Secorvo Security News
Dezember 2003

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

Nr. 12, 2. Jhrg. 2003
Stand 17. Dezember 2003

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

Inhalt

Editorial: Patchwork

Was haben aktuelle Softwareversionen und neumodische Jeans gemeinsam? Ganz einfach: Beide sind nur mit Löchern echt.

Mittlerweile haben wir uns daran gewöhnt: Ein neues Programm ist ein unsicheres Programm. Nicht etwa, weil es nicht funktioniert oder ständig abstürzt – das war früher – sondern weil es mit Sicherheitslöchern ausgeliefert wird. Erst nach mehrmaligen Nachbesserungen reift es – Patch für Patch – zu einer Programm- oder Betriebssystemversion, die mit gutem Gewissen für den Produktivbetrieb frei gegeben werden kann.

Diese Entwicklung hat dazu geführt, dass sich die „Organisation der Flicken“ (Patchmanagement) zu einer neuen Disziplin der IT-Security gemausert hat, der das amerikanische NIST im vergangenen Jahr sogar eine Special Publication (SP 800-40) widmete. Keine einfache Disziplin. Nicht genug damit, dass ein rechtzeitiges Einspielen von Patches die Kenntnis von Sicherheitsloch und Flicken voraussetzt: Ohne Tests sollte ein Patch nicht in den operativen Betrieb „entlassen“ werden. Nicht selten verursachen Patches unerwünschte Seiteneffekte – es kann passieren, dass von systemspezifischen Bibliotheken abhängige Anwendungsprogramme anschließend den Dienst versagen. Bei einigen Software-Anbietern erlischt zudem die Betriebsgarantie, sobald das System unter modifiziertem Betriebssystemcode betrieben wird. Und die Zeit zwischen der Entdeckung eines Programmfehlers und der Verfügbarkeit eines „Exploits“ im Internet schrumpft kontinuierlich. Der Patch-Bezug selbst ist auch nicht frei von Fallen: Zahlreiche Empfänger sind den jüngsten, vermeintlich von Microsoft stammenden „Patch-E-Mails“ auf den Leim gegangen.

Zwar wissen wir nicht, ob die Sicherheits-Löcher wie die der Jeans kunstvoll und mit Vorsatz hineingerissen wurden. In einem unterscheiden sich Jeans und Programme jedoch sicher: Die Löcher in letzteren sind keine vorübergehende Modeerscheinung.

1 Security News

1.1 CERT für den Mittelstand

Computer Notfallteams (CERTs) existieren – auch in Deutschland – bereits seit einem Jahrzehnt. Meist richten sich die Dienstleistungen dieser CERTs, wie etwa die Bearbeitung von Sicherheitsvorfällen oder die Herausgabe von Sicherheitsbulletins, an größere Unternehmen. Auch Behörden und Forschungseinrichtungen betreiben eigene Notfallteams.

Bislang nicht bedient wurden jedoch klein- und mittelständische Unternehmen; dies hatte vor allem finanzielle Gründe. Diesem Umstand trug jetzt der Branchenverband BITKOM Rechnung: Am 09.12.2003 entließ er ein von einer Tochtergesellschaft getragenes Notfallteam für den Mittelstand, kurz Mcert, in den Echtbetrieb. Für eine Jahresgebühr ab € 50 (Basic) oder etwas individueller ab € 300 (Professional) stellt das Mcert Kunden z. B. Warnmeldungen über Software-Schwachstellen zur Verfügung. Zwar unterscheidet sich die Beispielmeldung kaum von den bis heute kostenlos verfügbaren Angeboten anderer CERTs (DFN-CERT, RUS-CERT, etc.), ein CERT mit klarem Mittelstands-Fokus wurde jedoch schon lange erwartet.

1.2 Biometrie-Fiasko

Am 27.11.2003 veröffentlichte das BSI den Abschlussbericht des Projekts BioFace, in dessen Verlauf vier verschiedene Gesichtserkennungssysteme beim BKA getestet wurden. Das ernüchternde Ergebnis: die Falsch-Rückweisungs-Rate (FRR) lag zwischen 64 % und 99,7 %. Das Urteil: Für einen Einsatz bei der Zutrittskontrolle „in keiner Weise akzeptabel“.

Ungeachtet solcher technischen Resultate haben just am selben Tag die Innen- und Justizminister der EU die Integration eines Chips in Visa und Aufenthaltstitel beschlossen – auf dem zukünftig Gesicht und Abdrücke zweier Finger gespeichert werden.

1.3 Murphy hat doch recht

Am 26.11.2003 führte eine für extrem unwahrscheinlich gehaltene Kette von Ereignissen zum ersten „unbeabsichtigten Distributed Denial-of-Service Angriff“ auf große Teile des europäischen DNS.

Die Chronologie: Anfang November wurde die Nord-Route des Transatlantik-Unterseekabels TAT-14 unterbrochen. Während der mehrwöchigen Reparaturarbeiten trat am 25.11.2003 auch bei der redundanten Süd-Route des Kabels ein Kabelbruch auf. Dadurch wurden die Europa-Verbindungen des amerikanischen Providers above.net gestört. Als dann am 26.11.2003 die Auto-Update Funktion der verbreiteten Personal-Firewall Software ZoneAlarm nach dem Server des Herstellers Zone Labs suchte, warteten europäische DNS-Server vergebens auf eine Antwort aus den USA – denn die DNS-Server von Zone Labs sind über above.net angebunden. Die Last der in kurzen Abständen vieltausendfach wiederholten DNS-Anfragen zwang kurz danach verschiedene DNS-Server in die Knie – ein neuer Beleg für die Unumstößlichkeit von Murphy’s Law.

Zone Labs wurde übrigens unabhängig von diesen Ereignissen am 15.12. vom Firewall-Marktführer Check Point übernommen.

1.4 Lücke in Zertifikatskette

Ab dem 07.01.2004 kann es zu Problemen mit SSL-Zertifikaten kommen, die von der VeriSign International Server CA – Class 3 ausgestellt wurden. Grund: Die Gültigkeit des Zertifikats einer unterhalb der VeriSign-Root-CA operierenden „intermediate CA“ läuft ab. Zwar hat VeriSign bereits 2001 auf dieses Problem hingewiesen und das Zertifikat bis 2011 verlängert. Das nun ablaufende Zertifikat befindet sich jedoch noch immer auf vielen Clients, vor allem Internet-Browsern. Das Problem lässt sich Server-seitig durch Übermitteln der neuen Zertifikatskette beim Verbindungsaufbau oder Client-seitig durch Download des neuen CA-Zertifikats beheben.

1.5 Neue Version des GSHB

Am 16.12.2003 erschien im Bundesanzeiger-Verlag die 5. Ergänzungslieferung zum IT-Grundschutzhandbuch des BSI. Darin wurden einige der Bausteine aktualisiert und Bausteine zu Outsourcing, IIS, Apache Webserver, Exchange/Outlook 2000 und der Archivierung von Daten ergänzt. Die Online-Version des neuen GSHB wird Ende Januar 2004 verfügbar sein.

Außerdem wurden zum 01.12.2003 das Prüfschema zur Durchführung einer Zertifizierung nach IT-Grundschutz, die Aufgaben des Zertifizierers und das Lizensierungsschema für IT-Grundschutz-Auditoren überarbeitet.

1.6 Einbruch bei Debian

Am 21.11.2003 wurde eine Kompromittierung verschiedener Server des Linux-Distributionsprojekts Debian entdeckt. Die Rekonstruktion des Vorfalls ergab, dass die Angreifer sich mit einem abgehörten Passwort eines Debian-Entwicklers auf einer Maschine anmeldeten und sich anschließend mit einem lokalen Root-Exploit Superuser-Rechte verschafften.

Hauptursache: Nachlässiges Patchmanagement. Denn die vom Root-Exploit ausgenutzte Sicherheitslücke im Linux-Kern war seit September bekannt und in Entwicklerversionen des Kernels schon eliminiert, wurde aber erst nach dem Vorfall im Kernel 2.4.23 beseitigt und auf den Debian-eigenen Servern gestopft.

1.7 Satelliten-Dialer

Mit ungebremster Kreativität legen sich die Dialer-Anbieter ins Zeug. Wie auf der Informationsseite dialerschutz.de ausführlich dargestellt, werden inzwischen sogar Verbindungen über Satelliten (Vorwahl 0088) von Dialer-Programmen genutzt. Die Kosten liegen bei gut 3 € pro Minute.

Mit Wirkung vom 14.12.2003 erklärte die RegTP daher Dialer, die nicht die registrierungspflichtige Vorwahl (0)9009 nutzen, als illegal: Für den geprellten „Nutzer“ entfällt damit die Zahlungspflicht.

1.8 Bürgerkarte in Österreich

Was in vielen europäischen Ländern noch immer ein Wunschtraum ist, soll in Österreich jetzt Wirklichkeit werden: die Einführung einer digitalen Bürgerkarte, mit der landesweit Behördengänge online und in abgesicherter Form erledigt werden können.

Das Konzept der Bürgerkarte genügt den Anforderungen des österreichischen Signaturgesetzes, gestattet jedoch explizit, dass „neue Speichermedien wie etwa USB-Tokens oder Handy-SIMs ebenfalls bürgerkartenfähig sein können.“ Es wurde bewusst darauf verzichtet, die in der Praxis noch immer wenig verbreiteten evaluierten „sicheren Signaturerstellungseinheiten“ zu fordern. Die Anerkennung derartiger elektronischer Signaturen durch andere EU-Mitgliedsstaaten könnte zwar daran scheitern (wie jüngst in der Studie der EU-Kommission erläutert), der praktische Nutzen der Karte steigt damit jedoch erheblich.

1.9 VDEW setzt auf ISIS-MTT

Am 01.09.2003 haben die sechs Spitzenverbände der deutschen Stromwirtschaft unter Führung des VDEW in einer gemeinsamen Erklärung die Sicherheitsrahmenbedingungen für den elektronischen Geschäftsverkehr innerhalb der Branche festgelegt. Mit Blick auf die Interoperabilität setzt das VEDIS Projekt dabei auf eine X.509-PKI und das Austauschformat S/MIME in der Ausprägung nach ISIS-MTT.

1.10 ENISA beschlossen

Das EU-Parlament hat am 20.11.2003 die Einrichtung einer Europäischen Agentur für Netzwerk- und Informationssicherheit (ENISA) beschlossen. Schon im Januar soll die zunächst auf fünf Jahre geplante und mit einem Budget von € 24,3 Mio. ausgestattete Behörde die Arbeit aufnehmen. Sitz und Besetzung sind noch umstritten.

2 Secorvo News

2.1 Secorvo College aktuell

Das Seminarangebot von Secorvo College startet im Januar mit dem fünftägigen Intensivseminar „Information Security Management von A(udit) bis Z(ertifizierung)“ (**19.-23.01.2004**), dessen erste beiden Tage (**19.-20.01.2004**) auch separat gebucht werden können. Konkretisiert werden die rechtlichen Anforderungen und Standards am Beispiel eines fiktiven Unternehmens.

Das Seminar „Public Key Infrastrukturen (PKI)“ (**27.-28.01.2004**) führt in Grundlagen, Aufbau und Organisation von Schlüsselinfrastrukturen ein – vor dem Hintergrund der Erfahrung von Secorvo aus zahlreichen PKI-Projekten. Für Experten folgt am **29.01.2004** eine eintägige Vertiefung („PKI für Fortgeschrittene“).

Im Februar (**10.-11.02.2004**) werden im „Live Hacking Lab“ spektakuläre und trickreiche Angriffe auf verbreitete Systeme und Anwendungen durchgeführt und analysiert.

2.2 DuD elektronisch

Zukünftig wird es die Fachzeitschrift „Datenschutz und Datensicherheit (DuD)“ auch in digitaler Form geben. In den Genuss einer pdf-Fassung des Jahrgangs 2003 kommt vorab jeder, der die DuD bis zum **31.01.2004** über Secorvo mit einem speziellen Bestellformular abonniert.

2.3 Video “trojan horse”

Aufgrund des großen Erfolgs des viel gelobten Videos „E-Mail-Sicherheit“ und zahlreicher Anfragen wird ab Februar 2004 auch das Video „Trojanische Pferde“ in einer grundlegend überarbeiteten Fassung als Flash-Video in deutscher und englischer Sprache (mit „Native Speaker“) erhältlich sein. Beide wurden bereits von der Linde AG und der T-Systems als Unternehmenslizenz für den Einsatz im Intranet erworben.

3 Veranstaltungshinweise

Dezember 2003	
24.12.	Bescherung
Januar 2004	
19.-20.01.	IT-Security Management (Secorvo College, Karlsruhe)
19.-23.01.	Information Security Management (Secorvo College, Karlsruhe)
20.-21.01.	Einführung in die Praxis des betr. DSB (Euroforum, München)
27.-28.01.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
29.01.	PKI für Fortgeschrittene (Secorvo College, Karlsruhe)
Februar 2004	
03.-04.02.	Workshop Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
10.-11.02.	Live Hacking Lab (Secorvo College, Karlsruhe)
März 2004	
02.-03.03.	Lotus Notes Security (Secorvo College, Karlsruhe)
09.-10.03.	Einführung in die Praxis des betr. DSB (Euroforum, München)

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