secorvo
security consulting

Secorvo Security News

Dezember 2010

Lehren aus Wikigate

Was ist WikiLeaks? Ein Ventil der Entrechteten? Eine Klagemauer der Gutmenschen? Das Fünkchen Hoffnung im universellen Wahnsinn? Oder ein Racheportal für Wichtigtuer? WikiLeaks mag als der Beweisversuch durchgehen, dass sich im Zeitalter des Internet nur wenig auf Dauer vertuschen lässt. Der Zorn des „Establishments" jedenfalls lässt sich kaum mit der Veröffentlichung der Botschaftsdepeschen erklären, sondern eher durch Publikationen wie der Videoaufnahme aus einem US-Hubschrauber am 05.04.2010, die das Niedermähen von 12 offensichtlich unbewaffneten Zivilisten, darunter zwei Mitarbeiter der Nachrichtenagentur Reuter, am 12.07.2007 in Bagdad zeigt. Unstreitig ist, dass Publikationen dieser Art einseitige Darstellungen korrigieren, dabei aber selbst Gefahr laufen, eine einseitige Sicht hervorzubringen – schließlich kommen diejenigen (Staaten) am besten davon, die besonders gut vertuschen. Dennoch sind solche Internet-Enthüllungen das demokratische Prinzip der „öffentlichen Kontrolle" in Reinkultur: Müssen Unternehmen und Behörden damit rechnen, dass Fehlverhalten publik wird, werden sie sich konsequenter um die Einhaltung ethischer Standards und rechtlicher Rahmenbedingungen kümmern.

Das eigentliche Wikigate hinter der öffentlichen Aufregung betrifft jedoch einen anderen Punkt: Offenbar hatten mehr als eine Million Personen regulär Zugriff auf die 250.000 Depeschen – sie waren damit schon vorher semi-öffentlich. Sehr viele WikiLeaks-Dokumente wurden von Zugriffsberechtigten enthüllt – die keine Entdeckung fürchten mussten, weil es so viele davon gab. Das ist der wahre Skandal: Wer das „need-to-know"-Prinzip derart großzügig auslegt, sollte sich besser vor (Wirtschafts-) Spionage ängstigen, als nach Whistleblowern zu fahnden. Denn, wie der Politikwissenschaftler Herfried Münkler so treffend in einem Spiegel Essay formulierte: „In der sozialen Welt ist Vertrauen an die Möglichkeit des Geheimnisses gebunden." Bevor das Vertrauen weg (und die Kontrolle total) ist, sollten wir wohl lieber erstmal die Zugriffsrechte begrenzen...

Inhalt

secorvo
security consulting

Security News

RossLeaks

Während sich die Welt mit der Sichtung und Sortierung von 250.000 überwiegend irrelevanten Diplomaten-Äußerungen beschäftigt, sucht sich die Wahrheit andere Kanäle. So publizierte Ross Anderson am 24.12.2010 sein Antwortschreiben an die UK Cards Association, die versucht hatte, unliebsame Veröffentlichungen über Schwachstellen des EMV-Verfahrens von der Webseite der Universität Cambridge entfernen zu lassen.

Mit akademischer Eloquenz klärt er in seinem Schreiben zunächst einmal über das Verständnis der Freiheit der Wissenschaft an der „Universität von Erasmus, Newton und Darwin" auf – und schließt mit dem Hinweis, dass das Vertrauen in Kreditkarten wohl weniger durch die Veröffentlichung, als vielmehr durch die Vertuschung bekannter Schwachstellen unterminiert werde. Eine erquickliche Lektüre zum Jahreswechsel.

Nach dem Ende des Internet

Nicht nur wegen inhaltlicher Regulierungsbestrebungen wie dem Jugendmedienschutz-Staatsvertrag, sondern auch aus technischen Gründen naht das Ende des Internet: Am 30.11.2010 vergab das Internet-Koordinationsgremium IANA vier der letzten elf /8-Blöcke mit je gut 16 Mio. IPv4-Adressen zur Unterverteilung an regionale Adressverwaltungen. Hochrechnungen zufolge werden die restlichen Blöcke bis März 2011 vergeben sein. Dann ist das Internet „voll".

Es wird also Zeit, den Umstieg auf IP Version 6 vorzubereiten, deren 128-Bit-Adressraum das Internet für die absehbare Zukunft am Leben erhalten dürfte. Eine am 01.12.2010 veröffentlichte Studie von RIPE NCC zeigt jedoch, dass die Übertragung von IPv6 über IPv4-Netze schon rein funktional noch mit erheblichen Kinderkrankheiten zu kämpfen hat. Das lässt Schlimmes für die Sicherheitseigenschaften von IPv6 befürchten. Am 27.12.2010 stellte der Autor des IPv6-Sicherheitstest-Toolkits thc-ipv6 beim CCC-Kongress 27C3 neue Erkenntnisse zu Sicherheitsproblemen von IPv6 vor – trotz der Neuerungen in den Bereichen Multicasts und Source Routing keine guten Nachrichten.

Nicht in Wittenberg

Auf ihrer Webseite hat die Gesellschaft für Informatik (GI) am 01.12.2010 ihre Zehn Thesen zu Sicherheit und Datenschutz im Cloud Computing angeschlagen. Darin werden die Hauptrisiken bei der Nutzung von Cloud Computing kompakt auf den Punkt gebracht. In knapper Form werden viele Baustellen angerissen, die vor einem Einsatz von Cloud Computing sorgfältig bearbeitet werden sollten. Denn die Ausrichtung der IT auf die Cloud erfordert auch in Sicherheitsfragen ein radikales Umdenken. Ergänzt werden die zehn Thesen der GI durch eine umfangreiche Literaturliste zum Thema Sicherheit und Datenschutz beim Cloud Computing.

Umfangreicher werden die relevanten Fragestellungen im 34seitigen Leitfaden für sicheres Cloud Computing des Verbands der deutschen Internetwirtschaft (eco) behandelt, der fast zeitgleich am 02.12.2010 veröffentlicht wurde. Dieser Leitfaden ist auf Anfrage erhältlich. Lediglich der Bitkom schwächelt: Der bereits am 18.09.2009 veröffentlichte, 84seitige Leitfaden Cloud Computing behandelt Datenschutzaspekte auf drei und Sicherheitsfragen auf einer halben Seite – kein rühmliches Bild.

SSLiversum – (Un)bekannte Welten

Nicht erst seit dem Erscheinen von Tools wie Firesheep (SSN 10/2010) ist es empfehlenswert, für den Zugriff auf Internet-Dienste soweit möglich HTTPS zu verwenden. Aber wie vertrauenswürdig sind „blaue" und „grüne" TLS-Zertifikate (SSN 06/2007) in den Weiten des Internet wirklich?

Dieser Frage widmet sich das SSL-Observatorium der EFF. Dessen Mitarbeiter stellten am 30.07.2010 auf der Defcon 18 einen Überblick ihrer Beobachtungen vor, den sie am 28.12.2010 beim CCC-Kongress 27C3 aktualisieren werden. Neben dem einer Protonen-Kollision nicht unähnlichen Graphen der ca. 650 (!) CAs, denen gängige Browser vertrauen, findet man im „SSLiversum" einige Perlen für PKI-Spötter, so etwa CAs in Manchester und New Jersey, die sich ein Schlüsselpaar teilen, Tausende von offiziellen Zertifikaten für „localhost" oder das Generalschlüssel-Zertifikat für vier Dutzend verschiedene Hosts.

Another one bites the dust

Alle Welt redet bei passender Gelegenheit gern und viel über Sicherheit. Den Worten folgen allerdings oft keine Taten; wenn doch, dann oft solche, auf die man besser verzichtet hätte. Das lässt sich regelmäßig nicht nur beim Gesetzgeber beobachten, sondern auch in der Industrie.

Was die Sache erstaunlich macht, ist, dass dies auch für die Großen gilt – die es eigentlich besser können oder wissen müssten. Unlängst war Canon an der Reihe: Bekanntermaßen lassen sich Digitalbilder heute mittels moderner Bildbearbeitungswerkzeuge so manipulieren, dass gute Collagen kaum noch als solche zu erkennen sind. Canon hatte daher die – an sich gute – Idee, Bilder so zu

authentifizieren, dass ein Fotograf die Echtheit einer Aufnahme nachweisen kann. Die Authentifizierung übernimmt ein (teures) Security-Kit (OSK-E3), das man an die Kamera anschließen kann. Die Funktionsweise des Kits hält Canon geheim – zur Erhöhung der Sicherheit.

Es kam, wie es kommen musste (Mifair lässt grüßen, SSN 3/2008): Das Verfahren wurde analysiert – und am 28.11.2010 von Dmitry Sklyarov öffentlich gebrochen. Die Details sind peinlich: Der Authentifizierungsmechanismus ist keine Signatur, sondern ein „keyed hash", der HMAC-Key ist für alle Kameras eines Modells identisch und in der Kamera gespeichert, und der Hashwert verwendet kein „Salz" – da hält sich das Mitleid in Grenzen. Wie formulierte Bruce Schneier einmal so schön: Geheime Verfahren sind meist solche, deren sich die Hersteller eigentlich schämen müssten... Dmitry Sklyarow meinte launig, Canon sollte vielleicht Leute einstellen, die etwas von Sicherheit verstehen. Kein schlechter Vorschlag – auch für zahlreiche andere Unternehmen (und gelegentlich den Gesetzgeber).

Aufschub für die Bilanzübermittlung

Mit dem Steuerbürokratieabbaugesetz wurde am 20.12.2008 in Gestalt des § 5b EStG eine Verpflichtung buchführender Unternehmen zur elektronischen Übermittlung ihrer Bilanzen und Gewinn- und Verlustrechnungen eingeführt, die bereits für das kommende Wirtschaftsjahr gegolten hätte. Mit Schreiben vom 16.12.2010 hat das Bundesfinanzministerium nun die Pflicht zur elektronischen Bilanz- sowie Gewinn- und Verlustrechnungsübermittlung um ein Jahr auf die ab dem 01.01.2012 beginnenden Wirtschaftsjahre verschoben.

Zunächst sollen ausgewählte Unternehmen freiwillig an einer Pilotphase zum Test des Verfahrens und des amtlich vorgeschriebenen Datensatzes (Taxonomie) teilnehmen.

Die Übermittlung sollte ursprünglich durch einen den Unternehmen zur Verfügung gestellten Client erfolgen, an den diese ihre Schnittstellen anzupassen hätten. Da weder der auf eXtensible Business Reporting Language beruhende Datensatz noch die Client-Spezifikationen bisher abgeschlossen vorliegen und die Entwürfe umfassender Kritik begegneten, wurde nun die Reißleine gezogen. Auch für den um ein Jahr verschobenen Start ist zu befürchten, dass er in großer Eile erfolgen muss; darunter dürfte auch die Sicherheit des Verfahrens leiden.

Vielleicht aber ist von dem Verfahren bis dahin ähnlich wenig übrig, wie heute von der 2002 eingeführten „Elektronischen Steuererklärung mit digitaler Signatur" – im Wesentlichen der Name „Elster".

Hintertüren überall

Gleich drei schwer wiegende Bugs und Hintertüren wurden Mitte Dezember aufgedeckt: Am 14.12. 2010 wurde öffentlich, dass eine Netzwerkspeicherlösung von Hewlett Packard ein nicht dokumentiertes Benutzerkonto mit vollen Zugriffsrechten und Standardpasswort („!admin") besitzt. Am 13.12. 2010 wurde bekannt, dass in der freien SmartCard-Bibliothek OpenSC über einen Pufferüberlauf im Treiber durch bestimmte Seriennummern Code auf dem Zielsystem ausgeführt werden kann.

Schließlich beschuldigte der Gründer des OpenBSD-Projektes, Theo de Raadt, am 14.12.2010 in einer E-Mail ehemalige OpenBSD-Entwickler, im Auftrag des FBI Hintertüren in die VPN-Komponente eingebaut zu haben – vor etwa 10 Jahren. Man könnte sich nun fragen, ob eine Hintertür in einem Open-Source-Projekt tatsächlich so lange unentdeckt bleiben kann – genau das aber hat das Debian-OpenSSL-Debakel (SSN 5/2008) schon vor über zwei Jahren gezeigt. Vor Hintertüren kann man nie sicher sein – weder bei kommerziellen Produkten noch bei freien Projekten.

Secorvo News

T.I.S.P. wird Standard

Seit der Entwicklung des T.I.S.P.-Zertifikats (TeleTrusT Information Security Professional) wurden über 400 Security-Experten mit diesem Qualifikationsnachweis ausgezeichnet. Immer häufiger wird der T.I.S.P. in Unternehmen zum Qualifikationsstandard für alle Mitarbeiter, die mit Aufgaben der Informationssicherheit betraut sind. Mehr als 50 T.I.S.P.-Absolventen, die sich Anfang November in Köln zum diesjährigen T.I.S.P. Community Meeting trafen, bestätigten diesen Trend. Auch 2011 bietet Secorvo College wieder mehrere Gelegenheiten zur Schulung und unabhängigen T.I.S.P.-Zertifizierung.

Smart Grid Symposium

Am 01.-02.02.2011 sind wir mit einem spannenden Symposium zu Datenschutz- und Datensicherheit rund um das „Intelligente Stromnetz" wieder in der Buhlschen Mühle zu Gast. Werfen Sie einen Blick in das Programm – wir freuen uns auf Ihre Teilnahme!

Last Call for Feedback

Noch bis zum 31.01.2011 nehmen Sie anlässlich der 100. Ausgabe der Secorvo Security News mit Ihrem Kommentar zu unseren News automatisch an der Verlosung einer Teilnahme an einem Secorvo College-Seminar Ihrer Wahl teil. Wir freuen uns auf Ihr Feedback – und drücken die Daumen!

Veranstaltungshinweise

Januar 2011	
18.-20.01.	Omnicard 2011 (inTIME, Berlin)
Februar 2011	
01.-02.02.	Smart Grid Symposium (Secorvo, Ettlingen/KA)
02.-03.02.	21. SIT-SmartCard Workshop (SIT, Darmstadt)
08.-10.02.	CPSSE-Schulung (Secorvo College)
15.-16.02.	18. DFN-Workshop Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
März 2011	
01.-05.03.	CeBIT (Deutsche Messe, Hannover)
22.-24.03.	Sicherheitsmanagement heute (Secorvo College)
28.03.-01.04.	T.I.S.P.-Schulung (Secorvo College)
April 2011	
04.-06.04.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
07.-08.04.	Datenschutzaudit: Best Practice (Secorvo College)

Fundsache

Erstmals haben sich die Datenschutz-Aufsichtsbehörden mit einem Beschluss des Düsseldorfer Kreises (vom 24./25.11.2010) auf Mindestanforderungen an den Datenschutzbeauftragten festgelegt. Darin werden schon bei Bestellung „umfassende Kenntnisse zum Inhalt und zur rechtlichen Anwendung" des relevanten Datenschutzrechts erwartet, dazu „Kenntnisse der Informations- und Kommunikationstechnologie und der Datensicherheit". Bei externen DSB wird eine Mindestvertragslaufzeit von vier Jahren, bei Erstverträgen von 1-2 Jahren empfohlen.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, 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