secorvo
security consulting

# Secorvo Security News

**Juni 2007**

## Editorial: Zunehmendes Nichts

*Wenn Du entdeckst, dass Du ein totes Pferd reitest, steig ab. (Weisheit der Dakota-Indianer)*

Zehn Jahre ist es her, dass das deutsche Signaturgesetz im Rahmen des „Informations- und Kommunikationsdienste-Gesetzes" das Licht der Welt erblickte. Seitdem flossen Steuergelder in mehrstelliger Millionenhöhe und erhebliche Investitionen der Industrie in gesetzeskonforme CA-Infrastrukturen und eGovernment-Anwendungen. Mit bitterem Ergebnis: Bis heute ist keine Massenanwendung in Sicht, die die Ausgaben rechtfertigen würde; sogar Elster kommt ohne qualifizierte Signaturen aus. Doch es wird methodisch weitergeritten:

*Strategie 1: Richte eine unabhängige Behörde für das Hüten toter Pferde ein.*

Die Bundesnetzagentur wurde 1997 mit dem Betrieb der Wurzel-CA und der Aufsicht über die Einhaltung des Gesetzes beauftragt.

*Strategie 2: Schirre mehrere tote Pferde zusammen, damit sie schneller werden.*

Am 13.12.1999 verabschiedete die EU eine „Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen", an die das deutsche Signaturgesetz am 16.05.2001 angepasst wurde.

*Strategie 3: Bilde eine Task Force, um das tote Pferd wiederzubeleben.*

Am 03.04.2003 gründeten „Staat und Wirtschaft" auf Initiative von BMWi und BMI das „Bündnis für elektronische Signaturen". (Die „SigBü"-ChipKarte gibt es bis heute nicht, und unter „Aktuelles" findet man genau einen Eintrag - vom 28.03.2006.)

*Strategie 4: Stelle Vergleiche unterschiedlicher toter Pferde an.*

Derzeit lässt die EU die Anwendung elektronischer Signaturen in den Mitgliedsstaaten evaluieren. Erst im Oktober 2003 war eine Studie für die EU-Kommission zu ernüchternden Einsichten gelangt. Diesmal wurde ein anderes Autorenteam beauftragt...

*Strategie 5: Wetten, dass das Vieh nur simuliert?!*

Zum zehnten Geburtstag tröstet der Jahresbericht 2006 der Bundesnetzagentur optimistisch: „Damit steht auch dem (...) elektronischen Geschäftsverkehr zunehmend nichts mehr im Wege."

## Inhalt

secorvo
security consulting

# Security News

## Unterschriften gegen SPAM

Im Mai 2007 wurde von der IETF die RFC 4871 im Standards Track veröffentlicht. Hierbei handelt es sich um eine Spezifikation des DKIM-Ansatzes, an dessen Entwicklung Mitarbeiter namhafter Firmen wie Sendmail Inc., Yahoo, PGP und Cisco beteiligt waren. Die Motivation für DKIM wurde in RFC 4686 dokumentiert. Zur Sicherstellung der Identität von Absendern sollen E-Mails digital unterschrieben werden. Zur Überprüfung sind keine aufwändigen PKI-Infrastrukturen erforderlich, denn die öffentlichen Schlüssel werden über DNS-Mechanismen verteilt. Die Vorteile des Verfahrens liegen im geringen Aufwand für die Implementierung. Leider existieren zur Zeit nur wenige Lösungen, daher setzen bisher auch nur wenige Organisationen DKIM produktiv ein. Zur erfolgreichen Verbreitung von DKIM ist eine breite Akzeptanz erforderlich.

Derzeit ist noch nicht abzusehen, ob dieser Ansatz, auf den wir einige Hoffnung setzen, sich durchsetzen wird. Wir werden ihn weiterhin aktiv beobachten. Interessante Einblicke in aktuelle Anti-SPAM-Anätze bieten auch die Ergebnisse der ENISA.

## Baustein Datenschutz

Seit dem 01.06.2007 gibt es einen neuen Baustein zum Datenschutz in den IT-Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Dieser Baustein wurde von den Datenschutzbeauftragten des Bundes und der Länder und den Aufsichtsbehörden der Länder für den nicht-öffentlichen Bereich unter Federführung von Claus Simon, Referatsleiter Technik beim Landesbeauftragten für Datenschutz und Informationsfreiheit des Saarlandes erarbeitet.

Insbesondere die tabellarische Zuordnung der Grundschutzmaßnahmen zu den technisch-organisatorischen Schutzzielen in der Anlage zum § 9 BDSG am Schluss des 65seitigen Dokuments sind höchst wertvoll für die Praxis. Nach entsprechender redaktioneller Überarbeitung wird er auch auf den Webseiten des BSI zum Abruf bereitgestellt.

## Totgeglaubte leben länger

Auch wenn die Welt einige Zeit warten musste – die letzte Ausgabe von Phrack erschien am 16.01. 2004 – ist nun eine neue Ausgabe des wohl ältesten Online-Magazins der Hacker-Community erschienen: Phrack #64 ist seit dem 26.05.2007 online. Das neue Redaktionsteam, "The Circle of Lost Hackers", hat einige spannende Artikel beispielsweise zu Kernel Exploiting und aktuellen Möglichkeiten zum Blind TCP Hijacking zusammen gestellt.

## SSL-Zertifikate in XXL

Zum Erhalt eines offiziellen SSL-Zertifikats der bekannten Trustcenter benötigt man nicht mehr als die E-Mail-Adresse, unter der die Internet-Domain des Webservers registriert wurde – und ca. 100 Euro für die Begleichung der Jahresgebühr. Um diesem Umstand abzuhelfen, der z. B. Phishern in die Hände spielt, wurden „Extended Validation" (EV) Zertifikate aus der Taufe gehoben, für die man amtliche Dokumente wie einen Handelsregisterauszug vorweisen muss. Ergänzend färbt Microsoft im neuesten Internet Explorer den Adressbalken grün, wenn der SSL-Server ein EV-Zertifikat vorweist.

Allerdings sind die etwa zehnfachen Kosten für ein EV-Zertifikat eine Investition in eine ungewisse Zukunft: So lange nicht (fast) alle anderen legitimen Webserver ebenfalls EV-Zertifikate verwenden oder gar – wie am 29.05.2007 auf der von Microsoft gesponserten „Sicher im Netz"-Seite geschehen – trotz EV-Zertifikat den Nutzern ein Zertifikatsfehler serviert wird, kann EV den Phishern herzlich egal sein. Zudem hat eine Usability-Studie von Microsoft und der Stanford University vom 15.02.2007 ergeben, dass untrainierte Anwender die grüne EV-Anzeige nicht einmal wahrnehmen – nach Lektüre der Hilfe-Seiten hingegen neigen sie dazu, ihren gesunden Menschenverstand abzuschalten und allen Webseiten zu vertrauen, vor denen nicht explizit gewarnt wird.

## Dicke Fische

Vor der vietnamesischen Küste sind Dieben Ende März 2007 ziemlich dicke Fische ins Netz gegangen. Das staatliche e-Newspaper VietNamNet berichtete am 07.05.2007, dass Teile des optischen Kabels, über welches die Internet-Anbindung von Vietnam realisiert ist, von Unbekannten gestohlen wurden. Bis zur Reparatur des Schadens ist Vietnam jetzt nur noch über ein einziges Kabel erreichbar.

Das Beispiel zeigt, dass Risiko- und Bedrohungsanalysen regelmäßig aktualisiert werden müssen: War Diebstahl zum Zeitpunkt der Verlegung des Seekabels (1993-1995) kein realistisches Bedrohungsszenario, so haben sich seitdem (Schwarz-) Markt und technische Möglichkeiten der Angreifer erheblich entwickelt.

## Neue Richtlinien

Im Juni sind gleich drei Entwurfsversionen interessanter Sonderveröffentlichungen des NIST erschienen. Alle drei Richtlinien können bis Juli kommentiert werden. Dabei handelt es sich um einen User's

Guide to Securing External Devices for Telework and Remote Access, die Guidelines on Securing Public Web Servers und einen Guide for Assessing the Security Controls in Federal Information Systems, die wertvolle Anregungen auch für Sicherheitsorganisationen außerhalb amerikanischer Regierungsinstitutionen enthalten.

### Top Ten aktualisiert

Beim Lesen der aktuellen, gründlich überarbeiteten OWASP Top Ten Liste 2007, einer der wichtigsten aktuellen Übersichten über schwerwiegende Schwachstellen in Web-Applikationen, können sich durchaus unangenehme Gefühle einstellen. Mit der am 12.05.2007 veröffentlichten Zusammenstellung hat die OWASP-Gruppe das etablierte Referenzdokument an aktuelle Gegebenheiten angepasst und noch einmal deutlich verbessern können.

### Softwarehaftung

Auf dem 10. Deutschen IT-Sicherheitskongress des Bundesamts für Sicherheit in der Informationstechnik (BSI) vom 22.-24.05.2007 wurde von Dr. Thomas Ramsauer (BSI) im Rahmen seines Vortrags „Verantwortungsverteilung und Anreizstruktur im Bereich der IT-Sicherheit“ die zwischenzeitlich erschienene Auftragsstudie mit dem Titel „Rechtsentwicklung in der IT-Sicherheit“ von Prof. Dr. Gerald Spindler angekündigt. Die Studie setzt sich auf über 300 Seiten mit der rechtspolitischen Frage auseinander, inwieweit das nationale Recht mit seinen Steuerungsinstrumenten in der Lage ist, den Risiken der Informationstechnik Rechnung zu tragen. Damit soll der steigenden Anzahl an Meldungen über Sicherheitslücken in Softwareprogrammen, neue Viren, Würmer und Trojaner Rechnung getragen werden, die die Frage aufwerfen, wie Pflichten, Verantwortlichkeit und Haftung derjenigen nach geltendem Recht aussehen, die an Herstellung, Einsatz und Nutzung von IT-Produkten beteiligt sind.

Die Studie läutet einen neuen Abschnitt der Diskussion um sichere Software(entwicklung) und die Haftbarkeit im deutschen Rechtsraum ein und liefert Impulse dafür, die Handlungsnotwendigkeit mit dem Geldbeutel des Managements zu verknüpfen.

## Secorvo News

### Secorvo College aktuell

Das (noch junge) Qualifikationszertifikat T.I.S.P. hat seinen Siegeszug angetreten: Die Nachfrage nach T.I.S.P.-Seminaren ist so groß, dass die akkreditierten Anbieter Zusatzseminare auflegen. Bis Ende 2007 wird die Zahl der Absolventen voraussichtlich die Schwelle von 200 überschreiten – und nähert sich damit rapide der Zahl der seit 1989 angebotenen (ISC)²-Abschlüsse (CISSP, CAP und SSCP) in Deutschland: Im Mai 2007 waren es gerade einmal 477. Secorvo College führt vom 25.-30.06. ein T.I.S.P.-Seminar durch; auch für den Termin vom 05.-10.11.2007 gibt es bereits zahlreiche Buchungen – lassen auch Sie Ihre Qualifikation zertifizieren (Online-Anmeldung).

### Whitepaper “PKI-Policy”

Im aktuellen Secorvo White Paper vom 06.06.2007 fassen Petra Barzin und Stefan Kelm die Erfahrungen von Secorvo mit Policy-Rahmenwerken für PKIs zusammen. Das Whitepaper gibt eine strukturierte Einführung in drei zentralen Dokumente Certificate Policy (CP), Certification Practice Statement (CPS) und PKI Disclosure Statement (PDS). Der Schwerpunkt liegt auf der Darstellung des jeweiligen Zwecks und Inhalts und gibt Hilfestellung bei der Wahl der geeigneten Policy-Dokumente.

### Security Awareness Symposium

Vom 12. bis 13.06.2007 fand das fünfte „Security Awareness Symposium“ mit knapp 60 Teilnehmern aus Wirtschaft und öffentlicher Verwaltung statt. Die präsentierten Kampagnen und Erfahrungen von BSI, Carl Zeiss, European Investment Bank, FIDUCIA, M. Dumont Schauberg und e.on Ruhrgas zeigten, dass die Sensibilisierung der Mitarbeiter für Informationssicherheit inzwischen in vielen Unternehmen zum festen Bestandteil der Sicherheitsstrategie geworden ist. Dabei hat sich gezeigt, dass vor allem die Gewinnung und Einbindung des Managements von entscheidender Bedeutung für den Erfolg einer Kampagne ist. Die Dokumentation des Symposiums (sowie aller vorausgegangenen) kann online bestellt werden.

### Software ist sicher …

… und die Erde eine Scheibe. Am **28.06.2007** (18 Uhr) werden Dr. Boris Hemkemeier (Commerzbank AG) und Tom Schröer (SAP AG) im Karlsruher Schlosshotel im Rahmen eines Events der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) die Ergebnisse des vom BMWi geförderten Projekts „Secologic“ vorstellen. In dessen Rahmen wurden u. a. Goldene Regeln für Auftraggeber entwickelt, die helfen sollen, die Zahl sicherheitsrelevanter Fehler in Software systematisch zu reduzieren. Für ein spannendes Net(t)working wird nicht nur das Ambiente sorgen – auch die zahlreichen Anmeldungen lassen interessante Diskussionen und Gespräche erwarten. Online-Anmeldung über http://www.ka-it-si.de.

## Veranstaltungshinweise

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

| | |
|---|---|
| **Juni 2007** | |
| 25.-29.06. | T.I.S.P. Schulung (Secorvo, Karlsruhe) |
| 28.06. | Software ist fehlerfrei. Und die Erde eine Scheibe. (KA-IT-Si, Karlsruhe) |
| 30.06. | T.I.S.P. Zertifikatsprüfung (Secorvo, Karlsruhe) |
| **Juli 2007** | |
| 12.-13.07. | DIMVA 2007 (GI, Luzern/CH) |
| 28.07.-02.08. | Black Hat USA 2007 (Las Vegas/US) |
| **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** | |
| 18.-20.09. | IT-Sicherheit heute (Secorvo, Karlsruhe) |

## Fundsache

Auszug aus www.security-finder.de

Mitteilung der EU-Kommission zu den Vorteilen von Technologien zum Schutz der Privatsphäre. Die Mitteilung enthält die diesbezüglichen Ziele der Kommission, die durch eine Reihe gezielter Maßnahmen zur Förderung der Entwicklung solcher Technologien und ihrer Verwendung durch die für die Datenverarbeitung Verantwortlichen und die Verbraucher erreicht werden sollen.


## Impressum

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

ISSN 1613-4311

Redaktion: Petra Barzin, Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch, Kai Jendrian, 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