secorvo
security consulting

Secorvo Security News

Juli 2007

Editorial: Wiederentdeckung der Langsamkeit

Sten Nadolny war es, der vor fast 25 Jahren – zehn Jahre vor dem ersten WWW-Browser – die Langsamkeit zum deutschen Mega-Trend machte. Zumindest literarisch. In „Die Entdeckung der Langsamkeit" verklärt er sie in der Person des britischen Admirals Sir John Franklin zur entscheidenden Quelle von Zielstrebigkeit und Gründlichkeit, den späteren Erfolgsgaranten des Admirals bei Seegefechten und auf Forschungsreisen. Eine These, die, den Verkaufszahlen (1,7 Mio.) nach zu urteilen, wohl einen Kern der deutschen Seele traf.

Kurz darauf geriet die Welt in den Griff moderner Informations- und Kommunikationstechnik (WWW, E-Mail, SMS). Die Herausforderung der Globalisierung tat ein Übriges: Getrieben von der Furcht, wirtschaftlich den Anschluss zu verlieren, entdeckte Ende der 90er Jahre die Bundesregierung mit mehrjähriger Verspätung das Internet. Nun zählte Schnelligkeit. Um den internationalen Rückstand aufzuholen, wurden Unsummen in eGovernment-Programme gesteckt: allein 1,65 Mrd. € in „BundOnline 2005" (2002).

Langsamkeit ist jedoch geduldig. Nach dem Höhepunkt der Online-Euphorie meldete sie sich als „Entschleunigung" zurück. Ihre Renaissance erreicht nach der systematischen Beruhigung innerstädtischer Verkehrswege und der Erfindung von „Slow Food" nun auch das eGovernment. So wurden im Projekt „Deutschland-Online" seit 2003 ganze zwei von insgesamt 15 Vorhaben umgesetzt. Und über die Nutzung der seit 2002 möglichen elektronischen Steuererklärung mit digitaler Signatur werden lieber keine Zahlen veröffentlicht. Nun hat es auch die Bundesnetzagentur erwischt: Die Umstellung der Wurzel-Schlüssel und -Zertifikate auf die von ihr selbst empfohlenen Schlüssellängen und Hashfunktionen ist längst überfällig. Und für die Prüfung der von der (insolventen) Medizon AG ausgestellten qualifizierten Signaturzertifikate bietet sie neuerdings nicht etwa OCSP an, sondern empfiehlt das „SnailMail Certificate Status Protocol (SCSP)" – ein schriftliches Auskunftsersuchen per Post.

Inhalt

secorvo
security consulting

Security News

Kriminelle Tools

Aller Aufregung zum Trotz (siehe Editorial SSN 10/06) hat der Bundesrat die Änderung des § 202c StGB am 09.07.2007 durchgewunken. Der Wunsch des Gesetzgebers ist nachvollziehbar: Wenn einem Hacker nach gelungener Spurenverwischung schon die Tatdurchführung nicht nachgewiesen werden kann, dann soll wenigstens die Tatvorbereitung strafbar sein. Die publizistische Staubwolke um die Entscheidung ist vor dem Hintergrund der Gegenäußerung der Bundesregierung vom 30.11.2006 auch im Kontext der Anhörung vor dem Rechtsausschuss des Bundestages vom 18.04.2007 und der Empfehlung des Rechtsausschusses vom 23.05.2007 nur eingeschränkt nachzuvollziehen.

Eine Befürchtung bleibt allerdings: Wenn „Scheren im Kopf" zukünftig verhindern, dass Angriffstools weiterhin im Internet veröffentlicht und verbreitet werden, dann lassen sich die Möglichkeiten eines Angreifers weit weniger verlässlich abschätzen.

Versteckspiel im Web

Am 04.06.2007 hat finjan seinen vierteljährlichen Web Security Trends Report für das zweite Quartal 2007 veröffentlicht. Schlüsselfeststellung der Autoren: Durch sogenannten „Evasive Attacks" versuchen Angreifer mit immer ausgefeilteren Methoden der Entdeckung von Schadcode zu entgehen. Wurde Schadsoftware in der Vergangenheit hauptsächlich durch Verschleierung (Obfuscation) im Code versteckt, so finden sich heute ausgefeilte datenbankgestützte Mechanismen, durch die mit Hilfe spezieller Regeln angepasster Schadcode an Besucher infizierter Webseiten ausgeliefert wird. Der Code wird vor der weiteren Verteilung immer wieder verändert, so dass die Erkennbarkeit für herkömmliche Virenschutzlösungen erheblich erschwert wird. Daher gehört die Zukunft zweifellos geeigneten dynamischen Erkennungsverfahren als Ergänzung der derzeitigen signaturbasierten Methoden.

EAL 4+ für Red Hat – ein Plus?

Wieder einmal hat ein Hersteller den dornigen Weg einer Zertifizierung nach Common Criteria (CC) auf sich genommen: Am 07.06.2007 hat Red Hat Enterprise Linux 5 (RHEL) auf IBM-Hardware das begehrte Label „EAL 4+" erhalten. Wie immer lohnt für eine Bewertung dieser Evaluierung ein Blick in die zu Grunde liegenden Dokumente.

Jede CC-Evaluierung basiert auf so genannten „Schutzprofilen" (protection profiles), die auch Anforderungen an die Einsatzumgebung des zu untersuchenden Gegenstands beschreiben. Red Hat hat sein Betriebssystem gleich dreien dieser Profile ausgesetzt: Das schon von etlichen anderen Herstellern verwendete Controlled Access Protection Profile (CAPP) sowie Labeled Security Protection Profile (LSPP) und Role-Based Access Control Protection Profile (RBACPP). Im LSPP findet man Einschränkungen wie „The LSPP provides for a level of protection which is appropriate for an assumed non-hostile and wellmanaged user community", und auch das entsprechende Security Target bewertet die Schutzmechanismen als „appropriate for a controlled environment where attackers only have a low attack potential".

Bleibt die Frage nach der Aussagekraft dieser Evaluierung. Fakt ist, dass durch die Überprüfung die Sicherheit bestimmter Schutzmechanismen nachgewiesen wurde. Dennoch haben die Konfigurationen der evaluierten Gegenstände nicht selten wenig bis gar nichts mit einer realistischen Einsatzumgebung zu tun. Bei RHEL führt beispielsweise schon die Installation einer graphischen Benutzeroberfläche zum virtuellen Erlöschen des Gütesiegels.

Fluggastdatenaffäre

Am 28.06.2007 haben sich EU-Kommission und USA auf ein Fluggastdaten-Abkommen geeinigt – Meilenstein einer seit dem 05.03.2003 andauernden Posse. Seitdem zwingt die USA als Antiterror-Maßnahme ausländische Fluglinien unter Androhung des Entzugs der Landerechte, ihre Passagierdaten dem amerikanischen Zoll zu öffnen. Diese Praxis wurde am 09.10.2003 vom EU-Parlament wegen Verstoßes gegen EU-Datenschutzrecht gestoppt. In einer Einigung vom 16.12.2003 wurde die Zahl der zu übermittelnden Datensätze von 39 auf 34 reduziert und die Speicherdauer von sieben auf 3,5 Jahre gesenkt. Diese Einigung wurde von der EU-Kommission am 14.05.2004 bestätigt. Dagegen zog das EU-Parlament vor den Europäischen Gerichtshof – der die Einigung am 30.05.2006 als rechtswidrig kassierte.

Das Interim-Abkommen vom 16.10.2006 läuft am 31.07.2007 aus. Die Einigung vom 28.06.2007 sieht vor, dass von den 34 Datensätzen nunmehr lediglich 19 übermittelt werden. Allerdings beruht ein großer Teil der Reduktion auf der trickreichen Zusammenfassung von Datensätzen. Dafür wurde die Speicherdauer auf 15 Jahre erhöht.

Click 'n Hack Tools

Am 20.06.2007 wurde vom SANS Internet Storm Center auf das Untergrundprodukt „MPACK" hingewiesen, das für ca. 150 USD erworben werden kann. Dabei handelt es sich um eine hochspezialisierte

Software, die ungenügend gepatchte Clientsysteme mit Internet-Zugang zu Botnetzen für Clickbetrug und Pharming hinzufügt. Dazu werden Webseiten mit einer iframe-Seite präpariert, die beim Aufruf MPACK-Code nachlädt. Die Software unterstützt den Käufer unter anderem mit einer aktuellen Onlinedatenbank und wählt auf den Client zugeschnittene technische Schwachstellen aus (z. B. MS06-071, MS07-017, Buffer Overflows für WinZip, QuickTime etc.), bei Bedarf auch Phishing-Trojaner, Dialer, Backdoors oder Spamfunktionen.

Offenbar gibt es einen Markt für Malware. Damit dürfte die Motivation weiter sinken, effektiven Exploit-Code zu veröffentlichen. Ohne die Meldung gefundener Schwachstellen an die Hersteller wird sich die Bereitstellung von Patches jedoch weiter verzögern. Damit verschwände guter Angriffscode in Untergrund-Tools – „geschützt" vom neuen § 202c StGB (siehe oben).

Populäres Filecarving

Carving ist nicht nur unter Skifahrern sehr beliebt. Auch IT-Forensiker finden immer mehr Gefallen daran: Filecarving-Tools werten Header- und Footer-Informationen aus forensischen Images aus und können anschließend die entsprechenden Dateitypen extrahieren. Dies funktioniert auch dann, wenn kein „regulärer" Zugriff mehr auf die Dateien möglich ist – bspw. weil die Dateien gelöscht wurden oder die Dateizuordnungstabelle (FAT) defekt ist.

Scalpel ist ein solcher hoch-performanter Filecarver, der kostenlos ist und unter Unix/Linux, Windows (ohne Installation) sowie Mac OS X läuft. Scalpel ist eine Weiterentwicklung von Foremost und kann dd-Images direkt lesen, ohne dass diese zuvor gemountet werden müssen. Jedes Image wird dabei doppelt „durchforstet". Die Erkennungsraten sind sehr gut, so dass Scalpel auch regelmäßig von Secorvo in forensischen Analysen eingesetzt wird.

Noch einen Schritt weiter gehen Tools, die das sog. „In Place Carving" beherrschen. Tools wie CarvFS extrahieren die Dateien nicht, die in einem Image gefunden wurden: sie legen symbolische Links an, die direkt auf die entsprechende Stelle im Image verweisen. Diese Technik benötigt deutlich weniger Speicherplatz bei der forensischen Analyse, was sich im GB-Bereich positiv bemerkbar machen kann.

IIS – Bezahlpatch?

Am 05.06.2007 veröffentlichte Microsoft einen Knowledgebase-Artikel, in dem erläutert wurde, wie unter bestimmten Bedingungen die Authentifizierung von IIS 5.0/5.1 ausgehebelt werden kann. Inzwischen wurden diese Details aus dem Beitrag gestrichen; in Blogs und Diskussionsforen wird man jedoch schnell fündig. Nun ist die Veröffentlichung einer neu entdeckten Schwachstelle per se nichts Erwähnenswertes. Eigenartig ist jedoch, dass Details zur Ausnutzung der Schwachstelle fast im Stil einer Anleitung preisgegeben wurden. Und Microsoft liefert weder einen Patch, noch sind in dem Text Workarounds zu finden. Einzige Empfehlung für Betroffene: Ein kostenpflichtiges Upgrade auf IIS 6.0. Da drängt sich der Eindruck auf, dass Microsoft seine Kunden mit eigenwilliger Methode zu einem Serverversionswechsel zwingen will. Tatsächlich gibt es kostenlose Workarounds wie der Einsatz von URLScan, detailliert beschrieben im o. g. Blog.

Awareness in YouTube

Im Stil etwas überzeichnet, aber gut erläutert und inhaltlich zutreffend sensibilisiert ein knapp siebenminütiges, bereits am 15.10.2006 in YouTube veröffentlichtes Video der „American International Group" für die Bedrohung durch Externe, die sich Zugang zum Unternehmen verschaffen. Es wird gezeigt, wie leicht es sein kann, wertvolle Informationen zu gewinnen, wenn die Mitarbeiter auf Unbekannte im eigenen Unternehmen nicht angemessen reagieren. Trotz der etwas schwachen Bildqualität eine gute Ergänzung zum Secorvo-Video „Social Engineering".

Secorvo News

Secorvo College aktuell

Im September 2007 startet College nach der Sommerpause mit dem Seminar „IT-Sicherheit heute" (18.-20.09.2007) – dank reger Nachfrage mit nur noch wenigen freien Plätzen. Und auch für das nächste T.I.S.P.-Seminar (05.-10.11.2007) liegen bereits viele Anmeldungen vor – Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Sichere Software im Trend

Am 28.06.2007 präsentierten Dr. Boris Hemkemeier (Commerzbank) und Tom Schröer (SAP) auf einem Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) vor über 60 Teilnehmern „Goldene Regeln der IT-Sicherheit bei der Beauftragung und Erstellung von Software" – ein Ergebnis des Projekts Secologic (Vortragsunterlagen auf der Webseite der KA-IT-Si). Erst Mitte Juni hatte Secorvo für eine sechsköpfige Delegation von Vertretern unterschiedlicher Ministerien der indischen Regierung das Seminar „Sichere Softwareentwicklung" durchgeführt, erweitert um zwei Praxistage. Die Resonanz zeigt, dass das Thema nicht nur in Deutschland eine hohe Aufmerksamkeit genießt. Nächste Gelegenheit zum Besuch des Seminars: **13.-15.11.2007**.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

August 2007	
03.-05.08.	Defcon 15 (Las Vegas/US)
06.-10.08.	USENIX Security Symposium (Boston/US)
19.-23.08.	Crypto 2007 (IACR, Santa Barbara/US)
28.-29.08.	XCon2007 (Beijing/CN)
September 2007	
10.-13.09.	CHES 2007 (IACR, Wien/AT)
18.-20.09.	IT-Sicherheit heute (Secorvo, Karlsruhe)
24.-26.09.	ESORICS 2007 (TU Dresden, Dresden)
Oktober 2007	
04.-05.10.	3rd European Conference on Computer Network Defense (EC2ND) (Enisa, Heraklion/GR)
09.-12.10.	Public Key Infrastrukturen (Secorvo, Karlsruhe)
16.-19.10.	Information Security Management - von A(udit) bis Z(ertifizierung) (Secorvo, Karlsruhe)

Fundsachen

Auszug aus www.security-finder.de

Dass die Version 2.0 des SSL-Protokolls mehrere Sicherheitsschwachstellen aufweist und man daher nur noch Versionen ab SSL 3.0 einsetzen sollte, gehört fast zum Allgemeinwissen. Doch welche Schwachstellen gibt es eigentlich? In Abschnitt 2 der Analysis of the SSL 3.0 Protocol, die ursprünglich beim USENIX Workshop on Electronic Commerce 1996 veröffentlicht wurde, wird man fündig.

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