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