Secorvo Security News
Oktober 2005

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

Nr. 10, 4. Jhrg. 2005
Stand 28. Oktober 2005

ISSN 1613-4311

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

Inhalt

Editorial: Das Enigma-Trauma

Mit der Veröffentlichung in der Wirtschaftswoche platzte am 05.10.2005 die Bombe: In einer internen Studie vom 20.09.2005 bescheinigt das BSI dem auch liebevoll Tamagotchi für Manager genannten Blackberry des kanadischen Herstellers RIM, er sei „auf Grund der unsicheren Architektur (...) für den Einsatz in der öffentlichen Verwaltung und spionagegefährdeten Unternehmen nicht geeignet“ – ein Verdikt, dass die Wogen hoch schlagen ließ. Die Angst: Der britische Geheimdienst könnte trotz Verschlüsselung über das in Egham bei London gelegene RIM-Rechenzentrum auf Verbindungs- und Inhaltsdaten zugreifen.

Ob hier ein Enigma-Trauma nachwirkt? Lange glaubte man bei den Nachrichtendiensten, auch dem BSI-Vorläufer ZfCh, an die Sicherheit der von der Wehrmacht eingesetzten Verschlüsselungsmaschine, bis Ende der 60er Jahre bekannt wurde, dass der britische Geheimdienst seit Anfang der 40er Jahre in Bletchley Park deutsche Funksprüche entschlüsselte.

Damit sich die Geschichte nicht wiederhole, informierte Lutz Diwell, Staatssekretär im BMI, bereits am 16.09.2005 alle Bundesministerien und bat „nachdrücklich, keine weiteren Investitionen in Blackberry-Geräte zu tätigen“. Statt dessen empfahl er, sich an einer in den Informationsverbund Berlin-Bonn (IVBB) integrierten Alternativlösung zu beteiligen, die „aufgrund der hohen Bedarfslage in der Bundesverwaltung“ von BMI, BMF und BSI „mit Hochdruck“ entwickelt werde und sich bereits im Pilotbetrieb befinde.

Nach RIM-Managerin Eggberry beruhen die BSI-Schlussfolgerungen „auf einem kompletten Mangel an Kenntnis von RIMs Sicherheitsarchitektur und –infrastruktur“. Für RIM und die Mobilfunkbetreiber steht viel auf dem Spiel: Schon über 3,65 Millionen Manager lassen sich ihre E-Mails direkt auf Blackberry oder Handy liefern.

Zur Versachlichung der Diskussion plant Secorvo für den 30.11.2005 eine Veranstaltung mit einem Vertreter von RIM und dem BSI in Karlsruhe – Näheres in Kürze.

1 Security News

1.1 Open Source und zurück

Kürzlich wurde das Unternehmen Sourcefire, maßgeblich an der Entwicklung des Open Source IDS-Systems snort beteiligt, durch Checkpoint übernommenen. Nun soll auch die nächste Nessus Version 3 zwar kostenfrei bleiben, aber vom maßgeblich am Nessus-Projekt beteiligten Unternehmen Tenable (siehe SSN 2/2005) als closed source weiterentwickelt werden.

Die Begründung des Tenable-Geschäftsführers Ron Gula, dieser Schritt sei auf zunehmende Kundenanfragen zurück zu führen, die OpenSource nicht einsetzen möchten oder können, klingt vorgeschoben. Auch anderen scheint es so zu gehen: So wurden bereits Nessus-Ableger wie die Projekte Porz-Wahn und GNessUs gegründet, die Nessus als Open Source unter GPL weiterentwickeln möchten.

1.2 ISO 27001 + Grundschutz

Seit dem 14.10.2005 ist die ISO 27001 nun offiziell publiziert und kann für 124 CHF unter http://www.iso.ch bezogen werden.

Mit der ISO 27001 wurde der britische Standard BS7799-2:2002 in einen internationalen Standard überführt. Die Änderungen zu BS7799-2:2002 sind eher gering. Es gibt einige wenige zusätzliche Detailanforderungen, eine leichte Umstrukturierung der Gliederung (das Kapitel 6.4 "Internal ISMS audits" aus BS7799 ist nun als eigenes Kapitel 6 geführt) und der normative Annex A (control objectives and controls) verweist jetzt auf die ISO/IEC 17799:2005 statt der 2000er Version.

Bestehende bzw. laufende Zertifizierungen nach BS7799-2:2002 sollten eigentlich nach ISO 27001 überführt werden können. Die für Deutschland zuständige Akkreditierungsstelle (Trägergemeinschaft für Akkreditierung GmbH) müsste hierzu ein entsprechendes „certification transition statement“ veröffentlichen; bislang scheint es ein solches aber nicht zu geben.

Das BSI hat das Sicherheitsmanagement beim IT-Grundschutz maßgeblich an den neuen ISO-Standard 27001 angepasst. Der BS 7799-2 Nachfolger ist ab 2006 auch Bestandteil der Zertifizierung nach IT-Grundschutz. Daher wurde zum 01.10.2005 auch das Lizenzierungsschema für IT-Grundschutzauditoren geändert: Die Anforderungen der internationalen Norm EA 07/03 müssen zukünftig erfüllt werden. Für bereits lizenzierte Auditoren werden entsprechende Kompaktkurse angeboten.

1.3 No-NX

Seit 2004 verfügen moderne x86-Prozessoren über ein „No Execute“ (NX) genanntes Sicherheits-Feature. Dieses Feature realisiert die schon seit vielen Jahren (zumindest in der Theorie) bekannte strikte Trennung zwischen Daten- und Codesegmenten, die vor allem dem Missbrauch der weit verbreiteten Buffer Overflow Bugs ein Ende setzen sollen. AMD bezeichnet diese neue Funktionalität gar als „Enhanced Virus Protection“; führt sie doch dazu, dass nicht mehr beliebiger Code im Stack oder Heap des Prozessors ausgeführt werden kann.

Noch bevor dieses Feature von allen Betriebssystemen unterstützt wird, gibt es bereits erste erfolgreiche Angriffe dagegen: am 04.10.2005 veröffentlichte Suse-Mitarbeiter Sebastian Krahmer einen technischen Artikel, in dem er zeigt, wie entsprechende Prozessorregister trotz gesetztem NX-Bit mit beliebigen Werten vorbelegt werden können. Dabei handelt es sich nicht um ausführbaren Code, sondern um beliebige Einsprungadressen, an denen Angreifer dann z. B. eigenen Code platzieren könnten. Und obwohl dieser Angriff nicht trivial ist, veröffentlichte der Autor zeitgleich einen unter Linux laufenden Proof-of-concept.

Fazit: Leider ein weiteres Beispiel für „gut gedacht, schlecht gemacht“...

1.4 Pünktchen und Xerox

Schon länger wird gemunkelt, dass hochwertige Farblaserdrucker und –kopierer auf jedem Ausdruck für das bloße Auge

unsichtbare Markierungen anbringen. Hauptziel solcher individueller Wasserzeichen ist es, leichter die Herkunft gefälschter Banknoten oder anderer „Wert"-Papiere aufspüren zu können.

Missbrauchsmöglichkeiten dieses Überwachungsmechanismus liegen aber genau so auf der Hand. Daher hatte die Electronic Frontier Foundation (EFF) dazu aufgerufen, Testseiten möglichst vieler verschiedener Druckertypen für Vergleichstests einzuschicken. Am 13.10.2005 wurde nun als Ergebnis dieser Bemühungen die Analyse des von Xerox verwendeten Markierungscodes aus winzigen gelben Punkten veröffentlicht.

Ein grundsätzliches Problem von derlei Wasserzeichen ist es, korrekt auseinander zu halten, wenn mehrere davon nacheinander angebracht wurden. Es ist daher wohl nur eine Frage der Zeit, bis die erste Software bereit steht, die es erlaubt, beim Ausdruck einer Seite „eigene" Xerox-Pünktchen anzubringen – unabhängig vom Hersteller des Druckers.

1.5 Where Do You Want to Surf Today?

Gleich auf mehreren Wegen versucht man im Moment, der Phishing-Plage Herr zu werden. So hat der Gouvernator von Kalifornien am 30.09.2005 einen Anti-Phishing Act of 2005 in Kraft gesetzt, der bei Strafandrohung von mindestens US$ 2.500 pro Fall (zuzüglich US-üblich hohen Schadensersatzforderungen) Phishing verbietet. Ob dieses Gesetz mehr Wirkung zeigt als Verbote anderer Straftaten, bleibt abzuwarten.

Technisch statt legislativ versucht es Microsoft: Bereits am 29.08.2005 wurde unter dem sperrigen Namen Microsoft® Phishing Filter Add-in for MSN® Search Toolbar (Beta) ein Zusatzmodul für den Internet Explorer 6 veröffentlicht, das eine Funktion der Version 7 vorweg nimmt. URLs bzw. Webserver, die nicht in einer lokalen Whitelist aufgeführt sind, werden von einem zentralen, von Microsoft betriebenen Server geprüft. Ist einer davon als Phishing-Server bekannt, wird der Anwender gewarnt.

Gegen Pharming, bei dem eine gültige URL mit DNS-Tricks auf den falschen Server „verbogen" wird, hilft dieser Ansatz alleine jedoch nicht viel. Und ob der erzielbare Sicherheitsgewinn gegen Phisher es aufwiegt, Microsoft direkt über (fast) alle aufgerufenen URLs zu informieren, darf auch bezweifelt werden.

1.6 Langzeitarchivierung

Die Universität Kassel führt im Auftrag des Bundesministeriums für Wirtschaft und Arbeit (BMWA) eine Studie über Anforderungen und Trends zur Langzeitaufbewahrung elektronisch signierter Dokumente unter der Leitung von Prof. Dr. Roßnagel durch. Dazu sollen Anwender aus Verwaltung und Wirtschaft sowie Hersteller von Aufbewahrungssystemen befragt werden.

Auf der Webseite des Projekts können der Fragebogen und weitere Informationen zur Studie abgerufen werden. Die Universität Kassel freut sich über eine rege Beteiligung bis zum 11.11.2005. Die Ergebnisse der Studie werden Mitte Dezember publiziert.

1.7 Überlistete Scanner

Zentrale oder dezentrale Virenscanner gehören schon seit vielen Jahren zu den Standard-Anwendungen jeder IT-Infrastruktur: Immer mehr verlässt man sich auf hohe Erkennungsraten sowie einwandfreie Funktionalität zum Schutz lokaler Netze.

Um so schlimmer, wenn systematische Schwachstellen in diesen Scannern gefunden werden, wie im Oktober gleich doppelt geschehen: Am 05.10.2005 veröffentlichten Mitarbeiter der SecuBox Labs ein Advisory, in dem sie beschreiben, wie bestimmte Archive so manipuliert werden können, dass Virenscanner nicht mehr in der Lage sind, diese auszupacken und nach Viren zu suchen. Und am 25.10.2005 beschrieb Andrey Bayora in einem weiteren Advisory, dass viele Scanner beim Erkennen von Dateitypen überlistet werden können, in dem wenige Bytes einer Datei verändert

werden, die jedoch weiterhin ausführbar bleibt – interessanterweise ist auf ein ähnliches Problem bereits im Jahr 2000 hingewiesen worden.

Von beiden Schwachstellen sind nahezu alle gängigen Produkte betroffen; viele Hersteller haben jedoch kurzfristig mit entsprechenden Patches ihrer Scanner reagiert. Fazit: nicht nur die Viren-Datenbanken müssen oft und regelmäßig aktualisiert werden, auch die Programme selbst bedürfen ständiger Updates.

2 Secorvo News

2.1 Secorvo College aktuell

Angesichts der aktuellen Entwicklungen beim IT-Grundschutz und dem ISO-Standard 27001 (siehe oben) haben wir unser Seminar „Information Security Management“ entsprechend aktualisiert. Am 14.-16.11. bzw. 14.-18.11.2005 erhalten Sie einen aktuellen Einblick in Best Practices, Standards und Zertifizierungserfahrungen.

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

2.2 IsSec/ZertiFA 2005

Am 05.-06.12.2005 lädt COMPUTAS nach Berlin zu der von Dirk Fox und Stefan Kelm inhaltlich mitgestalteten Doppelkonferenz IsSec/ZertiFA 2005. Das Programm lässt eine spannende Tagung erwarten.

2.3 Secorvo White Paper ISM

Das von Jörg Völker im November 2003 veröffentlichte Secorvo White Paper zum Sicherheitsmanagement nach BS 7799 hat sich mit seitdem mehr als 25.000 Downloads zum meistgelesenen White Paper von Secorvo entwickelt.

Inzwischen hat die Veröffentlichung des ISO 17799:2005 eine Überarbeitung erforderlich gemacht. Die Neufassung des White Papers steht inzwischen auf den Secorvo-Webseiten zum Download bereit.

3 Veranstaltungshinweise

November 2005	
08.-11.11.	Kommunikationsschutz und Datensicherheit (Secorvo College, Karlsruhe)
14.-18.11.	Information Security Management (Secorvo College, Karlsruhe)
15.-16.11.	Einführung in die Praxis des DSB (Euroforum, Berlin)
22.-25.11.	Live Hacking Lab (Secorvo College, Karlsruhe)
Dezember 2005	
01.-02.12.	Einführung in die Praxis des DSB (Euroforum, Düsseldorf)
05.-06.12.	IsSec/Zertifa 2005 (COMPUTAS, Berlin)
06.-07.12.	Prüfung zum Certified IT Security Professional (CISP) (Secorvo College, Karlsruhe)
27.-30.12.	22nd Chaos Communication Congress (CCC, Berlin)
Januar 2006	
24.-26.01.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
30.-31.01.	Net-ID 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