secorvo
security consulting

Secorvo Security News

Dezember 2012

Das Analoge im Digitalen

Es mutet manchmal eigenartig an, wie bereitwillig viele Menschen die Risiken der digitalen Welt ignorieren. Bruce Schneier zeichnet in seinem jüngsten Crypto-Gram diese „schöne neue Welt" sogar als eine Art „digitaler Leibeigenschaft" – mit Amazon, Apple, Facebook und Google in der Rolle der Feudalherren, denen ihre Vasallen alles anvertrauen. Aus der Fürstenperspektive gibt es natürlich wenig Grund, die Legitimität dieses einseitigen Vertrauensverhältnisses und der Möglichkeit absoluter Kontrolle in Zweifel zu ziehen. Merkwürdig stimmt allerdings, dass Milliarden Nutzer sich begeistert in diese Abhängigkeit begeben – und sogar zu glühenden Anhängern werden, die bereitwillig mithelfen, nicht nur das Mantra ihres Herrn zu verbreiten, sondern es eifernd gegen jeden Skeptiker oder Kritiker und gegen alle Anhänger anderer Fürsten zu verteidigen.

Einige bemühen zur Rechtfertigung immerhin Fatalismus: „Warum ich die iCloud benutze? Apple weiß doch ohnehin alles über mich...". Dabei kämen die meisten von ihnen im wirklichen Leben kaum auf ähnliche Ideen: „Warum sollte ich meinem Nachbarn nicht meine Kreditkarte und die EC-Karte mit PIN anvertrauen? Den Haustürschlüssel hat er doch auch schon..." Helfen könnten daher bewährte Strategien aus der analogen Welt auch in der digitalen:

- Vertraue Dritten nie blind – sondern immer nur so, dass du das Vertrauen auch jederzeit wieder entziehen kannst.
- Setze nie alles auf eine Karte.
- Vertraue nie unbegrenzt – behalte immer einen Rest Kontrolle.

Weder frühmittelalterliche Fürstenhuldigung noch Bequemlichkeit oder Kostenfokussierung sind eine angemessene Haltung für Risikobewertung und Schadensbegrenzung. Aber wie formulierte Marie Freifrau Ebner von Eschenbach (1830-1916) doch so treffend: „Die glücklichen Sklaven sind die erbittertsten Feinde der Freiheit."

Inhalt

secorvo
security consulting

Security News

Rechtsverstoß Double-Opt-In

Am 27.09.2012 hat das OLG München mit einer Entscheidung für große Verunsicherung gesorgt, nach der die Bestätigungsanfrage beim Double Opt-In-Verfahren zur E-Mail-Werbung als unzumutbare Belästigung zu betrachten ist, wenn sie nicht nachweislich vom Empfänger veranlasst wurde.

Dies wird von der Beratungsszene und Anbietern kontrovers diskutiert. Klar ist: § 7 Abs. 2 Nr. 3 UWG verbietet E-Mail-Werbung ohne ausdrückliche und nachweisbare Einwilligung. Das Double-Opt-In soll daher sicherstellen, dass keine werbliche Ansprache via E-Mail erfolgt, wenn die Einwilligung nicht vom Inhaber der dabei angegebenen E-Mail-Adresse auf Anforderung bestätigt wird. Der BGH hat 2004 in anderer Konstellation bereits entschieden, dass ein Double Opt-In den notwendigen Nachweis der elektronischen Einwilligung führen kann.

Nun kann ein Teil eines Authentifizierungs- und Schutzmechanismus ohne werbliche Inhalte naturgemäß eigentlich keine unzumutbare Belästigung sein, solange sie durch einen Webseiteneintrag veranlasst wurde. Dieser freilich muss genauso wie die spätere Bestätigung protokolliert und aufbewahrt werden. Allerdings kann bei einer Anmeldung über ein Webformular selbst bei Protokollierung kein personenbezogener Veranlassungsnachweis gelingen – es sei denn, der Nutzer würde sich auf andere Weise authentifizieren. Dann wäre jedoch eine Bestätigung (und damit auch die E-Mail-Benachrichtigung) überflüssig. Für die Versender von E-Mail-Newslettern und -Werbung bleibt jedoch bis zur höchstrichterlichen Klärung das Risiko, für das Double Opt-In-Verfahren abgemahnt zu werden.

Smart Meter Profiles

Das Weihnachtsgeschenk des BSI vom 21.12.2012 sind Version 1.1.7 der Protection Profiles für Smart Meter Gateways und Version 1.0 der Protection Profiles der in Smart Meter Gateways enthaltenen Security Modules. Die Funktionalitäts- und Interoperabilitätsanforderungen wurden in der Technischen Richtlinie TR-03109 (Version 1.0, Release Candidate) spezifiziert. Alle drei Dokumente sollen zusammen mit dem Referentenentwurf der Rechtsverordnung nach § 21i EnWG Anfang 2013 von der EU notifiziert und damit für die Entwicklung von Komponenten der so genannten „intelligenten Energienetze“ rechtlich bindend werden.

Zwar handeln die Spezifikationen alle wichtigen Sicherheitsaspekte von der Authentifikation bis zur verschlüsselten Übermittlung systematisch ab. Themen des Datenschutzes werden jedoch – trotz Mitwirkung des BfDI – auf gerade einer der 90 Seiten behandelt, beschränkt auf Pseudonyme und Übertragungsschutz. Fragen nach Erforderlichkeit, Zweckbindung oder Datensparsamkeit bleiben ausgeklammert: die Protection Profiles sorgen also auch bei unzulässiger Erhebung für einen guten Schutz. Die Frage der Rechtmäßigkeit der mit Smart Meter Gateways geplanten und möglichen Verarbeitung von Verbraucherdaten bleibt damit dem politischen Diskurs vorbehalten.

Löschen nach Regeln

Die Festlegung von Regellöschfristen für verarbeitete personenbezogene Daten ist eine der größten praktischen Herausforderungen des Datenschutzrechts. Ausgelöst durch Veröffentlichungen der Toll Collect GmbH über ihr Datenschutz-Löschkonzept schrieb der DIN Anfang 2012 ein vom BMWI gefördertes Projekt im Programm „Innovation mit Normen und Standards“ aus, um die Möglichkeit einer standardisierten Vorgehensweise für die Entwicklung von Löschkonzepten zu untersuchen.

Am 10.12.2012 wurde nun die in intensiver Diskussion mit Datenschützern aus Industrie und Aufsichtsbehörden von Secorvo erarbeitete Leitlinie zur Entwicklung eines Löschkonzepts (Dr. Volker Hammer, Karin Schuler) vorgestellt. Die zuständige ISO/IEC-Arbeitsgruppe hat Interesse an einer Fortsetzung der Standardisierungsarbeiten signalisiert; sofern die Finanzierung der Arbeiten durch Förderunternehmen gesichert werden kann, könnte nun unter deutscher Federführung ein internationaler Lösch-Standard für personenbezogene Daten entstehen. Bei Interesse stellen wir gerne einen Kontakt her – E-Mail an redaktion-security-news@secorvo.de genügt.

Cyberentschlossenheit

Das Europäische Parlament hat am 22.11.2012 eine Entschließung zur Cybersicherheit und Verteidigung angenommen. Darin werden EU-Institutionen und Mitgliedstaaten aufgefordert, unter Einbindung privater Unternehmen Maßnahmen zu ergreifen. Die Zustandsfeststellungen dokumentieren vor allem ein EU-weit uneinheitliches Vorgehen gegen Cyberattacken – trotz gewachsener Bedrohung. Insbesondere sähen nur wenige Staaten bislang den Schutz ihrer IT-Infrastrukturen als Teil ihrer Sorgfaltspflichten, nur zehn Mitgliedstaaten besäßen eine nationale Strategie, und mangels Meldungen bestünde eine hohe Dunkelziffer an Angriffen.

Gefordert werden ein gemeinsames Weißbuch, eine gründliche Erfassung der Angriffe und Bewertung der Gefahren, eine koordinierte Reaktion auf EU-Ebene und die Erarbeitung von Notfallplänen in Kooperation mit der ENISA. Schließlich wird sogar

die Anerkennung eines schweren Cyber-Angriffs als Solidaritätsfall und Kriegsgrund postuliert.

Die Entschließung signalisiert zwar Entschlossenheit; die Maßnahmenvorschläge erscheinen jedoch als ein willkürliches Sammelsurium von Ausbildungsförderung bis Kriegserklärung. Der Weg zu einer geschlossenen Strategie ist noch weit.

Neues vom Bundestrojaner

Am 17.10.2012 hatte die SPD-Fraktion der Bundesregierung in einer kleinen Anfrage 55 spannende Fragen zum Bundestrojaner gestellt – unter anderem zur Weigerung der Fa. DigiTask, dem BfDI Einsicht in den Quellcode zu gewähren. Am 10.12.2012 wurden nun die Antworten der Bundesregierung vom 21.11.2012 veröffentlicht. Einige sind durch einen Hinweis auf die Vertraulichkeitsstufe (VS-NfD) ersetzt. Dennoch enthält das Dokument interessante Details – u. a. den Hinweis, dass Skype-Telefonate nicht abhörbar seien und mit einer vom BKA selbst entwickelten Überwachungssoftware erst Ende 2014 gerechnet werden könne.

Keylogger

Heutige Hardware-Keylogger sind günstig (ca. 60$), bescheren Aufmerksamkeit (wie im Fall vom 23.10.2012), arbeiten beinahe transparent und speichern mehrere GB Tastendrücke. Sofortmaßnahmen für den Finder sind Passwortwechsel, polizeiliche Spurensicherung, Sicherung der Gebäude-Zutrittsprotokolle und ggf. in Abstimmung mit Datenschutz und Betriebsrat eine Raumüberwachung oder die Hinterlegung der Adresse eines Honeypots auf dem Logger.

Ähnlich hässlich ist die am 25.10.2012 von Ryan Barnett auf der AppSecUSA präsentierte Idee: Dabei infiziert eine Web Application Firewall ausgewählte „Besucher“ mit dem Browser Exploitation Framework (kurz BeEF) per Angriff auf Web Browser-Schwachstellen, um dann z. B. einen Software-Keylogger zu platzieren.

Manchmal kommt ein Keylogger auch nicht allein: Scannen Sie daher nicht nur regelmäßig Ihr System, sondern prüfen Sie auch von Zeit zu Zeit Ihre Schnittstellen – oder sorgen Sie mit Klebstoff für eine feste Verbindung von Tastaturstecker und PC.

Neujahrsputz

Wer gleich zu Beginn des neuen Jahres die Angriffsfläche seines PCs reduzieren möchte, sollte Java in seinen Browsern deaktivieren. Denn während es kaum noch einen guten Grund gibt, mit aktiviertem Java im Browser zu surfen, öffnen unsichere Java-Versionen Angreifern Tür und Tor: Von lediglich drei im Jahr 2011 stieg die Zahl der 2012 veröffentlichten Security Vulnerabilities des JRE auf beeindruckende 58 – stattliche 23 davon mit der höchsten Gefährdungsstufe 10.

Hilfreiche Anleitungen um Java mit wenig Aufwand wirksam aus dem Browser zu verbannen finden Sie bei Andrew Tech Help, Brian Krebs oder OSXDaily.

Secorvo News

Eröffnung des Kryptologikums

In das Jahr 2013 startet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit einem besonderen Highlight: Am **31.01.2013** werden wir im Zentrum für Kunst und Medientechnologie (ZKM) das „Kryptologikum“ des Karlsruher Institute of Technology (KIT) eröffnen. Ähnlich dem Mathematikum in Gießen, dem Dynamikum in Pirmasens und dem Technoseum in Mannheim bietet das Kryptologikum in einer zunächst dreitägigen Ausstellung (vom 01.-03.02. 2013) Kryptographie zum „Begreifen“. Die Exponate veranschaulichen kryptographische Prinzipien und es werden historische Verschlüsselungsmaschinen gezeigt, die Kriege entschieden haben.

Das Eröffnungsevent beginnt um 18 Uhr im Kubus des ZKM in Karlsruhe. Wir freuen uns auf Ihre Teilnahme – und empfehlen Ihnen eine schnelle Anmeldung.

Sichere Systeme

Technisch verursachte Sicherheitsvorfälle können in der Regel auf eine von drei Ursachen zurückgeführt werden: Konfigurationsfehler, Programmierfehler oder ein fehlerhaftes Systemkonzept. Die letzte dieser Ursachen ist oft besonders heikel: Sie entsteht durch das Zusammenspiel komplexer Einzelkomponenten und lässt sich zumeist nur durch einen teuren Systemwechsel beseitigen.

Um dieses Problem an der Wurzel zu packen, haben wir gemeinsam mit dem Institut für Kryptographie und Sicherheit (IKS) am Karlsruhe Institute of Technology (KIT) ein Seminar für Systementwickler konzipiert, in dem wir in das Konzept des „Security by Design“ einführen: Security Engineering – Anleitung zur Entwicklung sicherer Systeme am 18.-21.03.2012.

Im April folgt die nächste Schulungen zum T.I.S.P. Zertifikat – von den Autoren des T.I.S.P.-Buchs. Nutzen Sie die Gelegenheit, Ihre Qualifikation abzurunden und zertifizieren zu lassen. Alle weiteren Seminarangebote und die Möglichkeit zur Online-Anmeldung finden Sie unter
http://www.secorvo.de/college

Veranstaltungshinweise

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

Januar 2013	
15.-17.01.	OMNICARD 2013 (in TIME berlin, Berlin)
31.01.	Eröffnung des Kryptologikums (KIT, ZKM & KA-IT-Si, Karlsruhe)
Februar 2013	
06.-07.02.	23. SIT-SmartCard-Workshop (Fraunhofer-Institut SIT, Darmstadt)
19.-20.02.	20. DFN-Workshop „Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
März 2013	
05.-09.03.	CeBIT (Deutsche Messe, Hannover)
11.-14.03.	CPSSE-Schulung (Secorvo College, Karlsruhe)
12.-15.03.	Black Hat Europe 2013 (Blackhat, Amsterdam/NL)
18.-21.03.	Security Engineering (Secorvo College, Karlsruhe)
April 2013	
09.-11.04.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
15.-19.04.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
16.-17.04.	Datenschutztage 2012 (Forum für Datenschutz, Wiesbaden)
23.-26.04.	PKI (Secorvo College, Karlsruhe)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Volker Hammer, Kai Jendrian, Michael Knopp, Sven Köhler.

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