager in deutschen Unternehmen, die mit Emissionsrechten handeln. "Leider gab es in allen Mitgliedsländern Angriffe auf den Emissionshandelsystem (EU ETS) Insbesondere am 07.01.2010", hieß es in einer Mail die Manager. Als Gegenmaßnahme sollten sie online einen neuen digitalen Sicherheitsschlüssel für ihre Benutzerkonten bestellen. Die Daten, die sie dabei preisgaben, nutzen die Gangster, um Emissionsrechte auf neue Konten zu übertragen und so die Firmen um Hunderttausende von Euro zu prellen.

Kein Kraut gegen Einfalt

Dann wieder schleusen die Angreifer aus dem Netz Hacker-Code auf die Firmen-Laptops, indem sie als vermeintliche virtuelle Freunde präparierte Links an die Facebook-Profile von Unternehmensmitarbeitern schicken. Vom Laptop schlüpfen die Trojaner dann beim nächsten Login des Mitarbeiters in andere Teile des Firmennetzwerks.

Gegen naive Mitarbeiter, die selbst Cybergangstern die Tore aufsperrten, ist bis heute kein Kraut gewachsen. Um so besorgniserregender ist, dass viele Mittelständler den neuen Bedrohungen völlig unvorbereitet gegenüber stehen. "Diese Sorglosigkeit spiegelt sich quer durch alle Bereiche", sagt Sauer. "Es fängt an bei der ungenügenden Vorbereitung von Mitarbeitern die ins Ausland entsandt werden, geht über die Benutzung von immer den gleichen, leicht nachvollziehbaren Passwörtern bis hin zu ungeschützten IT-Netzwerken." In 56 Prozent der Unternehmen ist nicht einmal geregelt, welche Dokumente als Geheim eingestuft werden und welche nicht, ergab eine Studie der Sicherheitsberatung Corporate Trust.

Abwehr immer auf dem neusten Stand

Doch nicht nur konzeptionell ist IT-Sicherheit viel Arbeit. Die effektive technische Abwehr von Hackerangriffen ist ebenfalls aufwendig. Bei Kuka Roboter in Augsburg etwa setzt man seit zehn Jahren Virens Scanner ein - hat aber im Laufe der Jahre noch etliche weitere Sicherheitskomponenten hin zugekauft, um 2000 Desktop-Rechner und 600 Laptops an vier Standorte plus einige Dutzend Heimarbeitsplätze gegen Computerangriffe abzuschirmen. Nur dank eines aufwendigen Mixes von Intrusion-Prevention-Software, Firewall, Geräte- und Virenschutz prallen auch hochkomplexe Angriffe ab. "Ein Virus ist bis jetzt noch nicht durchgeschlüpft", sagt Martin Kugelmann, Leiter des Bereichs IT-Infrastruktur bei Kuka. Der Preis, den Kuka zahlt, ist ein enormer Verwaltungsaufwand für den virtuellen Verteidigungsring, der mit Hilfe einer zentrale Managementsoftware auf ein erträgliches Maß heruntergefahren wird.

Viele Firmen können so einen Aufwand schlicht nicht leisten. Eine Antwort der Sicherheitssoftwarehersteller auf diese Entwicklung sind nun Lösungen, die in größerem Maße als bisher aus der Ferne betreut werden. Nur ein Teil der Sicherheitssoftwarepakete ist auf den Rechnern der Unternehmen gespeichert. Viele Produktkomponenten - etwa die Code-Bibliotheken, in denen alle Virensignaturen gespeichert sind und mit deren Hilfe ein Virens Scanner Hackersoftware erkennen kann - sind in die Netzwerke der Antivirensoftware-Hersteller ausgelagert. "Damit ist die Verwaltung solcher Programme einfacher als in der Vergangenheit", sagt Frank Schwittay, Zentraleuropachef des Sicherheitsanbieters Trend Micro in München. Auch ohne eigenen Sicherheitsexperten können Firmen so den Abwehrschirm für ihre Netze auf dem neusten Stand halten.

□

© 1999 - 2010 impulse

IHRE MEINUNG