Secorvo Security News
Februar 2003

Dirk Fox
Secorvo Security Consulting GmbH

Nr. 2, 2. Jhrg. 2003
Stand 28. Februar 2003

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

Inhalt

Editorial: Wie die Schildbürger die Signatur regulierten

Für Karl Simrock (1802-1876) wäre es ein gefundenes Fressen gewesen: Die Geschichte der Regulierung der elektronischen Signatur im Deutschland des 21. Jahrhunderts. Sie beginnt 1997 nach dreijähriger Reifung mit dem ersten nationalen Signaturgesetz der Welt, gewissermaßen dem dreieckigen Rathaus. Acht Seiten, ergänzt um eine zehnseitige Signaturverordnung, die alles Wesentliche in knappen Sätzen regeln – ganz untypisch deutsch und weltweit beachtet. Sogar die Verabschiedung eines 300 Seiten starken „Maßnahmenkatalogs“ ließ sich verhindern.

Die erhoffte Initialzündung für die Etablierung elektronischer Abläufe bleibt allerdings aus, denn das definierte Sicherheitsniveau ist so hoch, dass Wirtschaftlichkeit und Praktikabilität in Frage stehen. Zwar gibt es bald erste Zertifizierungsstellen, doch Anwendungen und Nutzer fehlen: Das dreieckige Rathaus hat keine Fenster.

Da kommt Ende 1999 die EU-Richtlinie mit mehr Markt: Statt technischer Festlegungen soll die Haftung der Anbieter hinreichende Sicherheit garantieren – das Dach wird abgedeckt, im Rathaus ist Licht. Nun regnet es aber hinein: Die Investitionen der Zertifizierungsanbieter drohen Makulatur zu werden. Prompt kommt das Dach wieder drauf: Zur fortgeschrittenen und qualifizierten Signatur gesellt sich im neuen Signaturgesetz die „freiwillige Akkreditierung“.

Damit es wieder hell wird, wird nun das Licht in Säcken ins Rathaus getragen: Die GDPdU fordert 2001 die „qualifizierte Signatur mit Anbieterakkreditierung“, das 3. VwVerfÄndG führt 2002 die „qualifizierte Signatur mit Einschränkung“ ein und die aktuelle StDÜV erfindet qualifizierte Zertifikate, die elf der Kriterien nicht erfüllen.

Glücklicherweise gab es im 19. Jahrhundert noch keine digitalen Signaturen. Sonst hätte die Regulierungswirklichkeit Simrocks Schildbürgern womöglich den literarischen Erfolg streitig gemacht.

1 Security News

1.1 Fortsetzungsgeschichte: IE und Windows Patches

Mit einem neuen Sammel-Patch vom 05.02.2003 (Update: 12.02.2003) dichtet Microsoft neu entdeckte, als „critical“ eingestufte Löcher im Internet Explorer, die einem Angreifer die Umgehung des Sicherheitsmodells und damit die Ausführung beliebigen Programmcodes auf der angegriffenen Maschine erlauben. Betroffen sind die Versionen 5.01, 5.5, 6.0 des IE.

http://www.microsoft.com/security/security_bulletins/ms03-004.asp

Der Patch schließt alle Sammel-Patches des Jahres 2002 ein:

http://support.microsoft.com/default.aspx?scid=kb;EN-US;810847

Bereits Ende Januar (22.01.2003) veröffentlichte Microsoft ein Security Update für die Betriebssystemversionen Windows NT 4.0, die Terminal Server Edition, Windows 2000 und Windows XP, das einen als „critical“ eingestuften Fehler im (üblicherweise nur auf Servern aktivierten) Locator-Service behebt:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms03-001.asp

1.2 Steuerdaten-Übermittlungsverordnung, StDÜV

Am 28.01.2003 erließ der Bundesfinanzminister eine „Verordnung zur elektronischen Übermittlung von Steuererklärungen und sonstigen für das Besteuerungsverfahren erforderlichen Daten“ (Steuerdaten-Übermittlungsverordnung – StDÜV). Darin werden die Bedingungen für eine zulässige elektronische Übermittlung von Steuerdaten festgelegt:

http://www.dud.de/dud/documents/stduev-030128.pdf (pdf, 45 kB)

§ 7 StDÜV legt die Anforderungen an die in diesem Zusammenhang benötigten elektronischen Signaturen fest – und schafft damit neben einfachen, fortgeschrittenen, qualifizierten, qualifizierten mit Anbieterakkreditierung und qualifizierten mit Einschränkung eine neue, sechste Klasse von Signaturen, die sich von qualifizierten Signaturen durch den Verzicht auf elf ausgewählte Anforderungen unterscheidet.

1.3 NGSCBFW

„Next-Generation Secure Computing Base for Windows“ heißt seit dem 23.01.2003 die im August 2002 gestartete, bislang unter dem Codenamen „Palladium“ geführte und nicht unumstrittene Sicherheitsarchitektur von Microsoft, die ab 2005 Teil des Windows-Betriebssystems sein soll.

Alle geheimen Passwörter und Schlüssel sollen in einem in einer Hardware-Komponente verankerten Trusted Platform Module (TPM) vor unberechtigtem Zugriff Dritter geschützt werden. Die Ein-/Ausgabe-Kanäle sollen so um Authentifikationsmechanismen erweitert werden, dass kein Programm mehr Ein- oder Ausgaben vortäuschen oder abfangen kann – ein wirksames Handicap für Trojanische Pferde.

http://www.microsoft.com/PressPass/features/2002/jul02/0724palladiumwp.asp

Welchen Preis hinsichtlich Flexibilität und Nutzbarkeit des Systems die Anwender für die unbestrittenen Sicherheitsgewinne zahlen müssen, ist dabei noch eine offene Frage.

1.4 The National Strategy to Secure Cyberspace

Im Februar 2003 veröffentlichte das Weiße Haus die Endfassung der „National Strategy to Secure Cyberspace“, deren Vorfassung am 17.09.2002 (nicht ganz freiwillig) öffentlich zur Diskussion gestellt worden war (siehe Secorvo Security News 4/2002).

http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf (pdf, 980 kB)

Die Strategie verfolgt drei Ziele: den Schutz von Amerikas kritischen Infrastrukturen vor Cyber-Attacken, die Verringerung der Verletzlichkeit und die Minimierung von Schäden und Ausfallzeiten. Sie setzt fünf Prioritäten: Die Entwicklung eines nationalen Security Response Systems, eines Programms zur Verringerung der Verletzlichkeit, eines Awareness- und Trainings-Programms, den Schutz der Regierungsinfrastruktur sowie den Aufbau einer internationalen Sicherheitskooperation.

1.5 PKI-Forum bei OASIS

Das 1999 gegründete PKI-Forum, eine internationale Vereinigung der Anbieter von PKI-Lösungen, wurde am 04.11.2002 in OASIS (Organization for the Advancement of Structured Information Standards) integriert. OASIS ist ein 1993 gegründetes Konsortium von inzwischen mehr als 600 Unternehmen weltweit, das die Entwicklung offener technischer Standards fördert.

http://www.pkiforum.org
http://www.oasis-open.org

Am 07.01.2003 gründete OASIS ein „Technical Committee to Advance PKI Adoption for Secure Transactions“. Ziel dieser Arbeitsgruppe ist die Förderung von Public Key Infrastrukturen durch White Papers, Informationssammlungen und Standardisierungsaktivitäten, die der Lösungsinteroperabilität, der Orientierung am tatsächlichen Business-Bedarf und der Verbreitung digitaler Signaturen und Zertifikate dienen.

http://www.oasis-open.org/committees/pki/

1.6 Vorratsspeicherung

Im Zusammenhang mit dem Angebot von Flatrate-Internetzugängen ist eine Diskussion darüber entbrannt, ob die Speicherung von Verbindungsdaten (dynamische IP-Adresse, Datum, Uhrzeit) über das Ende der Nutzung hinaus zulässig ist, da sie zu Abrechnungszwecken nicht benötigt wird.

Sowohl ein für T-Online erstelltes Gutachten als auch die Datenschutz-Aufsichtsbehörde Darmstadt sind zu dem Ergebnis gekommen, dass eine solche Speicherung zulässig sei (Schreiben vom 14.01.2003):

http://www.dud.de/dud/documents/tdsl-rp-da-030114.pdf (pdf, 124 kB)

Ganz anders die Stellungnahme des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein vom 16.01.2003:

http://www.datenschutzzentrum.de/material/themen/presse/ipspeich.htm

Im gleichen Sinne äußert sich der Hamburgische Datenschutzbeauftragte, Dr. Hans-Hermann Schrader (28.01.2003):

http://fhh.hamburg.de/stadt/Aktuell/weitere-einrichtungen/datenschutzbeauftragter/aktuelles/pressemeldung-2003-01-28-pdf,property=source.pdf (pdf, 56 kB)

1.7 Programm „DuD 2003“

Zum fünften Mal jährt sich die Fachkonferenz „Datenschutz und Datensicherheit“ – **DuD 2003** – am **05.-06.05.2003** in Berlin. Gemeinsam mit den Herausgebern der Fachzeitschrift „DuD“, Johann Bizer, Dirk Fox und Helmut Reimer, bietet der Veranstalter Computas eine zweitägige Konferenz mit Vorträgen namhafter Experten aus Politik, Industrie, Wissenschaft und Verwaltung zu zentralen, aktuellen Themen und (Streit-) Fragen des Datenschutzes und der IT-Sicherheit an.

http://www.computas.de/dud/dud2003.pdf
(pdf, 276 kB)

Diese Tagung erfreut sich jährlich steigender Teilnehmerzahlen und konnte sich als „feste Größe“ unter den deutschen Datenschutz-Veranstaltungen etablieren. Für „Wiederholungsteilnehmer“ winken Staffelpreise – und bei Anmeldung über Secorvo (an info@secorvo.de oder per Fax an 0721/6105-455) zudem zur Feier des Jubiläums ein Crémant-d‘Alsace des Weinguts Raymond Kieffer – jedem Kenner von Computas-Veranstaltungen ein Begriff.

2 Secorvo News

2.1 Secorvo College aktuell

Die sichere Konfiguration der Microsoft-Betriebssysteme gibt es nicht „out of the box“. Erfahrung nutzen bedeutet hier die Sicherheit Ihrer Systeme wirksam zu erhöhen.

Inside Windows Security, Windows 2000 und XP, 25.-26.03.2003

Angriffe auf Rechnersysteme selbst zu erleben und durchzuführen erleichtert die realistische Abschätzung der Gefahren, denen Ihre IT-Systeme ausgesetzt sind.

Defense Lab – Live Hacking, Angriffstechniken, Gegenmaßnahmen, 01.-02.04.2003

2.2 Neu: SSL-Zertifikate der PKI-1-Verwaltung

Das BSI hat den Betrieb der PKI-1-Verwaltung im Januar 2003 um die Ausstellung von SSL-Zertifikaten erweitert. Dazu wurden von Secorvo eine SSL-Studie und ein Umsetzungskonzept erstellt:

http://www.secorvo.de/publikationen/bsi-ssl-studie1.4.zip (pdf/zip, 316 kB)

http://www.secorvo.de/publikationen/bsi-ssl-umsetzungskonzept1.4.pdf (335 kB)

2.3 White Paper „VPN Basis-Interoperabilität“

Seit Ende Januar ist das sechste Secorvo White Paper verfügbar, diesmal zum Thema „VPN Basis-Interoperabilität“. Eine Kurzfassung der Untersuchung, in der das paarweise Zusammenspiel der VPN-Geräte von sechs Herstellern mit einer Basis-Sicherheitskonfiguration untersucht wurde, erschien in der Oktoberausgabe der Zeitschrift iX.

http://www.secorvo.de/whitepapers

3 Veranstaltungshinweise

März 2003	
25.-26.03.	Inside Windows Security (Secorvo College, Karlsruhe)
26.-28.03.	Workshop on Privacy Enhancing Technologies 2003 (TU Dresden)
April 2003	
01.-02.04.	Defense Lab (Secorvo College, Karlsruhe)
08.-09.04.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
13.-17.04.	RSA Conference 2003 (RSA, San Francisco)
Mai 2003	
05.-06.05.	DuD 2003 (Computas, Berlin)
06.-07.05.	Public Key Infrastrukturen (PKI) (Secorvo, Karlsruhe)
08.05.	PKI für Fortgeschrittene (Secorvo, Karlsruhe)
13.-15.05.	BSI-Kongress 2003 (BSI, Bonn)
19.-20.05.	IT Risk Management (ITRM 2003) (Computas, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feedback an
redaktion-security-news@secorvo.de