

FACTS

Das Test- und Wirtschaftsmagazin fürs moderne Büro

E-MAIL-PROGRAMME

Alternativen zu MS-Outlook

Seite 58

FAXEN FÜR PROFIS

**Alle Lasergeräte und Kosten
im Überblick**

Seite 10

Viele Funktionen, ein Gehäuse:

13 MULTIFUNKTIONS- GERÄTE IM TEST

Seite 20

IT-SICHERHEIT

**Keine Chance für Viren,
Würmer und Datenklau**

ab Seite 42

Keine Chance



... für Viren, Würmer und Datenklau

IT-Sicherheit ist eines der wichtigsten Themen der heutigen Zeit. In der digitalisierten Welt hat eine störungsfrei funktionierende IT-Landschaft für Unternehmen oberste Priorität.

Mehr als 72 Prozent aller Unternehmen und Organisationen in Europa betrachten die IT-Sicherheit als Kernthema unter den betrieblichen Prozessen. Aus gutem Grund: Allein im Jahr 2003 belief sich die Zahl der weltweit aufgetretenen IT-Störfälle auf rund 700 Millionen, meldete der Marktreport des IT-Dienstleisters Nextiraone. Die Art der Bedrohung ist dabei so vielfältig wie nie zuvor. Gefahr lauert sowohl außerhalb als auch innerhalb des Unternehmens.

FACTS zeigt auf den folgenden Seiten, was Unternehmen beachten müssen, um Daten bestmöglich zu schützen.

Der Feind ist überall

Die größte Gefahr lauert nach wie vor im „World Wide Web“. Hier prasseln täglich hunderte von neuen Viren, Würmern und Trojanern auf die Anwender nieder (siehe Seite 44). Hinzu kommt die stetig steigende Zahl von so genannten Spam-E-Mails (Müll-Mails), die die E-Mail-Server auf der ganzen Welt an die Grenzen ihrer Belastbarkeit führen.

Doch auch die Zahl der innerhalb der Betriebssysteme entdeckten Sicherheitslücken wächst stetig. Für Hacker ist es mittlerweile zum Sport geworden neue Lücken in Microsoft Windows zu finden und die Nutzer mit unsinnigen Attacken zu nerven. Im schlimmsten Fall bleibt es dabei nicht beim Nerven, sondern endet mit dem Diebstahl oder der Zerstörung sensibler Daten.

Datenklau spielt auch beim Thema Wireless LAN (WLAN) eine große Rolle: Noch immer nutzen Anwender das drahtlose Netzwerk ohne eine adäquate Verschlüsselung (siehe Seite 48). Die Folge: Mit legal erhältlicher Software kann sich jedermann innerhalb weniger Sekunden in das Funknetz einwählen und herumwüten. Im harmlosesten Fall surft er auf

Kosten des Unternehmens im Netz. Im schlimmsten Fall klaut oder vernichtet er komplette Datensätze. Und ausgesprochene Scherzbolde bestellen gerne mal in fremdem Namen einen neuen Porsche oder eine Millionenjacht.

Äußerst beliebt ist in letzter Zeit auch das so genannte Phishing (Passwort fischen). Dabei versuchen Betrüger mit täuschend echt wirkenden E-Mails etwa an Zugangsdaten für das Online-Banking zu kommen. Der Empfänger wird aufgefordert einen Link anzuklicken, der ihn auf die vermeintlich offizielle Internetseite der Bank bringt. Dort wird der Benutzer dann in einem Formular aufgefordert, seine Kontonummer mit dazugehöriger PIN mit einer Transaktionsnummer zu bestätigen. Die so gesammelten Daten nutzen die Betrüger, um fremde Bankkonten zu plündern.

Doch nicht nur von außen droht Unternehmen Ungemach. Datenangriffe drohen auch aus den eigenen Reihen (siehe Seite 54). Durch fingergroße USB-Sticks etwa, die in jede Hosentasche passen, ist es jedem Mitarbeiter möglich, schnell und unauffällig wichtige Kundendaten zu kopieren. Und selbst wenn die Angestellten dem Chef wohlgesonnen sind: Kein Mensch ist davor gefeit, aus Versehen auf den falschen Knopf zu drücken. Unter Umständen verschwinden so für Ihr Unternehmen lebenswichtige Daten (siehe Seite 52).

Schadensbegrenzung

Nur wer den Feind kennt, kann ihn erfolgreich bekämpfen. Dabei steht leider bereits von vornherein fest: 100-prozentigen Schutz gibt es selbst in der IT-Welt nicht. Dennoch gehen Unternehmen in keinen aussichtslosen Kampf. Denn mit passender Software und richtigen IT-Lösungen können sie die Risiken zumindest effektiv minimieren.

Robert Sopella

FACTS-TIPP

KONTROLLE, JA – ABER LEGAL!

IT-Sicherheit ist nicht ausschließlich ein technisches Thema. Wenn es darum geht, interne Gefahrenquellen auszuschließen, sind oftmals Arbeits- oder Datenschutz-Gesetze zu beachten. So unterliegen viele Unternehmer noch immer dem Trugschluss, sie könnten jegliche Aktivität der Angestellten im Internet überwachen und auswerten. Auch das Mitlesen der E-Mails ihrer Angestellten betrachten viele Chefs als selbstverständlich. Sie verstoßen damit allerdings gegen geltendes Recht.

Rechtlich ist das Feld der IT-Sicherheit mit Hunderten solcher kleinen Fallen versehen. Im Einzelfall drohen Firmenlenkern sogar Haftstrafen. Der IT-Dienstleister Blue Coat Systems hat nun in Zusammenarbeit mit dem Rechtsanwalt Horst Speichert einen Leitfaden herausgebracht, der die versteckten Fallen aufdeckt.

Die Broschüre behandelt die Themen private Internetnutzung und private E-Mails, rechtskonforme Archivierung von E-Mails sowie Haftung des Unternehmens oder der Geschäftsleitung. Der Ratgeber beschränkt sich nicht nur auf die rechtliche Darstellung, sondern liefert nützliche Praxistipps. Als besonderen Service enthält er eine umfassende Checkliste. Wenn Unternehmer diese an Bluecoat faxen, erhalten im Gegenzug eine kostenlose und unverbindliche erste Analyse ihrer individuellen Sicherheits-Situation.

Der Ratgeber steht unter:
[www.bluecoat.de/leitfaden/
checkliste.htm](http://www.bluecoat.de/leitfaden/checkliste.htm) kostenlos zum Download bereit. (sop)

Virenplage im Anmarsch

Virenschreiber beschränken sich längst nicht mehr auf Schadprogramme für PCs. Inzwischen haben Hacker auch mobile Endgeräte ins Visier genommen.

Den Anfang machte „Brain“. Der erste PC-Virus kam 1986 aus Pakistan. Brain war ein so genannter Boot-Virus – er nistete sich im Boot-Sektor eines Rechners ein. Ein Jahr später sorgte eine noch bösartigere Variante, der „Lehigh-Virus“, weltweit für Aufsehen. Er war das erste Schadprogramm, das die „command.com“ befiel. Damals konnte noch niemand ahnen, dass sich Computerviren zur größten Plage der IT-Welt entwickeln würden.

In den 80ern tauchten in jedem Jahr ein bis maximal zwei neue Computerviren auf. Die meisten waren jedoch noch relativ harmlos und verursachten keine nennenswerten Schäden. Doch die Bedrohung wurde von Jahr zu Jahr schlimmer und vielfältiger. Heute erblicken täglich (!) rund 50 neue Virusvarianten das Licht der IT-Welt. So registrierten die Sicherheitsexperten im ersten Halbjahr 2004 bereits genauso viele Viren, Würmer, Trojaner und sonstige Schadprogramme wie im gesamten Jahr 2003. Tendenz steigend.

Sogar mobile Endgeräte wie PDAs geraten mehr und mehr ins Visier der Hackergemeinde. „Die Anwender mobiler Geräte befinden sich in realer Gefahr“, konstatiert der Antivirus-Experte Eugene Kaspersky. Er rechnet damit, dass sich die Virenschreiber im laufenden Jahr auf Viren für mobile Geräte konzentrieren werden.

Ein erster Virus, der die Betriebssysteme „Windows mobile“ und „Windows CE“ angreift, ist mit „WinCE.Brador.a“ bereits gefunden. „Das alles erinnert stark an die Evolution von Viren für PCs und könnte bald zu Epidemien für mobile Geräte führen“, befürchtet Kaspersky.

Was das für wirtschaftliche Schäden mit sich bringen wird, möchte sich niemand so recht vorstellen. Schon jetzt verursachen Virenattacken auf Desktop-Systeme und Server Jahr für Jahr allein in Deutschland einen Schaden in dreistelliger Millionenhöhe. Und das, obwohl ein Großteil der Unternehmen angibt, eine Antivirus-Software einzusetzen.

Lücken schließen

Doch die beste Antivirus-Software nutzt nichts, wenn sie nicht regel-



Eugene Kaspersky: Der Antivirus-Experte befürchtet Virenepidemien für mobile Endgeräte.

mäßig gewartet wird. Wird beispielsweise die Virendefinitions-Datei nicht regelmäßig aktualisiert, fahndet das Programm lediglich nach „alten“ Schadprogrammen. Die Folge: Neue Viren, Würmer oder Trojaner gelangen unbehelligt ins System, weil die Antivirus-Software sie schlicht und einfach nicht identifizieren kann.

Eine große Gefahr geht zudem von unbedarften Anwendern aus, da sich die neuartigen Schadprogramme immer raffinierter in scheinbar harmlosen Dateien verstecken. Der Versuchung des Computerwurms „VB.SST@mm“ konnten 2001 vor allem männliche Kollegen nicht widerstehen. Grund: Der PC-Schädling tarnte sich als Bilddatei „Anna Kournikova.jpg“. Den Dateizusatz „vbs“ – ein untrügliches Zeichen für einen Virus – übersahen die Männer vor lauter Aufregung und klickten munter drauflos.

Doch selbst für ganz Vorsichtige besteht eine bittere Gewissheit: Im schlimmsten Fall leisten alle Sicherheitsmaßnahmen nur Schadensbegrenzung. Selbst ein auf dem neuesten Stand gehaltenes Abwehr-System und hoch sensibilisierte Mitarbeiter bieten bestenfalls eine 99-prozentige Sicherheit. Kleine Schlupflöcher wird es immer geben, genauso wie Schadprogramme, die diese Löcher schamlos ausnutzen.

Robert Sopella

VIRENKILLER FÜR IHR UNTERNEHMEN

Es gibt unzählige Antivirus-Programme auf dem Markt. Viren erkennen und beseitigen kann jedes dieser Programme. Was die Software darüber hinaus leistet, sagt FACTS in dieser Übersicht.

Symantec AntiVirus Corporate Edition 9.0

Symantec hat mit seiner AntiVirus Corporate Edition 9.0 großen Wert auf sichereren E-Mail-Verkehr gelegt. Die heuristische Technologie für die Wurm-erkennung erkennt bössartige Programme und verhindert, dass Client-Systeme Würmer per E-Mail verbreiten. Auch unbekannte Viren werden von Symantecs „BloodHound“ (frei übersetzt: Jagdhund) aufgespürt. BloodHound vergleicht dabei die Systemaktivität mit bekannten virentypischen Verhaltensmustern. Laut Symantec erkennt BloodHound bis zu 90 Prozent aller neuen Makroviren und bis zu 80 Prozent aller neuen und unbekanntenen Programmdateiviren. Weitere Informationen: www.symantec.de

McAfee VirusScan Enterprise 8.0i

McAfee VirusScan Enterprise 8.0i ist eine „proaktive“ Virenschutz-Lösung. Im Gegensatz zu reaktiven Sicherheits-Programmen soll die Software von vornherein verhindern, dass neue Viren in das System gelangen. Reaktive Programme reagieren dagegen erst, wenn die Schadprogramme bereits bekannt und im System sind. Mit Hilfe von VirusScan Enterprise 8.0i können Administratoren beispielsweise bestimmte Ports für ein- oder ausgehenden Netzwerkverkehr blockieren. Das Filtern von eingehendem Netzwerkverkehr führt zu einer verringerten Anfälligkeit gegen Würmer und Hacker. Das Sperren unbenutzter Ports verhindert zudem das Ausspähen von Schwachstellen im Betriebssystem und in den Anwendungen. Weitere Informationen: www.mcafee.de

Kaspersky Anti-Virus Corporate Suite

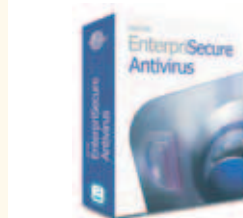
Die Kaspersky Anti-Virus Corporate Suite läuft auf allen gängigen Software-Plattformen und ist für Unternehmens-Netzwerke jeder Größe geeignet. Die Antiviren-Datenbanken werden dreistündlich aktualisiert. Der Office Guard sorgt für umfassenden Schutz gegen Makroviren. Der Script Checker fängt Scriptviren durch eine heuristische Code-Analyse ab. Die Software enthält zudem einen umfangreichen E-Mail-Schutz. Die Nachrichten werden beim Erhalt, beim Senden sowie beim Leseversuch samt Inhalt und Anlagen überprüft. Weitere Informationen: www.kaspersky.de

Panda EnterpriSecure

EnterpriSecure von Panda Software beinhaltet eine Antivirentechnik, die den kompletten TCP/IP-Traffic überwacht und somit eine sichere Internetverbindung ermöglicht. CVP Secure wurde beispielsweise entwickelt, um schädliche Codes direkt an der Firewall zu löschen. Zudem schützt die Software alle gängigen E-Mail-Programme vor Schadprogrammen aller Art. Eine Anti-Spam-Lösung ist ebenfalls integriert. Weitere Informationen: www.pandasoftware.de

GData AntiVirenKit professional 2005

Die 2005er-Version des AntiVirenKit (AVK) von GData arbeitet mit einer DoubleScan-Technologie. Zwei Virenschutz-Module sorgen für eine gründlichere Virenerkennung. GData greift dabei auf die Scan-Module von Kaspersky und BitDefender zurück. Integriert ist zudem ein Anti-Dialer-Modul und ein E-Mail-Virenblocker für Outlook, Outlook Express, Exchange, Mozilla, Eudora und weitere POP3- und IMAP-basierte Mail-Clients. Der AVK-Security Agent meldet Updates und Viren-News sofort, wenn sie verfügbar sind. Ein Virenlexikon, das auch offline verfügbar ist, gibt zusätzliche Hilfestellung beim Kampf gegen die ungebetenen elektronischen Eindringlinge. Weitere Informationen: www.gdata.de



PRAXISBERICHT: SPAM- UND VIRENSCHUTZ AN DER UNI

Die Carl von Ossietzky Universität in Oldenburg setzt bei der Viren- und Spam-Bekämpfung auf Sophos.

Die Carl von Ossietzky Universität gehört zu den jungen Hochschulen Deutschlands. Wahrscheinlich hat sie sich gerade deshalb die Offenheit bewahrt, neue Herausforderungen anzunehmen. So hat sie etwa bereits 1984 das Fach Informatik in den festen Studienplan aufgenommen. Auch beim Spam- und Virenschutz ist die Universität innovativ und freudig. System-Administrator Jürgen Weiß hat sich beispielsweise in Vorträgen mit dem Thema beschäftigt. Daher hatte er ganz genaue Vorstellungen davon, was eine Security-Lösung leisten sollte.

Die Ausgangsphase

Die Universität Oldenburg bietet Lehrenden, Angestellten und Studierenden modernste Kommunikations-Möglichkeiten. Dazu gehören auch E-Mail-Accounts, die vom Hochschulrechenzentrum bereitgestellt werden. Das Universitäts-Netzwerk verfügt über mehr als 14.000 Mailboxen auf zwei E-Mail-Servern. Diese verarbeiten durchschnittlich 125.000 E-Mails pro Tag. Rund 80 Prozent davon sind Spam. Die unerwünschten Massen-Mails führten zu zahlreichen Beschwerden der E-Mail-Nutzer. Gründe dafür waren nicht nur die große Menge, sondern auch die sexistischen Inhalte vieler Spam-Mails. Um die E-Mail-Nutzer davor zu schützen, setzte die Universität zunächst einen kostenlosen Open-Source-Spamschutz ein. Dieser stieß auf Grund der Masse an Spam jedoch schnell an seine Grenzen.

Die Bestandsaufnahme

Schon seit 2000 läuft Sophos Anti-Virus sehr erfolgreich auf 800 Desktops und 50 File-Servern der Universität. Ein Test der dazu

passenden Gateway-Lösung lag somit nahe. In Zusammenarbeit mit Peter Böhm von der novirdata GmbH wurde die Evaluierung von Sophos PureMessage vorbereitet. Der Geschäftsführer des Value Added Distributors von Sophos stand der Universität in allen Fragen rund um das Programm zur Seite.

Die Anforderungen

Mit der neuen Gateway-Lösung wollte Jürgen Weiß nicht nur das enorme Spam-Aufkommen in den Griff bekommen. Die Software musste auch bestmöglichen Virenschutz bieten. Neben sicherem Spam- und Virenschutz sollte das Filtern der Mails für den Nutzer transparent sein. Der Einsatz von PureMessage hing auch von der Zustimmung des Datenschutzbeauftragten ab. Es musste also möglich sein, den Schutz vor Spam mit dem Schutz der Privatsphäre der E-Mail-Nutzer in Einklang zu bringen.

Aus diesem Grund war Jürgen Weiß auch am Extended-Policy-Management interessiert. Das PureMessage-Modul bietet in dieser Hinsicht flexible Konfigurations-Möglichkeiten, mit denen universitätseigene E-Mail-Richtlinien festgelegt werden konnten. Dass die IT-Lösung zudem stabil arbeiten und sich in ein Hochverfügbarkeits-Konzept integrieren lassen sollte, war eine Selbstverständlichkeit.

Die Testphase

Schon nach zwei Monaten war die Testphase abgeschlossen. „Nach unseren Recherchen gab es keine vergleichbare kombinierte Antispam- und Antiviren-Lösung am Markt. Die Entscheidung fiel allerdings auch deshalb schnell zu Gunsten von Sophos, da Sophos Anti-Virus bereits im Windows-Umfeld unser Standard war“, fasst Jürgen Weiß das Testergebnis zusammen. Auch die zeitnahen

automatischen Updates sprachen aus Weiß' Sicht für PureMessage. Hintergrund: Viele Spam-Mails gehen in Oldenburg zwischen zwei und vier Uhr morgens ein. Dank der automatischen Updates ist das Netzwerk nun aber auch nachts optimal geschützt. Ein weiterer Pluspunkt: Die einfache Administration der Software. „Alle administrativen Aufgaben sind auch im Kommando-Line-Modus durchführbar“, sagt Weiß. Den Zeitaufwand für Administration beziffert er mit durchschnittlich rund vier Stunden pro Woche.

Die Installation

Das Produktsystem wurde in zwei Tagen installiert. Daran beteiligt war je ein Mitarbeiter von Sophos und der Universität. PureMessage läuft seitdem sehr stabil und zeichnet sich durch hohe Erkennungsraten aus. Dabei werden Mails ab 90 Prozent Spam-Wahrscheinlichkeit in Quarantäne verschoben und nach 30 Tagen gelöscht. Mails ab 50 Prozent Spam-Wahrscheinlichkeit werden in Header und Betreff gekennzeichnet und in einem speziellen Ordner des Empfängers abgelegt. Mails mit einer Spam-Wahrscheinlichkeit bis 50 Prozent werden direkt zugestellt.

Die ersten Erfahrungen

Nach der Einführung in Oldenburg kam es auf Empfehlung der Universität zum Abschluss einer Landeslizenz. Fast alle niedersächsischen Hochschulen verlassen sich damit auf den Spam- und Virenschutz von Sophos. Die Landeslizenz bringt nicht nur Kosteneinsparung. „Eine einheitliche Software-Landschaft erleichtert bei der engen Verzahnung der Hochschulen den Datenaustausch und ist ein guter Schritt zu einheitlichen Richtlinien bei der Viren- und Spam-Abwehr“, kommentiert Jürgen Weiß.

FAKTEN

Organisation:	Universität Oldenburg
Mailboxen:	14.200
Produkt:	PureMessage (Sophos) für Unix
Module:	Anti-Spam, Anti-Virus und Extended-Policy-Management
Netzwerk:	50 Windows-Server mit 800 Clients, 25 Linux-Server, zwei E-Mail-Server
Volumen:	125.000 E-Mails pro Tag
IT-Partner:	novirdata GmbH, Schönberg



Weitgehend spam- und virenfrei: Die Carl von Ossietzky Universität in Oldenburg.



Ungebetener Gast

Drahtlose Netze sind beliebt. Viele Nutzer vernachlässigen jedoch einfachste Sicherheitsregeln.

Nutzen Sie in Ihrem Unternehmen auch die unbegrenzten Möglichkeiten drahtloser Kommunikation? Gehören Bluetooth und Wireless-LAN (WLAN) zu Ihrem täglichen Geschäft? Oder planen Sie in nächster Zeit die Einrichtung eines Funknetzes? Dann steht vielleicht in nächster Zeit ein Porsche vor Ihrer Tür. Ob Sie wollen oder nicht. So erging es zumindest einem 39-jährigen Geschäftsmann aus Hagen. Einem so genannten „War-Driver“ (siehe Kasten) war es gelungen, über das Firmennetz im Internet zu surfen. Flugs loggte sich der ungebetene Gast über die „geborgte“ IP-Adresse des ahnungslosen Hagens bei einem Internet-Auktionshaus ein und ersteigerte die Nobelkarosse aus reiner Gaudi für schlappe 50.000 Euro.

Offensichtlich hatte der Hagener Unternehmer das frisch installierte WLAN nicht ausreichend gegen unbefugten Zugriff von außen geschützt. Dabei hätte er seinen unfreiwilligen Porsche-Kauf mit ganz einfachen Mitteln und mit wenig Aufwand verhindern können. Das Problembewusstsein beim Thema WLAN

scheint aber nicht nur bei ihm, sondern auch bei der breiten Masse nicht sonderlich ausgeprägt zu sein. Der FACTS-Praxistest (siehe Kasten) hat gezeigt: Fast die Hälfte der entdeckten Funknetze sind löchrig.

Erst die Arbeit...

Sicherheitsrisiken bringen WLAN-Komponenten bereits mit, wenn sie beim Nutzer eintreffen. Die Hersteller liefern die Systeme in der Standardeinstellung aus – jegliche Sicherheitseinstellung fehlt. Das Prinzip „Plug and Play“ (frei übersetzt: anschließen und loslegen) beschert den Anwendern damit ein Funknetz, in das sich jedermann problemlos einwählen kann. Bevor ein Unternehmen WLAN in Betrieb nimmt, sollten die IT-Experten sich also zunächst mit der Administration vertraut machen und zumindest einige Grundsicherungen aktivieren. Dazu gehört vor allem die so genannte WEP-Verschlüsselung. Diese sollte unbedingt eingeschaltet sein – wenn möglich mit 128 Bit. WEP schützt zwar nicht grundsätzlich vor ungebetenen Gästen. Allerdings ist der zeitliche Auf-

FACTS-TIPP

So sichern Sie Ihr Funknetz

1. Prüfen Sie, ob ein WLAN überhaupt Sinn macht. Stellen Sie im Zweifelsfall eine Kabelverbindung her.
2. Schalten Sie die WEP-Verschlüsselung ein – wenn möglich mit 128 Bit.
3. Führen Sie eine MAC-Adressen-Zugriffsliste.
4. Schalten Sie das SSID-Broadcasting aus. Geben Sie Ihrem Netzwerk eine neutrale SSID. Verwenden Sie keinesfalls Ihren Firmennamen.
5. Schützen Sie die Access Points durch neue, regelmäßig geänderte Usernamen und Passwörter.
6. Schalten Sie die Access Points ab, wenn Sie nicht benötigt werden. Das spart Strom und liefert zudem keine Angriffsmöglichkeit.
7. Schützen Sie die Notebooks, die auf das WLAN zugreifen, mit einer Personal Firewall.

wand, den Schlüssel zu knacken, wesentlich größer. Diese Mühe wird sich kein War-Driver machen.

Auch die Einrichtung einer MAC-Adressen-Liste macht WLAN sicherer. Jede Netzwerkkarte verfügt über eine eindeutige Hardware-Kennung, die so genannte MAC (Media-Access-Control)-Adresse. Ist solch eine Liste angelegt, fragt der Access Point bei jedem Einwahlversuch die MAC-Adresse ab. Stimmt sie nicht mit den in der Liste aufgeführten Adressen überein, wird der Zugang zum Netz verweigert. Diese Methode bietet sich allerdings nur bei WLANs an, die von wenigen externen Geräten fre-

quentiert werden. Denn die MAC-Adressen müssen von Hand eingepflegt werden.

Darüber hinaus sollte jedes WLAN einen Namen erhalten („SSID“). Dieser eingetragene Name wird bei jedem Zugriffsversuch geprüft. Nur Teilnehmer mit der gleichen SSID können so auf das Funknetz zugreifen. Als SSID eignet sich jede beliebige neutrale Bezeichnung. Doch Vorsicht: Der Firmenname oder schlicht die Bezeichnung „WLAN“ ist für ungebetene Gäste kein ausreichendes Hindernis. Mobile Geräte wie zum Beispiel Notebooks, die auf das Funknetz zugreifen, sollten zudem

mit einer Personal Firewall geschützt sein.

Insgesamt betrachtet sind herkömmliche Kabelverbindungen zum jetzigen Zeitpunkt noch wesentlich sicherer als drahtlose Kommunikation. Wer daher derzeit noch darüber nachdenkt, WLAN einzusetzen, sollte genau prüfen, ob er drahtlose Kommunikation in seinem Unternehmen wirklich benötigt.

Der Geschäftsmann aus Hagen hatte noch mal Glück. Er muss künftig nicht wider Willen Porsche fahren. Das Auktionshaus verzichtete auf den Vollzug des Kaufvertrags.

Robert Sopella

PRAXISTEST: WAR-DRIVING IN DÜSSELDORF

Drahtlose Netzwerke (WLAN) werden vermehrt auch geschäftlich eingesetzt. Wer sein WLAN allerdings nicht ausreichend schützt, lädt so genannte War-Driver zum Surfen im Firmennetzwerk ein. War-Driver spüren gezielt ungeschützte WLANs auf. Einer fährt, der andere steigt mit modernster Technik ausgerüstet auf der Beifahrerseite eines normalen Pkw ein. Die klassische Ausrüstung der Netzspione besteht aus einem Notebook mit externer WLAN-Antenne und einem GPS-Empfänger.

In jedem Auto, das an Firmengebäuden vorbeifährt, könnte ein War-Driver sitzen. Doch offensichtlich sind sich nur wenige WLAN-Nutzer der verborgenen Gefahren bewusst. FACTS hat die Probe aufs Exempel gemacht.

Als Zielort haben wir Düsseldorf ausgewählt. Dort sind wir rund eine Stunde lang durch die Stadt gefahren. Unsere War-Driving-Ausrüstung bestand aus einem „Intel Centrino“-Notebook und zwei Open-Source-Programmen. Die Software haben wir ohne große Mühe innerhalb weniger Minuten im Internet gefunden.

Das Ergebnis ist schockierend: Wir bekamen insgesamt 350 drahtlose Netzwerke auf den Schirm. Fast die Hälfte war nicht mit einer WEP-Verschlüsselung versehen. Das heißt: Hätten wir es darauf angelegt, hätten wir in rund 170 Netzwerken herumstöbern, im Internet surfen oder sonstiges Schindluder treiben können. (p)

Typisches Bild: 14 von 23 WLANs sind ungeschützt. Das Y in der Spalte „WEP“ zeigt an, dass ein drahtloses Netzwerk mit einem WEP-Key geschützt ist.

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Intersect
	00:AO:C3:54	latscher	Y	Fri Dec 17 09:45:50 2004 00:00:00	6	3	0	0	
	00:09:5E:C4	IS.apel	Y	Fri Dec 17 09:46:01 2004 00:00:00	6	8	0	0	
	00:90:4E:17		Y	Fri Dec 17 09:46:03 2004 00:00:00	6	1	0	0	
	00:30:F1:81	WLAN	N	Fri Dec 17 09:46:09 2004 00:00:00	11	7	0	0	
	00:30:F1:81	WLAN	N	Fri Dec 17 09:47:15 2004 00:00:00	11	80	0	0	
	00:0F:F7:00	T-Mobile_T-Com	N	Fri Dec 17 09:46:23 2004 00:00:00	1	2	0	0	
	00:30:F1:F4	lNet	Y	Fri Dec 17 09:47:25 2004 00:00:00	2	17	0	0	
	00:09:5E:3E	carosolico	Y	Fri Dec 17 09:47:15 2004 00:00:00	11	1	0	0	
	00:04:E2:AD	Sommer	Y	Fri Dec 17 09:47:18 2004 00:00:00	2	2	0	0	
	00:09:5E:20	Wielros	N	Fri Dec 17 09:47:25 2004 00:00:00	10	6	0	0	
	00:90:4E:25	default	Y	Fri Dec 17 09:47:28 2004 00:00:00	6	2	0	0	
	00:30:F1:06	WLAN	N	Fri Dec 17 09:47:33 2004 00:00:00	11	7	0	0	
	00:30:A8:23	SASCHA	N	Fri Dec 17 09:47:54 2004 00:00:00	11	6	0	0	
	00:90:4E:1E	Zahaus	Y	Fri Dec 17 09:47:56 2004 00:00:00	6	1	0	0	
	00:1E:83:02	ConnectionPoint	Y	Fri Dec 17 09:48:06 2004 00:00:00	10	7	0	0	
	00:0D:88:C1	default	Y	Fri Dec 17 09:48:07 2004 00:00:00	6	2	0	0	
	00:09:5E:83	NETGEAR	N	Fri Dec 17 09:48:15 2004 00:00:00	11	17	0	0	

Mit Tunnel und Feuerwand

Sobald eine Verbindung zwischen Firmennetzwerk und Außenwelt besteht, haben Hacker ein leichtes Spiel. Unternehmen müssen ihre Schaltzentrale vor unbefugten Zugriffen schützen.

Das Herz eines Unternehmens ist das Netzwerk. Hier laufen alle Fäden zusammen. Sämtliche Daten, auf die die Mitarbeiter zugreifen müssen, sind hier wohl behütet abgelegt. Dort bleiben sie grundsätzlich auch. Dass ein bössartiger Mitarbeiter das Netzwerk mit eingeschleusten Schadprogrammen attackiert, ist eher die Ausnahme.

Sobald jedoch eine Verbindung zur Außenwelt besteht, zum Beispiel ins Internet, bietet die heile Datenwelt riesige Angriffsflächen. Hacker können blitzschnell Lücken im Netzwerk ausfindig machen und ungehindert in den Firmeninterna herumstöbern. Die Folgen sind fatal: Mitbewerber könnten wichtige Dokumente stehlen, eingeschleuste Schad-Software das Netzwerk für Stunden oder Tage lahm legen.

Unbefugter Zugriff

Eine vom FBI und dem Computer Security Institute durchgeführte Umfrage präzisiert das Ausmaß der Bedrohung. 85 Prozent der befragten Unternehmen gaben an, dass sie in den vergangenen zwölf Monaten Hackerangriffen ausgesetzt waren. 64 Prozent von ihnen erlitten dabei fi-

nanzielle Verluste. In sage und schreibe 70 Prozent der Fälle war die Verbindung zum Internet der Angriffspunkt. Die Unternehmens-Schaltzentrale vor unbefugten Zu-

WER BENÖTIGT WELCHE FIREWALL

Kleine Unternehmen

Kleinere Betriebe haben im Allgemeinen weniger als 50 Mitarbeiter, die oft nur in einem einzigen Gebäude untergebracht sind. Beispiele für solche Unternehmen sind Wirtschaftsprüfer, Anwaltskanzleien, Arztpraxen oder Beraterfirmen. Sie beschäftigen selbst meist keine IT- oder Sicherheitsexperten. Daher benötigen sie einfache, leicht installierbare und administrierbare Lösungen. Firewalls, die automatisch installiert werden, sind in diesem Fall zu empfehlen. Falls im Unternehmen kein Mitarbeiter über das erforderliche Fachwissen verfügt, ist Outsourcing der Installations- und Sicherheits-Services eine Alternative.

Mittelgroße Unternehmen

Mittlere Unternehmen beschäftigen 500 bis 5.000 Mitarbeiter, die häufig über mehrere Gebäude verteilt sind. Die Installation und Administration eines Firewall-Systems kann hier schon etwas anspruchsvoller sein. In Unternehmen dieser Größe sind zu meist ein oder mehrere Mitarbeiter beschäftigt, die über grundlegende Sicherheitskenntnisse verfügen und anfallende Netzwerkaufgaben erledigen. Es ist besonders wichtig, dass Firewall-Lösungen für diese Unternehmen Kriterien wie Zertifizierung, hervorragende Beurteilungen und Auszeichnungen erfüllen. Falls zu dem Unternehmen einige kleinere Niederlassungen gehören, ist eine einfache Implementierung und Fernverwaltung ebenfalls entscheidend. Zudem sollte über eine VPN-Funktionalität nachgedacht werden, mit der sich sichere und einfach zu verwaltende Verbindungen für den Fernzugriff einrichten lassen.



griffen von außen ausreichend abzuschirmen, ist demnach dringend notwendig.

Grundabsicherung

So sollte das Netzwerk mindestens mit einer so genannten Firewall gegen Angriffe von außen geschützt werden. Eine Firewall hat die Aufgabe, nicht autorisierte Zugriffe auf das gesamte Netzwerk oder bestimmte Segmente davon zu verhindern. Sie kann aus einer Software, einer Hardware oder aus einer Kombination aus beiden bestehen. Welche Lösung am sinnvollsten ist, hängt von den individuellen Anforderungen des Unternehmens ab (siehe Kasten).

Eine gut funktionierende Firewall untersucht und analysiert den gesamten Datenverkehr, der aus dem Internet oder einem externen Netz-

werk in das geschützte Netzwerk fließt. Bei diesem Vorgang blockiert sie alle Daten, die die zuvor festgelegten Sicherheitsregeln nicht erfüllen. So kommen grundsätzlich nur Daten und Personen in das Unternehmens-Netzwerk, die dort auch wirklich erwünscht sind.

Sind in den Unternehmen zahlreiche Außendienstmitarbeiter beschäftigt, die ständig auf Daten aus dem internen Netzwerk zugreifen müssen, empfiehlt sich die Einrichtung eines Virtual Private Networks (VPN) (siehe Kasten). Dabei wird zwischen dem Notebook des Außendienst-Mitarbeiters und dem Firmennetzwerk ein kryptografischer Tunnel aufgebaut. Dadurch haben Angreifer keine Chance, wichtige Geschäftsdaten mit einer so genannten Sniffer-Software abzufangen.

Robert Sopella

FACTS-INFO

Mythos Dialer

Noch immer wird das Thema Dialer im Internet unnötig aufgebauscht. Natürlich stellen die Schadprogramme, die sich unbemerkt installieren und automatisch mit einer teuren 0190-Nummer verbinden, eine große – vor allem finanzielle – Gefahr dar. Allerdings benötigt Dialer-Software eine Einwahlverbindung. Dazu gehören sowohl analoge Modem- als auch ISDN-Verbindungen. Die nutzt jedoch mittlerweile kaum noch jemand, um ins Internet zu gelangen – schon gar nicht Unternehmen.

Wer ausschließlich eine DSL-Leitung für den Internet-Zugang nutzt, braucht sich über Dialer keine Gedanken zu machen. Über diese Leitung kann sich das Programm nicht mit einer teuren Rufnummer verbinden. Doch Vorsicht: Sobald jemand eine PC-ISDN-Karte nutzt, um beispielsweise Fax vom PC aus zu verschicken, lebt die Dialer-Gefahr wieder auf. (sop)

SICHERER DATEN-TRANSFER

Das mobile Office ist zum festen Bestandteil der heutigen Arbeitswelt geworden. Oft müssen die Mitarbeiter unterwegs oder zu Hause auf das interne Firmennetzwerk zugreifen, um beispielsweise E-Mails oder Unternehmens-Präsentationen abzurufen. Doch Vorsicht: Stellen sie die Verbindung zum Netzwerk über das Internet her, besteht für Dritte die Möglichkeit, die übertragenen Datenpakete mit so genannter Sniffer-Software abzufangen. Ein VPN (Virtual Private Network) verhindert den Zugriff ungebeter Schniffer. Der An-

wender baut einen „Tunnel“ zwischen Home-PC oder Notebook und dem Unternehmens-Netzwerk auf. Folge: Er kann sämtliche Daten verschlüsselt senden und empfangen.

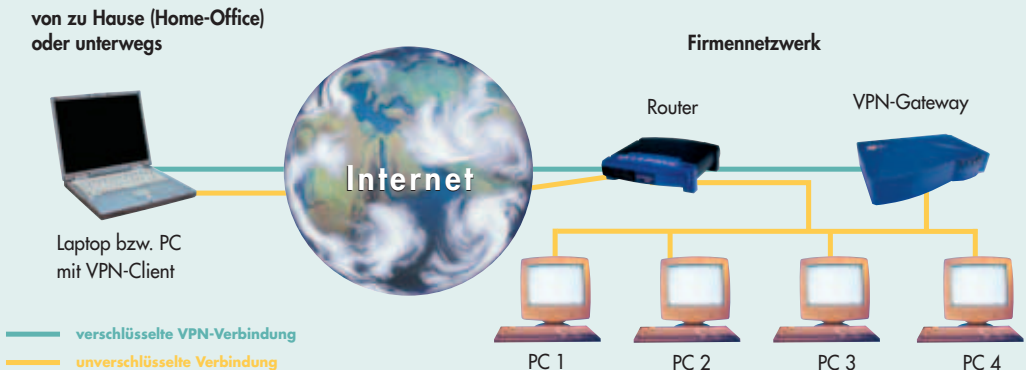
Der Computer des Mitarbeiters benötigt dazu eine Internetanbindung und eine VPN-Client-Software, zum Beispiel „Cisco-VPN-Client“. In das Unternehmensnetzwerk muss lediglich ein so genanntes VPN-Gateway eingebunden werden. Mit Hilfe der Software verbindet sich der Mitarbeiter mit dem VPN-Gate-

way des Unternehmens und kann anschließend an jedem Ort der Welt arbeiten, als wäre er im eigenen Büro. Dieses Verfahren heißt End-to-Site-VPN (siehe Grafik).

Über VPN lassen sich darüber hinaus zwei Firmennetzwerke miteinander verbinden. Voraussetzung: zwei VPN-Gateways, die über das Internet miteinander in Verbindung stehen. Die Verschlüsselung findet hierbei zwischen den beiden VPN-Gateways statt (Site-to-Site-VPN).

Christian Pachocki

Aufbau eines VPN nach dem End-to-Site-Prinzip



Vorbeugen statt Nachsorgen

Geschäftsrelevante Daten existieren heutzutage fast ausschließlich in digitaler Form. Eine zuverlässige, sichere und lückenlose Datensicherung ist daher unabdingbar.

In den meisten mittelständischen Betrieben bietet sich das gleiche erschütternde Bild: Wild zusammengewürfelte, veraltete Server und PCs, deren Festplatten bereits seit längerer Zeit auf dem letzten Loch pfeifen. Auf ihnen ruhen hochsensible Daten wie der aktuelle Geschäftsbericht, Unterlagen für das Finanzamt, Kundendateien, Angebotstabellen, Wettbewerbsanalysen, Studien und Vertragsentwürfe. Was passiert, wenn die Festplatten ihren Geist aufgeben und die Daten für immer im digitalen Nirwana verschwinden, fragen sich die wenigsten Unternehmer. „Wir haben die Dateien irgendwo auf CD-ROM gesichert“, lautet die unbedarfte Antwort. „Eine strukturierte Speicherlösung? Viel zu teuer.“

Ein Trugschluss, der unter Umständen existenzbedrohend ist. Denn in der heutigen Zeit werden geschäftsrelevante Informationen fast ausschließlich digital erstellt, versandt und abgelegt. Wer bei einem Systemcrash keine schnelle und vor allem lückenlose Rekonstruktion der Daten gewährleisten kann, muss im schlimmsten Falle einpacken. Ein Unternehmen ohne Kundendatei wird nicht lange überleben. Und der Finanzbeamte ist in der Regel nicht sonderlich erfreut, wenn ihm bei der Betriebsprüfung wichtige Daten feh-

len. Die Ausrede „Systemabsturz“ wird er nicht gelten lassen.

Selbst wenn Unternehmen eine homogene und auf technisch neuestem Stand laufende Serverlandschaft inklusive topmoderner Desktop-PCs beherbergen, droht Gefahr. Zwar ist die Wahrscheinlichkeit, Daten durch einen Festplatten-Crash zu verlieren, sehr gering. Doch die menschliche Fehlerquote wird selbst mit der teuersten Top-Technik nicht komplett ausgeschaltet. Ein falscher Tastendruck genügt und die Kundendatei ist genauso unwiederbringlich verschwunden, wie nach einem Festplatten-Absturz.

Sicher aufbewahrt

So oder so ist eine strukturierte Backup-Lösung unabdingbar. Der Markt bietet hierfür derzeit drei Alternativen. Bewährt hat sich über Jahrzehnte die Sicherung der Daten auf Magnetbändern – so genannte Tapes oder Cartridges. Darüber hinaus gibt es die Möglichkeit, die Daten auf zusätzliche Festplatten zu sichern (Disk Storing).

Die dritte Lösung ist eine Kombination aus beidem. Die Sicherungen lassen sich zunächst auf die Festplatte schreiben und von dort aus zur Archivierung auf Bänder

überspielen. Diese Lösung hat zwei Vorteile: Zum einen werden die Daten beim Schreiben auf die Festplatte schneller übertragen und von dort aus im Falle eines Falles auch schneller wiederhergestellt. Zum anderen erfolgt die Übertragung auf die Tapes nicht mehr über das Netzwerk. Folge: Sie ist sicherer und beeinträchtigt die Netzwerkleistung nicht mehr.

Für kleine und kleine mittelständische Unternehmen völlig ausreichend. Zudem sind sie derzeit noch die kostengünstigste Alternative.

Die Durchführung der Datenarchivierung ist mittlerweile einfacher als viele denken. So genannte Autoloader ersparen das ständige Cartridge-Wechseln. Die Inventarisierung der Bänder erfolgt darüber hinaus durch einen integrierten Barcode-Leser. Da die Bänder damit nicht erst komplett eingelezen werden müssen, um ihren Inhalt darzustellen, verringert sich die Zugriffszeit bei einer Wiederherstellung immens.

Robert Sopella

PRAXISBERICHT: DATENFLUT IM GRIFF

Die Erneuerung der Backup-Lösung nutzte das Hochschulbibliothekszentrum in Köln, um die Speicherorganisation maßgeblich zu verbessern.

Üblicherweise steht die Bandsicherung am Ende eines IT-Projekts. Nicht so beim Hochschulbibliothekszentrum in Köln. Dort ging die Einführung einer neuen Library der Erneuerung der Systemumgebung voraus.

Die Ausgangslage

Als zentrale Dienstleistungs- und Entwicklungseinrichtung für die Hochschulbibliotheken in Nordrhein-Westfalen, aber auch für weitere Bibliotheken innerhalb und außerhalb dieses Bundeslandes, stellt das Hochschulbibliothekszentrum (HBZ) seinen Verbundpartnern eine Fülle von Daten bereit. Herzstück ist die Verbunddatenbank, in der alle Titel der Bücher und wissenschaftlichen Publikationen mit ihren Bibliotheksstandorten zentral hinterlegt sind. Sie enthält heute zirka 12 Millionen Titelsätze und 26 Millionen Nachweise. Die Datenmenge stieg kontinuierlich auf mehr als 600 Gigabyte an. Dadurch stießen die vorhandenen Backup-Systeme an ihre Grenzen.

Die Bestandsaufnahme

Die anstehende Investition in eine neue Backup-Lösung nutzte Christine Baron, Leiterin der Abteilung EDV-Grunddienste, um die Rechner- und Speicherorganisation des HBZ zu vereinheitlichen und für die kommenden Jahre fit zu machen. „Durch neue Aufgaben und immer höheres Datenaufkommen war die Anzahl der Server auf mehr als 40 angestiegen. Zur Datensicherung wurden insgesamt vier Systeme eingesetzt“, beschreibt die EDV-Chefin den allmählich entstandenen Wildwuchs. Auch die eingesetzte Backup-Software und die Sicherungsroutinen hielten einer kritischen Überprüfung nicht mehr Stand. Zu Gunsten eines schnellen Backups wurden die Daten während der Sicherungen in mehreren Threads parallel auf Band geschrieben, was eine Wiederherstellung der Daten relativ zeitaufwändig werden ließ. Diese Erfahrung musste das HBZ bei der letzten großen Umstellung im Jahr 2001 machen, als die Verbunddatenbank bei der Migration vom Mainframe auf einen Sun-Server lahm gelegt wurde. „Es dauerte fünf Tage, bis wir mit Hilfe der Supportlines verschiedener Hersteller das Problem erkannt hatten, und weitere zwei Tage, bis alle Daten wiederhergestellt waren“, erinnert sich Baron noch genau.

Die Anforderungen

Die Sichtung des Marktangebots erfolgte unter der Prämisse „Schnelleres Backup und

Verkürzung der Recovery-Zeiten durch verzeichnisweise Sicherungen“. Als geeignete und zugleich zukunftssträchtige Hardware-Plattform kristallisierten sich LTO2, die damals neueste Laufwerkstechnologie, und die Tandberg Libraries der M-Serie mit ihrem modularen Aufbau heraus. Bei der Backup-Software entschied sich das HBZ für NetVault von BakBone. Beim Backup-Server fiel die Wahl in Anbetracht der Sun/Unix-Historie auf eine SunFire V-240 mit aktualisiertem Betriebssystem Solaris 9.

Die Installation

Nachdem das neue Datensicherungssystem installiert war, wurden schrittweise alle Daten der Verbunddatenbank auf ein Cluster-System mit einem angeschlossenen SAN migriert. Als Server wurden zwei Parallelrechner vom Typ Sun V1280 angeschafft, die im SAN auf die Disk Arrays mit den Daten zugreifen. Neben gespiegelten Plattensystemen im SAN sollte auch die Verteilung der Datenbankprozesse auf zwei parallele Rechner zur Ausfallsicherheit der Datenbank beitragen. Die Vorbereitungsphase für die Übernahme der auf Oracle basierenden Verbunddatenbank auf das Cluster-System war zugleich Pilotphase für die neue Backup-Lösung. Log-Files und Dateisysteme wurden täglich auf die Library gesichert, die über einen SCSI-Bus an den Backup-Server angeschlossen ist. Die Kommunikation zwischen Backup-Server und Sun-Rechnern erfolgt über das LAN. Bei den ersten Sicherungsläufen wurde insbesondere auch das Zusammenspiel zwischen Backup-Software und dem Oracle-internen Sicherungstool RMAN getestet. „Die Datensiche-

runslösung bewährte sich vom ersten Tag an“, resümiert Baron.

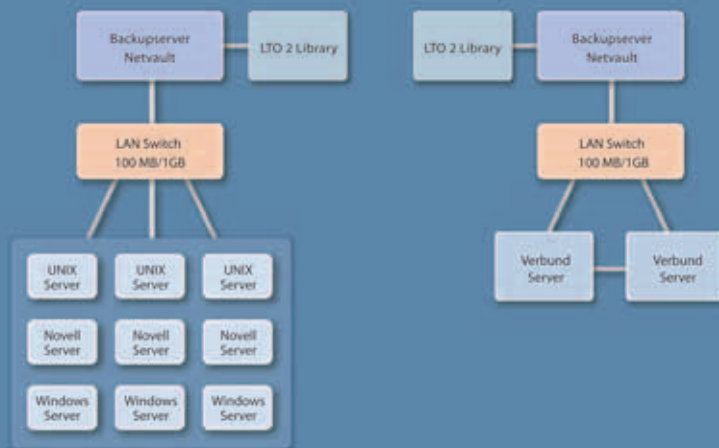
Die ersten Erfahrungen

Seit Juli 2004 läuft die Library im Echtbetrieb. Einmal wöchentlich erfolgt ein Voll-Backup, an den anderen sechs Tagen wird inkrementell gesichert. Durch die zwei Laufwerke können bis zu 108 Gigabyte Daten pro Stunde auf Band geschrieben werden, sodass der gesamte Datenbankbestand von 600 Gigabyte innerhalb von sechs Stunden auf die Bänder übertragen ist. In der jetzigen Ausbaustufe ist die Library mit 24 LTO2-Medien bestückt, sodass eine Speicherkapazität von insgesamt 4,7 Terabyte unkomprimiert bereitsteht.

Das Medienmanagement sieht vor, dass stets zwei Voll-Backups pro Woche auf Band gesichert werden. Das eine bleibt im Haus, das andere wird in ein anderes Gebäude ausgelagert. Die Bänder mit den kompletten Backups werden ein Jahr, die Bänder mit den inkrementellen Sicherungen einen Monat lang aufbewahrt. Damit ist gewährleistet, dass die Daten über einen Zeitraum von einem Monat tagessgenau, die RMAN-Sicherungen auf die Minute genau zurückgesichert werden können.

Für weiter zurückliegende Recoveries entsteht der Zeitraum einer Woche. „Sollte es zu einem Systemabsturz kommen, können wir durch die neue Aufzeichnungsstrategie – es werden gesamte Verzeichnisse hintereinander auf Bänder geschrieben – innerhalb von sechs Stunden wieder online gehen“, konkretisiert Baron die jetzt deutlich verbesserte Datenverfügbarkeit des HBZ.

Geplante, teils bereits realisierte Backup-Organisation im HBZ



So muss eine gut funktionierende Datensicherungs-Landschaft aussehen: Klare Struktur und einheitliche Systeme ermöglichen ein schnelles und sicheres Backup.

Daten an der Angel



Phishing und Spam-E-Mails werden die Computerwelt in diesem Jahr in Atem halten. Wer nicht aufpasst, ist schnell bankrott.

Das Netzwerk ist geschützt, die Antivirus-Software läuft, das WLAN ist verschlüsselt, die Daten werden gesichert – eigentlich dürfte nichts mehr passieren. Doch die Gefahren der IT-Welt lauern an jeder Ecke. Haben Sie eigentlich schon einmal über Datenklau per USB-Sticks nachgedacht (siehe Kasten)? Und haben Sie schon einmal etwas von Phishing gehört?

„Phishing“ ist eine Wortschöpfung aus den Begriffen „Password“ und „Fishing“ (deutsch: Angeln). Es bezeichnet den Versuch, in den Besitz vertraulicher Informationen von Personen, Gruppen oder Unternehmen zu gelangen. Die Objekte der Begierde sind dabei meistens Kreditkartennummern, Kontoinformationen für das Online-Banking oder andere vertrauliche Daten, die sich schnell zu Geld machen lassen. Um an diese Daten zu gelangen, sind „Phisher“ sehr kreativ.

Die beliebteste Methode ist derzeit, gefälschte E-Mails zu verschicken. Der

Empfänger wird aufgefordert, einen Link anzuklicken, der ihn auf eine vermeintlich offizielle Internetseite der Bank, des Telefon-Dienstleisters oder eines Online-Shops umleitet. Die ist jedoch keineswegs offiziell, sondern nur eine täuschend echt wirkende Kopie. Wer nun der Aufforderung nachkommt, seine Benutzerdaten oder seine Kontoinformationen mit dazugehöriger PIN (persönliche Identifikationsnummer) und TAN (Transaktionsnummer) in das vorbereitete Formular einzugeben, hat verloren. Die Betrüger, die die Phishing-

GEFAHR AUS DER HOSENTASCHE

Schutz gegen Viren, Würmer und Hacker allein reicht längst nicht mehr. In Zeiten von USB-Sticks und Mini-Festplatten droht zusätzlich Ungemach aus den eigenen Reihen.

Als der Geschäftsmann Guido V. das ganze Ausmaß der Katastrophe abschätzen konnte, war es bereits zu spät. Die Konkurrenz hatte ihn mit deutlich günstigeren Angeboten ausgebrems. Diese Offensive hat ihn zahlreiche Kunden gekostet. Bittere Folge: Guido V. musste schließlich für sein Unternehmen Insolvenz anmelden. Auslöser seiner unternehmerischen Pleite war ein Vorgang, der tagtäglich in jedem Unternehmen stattfindet: Guido V. hatte seinen Vertriebschef entlassen. Was

dem Geschäftsmann jedoch erst viel später bewusst wurde – der Vertriebsmanager hatte vor seinem Abgang die komplette Kundendatei sowie sämtliche Angebote kopiert und war mit diesen Schätzen als Einstand im Gepäck zur Konkurrenz gewechselt.

Nie war es einfacher, sich wichtige Geschäftsdaten zu kopieren als heutzutage. USB-Sticks und Festplatten passen mittlerweile in jede Hosentasche. Ohne großes Aufsehen zu erregen, lassen sie sich in Sekundenschnelle in den PC stöpseln. Unauffällig werden die begehrten Daten kopiert, und schon ist der handliche Wechselspeicher wieder in der Hosentasche verschwunden.

Unglaubliche 86 Prozent aller deutschen Unternehmen haben Probleme mit dieser Form von Wirtschaftskriminalität, belegt eine Studie der Euler Hermes Kreditversicherung. Den



Seiten aufgebaut haben, sammeln die Daten und räumen im nächsten Augenblick ihr Bankkonto leer.

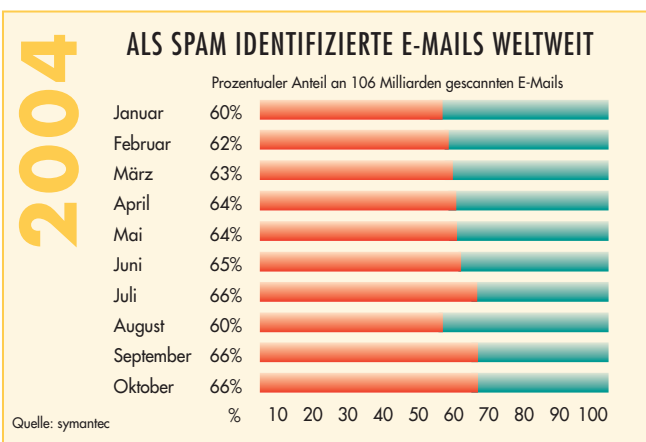
Gefährlicher Müll

Mit diesem banalen Trick ergaunern sich die Betrüger beachtliche Sümmchen. Im Jahr 2003 wurden weltweit schätzungsweise 1,78 Millionen Menschen Opfer von Phishern. Allein die US-Banken und Kreditkarten-Unternehmen beklagten 2003 durch Phishing einen Verlust in Höhe von 1,2 Milliarden US-Dollar. Das Ende der Fahnenstange ist damit allerdings noch nicht erreicht. Die

Experten von Symantec prognostizieren in einer aktuellen Studie, dass Spam die Phishing-Aktivitäten verstärken wird.

Bislang handelte es sich bei Spam-E-Mails in der Regel um Werbe-Mails, die für den Nutzer eher lästiges als gefährliches Übel waren. Nach Ansicht von Symantec wird Spam künftig ein echtes Sicherheitsproblem sein. Trojaner, Viren und Phishing-Versuche werden zunehmend über Spam verbreitet. Eine beängstigende Schätzung: Bereits mehr als 60 Prozent der weltweit versendeten E-Mails werden als Spam klassifiziert (siehe Grafik).

Robert Sopella



Schockierend: Weit mehr als die Hälfte der weltweit versendeten E-Mails sind Spam.

gesamtwirtschaftlichen Schaden beziffert diese Untersuchung mit mehr als 100 Milliarden Euro. Verursacher sind in den meisten Fällen unzufriedene Mitarbeiter. Dabei muss es noch nicht einmal der Datenklau sein, der Unternehmen in Gefahr bringt. Über USB-Sticks können Angestellte – bewusst oder unbewusst – auch jegliche Art von Schadprogrammen ins Unternehmensnetz einschleusen. Schon eine verseuchte Shareware-Datei reicht aus, um die IT-Landschaft schlimmstenfalls lahm zu legen. Selbst die beste Firewall kann solche Schädlinge nicht abblocken.

Wer auf Nummer sicher gehen will, muss daher die Gefahrenquelle USB-Stick komplett ausschalten. Die einfachste Möglichkeit ist, auf allen Arbeitsplatzrechnern die BIOS-Einstellungen so vorzunehmen, dass USB deaktiviert wird. Diese Maßnahme hilft oft jedoch nur vorüber-

gehend. Computererfahrene Mitarbeiter wissen diese Hürde meist mit Leichtigkeit zu nehmen. Weiterer Nachteil: Für den Betrieb eines Arbeitsplatzdruckers oder Scanners wird der USB-Anschluss oft benötigt. Besser schützt ein so genannter USB-Blocker. Das Institut für System-Management (ISM) hat beispielsweise ein System entwickelt, mit dem sich ein Rechte-Management für die Nutzung von USB-Geräten realisieren lässt. Der USB-Anschluss wird dabei nicht generell eingeschränkt, sondern es werden gezielt Nutzungsberechtigungen vergeben. Allerdings nutzt das System bei der Berechtigungssteuerung den Standardtreiber „USBStor.sys“, der bei allen Windows-Systemen im Treiberordner vorhanden ist. Unter Linux kann der USB-Blocker demzufolge nicht verwendet werden. Weitere Informationen gibt es unter: www.secu-sys.de

Robert Sopella

FACTS-INFO

So entgehen Sie Spam und Phishern

Um die Gefahren von Spam-Mails und Phishing-Attacken zu minimieren, reicht es, einige wenige Regeln zu beachten:

- Seien Sie grundsätzlich misstrauisch.
- Öffnen Sie in E-Mails unbekannter Herkunft keine Anhänge.
- Klicken Sie in E-Mails unbekannter Herkunft nicht auf Hyperlinks. Das Gleiche gilt für E-Mails, die vorgeblich von einem offiziellen Absender (z. B. Ihrer Bank) versendet wurden. Gehen Sie lieber direkt über den Browser auf die Ihnen bekannte Internetseite.
- Nutzen Sie niemals den in Spam-E-Mails angegebenen „Abmelde-mechanismus“ (z. B.: „Wenn Sie keine Informationen mehr von uns möchten, senden Sie uns eine E-Mail an: xy@abc.com“). Dadurch bestätigen Sie dem Absender lediglich, dass die Mail-Adresse aktiv ist. Innerhalb kürzester Zeit wird ihr elektronisches Postfach mit Spam überschüttet.