Secorvo Security News
Juli 2006

Dirk Fox, Stefan Gora, Kai Jendrian,
Stefan Kelm, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 7, 5. Jhrg. 2006
Stand 19. Juli 2006

ISSN 1613-4311

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

Inhalt

Editorial: FlieWaTüüt

Eine Lieblingsgeschichte meiner Kindheit, „Robbi, Tobbi und das FlieWaTüüt“ von Boy Lornsen, hat wahrscheinlich den Ingenieur in mir geweckt. Die phantastischen Abenteuer des kleinen Erfinders Tobbi mit einem Roboterjungen und seinem selbst entworfenen „FlieWaTüüt“, einer Kreuzung aus Mini-Wasserhubschrauber und dreirädriger Piaggio-APE, waren für mich der Jules Verne des 20. Jahrhunderts. (Die spektakuläre WDR-Verfilmung von 1972 gibt es übrigens seit 2005 auf DVD.)

Begeistert hat mich die Vision eines Fahrzeugs, das alle wesentlichen Funktionen vereint. Heute gibt es ein Wort dafür: Konvergenz – das Zusammenwachsen unterschiedlichster technischer Lösungen. Standardisierte anwendungsneutrale Basistechnologien wie PC, Internet und digitale Ton- und Bilddaten ermöglichen heute verschiedenste Funktionen auf einem Gerät.

So mutiert das mobile Telefon mit Fotoapparat, Radio, Armbanduhr, MP3-Player, Spielekonsole und mobilem Fernseher zum „TelMusKlick“. Als Smartphone enthält es Adressbuch, Taschenrechner, Terminkalender, E-Mailer, Notizblock und Internet-Browser, erlaubt es die Bearbeitung von Office-Dokumenten, schickt Präsentationen an einen Beamer und navigiert durch unbekannte Städte. Es ist Informationsdienst und Online-Auskunft, Vorleser, Fremdenführer und Dolmetscher in einem.

Bald sucht es sich automatisch die günstigsten Netze (UMTS, WLAN oder Bluetooth), synchronisiert seine Daten mit zentralen Adress- und Datenservern über das Internet, ersetzt Privatbibliothek, Tageszeitung und Musiksammlung. Es öffnet und verschließt Türen und Fahrzeuge und steuert Jalousien und Haushaltsgeräte.

Ein Alleskönner für die Hosentasche – und ein gefundenes Fressen für Angreifer. Firewall-freie Kommunikationsverbindungen und sensibelste Daten mit komplexer (ergo fehleranfälliger) Softwarekonzentration in den Händen unkundiger Nutzer – hätte Jules Verne das geahnt, wäre daraus ein spannender Science Fiction geworden.

1 Security News

1.1 BCM-Standard

Am 03.07.2006 hat das British Standards Institute (BSI) eine Vorabversion des Standards BS 25999-1 *Guide of Practice for Business Continuity Management (BCM)* zur Kommentierung bis zum 31.08.2006 und zur Diskussion veröffentlicht.

In der Tradition des BS 7799 gibt das BSI mit diesem Standard auf Best Practices beruhende Richtlinien und Empfehlungen heraus. Das Dokument liefert eine gute Einführung in BCM-Begriffe und Vorgehensweisen. Für BCM-Interessierte ist daher schon die Vorabversion des Standards eine Lektüre wert.

1.2 Security Tool Hitparade

Von Fyodor, dem Entwickler des bekannten Port-Scanners nmap wurde am 21.06. 2006 das Ergebnis seiner Umfrage zum Thema Security Tools auf der Mailing-Liste Nmap Hackers veröffentlicht. Aus den 3243 Antworten wurde eine repräsentative Rangliste von Security Tools erstellt und unter SecTools.Org publiziert. Die Liste ist eine wahre Fundgrube und gibt Auskunft über die Popularität eines Tools, den kommerziellen Status, das Abschneiden im Vergleich zur letzten Umfrage 2003 und die unterstützten Betriebssysteme. Sie enthält eine kurze Zusammenfassung der Funktionsweise und einen Link auf das Tool.

1.3 Operational Risk Survey

Am Henley Management College wird derzeit eine anonyme Online-Befragung über den Zusammenhang zwischen operationellen Risiken und Informationssicherheit in der Praxis durchgeführt. Zur Teilnahme sind Sicherheitsexperten mit Praxiserfahrung aufgerufen. Der Fragebogen umfasst 44 Multiple-Choice-Fragen und Statements und lässt sich in wenigen Minuten beantworten. Auf Wunsch erhalten Teilnehmer das Summary der Studie zugesandt.

1.4 Mehr Glück als Verstand

... könnte das Fazit des Datendiebstahl-Vorfalls bei der US-Armee sein, über den wir in den SSN 06/2006 berichtet haben: Am 29.06.2006 wurden der Laptop und die betroffene externe Festplatte sichergestellt; Untersuchungen des FBI ergaben, dass ein Zugriff auf die betroffenen Daten mit hoher Wahrscheinlichkeit ausgeschlossen werden kann.

Erwähnenswert ist der offizielle Bericht des Office of Inspector General der betroffenen Behörde. Das Dokument ist lesenswert für jeden Sicherheitsverantwortlichen, da hier auf über 40 Seiten ein GAU beim Umgang mit einem Sicherheitsvorfall schonungslos dokumentiert wird.

1.5 SSL Revisited

„Trau, schau, wem!“ war das Fazit des Artikels „Un-SSL-Zertifikate?“ aus den SSN 06/2006. Die negativen Erfahrungen mit dem Entfernen aller CA-Zertifikate unter Windows 2000 veranlassten uns zu untersuchen, welche Zertifikate gefahrlos aus dem Zertifikatsspeicher gängiger Browser entfernt werden können, um sie auf eine individuell vertrauenswürdige Sammlung zu reduzieren. Dazu wurden die gängigen Versionen von Internet Explorer, Firefox und Opera unter Windows 2000 untersucht. Als Ergebnis lässt sich festhalten, dass Windows 2000 nur die sechs von Microsoft zwingend vorgeschriebenen CA-Zertifikate benötigt. Bemerkenswerterweise sind von diesen bereits vier abgelaufen. Ein Windows XP System startete auch ohne diese sechs CA-Zertifikate fehlerfrei; zumindest für den Bootvorgang ist Microsofts Vorgabe an Minimalzertifikaten unter Windows XP demnach nicht erforderlich. Aus den Browsern Firefox und Opera ließen sich alle lokalen CA-Zertifikate ohne funktionale Einschränkung entfernen.

„Trau, schau, wem!“ bleibt also auch nach den Tests die Botschaft im Umgang mit SSL-Zertifikaten. Wer daher nicht blind jeder SSL-Verbindung trauen mag, sollte alle CA-Zertifikate löschen, deren Vertrauenswürdigkeit ihm nicht gesichert erscheint.

1.6 SAP-Baustein IT-GSHB

Auf den Webseiten des BSI wurde am 20.06.2006 eine Vorabversion des neuen Bausteins „B 5.13 SAP System“ für das IT-Grundschutzhandbuch bereit gestellt. Der recht umfassende Baustein (133 Seiten) gibt einen Überblick der potentiellen Gefährdungen sowie der relevanten Maßnahmen auf Basis von IT-Grundschtz. Die Maßnahmen sind recht gut beschrieben und wurden durch Kontrollfragen ergänzt. Somit wird nun mit SAP eine weitere wesentliche Anwendung und Plattform abgedeckt.

1.7 bDSB-Handreichung

Für den betrieblichen Datenschutzbeauftragten hat der Arbeitskreis Datenschutz des BITKOM am 21.04.2006 zwei wertvolle Handreichungen veröffentlicht: Einen Praxisleitfaden zum Verfahrensverzeichnis nach BDSG, der neben einigen wichtigen Klarstellungen, konkreten Beispielen und Formblättern für die Datenerhebung auch eine tabellarische Gegenüberstellung von Tools zur Gestaltung des Verfahrensregisters enthält. Eine wertvolle Hilfestellung zur Umsetzung des BDSG in der Praxis.

Das zweite Dokument zur Datenschutzproblematik bei grenzüberschreitender Datenübermittlung macht die nicht ganz einfache Rechtslage transparent und gibt konkrete Empfehlungen für die Praxis.

1.8 PIN-Reset bei O2 (UK)

Im aktuellen Cryptogram vom 15.07.2006 stellt Bruce Schneier das vereinfachte PIN-Reset-Verfahren von O2 in Großbritannien zur Diskussion. Danach kann nach einer Sperrung der SIM-Karte ein PUK (Personal Unlocking Key) ohne weiter gehende Authentifizierung allein mit Angabe der Handynummer beantragt werden.

In Ermangelung eines britischen Kartenvertrags konnten wir dies nicht verifizieren; nach den Angaben von Bruce Schneier wurde aber von O2 zu den Risiken des Verfahrens wie folgt Stellung genommen:

- Ist das gestohlene Handy ausgeschaltet, kann die Telefonnummer nicht in Erfahrung gebracht und so auch keine PUK beantragt werden.
- Ist das Handy eingeschaltet, kann ein Dieb auch ohne PIN/PUK telefonieren.

Das Risiko wird von O2 daher als gering eingestuft, da in beiden Fällen der Provider ohnehin umgehend über den Verlust informiert und die SIM-Karte sperren würde.

Von O2 wurden jedoch nicht alle denkbaren Fälle bedacht. Uns sind mindestens drei Denkfehler aufgefallen. Ihnen auch? Dann senden Sie Ihre Überlegungen bis 15.08.2006 an sommerquiz@secorvo.de. Unter allen Einsendern verlosen wir einen kostenlosen Zugang zum security-finder für ein Jahr. Die kreativsten Angriffsideen werden in den nächsten SSN veröffentlicht.

1.9 Spyware by Microsoft

Die aus Microsofts „Windows Genuine Advantage“ (WGA) Programm hervorgegangene Lizenz-Validation wurde am 27.06. 2006 zu einer WGA-Notification erweitert, die sich nach der Installation wie Spyware verhält: wiederholte Starts (bei jedem Windows Logon und alle 24 Stunden), Untersuchung von Hard- und Software (MAC-Adresse, IP-Adresse, Informationen zum Benutzerkontext), unaufgeforderte Anzeige von Informationen (Popups), Übermittlung von Daten ohne Autorisierung und Wissen des Endbenutzers an externe Microsoft-Server.

Das Unterschieben der erweiterten Funktionalität als sicherheitskritisches Update im Rahmen des (ggf. automatischen) Windows-Update Services führte insbesondere auf Privatsystemen zu einer starken Verbreitung. Allerdings handelt es sich bei diesem Update inhaltlich nicht um System-Sicherheit, sondern um Lizenzkontrolle. Für ein ähnliches Verhalten wurden Spyware-Anbieter unlängst rechtkräftig verurteilt (Smartbot.Net und Odysseus).

Auch wenn die bisherigen Stellungnahmen von Microsoft eine Identifizierung der Endbenutzer verneinen, bleibt eine negativer

Beigeschmack, da das Tool Informationen in der Privatsphäre des Nutzers erhebt und an Microsoft sendet.

2 Secorvo News

2.1 Secorvo College aktuell

Das Seminar IT-Sicherheitsaudits in der Praxis wurde auf Anregung zahlreicher Teilnehmer zu einem dreitägigen Seminar ausgebaut. Das Vortragsprogramm wird nun ergänzt durch drei Workshop-Teile; für das Thema „Rechtliche Rahmenbedingungen und Datenschutz“ ist mehr Raum vorgesehen.

2.2 Business Continuity

In Folge der insbesondere im Kontext von KontraG, SOX und Basel II verstärkten Bemühungen aller Unternehmen um Compliance, d.h. die Übereinstimmung der Form der Geschäftsausübung mit gesetzlichen Anforderungen aller Art, rückt neben dem Datenschutz auch die Beschäftigung mit denkbaren Notfällen in den Fokus der Informationssicherheit.

Aus mehreren Projektarbeiten ist nun eine ausführliche Darstellung unseres Leistungsangebots im Gebiet Business Continuity und Disaster Recovery entstanden.

2.3 5 Jahre KA-IT-Si

In diesem Jahr jährt sich die Gründung der Karlsruher IT-Sicherheitsinitiative zum fünften Mal. Dieses Jubiläum wird die KA-IT-Si am **18.10.2006** feiern – im **Saal Baden der IHK Karlsruhe**, dem Ort, an dem am 25.01.2001 die KA-IT-Si aus der Taufe gehoben wurde. Die Key Note wird Herr Dr. Udo Helmbrecht, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) halten, flankiert von anschaulichen Praxisberichten zur „Herausforderung IT-Sicherheit im Mittelstand“, einer Ausstellung der Sicherheitslösungen der KA-IT-Si-Partner und einem anschließenden „Net(t)-working-Büfett“. Online-Anmeldung unter www.ka-it-si.de.

3 Veranstaltungshinweise

Juli 2006	
31.07. - 04.08.	USENIX Security Symposium (USENIX, Vancouver/CA)
August 2006	
02.-03.08.	Black Hat USA 2006 (Black Hat, Las Vegas/USA)
04.-06.08.	DEFCON 14 (Defcon, Las Vegas/USA)
20.-24.08.	Crypto 2006 (IACR, Santa Barbara/USA)
September 2006	
19.-21.09.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
26.-29.09.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
Oktober 2006	
04.-05.10.	Inside Windows Security (Secorvo College, Karlsruhe)
10.-12.10.	ISSE 2006 (TeleTrusT/EEMA, Rom/IT)
16.-20.10.	Information Security Management (Secorvo College, Karlsruhe)
17.-18.10.	DACH Mobility 2006 (GI/ÖCG/BITKOM/SI, München)
18.10.	KA-IT-Si-Jubiläumsfeier (KA-IT-Si, IHK Karlsruhe)
23.-27.10.	Systems 2006 (Messe München, München)

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