



DENNIS
MONNER *

Eine aktuelle IDC-Befragung unter österreichischen CIOs zum Thema IT-Security legt es an den Tag: Jedes fünfte Unternehmen sah sich in den letzten zwölf Monaten über hundert virtuellen Angriffen ausgesetzt. Rund acht Attacken pro Monat, und die Professionalisierung der Täter wächst. Nicht mehr wahllos, gezielt werden sensible Daten abgeschöpft, so etwa bei finanziellen Transaktionen. Über die Hälfte der befragten IT-Leiter stuft daher die externe Gefahr durch eingeschleusten Schadcode als am höchsten für ihr Unternehmen ein. Immerhin ein Viertel sieht das größte Risiko in den eigenen Reihen: Die zunehmende Nutzung von Peer-to-Peer-Software und E-Mails öffnet zum einen Angreifern Tür und Tor, zum anderen steigt die Gefahr des Datenverlustes sensibler Daten. Unter dem Stichwort Data Leakage Prevention wird dieses Thema derzeit rege diskutiert. Hat diese bedenkliche Entwicklung eine verbessertes Sicherheitsmanagement der Unternehmen zu Folge? Leider nein. Zwar wächst das Bewusstsein, doch die Sicherheitskonzepte bleiben dürftig. Besonders in kleinen Unternehmen mit unter 250 Mitarbeitern fehlt es oft an durchdachten Security-Konzepten. Viele Entscheider tendieren dahin, ihre bestehende, oft stark heterogene IT-Landschaft punktuell mit einzelnen Sicherheitslösungen zu ergänzen. Die Sicherheit gerät strategisch wie steuerungstechnisch immer mehr außer Kontrolle, und die Lösung der eigentlich Aufgabe – nämlich die Sicherung der Geschäftsprozesse – bleibt verfehlt.

Doch mittlerweile bekommt der Mittelstand auch Druck von anderer Seite. Die Abhängigkeit geschäftlicher Erfolge von der Einhaltung gesetzlicher Vorschriften und interner Sicherheitsrichtlinien, bekannt unter dem Stichwort Compliance, wächst deutlich. Um dies zu erkennen, genügt ein Blick auf die aktuelle Entwicklung. Zum Beispiel das Regelwerk PCI DSS (Payment Card Industry Data Security Standard): Damit schreiben Kreditkartenorganisationen Händlern, welche Kreditkartentransaktionen abwickeln, detaillierte Sicherheitsrichtlinien vor, um die Transaktion vor Missbrauch zu schützen. Dies betrifft unter anderem die Kontrolle der Zugriffsrechte auf Daten und die kontinuierliche Netzwerküberwachung. Zum 29. Juni 2008 wurden die Richtlinien der Europäischen Kommission, EuroSOX, in nationales Recht umgesetzt. Sie legen für Kapitalgesellschaften Standards für transparente Rechnungslegung und Jahresabschlüsse fest. Auch hier ist die Sicherheit der IT-Infrastruktur gefragt, da ein Ausfall der EDV zu erheblichen Unternehmensschäden führen kann und somit für Aktionäre ein wichtiges Kriterium ist. Zweifelsfrei erhöhen Vorschriften dieser Art die Anforderungen an die IT enorm: Plötzlich müssen auch die kleinsten Unternehmen in E-Mail-Kontrolle und die Sammlung und Auswertung von Sicherheitsdaten investieren, um bei Bedarf dokumentieren zu können, inwieweit Controlling-, Revisions- oder rechtliche Vorgaben von den Mitarbeitern eingehalten wurden. Will man den neuen Anforderungen mit zahlreichen Einzellösungen begegnen, führt dies schnell zu einer ineffizienten Kostenfalle, die zudem keine Garantie für gesetzeskonforme Prozesse gibt.

Es ist also nicht nur im Sinne des Mittelstandes, IT-Sicherheit auf das notwendige Aufwand- und Kostenmaß zurückzuführen. Besonders für Betriebe mit kleiner IT-Mannschaft kann »Security as a Service« (SaaS) als Option interessant sein. Die zunehmende Auslagerung von Applikationen einschließlich geschäftskritischer ERP-Anwendungen verstärkt den Trend, auch den Betrieb flankierender IT-Sicherheitstechniken abzugeben. Unternehmen mit eigener IT-Mannschaft schätzen dagegen die Vorteile von Unified-Threat-Management-Appliances (UTM). Diese vereinen Hardware und alle wichtigen Software-Schutzkomponenten auf einer einzigen Plattform, was eine erhebliche Zeit- und Kostenersparnis für den Administrator bedeutet. UTM-Systeme punkten mit hochsicheren Verschlüsselungs- und umfassenden User Authentifizierungsverfahren, die den Missbrauch und Verlust sensibler Daten verhindern. Zudem erlauben Monitoring- und Reporting-Werkzeuge eine bequeme Auswertung des Nutzungsverhaltens. Analysten bestätigen den Trend: Laut IDC erzielten UTM-Anbieter im vierten Quartal 2007 die größten Umsätze auf die gesamte Security-Branche gesehen, noch vor den klassischen Firewalls. Der Quartalsumsatz wuchs im Jahresvergleich um 25 Prozent und damit deutlich stärker als das Firewall-Segment mit rund acht Prozent.

Das Thema Compliance ist für viele Unternehmen eine Chance, ihr bestehendes Sicherheitskonzept unter die Lupe zu nehmen. Bei der Betrachtung der IT-Sicherheit durch die Kosten/Nutzen-Brille sollte man jedoch über den Aspekt der direkten Einsparung hinausgehen: Wer rechtlichen Vorgaben nicht nachkommt, riskiert langfristig hohe Kosten oder gar einen Reputationsverlust. Beiden Herausforderungen – der kosteneffizienten IT-Sicherheit und mehr Transparenz bei geschäftlichen Vorgängen – können IT-Leiter mit einer UTM-Appliances umfassend begegnen.

* Dennis Monner ist Vorstandsvorsitzender von gateProtect und Leiter der Fachgruppe Netzwerksicherheit am Fraunhofer Institut für Sicherere Informationstechnik in Darmstadt. Diese Fachgruppe wiederum, der mehrere deutsche Unternehmen mit Produkten aus dem Bereich Netzwerksicherheit angehören, ist ein Teil der Initiative »IT Security Made in Germany« (ITSMIG).