trend

"trend" Nr. 6/07 vom 01.06.2007 Seite: 76 Ressort: Trend Spezial: Die Welt der Klein- und Mittelbetriebe

Peter Sempelmann

Weg sind die Daten

Spam, Viren & Co. Der Verlust wertvoller Files ist für Klein- und Mittelbetriebe eine erhebliche Bedrohung, denn auf die Katastrophe folgt oft die Pleite. Produkte von Unternehmen, die auf Datensicherung und-rettung spezialisiert sind, bieten den notwendigen Schutz.

Wer kennt und hasst sie nicht, die ungebeten eintreffenden e-Mails von völlig unbekannten Absendern, in denen bombensichere Anlagegeschäfte, wilde Sex-Abenteuer, Medikamente, Software oder Uhren zu Sensationspreisen angepriesen werden? Einer Schätzung des Messaging-Spezialisten Messagelabs zufolge waren im ersten Jahresviertel 2007 76,3 Prozent des weltweiten e-Mail-Verkehrs Spam-Mails. Eine Besserung ist nicht in Sicht, denn: "Spams sind für die Absender ein gutes Geschäft", weiß Joe Pichlmayr, Geschäftsführer der auf Internet Security und Virenschutz spezialisierten Ikarus Software AG.

Für Klein- und Mittelbetriebe kann der e-Mail-Müll dagegen schnell zu einem handfesten Problem werden. Obwohl Spam-Filter den Großteil der Nachrichten ausfiltern, geht erstens viel Arbeitszeit verloren, um hunderte Spams wieder zu löschen, zweitens verliert man dabei rasch den Überblick - immer wieder werden auch wichtige Nachrichten irrtümlich entfernt -, und drittens können Spams das e-Mail-System eines Unternehmens derart überlasten, dass am Ende gar keine Nachrichten mehr empfangen werden können.

Spam-Mails sind aber bei Weitem nicht das einzige Übel, mit dem sich Unternehmen auch aus eigenem Interesse ernsthaft auseinandersetzen müssen. Die Liste der kriminellen Aktivitäten und Bedrohungen, die mit dem Internet verbunden sind, ist lang und reicht von Datenschutzverletzungen über Kreditkartenmissbrauch, Finanzmanipulation, Betriebsspionage bis zur Datenmanipulation und womöglich sogar zu Produktionsausfällen oder Betriebsstillständen. Pichlmayr: "Trojaner, die andere Systeme ausspionieren oder kontrollieren können, sind um wohlfeile 300 Dollar zu haben - spezialisierte Modelle kosten bis zu 5000 Dollar, und 50.000 Dollar werden für geheime, also noch unbekannte Sicherheitslücken, so genannte Exploits, von Betriebssystemen oder anderen Softwareanwendungen bezahlt."

Gerade Klein- und Mittelbetriebe, die sich keine eigene IT-Abteilung leisten können, kommen da leicht unter die Räder, und - fast noch schlimmer - sie können von anderen Unternehmen auch zur Verantwortung gezogen werden, wenn sie sich nicht dem allgemeinen Standard entsprechend schützen.

Verlorene Daten. Besonders heikel ist es, dass im Zuge derartiger Angriffe wertvolle Daten unwiederbringlich verloren gehen, schlimmstenfalls droht sogar der komplette Datenverlust. Doch nur die wenigsten Klein- und Mittelbetriebe haben ihre Daten auch so gesichert, dass sie von den Backups wiederhergestellt werden können. Robert Rohrer, Technik-Chef des Grazer Unternehmens Data. Noah: "Einmannbetriebe und kleine Firmen sichern ihre Daten in der Regel gar nicht, erst KMUs ab etwa 30 Mitarbeitern tun das gelegentlich, legen dann aber oft nur alibihalber Backups auf Bändern an, die nicht sachgemäß behandelt werden und deshalb auch nicht sicher sind."

Das kann dramatische Folgen haben. 29 Prozent, also fast ein Drittel aller Unternehmen, die einen Datenverlust erleiden, müssen innerhalb von zwei Jahren zusperren, weil sie sich von dem Desaster nicht mehr erholen.

Edmund Haberbusch, Leiter Produktmanagement für Klein- und Mittelbetriebe bei der Telekom Austria, kümmert sich seit drei Jahren intensiv um die KMUs. Auch er weiß, dass es rund um das Thema Security noch viel Aufklärungsbedarf gibt - also großes Potenzial für die Anbieter von Sicherheitslösungen. "Die Notwendigkeit eines Virenschutzes und einer Firewall muss man glücklicherweise inzwischen kaum jemand mehr erklären, das Thema ist gegessen, aber über die weiteren Aspekte - Updates, Wartung, Datenaufbewahrung und Sicherung - machen sich die Unternehmen leider noch viel zu wenig Gedanken", meint Haberbusch.

Das Risiko, das die Firmen dabei eingehen, ist enorm. Ein Hardwarecrash, ein Feuer, ein Einbruch, eine Überschwemmung oder ein Anwenderfehler - und schon können wichtige Firmendaten unwiederbringlich zerstört sein. Dann bekommen die Unternehmen wirklich ernsthafte Schwierigkeiten, denn Versicherungen können zwar den entstandenen Schaden, der mit 1000 Euro pro Megabyte beziffert wird, wiedergutmachen, einmal verloren gegangene Daten aber auch nicht wieder herbeizaubern.

Mühsame Wiederherstellung. Unternehmen wie Kuert, Kroll Ontrack oder **Attingo** haben sich darauf spezialisiert, Daten von gelöschten oder beschädigten Festplatten wiederherzustellen. Kroll Ontrack gibt an, weltweit pro Jahr über 50.000 Datenwiederherstellungen durchzuführen und dabei in 90 Prozent aller Fälle Erfolg zu haben. Die Datenwiederherstellung ist jedoch nicht gerade billig. Wer möchte, dass seine Festplatte binnen 24 Stunden analysiert wird, muss schon alleine dafür 400 Euro auf den Tisch legen, und für die Wiederherstellung von Daten geben die Datenretter wohlweislich überhaupt keine Preise an. Auf der Website von Kuert (www.kuert.at) heißt es: "Der Preis für die Datenrettung kann nicht im Voraus bestimmt werden, da die dazu nötigen Informationen erst bei der Überprüfung des Datenträgers festgestellt werden. Die Kosten werden beeinflusst durch die Art der benötigten Technologien, die

Dauer der zur Lösung notwendigen Arbeit, eine eventuelle Ersatzteilbeschaffung und die von Ihnen festgelegte Frist."

Eine Garantie, dass die Daten nach einem Super-GAU wiederhergestellt werden können, gibt es natürlich nicht, und selbst wenn es möglich ist, brauchen darauf spezialisierte Unternehmen dafür Tage, was im knapp bemessenen Geschäftsalltag einer Ewigkeit und einer mittleren Katastrophe gleichkommt.

Diese Kosten und Mühen lassen sich jedoch leicht vermeiden, wenn bei der Datensicherung einige einfache Regeln beachtet werden oder wenn man einen Partner ins Boot holt, der die Datensicherung übernimmt. Eine solche, speziell auf Klein- und Mittelbetriebe zugeschnittene Methode ist die SaveBOX von Data.Noah, die vor Ort alle Daten auf einen eigenen kleinen Server schreibt, der beim Kunden steht. Über eine verschlüsselte Internetverbindung werden die Daten gleichzeitig in das Data.Noah-Rechenzentrum übertragen, wo sie ein zweites Mal gesichert werden. Das System erkennt automatisch, wenn eine Sicherung ausbleibt oder fehlerhaft ist. Müssen dann Daten oder eine frühere Version einer Datei wiederhergestellt werden, genügt ein Mausklick, und die Sache ist erledigt. Das Angebot ist für Unternehmen mit bis zu 400 Mitarbeitern geeignet und in der Einstiegsversion um 19 Euro pro Monat erhältlich.

Angreifer aus dem Internet oder Virenattacken sind im Übrigen nur selten am Datenverlust schuld. "In 28 Prozent aller Fälle sind die Ursache Bedienerfehler, und 59 Prozent aller Datenverluste werden durch Hardwaredefekte verursacht", weiß Rohrer. Computerviren würden dagegen, zumindest was den Datenverlust betreffe, in ihrer Gefährlichkeit etwas überschätzt: Sie sind nur in zwei Prozent aller Fälle für das Debakel verantwortlich.

Kompetente Partner. Die Telekom Austria steht Unternehmen ebenfalls zur Seite, wenn es um die Sicherung der Daten geht. "Die Security ist ein ganz zentrales Thema in unseren Business Solutions, und die Einstiegsschwellen dafür sind bewusst niedrig gehalten, um auch den Klein- und Mittelbetrieben entsprechende Leistungen anbieten zu können", sagt Haberbusch. Serverhousing und Hosting-Angebote, bei denen das Rechenzentrum der Telekom Austria die Server von Unternehmen betreibt, werden bereits ab 280 Euro pro Monat angeboten.

Der neueste Service im Bereich der Internet Security sind die so genannten Proxy Security Services. Dabei wird der Internetverkehr eines Unternehmens gescannt und der Zugriff auf nicht frei gegebene Web Sites mittels URL Filtering verhindert. Im Paket enthalten ist dabei unter anderem auch das Scannen und Entfernen von Viren, Trojanern, Malicious Codes, Dialer-Software, die Filterung von unerwünschten Datei-Typen und-Downloads sowie das Anlegen von Daten-Backups. Und da für die Mitarbeiter auch unterschiedliche Berechtigungsprofile angelegt werden können, ist die Lösung auch entsprechend flexibel. Haberbusch: "Wir implementieren und betreiben die für die Proxy Security Services benötigte Hard- und Software zentral rund um die Uhr als dedizierte Instanz für jeden einzelnen Kunden."

Komplexe Frage. "Obwohl die Probleme, die auf ein Unternehmen zukommen können, sehr wohl bekannt sind, beschäftigen sich die KMUs aber immer noch zu wenig mit ihrer eigenen Sicherheit", beklagt Gerhard Göschl, Plattform-Strategie-Manager und Sicherheitssprecher von Microsoft Österreich. Mit Schuld daran sei, dass der heutige Markt für Sicherheits-produkte komplex und fragmentiert ist. In eigenen, in Kooperation mit der Wirtschaftskammer Österreich veranstalteten Roadshows bemüht sich Microsoft, den Unternehmen die Notwendigkeit zum Schutz näherzubringen, doch der Erfolg stellt sich nur langsam ein.

Schuld daran ist, wie der Microsoft-Mann selbst zugibt, dass das Thema Netzwerksicherheit immer noch schwierig umzusetzen, zu nutzen sowie zu verwalten ist. Obendrein fallen dann auch noch Kosten an - gerade für die Klein- und Kleinstbetriebe sind das mehr als genug Gründe, um eine Entscheidung oft so lange vor sich herzuschieben, bis der Ernstfall auch schon eingetreten ist. Göschl: "Das liegt an der schlechten Interoperabilität der verschiedenen Produkte, an den separaten Verwaltungskonsolen für einzelne Lösungen und einem allgemeinen Mangel an einheitlichen Reporting- und Analysewerkzeugen. Der Großteil der Unternehmen weiß daher überhaupt nicht, ob er angegriffen wird."

Mit der Forefront-Produktfamilie macht Microsoft das Thema Security für Unternehmer leichter verwaltbar. Die Lösung bietet einen einheitlichen, einfach zu verwaltenden und zu überwachenden Schutz gegen Schadsoftware für Unternehmens-Desktops und Lap-tops sowie Serverbetriebs-systeme und lässt sich, was besonders wichtig ist, einfach mit anderen Sicherheitslösungen für Unternehmen kombinieren. "Forefront ist eine zentrale Komponente unserer Strate-gie, Unternehmenskunden eine End-to-end-Sicherheitslösung anzubieten", erklärt Göschl.

Schlussendlich werde auch dafür gesorgt, dass der notwendige Schutz selbst dann gewährleistet ist, wenn Dokumente oder Datenträger in die Hände nicht autorisierter Personen fallen, und das sei, so Göschl, gar nicht so selten: "Mitarbeiter verlieren ihre Memorysticks mit darauf gespeicherten Daten oder gleich ihr ganzes Notebook. In London werden pro Jahr etwa 6000 Laptops in Taxis vergessen."

"Wichtig ist, dass man das Thema Security nicht nur von seiner technischen Seite sieht, sondern auch die Probleme angreift, die durch die Benutzer entstehen", meint Christoph Riesenfelder, Security & Privacy Consultant, IBM Österreich, "wir sehen zwar, dass Internet-Kriminalität zunehmend zu einem organisierten Geschäftszweig wird und potenzielle Bedrohungen immer schwieriger zu entdecken sind. Viele Probleme lassen sich aber vermeiden, wenn sich in einem Unternehmen alle der Problematik bewusst sind und die wertvollen Daten auch entsprechend geschützt und gesichert werden."

Bild: Sondermüll. "Die Absender machen mit Spam-Mails gute Geschäfte." Joe Pichlmayr, Ikarus Software AG
Bild: Sorglos. "Die Unternehmen machen sich immer noch zu wenig

Gedanken." Edmund Haberbusch, Telekom Austria
Bild: "Security ist nicht nur ein technisches Problem." Christoph Riesenfelder, IBM