secorvo
security consulting

Secorvo Security News

November 2011

Lest Märchen!

Kennen Sie Grimms Märchen? Nein, das ist *keine* iPhone-App. Es war einmal vor vielen, vielen Jahren, da las man den Kindern abends vor dem Kamin Märchen vor – bevorzugt die der Gebrüder Grimm von 1812. Mancher macht das noch heute – sei es aus Tradition, aus Nostalgie oder in Ermangelung anderer Kinderbücher. Oder auch, weil der Fernseher kaputt und der iPhone-Akku leer sind. Wie dem auch sei: Beim Lesen werden Sie feststellen, dass jedes Märchen zahlreiche Lehren enthält – und nicht nur die, die ins Auge springen. Einige davon helfen sogar der Informationssicherheit.

Nehmen wir beispielsweise das Märchen vom Wolf und den sieben Geißlein. Zur Erinnerung: Der Wolf will in Abwesenheit der Geiß deren Kinder zum Öffnen der Haustüre überreden – die aber erkennen ihn erst an der Stimme, dann an der Pfote. Als er beides tarnt, öffnen sie ihm – und er verschlingt alle bis auf das siebte, das sich im Uhrkasten versteckt hat. Weil er sich in der Nähe zum Schlafen legt, wird er später von der Geiß aufgeschlitzt – und die Geißlein befreit.

Was können wir daraus lernen?

1. Plausibilitäts-Checks sind kein wirksamer Schutzmechanismus. (Auch wer redet wie eine Geiß, kann ein Wolf sein.)
2. Die erfolgreiche Abwehr von Angriffen sollte ein Alarmsignal sein. (Der nächste Angriff ist sicher besser als der abgewehrte.)
3. Security Policies sind ohne Sensibilisierung und gesunde Skepsis wertlos. (Angreifer sind erfindungsreicher als Policy-Autoren.)
4. Das Fehlen interner Schutzwälle gibt dem erfolgreichen Eindringling alles preis. (Interne Schotts begrenzen den Angriffserfolg.)
5. Nur bei tierisch dummen Angreifern gibt es eine Chance, die erbeuteten Daten zurück zu erhalten.

Vielleicht darf man wenigstens hoffen, dass bei einem erfolgreichen Angriff 14,3 % der Informationen verschont bleiben. Verstecken Sie daher sicherheitshalber schon mal das Wichtigste im Uhrkasten.

Inhalt

secorvo
security consulting

Security News

Ertappt

Am 02.11.2011 hat der Hamburgische Datenschutzbeauftragte einen Bericht vorgelegt, der der Nutzung von Cookies durch Facebook nachgeht. Die dem Bericht zugrunde liegende Prüfung orientiert sich an den Zweckangaben, die Facebook unter anderem gegenüber dem ULD Schleswig-Holstein angeführt hat. Zu den einzelnen Zweckangaben wurden für die Prüfung Szenarien gebildet, die dann in einer sicheren Umgebung dokumentiert durchgespielt wurden. Ziel war, festzustellen, ob die verschiedenen Cookies die angegebene Wirkung zeigen würden.

So soll etwa der „datr"-Cookie gemäß Facebook Hinweise auf Missbrauch liefern, indem er feststellt, ob über denselben Browser viele verschiedene Accounts genutzt werden. Bei den durchgeführten Versuchen konnte eine solche Wirkung nicht bestätigt werden. Ähnliches gilt für zahlreiche andere Zweckangaben.

Daraus kann zwar nicht geschlossen werden, dass die Cookies, wie vielfach vermutet, domainübergreifend für das Nutzertracking genutzt werden. Es indiziert jedoch, dass Facebook für einen Teil seiner Cookies keinen zulässigen Verwendungszweck angeben kann. So lassen sich jedenfalls nicht in rechtskonformer Weise Nutzertransparenz herstellen und die Erforderlichkeit der Datenerhebung nachweisen.

Zu Recht stellt der Bericht mindestens einen Verstoß gegen die jeweiligen nationalen Umsetzungen von Art. 5 Abs. 3 der E-Privacy-Richtlinie fest. Bei den Aufsichtsbehörden dürfte Facebook damit weiteres Vertrauen verspielt haben.

c = m

Kryptografie kann so einfach sein. Das dachen wohl auch die Programmierer der Entwicklerversion von Ruby bei der Implementierung des RSA-Verfahrens:

Wenn $c = m^e \bmod n$ zu berechnen ist – dann geht das mit $e := 1$ am schnellsten. Damit folgt:

$$c = m \bmod n,\ m < n \Rightarrow c = m$$

Sollten Sie mit dieser Ruby-Version zwischen dem 01.09.2011 und dem 04.11.2011 RSA-Schlüssel erzeugt haben, dann ersetzen Sie diese besser schnellstmöglich. Denn wenn man bei DES schon Schlüssel als schwache Schlüssel bezeichnet, die bei zweimaliger Verschlüsselung den Klartext liefern,

$$DES(k, DES(k, m)) = m$$

muss man hier wohl von einem überschwachen Schlüssel mit RSA(k, m) = m reden.

No, map!

Um ein erneutes Marketing-Desaster wie die Diskussion um die Abbildung deutscher Hausfassaden in Street View zu vermeiden, geht Google bei der Lokalisierungsfunktion in die Offensive: Wie viele Standort-basierenden Dienste (*location-based services*) verfügt auch Google Maps seit einer Weile über einen Standortbestimmungsdienst, aktivierbar über den „Knopf" oberhalb der Zoom-Einstellung.

Da Google – anders als ein Smartphone – keinen direkten Zugriff auf Dienste des Netzbetreibers zur Standortbestimmung hat, wertet Google u. a. die SSIDs erreichbarer WLANs aus. Deren Standort-Daten wurden beim Fotografieren der Hausfassaden gleich mit erhoben oder von Nachbarn gemeldet – und werden in einer zentralen Datenbank (*Google Location Server, GLS*) vorgehalten.

Am 15.11.2011 machte Google publik, dass jeder, der mit seinem SSID (*service set identifier*) nicht im GLS aufgenommen werden möchte, die Löschung mit einem ungewöhnlichen „Opt-Out"-Mechanismus veranlassen soll: durch die Ergänzung der eigenen SSID um die Endung „_nomap".

Sieht man einmal von der Frage ab, wie vielen privaten WLAN-Nutzern wohl eine entsprechende Umkonfiguration des eigenen WLAN-Routers gelingt, ohne Schaden anzurichten, bleibt die Gefahr, dass das Beispiel Schule machen könnte: Weitere Endungen wie z. B. „_noiphone" oder „_noandroid" dürften die verfügbaren 32 Byte maximaler SSID-Länge schnell abschmelzen. Vielleicht sollten die Standardisierungsgremien besser schon mal mit Anpassungsarbeiten am IEEE 802.11 beginnen...

OWASP.de gibt Gas

Beim deutschen Chapter von OWASP hat sich im November viel getan. Am 16.11.2011 wurde die deutsche Übersetzung der OWASP Top 10 unter der Projektleitung von Kai Jendrian fertig gestellt und publiziert. Damit steht der anerkannte Branchenstandard nun auch in Deutsch zur Verfügung, um das Sicherheitsbewusstsein bei der Entwicklung von Webanwendungen zu verbessern – besonders bei Entwicklern in mittelständischen Unternehmen.

Am 17.11.2011 folgte in München der 4. German OWASP Day, bei dem sich mehr als 160 Experten über Sicherheitsfragen von Webanwendungen diskutierten. Zwei parallele Vortrags-Tracks deckten ein breites Spektrum an Themen ab – von Secure Software Development Life Cycle, Statischer Code Analyse über Web-Service-Security, Mobile Security und Browser-Sicherheit hin zu aktuellen Cyber-Bedrohungen. Ein Highlight war der Ausblick auf

bevorstehende Entwicklungen von Thomas Roessler (W3C).

Schließlich wurde am 19.11.2011 das Portal hacking-lab.com der OWASP Academy freigeschaltet, mit dem sich Entwickler und Sicherheitsfachleute an praktischen Anwendungen zur Sicherheit von Anwendungen fortbilden sollen.

Europäischer Treibsand

Der Europäische Gerichtshof hat am 24.11.2011 in einer Vorabentscheidung über die Auslegung von Art. 7 der Europäischen Datenschutzrichtlinie entschieden. Anlass war ein Rechtsstreit zwischen dem Verband spanischer Kreditinstitute (ASNEF), dem Verband für E-Commerce und Direkmarketing (FECEMD) und dem spanischen Staat. Nach der Entscheidung sind die nationalen Gesetzgeber auf die in Art. 7 aufgezählten Zulässigkeitstatbestände festgelegt und dürfen diese nicht weiter einschränken oder weitere Tatbestände einführen.

Nach Ansicht der Kläger geht Spanien in seinem Datenschutzgesetz über Art. 7 hinaus, indem es die Verarbeitung personenbezogener Daten für berechtigte Interessen des Verarbeiters ohne Einwilligung des Betroffenen nur für veröffentlichte Daten eröffnet. Dem hat der EuGH zugestimmt.

Den Mitgliedstaaten steht zwar offen, Leitlinien für die Abwägung zwischen dem Grundrechtsschutz der Betroffenen und den berechtigten Interessen aufzustellen, die den Unterschied zwischen veröffentlichten und unveröffentlichten personenbezogenen Daten berücksichtigen, er darf jedoch nicht durch den völligen Ausschluss unveröffentlichter Daten Art. 7 überschreiten. Dieser Grundsatz gelte allgemein für die Auslegung von Art. 7, der gleichzeitig für direkt anwendbar erklärt wurde.

Das deutsche Datenschutzrecht ist von der Entscheidung nicht direkt betroffen, da es in § 28 Abs. 1 Nr. 2 und 3 BDSG getrennte Tatbestände für die Wahrnehmung berechtigter Interessen und allgemein zugängliche Daten enthält. Die Entscheidung wirft jedoch die Frage auf, ob die zahlreichen Detailregelungen des Bundesdatenschutzgesetzes lediglich erlaubte Leitlinien innerhalb der Grenzen des Art. 7 darstellen oder Datenkategorien ausschließende neue Tatbestände außerhalb von Art. 7 sind. Die Diskussion um die Zukunft des Datenschutzrechts ist damit um eine europäische Dimension reicher geworden.

Secorvo News

Secorvo College aktuell

Das Jahr neigt sich langsam dem Ende zu und für die Planung Ihrer Weiterbildung im kommenden Jahr lohnt sich bereits jetzt ein Blick in unseren Seminarkalender 2012. Auch im neuen Jahr bietet Secorvo College wieder zahlreiche Weiterbildungsgelegenheiten.

Los geht es gleich im Januar mit dem Grundlagenseminar Sicherheitsmanagement heute (24.-26.01.2012). Im März folgen dann IT-Sicherheit heute (13.-15.03.2012) und Verlässliche Web-Anwendungs-Sicherheit (21.-22.03.2012). Die erste Gelegenheit zur Zertifizierung Ihrer persönlichen Qualifikation im Bereich sichere Softwareentwicklung bieten wir Ihnen am 26.-30.03.2012 beim Seminar Certified Professional for Secure Software Engineering (CPSSE). Das nächste T.I.S.P.-Seminar führen wir vom 07.-11.05.2012 durch – Ihr Exemplar des T.I.S.P.-Buchs erhalten Sie bei frühzeitiger Anmeldung vorab zugesandt.

Das vollständige Jahresprogramm 2012, die detaillierten Programme aller Seminare und die Möglichkeit zur Online-Anmeldung und finden Sie unter http://www.secorvo.de/college. Wir freuen uns auf Ihre Anmeldung!

Für den Weihnachtsmann

Sollten Sie noch Platz unterm Tannenbaum haben und Ihr Weihnachtsmann noch keine durchschlagende Geschenkidee, dann lohnt ein Hinweis auf das T.I.S.P.-Buch: Kann man sich etwas Schöneres vorstellen, als bei Kaffee und Keksen im Kerzenschein vor dem knisternden Kamin zu sitzen und genussvoll in den „Zentralen Bausteinen der Informationssicherheit“ zu schmökern? Wer sich das nicht entgehen lassen möchte, möge hier klicken – oder den Bestellwunsch gleich an den Weihnachtsmann weiterleiten.

Krypto zum Anfassen

Die Karlsruher IT-Sicherheitsinitiative (kurz: KA-IT-Si) erfreute sich in diesem Jahr erneut wachsender Teilnehmerzahlen – zuletzt konnten wir auf der Veranstaltung im November über 50 Teilnehmer begrüßen. Ab 2012 wird eine Kooperation mit dem Karlsruher Institute of Technology (KIT) und dem am 17.10.2011 feierlich eröffneten Kompetenzzentrum für angewandte Sicherheits-Technologie (KASTEL) die KA-IT-Si inhaltlich bereichern.

Am 26.01.2012 startet die Zusammenarbeit mit einem Highlight: Mit Vorträgen und Vorführungen werden wir einen Blick in die Geschichte der Kryptografie werfen – unterstützt durch historische Verschlüsselungsmaschinen u. a. aus der Sammlung des Instituts für Kryptografie und Sicherheit (IKS). Eine frühzeitige Anmeldung wird empfohlen.

Veranstaltungshinweise

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

Dezember 2011	
05.-06.12.	IsSec/ZertiFA 2011 (Computas, Berlin)
Januar 2012	
17.-19.01.	OMNICARD 2012 (in TIME berlin, Berlin)
24.-26.01.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
26.01.	Krypto zum Anfassen (KA-IT-Si, Karlsruhe)
Februar 2012	
08.-09.02.	22. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
21.-22.02.	19. DFN Workshop „Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
März 2012	
13.-15.03.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
14.-16.03.	Black Hat Europe 2012 (Blackhat, Amsterdam/NL)
21.-22.03.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College, Karlsruhe)
26.-30.03.	CPSSE (Secorvo College, Karlsruhe)

Fundsache

Seit August 2010 findet sich auf der Webseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) eine Handreichung zu § 11 des Bundesdatenschutzgesetzes. Darin bezieht der BfDI auf drei Seiten zu wichtigen Fragen Stellung, wie der Anpassung von Altverträgen oder dem Verständnis von „sich überzeugen".

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Michael Knopp

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