Secorvo Security News
Juli 2003

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch

Secorvo Security Consulting GmbH

Nr. 7, 2. Jhrg. 2003
Stand 24. Juli 2003

http://www.secorvo.de/security-news

Inhalt

Editorial: Vertrauensfrage(n)

Zuviel Vertrauen ist häufig eine Dummheit,
zuviel Misstrauen immer ein Unglück.
Johann Nestroy

Leicht geht uns in der IT-Sicherheit das Wörtchen „Vertrauen“ über die Lippen: Wir sprechen von dem Sicherheitsziel „Vertraulichkeit“, von „Vertrauensinfrastrukturen“ und „vertrauenswürdigen Dritten”. Tatsächlich aber sind Schutzmaßnahmen nichts anders als „institutionalisiertes Misstrauen“: Wir schützen uns, weil wir hinsichtlich der Vertrauenswürdigkeit unserer zunehmend digitalen Welt so unsere Zweifel hegen.

Für diese vorsichtige Haltung gibt es viele gute Gründe. Allerdings: Im „wirklichen Leben“ gründen unser zwischenmenschlicher Umgang und unser Wirtschaftsleben auf dem Gegenteil – einer vorwiegend von Vertrauen geprägten Haltung unseren Kollegen, Kunden und Geschäftspartnern gegenüber. Das ist, wie wir heute wissen, nicht nur gut so, sondern auch volkswirtschaftlich bedeutsam: Die wirtschaftliche Entwicklung eines Landes wird inzwischen über „Vertrauensindizes“ prognostiziert.

Tatsächlich vertrauen wir fast täglich „blind“ – z. B. darauf, dass unser Gesprächspartner am Telefon auch derjenige ist, der zu sein er behauptet, dass ein Fax oder eine E-Mail vom angegebenen Sender stammt (wofür es technisch keinen Beleg gibt), und dass ein Gast oder Besucher die auf der Visitenkarte genannte Person ist. Das geht auch fast immer gut – und bestärkt uns in unserem Verhalten. Gefährlich wird es, wenn diese Vertrauensseligkeit ausgenutzt wird und dabei Schäden entstehen, wie z. B. im jüngst bekannt gewordenen Fall einer vermeintlichen Bestellung von 6.000 Kfz von Citroën durch das österreichische Innenministerium.

Dieses Dilemma ist die zentrale Herausforderung für die Informationssicherheit: Ihr muss das Kunststück gelingen, bei Kollegen und Mitarbeitern eine Prise gesunder Skepsis in das notwendige Grundvertrauen zu mischen – ohne Flexibilität und Kundenorientierung zu beeinträchtigen.

1 Security News

1.1 Kreditkartenmissbrauch analysiert

Das Bestellen von Waren und Dienstleistungen per Internet wird auch in Deutschland immer beliebter. In zunehmenden Maße wird dabei – nicht zuletzt aus Bequemlichkeit – auch die Zahlung über E-Mail oder Web-Formular abgewickelt, häufig unter Angabe der Kreditkartennummer.

Dass solche Transaktionen potenziell gefährlich sind, ist lange bekannt. Nun hat es zum ersten Mal eine Gruppe von Securityexperten aus dem „Honeynet"-Projekt geschafft, genauere Informationen über die Vorgehensweise der „Carders" beim Kreditkartenmissbrauch zu dokumentieren. Die Gruppe beobachtete über einen Zeitraum von mehreren Jahren verschiedene einschlägige Foren, insbesondere IRC-Netze, und veröffentlichte am 23.06.2003 ihre Ergebnisse in dem Bericht "Know Your Enemy: Automated Credit Card Fraud".

Besonders interessant ist die Darstellung heutiger „Carder"-Infrastrukturen, die inzwischen über stark automatisierte Tools verfügen sowie Informationen über Online-Händler verbreiten, die keine oder schwache Sicherheitsmechanismen einsetzen.

1.2 CERT-Statistik Q2/2003

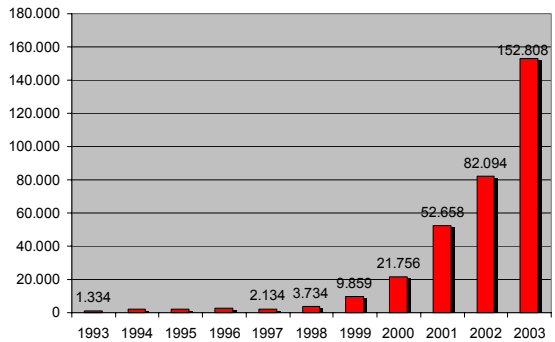

Abb. 1: Gemeldete Sicherheitsvorfälle des CERT/CC (2003: Prognose)

Am 15.07.2003 hat das CERT Coordination Center (CERT/CC) seine Quartalsstatistik veröffentlicht. Danach steigt die Zahl der berichteten Vorfälle nach wie vor steil – für die erste Jahreshälfte 2003 liegt der Wert knapp unter dem des Gesamtjahres 2002.

1.3 Bug in Microsofts HTML-Konverter

Das Konvertieren von Dateien in andere Formate ist eine Funktion des Microsoft Windows Betriebssystems. Sie ermöglicht Anwendungen z. B. die Anzeige und Speicherung von Dateien in HTML. Ein Fehler in der cut-and-paste Operation dieser Konverter-Routine wurde am 09.07.2003 publiziert. Er ermöglicht einem Angreifer, mit einer geeignet gestalteten HTML-E-Mail oder einer Webseite beliebigen Code auf dem Rechner des E-Mail-Empfängers respektive Web-Surfers (sofern dieser den Internet-Explorer verwendet) auszuführen.

Sicherheitseinstufung:

Windows 98/98 SE Windows NT 4.0 Server Windows 2000/XP	kritisch
Windows Server 2003	mittel

1.4 To update or not to update …

Seit dem 26.06.2003 ist das neue Windows 2000 Service Pack 4 verfügbar. Es enthält eine Vielzahl neuer Patches und alle Updates der vorhergehenden Service Packs. Die Installation verursacht allerdings in einigen Fällen Probleme: So warnt Microsoft vor Schwierigkeiten bei der Kombination von Terminaldiensten und dem .Net Framework 1.0 und einem Fehlverhalten des Key Management Service von Microsoft Exchange. Weitere Probleme traten beim Einsatz von Norton Internet Security 2001 auf: Nach der Installation von SP 4 war kein Internetzugriff mehr möglich. Symantec hat ein Update erstellt, welches mit der Option „Live-Update" *vor* der Installation des SP 4 heruntergeladen werden sollte.

In der Regel ist aus Sicherheitsgründen die Installation der aktuellsten Servicepacks zu empfehlen. Die Beispiele zeigen, dass dies jedoch nicht ohne vorausgehende Tests erfolgen sollte.

1.5 Bremen „Europäischer eGovernment Champion“

Bremen ist Sieger der Champions League des eGovernments: Aus dem Wettbewerb um den EU-Preis für vorbildliche Beispiele elektronischer Verwaltungsdienste ist bremen online services (bos), die eGovernment-Strategie der bremischen Verwaltung, am 08.07.2003 als Sieger in der Kategorie „Europäische Konkurrenzfähigkeit" hervorgegangen.

1.6 Hosten Sie Schmuddel-Seiten?

Die Spammer-Branche macht Ernst mit der Anonymität – zumindest mit der eigenen. Der am 11.07.2003 im Internet neu aufgetauchte Trojaner Migmaf erlaubt es, die Rechner nichts ahnender Remote- und Heim-Nutzer (bevorzugt solcher mit „always-on” DSL- oder Kabelmodem-Anschlüssen) nicht nur als Versender von Spam-Mails, sondern auch als Proxy-Server zu missbrauchen: Die Links in den verschickten Spam-E-Mails verweisen dabei nicht direkt auf den Webserver mit den beworbenen Inhalten, sondern auf einen der infizierten PCs; von dort leitet der Trojaner den Zugriff weiter.

Die Spammer sind dabei technisch auf der Höhe der Zeit: Per dynamischem DNS wird in Minutenabständen die IP-Adresse eines anderen missbrauchten PCs verwendet. Dadurch wird es Internet Service Providern praktisch unmöglich gemacht, die von den Spammern benutzten Systeme über eine IP-Filterung auszusperren.

Schutz vor dem beschriebenen Kapern durch Spammer (siehe Abb. 2) bietet eine sauber konfigurierte Personal Firewall.

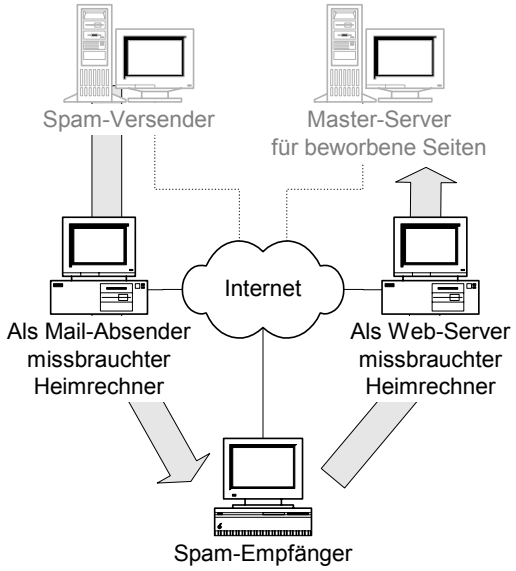

Abb. 2: Funktionsweise eines Trojaner-Spammers

1.7 Gefahr erkannt – Gefahr gebannt?

Zwei aktuelle Meldungen belegen, dass einige Sicherheitsprobleme trotz großer Publicity hartnäckig weiter bestehen:

Richard Smith – bekannt durch seine Untersuchungen über unerwünschte Zusatzinformationen in Office Dokumenten – meldete am 03.07.2003, dass noch immer viele Softwarehersteller ihre ActiveX-Controls als „sicher für Scripting“ markieren, obwohl sie bekannte Sicherheitsmängel aufweisen. Das legt den Verdacht nahe, dass sich die Prüfung dieser Hersteller auf „Absturzsicherheit“ beschränkt. Und die russische Softwarefirma ElcomSoft, deren Rechtsstreit mit Adobe weltweit Schlagzeilen machte, berichtet am 08.07.2003, dass auch zwei Jahre nach der ersten Veröffentlichung die von ElcomSoft entdeckten Sicherheitslücken in Acrobat und Acrobat Reader noch nicht beseitigt sind.

1.8 Denial of Service auf Ciscos IOS

Mit geeignet konstruierten IPv4-Paketen kann ein Denial-of-Service Angriff gegen

IOS-basierte Router von Cisco durchgeführt werden – das wurde am 16.07.2003 bekannt. Cisco stellt Vertragskunden Updates online zur Verfügung. Zur Erleichterung der Prüfung, ob eigene Geräte betroffen sind, hat Foundstone, Inc. eine Funktion zur Bestimmung der IOS-Version in das kostenfreie Tool SNS-Scan integriert.

2 Secorvo News

2.1 Secorvo College aktuell

Auf dem überarbeiteten Seminar „SAP-Sicherheit im Betrieb“ (30.09.-01.10.2003) beleuchten erfahrene Praktiker SAP-Systeme hinsichtlich der Stärken und Schwächen der Sicherheitsarchitektur und Sicherheitsfunktionalitäten von allen Seiten. Im Mittelpunkt stehen Konzepte und Maßnahmen zur Erreichung eines adäquaten Sicherheitsniveaus.

2.2 Neues Video zur „E-Mail Sicherheit“

Dass E-Mails offen wie eine „Postkarte” im Internet übertragen werden, gehört erfreulicherweise inzwischen fast zum Allgemeinwissen. Weniger bekannt ist allerdings, wie leicht es tatsächlich ist, mit frei verfügbaren Tools E-Mails abzuhören oder zu fälschen. Das ist vor allem deshalb bedenklich, weil immer mehr sensible Daten elektronisch übermittelt werden.

Um Mitarbeiter für einen bedachtsameren Umgang mit E-Mails zu sensibilisieren, hat Secorvo ein Lehrvideo entwickelt, das eindrucksvoll Angriffe auf elektronische Nachrichten demonstriert. Es hat eine Spielzeit von zehn Minuten und kann mit gängigen Flash-Playern abgespielt werden.

2.3 PKI-Symposium 2003

Noch ist das Programm in Vorbereitung – der Termin steht aber bereits: Das (vierte) „PKI-Symposium 2003“ wird am 07. und 08.10.2003 in Karlsruhe stattfinden. Über die Webseite können Sie sich schon jetzt einen Platz reservieren. Dort finden Sie auch Programme und Materialien der Symposien der Jahre 2000, 2001 und 2002.

3 Veranstaltungshinweise

August 2003	
04.-08.08.	12th USENIX Security Symposium (USENIX, Washington D.C.)
26.-27.08.	Einführung in die Praxis des betriebl. DSB (Euroforum, Berlin)
September 2003	
08.-10.09.	6th Internat. Symposium on Recent Adv. in Intrusion Detection RAID 2003 (CERT/CC, Pittsburg)
22.-26.09.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
29.09.-02.10.	Informatik 2003 – Teiltagung Sicherheit (GI, Frankfurt)
30.09.-01.10.	SAP-Sicherheit im Betrieb (Secorvo College, Karlsruhe)
Oktober 2003	
07.-08.10.	PKI-Symposium 2003 (Secorvo, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feedback an
redaktion-security-news@secorvo.de