Secorvo Security News
Mai 2006

Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim Knobloch, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 5, 5. Jhrg. 2006
Stand 22. Mai 2006

ISSN 1613-4311

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

Inhalt

Editorial: Zauberlehrlinge

Seine Wort und Werke merkt ich und den Brauch
und mit Geistesstärke, tu ich Wunder auch.

Sie erinnern sich – es war einmal... Nein, nicht Ihre Deutschstunde, sondern die Diskussion der Entwürfe des deutschen Signaturgesetzes. Zehn Jahre ist es her, dass sich die Hoffnungen des deutschen eCommerce auf die vertrauensbildende Wirkung des 10-seitigen Gesetzestextes richteten. Noch im Evaluierungsbericht schrieb die Bundesregierung dem Signaturgesetz „eine Lokomotivfunktion für den Einsatz und die Verbreitung digitaler Signaturen“ zu.

In der Erwartung von Millionen Signaturzertifikaten wurden seitdem erhebliche Summen in Trust Center investiert, die „elektronische Form“ im BGB verankert und eine eigene Aufsichtsbehörde geschaffen.

Immer neue Güsse bringt er schnell herein,
Ach! und hundert Flüsse stürzen auf mich ein.

Allein: Der erhoffte Durchbruch blieb aus – die Lokomotive zog nicht. Darauf reagierte der Bund mit konfusen neuen Signatur-Kreationen (SSN 02/2003), verstärktem Aktionismus wie dem Signaturbündnis und der Erfindung vermeintlicher Killer-Applikationen wie der elektronischen Steuererklärung Elster (tatsächlich mit SSL realisiert) oder der Konzeptidee Jobcard – ohne Erfolg.

Ein verruchter Besen, der nicht hören will!
Stock, der du gewesen, steh doch wieder still!

Sieben akkreditierte Zertifizierungsdiensteanbieter existierten zu Hochzeiten. Nun stoppte auch die Datev die Ausgabe qualifizierter Zertifikate: Der Nutzen war „schwer zu vermitteln“, die wenigen ausgestellten Zertifikate rechtfertigten die Kosten nicht.

Herr, die Not ist groß!
Die ich rief, die Geister werd ich nun nicht los.

Die Reaktion des Marktes ist unzweideutig: Fortgeschrittene Signaturen genügen in der Praxis fast immer, das Restrisiko wiegt die erforderliche Mehrinvestition in qualifizierte meist nicht auf. Zeit zur Einsicht und zum Umsteuern: Regulatives Beharren wird den Erfolg nicht herbeizwingen – und ist in einer Marktwirtschaft nie eine gute Idee.

"In die Ecke, Besen, Besen! Seids gewesen.“

1 Security News

1.1 Sicherheitsstudie 2006

Seit 1991 wird – gesponsert durch das Department of Trade and Industry (DTI) – alle zwei Jahre eine Studie zu Sicherheitsvorfällen in Großbritannien erstellt (SSN 04/2002). Diese Studien dienen Unternehmen als Informationsquelle und zur Einschätzung des unternehmensrelevanten Risikos.

Der aktuelle, von PwC erstellte „Information Security Breaches Survey 2006“ wurde Ende April veröffentlicht. Obwohl die Zahl betroffener Firmen gegenüber dem Vorjahr gesunken ist, stiegen die Anzahl der insgesamt gemeldeten Sicherheitsvorfälle und der Mittelwert der Schäden (um 20 % auf 12.000 £). Bei „worst-case incidents“, insbesondere in Konzernen, lag der Mittelwert sogar bei 90.000 £. 68 % der befragten Unternehmen erwarten eine Zunahme der Sicherheitsvorfälle.

1.2 DoD-Sicherheitslücken

Wie das Pentagon am 28.04.2006 in einer Stellungnahme einräumte, wurde in ein öffentliches System der vom Militär genutzten Krankenversicherungsanwendung TRICARE eingebrochen. Dabei konnten zahlreiche, auch personenbezogene Daten abgezogen werden. Alle potentiell betroffenen Personen wurden informiert und über die Gefahr aufgeklärt, möglicherweise Opfer eines Identitätsdiebstahls zu werden.

Eine erneute Peinlichkeit, nachdem das Department for Homeland Security im März für ihr Sicherheitsniveau das dritte „failed“ in Folge kassiert hatte (SSN 03/2006). Immerhin kündigte das Department of Defense (DoD) an, weiterte Schutzmaßnahmen zu ergreifen.

1.3 IT-Grundschutz News

Nach den aktuellen BSI-Standards (SSN 01/2006) wurden im April auch die Grundschutzkataloge (Bausteine, Maßnahmen, Gefährdungen) auf den Webseiten des BSI im HTML-Format online gestellt. Die vollständigen Grundschutzkataloge können jetzt auch als ZIP-Datei geladen werden.

Zur Erleichterung der Zuordnung von ISO 27001 und IT-Grundschutz publizierte das BSI Ende April eine tabellarische Gegenüberstellung (19.04.2006). Die umfassende Tabelle stellt zum Einen dar, wie die neue Struktur des IT-Grundschutzhandbuchs die Inhalte der ISO 27001 abdeckt. Zum Anderen erleichtert die Tabelle das Auffinden der jeweils zugehörigen Bausteine und Maßnahmen.

1.4 Codename Secure Blue

Am 10.04.2006 gab IBM die Entwicklung einer „Secure Blue“ genannten Sicherheitsarchitektur bekannt, die die ressourcenaufwändige Ver- und Entschlüsselung von Daten direkt im Prozessor durchführen soll. Ein weiterer konsequenter Baustein des „Trusted Computing“, das das Ziel verfolgt, mehr Sicherheitsfunktionen in manipulationsichere Hardware zu verlagern, um bösartigem Code die Angriffsfläche zu entziehen.

Mit der Ankündigung, „die Sicherheit von Daten in Elektronikprodukten wie Konsumer-Elektronik, Medizintechnik und Digital-Media-Produkten“ zu verbessern, wurde jedoch auch die seit Jahren andauernde Kritik am Trusted Computing wieder lauter, die spekuliert, dass es dabei nur um die Durchsetzung kommerzieller Kopierschutzinteressen im Unterhaltungssektor geht (SSN 02/2003, SSN 04/2003).

Die Qualität von „Secure Blue“ wird sich sicher an dem komplexeren Schlüsselmanagement und der noch immer erforderlichen Entschlüsselung der Daten vor der Nutzung durch den Anwender erweisen.

1.5 GPG-Schutz für E-Mails

Das Open-Source-Projekt GnuPG hat Zuwachs bekommen: Pünktlich zum Linux-Tag wurde vom BSI am 26.04.2006 Version 1.0.1 des Gnu Privacy Guard for Windows (gpg4win) veröffentlicht. Es umfasst

neben Schlüsselmanagement-Tools ein Plugin für Outlook. Die Lösung setzt dabei allerdings auf die Mitwirkung des Anwenders – ein „Auslaufmodell“, denn unsere Erfahrungen haben gezeigt, dass Plugins in Punkto Benutzerakzeptanz weit hinter transparenten Gateway-Lösungen liegen.

Eine attraktive „Mischlösung“ bietet GPG-relay (aktuell Version 0.959): Es sorgt anhand eines konfigurierbaren Regelsatzes als lokaler POP3/IMAP-Proxy zuverlässig für eine transparente Ver- und Entschlüsselung aller ein- und ausgehenden E-Mails – unabhängig vom E-Mail-Client.

1.6 Behörden-Desktop

Im Rahmen des BSI-Projekts ERPOSS – Erprobung des Einsatzes von Open Source Software – wurde von der credativ GmbH ein Desktop auf Basis von Debian GNU/Linux 3.1 (sarge) und KDE 3.3 entwickelt. Seit dem 28.04.2006 steht er zum Download bereit. Der Desktop bietet eine Verschlüsselung des Dateisystems, eine vorkonfigurierte Personal Firewall, einen E-Mail-Client mit Virenschutz und Spamfilter und unterstützt die vom BSI entwickelte Verschlüsselungslösung Ägypten.

1.7 Hase und Igel Reloaded

Nach der iTAN – die inzwischen von zahlreichen Banken zum Schutz des Online-Banking vor Phishing eingeführt wurde – bietet die Postbank ihren Kunden als erste Bank bundesweit die mTAN an. Dafür wirbt sie seit dem 18.04.2006 mit einem TÜV-Gütesiegel, dessen proprietäre Prüfgrundlagen dem Zertifikat zu entnehmen sind.

Beim mTAN-Verfahren erhält der Kunde zu jeder beauftragten Transaktion eine SMS mit einer einmalig gültigen, transaktionsspezifischen TAN. Zusätzlich werden Zielkontonummer und Betrag in der SMS mitgeschickt. Die Sicherheit des Verfahrens ist hoch, wenn die hinterlegte Mobilfunknummer vor Phishing-Tricks gefeit ist.

Während viele Banken die Bedrohung durch Phishing schrittweise reduzieren, spielen die Phisher Hase und Igel und erfinden ständig neue Angriffsmethoden: Inzwischen versuchen sie, Kunden die Telefon-Banking PIN zu entlocken, z.B. über die Aufforderung zur Eingabe der Telefon-PIN auf gefälschten Webseiten.

Auch der Wechsel des Kommunikationsmediums wird zum Ausspähen der persönlichen Informationen genutzt. So gibt es Angriffe, die dazu auffordern, Rufnummern anzurufen, hinter denen sich ein fingiertes Phone-Banking System verbirgt.

Den besten Schutz vor derartigen Angriffen bietet – Technik hin, Technik her – immer noch die Aufmerksamkeit der Nutzer. Denn Banken fordern Kunden grundsätzlich nicht per E-Mail zur Preisgabe vertraulicher Informationen auf. Auch sollte bei E-Mails der Absender überprüft werden – die Postbank versucht dies durch das Signieren von E-Mails zu vereinfachen.

Realistische Hoffnung auf eine Verschnaufpause für Banken und Kunden besteht allerdings nur, wenn es den Banken gelingt, Mechanismen zu etablieren, durch die der Aufwand für Phisher so ansteigt, dass er den Nutzen des Betrugs überwiegt, z.B. aufgrund einer niedrigen Erfolgsquote.

1.8 Zukunftsblick

Am 06.-09.06.2006 wagt die Konferenz „ETRICS 2006“ an der Universität Freiburg einen Blick in die Zukunft der Informations- und Kommunikationssicherheit. Allein 19 international renommierte Keynote-Speaker lassen spannende und erkenntnisreiche Tage erwarten: Professor Acquisti (Carnegie Mellon University) beleuchtet, was der Datenschutz von der Verhaltensökonomie lernen kann, David Gavrock (Intel) gibt Insider-Einblicke in Trusted Computing und Professor Kemmerer (University of California) zieht Lehren aus 30 Jahren Computer Security.

Das gesamte Programm umfasst 70 Vorträge, zahlreiche Workshops, Tutorien und ein attraktives Begleitprogramm – für einen Teilnahmebeitrag von 150 € (Studenten) bis 350 €. Noch sind Anmeldungen möglich.

2 Secorvo News

2.1 Secorvo College aktuell

Dem Hacker über die Schulter schauen – und dann sogar selbst Hand anlegen und live Systeme attackieren: völlig legal und ohne schlechtes Gewissen. Das bietet Ihnen das „Live Hacking Lab“ am **20.-22.06.2006**: Drei Tage, in denen wir Sie in die aktuellen Hacking-Technologien einweihen. Schließlich sollten Sie wissen, was Ihre Gegner können, wenn Sie Ihre IT-Infrastruktur schützen wollen.

Wenn du weder den Feind noch dich selbst kennst,
wirst du in jeder Schlacht unterliegen.
Sunzi, Die Kunst des Krieges (ca. 500 v. Chr.)

2.2 SAS 2006 – Nachlese

Dass Security Awareness bei vielen Unternehmen hoch im Kurs steht, belegt die steigende Teilnehmerzahl des von Secorvo veranstalteten „Security Awareness Symposium“, das in diesem Jahr schon zum vierten Mal die Plattform für einen intensiven Erfahrungsaustausch bot. Die engagierten Praxisberichte lieferten zahlreiche Anregungen, Denkanstöße – und sicherlich auch den einen oder anderen Motivationsschub. Die Unterlagen aller Awareness-Symposien (2003 bis 2006) sind für Interessierte auch auf CD erhältlich.

2.3 Wer haftet?

In Kooperation mit der Neuen Messe Karlsruhe findet das nächste Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am Abend des ersten Messetags der Midvision 2006 statt: Am 21.06.2006 wird Professor Dr. Michael Bartsch von der renommierten (Kanzlei des Jahres 2003/2004 in Baden-Württemberg) und im IT-Recht besonders ausgewiesenen Kanzlei Bartsch und Partner zum Thema „Risiken, Pannen, Schäden – und wer haftet?“ vortragen. Beginn 18 Uhr, anschließend Networking am Büfett (bei Live-Übertragung der Spiele Niederlande-Argentinien und Elfenbeinküste-Serbien/Montenegro auf Großleinwand). Um Anmeldung wird gebeten.

3 Veranstaltungshinweise

Mai 2006	
28.05. - 01.06.	Eurocrypt 2006 (IACR, St. Petersburg/RU)
29.05.	Linux-Sicherheit (eco AK Sicherheit, Frankfurt)
Juni 2006	
06.-09.06.	ETRICS 2006 (GI, Freiburg)
20.-22.06.	Live Hacking Lab (Secorvo College, Karlsruhe)
21.06.	Risiken, Pannen, Schäden (KA-IT-Si, Karlsruher Messe)
21.-22.06.	Midvision 2006 (Karlsruher Messe)
25.-30.06.	18th Annual FIRST Conference (FIRST, Baltimore/USA)
27.-28.06.	Lotus Notes Security (Secorvo College, Karlsruhe)
29.06.	Lotus Notes Security advanced (Secorvo College, Karlsruhe)
Juli 2006	
13.-14.07.	DIMVA 2006 (GI, Berlin)
31.07. - 04.08.	USENIX Security Symposium (USENIX, Vancouver/USA)
August 2006	
02.-03.08.	Black Hat USA 2006 (Black Hat, Las Vegas/USA)
20.-24.08.	Crypto 2006 (IACR, Santa Barbara/USA)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

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