Confidence in a connected world. symantec™

SYMANTEC SICHERHEITSBERICHT

Kernaussagen des
14. Symantec Internet Security Threat Reports

FAKTEN
TRENDS

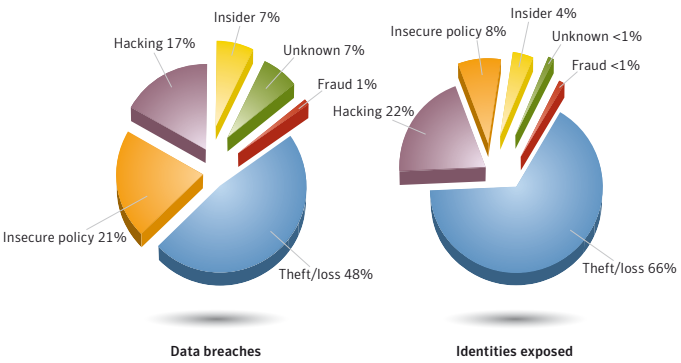
Wichtige Entwicklungen weltweit

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 aus dem Jahr 2008.

- Symantec dokumentierte 5.491 Vulnerabilities (unbekannte Schwachstellen) im Jahr 2008, also 19 Prozent mehr als im Vorjahr.
- Die Einstufung deren Gefahrenpotenzials: „Hoch“ zwei Prozent, „Medium“ 67 Prozent und „Niedrig“ 30 Prozent.
- 80 Prozent aller in diesem Zeitraum dokumentierten Schwächen waren leicht auszunutzen, im Vergleich zu 74 Prozent im Vorjahr.
- Mozilla Browser hatten mit 99 neuen Schwächen in 2008 die meisten Fälle gegenüber allen Browsern; 47 neue Vulnerabilities wurden im Internet Explorer, 40 in Apple Safari, 35 in Opera, und 11 in Google Chrome gefunden.
- 2008 hat Symantec insgesamt neun Zero-Day Vulnerabilities verzeichnet, 2007 waren es 15.

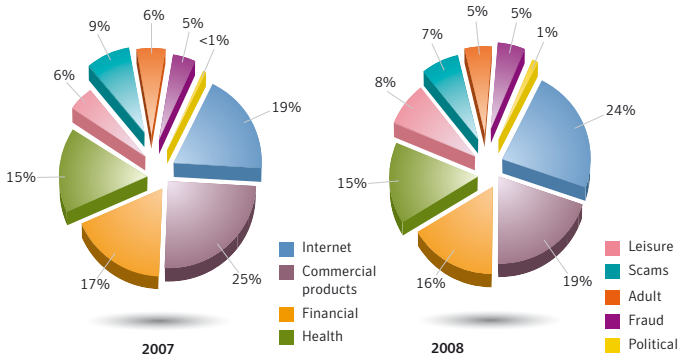
Gründe für Datenschutzverletzungen



Diebstahl und Verlust des Datenträgers bleiben die Hauptursache für Datenverluste und -schutzverletzungen.

Die meisten Datenverluste sind in Verbindung mit kleinen, tragbaren Geräten wie USB-Sticks, externen Festplatten und Smartphones passiert.

Spam Trends



Spam-Meldungen, die ausschließlich Internet-Dienste und -Güter anbieten, liegen mit 24 Prozent an der Spitze, gefolgt von 19 Prozent von Spam, die kommerzielle Produkte bewirbt.

Im vergangenen Jahr wuchs die Menge von Spam weltweit um 192 Prozent, von 119,6 Milliarden Spam-Nachrichten im Jahr 2007 auf 349,6 Milliarden in 2008.

2008 wurden 90 Prozent aller Spam-Meldungen per Botnet verschickt.

Gestohlene Informationen werden verkauft

2008 Rank	2007 Rank	Item	2008 Percentage	2007 Percentage	Range of Prices
1	1	Credit card information	32%	21%	$0.06–$30
2	2	Bank account credentials	19%	17%	$10–$1000
3	9	Email accounts	5%	4%	$0.10–$100
4	3	Email addresses	5%	6%	$0.33/MB–$100/MB
5	12	Proxies	4%	3%	$0.16–$20
6	4	Full identities	4%	6%	$0.70–$60
7	6	Mailers	3%	5%	$2–$40
8	5	Cash out services	3%	5%	8%–50% or flat rate of $200–$2000 per item
9	17	Shell scripts	3%	2%	$2–$20
10	8	Scams	3%	5%	$3–$40/week for hosting, $2–$20 design

Kreditkartendaten (32 Prozent) und Zugangsdaten zu Bankkonten (19 Prozent) gehören weiterhin zu den am häufigsten angebotenen Gütern.

Kompromittierte E-Mail Accounts können den Zugang zu weiteren vertraulichen Informationen und Ressourcen frei geben.

Browser Exploits

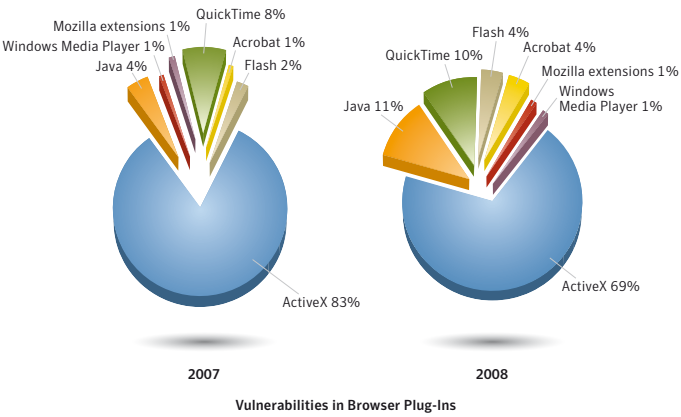
Rank	Web-based Attack	Percentage
1	Microsoft Internet Explorer ADODB.Stream Object File Installation Weakness	30%
2	Acrobat PDF Suspicious File Download	11%
3	ANI File Header Size Buffer Overflow	7%
4	Adobe SWF Remote Code Executable	7%
5	Microsoft Internet Explorer DHTML CreateControlRange Code Executable	6%
6	SnapShot Viewer ActiveX File Download	5%
7	Microsoft Internet Explorer XML Core Services XMLHTTP Buffer Overload	4%
8	Quicktime RTSP URI Buffer Overload	3%
9	AOL SuperBuddy ActiveX Code Executable	3%
10	Microsoft Internet Explorer WebViewFolderIcon ActiveX Control Buffer Overflow	2%

Die Top-Angriffe richteten sich gegen Vulnerabilities im Web-Browser selbst, dessen Plug-ins und in Client-Anwendungen.

Die Angreifer haben Sites mit hohem Verkehrsaufkommen gewählt und sie mit Hilfe von Vulnerabilities im Web-Host oder seinen lokalen Webanwendungen geknackt.

Sobald die Site kompromittiert war, haben die Angreifer die Seiten so modifiziert, dass sie die Besucher mit infizierten Inhalten versorgte.

Vulnerabilities in Browser Plug-ins



415 Vulnerabilities (unbekannte Schwachstellen) in Browser Plug-ins wurden in 2008 entdeckt. Das sind 51 weniger als die 475 aus dem Jahr 2007.

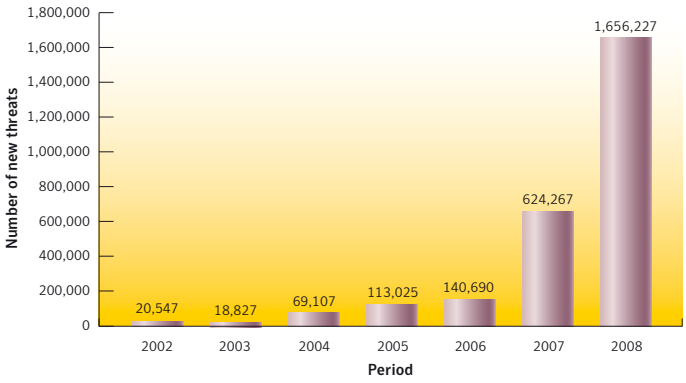
Den vollständigen Symantec Sicherheitsbericht finden Sie unter **www.symantec.com/threatreport**

Datenquellen des Sicherheitsberichts

Mit dem Symantec Global Intelligence Netzwerk hat Symantec den umfangreichsten Datenpool zu Gefahren für die Sicherheit im Internet etabliert. In dem Netzwerk werden die Mess- und Analysedaten zahlreicher Datenquellen zusammengefasst. Zu den Quellen zählen:

- Rund 240.000 Sensoren in mehr als 200 Ländern, die die aktuelle Bedrohungslage für die IT-Sicherheit beobachten.
- 130 Millionen installierte Antivirus-Engines auf Desktop, Gateways und Servern.
- Eine Vulnerability-Datenbank, in der derzeit 32.000 bekannte Sicherheitslücken aufgeführt sind, die 72.000 Technologien von mehr als 11.000 Anbietern betreffen.
- Der populäre Newsletter BugTraq™, der von rund 50.000 Abonnenten genutzt wird, um sich über die jüngsten Schwachstellen zu informieren.
- Das Symantec Probe Netzwerk mit seinen rund 2,5 Millionen Köder-Accounts und die MessageLabs Infrastruktur.
- Aktuell werden Daten aus mehr als 86 Ländern ausgewertet. Derzeit fallen täglich mehr als 8 Milliarden E-Mails und über eine Milliarde Webanfragen an, die insgesamt 16 Rechenzentren auf Malwarebefall untersuchen.
- Die Community zum Schutz vor Online-Betrug. Diese Gemeinschaft setzt sich aktuell zusammen aus Unternehmen, Sicherheitsanbietern und rund 50 Millionen Nutzern.

Erfasster Schadcode



2008 wurden pro Monat 28.7 Millionen neue Schadcode-Varianten entdeckt.

Von allen Schadcode-Varianten, die Symantec bisher erfasste, stammen 60 Prozent allein aus dem Jahr 2008.

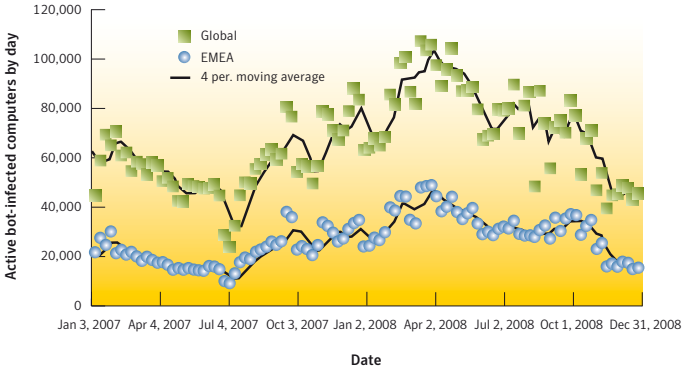
Malware-Aktivität pro Land (weltweit)

2008 Rank	2007 Rank	Country	2008 Overall Percentage	2007 Overall Percentage	Malicious Code Rank	Spam Zombies Rank	Phishing Websites Host Rank	Bot Rank	Attack Origin Rank
1	1	United States	23%	26%	1	3	1	2	1
2	2	China	9%	11%	2	4	6	1	2
3	3	Germany	6%	7%	12	2	2	4	4
4	4	United Kingdom	5%	4%	4	10	5	9	3
5	8	Brazil	4%	3%	16	1	16	5	9
6	6	Spain	4%	3%	10	8	13	3	6
7	7	Italy	3%	3%	11	6	14	6	8
8	5	France	3%	4%	8	14	9	10	5
9	15	Turkey	3%	2%	15	5	24	8	12
10	12	Poland	3%	2%	23	9	8	7	17
...	...	...	...	...	...	...	...	...	...
28	27	Switzerland	1%	1%	37	28	25	23	28
45	42	Austria	<1%	<1%	55	45	32	34	41

2008 spielten sich weltweit 23 Prozent der gesamten Malware-Aktivität in den USA ab. China folgt mit 9 Prozent auf dem zweiten Platz und Deutschland mit 6 Prozent auf Platz 3. Die Schweiz liegt auf Platz 28, Österreich auf Position 45.

Sobald die Rolle des Internets dank mehr Bandbreite in bestimmten Ländern wächst, steigt auch deren Anteil bei der Malware-Aktivität.

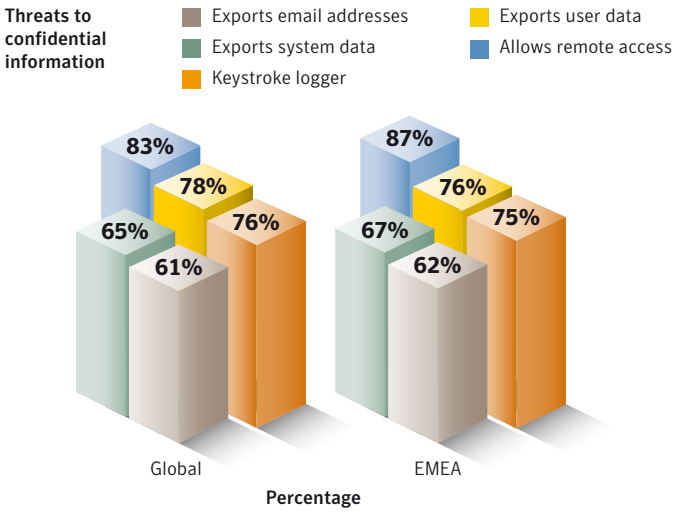
Aktive Bot-Computer in EMEA



2008 wurden in der Region EMEA insgesamt 4.776.967 aktive Bot-Computer entdeckt. Das sind 9 Prozent mehr als 2007.

In Spanien waren mit einem Anteil von 15 Prozent die meisten Bot-Rechner in EMEA zu finden, danach folgen Deutschland und Italien.

Intention von Schadcodes



Mehr als 80 Prozent aller Bedrohungen zielen auf vertrauliche Informationen ab.

Phishing Trends EMEA

2008 Rank	2007 Rank	Country	2008 Percentage	2007 Percentage	2008 Top Targeted Sector	Percentage of Lures in Country Targeting Top Sector
1	8	Poland	18%	4%	Financial	90%
2	4	France	11%	10%	Financial	74%
3	5	Russia	10%	8%	Financial	54%
4	1	Germany	9%	15%	Financial	70%
5	2	United Kingdom	9%	13%	Financial	77%
6	6	Italy	6%	8%	Financial	57%
7	3	Netherlands	6%	11%	Financial	57%
8	7	Israel	5%	6%	Financial	63%
9	9	Spain	5%	3%	Financial	71%
10	11	Turkey	3%	2%	Financial	81%

2008 hat Symantec global 55.389 Hosts mit Phishing-Sites aufgespürt. Dies ist ein Anstieg von 66 Prozent gegenüber 2007, als Symantec 33.428 Phishing-Hosts entdeckte.

2008 waren 43 Prozent aller gefundenen Phishing-Websites in den USA platziert. 2007 waren es noch 69 Prozent.

Die Kernaussagen des Symantec Internet Security Threat Reports

Cybercrime-Aktivitäten

- 2008 spielten sich weltweit 23 Prozent der gesamten Malware-Aktivitäten in den USA ab. China folgt mit neun Prozent auf dem zweiten Platz und Deutschland mit sechs Prozent auf Platz 3. Die Schweiz liegt auf Platz 28 (ein Prozent), Österreich auf Position 45 (unter einem Prozent).
- In EMEA bleibt Deutschland mit 14 Prozent weiterhin Spitzenreiter bei allen Malware-Aktivitäten.
- 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-Attacken zielten auf diese Lücke ab.

Sicherheitslücken

- Symantec dokumentierte 5.491 Sicherheitslücken. Im Jahr 2007 wurden 4.625 Schwachstellen, also 19 Prozent weniger erfasst.
- 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; der 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.
- 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.
- 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.
- 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 (2008).
- 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, einen Computerwurm mit Backdoor sowie einen 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 spähten 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 eine Backdoor.

- Zehn Prozent der Top 50 Schadcodes war gegen Online-Spiele gerichtet, 2007 waren es noch sieben Prozent.

Phishing und Spam

- Weltweit gehören 79 Prozent aller für Phishing-Angriffe benutzten Marken dem Finanzsektor an, 2007 waren es noch 83 Prozent.
- In Polen wurden 18 Prozent aller Phishing-Sites in der EMEA-Region gehostet. Damit belegt das Land den Spitzenplatz, gefolgt von Frankreich mit einem Anteil von 11 Prozent. Deutschland, 2007 mit einem Anteil von 15 Prozent noch an erster Stelle, hat sechs Prozentpunkte verloren und ist auf Platz vier gefallen.
- Symantec identifizierte 55.389 Phishing-Websites – ein Zuwachs von 66 Prozent seit 2007.
- 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.

Die wichtigsten Trends bei Viren und Trojanern

- Trojaner stellten die zahlenmäßig bedeutendste Bedrohung durch bösartigen Code dar. Trojaner machten 68 Prozent der 50 wichtigsten möglichen Bedrohungen in der Region aus. Dieser Prozentsatz hat sich seit dem ersten Halbjahr nicht geändert.
- Großbritannien meldete die meisten Infizierungen durch Backdoors, Trojaner, Viren und Würmer.
- Trojan.Vundo war im aktuellen Berichtszeitraum die am häufigsten gemeldete Variante von möglichem bösartigen Code in EMEA; der Trojaner war auch weltweit die am häufigsten gemeldete Variante.
- Die in diesem Berichtszeitraum am häufigsten gemeldete Gruppe von neuem bösartigen Code im EMEA-Wirtschaftsraum war Pidief. Dieser Trojaner nutzt eine Schwachstelle in PDF-Software aus.

Den vollständigen Symantec Sicherheitsbericht finden Sie unter **www.symantec.com/threatreport**

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 deckt den Zeitraum vom 01. Januar bis 31. Dezember des vergangenen Jahres ab.

Als Grundlage dienen Informationen, die vom Symantec Global Intelligence Netzwerk gesammelt werden. In dieses Netz fließen die Messungen zur aktuellen Bedrohungslage von 240.000 Sensoren in mehr als 200 Ländern ein. Die Ergebnisse zu Schadcodes stützen sich auf Informationen von mehr als 130 Millionen Kunden, Servern und Gateway-Systemen, die von Antivirus-Produkten geschützt werden. Symantec hat zudem ein globales Honeypot-Netz aus speziellen Mess-Sensoren gespannt, das in Echtzeit Daten über bislang unentdeckte Gefahren sammelt. Der Bericht bezieht auch die Einträge in der weltweit größten Datenbank zu Software-Schwachstellen mit ein. Darin sind derzeit 32.000 bekannte Sicherheitslücken zu 72.000 Technologien von mehr als 11.000 Anbietern aufgeführt.

Daten zur Spam- und Phishing-Entwicklung werden in dem Symantec Probe Netzwerk mit seinen rund 2,5 Millionen Köder-Accounts und der MessageLabs Infrastruktur erfasst. Darüber werden täglich mehr als 8 Milliarden E-Mails und über eine Milliarde Webanfragen aus mehr als 86 Ländern ausgewertet.

Über Symantec

Symantec ist ein weltweit führender Anbieter von Sicherheits-, Storage- und Systemmanagement-Lösungen. Damit unterstützt Symantec Privatpersonen und Unternehmen bei der Sicherung und dem Management von Informationen. Unsere Software und Dienstleistungen schützen effizient und umfassend gegen Risiken, um überall dort Vertrauen zu schaffen, wo Informationen genutzt und gespeichert werden.

Mehr zu Symantec finden Sie unter www.symantec.de

Confidence in a connected world. symantec™

Symantec (Deutschland) GmbH
Humboldtstraße 6
85609 Aschheim
Deutschland
Tel.: +49 (0)89 9 43 02-0
Fax: +49 (0)89 9 43 02-950
www.symantec.de

Symantec (Austria) GmbH
Wipplingerstraße 34
1010 Wien
Österreich
Tel.: +43 (0)1 5 32 85 33-0
Fax: +43 (0)1 5 32 85 33-3999
www.symantec.at

Symantec (Switzerland) AG
Andreasstraße 15
8050 Zürich
Schweiz
Tel.: +41 (0)44 3 05 72-00
Fax: +41 (0)44 3 05 72-01
www.symantec.ch