secorvo
security consulting

Secorvo Security News

September 2014

Nichts gelernt?

Diskussionen zur Inneren Sicherheit sind vermintes Gelände. Dort treffen – meist kraftvoll – Terroristenjäger auf Liberale und Datenschützer auf Nichts-zu-verbergen-Haber. Allem verbalen Hauen und Stechen zum Trotz ist aber in einem Punkt zumindest die heimliche Einigkeit groß: Auch wer „nichts zu verbergen" hat, mag sich nicht wie ein Staatsfeind behandeln lassen. Die eigenen E-Mails, SMS und Fotosammlungen möchte man als unbescholtener Bürger dann doch nur mit Personen des Vertrauens teilen – und nicht anlasslos mit unbekannten Staatsdienern.

So ist unstreitig, dass Kommunikationsdaten verschlüsselt gehören. Eigentlich keine große Sache – hätte man die Protokolle TCP/IP und DNS im Jahr 1981 gleich als das konzipiert, was sie heute sind: eine systemkritische Infrastruktur moderner Gesellschaften. Dann wären Verschlüsselungsmechanismen ein integraler Bestandteil des Internet und müssten nicht nachträglich aufgesetzt werden.

„Hätte, hätte, Fahradkette", würde Peer Steinbrück wahrscheinlich kommentieren. Denn einen wenigstens elementaren Schutz bei der Nutzung von Internet-Diensten hat nur, wer sich kümmert – zum Beispiel durch die Aktivierung von TLS beim Zugriff auf E-Mail-Konten oder die Verwendung von Chat-Programmen mit starker Verschlüsselung. Das ist, selbst für einen IT-Laien, so schwierig nicht. Angesichts des drastischen Vertrauenseinbruchs nach den Veröffentlichungen von Edward Snowden wäre eine spürbare Verhaltensänderung zu erwarten gewesen. Tatsächlich aber scheint die Wirkung schon wieder zu verblassen: das Vertrauen ins Internet wächst wieder, ohne dass sich substantiell viel geändert hat.

Mit unserer dritten „Anti-Prism-Party" wollen wir am 11.10.2014 erneut ein Zeichen gegen das „Weiter so" setzen, und hoffen, viele Tausend Besucher für eine sicherheitsbewusstere Nutzung des Internet zu gewinnen. Wer nicht kommen kann, dem sei unsere „Download"-Seite ans Herz gelegt.

Inhalt

secorvo
security consulting

Security News

Ende der Kulanz

Durch Online-Banking-Angriffe verursachte Schäden wurden bisher meist von den betroffenen Banken übernommen oder in außergerichtlichen Vergleichen geregelt. Auf die Zunahme von Phishing- und Trojanerangriffen haben die Institute in den vergangenen Jahren mit der Einführung neuer Schutzmechanismen wie SMS-TANs und TAN-Generatoren reagiert – und verweigern inzwischen gelegentlich die Schadensübernahme. Nun hat das LG Darmstadt in einem aktuellen Fall die Schadensersatz-Verweigerung mit Urteil vom 28.08.2014 bestätigt.

Da das von der beklagten Bank zur Verfügung gestellte Verfahren „Sm@rt-TAN-plus" eine Autorisierung der Überweisung mit Kennwort und EC-Karte fordere und die Überweisungsdaten auf dem TAN-Generator angezeigt würden, sei die Prüfung der Daten vor der Bestätigung der Transaktion (durch Eingabe der TAN) die Aufgabe des Kunden. Dieser müsse sich den durch die Verwendung der TAN entstandenen Rechtsschein zurechnen lassen, da die durch den Angreifer manipulierte Überweisung anhand der angezeigten Kontonummer und des Betrags für ihn erkennbar gewesen sei.

Es ist zu erwarten, dass Banken und Gerichte zukünftig die Verantwortung des Kunden bei Verwendung eines sicheren Online-Banking-Verfahrens höher ansetzen werden. Bei Schäden, die erst durch den leichtfertigen Umgang mit den Schutzmechanismen ermöglicht wurden, werden Verbraucher sich in Zukunft nicht mehr auf Kulanz und richterliches Wohlwollen verlassen können.

Meine grüne Welle

Auf der WOOT'14 (*8th USENIX-Workshop on Offensive Technologies*) stellten Forscher der Universität Michigan im August vor, wie verwundbar typische US-Verkehrsleitsysteme sind. Die untersuchten Ampeln kommunizieren über unverschlüsselte W-LAN-Kanäle, Voreinstellungen für Nutzername und Passwort wurden beibehalten, Kommandos des NTCIP-1202-Protokolls zur Verkehrssteuerung ließen sich per UDP an Ampelsteuerungen senden. Damit werden persönliche grüne Wellen und Verkehrsstaus auf Knopfdruck Wirklichkeit.

Eine ähnliche Verwundbarkeit der auch in Europa eingesetzten Verkehrsleittechnik von Sensys Networks zeigte Cesar Cerrudo, ebenfalls im August, auf der diesjährigen DEFCON. Das System erlaubt Code-Downloads ohne Integritätsprüfung und arbeitet ohne Verschlüsselung oder Authentisierung. Inzwischen liegen Software-Updates gegen die veröffentlichten Schwachstellen vor.

Da ausfallende Ampelsteuerungen ein Verkehrschaos auslösen können, werden Verkehrsleitsysteme in Deutschland zu Recht als kritische Infrastruktur angesehen. Dennoch ist auch hierzulande nach wie vor veraltete Technik im Einsatz. Auch hier ist Sicherheit ein Prozess, kein Zustand: Deshalb gehören regelmäßige Audits der Systeme, das Einspielen von Updates und Gespräche mit den Herstellern zu den regelmäßigen Aufgaben eines Sicherheitsmanagements.

Deutsche Post startet SIMSme

Am 13.08.2014 veröffentlichte die Deutsche Post AG ihren kostenfreien Messenger SIMSme. Nach anfänglichen technischen Schwierigkeiten läuft der Dienst inzwischen problemlos: Nutzer können Bilder, Nachrichten, Videos und andere Inhalte verschicken. Den Versand von Nachrichten, die sich wie bei Snapchat nach einer vorgegebenen Zeit selbstständig löschen, erlaubt ein 89-Cent-Upgrade.

Wie bei der oft empfohlenen schweizerischen WhatsApp-Alternative Threema werden die Daten Ende-zu-Ende-verschlüsselt, und das ausschließlich auf deutschen Servern. Der private Schlüssel kann bei einem persönlichen Treffen per QR-Code verifiziert werden. Eine anonyme Nutzung ist nicht möglich – zur Aktivierung benötigt man eine Telefonnummer. Ein Datenschutz-Patzer ist, dass der Sender mitgeteilt bekommt, wenn der Empfänger die Nachricht gelesen hat. Hier sollte die Post nachbessern und eine Deaktivierung dieser Funktion ermöglichen. Positiv sind hingegen die Nutzungsbedingungen hervorzuheben, die kompakt und übersichtlich gehalten sind. Im Gegensatz zu vielen insbesondere amerikanischen Anbietern verzichtet die Post darauf, sich Rechte an den Inhalten der Nutzer zu sichern.

Ein wenig Nacharbeit bei der handwerklichen Implementierungsqualität des aktuellen App-Releases sei der Deutschen Post allerdings angeraten: Vertrauen kann auch an Kleinigkeiten scheitern – zumindest bei Nerds.

OWASP Guides – reloaded

In diesem Sommer wurden zwei wichtige Arbeiten des OWASP zum Test von Anwendungen grundlegend überarbeitet. Am 11.08.2014 veröffentlichte OWASP Version 2.0 des Application Security Verification Standards (ASVS). Der ASVS dient zur Überprüfung der Umsetzung elementarer Sicherheitsmaßnahmen in Anwendungen und ist ein wichtiger Baustein sicherer Software. In die Überarbeitung sind zahlreiche Anmerkungen aus der Praxis einge-

flossen; die Lektüre lohnt sowohl für Anwendungsentwickler als auch für Tester. An Letztere wendet sich Version 4.0 des OWASP Testing Guide, der am 17.09.2014 publiziert wurde. Er enthält Praxistipps für die Durchführung von Sicherheitsüberprüfungen von Anwendungen.

Löschkriterien

Seit der Europäische Gerichtshof (EuGH) Mitte Mai die Suchmaschinenbetreiber als verantwortliche Stellen bestätigt (SSN 05/2014) und Betroffenen das Recht zugesprochen hatte, unter bestimmten Umständen die Löschung von Suchergebnissen zu verlangen, sind allein bei Google binnen vier Monaten 120.000 Anträge eingegangen. Da die Suchmaschinenbetreiber nicht allen Löschbegehren nachgekommen sind, sind zahlreiche Beschwerden bei den europäischen Datenschutzaufsichtsbehörden eingegangen.

Die Art. 29 Gruppe, das gemeinsame Gremium der europäischen Datenschutzaufsichtsbehörden, hat sich am 18.09.2014 nun auf erste Maßnahmen geeinigt. So wollen die Aufsichtsbehörden eine Übersicht über die von ihnen getroffenen Entscheidungen gewinnen und ähnliche, sowie besondere Fallkonstellationen identifizieren. Ziel ist die Entwicklung gemeinsamer Entscheidungskriterien. Auch wenn das kein einfacher Prozess werden dürfte, ist das allemal besser, als die Entscheidung den Suchmaschinenanbietern zu überlassen.

CrypTool 2.0

Das mehrfach preisgekrönte Krypto-Lernprogramm CrypTool erschien am 20.08.2014 in einer von rund 60 Open-Source-Entwicklern in siebenjähriger Entwicklungszeit rundumerneuerter Version 2.0. Die in Deutsch und Englisch verfügbare neue Version wird der Initiator und Gesamtprojektkoordinator, Herr Professor Esslinger, am 11.10.2014 auf der Karlsruher Anti-Prism-Party vorstellen (s. u.).

Secorvo News

Sichere Systeme sind möglich

Die Formulierung und Ausgestaltung angemessener Sicherheitsanforderungen an komplexe Systeme ist nicht trivial – aber möglich. Die Zertifikatsschulung Sichere Systeme dank System Security Engineering (T.E.S.S.) zeigt, wie Sicherheit erfolgreich in die Prozesse und Lebenszyklen der Systementwicklung integriert werden kann. Sie lernen aktuelle Standards, Vorgehensmodelle und Best Practices kennen und anwenden (17.-20.11.2014). Im Anschluss an die Schulung können Sie an der T.E.S.S. Prüfung teilnehmen, um Ihre erworbenen Kenntnisse mit dem T.E.S.S. Zertifikat bestätigen zu lassen. Speziell für die Entwicklung sicherer Software bieten wir die Zertifikatsschulung ISSECO Certified Professional for Secure Software Engineering (CPSSE) (20.-23.10.2014) an. Auf beiden Seminaren gibt es noch wenige freie Plätze.

Alle Termine und Seminarangebote sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Anti-Prism-Party, zum Dritten

Die „dritte Staffel“ der Anti-Prism-Party am **11.10.2014** findet anlässlich des Edward-Snowden-Stücks „Ich bereue nichts“ im Foyer des Badischen Staatstheaters Karlsruhe statt (ab 14 Uhr). Neben aktuellen Tipps und Empfehlungen rund um das Thema Selbstschutz im Internet wird das Kryptologikum des Karlsruher Instituts für Technologie (KIT) historische und zeitgenössische Verschlüsselungstechnik zum „Be-Greifen“ vorstellen. Ihre Kinder können Sie derweil in der Spion-Schule, die von der Pädagogischen Hochschule Karlsruhe betreut wird, zum Verschlüsselungsexperten ausbilden lassen oder zur Präsentation der KIT-Kinderuni schicken, die um 15 und 16:30 Uhr stattfindet. Krönender Abschluss ist ein Anti-Prism-Plenum um **19:30 Uhr** im Kleinen Haus des Staatstheaters Karlsruhe (Eintritt frei). Mehr zum Programm im APP-Newsletter.

„Das Buch“ auf der it-sa

Anlässlich des Erscheinens der zweiten, aktualisierten und erweiterten Ausgabe des T.I.S.P.-Buchs laden wir Sie am **07.-09.10.2014** herzlich zum Besuch unseres „T.I.S.P.-Buch-Stands“ auf der it-sa in Nürnberg ein. Sie finden uns in Halle 12 (Stand 12.0-646). Gerne lassen wir Ihnen einen Registrierungscode zukommen, mit dem Sie Ihr kostenfreies E-Ticket (Tageskarte) ausdrucken können. Schicken Sie uns bei Interesse bitte eine kurze E-Mail an security-news@secorvo.de.

Veranstaltungshinweise

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

Oktober 2014	
07.-09.10.	it-sa 2014 (NürnbergMesse, Nürnberg)
07.-09.10.	14. IDACON 2014 (WEKA-Akademie, Würzburg)
11.10.	Anti-Prism-Party, 3. Staffel (KA-IT-Si, Karlsruhe)
14.-17.10.	Blackhat Europe 2014 (Blackhat, Amsterdam/NL)
14.-15.10.	ISSE 2014 (TeleTrusT/eema, Brüssel/BE)
20.-24.10.	CPSSE – Schulung und Prüfung (Secorvo, Karlsruhe)
November 2014	
03.-04.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
03.-07.11.	Conference on Computer and Communications Security (CCS) (CASED/Fraunhofer SIT, Arizona/US)
10.-15.11.	T.I.S.P. – Schulung und Prüfung (Secorvo, Karlsruhe)
13.11.	Future IT-Kongress 2014 (AppSphere AG, Ettlingen)
17.-21.11.	Security Engineering – Schulung und T.E.S.S.-Prüfung (Secorvo, Karlsruhe)
20.-21.11.	38. Datenschutzfachtagung (DAFTA) (GDD, Köln)
Dezember 2014	
01.-02.12.	IsSec/ZertiFA 2014 (Computas, Berlin)
09.-10.12.	3. DFN-Konferenz Datenschutz (DFN-CERT Services, Hamburg)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Sven Köhler, Christoph Schäfer

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