

# Symantec-Bericht zu Bedrohungen aus dem Internet

## ÜBERBLICK

### EXECUTIVE EDITOR

Oliver Friedrichs  
*Symantec Security Response*

### EDITOR

Stephen Entwisle  
*Symantec Security Response*

### DEEPSIGHT THREAT ANALYST

Daniel Hanson  
*Symantec Security Response*

### MANAGER, DEVELOPMENT

Dave Ahmad  
*Symantec Security Response*

### SENIOR RESEARCH FELLOW

Sarah Gordon  
*Symantec Security Response*

### DEEPSIGHT THREAT ANALYST

Marc Fossi  
*Symantec Security Response*

### SECURITY ARCHITECT

Peter Szor  
*Symantec Security Response*

### SECURITY RESEARCHER

Eric Chien  
*Symantec Security Response*

Der *Symantec-Bericht zu Bedrohungen aus dem Internet* fasst die Bedrohungsaktivitäten im Internet der letzten sechs Monate zusammen. Diese Ausgabe enthält eine Analyse der zwischen dem 1. Juli und 31. Dezember 2003 aufgetretenen netzwerkbasierten Angriffe, bekannten Schwachstellen und böartigen Codes. Zudem wird untersucht, wie und warum Angriffe manche Unternehmen stärker beeinträchtigen als andere und wie sich gegenwärtige Trends in zukünftigen Internet-Bedrohungen niederschlagen werden. Symantecs Sicherheitsempfehlungen finden Sie im vollständigen Bericht, den Sie von folgender Webseite herunterladen können <http://ses.symantec.de/ISTRDE>

Im August 2003 erlebte das Internet einen der Höhepunkte der Bedrohungsaktivitäten. In nur 12 Tagen wurde die Internet-Gemeinschaft mit drei neuen Würmern der Kategorie 4 konfrontiert.<sup>1</sup> Diese Würmer – Blaster, Welchia und Sobig.F – infizierten Millionen von Computern weltweit und sollen nach Schätzungen von Computer Economics Schäden von bis zu 2 Milliarden US-Dollar verursacht haben.<sup>2</sup>

#### Weitere Schwerpunkte des Berichts:

- In der ersten Jahreshälfte 2003 berichtete lediglich ein Sechstel aller analysierten Unternehmen von gravierenden Sicherheitsverletzungen. Im zweiten Halbjahr meldete bereits die Hälfte der Unternehmen einen ernsthaften Zwischenfall.
- 2003 wurden sieben neue Schwachstellen pro Tag aufgedeckt.
- Weitere Schwachstellen werden ständig zusammen mit neuen Tools zur Ausnutzung dieser Sicherheitslücken veröffentlicht, so dass Administratoren immer schneller auf diese Sicherheitsbedrohungen reagieren müssen.
- 2003 stieg auch der Anteil von böartigem Code, der die Vertraulichkeit von Daten bedroht, sprunghaft an.
- Die Zahl der komplexen Bedrohungen, die gezielt Windows®-Betriebssysteme angreifen, nahm 2003 dramatisch zu.
- Angreifer und komplexe Bedrohungen nutzen zunehmend zuvor infizierte Systeme, um Angriffe zu starten.

<sup>1</sup> Das Symantec Security Response Threat Severity Assessment analysiert Computerbedrohungen (Viren, Würmer, Trojanische Pferde und Makros) und teilt sie in fünf Kategorien ein. Kategorie 5 stellt dabei die höchste und Kategorie 1 die niedrigste Gefahrenstufe dar.

<sup>2</sup> Computer Economics hat eine Schätzung der Auswirkungen der neuesten Angriffswelle vorgenommen: [www.computereconomics.com/article.cfm?id=867](http://www.computereconomics.com/article.cfm?id=867). Diese Zahlen berücksichtigen keine Kosten, die auf Verminderung des Börsenwerts, Verlust des Kundenvertrauens und negatives Image zurückzuführen sind.

### **Angriffstrends**

- Würmer sind weiterhin die häufigste Quelle der verzeichneten Angriffsaktivitäten.
- Fast ein Drittel aller Angriffssysteme zielt auf die Schwachstelle ab, die auch vom Blaster-Wurm ausgenutzt wird.
- Hacker visierten zunehmend "Hintertüren" im System an, die von anderen Angreifern oder Wurmern zurückgelassen wurden.
- Angriffssysteme wählten verstärkt geografische Regionen in ihrer Nähe als Angriffsziele.
- Finanz- und Gesundheitsdienstleister sowie Energieversorger waren am stärksten von ernsthaften Zwischenfällen betroffen.
- Die Zahl der gravierenden Zwischenfälle sank in dem Maß, wie die Dauer der Betreuung der Kunden anstieg. Über 70 Prozent aller Kunden, die länger als sechs Monate betreut wurden, konnten gravierende Attacken erfolgreich abwehren.

### **Trends bei Schwachstellen**

- 2003 dokumentierte Symantec 2.636 Schwachstellen, das entspricht sieben Schwachstellen pro Tag.
- Symantec-Daten weisen darauf hin, dass sich die Zahl der Schwachstellen auf hohem Niveau eingependelt hat.
- Neu entdeckte Schwachstellen sind zunehmend gravierender.
- Neu entdeckte Schwachstellen sind immer leichter ausnutzbar.
- 70 Prozent der 2003 entdeckten Schwachstellen wurden als leicht ausnutzbar klassifiziert.
- Der Prozentsatz der Schwachstellen, für die schädlicher Programmcode öffentlich erhältlich war, wuchs 2003 um 5 Prozent.

- Der Prozentsatz von Schwachstellen, die keine spezialisierten Tools zu ihrer Ausnutzung bedurften, wuchs 2003 um 6 Prozent.

### **Trends bei bösartigem Code**

- Komplexe Bedrohungen machten 54 Prozent der Top-Ten-Bedrohungen im zweiten Halbjahr 2003 aus.
- Symantec entdeckte zweieinhalb Mal so viele Win32-Viren und -Würmer wie im Vergleichszeitraum 2002.
- Unter den Top Ten der bösartigen Codes hat der Anteil an Wurmern mit eigener Mail-Engine (Massenmailer) um 61 Prozent gegenüber der ersten Jahreshälfte 2003 zugenommen.
- In der zweiten Jahreshälfte 2003 stieg die Zahl der Bedrohungen für vertrauliche Daten sprunghaft an. Hier gab es ein Wachstum von 519 Prozent.

### **Aktuelle Bedrohungen**

- Im Januar 2004 begann MyDoom sich ähnlich schnell wie Sobig.F zu verbreiten, indem er infizierte Systeme über eine "Hintertür" befiel und von dort einen gezielten Angriff ausführte.
- Zwei neue Würmer, Doomjuice und Deadhat, die MyDoom folgten, verbreiteten sich über die "Hintertür", die MyDoom hinterlassen hatte.
- Komplexe Bedrohungen dienen weiterhin als Medium für groß angelegte Denial-of-Service-Angriffe, wie das Beispiel von Blaster im August sowie MyDoom und seine Nachfolger (DeadHat und DoomJuice) in den ersten Monaten des Jahres 2004 deutlich gemacht haben.

## AUSNUTZUNG VORHANDENER "HINTERTÜREN" DURCH ANGREIFER

Eine große Zahl von Sicherheitssensoren zeichnete Aktivitäten auf, die von früheren Angriffen und komplexen Bedrohungen zurückgelassene "Hintertüren" (Backdoors) im System anvisierten. Durch die Nutzung existierender Backdoors konnten Angreifer die Kontrolle über Systeme erlangen, eigene Schlupflöcher einrichten oder das infizierte System für eine Denial-of-Service-Attacke ausnutzen.

Im ersten Vierteljahr 2004 durchsuchten Angreifer und neue komplexe Bedrohungen Netzwerke nach der "Hintertür", die im MyDoom-Wurm enthalten ist. Über diese Backdoor können Angreifer neuen bösartigen Code installieren (beispielsweise Software zum Aufzeichnen von Tastatureingaben) und sich vertrauliche Daten auf infizierten Systemen aneignen. Dies öffnet auch den Weg für komplexe Bedrohungen, die diese Systeme infizieren können.

## SCHWACHSTELLEN IMMER GRAVIERENDER UND LEICHTER AUSNUTZBAR

Durchschnittlich wurden in den letzten sechs Monaten 99 neue Schwachstellen mit hohem Bedrohungsgrad aufgedeckt. Bedrohungen mit hohem Gefährdungsgrad gewähren Angreifern mehr Rechte und Zugriff auf wichtige Ziele. Die Aussichten für die erfolgreiche Durchführung eines Angriffs steigen dadurch erheblich. Angreifer suchen gezielt nach gravierenden Schwachstellen, da diese eine verstärkte Aufmerksamkeit der Öffentlichkeit und der Medien auf sich ziehen.

Zudem sind Schwachstellen immer leichter ausnutzbar. Das kann bedeuten, dass keine speziellen Fachkenntnisse für den nicht autorisierten Zugriff auf ein Netzwerk erforderlich sind oder Angreifern eine Reihe von Angriffs-Tools zur Verfügung steht. Die Wahrscheinlichkeit von destruktiven Angriffen auf Netzwerke steigt dadurch beträchtlich. 70 Prozent der 2003 entdeckten Schwachstellen wurden als leicht ausnutzbar klassifiziert (im Vergleich zu 60 Prozent in 2002).

## WACHSENDER TREND BEI BÖSARTIGEM CODE

In den letzten sechs Monaten nahm der Anteil des an Symantec™ Security Response eingesendeten bösartigen Codes ständig zu. Komplexe Bedrohungen machten 54 Prozent der Top-Ten-Bedrohungen aus und sind damit weiterhin eine ernsthafte Gefahr. Blaster, Welchia, Sobig.F und Dumaru gehören zu den vier komplexen Gefahren, die sich in den letzten sechs Monaten mit enormer Geschwindigkeit ausgebreitet haben.

Bösartiger Code, der vertrauliche Daten wie Kennwörter, Entschlüsselungscodes und Tastatureingaben extrahiert, hat in den letzten sechs Monaten drastisch zugenommen. Das bekannteste Beispiel dafür ist Bugbear.B. Diese komplexe Bedrohung wurde gezielt programmiert, um vertrauliche Daten auszuspionieren. Andere Bedrohungen in dieser Kategorie enthalten "Hintertüren" und Spyware, über die sich Hacker wichtige, vertrauliche Daten aneignen.

## AUSBLICK

Die Sicherheitsanalysten von Symantec beobachten derzeit mehrere Trends. Zum einen arbeiten zahlreiche Windows-Betriebssysteme mit Komponenten, die sowohl in Unternehmensumgebungen als auch im Privatanwenderbereich weit verbreitet sind. Deshalb muss in Zukunft damit gerechnet werden, dass in diesen Komponenten vorhandene Schwachstellen zu einer immer schnelleren und flächendeckenderen Ausbreitung gravierender Zwischenfälle führen.

Zum anderen ist ein deutlicher Anstieg bei Client-seitigen Schwachstellen in Microsoft® Internet Explorer zu verzeichnen. Über diese Schwachstellen können Angreifer Systeme von Benutzern infizieren, die unwissentlich Webseiten mit bösartigen Inhalten besuchen. In den letzten sechs Monaten entdeckten Sicherheitsexperten 34 Schwachstellen in Internet Explorer.

Als Letztes lässt sich ein weiterer beunruhigender Trend erkennen: Die Zeit zwischen der Aufdeckung und der Ausnutzung einer Schwachstelle nimmt ab. In der Zeit zwischen der Ankündigung einer neuen Schwachstelle und der Entwicklung sowie Verteilung eines Patches sind Unternehmen Angriffen ungeschützt ausgesetzt. Da Angriffsmethoden, die diese Schwachstellen ausnutzen, immer schneller entwickelt und in Umlauf gebracht werden, steigt auch für Unternehmen das Risiko, Opfer eines Angriffs zu werden. Deshalb ist zu befürchten, dass in Zukunft immer häufiger komplexe Bedrohungen auftreten, die noch nicht veröffentlichte Schwachstellen ausnutzen. Symantec ist der Ansicht, dass solche sogenannten "Zero-Day"-Bedrohungen unmittelbar bevorstehen. Solche Bedrohungen nutzen Schwachstellen aus, bevor diese der Öffentlichkeit bekannt gemacht und Patches veröffentlicht werden. Ein solcher Angriff kann große Schäden anrichten, bevor Benutzer in der Lage sind, entsprechende Patches auf ihren Systemen zu installieren.

Diese und weitere Probleme werden ausführlich im vollständigen Symantec-Bericht zu Bedrohungen aus dem Internet, Band V, behandelt. Den Bericht können Sie von folgender Webseite herunterladen <http://ses.symantec.de/ISTRDE>

SYMANTEC IST EIN FÜHRENDER ANBIETER FÜR INTERNET-SICHERHEITSTECHNOLOGIEN. DIE UMFANGREICHE PALETTE AN LÖSUNGEN IN DEN BEREICHEN CONTENT- UND NETZWERK-SICHERHEIT SOWIE SICHERHEITS-APPLIANCES FÜR UNTERNEHMEN, PRIVATANWENDER UND INTERNET-DIENSTLEISTER UMFASST CLIENT-, GATEWAY- UND SERVER-SICHERHEITSLÖSUNGEN FÜR VIRENSCHUTZ, FIREWALL UND VPN (VIRTUAL PRIVATE NETWORK), SCHWACHSTELLEN-MANAGEMENT, INTRUSION DETECTION, INTERNET- UND E-MAIL-FILTER SOWIE TECHNOLOGIEN FÜR DIE FERNVERWALTUNG UND SICHERHEITSSERVICES FÜR UNTERNEHMEN UND SERVICEANBIETER WELTWEIT. DIE NORTON-SICHERHEITSPRODUKTE VON SYMANTEC SIND HINSICHTLICH IHRER VERKAUFZAHLEN UND ERHALTENEN AUSZEICHNUNGEN WELTWEIT MARKTFÜHREND. DAS UNTERNEHMEN HAT SEINEN HAUPTSITZ IN CUPERTINO, KALIFORNIEN, UND VERTREIBT SEINE PRODUKTE IN 38 LÄNDERN.

FÜR MEHR INFORMATIONEN BESUCHEN SIE UNS UNTER [WWW.SYMANTEC.DE](http://WWW.SYMANTEC.DE)



**WORLD HEADQUARTERS**

Symantec Corporation  
20330 Stevens Creek Blvd.  
Cupertino, CA 95014 U.S.A.  
Tel.: +1 (408) 253 9600  
Fax: +1 (800) 441 7234

**DEUTSCHLAND:**

Symantec (Deutschland) GmbH  
Lise-Meitner-Str. 9  
D - 85737 Ismaning  
Tel.: +49 (0) 69-6641 0315  
E-Mail: [enterprise.deutsch@symantec.com](mailto:enterprise.deutsch@symantec.com)

**ÖSTERREICH:**

Symantec GmbH  
Wipplingerstraße 34  
A - 1010 Wien  
Tel.: +43 (0)1- 532 85 33-0  
E-Mail: [infolineaustria@symantec.com](mailto:infolineaustria@symantec.com)

**SCHWEIZ:**

Symantec Switzerland AG  
Grindelstrasse 6  
CH - 8303 Bassersdorf  
Tel.: +41 (0) 1-838 49 00  
Fax: +41 (0) 1-838 49 01  
E-Mail: [infoline@symantec.com](mailto:infoline@symantec.com)

Symantec hat Niederlassungen in 38 Ländern. Adressen und Telefonnummern der Symantec-Niederlassungen in anderen Ländern finden Sie auf unseren Webseiten: [www.symantec.com](http://www.symantec.com) oder [www.symantec.de](http://www.symantec.de)

Informationen über Kundenservice und technischen Support finden Sie auf unserer Webseite: [www.symantec.com/desupport/](http://www.symantec.com/desupport/)

Symantec, das Symantec-Logo und DeepSight sind in den USA eingetragene Marken der Symantec Corporation. Digital Immune System, Symantec AntiVirus, Symantec AntiVirus Research Automation (SARA), Symantec Managed Security Services, Symantec Security Check und Symantec Security Response sind Marken der Symantec Corporation. Microsoft, FrontPage, Outlook, Windows und Windows NT sind eingetragene Marken der Microsoft Corporation. Andere Marken und Produkte sind Marken der jeweiligen Rechtsinhaber und werden hiermit anerkannt. Technisches Dokumentationsmaterial, das von der Symantec Corporation zur Verfügung gestellt wird, ist urheberrechtlich geschützt und Eigentum der Symantec Corporation. KEINE GEWÄHRLEISTUNG. Die technische Dokumentation wird OHNE Mängelgewähr bereitgestellt und die Symantec Corporation übernimmt keinerlei Gewähr für die Richtigkeit oder Verwendung der Dokumentation. Die Verwendung der technischen Dokumentation bzw. der darin enthaltenen Informationen erfolgt auf das Risiko des Benutzers. Die Dokumentation kann technische oder andere Ungenauigkeiten oder typografische Fehler enthalten. Symantec behält sich das Recht vor, Änderungen ohne vorherige Ankündigung vorzunehmen. Copyright © 2004 Symantec Corporation. Alle Rechte vorbehalten. DS00112-GE