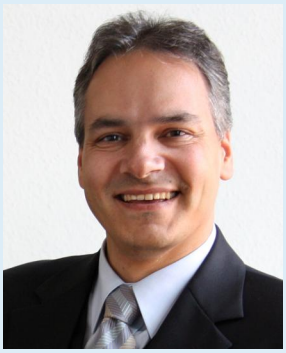
secorvo
security consulting

Secorvo Security News

September 2011



Wem ist noch zu trauen?

Kürzlich ließ sich eine Zertifizierung beobachten, die heftige Zweifel an der Praxis der Vergabe von Zertifikaten aufkommen lässt. Dabei handelte es sich nicht um den Commodo- oder DigiNotar-Hack, sondern um eine irreführende TÜV-Zertifizierung einer Billig-Wetterstation.

Der Vorfall wäre wenig mehr als eine amüsante Anekdote, wären nicht zahlreiche deutsche Webseiten und IT-Produkte mit ähnlichen TÜV-Siegeln verziert – so auch Version 9 des Internet Explorers (SSN 05/2011).

Zweifelhaft daran ist weniger die der Zertifizierung vorausgegangene Prüfung, denn diese ließe sich nur beurteilen, wenn bekannt wäre, *wofür genau* (IE9) oder *nach welchen Kriterien* (Wetterstation) die Prüfung erfolgte. In beiden Fällen schweigt der TÜV sich darüber jedoch aus: Betriebsgeheimnis. Und wie ist das mit den TÜV-Siegeln zahlreicher Webseiten? Welche Zusicherung ist mit einem solchen Siegel verbunden?

Transparenz ist gerade bei Prüfverfahren, die nicht nach internationalen Standards erfolgen, besonders wichtig, da ein Siegel andernfalls zu missbräuchlicher Verwendung einlädt – erst recht, wenn der Zertifizierer eigentlich im Ruf steht, sein Handwerk zu verstehen. Geheimniskrämerei oder Selbstgefälligkeit sind hier fehl am Platz – sie leisten nur Nachlässigkeit oder gar Betrug Vorschub.

Der Wert von Zertifikaten – ob vom TÜV oder von einer CA – beruht darauf, dass dem Aussteller vertraut wird, und dazu gehört, dass die Prüfung nach höchsten Maßstäben der Sorgfalt erfolgt. Fragwürdige oder gar irreführende Zertifizierungen können das Fundament jeder Vertrauensinfrastruktur ins Wanken bringen. Die TÜVs sind seit Jahrzehnten eine Institution, deren Name für Verlässlichkeit steht. Umso schlimmer ist es, wenn sich ausgerechnet der TÜV für zweifelhafte Siegel und Gutachten hergibt.

Wem soll man dann noch vertrauen?

Inhalt

secorvo
security consulting

Security News

Haftung bei Phishing

Das Landgericht Landshut hat am 14.07.2011 über die Haftung einer Bank nach einem erfolgreichen Phishing-Angriff auf das iTAN-Verfahren entschieden. Das Verhalten des Klägers, der gegenüber den Angreifern 100 TAN-Nummern durch Eingabe auf deren Seite preisgegeben hatte, wurde als fahrlässig, nicht aber als grob fahrlässig gewertet.

Nach § 675v Abs. 2 BGB haftet die Bank bei einem unautorisierten Zahlungsvorgang nur dann nicht, wenn der Kunde diesen betrügerisch, absichtlich oder grob fahrlässig ermöglicht hat. Grobe Fahrlässigkeit liegt bei einer Missachtung allgemein einleuchtender Überlegungen und einem damit einher gehenden diesbezüglichen schweren Verschulden vor. Die Unerfahrenheit des Klägers im Umgang mit Computern und seine sprachlichen Defizite mussten im vorliegenden Fall berücksichtigt werden.

Die Bank hatte ihre Kunden darauf hingewiesen, TANs nur zu verwenden, wenn zuvor *z. B.* eine Überweisung erfasst worden sei. Das Landgericht sah diesen Hinweis vor allem durch das „z. B." als zu unpräzise an, zumal der Trojaner SpyEye den Kläger auf eine Website lenkte, die äußerlich der Originalseite entsprach und die die nach dem Login geforderte TAN-Eingabe ausdrücklich als besondere Ausnahme darstellte. Erst recht könne die Bank dem Kläger nicht die Wahl des unsicheren von mehreren angebotenen Authentisierungsverfahren vorwerfen.

Für die Konstruktion von Trojanern stehen schon lange Baukästen wie Zeus bereit. Auch Smartphone-Betriebssysteme sind längst im Visier. Die Frage, ab welcher Grenze der Nutzer eine gestellte Falle erkennen muss, bleibt von den Umständen des Einzelfalls abhängig, doch mit steigender Qualität der Attacken wird die Chance der Banken schwinden, dem Kunden grobe Fahrlässigkeit vorzuwerfen. Sowohl Rechtsprechung als auch Gesetzgebung sind offenbar geneigt, dem Kunden ein hohes Maß an Unbesonnenheit zuzugestehen.

*Dis*Trust-Center

Über den Einbruch beim Trust-Center DigiNotar vom 17.06.-22.07.2011 (der ja nicht der erste Trust-Center-Einbruch war), den folgenden Lizenzentzug durch die niederländische Regierung am 14.09.2011 und die letztliche Liquidation des Unternehmens am 20.09.2011 wurde in verschiedenen Medien ausführlich berichtet. Was lehrt uns dieser Fall?

- Die Trust-Center-Branche betreibt nicht annäherungsweise ein Fraud-Management, wie es bei Finanz- und Zahlungsdienstleistern üblich ist. Ein Zertifikatsantrag für eine der weltweiten Top-Websites darf einfach nicht automatisiert ohne manuelle Prüfung zu einem Zertifikat führen.
- Das Krisenmanagement von GlobalSign, die angeblich ebenfalls kompromittiert wurden, war – Im Vergleich etwa zu RSA Security – geradezu vorbildlich und Vertrauen erweckend: Der Betrieb wurde gestoppt und häufige Updates zu den sofort eingeleiteten Sicherheitsuntersuchungen veröffentlicht. Eine seltene Ausnahme.
- Viele Trustcenter verschweigen schamhaft, wie viele ihrer qualifizierten Signaturzertifikate in Umlauf sind. In diesem Fall wurde es für DigiNotar öffentlich: 4.200.
- Der eigentliche Vertrauensanker für SSL/TLS sind nicht die Trust-Center, sondern die Browser-Hersteller, die deren Root-Zertifikate installieren oder löschen und jetzt schärfere Kontrollen fordern. Kaum ein Anwender kann sich die Mühe machen, etliche Dutzend vorinstallierter Roots (von denen viele noch nicht einmal mehr dem Unternehmen gehören, das sich vor Jahren im Root-Zertifikat „verewigt" hat) zu durchforsten.

Der letztgenannte Punkt könnte sich in den nächsten Jahren ändern, wenn TLS-Zertifikate per DANE über DNS verteilt werden. Dann würden die DNSSEC-Schlüssel der DNS-Root Zone zum Vertrauensanker für TLS – die Single Internet Root 2.0.

Konformes Google Analytics?

Kurz nachdem Prof. Dr. Caspar, Landesdatenschutzbeauftragter Hamburgs, das Verfahren des Reichweitenmessdienstleisters INFOnline (SSN 08/2011) als rechtskonform anerkannt hat, ist einer Pressemeldung vom 16.09.2011 nun auch seine Anerkennung der Anpassungen von Google Analytics zu entnehmen. Danach habe Google die Forderungen des Düsseldorfer Kreises vom 26./27.11.2009 durch die Verkürzung der IP-Adresse, das Bereitstellen eines Opt-Out-Verfahrens und seine Datenschutzhinweise erfüllt. Auf die Notwendigkeit späterer Anpassungen, sollte das Erfordernis eines Opt-In für die verwendeten Cookies eingeführt werden, wird am Rande hingewiesen.

Dennoch dürfen diese Aussagen nicht als Freifahrtschein für Webseitenanbieter verstanden werden. Jene werden zunächst die nach § 13 TMG geforderte Transparenz auf den Datenschutzerklärungen ihrer Webseiten herstellen müssen. Vor der Nutzung ist ein Auftragsdatenverarbeitungsvertrag abzuschließen und durch Löschung des alten Accounts für die Löschung der Altdaten zu sorgen.

Auch bei einer – vom Seitenanbieter zu veranlassenden – Kürzung der IP-Adressen bleibt die Datenverarbeitung im EG-Ausland ein Problem, das der Rechtskonformität durch Auftragsdatenverarbeitung im Weg steht. Selbst wenn der Webseitenbetreiber also seine Pflichten erfüllt (was sich der Überprüfung durch den Nutzer entzieht), bleibt die Rechtskonformität zweifelhaft, daher ist von einer Nutzung von Google Analytics weiterhin abzuraten.

Datenschutzkritik

Mit ihrem Einschreiten gegen eine Reihe von Diensten der Branchenriesen Google und Facebook haben Datenschutzbehörden in jüngster Zeit Schlagzeilen gemacht. In der Blogger-Szene werden die zweifelhaften Erfolge bereits als „Datenschutztheater" bezeichnet.

So sind das Verpixeln von einzelnen Häusern in Straßenzügen mit gleichartigen Reihenhäusern, die durchgesetzte Verkürzung von IP-Adressen unter gleichzeitiger Nutzung von mindestens gleichwertigen weiteren Identifikationsmerkmalen (Cookies) bei Tracking-Diensten oder die eher halbherzige Auseinandersetzung mit Facebooks Gesichtserkennung in der Tat Beispiele für „Datenschutzerfolge", die bestenfalls einzelne Symptome behandeln, das dahinter stehende Problem jedoch ungelöst lassen. Gleichzeitige Bestrebungen des Staates, eigene Datenbanken oder Überwachungsmittel wie die Vorratsdatenspeicherung neu oder wieder einzuführen, schwächen die Glaubwürdigkeit weiter.

Die Ziele des Datenschutzes angesichts immer vielfältigerer Mittel zur Verknüpfung von Informationen und einer Zunahme von verfolgbarem Kommunikationsverhalten umzusetzen wird nicht leichter, weder für den Gesetzgeber noch für die Exekutivorgane und Anwender. Es ist jedoch – und darin ist den Kritikern recht zu geben – dringend erforderlich, die vorhandenen Regeln konsequent umzusetzen. Auf der anderen Seite sind der Schutzbedarf und die angeordneten Mittel auf allen Ebenen zu überprüfen. Ansonsten droht eine substantielle Schwächung des Schutzumfangs der informationellen Selbstbestimmung.

Verkehr der Zukunft – eCall

In einer Empfehlung vom 08.09.2011 hat die EU-Kommission gefordert, anschließend an die europaweite Einführung der Notrufnummer 112 einen eCall als automatisierten Notruf aus Fahrzeugen einzuführen. Dieser Notruf mit einem standardisierten Minimaldatensatz soll von den Fahrzeugsystemen selbst erzeugt und genau wie ein 112-Notruf behandelt werden. Die Empfehlung gibt Definitionen und Standards vor, die eine europaweite Einheitlichkeit der Systeme sicherstellen sollen.

Eine Kommissionsempfehlung ist rechtlich unverbindlich, d. h. es ergibt sich hieraus keine Umsetzungsverpflichtung für die Mitgliedstaaten. Wird ein entsprechendes System eingeführt, sind die Maßgaben jedoch zu berücksichtigen. Die Einführung eines eCalls wird zur Einführung von eigenen Mobilkommunikationswegen in Fahrzeugen führen. Es ist absehbar, dass diese Entwicklung nicht beim eCall-Dienst stehen bleiben wird. Die entstehenden Datenschutz und Sicherheitsfragen werden daher künftig im Auge zu behalten sein.

Secorvo News

Secorvo College aktuell

Für die nächste T.I.S.P.-Schulung vom 17.-22.10. 2011 (einschließlich Prüfung) bei Secorvo College sind noch vier Plätze frei. Schnellentscheider erhalten unmittelbar nach Eingang der Anmeldung das Begleitbuch zum T.I.S.P. zur Prüfungsvorbereitung zugesandt (im Seminarpreis inbegriffen).

Im November folgen die Seminare PKI – Grundlagen, Vertiefung, Realisierung (08.-11.11.2011), IT-Sicherheit heute (15.-17.11.2011) und Certified Professional for Secure Software Engineering (CPSSE) mit anschließender Zertifikatsprüfung (22.-25.11. 2011). Die Programme aller Seminare, die Bewertungen unserer Teilnehmer und die Möglichkeit zur Online-Anmeldung finden Sie hier.

Security-Update 2011

Kein erfolgreiches Unternehmen kann sich mehr vor Angriffen auf seine Infrastruktur sicher wähnen. In einem Land, das seinen Erfolg Ideenreichtum und Wissen verdankt, setzt ein nachlässiger Umgang mit Daten jedoch die Zukunft aufs Spiel. Zwar wissen Unternehmen von diesen Risiken – allerdings ändern sich Bedrohungs- und Gesetzeslage ständig. Mit dem „Sicherheits-Update 2011„ am 05.10.2011 wollen LEITWERK, Secorvo und Securiton Abhilfe schaffen: Drei Expertenvorträge beleuchten die wesentlichen Fragestellungen – mit anschließender Gelegenheit zum Gedankenaustausch am Buffet.

Zweites Smart Grid Symposium

Vom 29. bis 30.11.2011 findet das "2. Smart Grid Symposium" in der Buhlschen Mühle in Ettlingen statt. Es erwarten Sie spannende Vorträge rund um Datenschutz und Datensicherheit im „intelligenten Stromnetz", u. a. vom Bundesamt für Sicherheit in der Informationstechnik (BSI), dem Bundesverband der Energie- und Wasserwirtschaft (BDEW) sowie der EnBW. Werfen Sie einen Blick in das Programm – wir freuen uns auf Ihre Anmeldung!

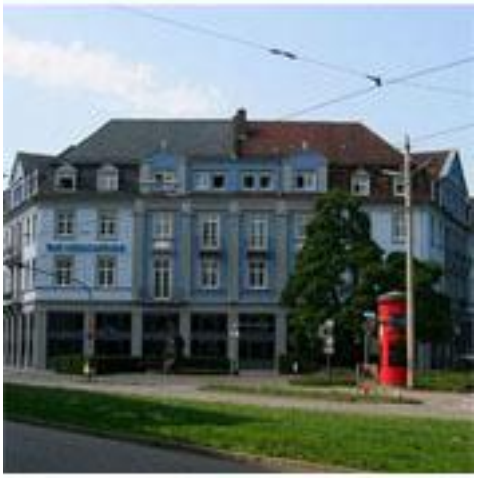
Veranstaltungshinweise

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

Oktober 2011	
05.10.	Security-Update 2011 (Leitwerk/Secorvo/Securiton, Appenweier)
11.-13.10.	it-sa (SecuMedia Verlag, Nürnberg)
17.-22.10.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
26.-29.10.	hashdays security & risk conference 2011 (DEFCON Switzerland, Luzern/CH)
November 2011	
08.-11.11.	PKI (Secorvo College, Karlsruhe)
11.11.	Outsourcing und Vendor Security (Gesellschaft für Informatik/Fachgruppe SECMGT, Frankfurt)
11.-13.11.	FIfF Jahrestagung 2011 zur Dialektik der Informationssicherheit (FIfF e.V., München)
15.-17.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
22.-23.11.	ISSE 2011 (TeleTrusT, Prag/CZ)
22.-25.11.	CPSSE (Secorvo College, Karlsruhe)
29.-30.11.	2. Smart Grid Symposium (Secorvo, KA-Ettlingen)
Dezember 2011	
05.-06.12.	IsSec/ZertiFA 2011 (Computas., Berlin)

Fundsache

Am 26.09.2011 hat das US-amerikanische NIST den Draft der Special Publication SP 800-153 "Guideline for Securing Wireless Local Area Networks (WLAN)" publiziert. Auf kompakten 12 Seiten gibt sie konkrete Empfehlungen zur Absicherung von WLANs – auch wertvoll für den privaten Router. Die Kommentierungsfrist endet am 28.10.2011.



Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Hans-Joachim Knobloch, 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