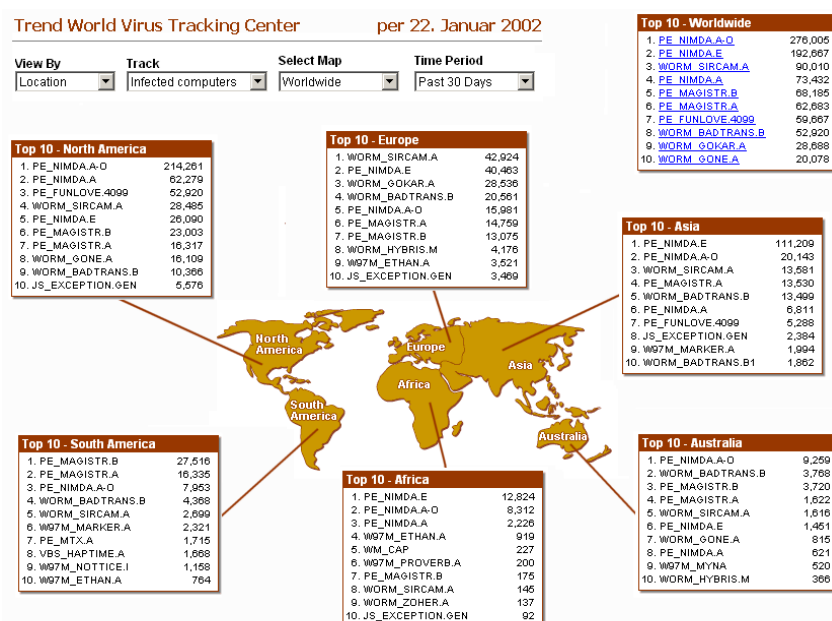


Das Internet wächst und wächst – und so die Risiken.

Die Zunahme der weltweiten Kommunikation über moderne Informationstechnologien war in 2001 ungebrochen. Nach wie vor gilt: nur wer gut informiert ist, setzt sich am Markt durch. Ganze Geschäftsmodelle hängen mittlerweile von funktionsfähigen IT-Infrastrukturen ab und immer mehr Prozessketten werden in allen Bereichen der Wirtschaft ausschließlich von IT-Systemen gesteuert. Diese Ketten können dabei nur so stark sein, wie ihre schwächsten Glieder. Proportional zum Wachstum der globalen Vernetzung steigen leider auch die Gefahren, die mit diesem Wachstum einhergehen.



Quelle: <http://wtc.trendmicro.com/wtc/> © 2002 Trend Micro Incorporated. All Rights Reserved.

2001 - das Jahr der Viren

Nie zuvor waren Computerviren und -würmer so aktiv, wie im vergangenen Jahr 2001 – nicht einen Monat blieb die IT-Welt von globalen Viren-Epidemien verschont. Neben den Erfolgen der Antiviren-Hersteller bei der Entwicklung und Verbesserung geeigneter Schutzmaßnahmen ist die Zahl der Opfer von Viren-Angriffen dramatisch gestiegen.

Laut Antiviren-Spezialist Sophos waren dabei allein zwei einzelne Viren für fast 50 Prozent aller Anrufe beim Sophos-Support verantwortlich.

Nimda führt diese Rangliste an, obwohl er von seinem noch immer unbekanntem Autor erst im September „in the wild“ ent-

Das Internet wächst und wächst – und so die Risiken.

lassen wurde. Nimda bediente sich dabei gleich mehrerer Sicherheitslücken und war dementsprechend effektiv.

Platz zwei belegt der **Sircam Wurm**, der sich bei jeder Replizierung automatisch mit individueller Betreffzeile an alle Einträge im Outlook-Adressbuch verschickt. Durch Diebstahl vertraulicher Dokumente verursachte dieser Wurm beachtlichen Schaden.

Fast **90% aller Infizierungen** geschehen mittlerweile durch Viren-Angriffe **via eMail** aber zusätzlich wuchs in 2001 auch die Zahl der Infektionen über das Internet drastisch. Waren bislang **Downloads** ungeprüfter Dateien hauptsächlich für Infektionen verantwortlich, so genügt nunmehr bereits der Besuch einer verseuchten Seite, um sich über **Sicherheitslücken im Web-Browser** der Gefahr offen auszusetzen.

Im Jahr 2001 wurden auch **erstmalig Instant Messaging und Peer2Peer Plattformen** (ICQ, Gnutella, MSN Messenger, IRC-Kanäle) im großen Stil Opfer von Virenattacken. Das Gnutella Netzwerk für Dateiaustausch fiel dabei beispielsweise dem **Netzwerk-Wurm Mandragore** zum Opfer.

Mitte Januar 2001 wurde der **Netzwerk-Wurm Ramen** entdeckt, dem innerhalb weniger Tage zahlreiche Unternehmen zum Opfer fielen; darunter die US-Raumfahrtbehörde NASA, die Texas A&M University und der taiwanische Hardware-Hersteller Supermicro. Das Besondere an Ramen: er infiziert Websites, die auf Linux-Servern gehostet sind und wird somit wohl als **erster tatsächlich verbreiteter Linux-Virus** in die Geschichte eingehen. Linux galt bis dato als virensicher.

Eine weitere unangenehme Überraschung des Jahres 2001 war im Juli die Entdeckung von **CodeRed** und dessen Funktionsweise. CodeRed funktioniert und verbreitet sich eigenständig, ohne dabei Dateien nutzen zu müssen. Der Schädling ist **ausschließlich im Systemspeicher existent und verbreitet sich in Form spezieller Datenpakete**. Die Antivirenhersteller wurden dadurch vor vollkommen neue Herausforderungen gestellt. Die düsteren Prognosen, CodeRed könne das Internet kollabieren lassen, erfüllten sich jedoch nicht – der Wurm taucht glücklicherweise nicht einmal unter den Viren Top-Ten des vergangenen Jahres auf.

Im Nachgang zu den Attentaten am 11. September 2001 wurde bereits im November bekannt, dass der US-amerikanische

Das Internet wächst und wächst – und so die Risiken.

Geheimdienst FBI ein Programm unter dem Namen **Magic Lantern** entwickelt hat. Bei Magic Lantern handelt es sich um einen **klassischen Trojaner**, der Daten über den (unwissenden) Anwender sammelt und in diesem Fall dem FBI geheim zur Verfügung stellt. Ungeklärt bleibt dabei aber bislang die Frage, ob die USA Antivirenhersteller verpflichten wollen, Magic Lantern aus ihren Datenbanken auszuschließen. Und was passiert, wenn das Programm danach in die falschen Hände gelangen sollte.

Die gute Nachricht des vergangenen Jahres: Entgegen vieler Meldungen sind bislang **noch keine Viren „in the wild aufgetaucht“**, die **Handys, Palms oder ähnliche Handheld Computer infiziert haben**:

Trend zu neuen Viren ungebrochen

Auch in diesem Jahr werden Verbreitung und Vielfalt der Viren, Würmer und Trojaner weiter zunehmen. Begünstigt wird diese Entwicklung durch eine wachsende Zahl neuer und unerfahrener User, die, angelockt durch immer mehr kostengünstige Angebote, fortlaufend ins Internet drängen.

Auch die Tatsache, dass viele User vorsichtiger mit dem Umgang von e-Mail-Anhängen geworden sind, konnte den Trend bisher nicht aufhalten. Viren-Entwickler suchen – und finden – **immer wieder neue Sicherheitslücken und alternative Methoden**, um Rechner oder Dateien zu infizieren.

Dabei lassen sich diese offenbar auch nicht von hohen Strafen abschrecken wie sie beispielsweise David Smith drohen. Dieser hatte sich Ende 1999 schuldig bekannt, den Virus Melissa in Umlauf gebracht und damit schätzungsweise einen Schaden von 80 Millionen US-Dollar verursacht zu haben. Nach Rechtsprechung in den USA verlangt dieser Schaden bei Berücksichtigung des Schuldeingeständnisses eine Gefängnisstrafe zwischen 46 und 57 Monaten sowie Schadenersatz bis zu 480.000 US-Dollar.

Eine Ursache für die **kaum abschreckende Wirkung** dürfte wohl sein, dass die Konsequenzen für Virenentwickler noch keineswegs eindeutig kalkulierbar sind. Ein rechtskräftiges Urteil gegen David Smith wurde bis heute nicht gefällt, der Urteilspruch bereits zum fünften Mal vertagt. David Smith befindet

Das Internet wächst und wächst – und so die Risiken.

sich seit 1999 gegen Kautions auf freiem Fuß. Sehr wohl rechtskräftig verurteilt wurde hingegen im niederländischen Leeuwarden der 21-jährige Schöpfer des Anna-Kournikova-Wurms Jan de Wit: zu 150 Stunden gemeinnütziger Arbeit.

So entdeckt das Virenlabor der Firma Sophos weiterhin **pro Monat bis zu 1.000 neue Viren oder Trojaner**; die Antiviren-Experten bei MessageLabs sprechen mittlerweile von einem Schädling auf 370 unbefallene e-Mails.

Symantec: Sieben Gebote für den Virenschutz

Sieben nach wie vor weit verbreitete Nachlässigkeiten im Umgang mit dem PC begünstigen das ungebrochene Wachstum der Virenverbreitung:

- **Virenschutzprogramme** gehören noch immer nicht zur Standardausstattung von PCs.
- Selbst vorhandene Virensoftware wird meist nur **unregelmäßig aktualisiert**.
- **Disketten** finden nach wie vor breite Verwendung als Datenaustauschmedium.
- Nur wenige Unternehmen sorgen mit Hilfe eines **zentralen serverbasierten Virenschanners** für ausreichenden Schutz.
- Noch immer sind PCs im BIOS standardmäßig auf die **Bootfunktion von Diskette** eingestellt.
- Dateien aus anonymen Quellen werden noch vielfach sorglos akzeptiert, e-Mail-Anhänge **bedenkenlos geöffnet**.
- Mitarbeiter werden **nicht hinreichend sensibilisiert** und handeln meist fahrlässig bei der Verbreitung von Viren.

Auch andere Risiken drohen

Viren stellen nicht das einzige Sicherheitsrisiko für Datenverluste und Schäden im IT-Bereich dar. Zusätzliche Gefahr droht durch **böswillige Einbruchsversuche** und **fehlerhafte Backup-Systeme**. Auch die aufwendigsten Backups sind wertlos, wenn sich ein Fehler in die **Prozesskette der Datensicherung** eingeschlichen hat und dieser dann erst beim Versuch der Datenwiederherstellung entdeckt wird. Ein funktionierendes Backup-System beugt zwar grundsätzlich dem reinen Verlust von Daten vor – zusätzlich muss aber es aber auch garantieren, dass das System im Ernstfall schnellstmöglich wieder produktiv wird!

Das Internet wächst und wächst – und so die Risiken.

Am 2. Oktober 2001 hat das *Institut für System Administration, Networking, and Security* (SANS Institute) in Zusammenarbeit mit dem FBI unter <http://www.sans.org/top20.htm> zum zweiten Mal eine Liste der kritischsten Sicherheitslücken Internet-angebundener Systeme veröffentlicht. Die Liste ist dabei mit zwanzig Einträgen doppelt so umfangreich wie im Vorjahr und wurde vom SANS Institute, dem National Infrastructure Protection Center (NIPC) des FBI sowie ca. 50 Sicherheitsexperten aus Wirtschaft, Militär und Forschung erarbeitet.

Die Brisanz dabei: In den meisten Fällen nutzen Angreifer genau diese **bekanntesten Schwachstellen immer und immer wieder** aus, da die Systemadministratoren vieler Unternehmen schlichtweg keine geeigneten Gegenmaßnahmen ergreifen. CodeRed und Nimda stehen dafür als Musterbeispiel.

Die Top-20 Sicherheitslücken im Überblick

Wer die sieben grundsätzlichen Sicherheitsaspekte der Liste des SANS Institute berücksichtigt und die wesentlichen Risiken seiner Microsoft- oder Unix-Systemlandschaft in den Griff bekommt, hat einen Großteil seiner Hausaufgaben gemacht.

Sicherheitsfragen, die für alle Systeme gelten:

- **Standardinstallationen** verlangen, dass Software regelmäßig upgedatet oder gepatcht wird.
- **Passwörter** stellen eine wichtige Zugangskontrollfunktion dar und verlangen eine regelgerechte Anwendung.
- Nur **korrekte Backups** können zerstörte, gelöschte oder verfälschte Daten retten und Risiken ausschließen.
- Nur gewollt freigeschaltete Anwendungen sollten auf **offenen Ports** Verbindungen annehmen können.
- Am Übergang vom eigenen zu fremden Netzen sollte der Datenaustausch durch **Paketfilter** gesteuert werden.
- **Logging** (Aufzeichnen) von Aktivitäten im eigenen Netzwerk erlaubt es, Angriffsversuche nachzuvollziehen.
- **CGI Beispielscripte** auf Apache-Webservern oder Microsoft IIS-Servern sollten entfernt werden.

Das Internet wächst und wächst – und so die Risiken.

Top-Sicherheitslücken, die Microsoft-Systeme betreffen:

- Über die **Unicode-Sicherheitslücke** kann ein Angreifer beliebige Programme auf dem System ausführen.
- Ein **ISAPI Extension Buffer Overflow** Angriff ermöglicht volle Kontrolle über den Microsoft IIS-Webserver.
- Durch einen Angriff auf die **IIS RDS** (Microsoft Remote Data Services) können Remote-Kommandos mit administrativen Rechten ausgeführt werden.
- **Windows Netzwerkfreigaben** erlauben Zugriff auf Verzeichnisse über das Server Message Block Protokoll.
- Eine **Null Session Verbindung** (Anonymous Login) ermöglicht, Informationen über das Netzwerk zu erlangen.
- Microsoft speichert Paßwörter in **unzureichend gesicherten LAN-Manager Hashs**, die leicht zu entschlüsseln sind.

Top Sicherheitslücken, die Unix Systeme betreffen:

- **Buffer Overflows in RPC-Diensten** ermöglichen es auf einem anderen Computer Programme auszuführen.
- Es sind diverse Sicherheitslücken bekannt, die den beliebten Mailserver **Sendmail** betreffen.
- Auch für den am meisten verwendeten DNS -Server **BIND** existieren diverse Sicherheitslöcher.
- **R Commands** (rlogin, rsh, rcp) verwenden zum Einloggen auf andere Systeme kein Passwort - es erfolgt lediglich eine Überprüfung der IP-Adresse.
- Ein Buffer Overflow Angriff auf den **LPD (remote print protocol daemon)** kann Angreifern erlauben, Programme auf der angegriffenen Maschine auszuführen.
- Buffer Overflow Sicherheitslücken der Programme **sadmind und mouted** können einem Angreifer Root-Zugriff gewähren.
- Zur Authentifizierung benutzt **SNMP** einen **Default String**, der standardmäßig sehr oft "public" lautet. Dieser String wird zudem unverschlüsselt über das Netzwerk geleitet.

Wenngleich die Absicherung der oben genannten zwanzig wichtigsten Schwachstellen einen wichtigen Schritt zu mehr Sicher-

IT-Sicherheit

Das Internet wächst und wächst – und so die Risiken.

heit darstellt, so gilt es auch danach, unvermindert auf der Hut zu sein. Denn **Sicherheit ist ein Prozeß**. Nur eine langfristig angelegte Sicherheitspolitik im Unternehmen, die auf klaren Verantwortlichkeiten und planvollen Prozessen basiert, gewährleistet einen auf Dauer ausreichenden Schutz.

Sollten Sie Fragen zu Ihrer individuellen IT-Sicherheit haben, stehen Ihnen unsere Berater gern zur Verfügung. Wir können Ihre IT-Landschaft auf Herz und Nieren testen.

Weitere Infos über IT-security by e-trend erhalten Sie unter:
<http://www.e-trend.de/it-security>

Ihr e-trend Team



e - t r e n d

Impressum

e-trends im Abo
Ausgabe 12
Januar 2002
ISSN 1618-5854

Verantwortlich
Hauke Peyn (Geschäftsführer)
Volker Liedtke (Geschäftsführer)

e-trend
Media Consulting GmbH
Herforder Str. 74
33602 Bielefeld
fon +49(521) 96751-0
fax +49(521) 96751-99

<http://www.e-trend.de>
e-Mail: newsletter@e-trend.de

Newsletter-Abo unter
<http://www.e-trend.de/newsletter>