secorvo
security consulting

Secorvo Security News

Mai 2011

So schlau als wie zuvor

Wenn mein Gedächtnis nicht trügt, begann alles in den frühen 90er Jahren mit dem ISO-9000-Hype – einem Qualitätssiegel, das häufig eher das Vorhandensein einer bürokratisch-peniblen Dokumentation belegt als die materielle Qualität des Produkts. Heute sind Zertifikate so allgegenwärtig, dass uns bei einem Produkt ohne Zertifikat schnell das Gefühl beschleicht, dass damit etwas nicht stimmt.

Meist ist es einer von zwei Gründen, der dem Brancheneinzug eines Zertifikats den Weg ebnet: der Wunsch (oft eines neuen „Marktbegleiters“), sich von seinen Mitbewerbern abzusetzen – oder die Hoffnung, nach einem Skandal verlorenes Vertrauen zurückzugewinnen. Wenige Jahre später ist in der Regel die gesamte Branche zertifiziert – und das Gütesiegel zur „conditio sine qua non“ geworden.

Was für die zertifizierende Stelle (und ihren Umsatz) gut ist, ist jedoch nicht notwendig gut für einen Käufer. Denn die Aussagekraft eines Zertifikats hängt von zahlreichen – häufig nicht einmal öffentlich zugänglichen – Kriterien ab: in erster Linie von dem gewählten Prüfschema (was wird geprüft?), dann von der Prüftiefe (wie intensiv wird geprüft?), vom Prüfumfang (welche Aspekte werden geprüft?), dem Prüfzeitpunkt (wurde das fertige Produkt oder bereits in der Konzeptions- und Entwicklungsphase geprüft?), und nicht zuletzt auch von Qualifikation und Sorgfalt der Prüfer. Zwar mag man von der Prüfung eines unabhängigen Dritten grundsätzlich erwarten, dass sich mindestens in der Vorbereitung darauf Qualitätsverbesserungen einstellen – eine Garantie gibt es jedoch nicht dafür.

So bleibt auch nach einem Blick in den Zertifizierungsbericht des TÜV TrustIT Austria zum IE9 eher Ratlosigkeit zurück. Schützt das Zertifikat beim Surfen vor Malware – oder vor Programmierfehlern im IE9? Wem das alles zu unspezifisch ist, sollte den Browser lieber anhand objektiver Kriterien wählen – zum Beispiel nach ihrem Stromverbrauch: das ist zeitgemäß, politisch korrekt und jederzeit überprüfbar. Zum Beispiel mit einem neuen Smart Meter.

Inhalt

Security News

BGH zum Accountmissbrauch

Am 11.05.2011 hat sich der BGH in einem Grundsatzurteil zur Haftung von ebay-Nutzern geäußert. Der Ehemann der Beklagten hatte ein Niedrigpreisangebot unter dem Account seiner Frau auf der Auktionsplattform ebay eingestellt, das diese vor Auktionsablauf zurückzog. Der zuletzt Höchstbietende hatte sie daraufhin auf Schadensersatz wegen entgangenen Gewinns verklagt.

Der BGH hat auf diese Konstellation das herkömmliche Stellvertreterrecht angewendet und eine Anscheinsvollmacht verneint: Danach kommt es ohne nachträgliche Billigung durch die Accountinhaberin nicht zum Vertragsschluss. Aus den bislang nur als Pressemitteilung verfügbaren Ausführungen zur Bindungswirkung der ebay-AGBs, die die Haftung des Account-Anbieters für Handlungen Dritter festschreiben, geht hervor, dass der BGH eine Geltung für Rechtsverhältnisse zwischen den Plattformnutzern verneint. Das hat Konsequenzen für Plattformbetreiber. Wenn sie sich weiterhin – wie ebay – aus den auf ihrer Plattform geschlossenen Geschäften heraushalten wollen, wird es für sie schwierig, Vertragsbedingungen zwischen ihren Nutzern wie den Umgang mit dem Account-Passwort durchzusetzen. Damit steht für Käufer und Verkäufer gegebenenfalls die Rechtsverbindlichkeit der Kaufverträge in Frage.

3544, 3653, 5072

Falls am 08.06.2011 Internetanbieter wie Google, Facebook & Co. nicht wie gewohnt erreichbar sein sollten, dann ist das vermutlich keinem DoS-Angriff geschuldet, sondern dem von der ISOC ausgerufenen World IPv6 Day. An diesem Tag wird getestet, zu welchen Effekten es führt, wenn das Internet im Parallelbetrieb von IPv4 und IPv6 läuft. Auch Anwender, die nur das herkömmliche IPv4 einsetzen, könnten durch die IPv6-Adressauflösung in die Irre geführt werden, wenn Netzwerkfunktionen ungenügend oder fehlerhaft implementiert sind. Testen kann man das vorab über Webseiten wie z. B. test-ipv6.com – leider meist mit viel JavaScript.

Der Test ist ein guter Anlass, zu überprüfen, wieviel unbeabsichtigte IPv6-Konnektivität im eigenen Netz besteht: In den meisten neueren Betriebssystemen ist IPv6 standardmäßig aktiviert. Zudem kann IPv6-Datenverkehr in IPv4-Paketen getunnelt u. U. Firewalls (auch eingehend!) aushebeln, die ausgehende Verbindungen nicht rigide kontrollieren. Man achte auf die drei im Titel genannten Zahlen: Das sind die UDP/TCP-Ports, die die Tunneling-Verfahren Teredo, TSP bzw. AYIYA nutzen.

EnWG-Novelle

Am 11.05.2011 hat die Bundesregierung einen Entwurf zur Novellierung des Energiewirtschaftsgesetzes (EnWGÄndG) vorgelegt. Er enthält u. a. umfassende Ergänzungen zu Smart Metern sowie diesbezügliche Datenschutzregelungen.

In § 21 Abs. 1 werden ausschließliche Zwecke für die Nutzung der durch Smart Meter gewonnenen Daten und in Abs. 2 die zum Datenumgang berechtigten Stellen festgelegt. Dabei wird der Terminus „Datenumgang“ eingeführt, der zukünftig die „Erhebung, Verarbeitung und Nutzung“ personenbezogener Daten bereichern soll. Ein überflüssiger Abs. 3 ermöglicht explizit die Auftragsdatenverarbeitung.

In § 21e werden umfassender als bisher die Anforderungen an Smart Meter aufgegriffen. Im Wesentlichen beschränkt sich der Entwurf jedoch auf einen Verweis auf eine zu erlassende Rechtsverordnung nach § 21i, die Forderung nach Verschlüsselung bei Versendung über offene Netze und den Hinweis auf den Stand der Technik.

Nach Abs. 5 dürfen Messsysteme, die vor Inkrafttreten der Neuerungen verbaut wurden, bis zum Ablauf der Eichgültigkeit (mindestens bis 31.12. 2013) verwendet werden: Damit liegt die Höchstgrenze für „Alt“-Geräte bei acht Jahren. Die Pflicht zum Einbau von Smart Metern nach § 21c Abs. 1, beschränkt auf Neubauten und größere Renovierungen, kann bei Feststellung der wirtschaftlichen Vertretbarkeit durch das Bundeswirtschaftministerium allgemein vorgeschrieben werden.

Substantielle Änderungen wie die von den Datenschutzbeauftragten der Länder geforderte Gestaltungsvorgabe, die Daten so weit wie möglich lokal und unter Kontrolle des Endnutzers zu verarbeiten, wurden jedoch nicht umgesetzt. Mit § 14a werden zudem von außen unterbrech- und steuerbare Verbrauchseinrichtungen eingeführt. Insgesamt gehen die Neuregelungen nicht weit über das bereits im BDSG Geregelte hinaus und verlieren sich teilweise in Details. Hinsichtlich der Sicherheitsanforderungen an Smart Meter werden nun mit Spannung die Endfassung des Protection Profiles des BSI sowie die zugehörige Rechtsverordnung erwartet.

Man-in-the-Middle XXS

Schon am 08.12.2010 präsentierte Vasco einen Chip in einer Folie, der über die „echten“ Kontaktflächen einer SIM-Karte geklebt wird, um unabhängig vom jeweiligen Netzbetreiber Sicherheitsfunktionen für das Online-Banking per Handy zu ergänzen.

Genau wie viele andere Sicherheitslösungen ist das Konzept eine Dual Use-Technologie: Man stelle sich vor, dass eine derartige Folie über den Kontakten eines Geldautomaten klebt, um diesen mit „Zusatzfunktionen“ anzureichern. Das wäre noch eleganter als das in der vorigen Ausgabe der SSN vorgestellte Chipkarten-Skimming-Gerät, das in den Schlitz des Kartenlesers passt. Es wird daher immer wichtiger, dass Chipkarten-Anwendungen auch gegen einen Man-between-Card-and-Reader-Angriff gefeit sind.

Zensus 2011 – aber sicher!

Derzeit wird zum Stichtag 09.05.2011 in Deutschland wieder gezählt. Im Rahmen des Zensus 2011 werden in Form einer repräsentativen Stichprobe Informationen über die Bevölkerung in Deutschland erhoben. Dem Schutz der erhobenen Daten widmet das Statistische Bundesamt auf der Zensus-Webseite einen ganzen Abschnitt. Darin bleiben allerdings Fragen offen: Wie steht es insbesondere um die Transportsicherheit bei der Befragung?

In der öffentlichen Berichterstattung entsteht der Eindruck, die Beantwortung der Fragen müsse in Form eines Interviews durchgeführt werden – in diesem Fall hinge die Sicherheit der persönlichen Daten stark vom Erhebungsbeauftragten ab. Dubiose Aufrufe zur Meldung als Erhebungsbeauftragte, wie der der sächsischen NPD, geben Anlass, die Vertrauenswürdigkeit der Interviewer zumindest kritisch zu hinterfragen.

Etwas versteckt findet sich auf der offiziellen Webseite zum Zensus ein Hinweis auf alternative Möglichkeiten zur Meldung der Daten: Online oder durch Postversand an die Meldestelle. Aber auch dabei ist Vorsicht geboten: In drei Bundesländern wurden externe Dienstleister mit der Beleglesung beauftragt. Bei Versand empfiehlt sich daher eine Prüfung der Rücksendeadresse auf dem Fragebogen.

Auch die Online-Meldung ist nicht ohne Risiken. Im Blog von Jan Schejbal finden sich Angriffsbeschreibungen, und auch das Statistische Bundesamt und das Bundesamt für Sicherheit in der Informationstechnik halten Sicherheitshinweise zur Online-Meldung für erforderlich.

Die deutliche Fokussierung auf die Interview-Erhebung könnte sich mit den Aufwandsentschädigungen für Erhebungsbeauftragte erklären: Jeder analog ausgefüllte Fragebogen wird zusätzlich mit 7,50 Euro entlohnt.

Bei der Meldung der Daten ist also Sorgfalt angeraten. Dann sollten auch Erfahrungen ausbleiben, die Volkszähler der TAZ Berlinern und clevere Betrüger auf der Suche nach Kontodaten Münchner Bürgern bescherten.

Secorvo News

Einblick in die Forensik

Kurz vor der Sommerpause bietet Ihnen Secorvo College mit dem Seminar Forensik – Verfahren, Tools, Praxiserfahrung vom 28.-30.06.2011 einen praxisorientierten Einblick in die Computer-Forensik. Hier erleben Sie in realitätsnahen Übungen, worauf es bei IT-forensicher Arbeit ankommt.

Im September startet Secorvo College mit dem Seminar **Sicherheitsmanagement heute** vom 27.-29.09.2011 in den Herbst. 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). Zudem bieten wir Ihnen vom 17.-22.10.2011 die nächste Gelegenheit zur T.I.S.P.-Zertifizierung. Alle Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Was nix koscht, isch au nix

„Sicherheit für umsonst“ lautet der Titel des kommenden Events der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 09.06.2011, bei dem Astaro-Technikvorstand Markus Hennig seine Erfahrungen und Einschätzungen zur Frage "Sicherheit durch OpenSource?!" vorstellen wird. Beginn ist um 18 Uhr im Schlosshotel Karlsruhe. Im Anschluss an den Vortrag gibt es wie gewohnt die Gelegenheit zum „Buffet-Networking“. Wir freuen uns auf Ihre Anmeldung.

3. Tag der IT-Sicherheit

Am 14.07.2011 findet zum dritten Mal der von der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) gemeinsam mit der IHK Karlsruhe und dem CyberForum e.V. veranstaltete „Tag der IT-Sicherheit“ statt.

Der Präsident des Bundesamtes fuer Sicherheit in der Informationstechnik (BSI), Michael Hange, wird in einer Keynote einen Ausblick auf die Bedrohungslage und die Arbeit des BSI in Deutschland geben. Außerdem erwarten Sie Praxisbeiträge zum elektronischen Personalausweis, De-Mail, Web-Angriffen und der Sicherheit im Online-Banking. Die Veranstaltung beginnt um 14 Uhr im Saal Baden der IHK.

Direkt im Anschluss lädt die KA-IT-Si zum Jubiläumsempfang anlässlich ihres 10jährigen Bestehens. Das vollständige Programm und die Online-Anmeldung finden Sie unter www.karlsruhe.ihk.de.

Veranstaltungshinweise

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

Juni 2011	
06.-07.06.	DuD 2011 (Computas, Berlin)
06.-11.06.	OWASP Global AppSec Europe (OWASP, Dublin/IE)
09.06.	Sicherheit für umsonst (KA-IT-Si, Karlsruhe)
28.-30.06.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)
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	
04.-07.08.	DEFCON 19 (DEFCON, Las Vegas/US)
14.-18.08.	Crypto 2011 (IACR, Santa Barbara/US)
September 2011	
20.-21.09.	8. Security Awareness Symposium (Secorvo, Karlsruhe-Ettlingen)

Fundsache

Am 27.04.2011 veröffentlichte das BSI ein Eckpunktepapier zu Sicherheitsempfehlungen für Cloud-Computing-Anbieter. Das 76seitige Dokument ist übersichtlich strukturiert und enthält – von einzelnen Skurrilitäten wie der Liste von Vorfällen im Kapitel Notfallmanagement abgesehen – viele wertvolle Hinweise. Eine Antwort auf die wichtige Frage, wie eine datenschutzkonforme Auftragsdatenverarbeitung in der Cloud funktionieren kann, bleibt es allerdings schuldig.

Impressum

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

ISSN 1613-4311

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

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