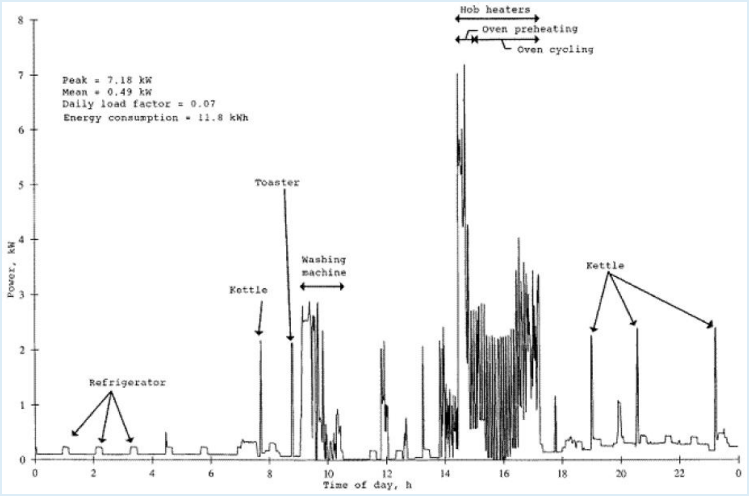
secorvo
security consulting

Secorvo Security News

April 2010

Der Feind in meiner Steckdose

Seit Januar müssen in Neubauten und bei Renovierungen „intelligente Stromzähler" verbaut werden, die Verbrauchswerte elektronisch übermitteln und eine Abrechnung nach wechselnden Tarifen erlauben. Damit sollen den Energieversorgungsunternehmen eine verbrauchsabhängige Energiebereitstellung ermöglicht und durch lastabhängige Tarife das Verbraucherverhalten gesteuert werden. Dass die vermeintlich unkritische Erfassung des Stromverbrauchs in 15'-Intervallen einen erheblichen Eingriff in den vom Bundesverfassungsgericht im Urteil zum „Großen Lauschangriff" vom 03.03.2004 definierten „Kernbereich privater Lebensgestaltung" darstellt, wird erst auf den zweiten Blick deutlich. Abgesehen von einem Gutachten des ULD vom 11.09.2009 und Kapitel 4 eines NIST-Drafts vom 02.02.2010 blieb selbst die fachöffentliche Diskussion weitgehend aus. Das ist, wie die Abbildung zeigt, wohl dringend nachzuholen.



Quelle: Elias Leake Quinn, Smart Metering & Privacy: Existing Law and Competing Policies, Frühjahr 2009, S. 3.

Inhalt

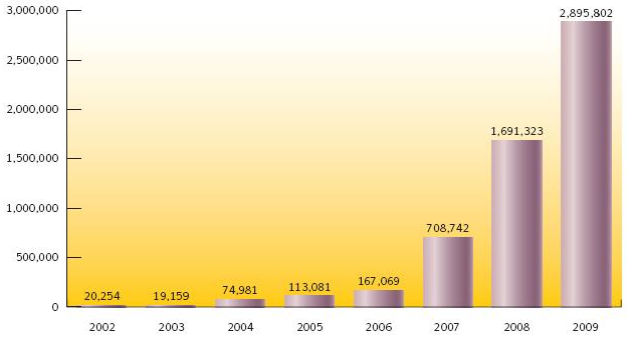
secorvo
security consulting

Security News

Symantec Report

Am 14.04.2010 erschien der immer wieder lesenswerte halbjährliche Internet Security Thread Report von Symantec. Einige der Ergebnisse, die Symantec über 240.000 eigene „Sensoren“ gewinnt, sind auch für Experten überraschend: So stürmten Angriffe mit bösartigen PDF-Dateien die Top-Ten; sie waren für 49% aller Web-basierten Attacken verantwortlich. Daher sollte dem Patchen des Acrobat-Readers eine mindestens ebenso hohe Priorität eingeräumt werden wie den Betriebssystem-Updates.

Während das „Window of Exposure“ trotz zahlreicher kritischer Bugs 2009 bei den meisten Browsern auf unter einen Tag schrumpfte, stieg die Zahl der neue Viren, Würmer und Trojaner 2009 auf durchschnittlich fast 8.000 – je Kalendertag.



Neue Viren, Würmer, Trojaner (Symantec)

Auch der Handel mit ergaunerten „Credentials“ floriert, wenn auch die Preise sinken: Kreditkartendaten gibt es schon ab 0,85 US$, E-Mail-Adressen ab 1,70 US$ je MB und Kontendaten bereits ab 15 US$. Offenbar überwiegt hier das Angebot die Nachfrage (bzw. die Zahl der „nützlichen Idioten“, die ihr Bankkonto für die Geldwäsche hergeben).

Internet zertifiziert

Am 29.04.2010 erfolgte im Rahmen eines Events der Karlsruher IT-Sicherheitsinitiative die offizielle Übergabe des ISO 27001-Zertifikats auf der Basis von IT-Grundschutz an den deutschen Internet-Knoten DE-CIX – mit einem Durchsatz von mehr als 600 GBit/s der größte Knoten Europas und der zweitgrößte weltweit. Gute drei Jahre dauerte das von der Karlsruher Connect GmbH begleitete Projekt von der Idee bis zum von Secorvo durchgeführten erfolgreichen Audit. Die Erfahrungsberichte finden sich auf der Webseite der KA-IT-Si.

Der Aufwand hat sich nach Überzeugung von Arnold Nipper (CTO des DE-CIX) gelohnt: Das Projekt habe konsequente Sicherheitsprozesse und ein durchgängiges, hohes Sicherheitsniveau erzwungen – wichtige Voraussetzung für die Vertrauenswürdigkeit eines Internet-Knotens. Bei der Übergabe scherzte Bernd Kowalski, Abteilungsleiter Zertifizierung beim BSI, daher auch: „Jetzt ist das deutsche Internet Grundschutz-zertifiziert.“

Leitfaden IS-Revision

Am 19.03.2010 wurde vom BSI Version 2.0 des Leitfadens IS-Revision auf Basis von IT-Grundschutz veröffentlicht. Die Vorgehensweise wird umfänglich beschrieben und enthält wenig Überraschendes. Interessant sind die Aufwandschätzungen für eine „Querschnitts-Revision“, die mit 30-60 Personentagen bei normaler und bis zu 60-100 Personentagen bei sehr hoher Komplexität angesetzt werden. Für eine „IS-Kurzrevision“ werden 8-10 Tage geschätzt, eine Methode, um einen ersten definierten Eindruck zum Stand der Informationssicherheit zu erhalten.

Ein als Hilfsmittel zur Verfügung gestelltes Dokument Prüfthemen für die IS-Kurzrevision soll diese Kurzrevision unterstützen. Der Titel „verbindliche Prüfthemen“ klingt vielversprechend; bei genauerer Betrachtung werden aber nur Themen aufgelistet. Wie diese konkret zu prüfen sind, ist nicht geregelt. Lediglich stichpunktartig werden Beispiele angeführt, die einen großen Interpretationsspielraum lassen.

Es bleibt zu hoffen, dass im Rahmen der Überarbeitung der IT-Grundschutzkataloge bei den jeweiligen Maßnahmen auch verbindliche Prüffragen definiert werden, die dann als Grundlage für die Erstellung von Informationssicherheitskonzepten bzw. einer ISO 27001-Zertifizierung auf Basis von IT-Grundschutz sowie für die IT-Revision verwendet werden können.

Diffie + Murphy = Lenin

Gut 33 Jahre ist die Epoche machende Veröffentlichung von Whit Diffie und Marty Hellman zur Public Key Kryptographie inzwischen alt. Und selbst die bekannte und oft genutzte PKI-Bibliothek OpenSSL liegt nach mehr als einem Jahrzehnt Anlauf seit dem 29.03.2010 offiziell in Version 1.0 vor.

Eigentlich ist also alles ganz einfach mit einer PKI, sollte man meinen: CAs als vertrauenswürdige Zertifizierungsinstanzen stellen nach eingehender Prüfung der Antragsteller Zertifikate aus und PKI-Anwendungen nutzen diese Zertifikate, um mit den zugehörigen Schlüsseln alle relevanten Daten zu signieren oder für den beabsichtigten Empfänger zu verschlüsseln. In der Praxis scheint aber immer noch eher Murphys Gesetz zu regieren, wie die folgenden aktuellen Ereignisse zeigen.

Am 02.04.2010 wurde bei einer Kontrolle unter den bei der Mozilla Foundation geführten vertrauenswürdigen Stammzertifikaten ein herrenloses Root-CA-Zertifikat entdeckt. Erst vier Tage später konnte geklärt werden, dass der Schlüssel dieser CA zwar nicht kompromittiert ist, aber weder verwendet noch auditiert wird; daraufhin wurde das Zertifikat – für künftig neu installierte Firefox-Browser – aus der vorgegebenen Stammzertifikatsliste entfernt.

Am 01.04.2010 wurde gemeldet (leider kein Aprilscherz), dass es ausreicht, als Kunde eines Free-Mail- oder Web-Mail-Providers die E-Mail-Adresse „ssladministrator@…“ zu belegen, um hochoffizielle SSL-Zertifikate für Server unter der Domäne des jeweiligen Providers zu beziehen.

Am 13.04.2010 erschien ein Microsoft-Patch für Authenticode, der dafür sorgt, dass jetzt tatsächlich der gesamte in einem Cabinet oder Portable Executable Container enthaltene Code in die Prüfung der Code-Signatur einbezogen wird. Bis dato konnte ein Angreifer diesen Containern Code anfügen, ohne dass deshalb die Signatur des ursprünglichen Herausgebers als ungültig gewertet wurde.

Und ebenfalls am 13.04.2010 wurde ein Bug bestätigt, der dazu führt, dass Thunderbird ausgehende E-Mails u. U. nicht mit dem Zertifikat des adressierten Empfängers, sondern mit einem ganz anderen verschlüsselt.

Auch nach 33 Jahren sollte man es bei der PKI-Nutzung also immer noch mit der (fälschlich) Wladimir Iljitsch Uljanow (vulgo: Lenin) zugeschriebenen Maxime halten: Vertrauen ist gut. Kontrolle ist besser.

OWASP Top 10 – 2010,5

In den SSN 11/2009 haben wir bereits auf die Entwurfsversion der überarbeiteten OWASP Top 10 hingewiesen. Seitdem verstrichen fast sechs Monate intensiven Feinschliffs, bevor am 19.04.2010 die endgültige Version veröffentlicht wurde.

Das 22-seitige Dokument, an dem noch die Reihenfolge einiger Risiken im Tabellenkeller verändert wurde, zeigt anschaulich allen Verantwortlichen und an der Entwicklung von Web-Anwendungen Beteiligten die gravierendsten Risiken auf. Zusätzlich wird das notwendige Handwerkszeug zur Risikoreduzierung vorgestellt. Das halbe Jahr bis zur Veröffentlichung hat geholfen, den Entwurf zu einem rundum gelungenen Arbeitswerkzeug reifen zu lassen.

Secorvo News

Secorvo College aktuell

Die Nachfrage nach dem T.I.S.P.-Zertifikat ist ungebrochen: Schon weit über 300 deutsche Security Professionals dürfen sich mit diesem Titel schmücken, und 2010 werden voraussichtlich weitere 100 Absolventen das Zertifikat erwerben. Freie Plätze gibt es noch auf dem T.I.S.P.-Seminar am **07.–11.06.2010** (mit anschließender Prüfung). Die nächste Gelegenheit zur T.I.S.P.-Zertifizierung bietet Secorvo College nach der Sommerpause vom 20.-25.09.2010.

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

Lesestoff

In der März-Ausgabe der Fachzeitschrift „Datenschutz und Datensicherheit (DuD)“ (Schwerpunktthema „Softwaresicherheit“) hat sich Kai Jendrian ausführlich zur Überprüfung von Webanwendungen mit dem „OWASP Application Security Verification Standard 2009“ geäußert (S. 138-142).

Nachlese

Unser erstes „Security News Symposium“ am 20.-21.04.2010, auf dem wir zahlreiche aktuelle Themen der IT-Sicherheit und des Datenschutzes vertieften, wurde von den Teilnehmern überschwänglich gelobt – nicht nur für das hervorragende Essen. Wer es verpasst hat, kann eine CD mit den Vortragsunterlagen zum Preis von 50 Euro per E-Mail an security-news-symposium@secorvo.de bestellen. Das Essen lässt sich allerdings erst auf dem nächsten Symposium nachholen.

Vorschau

Am **07.–08.06.2010** findet die diesjährige 12. Fachkonferenz „DuD 2010“ in Berlin statt – mit einem spannenden und aktuellen Programm (von Cloud Computing über Elena, Auftragsdatenverarbeitung und den neuen Personalausweis bis zum Intelligenten Stromzähler) und Rekordbeteiligung: Schon jetzt gibt es mehr als 100 Anmeldungen. Wer noch dabei sein möchte, sollte sich zügig anmelden.

Ebenfalls vormerken sollten Sie den **15.07.2010** – den zweiten Karlsruher „Tag der IT-Sicherheit“, der in Kooperation von KA-IT-Si, IHK Karlsruhe und dem Cyberforum e.V. veranstaltet wird. Es erwarten Sie Praxisberichte u. a. zu den Themen Wirtschaftsspionage, iPhone-Sicherheit und Security Awareness.

Veranstaltungshinweise

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

Mai 2010	
04.-05.05.	11. Datenschutzkongress 2010 (EUROFORUM, Berlin)
20.-21.05.	Datenschutzaudit – Best Practice (Secorvo College)
20.-21.05.	International Secure Systems Development Conference (Enabled Security Limited, London/UK)
25.-28.05.	3rd Int. Workshop on Post Quantum Cryptography PQCrypto 2010 (Cased, Darmstadt)
30.05.-03.06.	Eurocrypt 2010 (IACR, Nizza/F)
Juni 2010	
07.-08.06.	DuD 2010 (Computas, Berlin)
07.-11.06.	TISP-Schulung (Secorvo College)
22.-25.06.	Certified Professional for Secure Software Engineering (CPSSE) (Secorvo College)
Juli 2010	
15.07.	2. Karlsruher „Tag der IT-Sicherheit“ (KA-IT-Si/IHK/Cyberforum, IHK Karlsruhe)
24.-29.07.	Black Hat (Las Vegas/US)

Fundsache

Eine ausführliche Auseinandersetzung mit Sicherheits- und Datenschutzaspekten von Smart Metern (= „Intelligenten Stromzählern“) im Smart Grid hat das NIST am 02.02.2010 als zweiten Draft zur Kommentierung veröffentlicht: *Smart Grid Cyber Security Strategy and Requirements* (NIST IR 7628, 305 Seiten).

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch

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