



## **Symantec Internet Security Threat Report, Ausgabe XIV Frequently Asked Questions (FAQ) 2008**

### **Über den Symantec Internet Security Threat Report**

Der Symantec *Internet Security Threat Report* (ISTR) analysiert die weltweiten Cybercrime-Aktivitäten, gibt einen Überblick über bekannte Sicherheitslücken und analysiert die häufigsten Schadcodes. Gegenwärtige Phishing- und Spam-Trends werden ebenso beurteilt wie die Aktivitäten der Schattenwirtschaft. Der aktuelle Bericht befasst sich mit der IT-Sicherheitslage und den Internetbedrohungen im Jahr 2008.

Mit dem Symantec Global Intelligence Netzwerk hat Symantec den umfangreichsten Datenpool zu Gefahren für die Sicherheit im Internet etabliert. Rund 240.000 Sensoren in mehr als 200 Ländern beobachten die aktuelle Bedrohungslage für die IT-Sicherheit. Als Informationsquellen dienen Produkte und Dienstleistungen von Symantec sowie andere Wissensdepots. Die Ergebnisse zu Schadcodes stützen sich auf Informationen von mehr als 130 Millionen Kunden, Servern und Gateway-Systemen, die von Antivirus-Produkten geschützt werden. Außerdem hat Symantec ein Netzwerk von Honeypot-Systemen über den Globus gespannt, das in Echtzeit Informationen über bislang unentdeckte Gefahren und Angriffe sammelt. Symantec pflegt zudem die weltweit größte Datenbank zu Software-Schwachstellen. Darin sind derzeit 32.000 bekannte Sicherheitslücken aufgeführt, die 72.000 Technologien von mehr als 11.000 Anbietern betreffen. Zusätzlich unterstützt Symantec den populären Newsletter BugTraq™, der von rund 50.000 Abonnenten genutzt wird, um sich über die jüngsten Schwachstellen zu informieren.

Daten zur Spam- und Phishing-Entwicklung werden in mehreren Quellen gesammelt, darunter dem Symantec Probe Netzwerk mit seinen rund 2,5 Millionen Köder-Accounts und der MessageLabs Infrastruktur. Insgesamt werden die Daten aus mehr als 86 Ländern ausgewertet. 16 Rechenzentren werden Das sind derzeit mehr als 8 Milliarden E-Mails und über eine Milliarde Webanfragen täglich, die in 16 Rechenzentren untersucht werden. Symantec erhält ferner Informationen über Phishing-Attacks durch eine Community zum Schutz vor Online-Betrug. Diese Gemeinschaft setzt sich zusammen aus Unternehmen, Sicherheitsanbietern und rund 50 Millionen Nutzern.

Diese Quellen liefern den Analysten von Symantec einen einmaligen Datenpool, aus dem sie Informationen zu Cybercrime-Angriffen, Schadcodes, Phishing und Spam für den Symantec Internet Security Threat Report extrahieren können.

## Die globalen Highlights des Symantec Internet Security Threat Report

### Cybercrime-Aktivitäten

- 23 Prozent aller Cybercrime-Aktivitäten hatten ihren Ursprung in den USA, das waren 26 Prozent weniger als 2007.
- Im Bildungssektor ereigneten sich mit 27 Prozent die meisten Datenschutzverletzungen, die dazu führten, dass Kriminelle an Nutzeridentitäten gelangen konnten. Im Vergleich zum Vorjahr sank diese Zahl um ein Prozent.
- Im Finanzsektor wurden mit 29 Prozent die meisten Vorfälle bei identitätsbezogenen Daten verzeichnet, was einem Anstieg von zehn Prozent gegenüber 2007 entspricht.
- Symantec identifizierte pro Tag weltweit im Durchschnitt 75.158 Computer, die mit Bot-Programmen infiziert waren. Das waren 31 Prozent mehr als im Vorjahr.
- Zu der am häufigsten angegriffenen Schwachstelle zählte die ADODB.Stream Object File Installation im Microsoft® Internet Explorer®. 30 Prozent aller Web-Attacks zielten auf diese Lücke ab.

### Sicherheitslücken

- Symantec dokumentierte 5.491 Sicherheitslücken. Im Jahr 2007 wurden 4.625 Schwachstellen, also 19 Prozent weniger erfasst.
- Zwei Prozent (2007: vier Prozent) aller Sicherheitslücken wurden als besonders schwerwiegend eingestuft, 67 Prozent (2007: 61 Prozent) als mittelschwer und 30 Prozent (2007: 35 Prozent) als geringfügig schwerwiegend.
- 80 Prozent aller dokumentierten Sicherheitslücken wurden als einfach zu beheben eingestuft, das waren sechs Prozent mehr als 2007.
- Von allen von Symantec analysierten Browsern hat Apple Safari das größte „Window of Exposure“ (damit ist die Zeit zwischen dem Auftauchen des Schadcodes und der Veröffentlichung eines Sicherheitspatches durch den Anbieter gemeint) mit einer Durchschnittsdauer von neun Tagen; Mozilla Browser hatte mit durchschnittlich weniger als einem Tag das kleinste „Window of Exposure“.
- Beim Mozilla Browser traten 99 neue Sicherheitslücken auf, mehr als bei jedem anderen. Für den Internet Explorer wurden 47 neue Schwachstellen identifiziert, 40 bei Apple Safari, 35 bei Opera und elf bei Google Chrome.
- 415 Plug-in-Sicherheitslücken wurden bei Browsern festgestellt, das sind 60 weniger als im Vorjahr. ActiveX-Technologien machen mit 287 immer noch die Mehrheit aus; das sind 112 Schwachstellen weniger als 2007.
- 63 Prozent aller Sicherheitslücken betrafen Web-Applikationen, 2007 waren es noch 59 Prozent.
- Insgesamt wurden 12.885 Webseiten aufgespürt, die anfällig sind für Webangriffe des Typs Cross-Site-Scripting. Im Jahr davor waren es noch 17.697 Sites. Bei Redaktionsschluss des ISTR waren aber nur drei Prozent der betroffenen Sites repariert worden.
- Neun Zero-Day-Lücken wurden dokumentiert, 2007 waren es noch 15.
- Im Jahr 2008 wurden 112 Schwachstellen in Unternehmenslösungen aufgespürt, für die es im vergangenen Jahr noch keinen Patch gab. Im Vorjahr waren es noch 144.
- Die am häufigsten attackierte Schwachstelle war die in der Microsoft Windows Server Service RPC Handling Remote Code Execution.
- 95 Prozent der identifizierten Sicherheitslücken betrafen Endgeräte, fünf Prozent Server. 2007 waren es noch 93 Prozent beziehungsweise 7 Prozent.

### Schadcodes

- In der EMEA-Region wuchs der proportionale Anteil der Schadcode-Infekte am stärksten.
- Die Verbreitung von Schadcodes mit Hilfe von Shared Executable Files auf Wechselmedien wie USB-Sticks stieg kräftig an von 44 (2007) auf 66 Prozent.
- Die Anzahl der neuen Schadcode-Signaturen wuchs um 265 Prozent im Vergleich zum Vorjahr; 60 Prozent aller bislang bekannten Schadcode-Angriffe wurden 2008 aufgedeckt.
- Die Top 10 der neu entdeckten Schadcode-Familien umfassen drei Trojaner, drei Trojaner mit Backdoors, zwei Computerwürmer, ein Computerwurm mit Backdoor sowie ein Computerwurm mit Backdoor- und Virus-Komponente
- 68 Prozent der Top 50 Schadcodes waren Trojaner, das ist ein Prozent weniger als im Vorjahr

- Der Anteil von Angriffen gegen vertrauliche Daten, die per Fernzugriff zugänglich sind, sank von 91 Prozent im Jahr 2007 auf 83 Prozent. Sie zählen aber weiterhin zu den häufigsten Angriffen.
- 78 Prozent der Attacken auf vertrauliche Daten exportierten Nutzerdaten, davon wiederum späten 76 Prozent die Tastatureingaben von Anwendern aus. Im Jahr 2007 waren es noch 74 beziehungsweise 72 Prozent.
- Ein Prozent der Top 50 Schadcodes veränderten Websites, 2007 waren es noch zwei Prozent.
- Die Zahl der erfassten Schadcodes, die Sicherheitsschwachstellen ausnutzen, sank signifikant von 13 (2007) auf drei Prozent.
- Acht der Top 10 heruntergeladenen Schadcode-Komponenten waren Trojaner, einer war ein Trojaner mit Backdoor-Element und einer war selbst ein Backdoor.
- Zehn Prozent der Top 50 Schadcodes war gegen Online-Spiele gerichtet, 2007 waren es noch sieben Prozent.

### **Phishing, Server der Schattenwirtschaft und Spam**

- 79 Prozent aller für Phishing-Angriffe benutzten Marken gehörten dem Finanzsektor an, 2007 waren es noch 83 Prozent.
- 76 Prozent aller Phishing-Versuche betrafen den Finanzsektor, was einen Anstieg um 24 Prozent im Vergleich zu 2007 bedeutet.
- Symantec identifizierte 55.389 Phishing-Websites – ein Zuwachs von 66 Prozent seit 2007.
- 43 Prozent der von Symantec identifizierten Phishing-Websites stammen aus den USA. Das sind 26 Prozent weniger als 2007.
- Mit 39 Prozent war .com die am meisten verbreitete Top-Level-Domain, die für Phishing-Versuche missbraucht wurde. 2007 lag sie ebenfalls auf Platz 1, da allerdings mit einem Anteil von 46 Prozent.
- Ein ganz bestimmtes Phishing-Tool, das Symantec identifiziert hatte, war für 14 Prozent aller Phishing-Attacken verantwortlich.
- Auf den Servern der Underground Economy, die Symantec ermittelt hat, waren Kreditkartendaten mit einem Anteil von 32 Prozent das am häufigsten angebotene Gut. 2007 lag der Anteil noch bei 21 Prozent.
- Die meisten Spam-Meldungen, 24 Prozent, bezogen sich auf Internet- oder Computerdienstleistungen und -produkte. Im Vorjahr lagen diese Inhalte noch auf Platz 2 mit einem Anteil von 19 Prozent am gesamten Spam-Aufkommen.
- Die Menge erkannter Spam-Mails im Internet stieg um 192 Prozent – von 119,6 Milliarden Meldungen im Jahr 2007 auf 349,6 Milliarden in 2008.
- Bot-Netzwerke sind für 90 Prozent aller Spam-Mails verantwortlich.