secorvo
security consulting

Secorvo Security News

November 2010

Hybris kommt vor dem Fall

Seit dem 01.11.2010 gibt es den neuen „elektronischen" Personalausweis, der mit seinem kontaktlosen (Krypto-) Chip nicht nur die Speicherung zweier Fingerabdrücke sondern auch die Nutzung als Online-Ausweis und Signaturkarte ermöglichen soll. Dazu werden ein Kartenlesegerät sowie eine „AusweisApp" benötigt, die unter dem sperrigen Arbeitstitel „Bürger-Client" im Auftrag des BMI durch ein von Siemens geführtes Konsortium entwickelt wurde (SSN 12/2009).

Bereits am 21.09.2010 hatte der Chaos Computer Club medienwirksam demonstriert, dass die PIN durch einen Trojaner ausgespäht werden kann, sofern ein Kartenleser ohne eigene PIN-Tastatur verwendet wird. Das war in der Sache wenig überraschend; beim Online-Banking ist dieser Trojaner-Angriff lange bekannt. Der PC ist schließlich immer das schwache Glied in der Kette. Überraschend war allerdings die Reaktion der Bundesregierung: In einem Interview der FAZ versicherte die IT-Beauftragte der Bundesregierung Cornelia Rogall-Grothe („Bundes-CIO") am 01.11.2010: „Es gibt keine Sicherheitslücke. Vor Schadsoftware am PC kann sich jeder wirksam schützen, indem er Virenschutzprogramme benutzt und eine Firewall installiert. (...) Es ist die sicherste Technik, die es gibt."

Acht Tage später stellte das Bundesamt für Sicherheit in der Informationstechnik (BSI) die AusweisApp zum Download bereit. Und keine 24 Stunden später publizierte Jan Schejbal in seinem Blog ein fatales Sicherheitsleck: Die Update-Funktion der AusweisApp prüft nicht, ob das SSL-Zertifikat auch zu dem Server gehört, von dem das Update geladen wird, und entpackt es, ohne zuvor die Signatur zu prüfen. Seit dem 10.11.2010 findet man auf der AusweisApp-Seite nun einen Verweis auf eine Pressemitteilung des BSI, in der es heißt, dass in Kürze eine neue Version der AusweisApp verfügbar sein wird – nach „umfangreichen Tests".

Etwas spät für „die sicherste Technik, die es gibt".

Inhalt

secorvo
security consulting

Security News

Deep links am Ende?

Bereits am 29.04.2010 hat der Bundesgerichtshof ein wichtiges Urteil zur Frage der Verlinkung von Website-Inhalten unter Umgehung der Startseite (*deep link*) verkündet. Danach liegt ein Urheberrechtsverstoß vor, wenn Schutzmaßnahmen der verlinkten Seite den Willen erkennen lassen, keine Direktverlinkung gestatten zu wollen. Auf die Wirksamkeit der Maßnahmen kommt es dabei nicht an. Seit dem 10.11.2010 liegt nun die Urteilsbegründung vor. Mit der „Session-ID" genannten Entscheidung fällt der BGH hinter die sieben Jahre alte Paperboy-Entscheidung zurück, die *deep links* auf ungeschützte Inhalte für zulässig erklärt hatte.

In dem zu entscheidenden Sachverhalt bot die Klägerin im Internet Stadtpläne an. Einmalige Zugriffe über die Startseite waren kostenlos, die Nutzung durch Einbindung der Karte jedoch lizenzpflichtig. Zum Schutz wurden Session-IDs verwendet, die als Teil der weiterführenden URL beim Besuch der Startseite vergeben wurden. Die Beklagte überwand diese Maßnahme, indem sie via Skript eine Session-ID abholte und diese in die URL einband. Trotz der offensichtlichen Unwirksamkeit dieser Schutzmaßnahme sah der BGH hierin eine urheberrechtswidrige Umgehung.

Das Urteil wirft jedoch Fragen auf. Da nach der Begründung des BGH allein die Erkennbarkeit des Urheberwillens (unabhängig von der Wirksamkeit des Schutzmechanismus und der Umgehungsabsicht des „Verlinkers") für den Urheberrechtsverstoß wesentlich ist, bleibt offen, wie mit *deep links* rechtssicher umgegangen werden kann. Schließlich kann ein Urheber auch seinen Willen ändern und zunächst frei zugängliche Dokumente nur noch nach gebührenpflichtiger Anmeldung preisgeben – ist daher vom Verlinker zu fordern, dass er regelmäßig prüft, ob der Urheber seinen Willen geändert hat? Sollte er vor Einrichtung eines *deep link* zu Nachweiszwecken einen Snapshot der Startseite speichern, oder sich lieber gleich vertraglich mit dem Urheber einigen? Oder vielleicht sogar mit Blick auf mögliche Abmahn-Wellen ganz auf *deep links* verzichten? Letzteres wäre zweifellos nicht nur das Ende der Links in den SSN, sondern das Ende des Internet, wie wir es heute kennen.

Rundum sorgenreich

Am 15.11.2010 kündigte Facebook einen Unified-Messaging-Dienst für alle Benutzer an, der E-Mail, Chat und SMS vereinen soll. Keine ganz neue Idee – vor allem aber eine Kriegserklärung an die Freemailer Gmail, Yahoo, Hotmail, GMX und Web.de. Immerhin signalisierten über 28 Mio. Facebook-Nutzer, dass ihnen diese Ankündigung gefällt. Darunter dürften auch zahlreiche Deutsche User sein, deren Zahl sich im Jahresverlauf von etwa vier auf über acht Mio. täglich mehr als verdoppelt hat – jeder zehnte hierzulande verbringt im Schnitt 18 Minuten am Tag bei Facebook.

Dabei ist Vorsicht angeraten: Wie Google analysiert auch Facebook alle Nutzerdaten zur Erstellung von Profilen, um zielgruppenscharfe Werbung schalten zu können. Zudem kann bei einem Webmailer nicht ausgeschlossen werden, dass es der eine oder andere Administrator mit der Privatsphäre nicht so genau nimmt: Erst am 14.09.2010 hatte ein Blogger bekannt gemacht, dass ein (inzwischen ehemaliger) Google-Mitarbeiter offenbar mehrfach Gmail-Accounts von Teenagern mitgelesen und sich in deren Kommunikation eingeschaltet hatte.

Vor allem die Vielzahl der Dienste (Maps, News, Kalender, Textverarbeitung und Tabellenkalkulation, Fotoalbum, Kontaktnetzwerk und Messaging) versorgt den Anbieter mit einem präzisen Bild der Interessen, Neigungen, Vorlieben und sozialen Beziehungen seiner Nutzer, sowie inzwischen sogar deren Standort – besonders interessant, wenn die Dienste auf Smartphones genutzt werden. Die Informationen zu Facebooks neuem Messaging-Dienst, zum Datenschutz, zur Konfiguration der Privatsphäre und zur Sicherheit sollte man sich daher genau anschauen – vor der Anmeldung.

Geschütztes Smart Metering

Auf ihrer 80. Konferenz am 03./04.11.2010 forderten die Datenschutzbeauftragten des Bundes und der Länder Verbesserungen beim Datenschutz der Smart Meter (SSN 09/2010). So sollen bei der Messung des Stromverbrauchs anfallende Daten „unter ausschließlicher Kontrolle der Betroffenen verarbeitet und nicht mit [...] Personenbezug an Dritte übermittelt werden. Die Inanspruchnahme von umweltschonenden und kostengünstigen Tarifen darf nicht davon abhängig gemacht werden, dass Betroffene personenbezogene Nutzungsprofile offenbaren" – denn technisch ist eine Übermittlung der Zählerstände dafür nicht erforderlich.

Gängige Praxis ist hingegen eine Übermittlung des Zählerstandes in 15-min-Intervallen mit schriftlicher Einwilligung des Kunden. Diese setzt jedoch Freiwilligkeit und Widerruflichkeit voraus – er kann sich also weigern oder die Einwilligung später zurückziehen. Aus Sicht des Investitionsschutzes sind EVUs also gut beraten, auf datenschutzfreundliche statt einwilligungsbasierte Lösungen zu setzen. Zur Verbrauchsminimierung sind „Vor-Ort-Analysen" ohnehin kostengünstiger realisierbar.

Märchen von Übermorgen

Während sich die Praktiker freuen, dass mit der zunehmenden Verbreitung von Windows Vista/7 der Umstieg vom suspekt gewordenen SHA-1 auf den SHA-2 endlich in greifbare Nähe rückt, läuft bereits der Wettbewerb um den Ende 2012 zu kürenden SHA-3 (SSN 06/2009). Zwei der beteiligten Forscher gingen nun in Aufsätzen vom 04.10. und 12.11.2010 der Frage nach, wie sicher die SHA-3-Kandidaten vor Quanten-Computern sind, da sich dort mit dem Algorithmus von Grover der Brute-Force-Aufwand bei vielen Verschlüsselungs- und Einwegfunktionen von 2^n auf $2^{n/2}$ Operationen senken lässt.

Für Kryptologen ist das ein gewaltiger Unterschied – für die praktische Anwendung des künftigen SHA-3 allerdings etwa so relevant wie die Frage, ob ein neuer Sattel auch für das Reiten toter Pferde taugt: Falls es eines Tages Quanten-Computer gibt, sind dank Shors Algorithmus auch RSA und fast alle anderen Signaturverfahren sofort zu brechen.

Safe Harbor am Ende?

Der Düsseldorfer Kreis, die informelle Zusammenkunft der Datenschutzaufsichtsbehörden im nichtöffentlichen Bereich, hat sich am 28./29.04.2010 auf eine Prüfungspflicht für übermittelnde Stellen gegenüber Safe Harbor-Unternehmen in den USA geeinigt und dies am 23.08.2010 bestätigt. Da sich diese Unternehmen gegenüber der Federal Trade Commission (FTC) und europäischen Behörden lediglich selbst zertifizieren, findet eine Prüfung, ob die Safe Harbor-Grundsätze und ein angemessenes Datenschutzniveau eingehalten werden, nicht statt. Daher hat nach Auffassung des Düsseldorfer Kreises das übermittelnde Unternehmen die Pflicht, z.B. die Aktualität der Zertifizierung, die Erfüllung von Informationspflichten gegenüber Betroffenen und die ergriffenen Maßnahmen zur Einhaltung der Safe Harbor-Grundsätze selbst zu prüfen. Dies ist zu dokumentieren und auf Nachfrage den Aufsichtsbehörden nachzuweisen. Bestehen Zweifel an der Einhaltung der Grundsätze, wird die Verwendung der EU-Standardvertragsklauseln empfohlen.

Für deutsche Unternehmen gehen damit der Nutzen des Safe Harbor-Abkommens und die Rechtssicherheit bei der Übermittlung verloren. Die Forderung der Aufsichtsbehörden nach einer institutionellen Kontrolle der Selbstverpflichtungen ist berechtigt, sollte aber besser in eine Änderung des Abkommens statt in neue Prüfpflichten münden.

Happy Birthday Phrack!

Das Hacker-Magazin Phrack, nach Fyodor (Autor von Nmap) "the best, and by far the longest running hacker zine", feierte am 17.11.2010 seinen 25. Geburtstag. Pünktlich zum Termin erschien Heft Nr. 67 – knapp 1,5 Jahre nach Heft 66. Es enthält gewohnt unterhaltsames Material und technisch fundierte Artikel wie "Dynamic Program Analysis and Software Exploitation" oder eine detaillierte Schwachstellenanalyse im ProFTP-Server. Wir freuen uns auf die nächsten 25 Jahre – Thank you, Phrack Staff, and keep up the good work!

Bundesrat zum Datenschutz

Mit seinen umfassenden Änderungsvorschlägen zum Entwurf eines Gesetzes zum Beschäftigtendatenschutz hat der Bundesrat am 05.11.2010 eine erneute Überarbeitung des Gesetzesentwurfs eingefordert. So sollen Beschäftigtendaten enger definiert, auf europäischer Ebene Regelungen zum Konzerndatenschutz angestrebt, durch Verzicht auf ein Übermaß an Verweisen die Lesbarkeit verbessert, eine Löschfrist für die Daten abgelehnter Bewerber eingeführt und ein allgemeines Beschäftigten-Screening nur bei Vorliegen tatsächlicher Anhaltspunkte für das Vorliegen von Straftaten gestattet werden. Eine Änderung der Definition von Dritten soll die Auftragsdatenverarbeitung in EG-Drittstaaten ermöglichen. Die von Datenschützern und den Bundesratsausschüssen geforderte grundsätzliche Einschränkung der dauerhaften Videoüberwachung und der Möglichkeiten zur Abweichung in Tarifverträgen oder Betriebsvereinbarungen zu Ungunsten der Beschäftigten fanden zwar keine Mehrheit. Dennoch wird deutlich, dass der Gesetzentwurf noch einen weiten Weg vor sich hat.

Secorvo News

100 mal Security News

Sie lesen gerade die 100. Ausgabe der Secorvo Security News: 400 Seiten mit fast 1.000 Nachrichten, für Sie selektiert, recherchiert und formuliert, liegen damit hinter uns. Über 6.500 Abonnenten haben die News bis heute gewonnen – mehr als die meisten deutschsprachigen Fachzeitschriften im Gebiet Informationssicherheit und Datenschutz.

Wir würden uns freuen, wenn Sie das Jubiläum zum Anlass nähmen und uns in einem kurzen Kommentar verraten, was Sie uns schon immer einmal sagen wollten. Unter allen Einsendern verlosen wir am 31.01.2011 einen Teilnahme-Gutschein für ein Secorvo-College-Seminar nach Wahl.

Smart Grid Symposium

Am 01.-02.02.2011 sind wir mit einem Symposium zu Datenschutz- und Datensicherheit rund um das „Intelligente Stromnetz“ wieder in der Buhlschen Mühle zu Gast. Wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

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

Dezember 2010	
05.-09.12.	AsiaCrypt 2010 (IACR, Singapur/SGP)
06.-07.12.	IsSec/ZertiFA 2010 (Computas, Berlin)
27.-30.12.	27th Chaos Communication Congress (27C3) (Chaos Computer Club, Berlin)
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)

Fundsache

Am 05.02.2010 hat die EU-Kommission eine überarbeitete Fassung der Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (gemäß der EU-Datenschutzrichtlinie) verabschiedet (Amtsblatt der EU L 39/5 vom 12.02.2010), die seit dem 15.05.2010 in Neuverträgen sowie bei Vertragsänderungen zu berücksichtigen sind.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, 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