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

Herausgeber: Swisscom

Band: 83 (2005)

Heft: 3

Artikel: Viren- und Spamschutz zunehmend wichtig

Autor: Sellin, Rüdiger

DOI: https://doi.org/10.5169/seals-877115

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 11.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Viren- und Spamschutz zunehmend wichtig

Symantec

RÜDIGER SELLIN **Das gegen ein Unternehmen und dessen Kunden gerichtete Bedrohungspotenzial durch elektronische Angriffe von aussen hat in den letzten Jahren deutlich zugenommen. Dazu gehört auch die Sicherstellung des laufenden Betriebs zur gewohnten Bereitstellung von mobilen Diensten. Nur eine durchdachte Kombination physikalischer und elektronischer Massnahmen gewährleistet einen umfassenden Schutz.**

Zum Jahreswechsel 2004/05 häuften sich die Meldungen über Handy-Viren und Spam-SMS. Auch wenn die Zahl der Stammviren relativ konstant ist, so nimmt jene der Varianten jedoch zu. Zurzeit sind rund 15 Virenstämme (Tabelle) und etwa 25 Varianten bekannt, die sich vor allem auf das Betriebssystem Symbian konzentrieren. Symbian wird von verschiedenen Herstellern wie Nokia, Sony Ericsson oder Siemens in unterschiedlichen Versionen eingesetzt. Die heute bekannten Symbian-Viren sind jedoch nur auf den Gerätetypen lauffähig, die das Betriebssystem in der Serie 60 einsetzen (z. B. Nokia 3650, 7650, N-Gage, 6600). Mobile Endgeräte – vom modernen Handy bis zum PDA – sind heute Kleincomputer mit offenen Betriebssystemen. Ähnlich wie über das Internet Viren oder so genannte Würmer auf stationäre PCs gelangen können, sind Virusattacken auf mobile Endgeräte nicht mehr grundsätzlich auszuschliessen. In der Fachpresse und in Internetforen war zu lesen, dass so genannte Smartphones eher anfällig für Virenbefall zu sein scheinen als andere Kategorien. Smartphones, eine Mischung aus Handy und PDA, sind multifunktionale End-

Übersicht über die heute bekannten Handy-Viren (Stand: Ende März 2005)

Datum	Virus	Plattform	Aktivität	Gefahr
15.06.04	Cabir	Symbian	Proof of Concept, Weiterverbreitung via Bluetooth, keine Aktivität	klein
19.07.04	Duts	Windows Pocket-PC	Proof of Concept, infizierte Dateien auf Device, keine automatische Weiterleitung	klein
06.08.04	Brador	Windows Pocket-PC	Manuelle Verbreitung via E-Mail, Backdoor –> Kontrolle des Device Angriff über IP-Verbindung	mittel
10.08.04	Mosquitos	Symbian	Kopiertes Game ohne Lizenz generiert SMS an Premium Number	mittel
19.11.04	Skulls	Symbian	Ersetzt Icons durch Überschreiben des Device ROM, keine selbstständige Verbreitung	hoch
24.01.05	Gavno	Symbian	Trojaner, der Teile des Betriebssystems überschreibt	hoch
17.03.05	Comm Warrior	Symbian	Trojaner, Phone Reset (auf spezielles Datum hin), versendet sich via MMS und Bluetooth	hoch

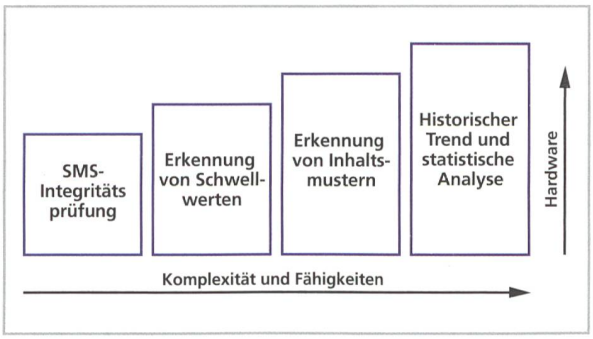

Bild 1. Vier Sicherheitsstufen zur Viren- und Spam-SMS-Erkennung.

geräte mit vergleichsweise hoher Prozessorleistung. Auch Microsoft dringt in diesen Markt ein und so kommen vermehrt Windows-basierte, mobile Endgeräte in den Handel. Was das für die Verbreitung von Viren bedeutet und ob hier ähnliche Effekte auftreten werden wie bei Windows-PCs, ist bisher reine Spekulation.

Zwar sind bis heute bei Swisscom Mobile keine Schadensmeldungen eingetroffen und bisher nur ein einziger Virenbefall bekannt geworden. Die Bedrohungen durch Viren und Belästigungen durch Spam-SMS werden nichtsdestoweniger Ernst genommen. Bereits heute haben Kunden von Swisscom Mobile die Möglichkeit, Spam-SMS der Hotline zu melden. Unter Angabe der Absender-Nummer ist es beispielsweise möglich, den Urheber einer lästigen SMS zu ermitteln, administrative Gegenmassnahmen zu treffen und diese mit dem Kunden zu besprechen.

Generell führt ein gemeinsames Vorgehen aller Beteiligten zu einem höheren Schutz als nur eine Massnahme alleine. Bereits auf Seite der Gerätehersteller können potenzielle Schwachstellen geschlossen werden, etwa durch eine engere Kooperation mit Lieferanten von Sicherheits-Software oder mit der Unterstützung von Sicherheitszertifikaten (digitale Signatur von Programmen). Netzbetreiber können in ihren Netzen die Weiterverbreitung von Viren verhindern. Bei mutwilliger Veränderung kann die Gerätekonfiguration wiederhergestellt werden. Zudem kann bei der Wiederherstellung betroffener Geräte aktive Unterstützung geleistet werden. Auch die Anwender können durch ihr Verhalten die Virenverbreitung aktiv verhindern. Sie sollten beispielsweise nur Software von vertrauenswürdigen Quellen akzeptieren, den Virenschutz installieren und ständig aktualisieren sowie nicht benötigte Funktionen wie beispielsweise Bluetooth ausschalten.

Umfassendes Schutzpaket aktiv

Aufgrund der vielfältigen Bedrohungsszenarien hat Swisscom Mobile weitergehende Schutzmassnahmen getroffen. Das Hauptziel des speziell darauf ausgerichteten Projekts ist der netzbasierte Schutz gegen Viren und Spam-SMS. In einem ersten Schritt werden die Netzüberwachungssysteme hinsichtlich der Früherkennung von Mobil-Viren und Spam-SMS erweitert. Damit werden potenzielle Virenepidemien und Spam-Fluten mit dem Ziel einer gezielten Bekämpfung rechtzeitig erkannt und deren Ausbreitung im Netz bestmöglich verhindert. Das neue Frühwarnsystem basiert unter anderem auf einem aktiven Filtermechanismus aufgrund von Verkehrsmustern, etwa beim massenhaften Versand von SMS mit gleichem Inhalt vom Ausland in das GSM-Netz von Swisscom Mobile. Mit der steigenden Bedrohung werden weitere Schutzmassnahmen gegen Viren und SPAM in die mobilen Netze von Swisscom Mobile eingeleitet. Generell sind vier Sicherheitsstufen zur Viren- und Spam-SMS-Erkennung möglich (Bild 1):

- SMS Integrity Check (SIC): Prüfung der Integrität einer eingehenden SMS
- Realtime Threshold Check (RTC): Erkennung von Schwellwerten in Echtzeit
- Content and Pattern Matching (CPM): Erkennung von Inhaltsmustern
- Historical Trend & Statistical Analysis (HSA): Historischer Trend und statistische Analyse

Mit steigender Funktionalität steigen sowohl die Komplexität, als auch die zum Betrieb des Systems erforderliche Hardware.

IT- und Gebäudesicherheit ein Thema

Bei Swisscom Mobile spielt selbstverständlich auch die IT- und die Gebäudesicherheit eine wichtige Rolle im Sicherheitskonzept. Neben der Sicherung des Zugangs aller Gebäude durch elektronische Schutzeinrichtungen sind die zu schützenden IT-Bereiche in verschiedene Schutzzonen eingeteilt. Diesen Zonen und deren unterschiedlichen Schutzbedürfnissen entsprechend werden vorsorgliche Schutzmassnahmen getroffen. Kriterien zur Zuteilung von Systemen zu einer Zone sind das Schadensausmass bei Nichterfüllen der Sicherheitskriterien (Vertraulichkeit, Verfügbarkeit, Integrität, Nachweisbarkeit). Sie reichen von Grundschutzanforderungen (z. B. allgemeine Arbeitsplätze) über hohe Sicherheitsanforderungen (z. B. Management Systeme) bis hin zu höchsten Sicherheitsanforderungen mit starker Unterteilung innerhalb der Sicherheitszonen (z. B. verkehrsführende Systeme und Datenbanken).

Hohe Verantwortung gegenüber den Kunden

Bei der Diskussion der Viren- und Spam-SMS-Problematik sollte bedacht werden, dass Swisscom Mobile sich überwiegend als Netzbetreiber und nicht als Service Provider betätigt. Viele so genannte Third Party Providers (Drittanbieter, die sich als reine Dienstanbieter betätigen) generieren SMS und versenden diese über das Mobilfunknetz von Swisscom Mobile. Sie nimmt gleichwohl ihre Verantwortung ihren Kunden gegenüber Ernst und versucht, die Bedrohung durch Viren und SMS-SPAM so weit als möglich einzudämmen. Um Schwachstellen möglichst früh zu erkennen und allfällig notwendige Sicherheitsmassnahmen vorzubereiten, wird die Sicherheit der neu auf den Markt kommenden Geräte bereits seit Längerem analysiert. Zudem finden innerhalb der Vodafone-Gruppe (über eine halbe Milliarde Mobilfunkkunden) intensive Dialoge mit den Geräteherstellern und Betriebssystemlieferanten statt, um die Sicherheit neuer Geräte mitbestimmen zu können. ■

Rüdiger Sellin, PR-Manager Swisscom Mobile