Secorvo Security News
November 2005

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

Nr. 11, 4. Jhrg. 2005
Stand 30. November 2005

ISSN 1613-4311

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

Inhalt

Editorial: Getrübter Blick

Stellen wir uns vor, wir seien Politiker. Einflussreich, gerne gesehener Gast im Fernsehen und bei öffentlichen Veranstaltungen. Jovial, eloquent, erfolgreich. Und täglich Seite an Seite mit unserem Bodyguard unterwegs. Gepanzerter Dienstwagen, Fahrer mit wachsamem Auge und Fluchttraining. Schusssicheres Glas in Büro und Wohnzimmer, Personenkontrollen für jeden, der sich auf Wurfweite nähert, überwachter Schulweg für unsere Kinder. Aus einer solchen Perspektive nimmt sich Freiheit anders aus. Ertrüge man diese Randbedingungen über Jahre, erscheint es unvorstellbar, dass sie unser Urteil unbeeinflusst ließen – vor allem bei Fragen der inneren Sicherheit.

Das war schon so in den Hochzeiten des Terrorismus in Deutschland. Obwohl sich die Zahl der Opfer der menschenverachtenden Ideologie der RAF zum Glück zahlenmäßig in Grenzen hielt, wurde ihr eine polizeiliche Aufmerksamkeit zu Teil, die kein anderer Mörder je fürchten müsste – dabei war die Identität der Täter bekannt. Die Folgen des Perspektivwechsels ließen sich bei niemandem so ausgeprägt beobachten wie bei Bundesinnenminister Schily, der als ehemaliger RAF-Anwalt nach den Attentaten des 11.09.2001 die Befugnisse der Strafverfolgung fast geräuschlos ausweitete wie kein Minister zuvor.

Kaum hat die Große Koalition mit der Opposition im Bundesrat die letzte Bastion des Widerstandes geschliffen, wachsen die Begehrlichkeiten weiter: Die Vorratsdatenspeicherung von Telekommunikationsdaten und die Umwandlung des LKW-Maut-Systems in ein PKW-Verfolgungs-System stehen jetzt auf der Tagesordnung. Dabei bleiben die Strafverfolgungsbehörden bis heute den Nachweis schuldig, dass Großer Lauschangriff, Telefonüberwachung oder Rasterfahndung auch nur einen einzigen Täter überführt oder wenigstens abgeschreckt hätten. Aus der Perspektive des Kaninchens, das auf den Fuchs starrt, ist der mit wachsender Überwachung einher gehende Verlust an Lebensqualität jedoch offenbar kein gewichtiges Argument.

1 Security News

1.1 Codebreaker im Plan

Am 02.11.2005 konnte die auf dem Gebiet der angewandten Faktorisierung führende Arbeitsgruppe der Universität Bonn die beiden Primfaktoren der Zahl RSA-640 benennen und den von RSA Security Inc. ausgelobten Preis von $ 20.000 einstreichen.

Kein Grund zur Panik für Anwender des RSA-Verfahrens – es liegt alles im Plan: Weder ist dies ein neuer Weltrekord (bereits am 09.05.2005 hatte die selbe Gruppe die 663-Bit-Zahl RSA-200 gebrochen, siehe SSN 05/05), noch wurde ein radikal neuer Algorithmus angewandt. Das Resultat bestätigt lediglich die in den Jahren 2001 (Lenstra) und 2002 (Secorvo) aufgestellten Prognosen über den Fortschritt der Faktorisierung unter Berücksichtigung der Entwicklung der Rechenleistung.

Vielleicht gelingt der nächste große Durchbruch ja den Nachwuchs-Codebreakern, die die NSA derzeit mit ihrer CryptoKids™ Kampagne sucht.

1.2 BlackBerry Symposium

Die Diskussion um die bislang unveröffentlichte BSI-Studie vom 20.09.2005, die dem Push-Mail-System „BlackBerry“ der Firma RIM die Eignung für sicherheitskritische Bereiche abspricht, dauert an. Zum Glück hat sie wieder die Sachebene erreicht.

Zwei Veranstaltungen sind in den kommenden Tagen dieser Fragestellung gewidmet: Das von Secorvo veranstaltete „BlackBerry Security Symposium“ am 30.11.2005 in Karlsruhe und das Simedia-Tagesseminar „Sicherheit von E-Mail-Push-Diensten“ am 08.12.2005 in Bonn. Wer am 30.11.2005 verhindert ist, kann die Teilnehmerunterlagen auf CD online ordern.[1]

[1] Security Finder-Abonnenten finden Materialien zum Thema unter *Mobile Security*. Eine Darstellung des BlackBerry-Sicherheitskonzepts erschien in der DuD 11/05.

1.3 High-speed spoofing

Dass IP- sowie MAC-Adressen leicht gefälscht werden können, ist seit langem bekannt. Inzwischen existieren zahlreiche frei verfügbare Tools, mit denen ein Angreifer – ohne eigenes Know-how zu besitzen – derartige Spoofing-Angriffe durchführen kann. Dennoch wird vor allem die Kombination aus IP- und MAC-Adresse noch immer in vielen Netzbereichen zur Authentisierung verwendet.

Am 03.11.2005 nun veröffentlichte Paweł Pokrywka ein im Rahmen seines Master of Science-Studiengangs erstelltes Angriffsprogramm namens multispoof. Dieses Tool unterscheidet sich in zwei wesentlichen Punkten von bisher verfügbaren Spoofing-Programmen: zum einen kann es mehrere IP-/MAC-Adresskombinationen gleichzeitig fälschen (was den Datendurchsatz deutlich erhöhen kann), zum anderen fälscht multispoof nur inaktive Adressen, so dass es nicht zu Konflikten mit legitimen Benutzern kommt – was das Entdecken solcher Angriffe erheblich erschwert.

Will man diese Funktionalität nutzen, wird multispoof zunächst in einer Art „Lernmodus“ betrieben: Das Tool protokolliert dazu über einen bestimmten Zeitraum alle gültigen Adressen eines Netzes in einer eigenen Datenbank; anschließend nutzt es diese Informationen, um inaktive Adressen zu missbrauchen.

Wer noch immer auf IP- und MAC-Adressen als Authentisierungsmechanismus vertraut, den wird ein Probelauf von multispoof eines Besseren belehren...

1.4 Literaturpreis für Sober

Seit dem 19.11.2005 grassiert eine neue Variante des altbekannten E-Mail-Wurms Sober, die mancherorts sogar das Aufkommen an Spam-Mails in den Schatten stellt. Die hohe Verbreitung verursacht nicht etwa eine neue Verbreitungstechnik – sie ist einzig auf die bessere „literarische Qualität“ der Social-Egineering Komponente, vulgo E-Mail-Betreff und -Text, zurück zu führen: Unzählige Empfänger starten das komprimierte anhängende Schadprogramm.

Bleibt nur zu hoffen, dass die Versender von Phishing-Mails und Anwerbeversuchen für Geldwäscher noch eine Weile brauchen, bis sie mit ihren bislang meist sehr holprigen Texten diese Verführungsqualität erreichen.

1.5 Standards-Workshop

Für den 05.12.2005 lädt der ISO/IEC SC27 „Security Techniques" des DIN zu einem eintägigen internationalen Workshop nach Berlin. Das Programm der Veranstaltung ist viel versprechend; eine Anmeldung zu dieser unentgeltlichen Veranstaltung ist auch online möglich.

1.6 (w)Or(m)acle

Der Ablauf war schulbuchartig: Erst sprach man darüber (2002), dann wurde fachlich präzisiert (Q3/2005) – die praktische Umsetzung stellte sich dann von selbst ein. Am 31.10.2005 wurde der „Voyager Beta Worm" für Oracle anonym auf der Mailingliste Full-Disclosure veröffentlicht. Am 05. 11.2005 folgte eine Warnung von Oracle an alle Kunden.

Käme nun noch eine erfolgreiche Freisetzung des „Proof of Concept", müsste sich der Hersteller Oracle mit seinen 22 Sicherheitszertifizierungen wohl zu den Themen Compliance, SOX, Haftungs- und Schadensersatzansprüche neu positionieren. Die Checkliste anlässlich des aktuellen Vorfalls könnte sich dafür als unzureichend erweisen.

1.7 Dunkle Seite der Macht

Das durch das vielfältige Medienecho seit der ersten Meldung am 31.10.2005 zur Affäre gewordene Kopierschutz-„Rootkit" auf CDs von Sony BMG hat eine Welle der Empörung ausgelöst. Es lehrt zweierlei:

- Erstens sollte insbesondere derjenige, der bestrebt ist, sein eigenes geistiges Eigentum zu schützen, dasjenige von anderen peinlich genau beachten.

Denn sollte die eingesetzte Kopierschutz-Software tatsächlich die Open-Source Lizenzen GPL und LGPL verletzen, dann muss dies Konsequenzen für den Lieferanten der Software haben.

- Zweitens ist die Grenze zwischen unerwünschter Malicious Software und nützlichen System-Tools mindestens so durchlässig wie die zwischen den beiden Seiten der StarWars Macht.

Denn die Eigenschaften „gut" und „böse" lassen sich nicht aus technischer Funktionalität ableiten, sondern einzig aus der jeweiligen Nutzung. Und die ist oft nicht eindeutig, wie die Wandlung von NetBus vom Saulus (Trojaner) zum Paulus (Administrations-Tool) eindrucksvoll demonstriert.

Auch für Sony BMGs Kopierschutz, der in der öffentlichen Wahrnehmung ein Schritt auf die „dunkle Seite" war, haben findige Online-Spieler schon eine neue Anwendung ausgemacht: Sie verstecken damit ihre kleinen „Schummel"-Programme.

1.8 Neue Top 20-Liste

Zum fünften Mal veröffentlichte SANS am 20.11.2005 seine Liste der 20 kritischsten IT-Sicherheitslücken. Teilten sich diese bis 2004 nur zwei Klassen, nämlich Windows und Unix, wurde die Liste 2005 deutlich erweitert: Neben den Betriebssystemen Windows und Unix werden Sicherheitslücken in systemübergreifenden Programmen (wie Backup, DNS, PHP und Datenbanken) und in Netzkomponenten (wie Cisco) unterschieden.

Auch hat sich das Gewicht verschoben: Nur noch sieben der 20 Sicherheitslücken betreffen Microsoft (5) oder Unix (2). Die Liste ist auch nicht mehr „kumulativ", d.h. Sicherheitslücken, die 2005 in der Top 20-Liste vermerkt waren, werden 2006 nicht mehr aufgenommen.

Die in der – als Hilfestellung für Unternehmen gedachten – Aufstellung gelisteten Top-Sicherheitsmängel sollten schnellstmöglich durch das Einspielen der entsprechenden Patches beseitigt werden.

2 Secorvo News

2.1 Secorvo College aktuell

Das Seminarangebot von Secorvo College wartet im Jahr 2006 mit zahlreichen neuen Themen auf, darunter die sichere Gestaltung von IT-Outsourcing, die Praxis von IT-Sicherheitsaudits und das kürzlich erstmalig durchgeführte Seminar Kommunikationsschutz und Datensicherheit, das eine besonders gute Seminarbewertung erhielt.

Auf vielfachen Wunsch hat endlich auch der E-Commerce bei College Einzug gehalten: Mit dem Programm 2006 ist nun auch eine Online-Seminaranmeldung möglich – natürlich SSL-gesichert.

Weitere Seminarthemen und Termine von Secorvo College finden Sie unter http://www.secorvo.de/college

2.2 White Paper: BlackBerry

Die Sicherheit des BlackBerry-Push-Mail-Systems ist seit Bekanntwerden der internen BSI-Studie Gegenstand zahlreicher Diskussionen. Das am 23.11.2005 publizierte 12. Secorvo White Paper „BlackBerry Security“ stellt das Sicherheitskonzept des Push-Dienstes vor und bewertet die von RIM verwendeten Schutzmechanismen.

2.3 DuD 2006 – 27.-28. März

Das Programm der achten jährlichen Fachkonferenz „Datenschutz und Datensicherheit – DuD 2006“ am 27.-28.03.2006, seit 1999 von COMPUTAS in Zusammenarbeit mit den Herausgebern der Zeitschrift DuD konzipiert und durchgeführt, wird in Kürze verfügbar sein.

Das etablierte Treffen führender Datenschützer und IT-Sicherheitsverantwortlicher in Deutschland wird sich aktuellen Themen wie Phishing, Spam, Pharming, BlackBerry Security, Kundenkarten, Scoring und Honeynets widmen. Schon jetzt ist eine Voranmeldung möglich.

3 Veranstaltungshinweise

November 2005	
30.11.	BlackBerry Security Symposium (Secorvo, Karlsruhe)
Dezember 2005	
01.-02.12.	Der bDSB in der Praxis (Euroforum, Düsseldorf)
05.-06.12.	IsSec/Zertifa 2005 (COMPUTAS, Berlin)
06.-07.12.	Prüfung zum Certified IT Security Professional (CISP) (Secorvo College, Karlsruhe)
08.12.	Sicherheit von E-Mail-Push-Diensten (Simedia, Bonn)
27.-30.12.	22nd Chaos Communication Congress (CCC, Berlin)
Januar 2006	
24.-26.01.	IT-Sicherheit heute – Angriffe, Konzepte, Lösungen (Secorvo College, Karlsruhe)
30.-31.01.	Net-ID 2006 - Identity, Trust, Privacy & Security (COMPUTAS, Berlin)
Februar 2006	
07.-10.02.	PKI (Secorvo College, Karlsruhe)
14.-15.02.	Inside Windows Security (Secorvo College, Karlsruhe)
März 2006	
27.-28.03.	DuD 2006 (COMPUTAS, Berlin)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de