secorvo
security consulting

Secorvo Security News

März 2010

Innovationsklima

Erfolgreiche Innovationen sind das Lebenselixier eines an Rohstoffen armes Landes. Kein Wunder, dass mit Initiativen wie „Land der Ideen“ oder „Partner für Innovation“ der Erfindergeist beschworen und mit Innovationsindikatoren die Innovationsfähigkeit gemessen wird. Viel wichtiger als die Höhe der Investitionen in Bildung, Forschung und Entwicklung oder die Zahl der Patentanmeldungen ist in der Praxis aber eine andere Frage: Woran lässt sich erkennen, dass aus einer Innovation ein erfolgreiches Produkt wird? Diese Frage stellen sich täglich unzählige Manager, Unternehmer, Analysten und Investoren. Meist liegen sie mit ihren Einschätzungen daneben: Obwohl nur ein Bruchteil aller Ideen Produktreife erlangt, liegt deren „Floprate“ bei 70-90%.

Viel Geld ließe sich sparen, gelänge es, die Trefferquote zu erhöhen. Die Geschichte zeigt jedoch, dass das nicht so einfach ist. „Das Telefon hat zu viele ernsthaft zu bedenkende Mängel für ein Kommunikationsmittel. Das Gerät ist von Natur aus von keinem Wert für uns“, hieß es 1876 in einer internen Meldung von Western Union. „Ich denke, es gibt weltweit einen Markt für vielleicht fünf Computer“, prognostizierte 1943 Thomas Watson, Vorsitzender von IBM. Und Ken Olson, Präsident von DEC, stellte 1977 fest: „Es gibt keinen Grund, warum irgend jemand einen Computer in seinem Haus wollen würde.“ Selbst Bill Gates lag daneben, als er 1981 konstatierte: „640 Kilobyte sind genug für jeden.“

Einfacher ist es, mit der Prognose bis zum kommerziellen Durchbruch der Innovation zu warten. So muss wohl auch Spam, Bot-Netzen, Zero Day Exploits und neuerdings Banking Trojanern wie insbesondere ZeuS der Status einer erfolgreichen Innovation zugebilligt werden. Offenbar herrscht im Bereich der Internetkriminalität ein äußerst fruchtbares Innovationsklima – ganz ohne F&E-Förderung und Innovationsindikatoren. Das sollte zu denken geben. Hoffen wir, dass es Auszeichnungen wie dem Deutschen IT-Sicherheitspreis gelingt, den Tüftlergeist der „White Hats“ zu beleben.

Inhalt

secorvo
security consulting

Security News

Fog Computing

Cloud Computing ist derzeit in aller Munde. Google, Amazon und Co. vermieten überschüssige Kapazität kostengünstig oder gar umsonst als virtualisierte Dienste. Mit der Frage, was dabei aus Sicherheitssicht zu beachten ist, beschäftigen sich u. a. der Report „Cloud Computing Security Risk Assessment“ der ENISA (Fundsache in SSN 11/09), die am 01.03.2010 erschienenen „Top Threats to Cloud Computing“ der gerade einmal ein Jahr alten Cloud Security Alliance und der seit 14.03.2010 elektronisch verfügbare Forschungsartikel „A 'cloud-free' security model for cloud computing“ von Manal Yunis.

Beim genaueren Hinschauen bestehen die Handlungsempfehlungen überwiegend darin, dass der Wolkenmieter seine Hausaufgaben machen sollte: Risikobewertung, Security Management und insbesondere umfangreiche Überwachung und Revision dessen, was da in der Cloud vor sich geht. Und wie immer beim Outsourcing sollte man sich vergegenwärtigen, dass die Verantwortung zur Kontrolle - ernst genommen - den eingesparten Betriebsaufwand zumindest relativiert.

Allerdings wird der Kunde beim standardisierten Angebot eines großen Cloud Computing Providers im Gegensatz zum herkömmlichen Outsourcing deutlich schlechtere Karten haben, ein individuelles Service Level Agreement mit weitreichenden Einblicks- und Kontrollmöglichkeiten auszuhandeln – Cloud Computing wird damit zum Fog Computing.

Werden in der Wolke personenbezogene Daten verarbeitet, entstehen damit auch Risiken für Dritte – schön zusammengefasst in dem Bericht „Privacy in the Cloud“ von Robert Gellmann vom 23.02.2009.

In Deutschland ist eine solche Verarbeitung schnell rechtswidrig, denn die erst im vergangenen Jahr präzisierten Anforderungen des § 11 BDSG zur Auftragsdatenverarbeitung stellen strikte Bedingungen an die Zulässigkeit einer Verarbeitung durch Dritte. Vor Vertragsabschluss ist daher besondere Sorgfalt geboten, denn die Verantwortung für den Schutz der durch Dritte verarbeiteten personenbezogenen Daten verbleibt nach BDSG beim Auftraggeber.

ISMS-Hilfe

Mit dem am 01.02.2010 veröffentlichten und nun auch erhältlichen Standard ISO/IEC 27003: 2010 „Informations technology - Security techniques – Information security management system implementation guidance" hat das JTC 1/SC 27 eine konkrete Implementierungshilfe für ein Informationssicherheitsmanagement nach ISO/IEC 27001: 2005 entwickelt.

Auf 68 Seiten werden in dem Standard Empfehlungen zur Anwendung des ISO/IEC 27001:2005 und zum Aufbau eines ISMS gegeben sowie einige unklare Anforderungen präzisiert. Wer einen einfach zu befolgenden Fahrplan zum ISMS-Aufbau erwartet hat, wird von dem Dokument enttäuscht. Einem erfahrenen Sicherheitsverantwortlichen wird das Dokument in der Praxis allerdings für das eine oder andere Detail eine echte Arbeitshilfe sein.

Ladegerät mit Trojaner

Nachrichten über Trojaner sind leider inzwischen nichts Besonderes mehr. Die Meldung des US CERT vom 02.03.2010, dass ein USB-Batterieladegerät mit einem Trojaner ausgeliefert wurde, zeigt jedoch, dass immer kreativere Wege zur Verbreitung schädlicher Software gewählt werden.

Daher sollte grundsätzlich auch Software aus vermeintlich vertrauenswürdiger Quelle mit gesunder Skepsis begegnet und diese vor einer Installation überprüft werden.

Digitale Wahlen

Im März 2010 führte die International Association for Cryptologic Research (IACR) einen Probelauf für digitale Wahlen durch. Lange Zeit gab es Vorbehalte gegen diese Form der Wahl, nicht zuletzt, weil dies als Werbung für ein bestimmtes Produkt missverstanden werden könnte. Aus Gründen der Benutzerbequemlichkeit entschloss man sich jedoch, digitale Wahlen auszuprobieren – in einer nicht bindenden Probeabstimmung fand das Verfahren große Zustimmung.

Da mittlerweile immer öfter digitale Wahlen zu allen denkbaren Anlässen durchgeführt werden, scheint die Zeit möglicherweise reif dafür zu sein. Die von der IACR genutzte Technologie Helios beruht auf einem Konzept, das von Ben Adida als Dissertation am MIT unter der Betreuung von Ron Rivest entwickelt wurde. Es handelt sich um ein Wahlsystem, bei dem die Stimme anonym abgegeben wird (die Wähler selbst sind nicht anonym und müssen aber zuvor registriert sein), und bei dem jeder Wähler im Nachhinein (wie bei Bingo Voting, SSN 3/2009) verifizieren kann, ob seine Stimme gezählt wurde. Die HeliosSoftware ist quelloffen. Wem Download und Installation zu kompliziert sind, kann seine Wahl auch im Web organisieren: Heliosvoting bietet dazu eine virtuelle Wahlkabine mit virtuellen Stimmzetteln. Sobald alle Wahlberechtigten registriert sind, steht einer Abstimmung nichts mehr im Wege.

secorvo
security consulting

Ach wie gut, dass niemand ...

Dass Kontrollfragen wie die nach dem Mädchennamen der Mutter nicht nur im spanischen Sprachraum eine einfache Hintertür für gut gesicherte Zugänge sind, sollte sich herumgesprochen haben, als im US-Wahlkampf persönliche E-Mails von Sarah Palin publiziert wurden. Das Problem: Durch persönliche Kontakte oder sogar Internet-Recherchen sind die richtigen Antworten auf derartige Fragen oft leicht herauszufinden.

Forscher aus Cambridge und Edinburgh haben nun den Blickwinkel gewechselt: Ein Angreifer könnte im Stil der Rasterfahndung bei allen Anwendern z. B. auf die Frage nach dem Vornamen des Lieblingslehrers einfach eine Handvoll der geläufigsten Namen ausprobieren. Ihrer am 04.03.2010 veröffentlichten Studie zufolge ist die zu erwartende Trefferquote erschreckend hoch. Neben Tabellen, denen man u. a. den beliebtesten weiblichen Vornamen in den USA der 60er Jahre (Lisa) entnehmen kann, enthält das Papier einen Vorschlag für ein passendes Komplexitätsmaß und eine Literaturliste, die gute Argumente für den sicheren Einsatz resp. Verzicht bestimmter Kontrollfragen liefert.

SSL am Ende?

Die Sicherheit einer SSL/TLS-Verbindung steht und fällt mit der Vertrauenswürdigkeit des Server-Zertifikats. Soweit die Theorie. In der Praxis ist die jedoch gar nicht so einfach zu überprüfen: Viele der mehr als 250 von verbreiteten Browsern anerkannten Zertifizierungsstellen wurden inzwischen übernommen oder haben umfirmiert: Aus Baltimore wurde Cybertrust wurde Verizon, aus SecureTrust und XRamp wurde TrustWave – die alten Zertifikate haben jedoch noch bis zu 30 Jahre Gültigkeit. Wie vertrauenswürdig ist da das zugehörige CA-Zertifikat? Ist auf die Identitätsverifikation der Zertifizierungsstelle noch Verlass? Warnt der Browser, wenn eine oft besuchte Webseite ein neues Zertifikat von einer anderen Zertifizierungsstelle erhält?

Am 24.03.2010 stellten Christopher Soghoian und Sid Stamm in ihrem Papier „Certified Lies“ eine neue Angriffsklasse vor: Stellt eine CA z. B. einer Strafverfolgungsbehörde oder einem Nachrichtendienst ein „Intermediate CA“-Zertifikat aus, lassen sich gefälschte Zertifikate erzeugen und damit „man-in-the-middle“-Abhörangriffe durchführen. Die Firma Packet Forensics bietet dafür sogar eine fertige Appliance namens „5 Series“ mit einem Durchsatz von mehreren Gb/s an.

Als Gegenmaßnahme entwickeln sie ein Firefox-PlugIn namens CertLock, das in Kürze verfügbar sein soll. Es folgt einem „Trust-On-First-Use“-Prinzip und warnt, wenn der Zertifikatsaussteller wechselt oder die Länderkennungen von CA, besuchter Webseite oder Besucher sich unterscheiden.

Das ursächliche Problem – die Schwierigkeit, die Vertrauenswürdigkeit von SSL-Zertifikaten zu beurteilen – ist damit nicht gelöst. Folgt man Matt Blaze, so brauchen wir ein gänzlich neues Konzept.

Samurai gegen Web-Apps

Der Umfang der Tool-Sammlung „Samurai“ zur Analyse der Sicherheit von Web-Anwendungen hat sich mit Veröffentlichung der Version 0.8 vom 15.03.2010 auf ca. 1,7 GB mehr als verdoppelt. Die Installation der herunterladbaren ISO-Datei basiert immer noch auf der Ubuntu-Version 9.04, bietet aber einen zur Vorgängerversion deutlich erweiterten Werkzeugumfang. Sehr hilfreich ist die Möglichkeit, diese einfach aus den Code-Repositories der Entwickler zu aktualisieren.

Secorvo News

Security News Symposium 2010

Wie übt man einen Krisenfall? Sollte man iPhones verbieten? Welche verborgenen Risiken schlummern in USB-Sticks? Was kommt nach dem Mifare-Hack? Hängen wir an Passwort-Mythen? Diesen und weiteren aktuellen Fragen werden wir am **20.–21.04.2010** auf dem ersten „Security News Symposium“ in Karlsruhe/Ettlingen auf den Grund gehen. Wir freuen uns auf Ihre Teilnahme.

Teamverstärkung

Ab dem 01.04.2010 wird Michael Knopp das Secorvo-Team mit juristischer Kompetenz verstärken. Als Mitarbeiter der „Projektgruppe Verfassungsverträgliche Technikgestaltung“ (provet) und des „Instituts für Europäisches Medienrecht“ (EMR) hat er sich unter anderem mit rechtlichen Fragen der Langzeitarchivierung elektronischer Dokumente, mit Bürgerportalen und eGovernment-Lösungen auseinander gesetzt und sich als „Mittler zwischen den Welten“ von Recht und Technik bewegt.

Die guten ins Töpfchen

IT-Grundschutz-Zertifikate sind nach wie vor rar: Wenige Unternehmen schafften bisher eine Zertifizierung ihres Sicherheitsmanagements und der Umsetzung der in den Grundschutzkatalogen definierten Maßnahmen. Auf dem KA-IT-Si-Event am **29.04.2010** wird der DE-CIX, dem größten europäischen Internet-Knoten, im Panoramasaal der IHK Karlsruhe das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz verliehen. Begleitet wird die Prämierung von einem Erfahrungsbericht - und einem Sektempfang zum Büfett-Networken (Anmeldung).

Veranstaltungshinweise

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

April 2010	
19.-20.04.	Datenschutz kompakt (Gesellschaft für Datenschutz und Datensicherung e.V., Köln)
20.-21.04.	Security News Symposium 2010 (Secorvo, Ettlingen)
20.-22.04.	Datenschutztage 2010 (FFD Forum für Datenschutz, Frankfurt)
23.04.	Verbandstagung des Berufsverbandes der Datenschutzbeauftragten (BvD e.V., Berlin)
27.-28.04.	a-i3/BSI-Symposium 2010 (Arbeitsgruppe Identitätsschutz im Internet/BSI, Bochum)
29.04.	Die guten ins Töpfchen... (KA-IT-Si, IHK Karlsruhe)
Mai 2010	
04.-05.05.	11. Datenschutzkongress 2010 (EUROFORUM, Berlin)
17.-19.05.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
20.-21.05.	Datenschutzaudit – Best Practice (Secorvo College)
25.-28.05.	3rd Int. Workshop on Post Quantum Cryptography PQCrypto 2010 (Cased, Darmstadt)
Juni 2010	
07.-11.06.	TISP-Schulung (Secorvo College)

Fundsache

Am 17.03.2010 wurde die Studie „Know-How-Schutz in Baden-Württemberg 2009/2010“ des Sicherheitsforums BW und des Steinbeis-Instituts Stuttgart vorgestellt, für die 239 Unternehmen befragt wurden. Sie gibt ein detailliertes Bild der Einschätzung der Bedrohung durch Wirtschaftsspionage und der ergriffenen Schutzmaßnahmen.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Hans-Joachim Kobloch, Kai Jendrian

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