secorvo
security consulting

Secorvo Security News

September 2013

Lasst euch nicht verwursten!

Freiheit ist ein kompliziertes Ding. Als „Abwesenheit von Zwang“ ist sie schlicht utopisch – der Begrenztheit von Ressourcen und der Endlichkeit des Lebens können sich Menschen nun einmal nicht entziehen. Auch gesellschaftlich stößt sie an Grenzen, und das nicht erst in der Freiheit des Anderen – Beschränkungen sind sogar essentielle Voraussetzung für reale Freiheit: Die Festlegung und Durchsetzung von Regeln definiert erst die Räume, in denen Freiheit stattfinden kann. Diese Freiräume wiederum sind vor ihrer Abschaffung zu schützen. Daher setzt das Grundgesetz – aus bitterer Erfahrung – in Art. 20 auch Regierung und Gesetzgebung klare Grenzen.

Umfang und Eingriffstiefe der Freiheitsbeschränkungen sind politisch umstritten: Wie viel soziale Umverteilung, Gängelung und Kontrolle müssen dem Souverän zugemutet werden, um seine Freiheit wirksam zu schützen? Unstreitig aber ist, dass Freiheit zentrale Voraussetzung ist für die persönliche Entfaltung (Art. 2 GG) – und allein diesem Zweck müssen Maßnahmen zur Erhaltung der inneren und äußeren Sicherheit in einer freiheitlichen Gesellschaftsordnung dienen. Sicherheit darf nie zum Selbstzweck werden, sondern ist ein (zweifellos wichtiger) Beitrag zur Freiheitsermöglichung.

Die schleichende Mutation des Internet zu einer Überwachungsinfrastruktur – durch Tracking, Profiling und den Zugriff von Sicherheitsbehörden – ist dabei, den offenbar noch immer unterschätzten Beitrag des Internet zur Entwicklung der Menschheit zu ersticken. Wer mit Brockhaus, Bibliothek und Bundesbahn aufgewachsen ist, der weiß, dass Wissen nie leichter zugänglich, Transparenz von Wirtschaft, Wissenschaft und Politik nie größer und die ortsübergreifende Zusammenarbeit von Menschen nie leichter war als heute. Wer diese Freiheit will, sollte sich dafür einsetzen. Mindestens durch Selbstdatenschutz. Einer der unsterblichen Cartoons F. K. Waechters (1937-2005) bringt es auf den Punkt: „Wenn ihr Schiss habt vor der Freiheit geht zurück in euren Stinkstall und lasst Euch verwursten!“

Inhalt

secorvo
security consulting

Security News

Zwiebel gegen Riesen

Staatliche Sicherheitsdienste wie die NSA scheinen mit juristischen Hebeln, viel Geld und Mittelsmännern jedermanns Privatsphäre über deren Spuren im Internet überwachbar machen zu wollen. Der NSA kommt dabei zugute, dass viele Internetriesen wie Google oder Facebook in den USA firmieren. Auch freie Projekte, wie der Anonymisierungsdienst TOR stehen im Fokus. Am 08.09.2013 zeigte die brasilianische Fernsehshow „Fantastico" NSA-Enthüllungsfolien, die suggerieren, dass TOR-Nutzer nicht völlig anonym sind. Nutzer älterer TOR-Versionen sind dabei wegen vermuteter Krypto-Schwächen besonders gefährdet. Auch könnte die NSA eigene TOR-Knoten betreiben. Jüngere wissenschaftliche Arbeiten zur Anonymität zeigen, dass die Nutzer-Anonymität auch durch die Auswertung von TOR-Datenströmen bedroht sein kann.

Wer Wert auf seine Privatsphäre legt, sollte sich daher nicht allein auf Anonymisierungsdienste verlassen, sondern sich bemühen, möglichst wenig Spuren zu hinterlassen (z. B. durch den Verzicht auf die Nutzung vor allem ausländischer Sozialer Netzwerke und die Sperrung von Tracking-Diensten im Browser) und seine Datenverbindungen wirksam verschlüsseln.

4get RC4

Den Veröffentlichungen vom 05.09.2013 zufolge kann die NSA einen großen Teil des (SSL-)verschlüsselten Datenverkehrs lesen. Details zu den betroffenen Verfahren, Protokollen oder Schlüssellängen wurden nicht publiziert, daher kann selbst der Experte Bruce Schneier, der über Hintergrund-Informationen verfügt, die Risiken nur spekulativ abwägen.

Eine plausible Spekulation ist, dass die NSA die RC4-Chiffre entschlüsseln kann, die zumindest beim Einsatz in WEP nachweislich gebrochen ist. Anwender, die diese Befürchtung teilen, können in Firefox, Chrome oder Internet Explorer die RC4-basierten SSL/TLS Cipher-Suites deaktivieren. Gegen BEAST und ähnliche Attacken, derentwegen RC4 von vielen SSL/TLS-Servern angeboten wird, gibt es andere Abhilfe, speziell auf Browser-Seite. Auch der am 24.09.2013 veröffentlichte Entwurf der neuen NIST Guidelines zu TLS (siehe Fundsache) sieht, anders als die am 13.03.2013 zurückgezogene Vorgängerversion, keine Nutzung des RC4 mehr vor.

Protest gegen PRISM

Am 05.09.2013 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder einen Beschluss zu den Berichten über die Telekommunikationsüberwachung durch ausländische Nachrichtendienste gefasst. Der Beschluss fordert die deutschen und europäischen Regierungs- und Legislativorgane auf, im nationalen und internationalen Recht einen umfassenden Schutz der Privatsphäre zu verankern. Verfassungswidrige Kooperationen deutscher Dienste seien aufzuklären und ggf. abzustellen. Es sei weiter zu prüfen, ob eine Begrenzung des Routings von europäischen TK-Verbindungen auf Netze innerhalb der EU möglich sei. Die anonymen Nutungsmöglichkeiten von Telekommunikationsangeboten seien auszubauen.

Angesichts der Überwachung seien Fluggastdatenabkommen und Überwachungsprogramm auf den Prüfstand zu stellen und völkerrechtliche Abkommen zum Datenschutz zu schließen oder Handel von einem ausreichenden Datenschutz abhängig zu machen. Im Gegensatz noch zu einer Presseerklärung vom Juli (SSN 7/2013) wird jedoch keine Aussetzung des Safe Harbor Abkommens oder der Anwendung Europäischer Standardvertragsklauseln gefordert. Insgesamt vermittelt die Entschließung eher den Eindruck von Hilflosigkeit.

Schutz vor Safträubern

Mobile Geräte sind – vor allem unterwegs – äußerst praktische Helfer. Wäre da nicht das Problem der Stromversorgung: Wer transportiert schon gerne Ersatz-Akku und Ladekabel in der Jackentasche. Praktisch, dass auf Konferenzen, Bahnhöfen usw. immer häufiger öffentliche Ladestationen zu finden sind. Doch Vorsicht: Schon auf der DEF CON 2011 warnte der IT-Sicherheitsexperte Brian Markus vor „Juice Jacking", dem Diebstahl von Daten während des Aufladens mobiler Geräte. Möglich wird dies, weil die Geräte meist ein USB-Kabel zum ‚Stromtanken' verwenden. Dabei werden fast immer auch Daten übertragen, denn die höhere Stromstärke ermöglicht ein schnelleres Laden. Übrigens funktioniert Juice Jacking auch ‚rückwärts' – ein manipuliertes Smartphone kann während des USB-Ladevorgangs auch auf die Daten des Strom spendenden Rechners zugreifen.

Schutz bietet das USBCondom des IT-Sicherheitsexperten Stephen A. Ridley, das dieser am 12.09.2013 per Twitter ankündigte. Der Adapter schleift nur Strom führende Anschlüsse durch, sodass keine Daten abgegriffen werden können. Wer viel unterwegs ist, sollte die Anschaffung des Adapters für 10 US$ erwägen.

Unerwünschte Werbung

Nach Verzicht des Bundesrats auf die Anrufung des Vermittlungsausschusses vom 20.09.2013 kann das

Gesetz gegen unseriöse Geschäftspraktiken in Kraft treten. Das Gesetz bringt Verschärfungen im Bereich der unerlaubten Werbung und Einschränkungen für die Abmahnungspraxis im Bereich des Urheberrechts.

Durch das Gesetz werden zunächst die Regelungen für unerwünschte Werbung durch eine Ergänzung der Definition der unzumutbaren Belästigung um die fehlende Kenntlichmachung von Werbung nach § 6 Abs. 1 TMG verschärft. Entscheidender ist jedoch die Verschärfung des möglichen Bußgeldes von 50.000 auf 300.000 Euro. Zur Begrenzung des Missbrauchs von Abmahnungen im Urheberrecht werden aus dem bislang weitgehend wirkungslosen § 97a UrhG die unbestimmten Rechtsbegriffe weitgehend gestrichen. Für private Nutzer werden die Abmahnkosten durch Festsetzung eines fiktiven Streitwertes (wie bereits beim ersten Gesetzentwurf geplant) auf etwa 100 Euro begrenzt. Außerdem wird der so genannte ‚fliegende Gerichtsstand' für Privatpersonen abgeschafft. Private Urheberrechtsverletzer müssen nun an ihrem Wohnsitz verklagt werden. Ausuferungen bei der Abmahnung von Urheberrechtsverletzungen wird hierdurch ein ernst gemeinter Riegel vorgeschoben.

Highlights der AppSecEU

Auf der mit über 400 Teilnehmern sehr gut besuchten OWASP AppSec Research 2013 EU in Hamburg (20.08.-23.08.2013) hielten Angela Sasse und Thomas Roessler wegweisende Keynotes. Angela Sasse setzte sich intensiv mit dem Spannungsfeld zwischen Security und Usability auseinander und gab zahlreiche Denkanstöße. Thomas Roessler zeigte die Herausforderungen auf, die mit der Einbindung von immer mehr Endgeräten ins WWW und dem Übergang von traditionellen Webanwendungen hin zu Rich-Client-Applications im Browser einhergehen: „Good-bye Web Security, welcome Web Application Security". Die Vorträge sind als Präsentationen und als Videos verfügbar.

Secorvo News

Rückblick

Wer die größte Verschlüsselungsparty Deutschlands am 05.09.2013 im ZKM Karlsruhe mit mehr als 600 Besuchern verpasst hat, darf sich auf die „zweite Staffel" freuen: Wegen der großen Nachfrage gibt es Anfang 2014 eine inhaltlich erweiterte Neuauflage – „Anti-Prism-Party 2.0". Bis dahin entschädigen vielleicht die Handouts und Anleitungen zu den vorgestellten Schutzmechanismen sowie die Zusammenstellung hilfreicher Links.

Verstärkung

Seit August 2013 verstärkt der Datenschutz-Experte Christoph Schäfer das Secorvo-Team. Er ist Wirtschaftsrechtler und GDD-zertifizierter Datenschützer mit über fünf Jahren intensiver praktischer Erfahrung als externer und interner Datenschutzbeauftragter.

Ausblick

Der ständigen Weiterentwicklung des Themas IT-Sicherheit trägt das Seminar IT-Sicherheit heute mit der Behandlung aktueller Fragestellungen Rechnung, das Secorvo College vom **12.-14.11.2013** anbietet. Hier erfahren Sie das Wesentliche über die aktuellen Entwicklungen und Bedrohungen, und lernen Best Practice-Vorgehensweisen kennen, mit denen Sie Ihr Unternehmen effizient schützen können.

Auf die wichtigste Ursache von Sicherheitslücken, nämlich fehlerhafte Software, zielt die Zertifikatsschulung CPSSE (**14.-17.10.2013**). Das Seminar vermittelt die Grundlagen der sicheren Software-Entwicklung; mit der Zertifikatsprüfung belegen Sie Ihre Qualifikation als *Certified Professional for Secure Software Engineering*.

Für alle Spezialisten, die sich mit Verschlüsselungsinfrastrukturen – auch als *Public Key Infrastructure* (PKI) bezeichnet – beschäftigen, ist unser Seminar PKI am **19.-22.11.2013** ein besonderer ‚Leckerbissen'. Von Konzeption über Aufbau und Betrieb vermittelt das Seminar für jede Fragestellung sowohl die wesentlichen theoretischen und praktischen Grundlagen als auch einen reichen Erfahrungsschatz aus 15 Jahren PKI-Projektarbeit.

Alle Termine und Seminarangebote – auch bereits für 2014 - sowie die Möglichkeit zur Online-Anmeldung finden Sie unter
http://www.secorvo.de/college

Wer hat, der hat.

Eher außerhalb des Wahrnehmungsbereichs der IT-Security bleibt in vielen Unternehmen das „Software Asset Management". Dabei lauern auch hier zahlreiche Gefährdungen. „SAM für Kenner" ist daher das Thema des nächsten KA-IT-Si Events am **07.11.2013** um 18 Uhr im Raum TelemaxX des CyberForum e.V. in Karlsruhe. Marcel Lepkojis (CONNECT Karlsruhe GmbH) wird in seinem Vortrag Sicherheitsaspekte des Software Asset Managements vorstellen und Schutzmaßnahmen empfehlen. Anschließend haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim Buffet-Networking.

Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

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

Oktober 2013	
08.-10.10.	it-sa 2013 (NürnbergMesse GmbH, Nürnberg)
14.-16.10.	13. IDACON (WEKA-Akademie, Würzburg)
14.-17.10.	CPSSE-Schulung (Secorvo College, Karlsruhe)
22.-23.10.	ISSE 2013 (TeleTrusT e.V./eema, Brüssel)
November 2013	
07.11.	Wer hat, der hat. (KA-IT-Si, Karlsruhe)
12.-14.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
13.-15.11.	37. DAFTA (GDD, Köln)
14.-15.11.	Smart Energy 2013 (Fachhochschule Dortmund)
14.11.	Future IT-Kongress 2013 (AppSphere AG, Ettlingen)
18.-21.11.	OWASP AppSec USA 2013 (OWASP Foundation, New York)
19.-22.11.	PKI (Secorvo College, Karlsruhe)
21.-22.11.	DeepSec ISDC 2013 (DeepSec GmbH, Wien)

Fundsache

Das NIST hat am 24.09.2013 den 64seitigen Draft einer Neufassung der Special Publication 800-52 zur Auswahl und Konfiguration von SSL/TLS-Implementierungen veröffentlicht. Auch wenn mancher angesichts der Verflechtungen von NIST und NSA die Guidelines mit Vorsicht genießen wird, spiegeln sie doch den State-of-the-Art (soweit öffentlich bekannt) wider. Obendrein gibt der Anhang einen Überblick über die Ansätze zur Überwindung der anderen Misere von SSL/TLS: dubiosen Trustcentern und fragwürdigen Serverzertifikaten (vgl. u. a. SSN 09/2011).

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, 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