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

Secorvo Security News
August 2002

Dirk Fox
Secorvo Security Consulting GmbH

Nr. 2, 1. Jhrg. 2002
Stand 09. August 2002

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

Inhalt

Editorial: Lang ist lang genug

Seit 25 Jahren tobt die Diskussion über angemessene Mindestschlüssellängen für kryptografische Verfahren. Sie begann mit dem Data Encryption Standard (DES): Erst nachdem die National Security Agency (NSA) die Schlüssellänge des ursprünglichen IBM-Entwurfs von 128 auf 56 bit verkürzt hatte, wurde der DES 1977 zum amerikanischen NBS-Standard. Im selben Jahr skizzierten die Kryptologen Diffie und Hellman die Konstruktion eines Chips, der in etwa 12 Stunden einen DES-Schlüssel finden sollte.

Tatsächlich wurde erst 22 Jahre später eine funktionierende DES-Entschlüsselungsmaschine konstruiert: Die von der Electronic Frontier Foundation (EFF) finanzierte Entwicklung benötigte mit 1.800 parallelen Spezialchips ("Deep Crack") immer noch knapp 56 Stunden, um einen DES-Schlüssel heraus zu finden.

Das Beispiel zeigt, dass aus theoretischen Betrachtungen abgeleitete Befürchtungen und reale Möglichkeiten weit auseinander klaffen können. Das gilt gelegentlich auch für Empfehlungen einer Mindestlänge für kryptografische Schlüssel. Insbesondere bei asymmetrischen Kryptoverfahren ist für die Bestimmung der Mindestschlüssellänge nicht nur die zukünftige Entwicklung der Rechenleistung zu prognostizieren, sondern es müssen auch mögliche neue mathematische Erkenntnisse berücksichtigt werden. Groß ist die Versuchung, auf „Nummer Sicher“ zu gehen, wie im Entwurf der Algorithmenempfehlung 2002 des BSI zum Signaturgesetz, deren Endfassung von der RegTP für Herbst 2002 angekündigt wurde:

http://www.bsi.bund.de/esig/basics/techbas/krypto/bund02v5.pdf (43 kB)

In einer Stellungnahme hat Secorvo die Entwicklung der Faktorisierungserfolge der vergangenen 25 Jahre ausgewertet – und hält deutlich kürzere RSA-Schlüssellängen für ausreichend sicher:

http://www.secorvo.de/whitepaper

1 Security News

1.1 SPHINX-Einsatzempfehlungen des BSI

Das BSI hat jüngst die Ergebnisse der im ersten Quartal 2001 durchgeführten Interoperabilitätstests mit einer Empfehlung für Sphinx-konforme E-Mail-Verschlüsselungslösungen publiziert. Darin erhielten nur drei Produkte (zwei Plugins für Outlook 98 und eine Lösung für Groupwise 5.5) eine uneingeschränkte Empfehlung:

http://www.bsi.de/aufgaben/projekte/sphinx/interop/empf102.htm

1.2 ISIS-MTT Version 1.0.2

Mit Unterstützung des BMWi wurde im vergangenen Jahr unter der Federführung von TeleTrusT Deutschland der Standard ISIS (Industrial Signature Interoperability Specification) der Trustcenter-Gruppe „T7“ mit dem von Secorvo für TeleTrusT entwickelten PKI- und E-Mail-Sicherheitsstandard MailTrusT zu einem gemeinsamen Standard ISIS-MTT verschmolzen. Die erste Version dieser auf X.509, PKIX und S/MIME aufbauenden Spezifikation wurde am 01.10.2001 veröffentlicht. Inzwischen ist ISIS-MTT obligatorischer Teil von SAGA (Standards und Architekturen für eGovernment Anwendungen). Auf der Grundlage zahlreicher Kommentare wurde am 19.07.2002 die Version 1.0.2 publiziert:

http://www.teletrust.de/teletrust.asp?id=61040

1.3 Bugs in OpenSSL, Trojaner in OpenSSH

Am 30.07.2002 informierten DFN- und RUS-CERT über fatale Fehler in OpenSSL: In allen Versionen bis einschließlich 0.9.6d kann auf unterschiedliche Weise ein Buffer Overflow verursacht werden, der die Ausführung beliebigen Codes auf dem SSL-Server im privilegierten (Root-)Mode ermöglicht. Gegenmaßnahme: Update auf OpenSSL Version 0.9.6e oder Lösungen der Hersteller abwarten:

http://cert.uni-stuttgart.de/ticker/article.php?prev=905

Ende Juli 2002 wurden die Domainen ftp.openbsd.org und ftp.openssh.org Hackeropfer: Am 01.08. wurden mehrere SSH-Versionen mit integriertem trojanischen Pferd entdeckt (und entfernt):

http://cert.uni-stuttgart.de/ticker/article.php?mid=911

1.4 Win2000 Security Patch

Am 01.08.2002 wurde von Microsoft das lange angekündigte Service Pack 3 (SP3) für Windows 2000 publiziert, das überwiegend Sicherheitslücken behebt:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/w2ksp3.asp

1.5 AES im SSL-Standard

Ende November 2001 wurde nach einem vierjährigen fachöffentlichen Bewertungsprozess der in Belgien entwickelte Verschlüsselungsalgorithmus Rijndael vom amerikanischen National Institute of Standards and Technology (NIST) als Advanced Encryption Standard (AES) ausgewählt und als FIPS 197 veröffentlicht:

http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (243 kB)

Nun wird diesem Nachfolger des in die Jahre gekommenen DES der Weg in die Anwendungen geebnet: Mit RFC 3268 hat die Internet Engineering Task Force (IETF) im Juni 2002 die Liste der von SSL (Transport Layer Security Protocol – TLS) unterstützten Verschlüsselungsverfahren um den AES ergänzt:

http://www.ietf.org/rfc/rfc3268.txt

Bisher unterstützte der SSL-Standard (RFC 2246 vom Januar 1999) nur die Algorithmen RC2, RC4, IDEA, DES und 3DES.

1.6 PKI-Umfrage

Die TeleTrusT-Arbeitsgruppe „Public Key Infrastrukturen“ (AG 7) hat eine Web-Umfrage zum Stand von Public Key Infrastrukturen in Deutschland gestartet:

http://www.teletrust.de/glossar.asp?ID=60880,3&HomePG=0&sw=1&Sprache=D

Die Arbeitsgruppe erhofft sich eine repräsentative Erfassung aktueller PKI-Trends. Einen Zwischenstand der Umfrage wird der Leiter der AG 7, Fritz Bauspieß, auf dem diesjährigen PKI-Symposium 2002 in Karlsruhe vorstellen.

1.7 IT-Sicherheitskongress

Der 8. Deutsche IT-Sicherheitskongress des BSI wird vom **13.-15.05.2003** in Bonn stattfinden. Das Programmkomitee des alle zwei Jahre organisierten Kongresses hat am 18.07.2002 den "Call for Papers“ veröffentlicht. Damit werden interessierte Autoren zur Einreichung fachkundiger Beiträge bis 10.10.2002 aufgefordert:

http://www.bsi.bund.de/veranst/bsikongr/cfp.pdf (91 kB)

1.8 EU-Datenschutzrichtline

Die am 12.07.2002 verabschiedete EU-Datenschutzrichtlinie für elektronische Kommunikation ist nun online verfügbar. Sie muss bis 31.10.2003 in nationales Recht umgesetzt werden:

http://europa.eu.int/eur-lex/de/dat/2002/l_201/l_20120020731de00370047.pdf (167 kB)

1.9 „Liberty Alliance“ strikes back

Nachdem die Akzeptanz von Microsofts .NET-Konzept, eines Web-basierten Authentifikationsdienstes, bisher bescheiden ausfällt, haben nun die unter Führung von Sun in der „Liberty Alliance“ zusammengeschlossenen Mitbewerber am 15.07.2002 ihre Architektur-Spezifikation publiziert:

http://www.project-liberty.org/specs/main.html

2 Secorvo News

2.1 ISIS-MTT-Testbed

Im Auftrag von TeleTrusT Deutschland e.V. hat Secorvo auf Basis der Testspezifikation für ISIS-MTT-konforme Produkte einen Testbed Prototyp entwickelt, der am 01.08.2002 fertiggestellt wurde.

Diese weit gehend automatisierte, auf angepasster Open-Source-Software und eigenen Tools basierende Testumgebung wird im Herbst verfügbar sein. Den Prototyp wird Projektleiter Hans-Joachim Knobloch auf dem diesjährigen PKI-Symposium 2002 in Karlsruhe präsentieren.

2.2 IT-Grundschutz-Audit

Mit dem IT-Grundschutz-Zertifikat hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Februar 2002 ein amtliches Prüfsiegel geschaffen, mit dem die wirkungsvolle Umsetzung von IT-Grundschutzmaßnahmen in einem Unternehmen bzw. einer Behörde dokumentiert werden kann. Voraussetzung für die Erteilung eines solchen Zertifikats durch das BSI ist die Durchführung eines Grundschutz-Audits nach einem festgelegten Prüfschema durch einen vom BSI lizenzierten Auditor:

http://www.bsi.bund.de/gshb/zert/pruef.pdf (105 kB)

Seit dem 10.07.2002 zählt Claus Stark, Security Consultant bei Secorvo, zu den bisher vierzig vom BSI lizenzierten IT-Grundschutz-Auditoren. Damit kann Secorvo zukünftig Grundschutz-Audits durchführen und, bei Erfüllung der Anforderungen des Prüfschemas, dem BSI die Ausstellung eines IT-Grundschutz-Zertifikats empfehlen.

2.3 Anwendungsintegration statt „One Size Fits All“

Das Image der sicherheitstechnischen „Eier legenden Wollmilchsau“, das Public Key Infrastrukturen lange anhaftete, hat Risse bekommen – und gibt den Blick frei auf den wahren Kern einer PKI: Sie ist eine notwendige Infrastruktur für ausgewählte Mechanismen der IT-Sicherheit. Der Hype ist der ernsthaften Hinwendung zu sinnvollen Anwendungen gewichen.

Diese Entwicklung spiegelt das Programm des diesjährigen PKI-Symposiums 2002 (**08.-09.10.2002**): Mit PKI-Praxisberichten wie den „Lessons Learned“ der UBS AG, der Vorstellung spezieller PKI-basierter Anwendungen wie dem digitalen Fahrtenschreiber und einem Microsoft-Blick in die Zukunft der Webservices wird die Diskussion aktueller Entwicklungen und realistischer Perspektiven von PKIs eröffnet. Workshops und das Begleitprogramm werden auch in diesem Jahr reichlich Gelegenheit zu Erfahrungsaustausch und Diskussion geben:

http://www.pki-symposium.de

Kostenbeitrag: 390 € zzgl. MwSt.
(Aus der Erfahrung der Vorjahre empfehlen wir eine möglichst frühzeitige Anmeldung.)

2.4 „PKI-Woche 2002“

Die 41. Kalenderwoche haben wir in Karlsruhe dem Thema Public Key Infrastrukturen gewidmet: Um Ihren Reiseaufwand zu minimieren, haben wir unser PKI-Seminar, das PKI-Symposium 2002 und ein PKI-Vertiefungsseminar in derselben Woche konzentriert. So können Sie an vier aufeinanderfolgenden Tagen, vom **07.-10.10.2002**, in das Thema PKI eintauchen:

http://www.secorvo.de/college/pki-woche

Teilnehmern des PKI-Symposiums bieten wir die Seminarteilnahme zu einem Sonderpreis an (siehe Anmeldung). Natürlich können die Seminare und das PKI-Symposium auch unabhängig von einander gebucht werden.

3 Veranstaltungshinweise

September 2002	
23.-24.09.	IT Risk Management 2002 (Computas)
24.-25.09.	Einführung in die Praxis des betrieblichen DSB (Euroforum)
Oktober 2002	
02.-04.10.	Information Security Solutions Europe – ISSE 2002 (EEMA)
	„PKI-Woche“
07.-08.10.	Public Key Infrastrukturen (Secorvo College)
08.-09.10.	PKI-Symposium 2002 (Secorvo)
10.10.	PKI für Fortgeschrittene (Secorvo College)
14.-16.10.	7th European Symposium on Research in Computer Security – ESORICS 2002 (ETH/IBM Zürich)
22.-23.10.	Virtual Private Networks im praktischen Einsatz (Secorvo College)
29.-30.10.	SAP-Sicherheit im Betrieb (Secorvo College)

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 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 Feedback an
redaktion-security-news@secorvo.de

Secorvo Security News
September 2002

Dirk Fox
Secorvo Security Consulting GmbH

Nr. 3, 1. Jhrg. 2002
Stand 09. September 2002

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

Inhalt

Editorial: Freiwild WLAN

Wireless LANs verbreiten sich schier unaufhaltsam – eingefrorenen IT-Budgets zum Trotz. Dabei wird die kabellose Freiheit mit Risiken erkauft: Häufig werden WLANs gänzlich ohne Sicherheitsmechanismen betrieben, oft beschränken sich die Betreiber auf einen reinen Passwortschutz, und selten nur wird das Wired Equivalent Privacy (WEP) Protokoll verwendet. Selbst WEP bietet – anders als der Name verspricht – nur ungenügenden Schutz: Im Februar, April und Juli 2001 wurden mehrere kryptoanalytische Angriffe veröffentlicht; kurz darauf waren zahlreiche Angriffsprogramme im Internet verfügbar.

Daher ist seit einer Weile Hacking „by driving around“ in Mode – ein Laptop mit WLAN-Karte und ein Auto genügen auch Laien, um sich in fremden Netzen zu tummeln. Erleichtert wird die Suche nach WLANs in jüngster Zeit durch Kreidezeichen an Hauswänden und auf Trottoirs: Matt Jones, ein Web-Designer aus London, entwickelte im Juni einen Kennzeichnungscode, mit dessen Hilfe „WLAN-Surfer“ gefundene Einwahlpunkte markieren. Die Zeichen wurden kürzlich in Paris, New York und Los Angeles entdeckt – und bald werden vielleicht auch aus deutschen Administratoren Spurenleser:

Die IEEE WG 802.11 arbeitet an einer „Reparatur“ des Standards, dem Temporal Key Integrity Protokoll (TKIP). So lange ist Vorsicht die beste Empfehlung.

Resultate von Borisov, Goldberg, Wagner; Umsetzung des Fluhrer-Mantin-Shamir-Angriffs von Rubin, Joannidis, Stubblefield:

http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

http://www.cs.rice.edu/~astubble/wep

1 Security News

1.1 Neuer SHA-Standard

Am 28.08.2002 gab das amerikanische National Institute of Standards and Technology (NIST) einen neuen Secure Hash Standard (SHS) bekannt, der den SHS (FIPS PUB 180) aus dem Jahr 1993 (aktualisiert im Mai 1995) ab 01.02.2003 ersetzt:

http://csrc.nist.gov/encryption/tkhash.html

FIPS PUB 180-2 umfasst neben SHA-1, dem Secure Hash Algorithmus mit Hashwertlänge 160 bit, drei weitere Algorithmen, die jeweils einen 256 bit (SHA-256), 384 bit (SHA-384) und 512 bit (SHA-512) langen Ausgabewert erzeugen. Die neuen Hashfunktionen ermöglichen ein höheres Sicherheitsniveau für digitale Signaturen: Ab einer Schlüssellänge von 1.500 bit (RSA) bzw. 168 bit (DSS) ist bislang der Hashwert das kryptografisch schwächste Glied.

1.2 PGP auferstanden

Tot Geglaubte leben länger: Seit der unerwarteten Ankündigung von Network Associates (NAI) im Oktober 2001, dass die Produktsparte Pretty Good Privacy (PGP) verkauft werden solle, sowie der Einstellung des Vertriebs am 26.02.2002 galt PGP als „klinisch tot“. Abgesehen von der vom BMWi geförderten Open-Source-Entwicklung GnuPG bot einzig die Anfang 2002 aus der insolventen Biodata AG neu gegründete Glück & Kanja GmbH noch eine kommerziell verfügbare, PGP-kompatible Produktlösung an.

Überraschend kam daher am 19.08.2002 die Nachricht von der Ausgründung der PGP Corporation – mit Venture Capital (14 Mio. US$) und dem „Vater“ Phil Zimmermann an Bord:

http://www.pgp.com

Schon für November 2002 ist eine neue PGP-Version 8.0 für MacOS und Windows XP angekündigt.

1.3 Grundschutzhandbuch des BSI aktualisiert

Seit Mitte August 2002 ist die aktualisierte und erweiterte Version des IT-Grundschutzhandbuchs des BSI (Stand Mai, letzte Änderung 7/2002) online verfügbar:

http://www.bsi.de/gshb/deutsch/menue.htm

In der Neufassung wurde das Methodik-Kapitel (Kapitel 2) überarbeitet. Weiter enthält sie die folgenden zusätzlichen Bausteine:

- Windows 2000 Client und Server
- Internet PC
- Novell eDirectory

Das IT-Grundschutzhandbuch kann beim BSI auf CD-ROM bezogen (frankierter Rückumschlag) oder als Loseblattsammlung beim Bundesanzeiger Verlag bestellt werden (Grundwerk: € 111,50):

http://www.bsi.bund.de/gshb/deutsch/aktuell/bezug.htm

1.4 CrypTool (v1.3.03)

Mit Hilfe des Freeware-Programms CrypTool können kryptografische Verfahren angewendet, demonstriert und analysiert werden. Es ermöglicht damit einen „spielerischen" Einstieg in die klassische und die moderne Kryptografie. CrypTool wurde vor vier Jahren von der Deutschen Bank initiiert und zusammen mit der Secude GmbH, dem FZI Karlsruhe und den Universitäten Darmstadt, Siegen und Karlsruhe zu einem didaktischen Hilfsmittel für die Sensibilisierung der Mitarbeiter für IT-Sicherheit sowie für Ausbildung und Lehre weiterentwickelt. Das Programm wurde für MS-Windows-Betriebssysteme implementiert:

http://www.cryptool.de

Mit der in Kürze verfügbaren Version 1.3.03 gibt die Deutsche Bank die Projektleitung der Weiterentwicklung an die Fraunhofer Gesellschaft ab. Eine Umsetzung in Open Source unter GNU-ähnlichen Lizenzbedingungen ist geplant.

1.5 TKÜV 2002

Seit 24.08.2002 ist die geänderte Fassung der Telekommunikations-Überwachungs-Verordnung (TKÜV) vom 16.08.2002 in Kraft. Sie verpflichtet alle Betreiber von Telekommunikationsanlagen, die Telekommunikationsdienste für die Öffentlichkeit anbieten, zur Aufzeichnung der Kommunikationsdaten und Weiterleitung an die Strafverfolgungsbehörden. Die dafür erforderlichen technischen Einrichtungen müssen die Betreiber auf eigene Kosten einrichten und vorhalten:

http://217.160.60.235/BGBL/bgbl1f/bgbl102s3317.pdf

1.6 Bug in Macromedia Flash

Jetzt hat es auch die beliebten Flash-Programme erwischt: Am 13.08.2002 wurde ein Fehler in Macromedias Shockwave Flash-Plugin bekannt, der einem Angreifer über einen Buffer Overflow die Ausführung beliebigen Codes ermöglicht – und zwar unabhängig von verwendetem Browser und Betriebssystem. Dringende Empfehlung: Download und Installation der korrigierten Flash-Version des Herstellers:

http://www.macromedia.com/shockwave/download/frameset.fhtml?P1_Prod_Version=ShockwaveFlash

2 Secorvo News

2.1 VPN-Interoperabilität

Nicht nur bei Firmenzusammenschlüssen, sondern auch bei heterogenen, gewachsenen IT-Infrastrukturen ist ungenügende Interoperabilität der Produkte unterschiedlicher Hersteller oft Ärgernis und Kostentreiber. Bei IT-Sicherheitslösungen gilt dies besonders für Virtual Private Network (VPN) Gateways: Verschlüsselte Verbindungen zwischen unterschiedlichen Standorten lassen sich am elegantesten über VPN-Tunnel realisieren – und stellen dabei erhöhte Anforderungen an die Interoperabilität der unterschiedlichen Komponenten.

Im Evaluationslabor von Secorvo wurden daher in einer internen Untersuchung acht VPN-Geräte führender Hersteller auf ihre Interoperabilität in einem Standardszenario untersucht. Die (ermutigenden) Ergebnisse wurden in einem Beitrag für die Zeitschrift iX zusammengefasst, der in Ausgabe 10/2002 am 12.09.2002 erscheint.

Hintergründe, Testerfahrungen und Konfigurationsempfehlungen werden außerdem im Rahmen des Seminars von Secorvo College VPNs im praktischen Einsatz vermittelt. Das zweitägige Seminar findet am **22.-23.10.2002** in Karlsruhe statt.

2.2 Bluetooth Security

Der Kommunikationsstandard Bluetooth erfreut sich zunehmender Herstellerunterstützung: Neben Handy-Zubehör werden nun auch Produkte angeboten, die die „letzte Meile“ lokaler Netzwerke kabellos realisieren. Damit wird Bluetooth zur ernsthaften Konkurrenz zu Wireless LAN (WLAN) Lösungen. Der rapide Preisverfall durch den Masseneinsatz von Bluetooth-Chips könnte diese Entwicklung in den kommenden Jahren noch verstärken. Um so größer wird die Bedeutung der Sicherheitsarchitektur von Bluetooth.

Die Darstellung der Sicherheitsmechanismen im Bluetooth-Standard wenig geeignet, einen schnellen Überblick zu vermitteln. Das erschwert eine Bewertung der spezifizierten Verfahren. Das noch „druckfrische“ **Secorvo White Paper** „Bluetooth Security“ von Dirk Fox will Abhilfe schaffen:

http://www.secorvo.de/whitepapers

2.3 „KA-IT-Si“ am 24.10.2002

Ende des Jahres 2000 wurde von Secorvo gemeinsam mit den Karlsruher Versicherungen die „Karlsruher IT-Sicherheitsinitiative“ (kurz: KA-IT-Si) aus der Taufe gehoben. Sie will für das Thema IT-Sicherheit sensibilisieren, Grundwissen vermitteln und

versteht sich als Plattform für den Erfahrungsaustausch von Führungskräften und IT-Sicherheitsverantwortlichen.

Zahlreiche Unternehmen aus der TechnologieRegion Karlsruhe, darunter die Deutsche Bausparkasse Badenia, die L-Bank, SAP und die Sparkassen Informatik, schlossen sich inzwischen der Initiative als Partner an. Der Oberbürgermeister der Stadt Karlsruhe übernahm die Schirmherrschaft, und IHK und der Technologiepark Karlsruhe unterstützen die Aktivitäten.

Gut besucht sind die von der KA-IT-Si angebotenen abendlichen Vortragsveranstaltungen – mit intensiven Kontaktmöglichkeiten und anschließendem Buffet. Die nächste Veranstaltung der KA-IT-Si findet am **24.10.2002 (18 Uhr)** statt. Unter dem Titel „**Wie gut schwimmt Ihr Server?**“ wird Wolfgang Mühlböck von den Karlsruher Versicherungen über die Frage des Transfers von Restrisiken vortragen:

http://www.ka-it-si.de

2.4 Video „Safer Surfen“

Ermutigt durch die große Nachfrage, der sich das Video „Trojanisches Pferd“ erfreut, hat Secorvo ein weiteres Lehrvideo entwickelt. Thema diesmal: „Browsen ohne Reue“ mit Microsofts Internet Explorer.

Das Video besteht aus zwei Teilen: Einer frappierenden Demonstration dessen, was bösartige aktive Komponenten auf einer Webseite (ActiveX, VisualBasic Script etc.) bei einem schlecht konfigurierten Internet Explorer anrichten können, sowie einer Kurzeinführung in die wichtigsten Aspekte einer sicheren Konfiguration des Browsers.

Das auf CD ausgelieferte Video wird ab Mitte Oktober verfügbar sein und kann bis zum 30.09.2002 zu einem Vorzugspreis von 59 €[1] reserviert werden (Preis ab 01.10.2002: 64 €[1]):

http://www.secorvo.de/video

[1] Alle Preisangaben zzgl. MwSt.

3 Veranstaltungshinweise

September 2002	
23.-24.09.	IT Risk Management 2002 (Computas)
Oktober 2002	
02.-04.10.	Information Security Solutions Europe – ISSE 2002 (EEMA)
	„PKI-Woche“ (Secorvo und Secorvo College)
07.-08.10.	Public Key Infrastrukturen (Secorvo College)
08.-09.10.	**PKI-Symposium 2002** (Secorvo)
10.10.	PKI für Fortgeschrittene (Secorvo College)
22.-23.10.	Virtual Private Networks im praktischen Einsatz (Secorvo College)
24.10.	„Wie gut schwimmt Ihr Server?“ (KA-IT-Si, Karlsruhe)
28.-29.10.	IT-Sicherheit für kleine und mittelständische Unternehmen (VDI/IHK Köln)
29.-30.10.	SAP-Sicherheit im Betrieb (Secorvo College)

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 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

Secorvo Security News
Oktober 2002

Dirk Fox
Secorvo Security Consulting GmbH

Nr. 4, 1. Jhrg. 2002
Stand 13. Oktober 2002

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

Inhalt

Editorial: Was die 40 Räuber dem Präsidenten voraus hatten

Die Diskussion über Mindestanforderungen an Passworte ist mindestens so alt wie die 270ste Geschichte der 1001 märchenhaften Nächte des Kalifen von Bagdad aus dem 9. Jahrhundert. Darin knackt Ali Baba den Zugang zur Räuberhöhle durch Abhören des Passworts „Sesam, öffne dich!“. Immerhin ein Passwort mit 18 Zeichen, darunter zwei Sonderzeichen – zumindest in der deutschen Übersetzung.

Damit waren die Räuber weit fortschrittlicher als 1.100 Jahre später Bill Clinton, der als Präsident der Vereinigten Staaten Ende Juni 2000 das Bundesgesetz zur digitalen Signatur elektronisch unterzeichnete – und dabei den Namen seines Hundes Buddy als Passwort wählte. Offenbar hatte ihn niemand darauf hingewiesen, dass nicht nur ein Passwort mit lediglich fünf Stellen ohne Sonderzeichen viel zu leicht erratbar ist, sondern dass Namen von Familienangehörigen auch keinen Schutz vor Social Engineering bieten und daher grundsätzlich tabu sein sollten. Mit dem Ausplaudern des verwendeten Passworts vor laufenden Kameras outete er sich gänzlich als Negativbeispiel – Ali Baba musste sich immerhin in einem Baum verstecken, um das Passwort belauschen zu können.

Trotz der gestiegenen Sensibilität in Fragen der IT-Sicherheit sind Passworte bis heute nicht nur zentrales, sondern häufig auch wohlfeiles Objekt der Begierde. Dabei gibt es zahlreiche öffentlich verfügbare Empfehlungen zur Wahl guter Passworte, wie z. B. – pars pro toto – die des Datenschutzbeauftragten des Kantons Zürich:

http://www.cnlab.ch/pwcheck/empfehlungen.html

Einen Vorzug zumindest haben moderne Passwortsysteme gegenüber dem Schutzmechanismus der Räuberhöhle: Ein Passwort kann (und sollte regelmäßig) geändert werden – damit lässt sich der mögliche Schaden immerhin begrenzen.

1 Security News

1.1 Cyber Security – strategisch

Die amerikanische Regierung hat am 17.09.2002 den Entwurf eines Strategie-Papiers zur Verbesserung der Sicherheit des Internet („National Strategy To Secure Cyberspace“) veröffentlicht:

http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf (2,4 MB)

Die Veröffentlichung erfolgte nicht ganz freiwillig: Durch eine Indiskretion war eine Vorversion des Konzepts an die Öffentlichkeit geraten – und hatte einen Aufschrei der Internet-Zugangs-Provider ausgelöst: Sie sollten zur kostenlosen Verteilung von Schutzsoftware an private Kunden verpflichtet werden. Aus der nun für zwei Monate zur öffentlichen Kommentierung freigegebenen Fassung wurden alle „Kanten“ herausgefeilt. Sie hat daher eher den Charakter einer Empfehlungssammlung denn den eines wirksamen Maßnahmenpapiers.

1.2 Zeit der Security Surveys

In unübersichtlichen Zeiten schlägt die Stunde der Studien. Zahlreiche Security Surveys bieten derzeit Einschätzungen der Bedrohungslage, des Verbreitungsgrads von Sicherheitslösungen und Abschätzungen der Budgets für IT-Sicherheit.

Die Repräsentativität der einzelnen Erhebungen ist allerdings sehr unterschiedlich. Und auch die Ergebnisse klaffen zum Teil stark auseinander. Die konkreten Zahlen erscheinen daher wenig verlässlich. Aussagekraft haben eher Studien übergreifende Trends. Davon sind einige wenig überraschend, wie z. B. die nach wie vor hohe Bedeutung der Bedrohung durch Viren.

Eine Entwicklung ist jedoch bemerkenswert: Der Anteil externer Attacken hat erheblich zugenommen – und übertrifft in einigen Befragungen erstmals den der Insiderangriffe. Offen bleibt, ob dies tatsächlich auf eine geänderte Bedrohungslage hinweist – oder eher Resultat einer verbesserten Protokollierung ist.

Hier eine Auswahl aktueller Studien:

Global Information Security Survey (März 2002), Ernst & Young, 459 Teilnehmer (weltweit):
http://www.ey.com.pl/gcrdownload/GISS_2002.pdf (2 MB)

KES/KPMG-Studie (Frühjahr 2002), 260 Teilnehmer (D):
http://www.kes.info/studie2002/ (mehrteilig)

CSI/FBI Computer Crime and Security Survey (April 2002); 503 Teilnehmer (US):
http://www.gocsi.com/pdfs/fbi/FBI2002.pdf (2,2 MB)

Information Security Breaches Survey 2002 (April 2002) von PWC und dem britischen dti; 1000 Teilnehmer (UK):
https://www.security-survey.gov.uk/isbs2002_detailedreport.pdf (1 MB)

Australian Computer Crime and Security Survey (Mai 2002) von AusCert und Deloitte Touche Tohmatsu; 95 Teilnehmer:
http://www.auscert.org.au/Information/Auscert_info/2002cs.pdf (347 kB)

Umfrage „IT-Sicherheit 2002“ (Juni 2002) von silicon.de; 483 Teilnehmer (D):
http://www.sicherheit-im-internet.de/download/IT-Sicherheit.pdf (428 kB)

BSA Cyber Security Survey (Juli 2002), BSA, 395 Teilnehmer (US):
http://www.bsa.org/security/resources/2002-07-22.131.pdf (315 kB)

Information Security Magazine Survey (September 2002), 215 Teilnehmer (US):
http://www.infosecuritymag.com/2002/sep/2002survey.pdf (267 kB)

IT-Security Studie (September 2002) von InformationWeek, 8.188 Teilnehmer weltweit (828 aus D):
http://www.informationweek.de/studien/stud_it_security2002.ppt (8,5 MB)

1.3 CERT-Verbund

Mit der Gründung eines CERT Verbunds durch sechs deutsche Computer Emergency Response Teams – CERT-Bund (BSI), DFN-CERT, S-CERT (Sparkassenorganisation), Siemens-CERT, BCRS (IBM) und Telekom-CERT – gibt es seit dem 01.09.2002 ein Koordinationsgremium für übergreifende CERT-Aktivitäten in Deutschland. Durch eine Intensivierung der Zusammenarbeit sollen u. a. die Reaktionszeiten bei sicherheitsrelevanten Ereignissen verkürzt werden:

http://www.bmi.bund.de/dokumente/Pressemitteilung/ix_90395.htm

1.4 RC5-64 Contest gelöst

Am 28.01.1997 startete RSA Security Inc. einen groß angelegten „Crypto Contest“: 13 „Krypto-Rätsel“, mit unterschiedlich langen (40 bis 128 bit) Schlüsseln verschlüsselte Texte (einmal DES, zwölf mal RC5), wurden zur Kryptoanalyse freigegeben:

http://www.rsasecurity.com/rsalabs/challenges/secretkey/secret-key.html

Die ersten vier Rätsel (RC5-40/-48/-56 und DES-56) wurden noch im Jahr 1997 gelöst. Seitdem war es ruhig um den Contest geworden – bis nun die mit einem Preis von 10.000 US$ dotierte RC5-64-Verschlüsselung gebrochen wurde: von 331.252 über das Internet verbundenen Rechnern, die in vier Jahren 15.769.938.165.961.326.592 verschiedene Schlüssel – 47% des Schlüsselraums – systematisch ausprobiert hatten („Brute Force“):

http://www.distributed.net/rc5

Zuletzt erreichten die vernetzten Rechner einen Durchsatz von über 127 Milliarden Schlüsseln pro Sekunde. Die richtige Lösung wurde schon am 14.07.2002 entdeckt; durch einen Softwarefehler wurde die Entschlüsselung – und damit der Beleg für die faktische Unsicherheit von 64 bit langen symmetrischen Schlüsseln – aber erst am 27.09. 2002 bekannt.

1.5 Würmerplage

Zwei Würmer mit dramatischen Auswirkungen halten derzeit Administratoren in Atem:

Der Wurm „Slapper“ bzw. „bugtraq.c“ nutzt einen bekannten Fehler im SSLv2-Handshake des OpenSSL-Moduls (siehe Secorvo Security News 2/2002), um auf einem Linux-Server einen Buffer Overflow zu erzeugen. Dann kopiert er das Programm „bugtraq.c“ auf den kompromittierten Server und übersetzt es mit gcc. Dieses schaltet einen Port zur Nutzung des Servers für verteilte DoS-Angriffe frei und sucht dann nach weiteren Linux-Servern. Betroffen sind Linux-Systeme mit Apache und mod_ssl. Schutz bietet die Installation der OpenSSL-Versionen ab 0.9.6e:

http://www.openssl.org

Derweil leidet die Windows-Welt unter dem Wurm „Bugbear“, der sich über E-Mail-Anhänge mit zufälligem Dateinamen und wechselndem Betreff sowie Netzlaufwerke verteilt. Er nutzt eine Schwachstelle im IE 5.01 und 5.5, durch die Attachments von HTML-E-Mails beim Öffnen ausgeführt werden. Anschließend versucht er, installierte Virenscanner und Sicherheitsprogramme zu deaktivieren. Er öffnet eine Hintertür auf Port 36794, über die ein entferntes System beliebige Kommandos und Programme ausführen kann, protokolliert alle Tastatureingaben und versendet sie per E-Mail an ein externes System:

http://cert.uni-stuttgart.de/ticker/article.php?mid=974

2 Secorvo News

2.1 Secorvo College aktuell

„Security Awareness“ wird zunehmend zum zentralen Thema in Unternehmen und Behörden. Mit dem Seminar „Defense Lab“ bietet Secorvo College am 03.-04.12.2002 in Zusammenarbeit mit der Schweizer Firma Compass Security Network Computing erstmals ein „Online-Hacking“-Seminar, in

dem die Vorgehensweise von Angreifern erläutert und zahlreiche typische Angriffe life vorgeführt werden:

http://www.secorvo.de/college

2.2 Browser-Konfiguration

Dass von aktiven Komponenten auf Webseiten erhebliche Bedrohungen ausgehen können, ist keine Neuigkeit. Viele Unternehmen haben inzwischen zentrale Filtersysteme eingerichtet, die das Eindringen bösartigen Codes über Webseiten verhindern. Aber nicht jeder PC nimmt hinter einer gut konfigurierten Firewall Deckung: Mobile Systeme mit Internet-Zugang, die sich nicht nur bei Außendienstmitarbeitern großer Beliebtheit erfreuen, sind oft unzureichend geschützt. Denn hier hängt alles an der Konfiguration des Browsers (oder der „Personal Firewall“).

Eine anschauliche Darstellung von Bedrohungen durch aktive Komponenten und Konfigurationshinweise für Microsofts Internet Explorer bietet das von Secorvo in Zusammenarbeit mit Microsoft Deutschland entwickelte Video „Safer Surfen“, das Mitte Oktober fertiggestellt wird. Vorbestellung:

http://www.secorvo.de/video

Für Surfer, die sich ihrer Sache nicht sicher sind, hat der Datenschutzbeauftragte des Kantons Zürich zusammen mit der Hochschule für Technik in Rapperswil (CH) einen Online-Sicherheitscheck für Browser entwickelt, den seit Ende März 2001 schon mehr als 400.000 Besucher genutzt haben:

http://152.96.120.35/

Nach Abschluss des vierstufigen Tests gelangen Sie zur statistischen Auswertung, die Erschreckendes offenbart: 69-85% aller getesteten Systeme haben Scriptsprachen (VBScript, JScript, JavaScript) freigeschaltet, und 25,5% erlauben die Ausführung von signierten ActiveX-Komponenten. Obwohl die Test-Teilnehmer sicher für Datensicherheit sensibilisiert waren: ca. 3.600 Systeme (1,5%) waren für ActiveX ein offenes Scheunentor, und auf etwa 4.800 Rechnern (1,6%) waren freigegebene Laufwerke sichtbar.

3 Veranstaltungshinweise

Oktober 2002	
24.10.	„Wie gut schwimmt Ihr Server?“ (KA-IT-Si, Karlsruhe)
28.-29.10.	IT-Sicherheit für KMU (VDI/IHK Köln)
November 2002	
05.-07.11.	IT-Sicherheit heute (Secorvo College)
07.-08.11.	Praxis des betrieblichen DSB (Euroforum, Berlin)
12.-13.11.	Inside Windows Security (Secorvo College)
19.-20.11.	Lotus Notes Security (Secorvo College)
20.-22.11.	IT-Security- und Riskmanagement (ZfU, Zürich)
26.-27.11.	Sichere E-Mail-Kommunikation (Secorvo College)
Dezember 2002	
02.-03.12.	IsSec 2002 (Computas, Berlin)
03.-04.12.	Defense Lab (Live Hacking) (Secorvo College)

Aktuelle Veranstaltungsübersicht:
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 automatische Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail an security-news@secorvo.de (Subject: „Subscribe Security News“) anfordern.

Secorvo Security News
November/Dezember 2002

Dirk Fox
Secorvo Security Consulting GmbH

Nr. 5, 1. Jhrg. 2002
Stand 29. November 2002

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

Inhalt

Editorial: Das Dorf, die Sau und die Kryptologie

Nachdem die Veröffentlichung einer neuen, vermeintlich wesentlich effizienteren Methode zur Kryptoanalyse von RSA-Schlüsseln durch Daniel Bernstein im vergangenen Jahr große Verunsicherung ausgelöst hatte, wird derzeit eine neue „Krypto-Sau“ durch‘s Dorf gejagt. Diesmal hat es die symmetrischen Verfahren erwischt.

Schon 2001 war es Ferguson, Schroeppel und Whiting gelungen, den AES als überraschend einfache geschlossene Formel auszudrücken. Dies ist eine beunruhigende Erkenntnis, wenn daraus auch nicht unmittelbar ein Angriff abgeleitet werden konnte. Auf der diesjährigen Welt-Kryptologie-Konferenz „Crypto“ versetzte jedoch ein neuartiger Angriff auf den AES, die „eXtended Sparse Linearization“ (XSL), die Kryptologen-Elite in Aufregung. Als elektronische Vorab-Veröffentlichung kursierte eine diesbezügliche Arbeit von Courtois und Pieprzyk, die die Autoren auf der Konferenz „AsiaCrypt 2002“ Anfang Dezember präsentieren werden.

http://eprint.iacr.org/2002/044

Nachdenklich stimmt weniger der Angriff selbst: Er ist bislang „nur“ ein theoretisches Konzept, und der tatsächliche Aufwand ist mit 2^{200} Operationen so groß, dass er sich zumindest zu Lebzeiten der Autoren nicht testen lassen wird. Der AES könnte gut damit leben – ein Sicherheitsniveau von 2^{200} liegt jenseits des heute Angreifbaren, und das gilt nach Kryptografenschätzungen sicher noch bis weit in das 22. Jahrhundert. Der Ansatz des Angriffs ist jedoch bedenklicher, denn er wirkt auch beim AES-Kandidaten „Serpent“, den alle Experten für den sichersten Algorihmus im Auswahlverfahren hielten.

Wieder ein Beleg, dass die Kryptografie immer für Überraschungen gut ist. Und dass sich die Krypto-Forschung daher nicht auf ihren Erfolgen ausruhen darf. Und – dass auch bei den besten Kryptologen Irren eine menschliche Eigenschaft ist.

1 Security News

1.1 Big Brother Awards

Die 1990 gegründete internationale Menschenrechtsgruppe „Privacy International“ (PI) initiierte im Jahr 1988 die „Big Brother Awards“ als „Oskar für Datenkraken“. Inzwischen wird diese Auszeichnung für besondere Leistungen beim Missbrauch personenbezogener Daten jährlich in 12 Ländern vergeben.

http://www.privacyinternational.org/bigbrother/

In Deutschland organisiert der Bielefelder „Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs“ (FoeBuD e.V.) seit dem Jahr 2000 die Auswahl der Preisträger und die Preisverleihung. Die diesjährigen deutschen Awards wurden am 25.10.2002 in acht Kategorien verliehen. Die Preisträger finden sich unter

http://www.bigbrotherawards.de/

1.2 TCPA

Ziel der im Frühjahr 1999 von Intel initiierten Trusted Computing Platform Alliance (TCPA) ist die Schaffung einer Betriebssystemumgebung, in der durch einheitliche Mechanismen Integrität und Identität überprüfbar sichergestellt werden. Zu den Gründungsmitgliedern gehören IBM, HP, Compaq und Microsoft. Inzwischen haben sich der Initiative mehr als 160 Unternehmen angeschlossen.

http://www.trustedcomputing.org

Die aktuelle Version 1.1b der „Main Specification“ vom 22.02.2002 (frei gegeben im Mai 2002) findet sich unter:

http://www.trustedcomputing.org/docs/main%20v1_1b.pdf (pdf, 1,7 MB)

Durch eine in mehreren Sprachen verfügbare „FAQ“-Liste von Ross Anderson kommt jetzt allerdings Wirbel in das Thema: Er vermutet hinter der Initiative den Versuch, mit in Hardware realisierten kryptografischen Mechanismen zum Digital Rights Management (DRM) die Nutzung manipulierter oder nicht lizenzierter Software und unerwünschter Daten (z.B. MP3-Files) zu kontrollieren sowie Nutzer-Informationen zentral zu registrieren – eine Breitseite auf den Datenschutz mit Zensurpotential.

http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html

1.3 Windows 2000 zertifiziert

Im Oktober 2002 hat Microsoft für Windows 2000 die Sicherheitszertifizierung nach den Common Criteria bezüglich des Controlled Access Protection Profile und für Evaluation Assurance Level EAL-4 bestanden.

Hinweise für die erforderliche Konfiguration für einen mit dieser Zertifizierung konformen Betrieb von Windows 2000 gibt:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/w2kccwp.asp

1.4 „Backdoor“ im EFS

Unter Windows 2000 enthält das Encrypted File System (EFS) eine hässliche ungeplante Hintertür, wie die Fachzeitschrift c’t (23/2002, S. 33) berichtet: Bootet man beispielsweise einen mit EFS gesicherten Laptop mit der Startdiskette, kann man hinter dem Rücken des Rechnerinhabers das Zugriffspasswort ändern. Anschließend kann auf EFS-verschlüsselte Dateien frei zugegriffen werden.

Microsoft empfiehlt, diese Aushebelung der integrierten Dateiverschlüsselung in Windows 2000 durch die Verwendung eines höheren Syskey-Modus (2 oder 3) zu verhindern: Dann ist ein zusätzliches Passwort bzw. sogar eine Schlüsseldiskette beim Systemstart erforderlich.

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/efs.asp

1.5 Sammelpatch IE 5.x-6.0

Microsoft hat mit dem Siegeszug des Internet Explorers die Browser-Schlacht für sich entschieden: In den meisten Unternehmen genießt der IE heute den Status des Standard-Browsers. Der große Funktionsumfang des IE gibt aus Sicht der IT-Sicherheit allerdings wenig Anlass zur Freude: ActiveX, JScript, VBScript und ActiveScripting eröffnen auch Angreifern großartige Möglichkeiten. Immer wieder werden zudem sicherheitsrelevante Programmierfehler entdeckt und „Exploits" – Programme, die die Nutzung dieser Schwächen exemplarisch vorführen – im Internet veröffentlicht.

Zuletzt gab Microsoft am 20.11.2002 einen aktuellen Sammelpatch für den Internet Explorer heraus, der zahlreiche, z.T. schwere Fehler der Versionen 5.x-6.0 (SP 1) korrigiert:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-066.asp

Software-Updates „hinken" den Entdeckungen findiger Programmierer zwangsläufig hinterher. Dass einige Fehler allerdings auch von dem aktuellen Patch nicht behoben sind, zeigt die von Thor Larholm gepflegte „unpatched"-Liste ungelöster Fehlerreports zum Internet Explorer:

http://www.pivx.com/larholm/unpatched

Eine Online-Prüfung auf von Angreifern nutzbare Konfigurations- und Programmierfehler für den Internet-Explorer findet sich auf den Webseiten der Zeitschrift c't:

http://www.heise.de/ct/browsercheck/e5demo.shtml

Sensibilisierung für die sichere Nutzung des Internet Explorers und Hinweise zur geeigneten Konfiguration bietet auch das von Secorvo erstellte Video „Safer Surfen mit dem Internet Explorer", das seit kurzem verfügbar ist:

http://www.secorvo.de/video

1.6 Mcert gegründet

Am 15.10.2002 wurde vom Präsidium des Branchenverbands Bitkom der Aufbau eines Computer-Notfall-Teams (CERT) beschlossen. Die Finanzierung dieses „Mittelstand-CERTs" übernehmen in den ersten drei Jahren BMWi, BMI, Bitkom sowie sieben Unterstützer aus der Industrie. Mit speziell aufbereiteten Warn- und Schwachstellenmeldungen sowie einer koordinierten Behandlung von Sicherheitsvorfällen und -problemen soll speziell der Mittelstand beim Thema IT-Sicherheit unterstützt werden.

Diese Entscheidung basiert unter anderem auf einer im Auftrag des BMWi erstellten Studie zu „CERT-Dienstleistungen für kleine und Mittlere Unternehmen (KMU)" vom 08.07.2001 (pdf, 479 kB):

http://www.bitkom.org/gbgateinvoker.cfm/Studie_CERT_KMU.pdf?gbAction=gbFileDownload&ObjectID=F93098A0-2DB0-4818-8334CEA5E3FFFB61&DownloadObject=documents&index=1&cacheLevel=0

Die konstituierende Sitzung zum offiziellen Projektstart und der Gründung einer Mcert-Betreiber-GmbH sowie der Berufung eines Mcert-Beirats ist am 03.12.2002 in Berlin geplant.

2 Secorvo News

2.1 Secorvo College aktuell

Alles wird teurer – jedenfalls fast alles. Ein kleines Unternehmen aus Karlsruhe schwimmt gegen den Strom: Wir senken die Teilnahmegebühren für Seminare von Secorvo College durchgängig um ca. 7 %. Denn es ist uns gelungen, Kosten für Druck und Versand unserer Prospekte durch verschiedene Maßnahmen deutlich zu senken. Diese Einsparungen geben wir an Sie weiter: Sie erhalten „schlankere" Post von uns – und sparen bei den Seminargebühren bis zu 140 €.

http://www.secorvo.de/college

2.2 Förderpreis Baden-Württemberg für Secorvo

Am 13.11.2002 wurde Secorvo von Ministerpräsident Erwin Teufel als zweiter Sieger des „Förderpreises des Landes Baden-Württemberg für junge Unternehmen 2002“ für vorbildliche unternehmerische Leistungen ausgezeichnet. Um diesen renommierten Preis hatten sich mehr als 630 Unternehmen aus Baden-Württemberg beworben.

http://www.secorvo.de/presse/pm21-foerderpreis-bw-2002.html

2.3 In neuem Gewand

Seit Ende November hat Secorvo ein neues „Outfit“: Unserem Internetauftritt haben wir eine gründliche Überarbeitung angedeihen lassen. Nicht nur Farbe, Form und Design sind frisch, sondern auch Struktur und Navigation der Seiten wurden neu gestaltet – wir hoffen, zu Ihrem Gefallen und Nutzen. Aber urteilen Sie selbst – wir freuen uns über Ihre Kommentare:

http://www.secorvo.de

2.4 IT-Grundschutz-Auditor

Mitte November 2002 erhielt Stefan Gora, Consultant bei Secorvo, vom Bundesamt für Sicherheit in der Informationstechnik (BSI) seine Lizenz als IT-Grundschutz-Auditor. Herr Gora ist damit berechtigt, IT-Grundschutz-Audits für die Erlangung von IT-Grundschutz-Zertifikaten des BSI durchzuführen sowie IT-Grundschutz-Selbsterklärungen durch ein Testat zu bestätigen.

http://www.secorvo.de/leistungen/grundschutz-audit.html

3 Veranstaltungshinweise

Dezember 2002	
01.-05.12.	AsiaCrypt 2002 (IACR, Otago/NZ)
02.-03.12.	IsSec 2002 (Computas, Berlin)
03.-04.12.	Defense Lab (Live Hacking) (Secorvo College, Karlsruhe)
04.-05.12.	TrustD@y – IT-Sicherheit ist Chefsache (TimeContor, Berlin)
09.-13.12.	ACSAC 2002 (ACSA, Las Vegas)
13.12.	Trust in Electronic Signatures (ETSI, London)
Januar 2003	
15.-17.01.	Omnicard 2003 (inTIME, Berlin)
22.-23.01.	Einführung in die Praxis des betrieblichen DSB (Euroforum)
22.-24.01.	IT-Defense (Cirosec, Leverkusen)
28.-29.01.	PKI – Public Key Infrastrukturen (Secorvo College, Karlsruhe)
30.01.	PKI für Fortgeschrittene (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 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