

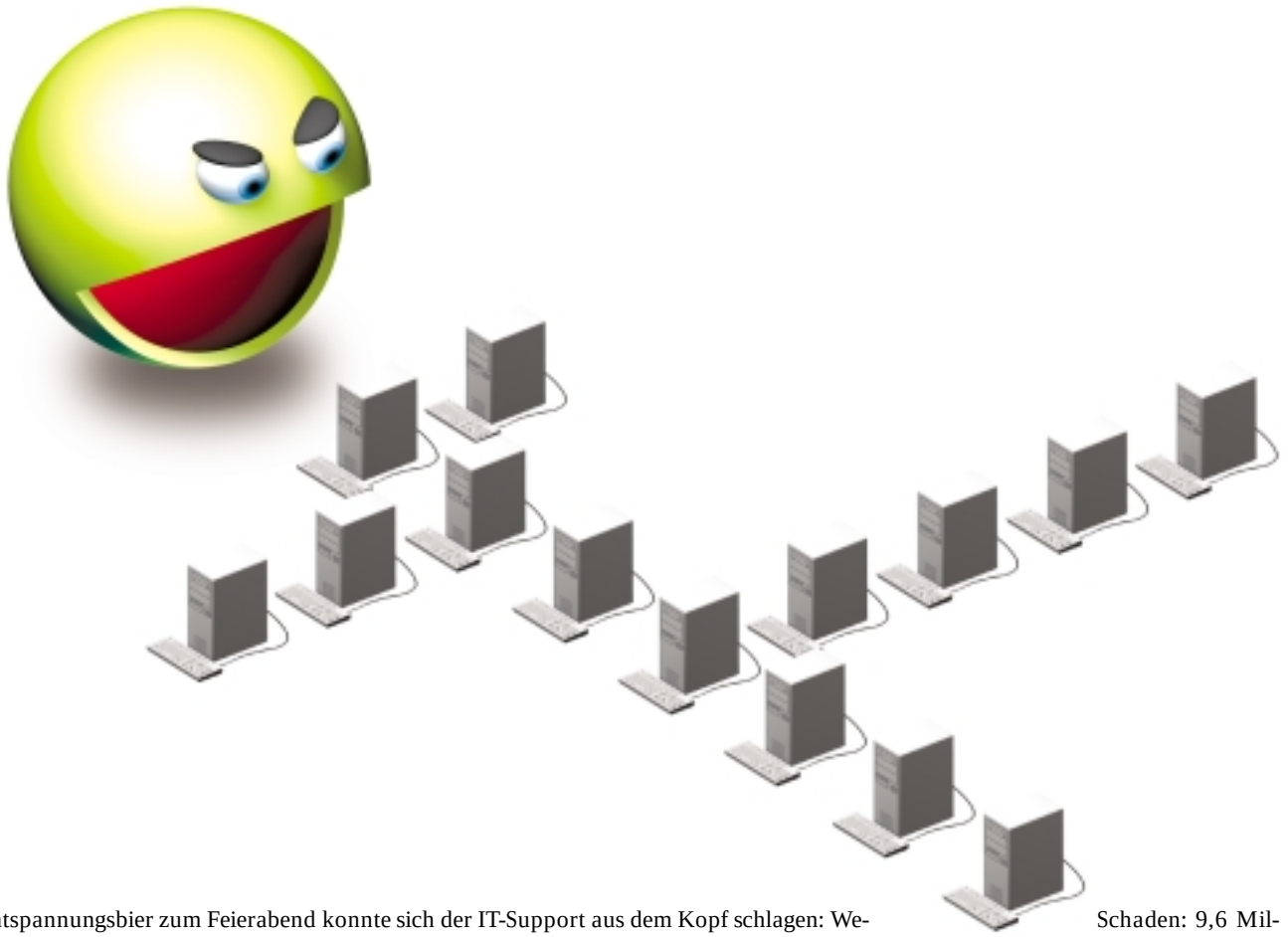
Viren klicken sich in das Adressverzeichnis von E-Mail-Programmen ein und verbreiten sich dadurch selbständig weiter.

Schon durch Mitarbeiterschulung und Betriebsvereinbarungen lässt sich die Verbreitung von Viren weit gehend unterbinden.

Die aktuellen Versionen der Outlook- und Exchange Server-Software blockieren via E-Mail eingeschleuste Viren einfach und schnell.

Attacke aus dem Netz

Computerviren sind die biblische Plage der Internetära. Sie überlisten PC-Anwender wie Netzadministratoren.



Das Entspannungsbier zum Feierabend konnte sich der IT-Support aus dem Kopf schlagen: Wenige Stunden nach dem ersten Auftreten des Computervirus W32.Nimda-A am 17. September in Korea mussten auch hierzulande viele EDV-Betreuer ihre Freizeit neu planen. Allerorten koordinierten Krisenstäbe Sofortmaßnahmen gegen den PC-Schädling, der sich rasend schnell in Tausenden von Netzwerken verbreitete.

Alltag im globalen Dorf: Trojanische Pferde, Würmer und PC-Viren wie Nimda haben im Jahr 2001 weltweit bereits einen Schaden von mehr als zwölf Milliarden Euro verursacht, wie das US-Marktforschungsunternehmen Computer Economics in Carlsbad, Kalifornien, schätzt. Die bislang größten Kosten gehen jedoch auf das Konto des im Jahr 2000 aktiven „I Love You“-Virus. Geschätzer

Schaden: 9,6 Milliarden Euro. Vergleichsweise glimpflich über die Bühne gingen dagegen die Infektionen mit „Code Red“ (Schaden: 1,3 Milliarden Euro) und „Melissa“ (1,1 Milliarden Euro). Insgesamt, so die US-Analysten, gibt es derzeit mehr als 50 000 Computerviren. Täglich werden 15 bis 30 neue entdeckt. Dabei kann der Attacke recht simpel Einhalt geboten werden: Böartige Codes verbreiten sich hauptsächlich per Anhang über E-Mails, die unwissentlich auf einzelnen Rechnern aktiviert werden und von dort ihren Siegeszug antreten. „Im Zusammenhang mit E-Mail ist zu beachten, dass nicht unsere populären Programme Outlook und Exchange Schuld an der rasenden Verbreitung von Viren haben, sondern vielmehr fehlende Sicherheitskonzepte in Unternehmen“, sagt Stefan Lindemann, Product Manager Exchange bei Microsoft. „Würden die Geschädigten aktuelle Microsoft Produkte einsetzen und Richtlinien zur Absicherung von Netzwerken einhalten,

Illustration: Yekon

Markus Ehrl alias Captain Meso: Unter diesem Pseudonym ist der Ex-Hacker bekannt. Heute arbeitet er als Unternehmensberater.

gäbe es kein Problem“, betont Markus Ehrl. Er ist einer der drei deutschen Microsoft Most Valuable Professionals zum Thema Exchange und Moderator der Exchange 2000 Newsgroup. Schließlich, so Ehrl, gebe es seit mehr als einem Jahr eine verbesserte Version der Exchange Server Software mit einer Schnittstelle, die schädliche Dateien im E-Mail-Strom aufspüren kann. Die Basisfunktionalität ist selbst im Vorgängerprodukt enthalten. Auch für Office 2000 existiert ein Service Release, das die versehentliche oder unbefugte Aktivierung von Dateien mit den Endungen „exe“ oder „vbs“ unterbindet.

Blass vor Schreck waren 500 Sicherheitsexperten, als Markus Ehrl während eines Vortrages im Oktober 2000 in Köln live verschiedene Web-Server attackierte und dem Publikum vertrauliche Gehaltslisten präsentierte. „Selbstverständlich wollte ich die Zuhörer nicht zum Hacken erziehen“, betont der Sicherheitsexperte, der unter seinem Pseudonym Captain Meso bekannt ist. „Mir geht es darum, IT-Experten aufzuschrecken.“

Der 31-jährige Unternehmensberater sieht Sicherheitslücken nicht bei den Microsoft-Produkten, sondern in den Versäumnissen bei der Pflege der Netzinfrastruktur. „Das A und O der Sicherheit ist die Aus- und Weiterbildung von Fachpersonal.“ Welche Aufgaben die Systemadministratoren zu erledigen haben, dokumentierte das Fachmagazin Funkschau kürzlich: „Die aufgezeigten Mängel lassen erkennen, dass Sicherheit nicht nur



»Das A und O bei der Sicherheit ist die Ausbildung des Fachpersonals.«

Markus Ehrl, Gründer der Unternehmensberatung Mesoproducts

Sache der Technologie, sondern vielmehr eine Frage des Know-hows ist.“

Die Schwachstelle Mensch nahmen auch andere ins Visier: „Nimda-Virus entlarvt fahrlässige Administratoren“ titelte der Branchendienst Silicon.de unlängst. Und: „Solange einige Administratoren nach der biblischen Empfehlung ‚Schlägt dich einer auf die rechte Wange, so halte ihm auch die andere hin‘ verfahren, werden wohl 1000 Viren nichts an ihrer Nachlässigkeit ändern.“

Ob dieser schroffe Appell in den Chefetagen Gehör finden wird, bleibt fraglich. Zwar sind Schutzprogramme gegen Viren weit verbreitet, doch sie haben oft nur eine Alibifunktion. Und dies, obwohl 99 Prozent der Schädlinge innerhalb einer Firma von Mitarbeiter zu Mitarbeiter verschickt werden. „Mit der Installation eines elektronischen Zertifikats auf dem Arbeitsplatz lassen sich die E-Mail-Systeme so einstellen, dass für das Mailen der Einsatz einer elektronischen Signatur notwendig ist“, analysiert Wilhelm Alms, Vorstandsvorsitzender der Hamburger Unternehmensberatung Mummert + Partner. Viren könnten sich so zwar weiterhin von außen einschleichen, die automatische Verteilung Hunderter von Kopien innerhalb des Firmennetzwerks würde damit jedoch unterbunden, ist Alms überzeugt. Der Schaden bleibe auf den befallenen Rechner begrenzt. „Das ist ein einfacher, aber wirksamer Schutz vor E-Mail-Würmern, den leider noch die wenigsten Unternehmen einsetzen“, bedauert der Unternehmensberater.

KOMPAKT

SECURITY-LÖSUNGEN

So sieht ein effizientes Sicherheitskonzept für Outlook und Exchange aus

- Einführung von Betriebsvereinbarungen und Ergänzung der Datenschutzbestimmungen für den Umgang mit E-Mails und Anhängen
- Mitarbeiter- und Fachpersonalschulungen
- Harmonische Abstimmung der Maßnahmen auf Server- und Client-Seite
- Auswahl von Power-Usern im Unternehmen, die erweiterte Mail-Rechte erhalten
- Redaktionelle Blockade bestimmter Inhalte
- Einsatz von Virenscannern beim Anwender und Aufbau von Serverschutzprogrammen (Antiviren-Firewalls und -Software)
- Automatischer Update der Antiviren-Signaturen und -Pattern
- Regelmäßiger Update der Service Releases
- Nutzung von Antiviren-Schnittstellen (AVAPI) in Microsoft Produkten
- In Netzwerken sollte das Öffnen von exe- und vbs-Dateien sowie weiteren ausführbaren Dateien bei Mails deaktiviert werden (enthalten in Office 2000 Service Release und Office XP). Der Administrator kann den Empfang bereits an der Schnittstelle zum Internet deaktivieren.
- Ausschalten der Voransicht bei Outlook (nicht zwingend erforderlich, wenn Service Release beziehungsweise Office XP im Einsatz)
- Einrichtung einer elektronischen Unterschrift (digitale Signatur) ermöglicht eine eindeutige Identifizierung des Senders



Spezielle Sicherheits-Tools von Microsoft sowie den Security Administration Operations Guide finden Sie unter www.microsoft.com/germany/business/magazin/management

Mehr Infos zum Thema Sicherheit finden Sie auf den Seiten 26/27

mehr >