secorvo
security consulting

Secorvo Security News

Januar 2015

Déjà-vu

„Kryptoregulierung“ nannte sich die Debatte vor 20 Jahren, „Verschlüsselungsverbot“ war gemeint. Nun hat der britische Premier diese Büchse der Pandora wieder geöffnet, und ein westlicher Politiker nach dem anderen schiebt sich in seinen Windschatten. Flankierend ruft der Bundesinnenminister nach Vorratsdatenspeicherung, die der Justizminister noch tapfer zu verhindern sucht.

Wie nach 9/11 ziehen nach dem feigen Pariser Mordanschlag nicht nur konservative Politiker reflexartig Ermächtigungen für Strafverfolger und Geheimdienste aus den Schubladen. Damals bescherte es der Welt den „USA Patriot Act“, Rechtsgrundlage der von Edward Snowden aufgedeckten NSA-Überwachungsmaßnahmen.

Keine Frage: Auch wenn die Zahl der Terror-Opfer verglichen mit den Verkehrstoten (in Deutschland: 180 bis 380 – pro Monat) klein wirkt – gegen Morde im Namen totalitärer Überzeugungen muss sich eine Demokratie wehren. Terror will Angst schüren, will offene Gesellschaften zwingen, sich zur Trutzburg zu machen und ihr vermeintlich „totalitäres Antlitz“ zu zeigen – um rückwirkend das eigene Weltbild und Morden zu rechtfertigen. Eine offene Gesellschaft, die auf Terror mit Überwachung reagiert, anlassunabhängig Daten speichert und die Vertraulichkeit der Kommunikation aufhebt, in der vagen Hoffnung, dass sich ein zukünftiger Anschlag verhindern lässt, begeht Selbstmord aus Angst vor dem Tod. Terroristen halten sich nicht an nationale Verschlüsselungsverbote, und die französische Vorratsdatenspeicherung hat den Anschlag auch nicht verhindert.

Für einen Politiker mag es schwer zu akzeptieren sein, dass eine offene Gesellschaft bestimmte Gefahren ertragen muss. Dabei wusste schon Benjamin Franklin 1775: “*They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety.*” Leider stimmt aber wohl auch Ingeborg Bachmanns ernüchternde Einsicht: „*Die Geschichte lehrt dauernd. Aber sie findet keine Schüler.*“

Inhalt

Déjà-vu

Security News

Würdiger TrueCrypt-Nachfolger?

Bußgeld für Tippsammler

Umsetzungsdefizit

IT-Grundschutz-Kataloge

DIN-Norm Löschkonzept

Vorwärts, E-Health

Secorvo News

Weiterbildung 2015

Ei des Kolumbus – oder Kuckucksei?

Lesestoff

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

Würdiger TrueCrypt-Nachfolger?

Das Ende der beliebten Kryptografie-Software TrueCrypt kam unerwartet und unter nach wie vor unklaren Umständen. Ob man aufgrund der Warnung „*Using TrueCrypt is **N**ot **S**ecure **A**s it may contain unfixed security issues*“ tatsächlich auf eine Einflussnahme der Geheimdienste schließen muss, bleibt Verschwörungstheoretikern überlassen. Mit VeraCrypt der französischen Firma IDRIX wird nun ein auf dem TrueCrypt-Code basierender Nachfolger unter Ms-PL als Open-Source-Lösung angeboten. Version 1.0f-1 vom 30.12.2014 besitzt einen „TrueCrypt Mode“, mit dem alte TrueCrypt-Volumen eingebunden werden können.

VeraCrypt macht keinen Hehl aus seiner Herkunft – optisch erinnert es stark an den Vorgänger. Dank einer wesentlich höheren Anzahl an Iterationen beim Passwort-Hash sei es besser gegen Brute-Force-Angriffe geschützt, erläutert der Entwickler.

Kann man VeraCrypt vertrauen? Ein positives Signal ist die Veröffentlichung unter Open-Source-Lizenz, allerdings fehlt bislang eine Code-Analyse, wie es sie zuletzt für TrueCrypt gab (SSN 04/2014).

Bußgeld für Tippsammler

An Kunden zu gelangen kann ein aufwendiges Unterfangen sein. In der Versicherungsbranche setzt man u. a. auf sogenannte Tippgeber, die dem Vertrieb potentielle Neukunden aus dem Freundes- oder Kollegenkreis nennen. Dieser für Branchenfremde eher wundersame Vorgang wird sogar vom Gesetzgeber anerkannt (vgl. BT-Drs. 16/1935, S.17).

Übertrieben hat es allerdings die Debeka. Jahrelang waren Tippgeber eine übliche Praxis, bis sich im Herbst 2013 der rheinland-pfälzische Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI) damit beschäftigte. Entgegen offizieller Weisungen hatten Debeka-Mitarbeiter Kontaktdaten potentieller Kunden teilweise entgeltlich erworben, ohne dass diese zuvor eingewilligt hatten. Damit wurden Kundendaten ohne eine gültige Rechtsgrundlage erhoben.

In seiner Pressemitteilung vom 29.12.2014 teilt der LfDI mit, dass die Debeka eine Geldbuße in Höhe von 1,3 Mio. € wegen Verletzung von datenschutzrechtlichen Bestimmungen akzeptiert hat. Außerdem richtet die Debeka für 600.000 € eine Stiftungsprofessur für Datenschutz in Mainz ein. Die Datenschutzaufsichtsbehörde folgt damit ihrem Kurs, bei kleineren Verstößen auf Einsicht zu setzen, bei systematischen allerdings die Bußgeldkeule zu schwingen. Durch den Debeka-Vorfall wurde auch die BaFin aufgeschreckt, die den Versicherungsvertrieb nun künftig stärker regulieren will.

Umsetzungsdefizit

Technischer Datenschutz ist kein neues Konzept, aber noch lange nicht allgemeine Praxis. Anlässlich Art. 23 der geplanten Datenschutz-Grundverordnung, der Datenschutz durch Technik zu einer Ausschreibungsvoraussetzung und Anforderung für Auftragsdatenverarbeiter erhebt, hat die ENISA (*European Union Agency for Network and Information Security*) am 12.01.2015 einen Empfehlungsbericht vorgelegt.

Er soll Datenschutzaufsichtsbehörden und verantwortlichen Stellen als Referenz zum aktuellen Stand der Technik dienen. Dementsprechend enthält der Bericht eine Reihe von datenschutzrelevanten Technikmaßnahmen: von Authentifikationsmethoden über Verschlüsselung und Anonymisierungsdienste bis hin zu Zukunftstechnologien wie homomorper Verschlüsselung oder *Secure Multi-party Computation*. Er umfasst außerdem eine Auflistung von Datenschutzstrategien, eine Anleitung zur Bewertung von Datenschutzgütesiegeln und Empfehlungen für Gesetzgeber, Standardisierungsgremien, Wissenschaft und Softwarehersteller.

Leider bleiben die Empfehlungen sehr allgemein und unbestimmt in Inhalt und Adressaten. Als Diskussionsgrundlage enthält der Bericht jedoch viele Anregungen.

IT-Grundschutz-Kataloge

Am 19.12.2014 hat das BSI die 14. Ergänzungslieferung der IT-Grundschutz-Kataloge veröffentlicht. Darin stechen vor allem die neuen Bausteine zum Cloud-Computing und für Allgemeine Anwendungen hervor. Damit nimmt sich das BSI wichtiger aktueller Themen in Sicherheitskonzeptionen an. Überarbeitet wurden die Themen Mobilkommunikation und Awareness.

Bisher stehen die Kataloge nur als PDF-Version zum Download zur Verfügung. Eine HTML-Fassung und ein Update der Metadaten für das GSTOOL sind noch nicht verfügbar. Die Prüfgrundlagen für eine Zertifizierung berücksichtigen in der auf der BSI-Seite veröffentlichten Version 2.81 vom 19.02.2014 die 14. Ergänzungslieferung ebenfalls noch nicht. Bei anstehenden BSI-Grundschutz-Zertifizierungen sollte man sie dennoch bereits berücksichtigen.

DIN-Norm Löschkonzept

Ende 2013 starteten die Unternehmen Deutsche Bahn, DATEV, Blancco, Secorvo und Toll Collect ein

gemeinsames Projekt, um die Leitlinie Löschkonzept zu einer DIN-Norm weiterzuentwickeln (SSN 02/2014). Seit dem 09.01.2015 liegt ein Entwurf der Norm 66398 vor und kann auf dem Entwurfsportal des DIN kommentiert werden. Die Norm soll im Herbst 2015 verabschiedet werden. Bereits der Normentwurf gibt wesentliche Hilfestellung für die Entwicklung eigener Löschkonzepte.

Vorwärts, E-Health

Das Bundesgesundheitsministerium hat am 13.01. 2015 einen Referentenentwurf für ein Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz) vorgelegt.

Der Gesetzesentwurf schreibt die Einführung der elektronischen Gesundheitskarte als Ersatz für die Krankenversicherungskarte im Sozialgesetzbuch V (SGB V) fest und droht der Gesellschaft für Telematik mit Zahlungssanktionen, wenn sie die Fristen zur Umsetzung der Infrastruktur nicht einhält. Weite Teile des Gesetzes gelten der Ergänzung und Anpassung der Aufgaben der Gesellschaft für Telematik sowie den Verfahrensbestimmungen für Zulassungs- und Schlichtungsverfahren. In den §§ 291f ff SGB V sollen zudem erste Anwendungen wie der elektronische Entlassbrief und elektronische Briefe geregelt werden.

Bestimmungen zur Datensicherheit und zum Datenschutz sind dagegen nur wenig und nur in sehr allgemeiner Form zu finden, was bereits die Kritik des ULD Schleswig-Holstein auf sich gezogen hat. Zu wünschen wäre hier mehr Ausgewogenheit, denn die Sicherheit der mit der elektronischen Gesundheitskarte verbundenen Anwendungen ist ein wesentliches Akzeptanzkriterium.

Secorvo News

Weiterbildung 2015

Die zentralen Bausteine der Informationssicherheit stehen im Mittelpunkt des T.I.S.P. (TeleTrusT Information Security Professional) vom 09.-13.03.2015. Wenn Sie bereits mehrjährige Berufserfahrung im Gebiet IT-Sicherheit, Informationssicherheit oder Datenschutz haben, können Sie Ihre Kenntnisse mit dem T.I.S.P.-Zertifikat bestätigen lassen. Darauf werden Sie von einem Experten-Team in einem fünftägigen Seminar vorbereitet, das zusammen über 200 Jahre Berufserfahrung verfügt. Diese Expertise hilft Ihnen, Ihr Wissen zu festigen und zu vervollständigen.

Wer sich aktiv mit dem Thema PKI in Unternehmen oder Verwaltung beschäftigt und einen produktunabhängigen Überblick sowie vertiefende Antworten sucht, kommt um diese PKI-Schulung nicht herum. Hier lernen Sie das Thema PKI aus vielen verschiedenen Blickwinkeln kennen. Die Referenten wissen aus zahlreichen Realisierungsprojekten, worauf es bei der Konzeption, dem Aufbau und dem Betrieb einer PKI ankommt. Ihre Erfahrung und ihr Wissen haben wir in diesem Seminar gebündelt. Nutzen Sie die Gelegenheit vom 21.-24.04.2015 in Karlsruhe.

Ei des Kolumbus – oder Kuckucksei?

IT-Outsourcing in „die Cloud“ liegt im Trend. Die Anbieter locken mit skalierbaren und anpassungsfähigen Anwendungen und Infrastrukturen. Hard- und Software befinden sich ganz oder teilweise in den Rechenzentren des Anbieters. Auch kurzfristige Anpassungen an den tatsächlichen Bedarf sind oft viel schneller möglich als beim klassischen Outsourcing. Höhere Flexibilität bei geringeren Kosten ist die gewünschte Folge.

Eine solche Lösung ist auch Microsoft Office 365, bei dem die Anwendung aus der Microsoft-Cloud bezogen und Dokumente und E-Mails in Microsoft-Rechenzentren gespeichert werden. Doch wie verträgt sich das mit dem Datenschutz? Auf der kommenden KA-IT-Si Veranstaltung am **19.03. 2015** im CyberForum e.V. werden die datenschutzrechtlichen Hürden und Gestaltungsmöglichkeiten vorgestellt. Anschließend gibt es – wie gewohnt – Gelegenheit zum „Buffet-Networking“. Anmeldung unter www.ka-it-si.de.

Lesestoff

Noch ist es abends früh dunkel – die richtige Jahreszeit, um zu einer guten Lektüre zu greifen. Neben dem neu aufgelegten T.I.S.P.-Buch (als Hardcover oder pdf) – hier finden Sie eine Leseprobe – gibt es auch einige aktuelle Publikationen von Secorvo, die wir Ihnen ans Herz legen, wie z. B. den Beitrag von Dirk Fox über die Hintergründe der NSA-Überwachung von SSL/TLS in Ausgabe 2/2015 der DuD. Eine vollständige Liste unserer Publikationen finden Sie in unserer Publikationsübersicht.

Und auch hören können Sie Secorvo – z. B. Dr. Safuat Hamdy auf dem 14. Deutschen IT-Sicherheitskongress des BSI am 21.05.2015 in Bonn-Bad Godesberg zu Datenschutzaspekten in IPv6.

Veranstaltungshinweise

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

Februar 2015	
04.-05.02.	25. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
24.-25.02.	22. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
März 2015	
03.-05.03.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen, Schutzmechanismen (Secorvo, Karlsruhe)
09.-13.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
23.-26.03.	2nd DFRWS EU Conference (DFRWS, Dublin/IE)
April 2015	
14.-15.04.	Datenschutztage 2015 (FFD Forum für Datenschutz, Wiesbaden)
21.-24.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
22.-23.04.	Security Forum 2015 (Hagenberger Kreis, Hagenberg/AT))

Fundsache

Am 17.12.2014 veröffentlichte das BSI den Bericht zur Lage der IT-Sicherheit in Deutschland 2014. Er führt Entwicklungen bei Angreifern und Vorfälle bei Privatanwendern und in der Wirtschaft auf und zeigt Lösungsansätze. Besonders spannend ist die Darstellung eines gezielten Angriffes auf ein Deutsches Stahlwerk, das Opfer einer so genannten *Spear-Phising*-Attacke war. Steuerungskomponenten wurden so manipuliert, dass an einer Hochofenanlage erheblicher Schaden entstand.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Kai Jendrian, Michael Knopp, Christoph Schäfer, Dr. Volker Hammer

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