secorvo
security consulting

Secorvo Security News

Juni 2011

Editorial: Sieg der Vernunft

Das Schlimmste ist, dass wir die einfachsten Fragen mit Tricks zu lösen versuchen, darum machen wir sie auch so kompliziert. *Anton Tschechow (1860-1904)*

Manchmal kommt die Vernunft auf ganz leisen Sohlen. Diesmal versteckt sie sich im Steuervereinfachungsgesetz 2011, das am 09.06.2011 vom Bundestag verabschiedet wurde. Darin wird § 14 Abs. 1 des Umsatzsteuergesetzes geändert – und damit GDPdU und deutsches Signaturgesetz (SigG) zugleich „geschleift".

Aber der Reihe nach. Seit dem Inkrafttreten des „Gesetzes über Rahmenbedingungen für elektronische Signaturen" im Jahr 2001 mangelte es nicht an Versuchen, der qualifizierten Signatur zum Durchbruch zu verhelfen. So führte der Gesetzgeber nicht nur die „elektronische Form" im Bürgerlichen Gesetzbuch (BGB) ein, sondern schob auf der Suche nach einer „Killer-Applikation" zahlreiche Initiativen an, darunter – um die prominentesten zu nennen – die elektronische Steuererklärung mit Signatur (ELSTER), das ELENA-Verfahren, den neuen Personalausweis (nPA) mit Signierfunktion und zuletzt das am 03.05.2011 in Kraft getretene De-Mail-Gesetz.

Jedoch signierte nur eine verschwindend geringe Zahl an Bürgern die elektronische Steuererklärung, ELENA wurde gestoppt und für die Signierfunktion des nPA gibt es auch acht Monate nach Einführung kein Trustcenter, das die Nachladefunktion für Signaturzertifikate unterstützt. Daher waren die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen" (GDPdU) vom 16.07.2001 die letzte Bastion: Milliarden elektronischer Rechnungen von TK-Unternehmen, Fluggesellschaften und Online-Shops mussten qualifiziert signiert und vom Empfänger geprüft und protokolliert werden.

Ab dem 01.07.2011 ist das Geschichte. Zwar darf weiterhin signiert werden. Eine Übermittlung per E-Mail ohne Signatur genügt jedoch für den Vorsteuerabzug. Trauern dürften darüber nur externe „GDPdU-Prozessdesigner" – Unternehmer und Steuerberater hingegen werden die FAQ des Finanzministeriums mit ungläubigem Staunen lesen: So viel Bürokratieabbau war selten.

Inhalt

Editorial: Sieg der Vernunft

Security News

Key Escrow 2.0

Web 2.0

Alchemie 2.0

EnWG 2.0

Forensik 2.0

C++ 2.0

Secorvo News

TISP und mehr

3. Tag der IT-Sicherheit

Leseprobe

Veranstaltungshinweise

Fundsache

Security News

Key Escrow 2.0

Nachdem im März 2011 unbekannten Hackern ein Einbruch bei RSA gelang (siehe SSN 03/2011), hat der SecurID-Hersteller am 06.06.2011 seinen Kunden angeboten, alle One-Time-Password-Token auszutauschen. Dieser Schritt wird allgemein als ein Eingeständnis interpretiert, dass bei dem Einbruch tatsächlich die Seed-Werte vieler oder aller Token entwendet wurden – die Masterkeys, die es erlauben, alle von den Token angezeigten Einmalpasswörter nachzuberechnen.

Auch die Seed-Werte der neuen Token wird RSA archivieren, wenn auch vermutlich besser abgesichert. Da stellt sich die Frage, warum Anwender diese Art von Schlüsselhinterlegung („Seed Escrow") so ohne weiteres akzeptieren sollten. Schließlich käme auch niemand auf die Idee, beim Ausstellen eines SSL-Zertifikats den privaten Schlüssel des betreffenden Webservers dem Trustcenter zum Archivieren zu überlassen, nur für den Fall, dass er dem Besitzer verloren ginge – oder eine Kopie des Fahrzeugschlüssels dem Autohändler oder des Haustürschlüssels dem Makler. Die Hinterlegung großer Mengen sensibler Schlüssel war noch nie ein gutes Konzept, sondern ein meist unnötiger „Single Point of Failure".

Web 2.0

Das KG Berlin hat am 29.4.2011 über die Beschwerde wegen der Ablehnung einer einstweiligen Verfügung gegen einen Wettbewerber entschieden, der den „Gefällt-mir-Button" von Facebook nutzt. Einen abmahnungsfähigen Verstoß gegen eine Marktverhaltensvorschrift nach § 4 Nr. 11 UWG wegen fehlender Information über die Datenübermittlung (§ 13 Abs. 1 TMG) lehnte das Gericht ab.

Für Telemedienanbieter, die Social Plugins nutzen, stellt das Urteil dennoch keine Entwarnung dar: Es klammert die datenschutzrechtliche Bewertung der Fragen, wer verantwortliche Stelle beim Einsatz von Social Plugins ist, ob der Verwender ohne diesbezügliche Datenschutzerklärung seine Informationspflicht verletzt oder ob eine unerlaubte Datenübermittlung ohne Einwilligung vorliegt, gänzlich aus. Eine diesbezügliche Stellungnahme des „Düsseldorfer Kreises" dürfte nicht lange auf sich warten lassen – vom Vorliegen einer bußgeldbewehrten Ordnungswidrigkeit ist weiterhin auszugehen.

Alchemie 2.0

In den letzten Wochen überschlagen sich die Meldungen über Bitcoin, eine elektronische Währung, die ohne eine zentrale Ausgabestelle auskommt – jeder Teilnehmer kann als „Miner" neue „Münzen" erschaffen, wenn er Rechenzeit investiert, um bestimmte Krypto-Aufgaben zu lösen. Bitcoins können wie Bargeld anonym übertragen werden, da alle Teilnehmer nur unter Pseudonym bekannt sind. Dabei kontrollieren und beglaubigen in einem Peer-to-Peer-Verfahren andere Teilnehmer die Weitergabe und verhindern, dass digitale Münzen mehrfach ausgegeben werden.

Das Verfahren ist umstritten – die Bewertungen reichen von einem faszinierenden Stück Kryptographie oder einer finanztechnischen Revolution über Geldwäschemechanismus bis zur Unterstellung eines Ponzi-Schneeball-Systems. Jedenfalls werden Bitcoins bereits in Dollar oder Euro gewechselt, es wurden schon Razzien (23.05.2011) und echte oder vorgebliche Diebstähle (13.06.2011) gemeldet und erste Trojaner stehlen entweder Rechenzeit zum „Mining" oder gleich die ganze Bitcoin-Brieftasche. Seit dem 20.05.2011 gibt es überdies eine Javascript-Version, mit der Webseitenbetreiber ihre Besucher als Bitcoin-Miner für sich arbeiten lassen können.

Zwar sind Zweifel am Erfolg dieser Goldsuche des 21. Jahrhunderts angebracht – allerdings könnte Bitcoin das eine oder andere rätselhafte Verschwinden von Rechenleistung plausibel erklären.

EnWG 2.0

Am 06.06.2011 legte die Bundesregierung einen Entwurf zur Novellierung des Energiewirtschaftsgesetzes (EnWG) vor. Eine wesentliche Neuerung ist die Präzisierung des „Smart Meter"-Begriffs als „eine in ein Kommunikationsnetz eingebundene Messeinrichtung". Während es bislang laut EnWG ausschließlich um die Verbrauchsanzeige ging, werden die Kommunikationsschnittstelle und deren Nutzung nun Standard. Über die tatsächlich übertragenen Daten sagt das noch nichts aus – jedoch ist zu befürchten, dass dies zu Stromprodukten führen wird, die mit der Übertragung personenbeziehbarer Verbrauchswerte im 15-Minuten-Takt einhergehen.

In ihren Stellungnahmen plädieren sowohl der BfDI (zum Schutzprofil) als auch das ULD (zur EnWG-Novelle) für eine Lösung, die Datensparsamkeit bereits im Entwurf berücksichtigt. Die Tarifierung sollte im Haushalt vorgenommen und auch bei lastabhängigen Tarifen sollten nur aggregierte Daten übermittelt werden.

Immerhin ist in § 40 (5) verankert, dass „Lieferanten [...] stets mindestens einen Tarif anzubieten [haben], für den die Datenaufzeichnung und –übermittlung auf die Mitteilung der [...] verbrauchten

Gesamtstrommenge begrenzt bleibt". Wenigstens könnte sich Datensparsamkeit als Unterscheidungsmerkmal etablieren – dann würde möglicherweise schon ein Anbieter mit einem attraktiven Stromprodukt („Datenschutztarif") genügen, um datensparsame Tarifmodelle durchzusetzen.

Forensik 2.0

Die seit Anfang Juni 2011 im Betatest befindliche Public Preview 2 von EnCase Forensic Version 7 weist lange erwartete Verbesserungen auf. Neben einer klareren Strukturierung der Oberfläche sticht besonders der neue „Evidence Processor" hervor, der nun vor dem Beginn der inhaltlichen Analyse eine Reihe von derzeit neun Standardaufgaben (darunter eine Dateisignatur-Analyse und die Indexierung) konfigurierbar abarbeitet – für eine beliebige Anzahl forensischer Images. Erste Tests haben gezeigt, dass die Arbeitsabläufe deutlich komfortabler und schneller werden, solange man über ausreichend dimensionierte Hardware für den Evidence Processor verfügt.

In einer zehnten Standardaufgabe (Kategorie „Modules") kann z. B. der File Carver für bestimmte Datentypen eingestellt werden. Noch ist offen, ob dieser Bereich durch Endkunden selbst erweitert werden kann, wie dies z. B. bei EnScript der Fall ist. Falls Erweiterungen bspw. für CAD-Daten benötigt werden, wird man sonst wohl auf EnCase 8 warten oder auf ein forensisches „Schweizer Offiziersmesser" wie X-Ways Forensics ausweichen müssen.

Einen Schritt weiter geht Simson L. Garfinkel mit seinem bulk_extractor V 1.0.0 vom 15.06.2011, der als Stream-basierter Ansatz mit Named Entity Recognition fast in Echtzeit große Datenmengen unterschiedlicher Formate (wie Bilder, Diskimages oder Dateien) nach Zielbegriffen wie z. B. Kreditkartendaten durchsucht. Solche Carving-Ansätze dürften zukünftig maßgeblich die Erfolgschancen einer IT-Forensik-Software bestimmen.

C++ 2.0

Im Juni 2011 hat Michael Howard (Microsoft) eine Übersicht über gefährliche C und C++ Funktionen im Microsoft Developer Network (MSDN) veröffentlicht. Dieser Auszug aus Kapitel 11 seines mit Steve Lipner verfassten und bereits am 31.05.2006 erschienenen Buch The Security Development Lifecyle ist als konkrete Handreichung für Software-Entwickler gedacht. In dem kurzen Artikel findet sich eine Übersicht über potenziell gefährliche Funktionen – und Empfehlungen für sichere Alternativen. Diese Übersicht sollte über jedem Entwicklerschreibtisch hängen.

Secorvo News

TISP und mehr

Mit Blick auf die steigenden Anmeldezahlen möchten wir Sie schon jetzt auf die nächste T.I.S.P.-Schulung vom 17.-22.10.2011 (einschließlich Prüfung) hinweisen. Nutzen Sie die Gelegenheit, Ihre Kenntnisse zu erweitern, und lassen Sie sich Ihr Wissen zertifizieren.

Nach den Sommerferien startet Secorvo College zunächst mit dem Seminar „Sicherheitsmanagement heute" vom 27.-29.09.2011. Es folgen die Seminare „Verlässliche Web-Anwendungs-Sicherheit" (05.-06.10.2011), „IT-Sicherheitsaudit in der Praxis" (10.-12.10.2011) und „Datenschutzaudit: Best Practice" (13.-14.10.2011). Alle Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

3. Tag der IT-Sicherheit

Gemeinsam mit dem CyberForum e.V. und der IHK Karlsruhe veranstaltet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 14.07.2011 den „3. Tag der IT-Sicherheit" im Saal Baden der IHK Karlsruhe (Beginn: 14 Uhr, Teilnahmebeitrag 75 Euro).

Der Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Michael Hange, wird in seiner Keynote einen Ausblick auf die Bedrohungslage und die Arbeit des BSI in Deutschland geben. Außerdem erwarten Sie praxisnahe Beiträge zum elektronischen Personalausweis, De-Mail, Web-Angriffen und der Sicherheit im Online-Banking.

Im Anschluss lädt die KA-IT-Si anlässlich ihres 10-jährigen Bestehens zum Jubiläumsempfang. Bitte melden Sie sich rechtzeitig an, damit wir ausreichende Mengen Sekt kalt stellen... Nähere Informationen zum Programm und zur Online-Anmeldung finden Sie unter www.ka-it-si.de.

Leseprobe

Die Fachzeitschrift „Datenschutz und Datensicherheit" (DuD) erscheint bereits im 35. Jahr und seit knapp 15 Jahren unter der Mitwirkung von Dirk Fox als Herausgeber. Dank des wachsenden Interesses am Thema und der Erweiterung des Herausgeberteams um die Juristen Prof. Dr. Benedikt Buchner und Dr. Britta Alexandra Mester im Jahr 2009 wuchs der Umfang des Jahrgangs 2010 auf über 860 Seiten.

Von der Ausgabe 6/2011 ist nun eine digitale Leseprobe verfügbar. Auch ein kostenloses Probeabonnement wird angeboten – wer schnell ordert, erhält noch die Ausgabe 8/2011 mit dem Schwerpunkt „Smart Grids".

Veranstaltungshinweise

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

Juli 2011	
14.07.	3. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum und KA-IT-Si, Karlsruhe)
30.07.-02.08.	Blackhat USA 2011 (Blackhat, Las Vegas/US)
August 2011	
01.-03.08.	DFRWS 2011 (DFRWS, New Orleans/US)
04.-07.08.	DEFCON 19 (DEFCON, Las Vegas/US)
10.-12.08.	20th USENIX Security Symposium (Usenix, San Francisco/US)
14.-18.08.	Crypto 2011 (IACR, Santa Barbara/US)
September 2011	
19.-23.09.	OWASP Global AppSec North America (OWASP Foundation, Minneapolis/US)
27.-29.09.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
Oktober 2011	
17.-22.10.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)

Fundsache

Am 14.06.2011 hat das PCI Security Standards Council als Ergänzung zum PCI Data Security Standard das Dokument PCI DSS Virtualization Guidelines in der Version 2.0 veröffentlicht. In der 39seitigen Übersicht werden auf einem recht hohen Abstraktionsniveau Sicherheitsaspekte von Virtualisierung und Cloud Computing vorgestellt – für Nicht-Techniker ein lesenswerter Leitfaden.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Klaus J. Müller, 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