secorvo
security consulting

Secorvo Security News

März 2007

Editorial: Wolf im Schafspelz?

Sie erinnern sich: Nicht einmal fünf Jahre ist es her, da erhielt Microsoft Deutschland bei der Verleihung der „Big Brother Awards 2002“ am 25.10.2002 in Bielefeld den Hauptpreis – in der Kategorie „Lifetime“. Prämiert wurden die Verdienste Microsofts um die „flächendeckende Einführung von Kontrolltechnologie für Urheberrechte“. In seiner Laudatio erinnerte Patrick Goltzsch an die automatische Online-Registrierung unter Windows 98, die seinerzeit die Wogen der Entrüstung hoch gehen ließ: Microsoft hatte die Hardware-Konfiguration der Client-Systeme analysiert und diese Daten zusammen mit einer eindeutigen Kennung „nach Hause telefoniert“.

Und nun das: Am 16.02.2007 wurde Microsoft Deutschland durch den Ministerpräsidenten von Schleswig Holstein das Datenschutz-Gütesiegel des Unabhängigen Landeszentrums für Datenschutz (ULD) für den „Microsoft Update Service 6.0“ und den „Windows Server Update Service 2.0“ verliehen. Da reiben sich aufmerksame Beobachter die Augen: Wie ist das möglich? Wurde da ein Saulus zum Paulus?

Bei genauer Betrachtung löst sich der vermeintliche Widerspruch. Den Big Brother Award hatte der damalige Datenschutzbeauftragte von Microsoft Deutschland, Sascha Hanke, persönlich entgegengenommen – ein Novum in der Geschichte der Awards. Und er nahm ihn ernst: „Wir sind nicht erfreut über den Preis, akzeptieren aber das Urteil der Jury.“

Intern setzte er anschließend alle Hebel in Bewegung, um aus der „Vermarktungsbremse“ Datenschutz einen Wettbewerbsvorteil zu machen. Ein Ergebnis waren die „Privacy Guidelines“ für Softwareentwickler (SSN 12/2006). Sein Nachfolger konnte nun nach 18-monatiger Prüfung das Gütesiegel entgegennehmen. Auch wenn dies nur ein Anfang gewesen sein darf, soll die Mutation zum Lämmchen glaubwürdig bleiben, so drängt sich doch die Frage auf, warum erst ein *amerikanischer* Software-Konzern kommen muss, um in Deutschland Datenschutzgeschichte zu schreiben...

Inhalt

secorvo
security consulting

Security News

BKA-Forensik

Für Wirbel sorgte ein kurzer Artikel in der Süddeutschen Zeitung vom 07.03.2007. Danach gelang es BKA-Forensikern, die Festplatte des Computers eines der beiden mutmaßlichen Bombenleger von Köln zu spiegeln und die vom Besitzer zuvor gelöschten Dateien zu rekonstruieren. Das Ergebnis der forensischen Analyse ist allerdings wenig spektakulär: Moderne Forensik-Tools, auch kostenlose OpenSource-Toolkits, konnten schon immer Dateien wiederherstellen, die nicht sicher gelöscht oder physisch zerstört waren. Der Aufwand hierfür ist überschaubar, was auch Secorvo in etlichen forensischen Analysen nachweisen konnte. Zudem hatte der Verdächtige zuvor gestanden, die später gefundenen Bombenbauanleitungen auf dem Rechner gespeichert zu haben.

Interessant wird die Nachricht jedoch im Zusammenhang mit einer Rede des BKA-Präsidenten Jörg Zierke anlässlich des 10. Europäischen Polizeikongresses in Berlin. Zierke nahm die „Kofferbomber" zum Anlass, um eingehend für die Notwendigkeit von Online-Durchsuchungen zu plädieren, „mit der ganz gezielt schwere Straftaten aufgedeckt werden sollen." Dass die Beispiel-Straftat freilich ohne jede Online-Durchsuchung aufgeklärt wurde und auch durch diese nicht hätte verhindert werden können, erwähnte Zierke indes nicht. „99,99% der Menschen in Deutschland werden davon niemals betroffen sein", wollte Jörg Zierke beruhigen. Dass diese Einschätzung noch gilt, wenn das Instrument erst eingeführt ist, darf angesichts wachsender Begehrlichkeiten der Strafverfolgungsbehörden bezweifelt werden. Ein stichhaltiges Argument für den Grundrechtseingriff ist Zierke jedenfalls schuldig geblieben.

Drive-by Pharming

Unter der Bezeichung „Drive-by Pharming" wurde am 15.02.2007 von Zulfikar Ramzan auf Bugtraq eine neue Angriffsmethode veröffentlicht: Auf einer Webseite hinterlegter bösartiger JavaScript-Code, der beim Betrachten der Seite ausgeführt wird, ändert die DNS-Einstellungen des (DSL-) Zugangsrouters so, dass der Netzwerkverkehr über das Angreifersystem umgeleitet wird. Das funktioniert, wenn die Standard-Kennwörter beibehalten wurden – Proof-of-Concepts für Router von Linksys, D-Link und Netgear sind verfügbar. Zweifellos funktioniert die Methode auch bei weiteren Herstellern.

Das Prinzip ist nicht neu, die Kombination aber kreativ. Schutz vor derartigen Angriffen bietet eine der einfachsten und ältesten Sicherheitsmaßnahmen: Das sofortige Ändern von Default-Passworten. Wer diesen Aufwand scheut, darf sich nicht wundern, wenn seine Kommunikationsinhalte in dunklen Kanälen landen.

Mcert schließt, DSIN lebt (noch)

Nach einem bisher unbestätigten, aber undementierten Bericht der Financial Times Deutschland vom 16.03.2007 stellt das Mcert im Juni seine Tätigkeit ein. Das vom BITKOM am 15.10.2002 ins Leben gerufene Mittelstands-CERT (SSN 05/2002) litt schon unter Startschwierigkeiten: Die operative Arbeit nahm es erst knapp 14 Monate später am 09.12.2003 auf (SSN 12/2003). Nachdem es offenbar nicht gelang, eine nennenswerte Zahl Kunden für das Dienstleistungsangebot zu gewinnen, wenden sich die Sponsoren nun Microsofts und SAPs Marketing-Initiative „Deutschland sicher im Netz" zu.

Aber auch diese am 31.01.2005 medienwirksam von Bill Gates gestartete Initiative schwächelt: Der im Juni 2005 initiierte monatliche Newsletter erlebte nur acht Ausgaben, vom „wöchentlichen Sicherheitstipp" gibt es nur noch ein Archiv und der Webauftritt wirkt unkoordiniert und strukturlos – zu viele Köche verderben bekanntlich den Brei.

Seit dem 31.12.2006 ist ein Verein Träger der Initiative; Bundesinnenminister Wolfgang Schäuble soll die Schirmherrschaft übernehmen. Vor welchen Marketing-Karren er da gespannt werden soll, entlarvt erst der Blick in die Details: Für einen PC-Neukauf werden die Modelle von Fujitsu-Siemens mit dem „Gütesiegel Sicherheitsempfehlung der Initiative Deutschland sicher im Netz" und zum Schutz vor Viren die „Virenschutzlösung eTrust EZ Antivirus 2005 (!)" des Partners CA empfohlen. Ein Schelm, wer Arges dabei denkt...

27001 + 1 = 27006

Am 01.03.2007 hat die International Organization for Standardization (ISO) mit dem Standard ISO/IEC 27006:2007(E) das zweite Werk aus der 27000er Reihe veröffentlicht. Der Standard mit dem sperrigen Titel "Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems" (ISMS) spezifiziert Anforderungen an Organisationen, die Audits und Zertifizierungen von Informationssicherheitssystemen nach ISO/IEC 27001:2005(E) durchführen.

Diese Anforderungen ergänzen die allgemeineren Erfordernisse aus den Standards ISO/IEC 17021:2006 und ISO/IEC 19011:2002. Zusätzlich werden Hinweise zur Vorbereitung und Durchführung von ISMS-Audits gegeben; damit ist der Standard auch für Organisationen interessant, die sich aktiv mit ISMS-Audits beschäftigen.

Grundschutz extended

Im Newsletter vom 09.03.2007 hat das BSI die Veröffentlichung der neuen Grundschutz-Bausteine „Sicherheit in SAP Systemen“, „Speichersysteme und Speichernetze“, „Windows Server 2003“, „Wireless LAN“ und „Voice over IP“ bekannt gegeben. Auch wurde der Baustein „Datenbanken“ grundlegend überarbeitet. Die Metadaten für das vom BSI entwickelte GSTOOL wurden entsprechend angepasst und stehen zum Download zur Verfügung. An den zahlreichen Erweiterungen lässt sich erkennen, dass der Grundschutz lebt. Die enge Verknüpfung mit dem Standard ISO/IEC 27001:2005(E) bei gleichzeitigem Ausbau der technisch orientierten Gefährdungs- und Maßnahmenkataloge macht den IT-Grundschutz zu einem mächtigen Werkzeug.

Month of PHP Bugs

Am 01.03.2007 begann der „Month of PHP Bugs“ (MoPB), ausgerufen vom „The Hardened-PHP Project“. Zielsetzung der Initiatoren ist es, auf bekannte Fehler im Kern von PHP aufmerksam zu machen. Der zu den bisher veröffentlichten 26 Fehlern verfügbare Patch-Status vom Februar 2007 wird ebenfalls aufgelistet. Aus Gründen der Übersichtlichkeit werden Fehler in PHP-Anwendungen nicht berücksichtigt; dazu finden sich genügend Schwachstellen auf einschlägigen Mailinglisten wie Bugtraq und Full Disclosure.

Amüsant sind die Zitate im Titel des jeweiligen Fehlers, die allein schon eine eigene Geschichte über sichere Softwareentwicklung erzählen: „Let's not break binary compatibility in PHP4 anymore“ oder „Hello, is this the end of the buffer?“ Nicht ohne Grund gibt es im PHP-Umfeld auch Sicherheitsprojekte, die sich speziell der Härtung von PHP (z.B. Suhosin) widmen.

Secorvo News

Secorvo College aktuell

Mit der T.I.S.P.-Schulung Anfang März haben inzwischen 12 Absolventen bei Secorvo College ein T.I.S.P.-Zertifikat erworben. Von den Absolventen wurden die gelungene Darstellung des Gesamtzusammenhangs und die Abstimmung der Vorträge aufeinander, der Praxisbezug und die Kompetenz der Referenten gelobt. Wegen der großen Nachfrage bietet Secorvo College vom 25.-30.06.2007 eine zusätzliche T.I.S.P.-Schulung mit Prüfung an. Weitere Seminare vor der Sommerpause:

- IT-Sicherheitsaudits in der Praxis (17.-19.04.)
- Sichere Softwareentwicklung (24.-26.04.)
- Kommunikationsschutz und Datensicherheit (08.-10.05.)

Programm, Preise und Online-Anmeldung unter www.secorvo.de/college

Lizenz zum Prüfen

Neben Stefan Gora wird nun auch Kai Jendrian vom BSI lizenzierter ISO-27001 Auditor auf der Basis von IT-Grundschutz. Beide haben sich außerdem 2006 als T.I.S.P. qualifiziert. Ende November 2006 erwarb Jörg Völker zu seiner Zertifizierung als BS 7799 Lead Auditor auch die Zertifizierung zum Lead Auditor nach ISO 27001.

ITSF 2007

Vom 07.-10.05.2007 findet das diesjährige IT-Sicherheits-Forum (ITSF) 2007 von ComConsult und GAI Netconsult in Königswinter statt, an dem auch diesmal wieder Referenten von Secorvo mitwirken .

Virtuelle Sicherheit?

„Wie virtuell ist Ihre Sicherheit?“ lautet der Titel des kommenden Events der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 29.03.2007 (Beginn: 18 Uhr im Schlosshotel Karlsruhe). Dr. Christian Riede und Stefan Kratzer von der Firma CONNECT werden die Herausforderungen von Virtualisierungskonzepten für die IT-Security beleuchten. Das verspricht nicht nur ein spannender Vortrag zu werden: die bis heute eingegangenen über 50 Anmeldungen lassen spannende Diskussionen und ein interessantes Net(t)working am Buffet erwarten. Online-Anmeldung unter www.ka-it-si.de.

Security Awareness Symposium

2007 jährt sich das „Security Awareness Symposium“ zum fünften Mal. Auch diesmal erwarten wir einen regen Erfahrungsaustausch von Verantwortlichen aus Unternehmen und Behörden, die Security Awareness-Kampagnen durchgeführt haben, planen oder derzeit umsetzen.

Nach Präsentationen von u. a. BASF, BMW, Bosch, DAK, Fiducia, FinanzIT, Münchener Rück, Novartis, SAP, Swiss Re und T-Systems in den Vorjahren werden in diesem Jahr Airbus, das BSI, Carl Zeiss, e.on, M. DuMont und RWE Systems ihre Kampagnen und „Lessons Learned“ vorstellen.

Wegen der wachsenden Teilnehmerzahlen wird das Symposium erstmals nicht in den Räumen von Secorvo, sondern in der Tagungsstätte Buhlsche Mühle in Ettlingen stattfinden (10 min. Fahrt vom Karlsruher Hbf). Termin: 12.-13.06.2007.

Eine Vorversion des Programms und ein Anmeldeformular finden Sie unter
www.security-awareness-symposium.de

Veranstaltungshinweise

Auszug aus www.veranstaltungen-it-sicherheit.de

März 2007	
26.-28.03.	Fast Software Encryption 2007 (IACR, Luxembourg)
26.-29.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)
27.-30.03.	Black Hat Europe 2007 (Black Hat, Amsterdam)
29.03.	Wie virtuell ist Ihre Sicherheit? (KA-IT-Si, Karlsruhe)
April 2007	
10.-.13.04.	SecSE 2007 The First International Workshop on Secure Software Engineering (ENISA, Wien)
17.-19.04.	IT-Sicherheitsaudits in der Praxis (Secorvo, Karlsruhe)
24.-26.04.	Sichere Softwareentwicklung (Secorvo, Karlsruhe)
Mai 2007	
07.-10.05.	ITSF 2007 (ComConsult, Königswinter)
08.-10.05.	Kommunikationsschutz und Datensicherheit (Secorvo, Karlsruhe)
22.-24.05.	10. Deutscher IT-Sicherheitskongress (BSI, Bonn)

Fundsache

Auszug aus www.security-finder.de

Das über 30 Jahre alte Tutorial The Protection of Information in Computer Systems ist eine epochale Zusammenstellung der grundlegenden Entwurfsprinzipien und Mechanismen für sichere IT-Systeme aus der Sicht von Betriebssystemarchitekten. Eine historische Referenz, die belegt, wie lange einige der immer noch häufig angemahnten Prinzipien schon bekannt sein müssten.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

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

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