secorvo
security consulting

Secorvo Security News

November 2012

Überflüssig

„Nachweisbar, sicher, zuverlässig“. Klingt gut, was die Deutsche Telekom ihren De-Mail-Kunden verspricht. Allein – heißt das, dass T-Online-E-Mails weder sicher noch zuverlässig sind? 1&1 bewirbt De-Mail mit „sicherem digitalen Briefversand“ – muss man daran bei web.de, gmx und den E-Mail-Postfächern von Geschäftskunden zweifeln?

Der tatsächliche Vorteil von De-Mail gegenüber einer herkömmlichen E-Mail ist schnell benannt: Die Identität des Senders und vor allem der Empfang sind wie bei einem Einschreiben nachweisbar. Nutznießer sind daher in erster Linie die Absender: Mit der Aktivierung eines De-Mail-Accounts ermöglicht der Empfänger jedem De-Mailer eine nicht abstreitbare Zustellung. Anders als beim Einschreiben gilt die De-Mail jedoch als zugestellt, sobald sie im Postfach liegt – auch im Urlaub. Und damit starten auch etwaige Fristen.

Die wahren Profiteure sind jedoch die Provider: Ihnen bietet sich die einmalige Chance, den (D)E-Mail-Versand wie SMS transaktionsbezogen abzurechnen – und so am Rückgang des Briefverkehrs der Unternehmen zu Gunsten von E-Mails mitzuverdienen.

Das Geschäftsmodell hat jedoch einen Haken, wie jetzt auch die Telekom und 1&1 erkannt haben: Da eine De-Mail wie ein eingeschriebener Brief dem Sender in Rechnung gestellt wird, profitiert vor allem der Anbieter, der die Großversender (Versicherungen, Banken, Behörden) für den Dienst gewinnen kann. Telekom und 1&1 fordern daher eine Umsatzbeteiligung von der Deutschen Post, die die De-Mail derzeit bei ihren Geschäftskunden bewirbt.

Die Interessen der Endnutzer bleiben dabei auf der Strecke – darüber kann auch das „Schutzversprechen“ der De-Mail-Anbieter nicht hinwegtäuschen. Denn „sicher und zuverlässig“ sind (ggf. verschlüsselte) E-Mails auch ohne De-Mail. Und in den extrem seltenen Fällen, in denen eine Nachweisbarkeit erforderlich ist, genügt das gute alte Einschreiben vollauf. Hoffen wir, dass der Markt es richtet.

Inhalt

secorvo
security consulting

Security News

Das Tracking und die Standards

Beim „Tracken“ von Internet-Benutzern stehen sich Datenschützer und Werbewirtschaft scheinbar unversöhnlich gegenüber. Umso erstaunlicher die jüngsten Fortschritte bei technischen Ansätzen zur Abwehr von Tracking: So hat am 06.11.2012 auch Google die sehr versteckte Implementierung von „Do Not Track“ (DNT) für Google Chrome 23 angekündigt. Deutlich offensiver geht Microsoft vor, die mit dem Internet Explorer 10 DNT als Standard aktivieren. Damit haben sie eine hitzige Diskussion ausgelöst, die in einem Apache-Patch gipfelt, der die DNT-Option von IE 10 ignoriert.

Ergänzend hat das W3C am 02.10.2012 die Working Drafts für die Standards Tracking Preference Expression und Tracking Compliance and Scope veröffentlicht. Angesichts technischer Entwicklung, Standards und öffentlichen Diskussionen wächst die Hoffnung, dass sich DNT zu einem Werkzeug entwickelt, mit dessen Hilfe Benutzer ihren Willen zukünftig unmissverständlich und durchsetzbar zum Ausdruck bringen können.

Die Eltern und das Filesharing

Die Entscheidungen zur Störerhaftung des Anschlussinhabers bei Urheberrechtsverstößen sind seit dem 15.11.2012 um ein höchstrichterliches Urteil reicher. Mit der Feststellung, dass Eltern ihre Kinder zwar über Verbote aufklären müssen, dann aber bei Urheberrechtsverletzungen nicht wegen einer Aufsichtspflichtverletzung haften, hat der BGH eine weitere Streitfrage geklärt.

In dem entschiedenen Fall hatte der 13jährige Sohn der Beklagten 147 Audiodateien über einen längeren Zeitraum via Tauschbörse zum Download angeboten; die Icons der verwendeten Tausch-Software waren sogar auf dem Desktop seines Rechners zu sehen. Die Vorinstanzen hatten aus § 832 Abs. 1 BGB Aufsichtspflichten abgeleitet, die über eine einfache monatliche Verlaufskontrolle auf dem Rechner sowie die Installation eines „Security-programms“, das die Installation weiterer Programme verhindern sollte, hinausgingen: Danach hätten die installierten Programme über die Systemsteuerung überprüft werden müssen. Der BGH hat diese Pflichten auf Aufklärung reduziert, sofern mit der Einsichtsfähigkeit des Kindes zu rechnen ist.

Damit gewichtet der BGH zugleich das Gefahrenpotential des Internetzugangs als Schädigungsinstrument niedriger. Daher könnte das Urteil auch bei zukünftigen Entscheidungen zu den Pflichten von Internetanschlussinhabern zu zurückhaltenderen Forderungen führen.

Das BSI und die Macs

Lange hat sich zum Thema Mac OS beim BSI nicht viel bewegt – die Vorabversion des IT-Grundschutz-Bausteins MacOSx datiert vom Januar 2012. Aktuelle Mechanismen wie die Vollverschlüsselung vor allem mobiler Geräte mit FileVault 2 sucht man vergeblich. Am 15.10.2012 hat das BSI nun Empfehlungen zur sicheren Nutzung von Macs unter Apple OS X Mountain Lion veröffentlicht. Leider bleiben die Hinweise überwiegend oberflächlich oder schaffen Verwirrung: So widerspricht das Dokument den Empfehlungen des BSI im Anti-Botnet Beratungszentrum zum Einsatz von Virenschutzprogrammen unter Mac OS.

Dabei sollte man sich als Mac OS User besser nicht in Sicherheit wiegen – das belegt schon eine kurze Suche in der CVE-Liste. So lange weder Apple noch die NSA oder CISecurity aktuelle Security Guidelines für OSx veröffentlicht haben, bieten die Empfehlungen des BSI immerhin einen ersten Einstieg in die Sicherheitskonfiguration eines Macs.

Die Biometrie und die Software

Zumindest in Business-Laptops sind Fingerabdrucksensoren zur Benutzerauthentifikation inzwischen weit verbreitet. Sie vereinfachen das Betriebssystem-Login – und hinterlassen das gute Gefühl, den Laptop „biometrisch“ gesichert zu haben.

Tatsächlich ist es mit dem Schutz nicht ganz so weit her, wie schon am 28.08.2012 bekannt wurde: Geräte, die mit Sensoren der Firma UPEK ausgestattet waren, speichern die Windows-Passwörter ihrer Benutzer AES-verschlüsselt in der Registry – durch einen Implementierungsfehler allerdings so, dass es Mitarbeitern von ElcomSoft gelang, die Passwörter auszulesen.

Das wäre wenig mehr als ein Bug unter vielen – wenn da nicht die (inzwischen von der Webseite des Anbieters gelöschte) Liste der Hersteller wäre, die den UPEK-Sensor einsetzen: Acer, Asus, Dell, Gateway, Lenovo, MSI, NEC, Samsung, Sony und Toshiba. Sucht man auf der Webseite der (erst im Juli 2012 für 356 Mio. USD erworbenen) Apple-Tochter AuthenTec, zu der UPEC seit 2010 gehört, nach näheren Informationen, stößt man auf den lapidaren Hinweis: „AuthenTec's Smart Sensor products are no longer available.“

Gelöst ist das Problem (anders lautenden Ankündigungen zum Trotz) offenbar bisher nicht. Daher können wir nur dringend dazu raten, die entspre-

chenden Treiber zu deinstallieren und den Sensor nicht für das Windows-Login zu nutzen – selbst wenn die Festplatte des Rechners verschlüsselt ist.

Das OWASP und die DuD

Die OWASP AppSecUSA 2012 lockte am 25. und 26.10.2012 ca. 800 Interessierte nach Austin, und am 07.11.2012 trafen sich über 200 Teilnehmer beim OWASP Day Germany 2012 in München zum Thema sichere Webanwendungen. Beide Veranstaltungen zeichneten sich durch eine durchgängig sehr hohe Qualität der Vorträge und (den Teilnehmerzahlen sei Dank) vielfältige Möglichkeiten zum Networking aus. Die Vorträge aus München stehen inzwischen zum Download bereit. Die steigenden Teilnehmerzahlen unterstreichen die wachsende Bedeutung der Anwendungssicherheit. Interessierte finden auf den Seiten des deutschen Chapters der OWASP sowie im Schwerpunktheft 11/2012 der DuD einen guten Einstieg in das Thema.

Das Online-Banking und die mTAN

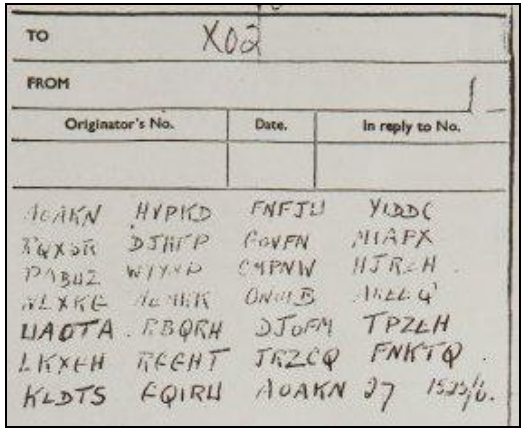
Am 13.11.2012 hat das Berliner Landeskriminalamt eine Warnung für Nutzer des mTAN- (oder SMS-TAN)-Verfahrens veröffentlicht. Diese Bedrohung ist nicht ganz neu – schon am 25.09.2010 hatte David Barroso in seinem Blog über Erweiterungen des Banking-Trojaners ZeuS zu einem „Man-in-the-Mobile"-Trojaner gewarnt (siehe auch Fundsache SSN 9/2010). Jetzt scheinen SMS-Trojaner deutsche Bankkunden im großen Stil ins Visier zu nehmen.

Der Angriff ist denkbar einfach – und hebelt den „getrennten Kanal" zur Übersendung der TAN vollständig aus. Der Trojaner fordert den Bankkunden am PC zum Download eines „Handy-Updates" auf – das anschließend dafür sorgt, dass jede SMS-TAN an den Angreifer weitergeleitet wird.

Gegen diesen Angriff ist nur ein einziges Kraut gewachsen: Die Geistesgegenwart des Nutzers. Denn strikte „Kanaltrennung" kann nur funktionieren, wenn niemals Software direkt oder indirekt über den (möglicherweise befallenen) PC auf das Smartphone übertragen wird.

Die Taube und die Nachricht

Die am 01.11.2012 von BBC News veröffentlichte verschlüsselte Nachricht, die in Südengland am Skelett einer Brieftaube gefunden wurde und wahrscheinlich von einem Sergeanten der Royal Air Force aus dem Ende des Zweiten Weltkriegs stammt, konnte bisher nicht entschlüsselt werden. Wer sich über Weihnachten daran versuchen möchte: Hier ist der Chiffretext.



Secorvo News

500 T.I.S.P.-Zertifkate

Jetzt ist es amtlich: Mitte November erhielt der 500ste T.I.S.P.-Absolvent sein Zertifikat. Das vom Bundesverband IT-Sicherheit (TeleTrusT) entwickelte Expertenzertifikat, das dreijährige Berufserfahrung in der IT-Sicherheit voraussetzt, hat sich damit als berufsqualifizierender Nachweis für Informationssicherheit durchgesetzt und genießt hohe Anerkennung.

Das von Secorvo verfasste, 500-seitige Begleitbuch zum T.I.S.P.-Seminar „Zentrale Bausteine der Informationssicherheit" (80 Euro) bietet eine Zusammenfassung des T.I.S.P.-Grundlagenwissens in 22 Kapiteln – eine unverzichtbare Lektüre für lange Winterabende. Wer sich zu einem T.I.S.P.-Seminar bei Secorvo anmeldet, erhält das Buch zur Vorbereitung übersandt. Nächster Termin: **15.–19.04.2013**.

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Eröffnung des Kryptologikums

In das kommende Jahr startet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit einem 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. Zur Einstimmung bieten wir um 16 und 17 Uhr eine Führung zur voll funktionsfähigen Zuse Z22 an, die im ZKM ausgestellt ist.

Wir freuen uns auf Ihre Teilnahme – und empfehlen Ihnen eine frühzeitige Anmeldung.

Veranstaltungshinweise

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

Dezember 2012	
03.-04.12.	IsSec/ZertiFa 2012 (Computas, Berlin)
27.-30.12.	29th Chaos Communication Congress (29C3) (Chaos Computer Club, Hamburg)
Januar 2013	
15.-17.01.	OMNICARD 2013 (in TIME berlin, Berlin)
31.01.	Eröffnung des Kryptologikum (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)

Fundsache

Jedes Kryptoverfahren ist immer nur so sicher wie seine Schlüssel – dieses Prinzip wird leider beim Design von Sicherheitslösungen allzu häufig missachtet. Am 16.11.2012 hat das US-amerikanische NIST als Special Publication SP 800-133 konkrete Empfehlungen zur Schlüsselgenerierung veröffentlicht – ein ‚Must Read' für jeden Systemdesigner.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), 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