Secorvo Security News
September 2003

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 9, 2. Jhrg. 2003
Stand 22. September 2003

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

Inhalt

Editorial: Happy Birthday

Der 01.09.2003 war für Secorvo ein besonderes Datum. Daher erlauben wir uns diesmal ein Editorial in eigener Sache: Auf den Tag genau am 01.09.1998 hat die Secorvo Security Consulting GmbH mit fünf Mitarbeitern das „Licht der Welt“ erblickt. Zwischen diesen beiden Daten liegen 1.826 ereignisreiche Tage: 167 erfolgreiche Projekte, 135 Publikationen, 133 öffentliche Vorträge, 58 Seminare von Secorvo College mit mehr als 600 überdurchschnittlich zufriedenen Teilnehmern (Note 1,45) aus mehr als 200 Unternehmen und Behörden, und weit über eine Million Webseitenzugriffe.

Secorvo entstand 1998 aus der Vision eines vollständig unabhängigen, ausschließlich den eigenen Kunden verpflichteten und auf IT-Sicherheit spezialisierten Beratungsunternehmens mit besonders kompetenten und erfahrenen Consultants, die durch aktives Engagement in Fachgremien, durch die Mitgestaltung von Normen und Standards der IT-Sicherheit und nicht zuletzt durch Publikationen und hochwertige Projektarbeit einen nachhaltigen Beitrag zur Verbesserung der IT-Sicherheit in Unternehmen und Behörden leisten.

Dieser Vision sind wir treu geblieben – und konnten sie auch in vielerlei Hinsicht Wirklichkeit werden lassen: So ist das Beratungsteam auf zehn anerkannte Experten für IT-Sicherheit angewachsen, Standards wie MailTrusT und ISIS-MTT wurden maßgeblich von Secorvo entwickelt, und namhafte mittelständische und zahlreiche große Unternehmen sowie Landes- und Bundesbehörden haben Secorvo in den vergangenen fünf Jahren mit herausfordernden Projekten betraut.

Dass dieser Erfolg möglich war, verdanken wir neben dem Engagement und dem Einsatz unseres inzwischen 16-köpfigen Teams vor allem den vielen Kunden, die auf Secorvo vertraut haben. Wir sind stolz darauf, deren hohe Erwartungen nicht enttäuscht zu haben – für die Zukunft Ansporn und Anspruch zugleich.

1 Security News

1.1 PGP in neuem Gewand

Am 16.09.2003 stellte die PGP Corp. in London ihr neuestes Software-Release – „PGP Universal“ – der Öffentlichkeit vor. Diese neue Version basiert auf der seit über einem Jahrzehnt bekannten und verbreiteten Verschlüsselungssoftware von Phil Zimmermann, unterscheidet sich aber konzeptionell erheblich von allen Vorgängerversionen: PGP Universal implementiert eine serverbasierte (proxy-artige) Lösung, die transparent und automatisch sämtliche E-Mails (oder solche für festgelegte Kommunikationspartner) ver- und entschlüsselt. Auch mit Kommunikationspartnern, die über kein Schlüsselpaar verfügen, kann man mit PGP Universal gesichert kommunizieren.

Die wichtigste Neuerung bilden sogenannte „Domain Policies“, die es ermöglichen, eine organisationsweite Security Policy zentral zu definieren und duchzusetzen. Damit ist PGP Universal insbesondere für Unternehmen und Behörden interessant. Eine Übersicht finden Sie in einem Beitrag von Dr. Rainer Gerling und Stefan Kelm in der Zeitschrift „DuD“ (10/2003).

Zum Vormerken für Interessierte: Secorvo bietet am 03.-04.12.2003 ein zweitägiges Seminar an, in dem der betriebliche Einsatz von PGP, auch der neuen Produktversion, im Detail beleuchtet wird.

1.2 Kritischer RPC-Bug

Eine neue, als sehr kritisch einzustufende Schwachstelle im RPC-Dienst der Betriebssysteme Windows NT 4.0, 2000, XP und 2003 wurde am 10.09.2003 vom Microsoft veröffentlicht. Sie erlaubt einem Angreifer, über das Protokoll Netbios durch einen Heap Overrun beliebigen Code auf dem Zielsystem auszuführen. Eine Erläuterung mit Patch findet sich im Microsoft Security Bulletin MS03-039.

Delikat: Seit dem 16.09.2003, nur sechs Tage nach Veröffentlichung, ist im Internet ein Exploit zu finden, dass diese Schwachstelle ausnutzt. Wir testeten den Angriffscode im Secorvo Security Labor: Ein Angreifer erhält damit über ein neu angelegtes Konto mit Administrationsberechtigungen vollen Zugriff auf das Zielsystem.

Nach den Erfahrungen der vergangenen Monate muss davon ausgegangen werden, dass diese Schwachstelle sehr bald auch von Würmern ausgenutzt werden wird. Ein umgehendes Einspielen des Patches ist daher dringend zu empfehlen.

1.3 Gefälschte eBay-Server

Wie am 08.09.2003 bekannt wurde, haben Betrüger einen gefälschten eBay-Webserver aufgebaut, um an die Daten von eBay-Kunden zu kommen. Der Trick: Mit einer scheinbar von eBay stammenden E-Mail versuchen sie, ihre Opfer auf den vorgeblichen eBay-Server zu locken. Tatsächlich enthält die E-Mail mit dem korrekt aussehenden Link keinen Text, sondern ein Bild – das mit einer völlig anderen URL hinterlegt ist.

1.4 Trauen Sie Ihrem Browser?

Die Aufdeckung kritischer Schwachstellen in Betriebssystemen und Anwendungen ist leider mittlerweile an der Tagesordnung. Meist handelt es sich dabei um Programmierfehler („Bugs“), die es erlauben, z. B. den Rechner zum Absturz zu bringen oder lokale Dateien auszulesen. Dass immer wieder auch konzeptionelle Sicherheitslücken entdeckt werden, deren Ursache im mangelhaften Design der Software zu finden ist, ist oft weniger geläufig.

Ein prominentes Beispiel für derartige Schwachstellen sind die vom Dartmouth PKI Lab durchgeführten Forschungen zum Thema „Web Spoofing“. Nachdem dieser Begriff bereits 1996 zum ersten Mal in der Literatur auftauchte, testeten die Forscher aus Dartmouth in den vergangenen Jahren

vor allem die gängigen Browser auf Lücken und konnten dabei beeindruckende Ergebnisse erzielen: So gelang es ihnen – unter Verwendung von JavaScript auf präparierten Webseiten – einen Mozilla-Browser so zu überlisten, dass der Benutzer glaubte, eine sichere SSL-Verbindung zu nutzen. Tatsächlich waren sämtliche Fenster, Icons und Links „gefälscht"; sogar die Eingaben auf der Tastatur wurden überwacht.

Etliche detaillierte Lösungsvorschläge der Forscher, die schon Anfang 2002 publiziert wurden, haben leider bis heute keinen Einzug in die Anwendungen gehalten.

1.5 Digitalbilder: Echt oder retuschiert?

Dass Fotos mit zunehmenden Fortschritten in der digitalen Bildbearbeitung mehr und mehr an Beweiskraft verlieren, ist offenkundig. Ein neuer Ansatz zur Rettung der Authentizität digitaler Bilder versucht nun, anhand statistischer Eigenschaften des per Wavelet-Transformation mathematisch umgeformten Bildes Originalaufnahmen von manipulierten Bildern zu unterscheiden.

Dieser Ansatz trifft auch die Steganografie: Sie steht nun vor der Herausforderung, ein Verfahren zu finden, das bei veränderten Bildern die Statistik wieder „richtet".

1.6 GSM-Verschlüsselung unter Beschuss

Vom Israel Institute of Technology (Technion) in Haifa wurde am 03.09.2003 ein Angriff auf die GSM-Verschlüsselung veröffentlicht, der effizienter ist als alle bisher publizierten Attacken auf den Kryptoalgorithmus A5. Die Methode der Forschungsgruppe um Eli Biham reiht sich ein in den Trend, bei der Kryptanalyse zusätzliche Informationen zu nutzen – in diesem Fall aus Verbindungsaufbau und Fehlerkorrektur. Merke: Ein guter Algorithmus alleine ist höchtens die „halbe Miete" – das Einsatzumfeld ist ebenso von Bedeutung.

1.7 Private Internet-Nutzung

Die private Nutzung des dienstlichen Internetzugangs ist eines der derzeit heftigst diskutierten Themen. Zwar ist die Besteuerung als „Geld werter Vorteil" vom Tisch. Doch bei erlaubter oder auch nur geduldeter privater Nutzung unterliegt der Betrieb erheblichen Einschränkungen aus Telekommunikations- (TKG) und Teledienstedatenschutzgesetz (TDDSG), da der Arbeitgeber zum geschäftsmäßigen Anbieter von Telekommunikationsdiensten wird – auch, wenn er die Leistungen unentgeltlich bereitstellt. Denn Inhalts- und Verbindungsdaten einer privaten Kommunikation genießen den strengen Schutz des Fernmeldegeheimnisses (Art. 10 GG, § 87 TKG).

Zwei aktuelle Leitfänden zu diesem Thema klären die Rechtslage und unterstützen mit Mustervereinbarungen die betriebliche Regelung: Der Leitfaden „Datenschutzrechtliche Grundsätze bei der dienstlichen/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz" des Bundesdatenschutzbeauftragten (14.03.2003) und der BITKOM-Leitfaden „Die Nutzung von E-Mail und Internet im Unternehmen" (21.08.2003).

2 Secorvo News

2.1 Secorvo College aktuell

Die erste Oktoberwoche ist „PKI-Woche": In einer zweitägigen Einführung in Public Key Infrastrukturen vom **06.-07.10.2003** und einem eintägigen Vertiefungsseminar PKI für Fortgeschrittene am **09.10.2003** bietet Secorvo einen vertieften Einblick aus umfassender Beratungserfahrung in die Grundlagen und ausgewählte Herausforderungen der Konzeption und des Aufbaus von PKIs.

Seit der Ankündigung von NAI im Oktober des vergangenen Jahres, die PGP-Produktlinie einzustellen, war es um PGP stiller geworden. Nun hat sich die neue PGP Corporation mit neuen Produktversionen zurückgemeldet (siehe oben).

Anfang Dezember (**03.-04.12.2003**) stellen wir in unserem Seminar „PGP & Co. Im betrieblichen Einsatz“ vor, was sich hinter OpenPGP und den aktuellen Konzepten verbirgt, wie PGP sich zum Schutz von E-Mails und zur Verschlüsselung von Dateien in der Unternehmenspraxis einsetzen lässt und was PGP von anderen PKI-Lösungen unterscheidet.

Wegen der großen Nachfrage werden wir das Fünf-Tages-Intensivseminar „Information Security Management von A(udit) bis Z(ertifizierung)“ am **03.-07.11.2003** ein drittes Mal durchführen. Das Seminar vermittelt die wesentlichen Grundlagen eines verlässlichen Sicherheitsmanagements auf technischer und organisatorischer Ebene und liefert konkrete Hilfestellungen für Konzeption und Umsetzung in der Praxis.

http://www.secorvo.de/college

2.2 „IT – Aber sicher!“

Am **30.10.2003** wird Lutz Bleyer, Leiter Zentrale Security der Fiducia AG, im Rahmen des nächsten Events der „Karlsruher IT-Sicherheitsinitiative“ (KA-IT-Si) die Security Awareness-Kampagne der Fiducia „IT – Aber sicher!“ vorstellen. Beginn 18 Uhr, anschließend „Badisches Buffet“.

2.3 „ZertiFA 2003”

Um Licht ins Dunkel des Zertifikate-Dschungels zu bringen, haben Dr. Johann Bizer und Dirk Fox, Herausgeber der Fachzeitschrift „Datenschutz und Datensicherheit (DuD)“ mit COMPUTAS, einem für hochwertige Security-Konferenzveranstaltungen bekannten Anbieter, eine neue Fachtagung konzipiert. Auf der „ZertiFA 2003“ am **10. und 11.11.2003** im Kölner Hotel Hilton werden Zertifikate und Gütesiegel von BS 7799 über BSI-Grundschutz- und Datenschutzaudits bis ITSEC- und CC-Zertifizierungen vorgestellt und vor dem Hintergrund aktueller Erfahrungsberichte diskutiert.

3 Veranstaltungshinweise

September 2003	
29.09.-02.10.	Informatik 2003 – Teiltagung Sicherheit (GI, Frankfurt)
Oktober 2003	
06.-07.10.	Public Key Infrastrukturen (Secorvo College, Karlsruhe)
09.10.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
14.-15.10.	Lotus Notes Security (Secorvo College, Karlsruhe)
28.-29.10.	Defense Lab (Secorvo College, Karlsruhe)
30.10.	„IT – Aber sicher!“ (KA-IT-Si, Karlsruhe)
November 2003	
03.-07.11.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
10.-11.11.	ZertiFA 2003 (Computas, Köln)
11.-13.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
18.-19.11.	Inside Windows Security (Secorvo College, 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