Secorvo Security News
Juli 2002

Dirk Fox
Secorvo Security Consulting GmbH

Nr. 1, 1. Jhrg. 2002
Stand 04. Juli 2002

Inhalt

Editorial: Eine Schneise in die Informationsflut

Der Berg an Nachrichten und Informationen wächst auch im Gebiet IT-Sicherheit täglich – und damit auch der Zeitbedarf, den Sie aufwenden müssen, um „auf dem Laufenden“ zu bleiben, wesentliche Entwicklungen nicht zu verpassen und die wichtigsten Informationen zu bewerten: Was bedeutet diese Erkenntnis oder jenes Ereignis für mich und meine IT-Systeme?

Mit den in dieser Ausgabe erstmals vorliegenden Secorvo Security News möchten wir Sie dabei unterstützen.

Auch auf uns prasseln täglich unzählige Informationen ein, die wir in unserem Expertenteam filtern, diskutieren, abwägen und bewerten. Daraus entstand die Idee, auch Sie davon profitieren zu lassen.

Die Secorvo Security News sollen

- Sie auf **wichtige aktuelle Ereignisse und Entwicklungen** in der IT-Sicherheit aufmerksam machen,
- Ihnen durch die **Angabe der wesentlichen Quellen** die Informationsrecherche erleichtern und
- Ihnen durch eine **unabhängige Expertenmeinung** bei der Bewertung dieser Nachrichten helfen.

Zugleich möchten wir die Informationsflut nicht unnötig vermehren. Daher erscheinen die Secorvo Security News nicht mehr als **12 mal im Jahr** – genug, um der Schnelllebigkeit heutiger Entwicklungen ein besonnenes Urteil entgegen zu stellen.

Außerdem beschränken wir uns auf Wesentliches: Sie erfahren nicht alles, aber das, was Sie unserer Ansicht nach wissen sollten – weniger erscheint uns hier mehr.

Schließlich schicken wir Ihnen nicht das gesamte Dokument, sondern nur das Inhaltsverzeichnis der aktuellen Ausgabe und den Web-Link: Sie entscheiden, ob Sie das etwa 100 kB große PDF-Dokument laden möchten.

1 Security News

1.1 „Gummi Fingers“

Mit seinem Beitrag auf der „Rump Session“ der diesjährigen Kryptokonferenz „Eurocrypt“ ließ der japanische Forscher T. Matsumoto eine „Bombe“ hochgehen: Er stellte die Ergebnisse von Experimenten seiner Forschungsgruppe vor, die sich vorgenommen hatte, mit „Hausmitteln“ wie Silikon und Gelatine und einfachsten Hilfsmitteln Fingerprint-Scanner zu überlisten.

Die Ergebnisse sind ernüchternd: Alle 11 getesteten kapazitiven und optischen Fingerprint-Systeme unterschiedlicher Hersteller ließen sich in mindestens 67% der Testfälle von den falschen Fingern täuschen. Ein herber Schlag für den Hoffnungsträger der Biometrie.

Original: http://cryptome.org/gummy.htm

Präsentation: http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.pdf

1.2 Bugs in Open Source

Gerne werden in der Diskussion um Open Source Software Sicherheitsargumente bemüht: Ist der Quellcode offengelegt, so die Open-Source-Verfechter, könne er von einer weit größeren Zahl von Experten überprüft werden als bei herkömmlicher kommerzieller Software.

Das Argument verkennt, dass im wirklichen Leben häufig Welten zwischen „Können“ und „Tun“ liegen. Das hat nicht zuletzt der schwere Spezifikationsfehler im OpenPGP-Standard bewiesen, der von Klíma und Rosa im April 2001 entdeckt wurde – 2,5 Jahre nach Veröffentlichung des Standards als RFC.

Die Security Alerts des Juni 2002 haben dem Glauben an fehlerarme Open Source Software weiter zugesetzt: In drei wichtigen Softwarepaketen wurden schwer wiegende Bugs entdeckt – die dort jahrelang unbemerkt schlummerten.

1.2.1 Löcher in Apache

Oft als die „sichere Alternative“ gelobt und nicht zuletzt deswegen mit einem erheblichen Marktanteil unter installierten HTTP-Servern, traf es Apache im Juni gleich zweimal hart: Am 17.06.2002 wurde ein Heap Buffer Overflow gemeldet, der einen DoS-Angriff und das Ausführen beliebigen Codes auf dem Server erlaubt. Betroffen sind die Versionen 1.2 bis 2.0 sowie OpenBSD und eine große Zahl verbreiteter Linux-Derivate von Caldera bis SuSE.

http://www.iss.net/security_center/static/9249.php

Nur acht Tage später wurde ein zweiter Buffer Overflow gemeldet, über den ein Angreifer beliebige Kommandos auf dem System ausführen kann. Diesmal sind alle Versionen des Apache HTTP Server, alle Linux- und Unix-Versionen, OpenBSD 3.1 sowie alle Versionen des mod_ssl Moduls bis Version 2.8.9 betroffen.

http://www.iss.net/security_center/static/9415.php

1.2.2 Fehler in OpenSSH

Am 26.06.2002 wurde von ISS und CERT ein schwerer Fehler in OpenSSH publiziert: Mit geeignet formatierten Response-Paketen kann ein Angreifer einen Integer Überlauf im Code der Challenge Response Authentication (SKEY oder BSD_AUTH) verursachen und beliebigen Code mit den Privilegien des sshd Prozesses ausführen – wenn Privilege Separation nicht aktiviert ist, entspricht das der Root-Berechtigung.

Betroffen sind alle OpenSSH-Versionen von 2.9.9 bis einschließlich 3.3.

http://www.kb.cert.org/vuls/id/369347

Die fehlerfreie Version 3.4 findet sich unter

ftp.openbsd.org:/pub/OpenBSD/OpenSSH

1.2.3 BIND Bugs

Das CERT-Advisory vom 05.06.2002 warnt vor einem Fehler in der aktuellen Version 9

des Berkeley Internet Name Daemon (BIND). Angreifer können den Fehler nutzen, um den Dienst zum Absturz zu bringen. Ausnahmsweise sind Sie diesmal mit älteren Versionen besser bedient.

http://www.kb.cert.org/vuls/id/739123

Alle BIND-Versionen sowie OpenBSD 2.9 bis 3.1 ermöglichen einem Angreifer, einen Buffer Overflow in der DNS Resolver Library zu verursachen, der die Ausführung beliebigen Codes erlaubt (27.06.2002):

http://www.iss.net/security_center/static/9432.php

1.3 Überwachung am Arbeitsplatz

Die Datenschutz-Arbeitsgruppe der EU-Kommission („Art. 29 Gruppe“) hat am 29.05.2002 ein Arbeitspapier zur "Überwachung der elektronischen Kommunikation von Beschäftigten" veröffentlicht. Dort werden die (EU-) rechtlichen Grenzen der Kommunikationsüberwachung am Arbeitsplatz zusammengefasst und eine Unterscheidung von privat nutzbarer und geschäftlicher E-Mail-Adresse empfohlen:

http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp55_en.pdf

1.4 Telekommunikations-überwachung

Telekommunikationsüberwachung hat seit dem 11.09.2001 Konjunktur. Fast monatlich erweitern neue Bestimmungen die Eingriffsbefugnisse des Staates. Lesenswert dazu der Bundesratsantrag des Landes Thüringen vom 12.06.2002:

http://www.dud.de/dud/documents/brdrs513-02-020612.pdf

Beunruhigend auch die Tischvorlage zum Europol Expert Meeting on Cyber Crime zwischen Law Enforcement Experten vom 11.04.2002, die nun bekannt wurde:

http://www.dud.de/dud/documents/europol-expmeeting-020411.pdf

Auch die deutschen Behörden waren nicht untätig. Auf der Grundlage des § 11 TKÜV wurde von der Regulierungsbehörde für Telekommunikation und Post (RegTP) am 07.05.2002 eine ETSI-konforme Richtlinie (Version 3.1) der Anforderungen an technische Einrichtungen zur Überwachung der Telekommunikation veröffentlicht (pdf, 1,58 MB).

http://www.dud.de/dud/documents/trtkue31.pdf

Liste aller wichtigen Abhörbestimmungen:

http://www.datenschutz-und-datensicherheit.de/dudserver/abhoeren.htm

2 Secorvo News

2.1 IT-Outsourcing? Aber sicher!

Spätestens seit der spektakulären Ankündigung der Deutschen Bank AG, über ein Outsourcing ihrer gesamten IT-Infrastruktur nach zu denken, steht das Thema „IT-Outsourcing“ – gewollt oder ungewollt – oben auf der Tagesordnung vieler CIOs und IT-Verantwortlicher.

Welche Argumente auch immer für oder gegen ein IT-Outsourcing sprechen mögen: Ohne Zweifel kommt der IT-Sicherheit bei Planung und Umsetzung eine zentrale Rolle zu.

Welche Fragen sich dabei stellen und von Ihnen gelöst werden sollten, skizzieren Ingmar Camphausen, Dr. Volker Hammer, Stefan Kelm, Dr. Dörte Neundorf und Dr. Holger Petersen im neuen, noch „druckfrischen“ **Secorvo White Paper „IT-Outsourcing? Aber sicher!“**.

Nicht das „ob“ oder „ob nicht“ ist Gegenstand dieses vierten Secorvo White Papers: In Gestalt einer Checkliste will es Ihnen Hilfestellung bei der Bewältigung sein.

http://www.secorvo.de/whitepapers

2.2 IT Risk Management

KontraG und Basel II haben mit der Forderung einer unternehmensweiten Risikovorsorge auch IT Risiken in das Blickfeld des Managements gerückt. Mit den brutalen Anschlägen des 11. September 2001 haben diese Risiken eine neue Dimension gewonnen; „Best Practices" erfreuen sich seither großer Nachfrage.

Zusammen mit der Computas GmbH, mit der uns viele Jahre enger Zusammenarbeit verbinden und die als Veranstalter besonders hochwertiger Fachkonferenzen bekannt ist, haben wir die Konferenz „**IT Risk Management 2002**" (**23.-24.09.2002**) inhaltlich konzipiert. „Best Practices" wurde dabei breiter Raum gewährt.

http://www.computas.de/itrisk2002-fly.html

2.3 Secorvo College

Im Oktober 2002 beginnt die „Herbst-Saison" von Secorvo College.

http://www.secorvo.de/college

Erstmalig bieten wir am **10.10.2002** ein PKI-Vertiefungsseminar „**PKI für Fortgeschrittene**" an.

2.4 PKI-Symposium

In den beiden vergangenen Jahren war es bis auf den letzten Platz ausgebucht – das von Secorvo im Jahr 2000 erstmals durchgeführte „PKI-Symposium" für den Erfahrungsaustausch und die Diskussion aktueller Fragestellungen im Bereich PKI.

Der Hype ist vorüber: Welche Anwendungen bergen nun den erwarteten Return of Invest? Was lässt sich aus den Erfahrungen der Innovationsträger lernen? Was sind die Herausforderungen von morgen?

Auf der Agenda des diesjährigen **PKI-Symposiums 2002** (**08.-09.10.2002**) werden wieder spannende Fragestellungen und aktuelle Praxisberichte rund um das Thema PKI stehen (in Kürze online).

http://www.pki-symposium.de

3 Veranstaltungstermine

August 2002	
24.08.	Kieler Datenschutz Sommerakademie 2002 (ULD SH)
September 2002	
23.-24.09.	IT Risk Management 2002 (Computas)
24.-25.09.	Einführung in die Praxis des betrieblichen DSB (Euroforum)
Oktober 2002	
07.-08.10.	Public Key Infrastrukturen (Secorvo College)
08.-09.10.	PKI-Symposium 2002 (Secorvo)
10.10.	PKI für Fortgeschrittene (Secorvo College)

Web-Tipp: 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. Ein Archiv aller Ausgaben finden Sie unter

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

Eine automatische 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 Feed-Back an
redaktion-security-news@secorvo.de