secorvo
security consulting

Secorvo Security News

Juli 2010

Makellose Bürger

Für den Staatsphilosophen Thomas Hobbes (1588-1679), aufgewachsen im von Bürgerkriegen geprägten England des 17. Jahrhunderts, legitimiert sich das Gewaltmonopol des Staates aus einem (fiktiven) Gesellschaftsvertrag, mit dem die Bürger alle Macht uneingeschränkt dem Souverän übertragen. Sie gewinnen damit Sicherheit vor äußeren Feinden und ihrer eigenen „wölfischen" Natur – zum Preis eines weitgehenden Verzichts auf freie Entfaltung.

Nun sind wir in den westlichen Industrieländern heute zum Glück weit von bürgerkriegsähnlichen Verhältnissen entfernt – aller organisierten Kriminalität und terroristischen Bedrohungen zum Trotz. Dennoch erfreut sich der Kerngedanke der Hobbes'schen Lehre auch in repräsentativen Demokratien zahlreicher Anhänger. Bürgerliche Freiheiten, wie sie sich in allen Verfassungen der Aufklärung als Abwehrrecht des souveränen Bürgers gegenüber einem übermächtigen Staat finden, werden in wachsendem Umfang Sicherheitsbedürfnissen geopfert – selbst dann, wenn es sich um nachweislich wirkungslose Symbolik handelt: „Nacktscanner" und Internet-Sperren lassen grüßen.

Nun sind innere und äußere Sicherheit zweifellos von hohem Wert – ohne sie können sich weder Freiheit noch Wohlstand entfalten. Man beachte jedoch die Kausalität: Sicherheit dient dem Schutz der freien Entfaltung. Tastet sie deren Substanz an, gefährdet sie das zu schützende Gut – und verfehlt ihren Zweck. Selbstmord ist eben keine angemessene Reaktion auf die Angst vor dem Tod.

Wie weit dieser Werterahmen bereits aus dem Blick geraten ist, zeigt die schamlos zynische Namenswahl der NSA für ein Überwachungsprojekt kritischer Infrastrukturen im Volumen von 100 Mio. US$, das das Wall Street Journal am 08.07.2010 öffentlich machte: „Perfect Citizen". Von der „Anomalie-Erkennung" ist es dann nicht mehr weit bis zu deren präventiver Beseitigung. Noch einfacher ginge es allerdings gleich ganz ohne Bürger.

Inhalt

secorvo
security consulting

Security News

Whitelisting am Ende?

Der Stoßseufzer „Wem kann man eigentlich noch trauen?“ ist leider eben so abgedroschen wie berechtigt. Anfang Februar 2010 wurde auf der Konferenz Black Hat DC demonstriert, dass sich Malware für iPhones sogar über Apples offiziellen App Store verteilen lässt – wie zuvor schon bei Stores anderer Hersteller. Am 17.06.2010 wies Marissa Vicario (Symantec) in ihrem Blog darauf hin, dass über 90% aller Malware-infizierten Webseiten von seriösen Anbietern stammen. Sie wurde am 28.06.2010 vom tschechischen Antiviren-Hersteller Avast bestätigt: Auf eine „Schmuddelkram“-Webseite kämen mittlerweile 99 seriöse Seiten, über die man sich beim Browsen infizieren kann. Dann wurde im offiziellen Download-Bereich für Firefox-Addons am 13.07.2010 die Schadsoftware „Mozilla-Sniffer“ entdeckt. Und schließlich musste Dell am 20.07.2010 Austausch-Motherboards zurückrufen, die ab Werk mit Malware bestückt waren.

Die Häufung derartiger Meldungen legt nahe, dass man sich immer weniger auf vermeintlich zuverlässige Quellen verlassen kann, von denen man Daten, Anwendungen oder Systeme bezieht. Der Whitelisting-Ansatz „Erlaube seriöse Quellen und behandle alle anderen restriktiv“ dürfte mittelfristig ins Leere laufen. Solange noch Zeit ist, sollten sich Unternehmen, die sich darauf stützen, Gedanken über einen Plan B machen.

Microsoft is evil, ...

... so die allgemeine Wahrnehmung, wenn es um die Sicherheit von PCs geht. Eine der wichtigsten Erkenntnisse im „Secunia Half Year Report 2010“ vom 13.07.2010 zeigt, dass diese Wahrnehmung nicht mehr der Realität entspricht: Von den 50 meist installierten Programmen auf PCs sind 24 Programme nicht von Microsoft – und weisen im Untersuchungszeitraum 3,5-mal so viele entdeckte Schwachstellen auf. Berücksichtigt man, dass die Zahl der „Bug-Searcher“ bei Microsoft deutlich höher sein dürfte, könnte das Verhältnis der tatsächlichen Schwachstellen noch größer sein. Diese Entwicklung sollte Anlass sein, auch für Programme von „Drittherstellern“ ein funktionierendes Patch-Management zu etablieren.

Viel Rauch um Skype

Seit dem 07.07.2010 geistern Meldungen durch die Presse, nach denen Sean O'Neil die Skype-Verschlüsselung „geknackt“ habe (siehe z. B. Spiegel Online oder Chip Online). Tatsächlich wurde ein von Skype verwendetes Verschlüsselungsverfahren *aufgedeckt*, auf dessen Geheimhaltung Skype sehr viel Mühe verwendet hat. So enthält der Code der Skype-Clients verschiedene Reverse-Engineering-Gegenmaßnahmen. Durch die Publikation des Codes sind diese *Gegenmaßnahmen* als gebrochen anzusehen.

Eine erste Begutachtung des Quellcodes hat ergeben, dass Skype als Stromchiffre eine Variante von RC4 nutzt – mit dem Ziel einer beabsichtigten Inkompatibilität. Da der Code nun offenliegt, wird sich bald zeigen, ob das modifizierte Verfahren ebenso sicher ist wie RC4, oder ob demnächst Millionen Nutzer unter den Folgen schlechter Kryptographie zu leiden haben werden.

Rückzug von der Signatur?

Der Rat der Europäischen Gemeinschaft hat am 13.07.2010 Vereinfachungen der Richtlinie über das gemeinsame Mehrwertsteuersystem (2006/112/EG) erlassen. Diese betreffen auch die vereinheitlichten Anforderungen an die elektronische Rechnungsstellung. Entscheidend ist die Änderung des Art. 233 Abs. 1, der bislang die Verwendung einer qualifizierten elektronischen Signatur oder die Nutzung des EDI-Verfahrens vorgab. Nun stellt sie dem einzelnen Steuerpflichtigen frei, mit welchen Mitteln er Authentizität, Integrität und Lesbarkeit der Rechnung vom Ausstellungszeitpunkt bis zum Ende der Aufbewahrungsfrist sicherstellt. Auch der Einsatz organisatorischer Kontrollmittel soll zulässig sein, solange eine verlässliche Buchungskontrolle zwischen dem Waren- oder Dienstleistungsbezug und der Rechnung gewährleistet wird. § 14 Abs. 3 UStG, der das Signaturerfordernis im deutschen Recht festschreibt, wird nun bis zum 31.12.2012 angepasst und gelockert werden müssen.

Unternehmen werden diese Entwicklung vermutlich mit Erleichterung zur Kenntnis nehmen. Die Bundesregierung hat die Signaturpflicht des § 14 Abs. 3 UStG ohnehin auf die Streichliste zum Bürokratieabbau gesetzt (dort lfd. Nr. 14) und plant eine Befassung mit der Thematik noch in diesem Jahr. Allerdings geht die Erleichterung auf Kosten der Rechtssicherheit, denn während sie die Mittel freigibt, bleibt die Verpflichtung zur Sicherung von Authentizität und Integrität erhalten. Ob allein organisatorische Maßnahmen hierfür ausreichen, wird für den Gesetzgeber, die Steuerpflichtigen und die Rechtsprechung schwer bestimmbar sein. So wird der Zwang zur ungeliebten Signatur durch ein erhöhtes Eigenrisiko der Unternehmen ersetzt.

CC-BS-Schutzprofil

Schutzprofile ermöglichen für eine definierte Produktkategorie von IT-Systemen eine standardisierte Beschreibung der Bedrohungen, Sicherheitsziele,

Annahmen über die Betriebsumgebung und daraus resultierenden Sicherheitsanforderungen. Sie legen die Mindeststandards für eine Zertifizierung nach den international vereinheitlichten „Common Criteria for Information Technology Security Evaluation“ fest.

Am 24.06.2010 veröffentlichte das BSI ein neues Schutzprofil für moderne verteilte Betriebssysteme. Das „Operating System Protection Profile (OSPP)“ wurde von einem Konsortium bestehend aus BSI, Vertretern des amerikanischen Zertifizierungsschemas (NIAP) und namhaften Betriebssystemherstellern entwickelt. Die aktuelle Version 2.0 der OSPP definiert die Anforderungen an ein sicheres Betriebssystem und fordert die Evaluierungsstufe EAL 4, die nicht nur formale Anforderungen an die Entwicklung stellt, sondern auch die Analyse von Design und Quellcode verlangt.

Dabei bezieht sich ein Schutzprofil wie auch eine CC-Zertifizierung immer auf eine definierte Einsatzumgebung. OSPP setzt voraus, dass die Plattform (Hardware, Geräte, Firmware), auf der das Betriebssystem ausgeführt wird, gegen physische Angriffe und Manipulationen geschützt ist und alle Managementaktivitäten von vertrauenswürdigen und geschulten Anwendern durchgeführt werden. Immerhin: Eine Abkoppelung des PCs vom Netz ist keine Voraussetzung für den sicheren Betrieb.

State of the Crypto-Art

Als Referenz dafür, welche Kryptoalgorithmen und Schlüssellänge dem Stand der Technik entsprechen, wird – zumindest hierzulande – gerne die vom BSI erarbeitete und von der BNetzA jährlich aktualisierte Übersicht über geeignete Algorithmen heran gezogen. Da sie sich auf das Signaturgesetz bezieht, berücksichtigt sie zwar nur Verfahren, die für Signaturen nötig sind. Allerdings lassen sich daraus die Anforderungen an ein entsprechendes Schutzniveau von Verschlüsselungsverfahren ableiten.

Am 16.07.2010 endete die Kommentarfrist für den Draft der NIST Special Publication 800-131, der Empfehlungen für Algorithmen und Schlüssellängen in allen wichtigen Anwendungsgebieten von Verschlüsselung über Signatur und Schlüsselableitung bis zu Message Authentication Codes geben wird. Er fordert für Verfahren der amerikanischen Bundesbehörden ab 2011 ein Sicherheitsniveau von mindestens 112 bit – das Doppelte dessen, was der (einfache) DES bot, und 32 bit mehr als die bis Ende 2010 verlangten 80 bit. An dieser Empfehlung werden auch nationale Standards künftig nicht vorbei kommen, die für sich reklamieren, kryptografisch „State of the Art“ zu sein.

Sichere Virtualisierung

Ein „Guide to Security for Full Virtualization Technologies“ wurde am 07.07.2010 vom NIST in einer Draft-Version veröffentlicht. Auf 35 Seiten werden anschaulich Begriffe und prinzipielle Sicherheitsmaßnahmen beim Einsatz von Server- und Desktop-Virtualisierung beschrieben. Der Guide eignet sich gut für einen systematischen Einstieg in die Thematik; konkrete technische Empfehlungen für bestimmte Virtualisierungslösungen bleibt er allerdings schuldig.

Deadlines

Zahlreiche Konferenzen zur IT-Sicherheit werfen ihre Schatten voraus – und werben noch um Beiträge. Schnell Entschlossene können bis zum **01.08.2010** einen Vorschlag für den 18. DFN Workshop „Sicherheit in vernetzten Systemen“ (15.-16.02.2011) einreichen.

Ebenfalls bis zum **01.08.2010** werden spannende Vorträge für die OWASP-Konferenz Appsec Germany 2010 (20.10.2010) gesucht. Und das Bundesamt für Sicherheit in der Informationstechnik (BSI) freut sich bis zum **10.10.2010** auf Einreichungen für den 12. Deutschen IT-Sicherheitskongress (10.-12.05.2011).

Secorvo News

Secorvo College

Gleich nach Ende der Sommerferien bietet Secorvo College die nächste Gelegenheit zur Zertifizierung als Information Security Professional mit dem TISP-Seminar am **20.–24.09.2010**. Nähere Informationen zu den Zulassungsvoraussetzungen, den Inhalten und der unabhängigen Zertifikatsprüfung finden Sie unter www.tisp.de (Online-Anmeldung).

Alle weiteren Seminarangebote im Oktober und November mit ausführlichem Programm unter http://www.secorvo.de/college

Security Awareness Symposium

Am **28.–29.09.2010** findet das von Secorvo, dem Berliner eLearning-Spezialisten digital spirit und der Karlsruher Agentur DauthKaun initiierte siebte „Security Awareness Symposium“ in Ettlingen statt. Auch diesmal erwartet Sie ein „Erfahrungsfeuerwerk“ von Projektleitern zahlreicher Awareness-Kampagnen, die ihre Ideen, Erfolge und „Lessons Learned“ präsentieren – ein Treffen, das Sie sich nicht entgehen lassen sollten, wenn die Sensibilisierung Ihrer Kollegen für IT-Sicherheit oder Datenschutz auch auf Ihrer Agenda steht (Anmeldung).

Veranstaltungshinweise

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

Juli 2010	
29.07.-01.08.	DEFCON 18 (DEFCON, Las Vegas/US)
August 2010	
02.-04.08.	DFRWS 2010: Digital Forensic Research Workshop (DFRWS, Portland/US)
09.-13.08.	19th USENIX Security Symposium (Washington/US)
15.-19.08.	Crypto 2010 (IACR, Santa Barbara/US)
30.08.	Sommerakademie 2010 (ULD, Kiel)
September 2010	
07.-10.09.	OWASP AppSec US (Irvine/US)
20.-24.09.	TISP-Schulung (Secorvo College)
28.-29.09.	7. Security Awareness Symposium (Secorvo, Ettlingen)
28.-30.09.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)
Oktober 2010	
21.10.	it-sa Datenschutztag 2010 (Computas, Nürnberg)

Fundsache

Grundlegende praktische Regeln für die Informations- und IT-Sicherheit in kleinen und mittelständischen Unternehmen wurden im Interagency Report „Small Business Information Security: The Fundamentals“ (NISTIR 76121) der Computer Security Division des NIST vom Oktober 2009 zusammengefasst – prägnant auf 20 Seiten die wichtigsten Sicherheitsaspekte für Mensch und Technik.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Petra Barzin, Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp

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