Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 80 (2002)

Heft: 2

Rubrik: News

Security

Viren Top Ten 2001

Die von Sophos erstellte Viren Top Ten 2001 zeigt auf, dass E-Mail-fähige Würmer auf dem Vormarsch sind.

Sophos, weltweit einer der führenden Spezialisten für Antiviren-Lösungen in Unternehmen, teilt mit, dass 2001 nur zwei einzelne Viren, nämlich Nimda und Sircam, für fast 50% aller Anrufe beim Sophos-Support gesorgt haben. Code Red, der medienpräsentesteste Virus dieses Jahres, ist in der Statistik nicht einmal vertreten. Sophos hat bis jetzt in diesem Jahr 11 160 neue Viren, Würmer und Trojaner entdeckt, womit das Unternehmen heute vor fast 70 000 Viren schützt. Die Sophos-Virenlabore entdecken heute durchschnittlich über dreissig Viren pro Tag.

Top-Ten-Liste

Die Viren-Top-Ten-Liste sieht nach Angaben des technischen Supports von Sophos folgendermassen aus (an erster Stelle steht der am häufigsten gemeldete Virus):

1.	W32/Nimda	27,2%	Nimda
2.	W32/Sircam-A	20,3%	Sircam
3.	W32/Magistr	12,0%	Magistr
4.	W32/Hybris	6,2%	Hybris
5.	W32/Apology	3,8%	Apology
6.	VBS/VBSWG-X	3,6%	Homepage
7.	VBS/Kakworm	3,1%	Kakworm
8.	VBS/SST-A	2,0%	Kournikova
9.	W32/BadTrans	1,8%	BadTrans
10.	W32/Navidad	1,8%	Navidad
Andere:		18,2%	

«Der unbekannte Nimda-Autor hat seine Kreation erst im September 2001 vom Stapel gelassen, und dennoch ist Nimda der Grund für mehr als ein Viertel aller Anrufe beim Sophos-Support gewesen», erklärt Gernot Hacker, Senior Technical Consultant bei Sophos Anti-Virus. «Nimda war sehr effektiv, da er sich mehrerer Sicherheitslücken bediente. Wahrscheinlich werden wir in Zukunft noch weitere Attacken dieser Art erleben.»
Knapp hinter dem Nimda-Wurm befindet sich der Sircam-Wurm in der Rangliste. Da Sircam bei jeder Replizierung eine neue Betreffzeile erzeugt, klickten zahlreiche Anwender achtlos infizierte E-Mail-Attachments an. Sircam richtete besonders viel Schaden an, da er vertrauliche Dokumente stahl und an alle im Adressbuch eingetragene E-Mail-Adressen weiterschickte.
Neben allen neu entdeckten Viren und Würmern, wie Nimda, Sircam, Anna Kournikova und Homepage, erscheint in der Viren Top Ten 2001 auch ein Wurm, der erstmals 1999 auftauchte. Der Kakworm führte die Statistik bereits letztes Jahr an und ist dieses Jahr noch auf Platz sieben zu finden.

Erstes Konsolenspiel mit Virus

Sophos hat erfahren, dass die japanische Version von Atelier Marie, ein Strategiespiel für die Sega-Dreamcast-Spielekonsole, mit einem zerstörerischen Computervirus infiziert ist. Das Spiel enthält einen Bildschirmschoner, der nach der Installation versucht, den PC des Anwenders mit dem schädlichen Virus W32/Kriz zu infizieren.
«Kriz kann einen Computer unbrauchbar machen», sagt Graham Cluley, Senior Technology Consultant bei Sophos Anti-Virus. «Er führte seinen Nebeneffekt am 25. Dezember 2001 aus, was jedem, der dieses Spiel als Geschenk bekam, das Weihnachtsfest gründlich verleiden konnte. Auch wenn Dreamcast selbst dabei nichts geschah, wartete auf jeden, der den Bildschirmschoner auf seinen PC lud, eine unangenehme Überraschung. Es ist eigentlich unglaublich, dass dieser Virus auch ein Jahr, nachdem er das erste Mal aufgetreten ist, noch immer in Umlauf ist.»
Kool Kizz, die Entwicklungsfirma von Atelier Marie, hat das Spiel aus den Geschäften zurückgerufen und entschuldigte sich auf ihrer Website, www.kool kizz.co.jp, bei den betroffenen Anwendern. Obgleich sich die infizierte Version des Spiels wahrscheinlich nur in Japan verbreitet hat, rät Sophos jedem, der ein Exemplar des Spiels hat, dieses zurückzugeben oder zu vernichten.
Kriz löscht das CMOS-Setup und versucht, den BIOS-Chip eines Computers zu zerstören, ähnlich wie der Virus CIH (alias Chernobyl). Dadurch wird der gesamte Computer lahmgelegt, sodass er völlig unbrauchbar wird und der Anwender den ganzen Chip ersetzen muss. Der Virus versucht weiterhin, alle Dateien auf den lokalen Festplatten und Netzlaufwerken mit Unsinn zu überschreiben.

Magic Latern – Trojanisches Pferd vom FBI

Sophos versichert seinen Kunden heute, dass Sophos nicht gebeten wurde, das Trojanische Pferd vom FBI – Codename: Magic Lantern – unerkannt durchzulassen. Sophos ist überzeugt, dass der Einsatz von «elektronischen Wanzen» zum Ausspionieren von verdächtigen Kriminellen und Terroristen voller Gefahren ist, da es keine Möglichkeit gibt, sicherzustellen, dass der Code von den Empfängern nicht für illegale Zwecke missbraucht wird.
«Schäden verursachender Code ist Schäden verursachender Code», sagt Graham Cluley, Senior Technology Consultant bei Sophos Anti-Virus. «Es besteht Grund zu der Annahme, dass Einrichtungen, die von Magic Lantern betroffen sind, eine Variante der elektronischen Wanze für ihre eigenen Zwecke schreiben. Bevor wir es bemerken, werden wir von aller Welt bespitzelt – sogar das FBI kann ein Opfer seines eigenen Codes werden.»
Sophos bezweifelt, dass das Konzept von Magic Lantern jemals erfolgreich als Methode zur Beobachtung von verdächtigen Kriminellen und terroristischen Aktivitäten funktionieren wird.
«Wenn ein Kunde den Verdacht hat, überwacht zu werden und ein Trojanisches Pferd an uns sendet, werden wir ihm einen Schutz davor zur Verfügung stellen», erklärt Graham Cluley. «Wir können nicht herausfinden, ob er vom FBI geschrieben wurde, und selbst wenn wir es wüssten, könnten wir nicht erfahren, ob es vom FBI verwendet wurde oder ob es von Dritten genutzt wird, um unsere Kunden zu bespitzeln – die Situation ist völlig uneinschätzbar.»

Entwicklungen im Jahr 2001
Das Schicksal von Virenautoren gibt weiterhin Anlass für Diskussionen. Der Autor des Anna-Kournikova-Wurms, Jan de Wit, wurde zwar für schuldig erklärt, aber nur zu 150 Stunden gemeinnütziger Arbeit in Holland verurteilt. Fünfzig Unternehmen gaben zu, von diesem Wurm befallen worden zu sein. In den USA hingegen wartet David L. Smith, zwei Jahre nachdem er sich schuldig bekannt hatte, den Melissa-Virus geschrieben zu haben, immer noch auf seine Verurteilung. Der Melissa-Virus verursachte einen Schaden in Höhe von 80 Millionen Dollar.
Im März trat mit Lindose zum ersten Mal ein Virus auf, der sowohl Windows- als auch Linux-Betriebssysteme befiel. Der Unix-Wurm Sadmind (der erstmals im Mai entdeckt wurde) zeigte auf, dass nicht nur Microsoft-Systeme von Viren heimgesucht werden.
Mit FunnyFile und Choke wurden erstmalig Viren entdeckt, die Instant-Messaging-Plattformen angriffen. Dies zeigte Anwendern, dass es notwendig ist, umsichtiger zu sein. Unternehmen erkannten, dass Viren nicht nur über E-Mails verbreitet werden.
Trotz eines künstlich erzeugten Hypes tauchte 2001 kein Virus auf, der Palms oder Handys befiel.
Code Red sorgte seit Juli 2001 für Schlagzeilen und war der Grund für Tausende besorgter Anfragen von Anwendern. Obwohl einige Sicherheitsexperten vorausgesagt hatten, dass durch Code Red das Internet kollabieren werde, erscheint der Wurm jetzt nicht einmal in der Viren Top Ten dieses Jahres.

Prognose für 2002
Laut Sophos wird es 2002 zu noch mehr Virusattacken kommen. Ständig offene Verbindungen zu Hause mittels ADSL und Kabelmodems erhöhen die Verwundbarkeit für Hackerangriffe. [4]

Pino von Kienlin
Sophos GmbH
Tel. +49 (0)6136 9119-3
E-Mail: pino@sophos.de

Clariant und Nestlé SA wählen Infonet

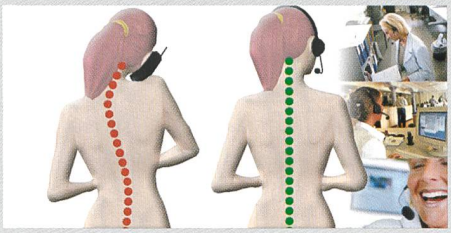
Wie Infonet Services Corporation bekannt gab, ist sie von der Firma Clariant zum exklusiven Telekommunikationspartner ernannt worden. Der Outsourcing-Vertrag mit einer Laufzeit von fünf Jahren deckt die Bereitstellung verschiedener Dienste ab und verleiht Infonet die Stellung eines wichtigen strategischen Beraters in Bezug auf die Telekommunikationsanforderungen von Clariant. In dieser beratenden Rolle ist Infonet vor allem dafür verantwortlich, dass die Leistungen des aktuellen Telekommunikationssystems die Ziele von Clariant optimal erfüllen.
Clariant ist ein weltweit führender Hersteller für Fein- und Spezialchemikalien mit rund 30 000 Beschäftigten und mehr als 100 zur Gruppe gehörenden Unternehmen auf fünf Kontinenten. Clariant entstand aus der Chemiedivision von Sandoz. Mit Büros und Produktionsstandorten in der ganzen Welt und einer Basis von 12 000 SAP-Anwendern ist das weltweite Telekommunikationsnetz der Firma hohen und wachsenden Belastungen ausgesetzt.
Clariant entschied sich für eine Auswahl an Infonet-Diensten für den Betrieb ihrer internen Anwendungen und den Aufbau von E-Commerce-Anwendungen. Infonet konnte sich dabei gegen viele Mitbewerber durchsetzen. Zum Infonet-Service-Portfolio gehören priorisierte Intranetdienste an 45 Standorten in Europa und Asien und ein grosses Angebot an Internet-Diensten, einschliesslich vor Ort eingerichteter Firewalls.

Globales Kommunikationsnetz für Nestlé SA

Infonet Services Corporation hat kürzlich einen Fünf-Jahres-Vertrag mit der schweizerischen Nestlé SA abgeschlossen, der die Bereitstellung mehrerer Dienste umfasst. Der Auftrag wird Infonet während der fünfjährigen Laufzeit des Vertrags schätzungsweise über 125 Millionen US-$ einbringen.
Das globale Kommunikationsnetz der Nestlé SA verbindet 1500 Nestlé-Standorte in neunzig Ländern. Nestlé besitzt eine globale strategische Geschäftsinitiative, genannt GLOBE (GLObal Business Excellence). Der Zweck dieser Initiative ist die Einführung gemeinsamer Geschäftsprozesse, gemeinsamer interner und externer Stammdaten und einer gemeinsamen Informationssysteminfrastruktur.
Um dieses Ziel zu erreichen, muss sich Nestlé von den bisherigen individuellen Ländernetzwerken trennen und ein globales Kommunikationsnetz mit verbesserter Servicequalität und Konsistenz aufbauen.
Infonet Services Corporation ist ein führender Anbieter von innovativen globalen Kommunikationslösungen, die multinationalen Konzernen einen echten Mehrwert bieten. In der Schweiz wird das Unternehmen von Infonet Schweiz AG vertreten. Beteiligt sind Swisscom AG mit 90% und Infonet Service Corporation mit 10% Aktien. In ihrem Leitsatz setzt sich Infonet Schweiz AG zum Ziel, globale Kommunikation für multinationale Unternehmen in der Schweiz weltweit zu ermöglichen und sie entweder direkt oder durch Swisscom zu unterstützen.

Infonet Schweiz AG
Postfach 693, CH-3000 Bern 9
Tel. 031 390 70 53, Homepage:
www.ch.infonet.com oder
www.infonet.com

Gesund telefonieren



Kommunikation und Telefonie sind ein wichtiger Bestandteil unserer Gesellschaft geworden. Trotz allen Vorteilen der heutigen Kommunikationsmittel steht immer noch der gesunde Mensch im Vordergrund. Um diesem Anspruch gerecht zu werden, bietet die Suprag AG eine ganze Palette an Freisprechgarnituren. Damit können sich die Mitarbeiterinnen und Mitarbeiter entspannt zurücklehnen und ihre Kunden freihändig beraten. Gesundheit ist Investitionsgut. Eine Suprag-Sprechgarnitur ist ein modernes Kommunikationsmittel, das zudem eine entspannte Körperhaltung ermöglicht. Dies wiederum wirkt sich positiv auf das Wohlbefinden der Mitarbeitenden aus. Diese werden eine neue und wohltuende Art zu telefonieren entdecken.

Suprag AG
Friedackerstrasse 14, CH-8062 Zürich
Tel. 01 317 20 60, E-Mail: info@suprag.ch,
Homepage: www.suprag.ch