secorvo
security consulting

Secorvo Security News

September 2006

Editorial: 5-50-I000

Jubiläen sind bekanntlich ebenso wichtig wie willkürlich. Wichtig, weil sie die Wurzeln in Erinnerung rufen, zugleich etwas Vollbrachtes vor Augen führen, und sowohl Ermutigung als auch Ansporn sein können. Willkürlich, weil der Termin eines Jubiläums weniger vom objektiven Zeitablauf als vom gewählten Maßsystem abhängt, wie jeder Informatiker weiß. Denn auch wenn die natürliche Beschaffenheit unseres Körpers die Nutzung des Dezimalsystems nahe legt (zehn Finger), versteht sich dies keineswegs von selbst, wie nicht zuletzt die Rechenwerke unserer elektronischen Gehilfen belegen.

Gleich drei Jubiläen feiern wir in diesem Frühherbst:

- Am 18.10.2006 begehen wir das fünfjährige Jubiläum der Karlsruher IT-Sicherheitsinitiative – mit einer halbtägigen Veranstaltung in der IHK Karlsruhe und einer Key Note des BSI-Präsidenten, zu der wir Sie sehr herzlich einladen (Anmeldung).
- Vor Ihnen liegt die 50. Ausgabe der „Secorvo Security News" – und hinter uns 50 Monate, in denen wir Nachrichten recherchiert, gefiltert, bewertet und für Sie aufbereitet haben. Ausgedruckt ein ansehnliches Büchlein von 200 Seiten.
- Am 01.09.2006 konnten wir ein besonderes Ereignis begehen: Vor I000 Jahren wurde Secorvo gegründet – in der Schnelllebigkeit des dot-com-Zeitalters ein gar „biblisches" Alter, dem die Verwendung des Dualsystems angemessen Rechnung trägt.

Das Jubiläum unserer kleinen News, deren Leserzahl ständig wächst, haben wir zum Anlass genommen, die Gestaltung einer gründlichen Überarbeitung zu unterziehen. Dabei wollten wir insbesondere den einzigen Kritikpunkt, der aus Ihren Reihen gelegentlich geäußert wurde, ausräumen: das durch die Spaltenformatierung erforderliche Vor- und Zurückblättern innerhalb einer Seite.

Und auch der security-finder hat ein neues Gesicht bekommen – schauen Sie einmal hinein. Wir freuen uns auf Ihre Rückmeldungen.

Inhalt

secorvo
security consulting

Security News

Krypto-Bug in OpenSSL

Auf der legendären „Rump Session" der diesjährigen Weltkonferenz der Kryptologen, der Crypto 2006 in Santa Barbara, präsentierte Daniel Bleichenbacher am 22.08.2006 eine Möglichkeit zur Fälschung von RSA-Signaturen, die den öffentlichen Exponenten „3" verwenden. So überprüfen die betroffenen OpenSSL-Implementierungen (bis v0.9.7j und v0.9.8b) die Füllbytes („padding") nicht korrekt. Ein Angreifer kann diese Schwachstelle relativ einfach nutzen, um eine dritte Wurzel als gültige Signatur in den überschüssigen Bytes zu verstecken. Forscher der TU Darmstadt haben einen Exploit entwickelt.

Ein am 05.09.2006 veröffentlichtes Advisory empfiehlt ein Update auf neuere OpenSSL-Versionen. Produkte, die direkt auf OpenSSL aufsetzen (z.B. BIND in Verbindung mit DNSSEC-Signaturen) sind ebenfalls betroffen, genauso die Browser Firefox (bis v1.5.0.6), SeaMonkey (bis v1.0.4), Opera (bis v9.01) sowie alle Netscape-Browser. Lachende Dritte sind diesmal der nicht betroffene Internet-Explorer (v6) und Apples Safari. Eine Alternative zu einem Upgrade ist das Entfernen von Root-Zertifikaten mit dem öffentlichen Exponenten „3" aus dem Zertifikatsspeicher des Browsers – die leider nach wie vor verwendet werden, obwohl deren Anfälligkeit für Angriffe seit mehr als 10 Jahren bekannt ist.

ISO 27001-Zertifikat für SAP SI

Den hochverfügbaren Serverzentren des Geschäftsbereichs Hosting der SAP Systems Integration AG am Standort Dresden wurde am 31.07.2006 vom BSI ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz verliehen. Diesem Beispiel werden in Kürze zweifellos weitere Unternehmen folgen, die in den beiden vergangenen Jahren eine IT-Grundschutz-Zertifizierung erfolgreich absolviert haben, da die Umstellung auf ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz mit moderatem Aufwand möglich ist.

BDSG 2006 in Kraft

Am 25.08.2006 wurde das „Gesetz zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft" veröffentlicht. Es trat am 26.08.2006 in Kraft. Artikel 1 ändert das Bundesdatenschutzgesetz (BDSG): So wurde das Quorum, bis zu dem kein betrieblicher Datenschutzbeauftragter zu bestellen ist, von „höchstens vier Arbeitnehmer" in „höchstens neun Personen" geändert. Damit stellt der Gesetzgeber klar, dass es um die Zahl der Personen unabhängig von ihrem arbeitsrechtlichen Status geht – Geschäftsführer, Praktikanten, Auszubildende und externe Hilfskräfte zählen nun unstreitig dazu. Unternehmen, die unterhalb des Quorums liegen, werden damit jedoch nicht von den Pflichten des betrieblichen Datenschutzbeauftragten befreit. Die Neufassung des § 4g legt für diesen Fall fest, dass „der Leiter der Stelle die Erfüllung der Aufgaben (...) in anderer Weise sicher zu stellen" hat.

.dd -> .vmdk

Der erste Schritt in fast jeder forensischen Analyse ist das Erstellen einer Bit-genauen Kopie (Image) des zu untersuchenden Datenbestands, um die Analyse anschließend auf dieser Kopie durchführen zu können, ohne Originaldaten zu verändern. Oft kommt dabei das in der Unix-Welt verbreitete Tool „dd" zum Einsatz. Die so erstellten Images können dann einer statischen oder dynamischen Analyse unterzogen werden. Nachteil der dynamischen Analyse ist, dass dabei das Image grundsätzlich verändert wird – der Forensiker wird daher mehrere Images des Originals erstellen, damit er immer wieder auf den Ausgangszustand der Daten zurückgreifen kann.

Am 25.08.2006 wurde Live View vorgestellt, ein neuartiges Tool, das es erlaubt, dd-Images in virtuelle Maschinen zu konvertieren. Diese können anschließend mit der Software VMware analysiert werden, um beispielsweise Details über laufende Prozesse oder offene Netzwerkverbindungen auf dem zu untersuchenden Rechner zu erhalten.

Das Tool wurde im CERT-Umfeld entwickelt und setzt Java voraus. Es befindet sich noch in einem sehr frühen Entwicklungsstadium, läuft jedoch bereits recht stabil.

Besser zweimal messen ...

... als einmal vergessen. Getreu diesem Motto fand am 01.08.2006 im Rahmen des 15th Usenix Security Symposium in Vancouver der Workshop Metricon 1.0 engagierter Experten der securitymetrics.org-Community statt. Die 44 Teilnehmer diskutierten intensiv über den Sinn von Metriken, Software-Security-Metriken, Governance und insbesondere Case-Studies. Die Zusammenfassung und einzelnen Vortragsunterlagen geben einen guten Überblick über die aktuellen Entwicklungen. Dan Geer, Initiator von securitymetrics.org, hielt auf dem Symposium ein Tutorial zum Thema Measuring Security. Darin gab er einen umfassender Überblick über das Thema Metriken im Allgemein und in Bezug auf Sicherheit im Besonderen. Ein begrüßenswerter Trend zu mehr Mess- und Vergleichbarkeit in der IT-Sicherheit.

Awareness @ ENISA

Dass die Sensibilisierung von Mitarbeitern und Benutzern – neudeutsch auch „Security Awareness“ genannt – ein wichtiger Bestandteil eines übergreifenden Sicherheitskonzepts sein sollte, ist längst bekannt. Dennoch sind Konzeption und Umsetzung von erfolgreichen Awareness-Maßnahmen ein anspruchsvolles Unterfangen, wie Erfahrungsberichte auf Symposien oder in E-Books zeigen.

Diesem Umstand hat sich jetzt auch die noch relativ junge europäische Sicherheitsbehörde ENISA angenommen und am 10.08.2006 den Leitfaden “A Users' Guide: How to Raise Information Security Awareness“ veröffentlicht. Der Leitfaden enthält zahlreiche Tipps und Hilfestellungen für die Umsetzung eigener Awareness-Kampagnen und richtet sich auch an KMUs, deren Budget für derartige Projekte meist sehr begrenzt ist.

Dynamische Malware-Analyse

Kostenlose Web-Dienste zur Analyse von Viren und anderen verdächtigen Dateien existieren bereits seit einiger Zeit. Viele Antiviren-Hersteller bieten auf Ihren Webseiten entsprechende Online-Schnittstellen an (z.B. norman, virustotal oder jotti). Die Ergebnisse beschränken sich jedoch im Wesentlichen auf die Information, ob die untersuchte Datei mit einem bekannten Virus oder Wurm infiziert ist.

Einen Schritt weiter geht der am 20.09.2006 öffentlich angekündigte Dienst CWsandbox: Entstanden aus einer Diplomarbeit an der Uni Mannheim wurde eine Web-Schnittstelle zum Hochladen verdächtiger Dateien entwickelt. CWsandbox unterzieht diese Datei anschließend einer dynamischen Analyse; die Datei wird in einer kontrollierten Umgebung ausgeführt und beobachtet. CWsandbox dokumentiert für den untersuchten Prozess z.B. die nachgeladenen Systembibliotheken (DLLs), das Starten und Beenden weiterer Prozesse, Verändern oder Lesen von Registry-Einträgen, das Installieren oder Starten von Diensten sowie aktive Netzwerkverbindungen. Das Ergebnis wird dem Benutzer anschließend in Form einer XML-Datei per E-Mail übermittelt – ein echter Mehrwert bei der Analyse verdächtiger Anwendungen.

Wer AN.ONymisiert, wird beschlagnahmt

Im Rahmen aktueller Vorermittlungen der Staatsanwaltschaft Konstanz gegen die Verbreitung von Kinderpornografie wurden Anfang September ca. ein Dutzend IT-Systeme beschlagnahmt, unter denen sich auch Exit-Nodes und Kaskadensysteme der Anonymisierungsdienste TOR und AN.ON befanden, darunter auch ein System des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD). Ein déjà vu – AN.ON wurde am 03.07.2003 schon einmal per Gerichtsbeschluss verpflichtet, Protokollierungsdaten an Strafverfolgungsbehörden herauszugeben, mit längerem Nachspiel.

Der Informationsgewinn über die anonymisierten Dienstnutzer dürfte gering ausfallen, da in Mix-Netzen die Kommunikationsbeziehung nur dann rekonstruiert werden kann, wenn alle Systeme eines vollständigen „Kommunikationspfads“ vorliegen. Inwieweit die Professionalisierung zukünftiger Ermittlungen auch die Recherche bereits verfügbarer Informationen umfassen wird, bleibt abzuwarten.

Als sicher dagegen kann gelten, dass die Fahndungszielgruppe einfach auf ausländische Serverknoten solcher Anonymisierungsnetzwerke ausweichen wird, und dass sicherlich auch keine Backbonerouter von großen ISPs beschlagnahmt werden, die illegalen Inhalt transportieren (genauer: durchleiten und nicht speichern). Die nächste Generation von autonomen Anonymisierungsnetzwerken wird sich wohl ohnehin über Wurm-Mechanismen automatisch verbreiten, sodass der direkte Bezug zwischen Infrastruktur und Betreiber wegfällt – wie aber beschlagnahmt man einen Wurm?

Secorvo News

Secorvo College aktuell

Der Herbst steht bei Secorvo College im Zeichen des Sicherheitsmanagements: Einen umfassenden Einstieg bietet das bewährte Seminar „Information Security Management von A(udit) bis Z(ertifizierung)“ vom 17.-18./20.10.2006. Im November folgt ein ganz besonderes Seminar: Über 3,5 Tage werden vom 06.-09.11.2006 die „Erfolgsfaktoren für IT-Security Management“ beleuchtet. Darin werden die besonderen Anforderungen an Kommunikation, Präsentation, Gruppenmanagement und Führung vertieft und geübt, denen sich IT Security Verantwortliche stellen müssen. Das Seminar wird im Januar fortgesetzt.

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

White Paper Security Management Praxis

Nach dem großen Erfolg seines Secorvo White Papers “BS 7799 – von Best Practice zum Standard“ (über 30.000 Downloads) hat Jörg Völker seine Einführung in das Sicherheitsmanagement nun um eine Case Study ergänzt, in der er an einem konkreten Fall seine Erfahrungen mit dem Aufbau zertifizierter Information Security Management-Systeme dokumentiert. Es ist als Secorvo White Paper Nr. 13 seit dem 24.09.2006 online.

Veranstaltungshinweise

Auszug aus www.veranstaltungen-it-sicherheit.de

Oktober 2006	
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)
November 2006	
06.-09.11.	Erfolgsfaktoren für IT-Security Management (Secorvo College, Karlsruhe)
07.11.	IT Risk Management 2006 (COMPUTAS, Berlin)
14.-16.11.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
20.-25.11.	TISP-Schulung (Secorvo College, Karlsruhe)
26.11.	TISP-Prüfung (Secorvo College, Karlsruhe)
28.-30.11.	Kommunikationsschutz und Datensicherheit (Secorvo College, Karlsruhe)

Fundsachen

Auszug aus www.security-finder.de

Introducing a Free New Self-Service Tool That Runs Comprehensive Security Checks in Minutes, Not Days. Vorstellung des SAP-Tools "Security Optimization Self-Service", das mit dem SAP Solution Manager (ab Version 3.1) kostenfrei mitgeliefert wird. Es erleichtert Überprüfungen der Berechtigungen in einer SAP-Systemlandschaft.

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