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

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 homomorpher 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.

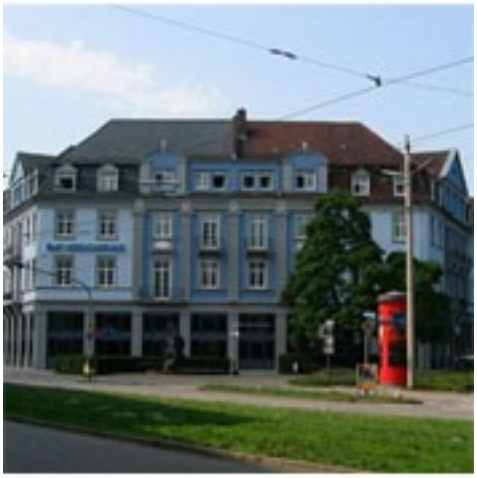
Veranstaltungshinweise

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Februar 2015

Why privacy matters.

Der Amerikaner *Glenn Greenwald*, Jurist, Blogger und seit Juni 2012 Journalist der britischen Tageszeitung The Guardian, bekam als einer der ersten Edward Snowdens Materialien zu Gesicht.

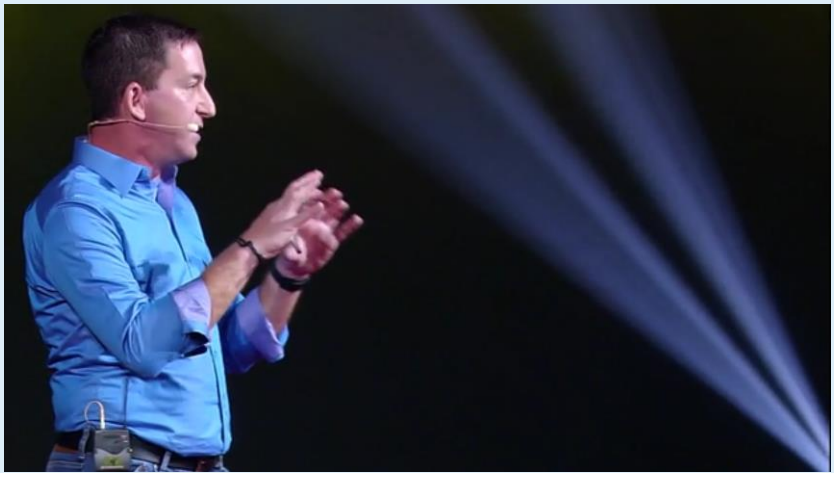
Snowden hatte ihn mit Bedacht gewählt: 2009 war Greenwald mit dem Izzy Award for Independent Journalism ausgezeichnet worden, 2010 erhielt er den Online Journalism Award for Best Commentary für seinen damaligen Blog Salon.com.

Anfang 2014 initiierte er mit finanzieller Unterstützung des Ebay-Gründers *Pierre Omidyar* das Portal „The Intercept", dessen Ziel es ist, „*auf Pressefreiheit zu bestehen und sie gegenüber denjenigen zu verteidigen, die diese verletzen.*"

Am 07.10.2014 hielt Glenn Greenwald eine Rede auf der Konferenz TEDGlobal 2014 in Rio de Janeiro. Sein Titel: „Why privacy matters".

Es ist eine brilliante Rede: Ein Muss für jeden, der meint, Datenschutz sei wohl eher etwas für diejenigen, die etwas zu verbergen haben. Und für alle anderen ebenfalls. Zum Nachlesen existiert eine deutsche Übersetzung.

Es ist eine Rede, bei der sich jeder weitere Kommentar erübrigt.



Inhalt

secorvo
security consulting

Security News

ISO-Norm für Datenschutz

Am 30.07.2014 wurde die ISO/IEC 27018 als neuer internationaler Standard für den Datenschutz in der Cloud veröffentlicht. Der Standard orientiert sich im Wesentlichen an den Schutz- und Überwachungspflichten des europäischen Datenschutzrechts. Wie das Bundesdatenschutzgesetz fordert er die sorgfältige Auswahl des Dienstleisters. Auch Anforderungen an die Auftragsdatenverarbeitung aus § 11 BDSG sind bereits enthalten; beispielsweise dürfen personenbezogene Daten ausschließlich nach den Vorgaben des Kunden verarbeitet werden und es muss transparent sein, in welchen Ländern die Verarbeitung erfolgt.

Am 16.02.2015 ging Microsoft in die Offensive und gab bekannt, dass das British Standards Institute (BSI) die ISO-27018-Konformität der Cloud-Services Azure, Office 365 und Dynamics CRM Online bestätigt hat. Die Beauftragung eines nach ISO/IEC 27018 zertifizierten Dienstleisters bestätigt – unabhängig von der unklaren Perspektive der EU-Datenschutz-Grundverordnung – zumindest die unternehmerische Sorgfalt bei der Auswahl.

Libellen im Kraftwerk

Schon seit 2013 sind Industrieanlagen der Pharmabranche Ziel der Malware Dragonfly, Warnmeldungen gibt es jedoch erst seit dem vergangenen Jahr. Dragonfly nutzt Spear-Phishing-E-Mails mit viralen Anhängen gefolgt von Malware-Ködern auf Branchen-Webseiten – kombiniert mit infizierten Software-Updates auf Webseiten vertrauter Produkt-Lieferanten wie dem Routerhersteller eWON. In einem Whitepaper vom 09.12.2014 analysiert Joel Langill die Wirksamkeit üblicher Schutzmaßnahmen gegen Dragonfly. Nach bisherigen Erkenntnissen sind Patch-Management, Application-Listing oder VPNs nutzlos. Der Bericht stellt sieben wirksame Techniken vor, die gegen solche Angriffe in der Lieferkette helfen. Zwei der wichtigsten sind:

- Detaillierte Sicherheitsanforderungen an alle Lieferanten, insbesondere bei Fernwartung – Dragonfly attackiert gezielt kleine Dienstleister, die IT-Sicherheit eher ‚pragmatisch' sehen.
- Nutzung von Industrie-Sicherheitsstandards und Isolation durch Netzwerksegmentierung – Dragonfly sucht nach erreichbaren OPC-Servern, die den Datenaustausch zwischen Automatisierungsanwendungen steuern.

Der Angriff zeigt, wie gefährlich es inzwischen ist, „Legacy"-Systeme z. B. im Anlagenbereich von strikten Sicherheitsvorgaben auszunehmen.

Outsourcing und Berufsgeheimnis

Auch Rechtsanwälte, Steuerberater und Ärzte setzen zunehmend Dienstleister ein, um personenbezogene Daten zu verarbeiten. Zu den datenschutzrechtlichen Anforderungen der Auftragsdatenverarbeitung (§ 11 BDSG) kommen hier die strengen Regeln des Berufsgeheimnisses hinzu (§ 203 StGB).

Dennoch finden sich in der Presse regelmäßig Berichte über sensible Daten im Altpapier. Besonders schwer wiegt dies bei Patientendaten wie jüngst in Bayern, wo Röntgenbilder am Straßenrand entdeckt wurden, mit deren Entsorgung ein Krankenhaus einen Dienstleister beauftragt hatte. Die Bayerische Datenschutz-Aufsichtsbehörde äußerte sich am 19.02.2015 unmissverständlich zum Outsourcing im Krankenhaus: Im Regelfall sei das unzulässig. Nach Auffassung der baden-württembergischen Datenschutzaufsicht gibt es nur zwei Lösungen für die Auslagerung der Datenlöschung: Der Dienstleister vernichtet mit einem mobilen Schredder vor Ort oder ein Mitarbeiter des Krankenhauses begleitet den Transport und überwacht die Vernichtung.

Zu beachten ist: Was für Krankenhäuser gilt, müssen auch Rechtsanwälte und Steuerberater beachten. Dienstleister mit der Verarbeitung personenbezogener Daten zu beauftragen ist bei Berufsgeheimnisträgern – wenn überhaupt – nur sehr eingeschränkt zulässig.

Klare Vorgaben für Cookies gefordert

Bereits im Mai 2011 hätte Deutschland die Neufassung der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG („Cookie-Richtlinie") in deutsches Recht umsetzen müssen. Wesentliche Änderung war die Ersetzung der bisherigen Opt-out-Regelung für den Einsatz von Cookies auf Webseiten durch ein Opt-in: „(...) die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, [ist] nur gestattet (...), wenn der betreffende Teilnehmer oder Nutzer (...) seine Einwilligung gegeben hat."

Die Bundesregierung vertritt bisher die Auffassung, dass die Regelungen des § 13 Abs. 1 S. 2 TMG ausreichen. Das sehen die Datenschutz-Aufsichtsbehörden anders: Mit ihrer Entschließung vom 05.02.2015 stellen sie fest, dass Cookies nur mit Einwilligung der Internetnutzer eingesetzt werden dürfen. Im Telemediengesetz sei die Richtlinie nur unzureichend umgesetzt.

secorvo
security consulting

Insecure by Default

Schon am 21.09.2014 wurde berichtet, dass Lenovo Notebooks für Endverbraucher ab Werk mit der Adware Superfish ausliefert. Superfish schleust Werbung in verschlüsselte HTTPS-Verbindungen ein und registriert sich dazu ungefragt im Zertifikatsspeicher von Windows als Root-CA. Der private Schlüssel für das Superfish-Zertifikat liegt dabei quasi ungeschützt auf der Festplatte.

Gefährlicher als die störende Werbung durch Superfish ist die Möglichkeit für Angreifer, damit Man-in-the-Middle-Angriffe auf beliebige HTTPS-Verbindungen durchzuführen. Dafür stellen diese sich mit dem Superfish-Schlüssel Zertifikate für beliebige Domänen aus. Inzwischen konnten derartige Angriffe bei mehr als einem Dutzend verschiedener Malware-Typen beobachtet werden.

Lenovo hat inzwischen angekündigt, künftig nur noch erforderliche Programme vorzuinstallieren. Der Vorfall zeigt jedoch, dass einer Betriebssysteminstallation im Auslieferungszustand besser nicht vertraut werden sollte. Darin findet sich oft ab Werk Zusatzsoftware, die im normalen Betrieb nicht benötigt wird und die Angriffsfläche vergrößert. Gelegentlich erkaufen sich sogar Softwarehersteller ihren Platz in der Standardinstallation. Bei der Beschaffung eines neuen Geräts sollte daher immer zuerst eine Neuinstallation des Betriebssystems durchgeführt werden, die nur die betrieblich benötigten Softwarepakete einschließt.

Immer wieder Facebook

Mit Wirkung zum 30.01.2015 hat Facebook erneut seine Datenschutzrichtlinie, seine Cookie-Richtlinie, die Nutzungsbedingungen sowie weitere Hinweise zum Datenschutz geändert. Die Zustimmung des Nutzers soll ohne ausdrückliche Zustimmung per Login erfolgen. Nach Darstellung von Facebook erleichtert die Änderung das Verständnis der Funktionsweise von Facebook und verbessert die Nutzerkontrolle. Neu eingeführt wurden Lokalisierungsdienste, Einkaufsmöglichkeiten direkt aus Facebook heraus, neue Erläuterungen zu Privatsphäreneinstellungen, eine engere Verknüpfung der Facebook-Dienste sowie die Auswertung von App-Nutzungen. Werbetreibende Dritte sollen Informationen zur Individualisierung von Werbung ohne die Möglichkeit zur Identifizierung des Nutzers erhalten.

Eine Studie im Auftrag der belgischen Datenschutzaufsichtsbehörde kommt zu einem anderen Ergebnis: Bereits die Praxis, die Nutzung von Facebook als Einwilligung zu interpretieren, sei ebenso rechtswidrig wie das Fehlen einer effektiven Opt-out-Möglichkeit. Dasselbe gelte für die Zusammenführung der Daten unterschiedlicher Dienste. Facebook dehne durch die Änderungen seine Datenverwendungen ohne Rechtsgrundlage aus. Am 23.02.2015 hat daher der Bundesverband der Verbraucherzentralen ein Unterlassungsverfahren eingeleitet und Facebook abgemahnt.

Oldie but Goldie

Bereits am 03.11.2014 erschien Version 3.1.1 des bewährten Forensik-Werkzeugs Autopsy. Hinzu gekommen ist die lange ersehnte automatische Identifikation von Dateitypen. Sehr praktisch ist die neue skriptgesteuerte Reporterstellung, die auch für mehrere Festplattenimages übergreifend funktioniert. Dank einer Multi-Thread-Verarbeitung für beliebig viele CPU-Kerne sinkt die Bearbeitungszeit effektiv um die Hälfte. Hilfreichste Neuerung ist die überarbeitete grafische Zeitlinie: Man kann nun ein Analyse-Zeitfenster bis auf Millisekunden festlegen und die Ergebnisse aus allen verfügbaren Metadaten parallel darstellen.

Secorvo News

Ei des Kolumbus oder Kuckucksei?

Kann man das Microsoft-Cloud-Angebot Office 365 Datenschutz konform einsetzen? Welche Hürden sind dabei zu bewältigen? Diese Fragen wird *Christoph Schäfer* auf der kommenden KA-IT-Si Veranstaltung am **19.03.2015** im CyberForum e.V. beantworten. Nach dem Vortrag gibt es Gelegenheit zum „Buffet-Networking". **Anmeldung** unter www.ka-it-si.de (nur noch wenige Plätze!).

Kompetenz, wo sie gebraucht wird

Als Datenschutzbeauftragter in einem großen Unternehmen benötigen Sie Datenschutzkoordinatoren mit solidem Basiswissen im Datenschutz. Unsere zweitägige Schulung „Geprüfter Datenschutzkoordinator im Unternehmen" vom **28. bis 29.04.2015** hilft Ihnen dabei, Ihren Kollegen die erforderlichen Grundkenntnisse zu vermitt eln.

Viele Angriffsszenarien gäbe es gar nicht, wenn bei der Code-Entwicklung Schwachstellen systematisch vermieden würden. Wie man etablierte Verfahren der sicheren Softwareentwicklung in den gesamten Software-Lifecycle einbindet, zeigt die Schulung CPSSE – Certified Professional for Secure Software Engineering vom **04. bis 07.05.2015**.

Die nächste Möglichkeit zur T.I.S.P.-Zertifizierung bieten wir vom **09. bis 13.03.2015**.

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

Veranstaltungshinweise

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

März 2015	
03.-05.03.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen und Schutzmechanismen (Secorvo, Karlsruhe)
09.-13.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
19.03.	Ei des Kolumbus – oder Kuckucksei? (KA-IT-Si, 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)
23.-24.04.	8. GDD-Fachtagung „Datenschutz International“ (GDD e.V., Berlin)
26.-30.04.	Eurocrypt 2015 (IACR, Sifia/BG)
Mai 2015	
04.-07.05.	CPSSE (Certified Professional for Secure Software Engineering) (Secorvo, Karlsruhe)
06.-07.05.	16. Datenschutzkongress (EUROFORUM, Berlin)
11.-12.05.	BvD Verbandstag 2015 (BvD e. V., Berlin)

Impressum

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

ISSN 1613-4311

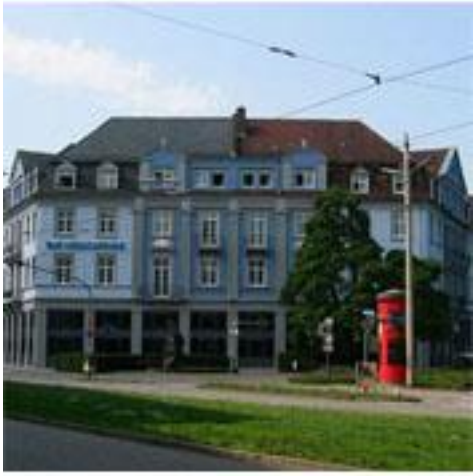
Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Michael Knopp, Sven Köhler, Christoph Schäfer, Jochen Schlichting

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

März 2015

Hobbyistensicherheit

Die zentrale Verschlüsselungsinfrastruktur des Internets hängt an 447.247 Programmzeilen von 147 Programmierer-Aktivisten: OpenSSL. Die geschützte Remote-Administration der wahrscheinlich meisten Systeme der Welt basiert auf 64.813 Zeilen C-Code von 92 unabhängigen Entwicklern: OpenSSH. Und die meisten (deutschen) PGP-Verschlüsselungen erledigt die Open-Source-Software GnuPG, entwickelt von 14 enthusiastischen Codern.

Manchmal ist die Abhängigkeit vielleicht nicht offensichtlich, weil sich der Open-Source-Code in einem Produkt „versteckt". Und ja, manche Open-Source-Projekte werden (teil-)finanziert von einem Unterstützer oder erhalten öffentliche Mittel.

Dennoch muss die Situation für jemanden außerhalb der „IT-Szene" ziemlich skurril anmuten. Das dürfte in etwa so wirken, als ob wir die Statik von Brücken durch Hobby-Architekten berechnen, ABS und Airbags von engagierten Bastlern konstruieren und Flugzeuge von Freizeitschraubern warten ließen.

Zwar muss das Ergebnis nicht schlecht sein – im Gegenteil: Wenn viele Engagierte eigeninitiativ und professionell zusammenarbeiten, kann sich das Resultat oft sehen lassen. Zu denken geben sollte uns diese Entwicklung trotzdem: Hat jemand einmal ausgerechnet, wie viel es volkswirtschaftlich kostet, wenn alle Unternehmen, die bspw. TrueCrypt zur Verschlüsselung einsetzen, auf BitLocker wechseln müssen, weil die Initiatoren es nicht weiterführen? Oder wenn eine GPG-Installation durch S/MIME ersetzt werden muss, weil der Hauptentwickler die Code-Pflege aufgibt?

Schließlich hat die Geschichte von OpenSSL gezeigt, dass Open Source nicht dasselbe ist wie „geprüfter" Code – sondern eben nur „prüfbarer" Code. Wäre es nicht angemessen, bei den zentralen Komponenten unserer Sicherheitsinfrastruktur für eine stabile Finanzierung und vor allem regelmäßige Code-Analysen zu sorgen?

Inhalt

secorvo
security consulting

Security News

Stromortung

Am 11.02.2015 veröffentlichten vier Forscher der Stanford University und des *National Research and Simulation Center* eine empirische Analyse zur Standortbestimmung über den Stromverbrauch eines Smartphones. Da das Senden und Empfangen von Daten den meisten Strom verbraucht und dieser stark schwankt (abhängig von der Entfernung zum Sendemast und der Signalstärke, die sich durch Hindernisse wie Häuser, Bäume oder Menschen schnell verändert), kann man jedem Ort einen spezifischen Verbrauch zuordnen. In aktuellen Smartphones sind die Strom- und Spannungswerte uneingeschränkt zugänglich; eine App kann diese also zyklisch an einen Server übermitteln, der die Werte mit bereits ausgemessenen Routen korreliert. Die Forscher konnten so innerhalb von zwei Minuten acht von zehn Teilstrecken erkennen.

Für einen flächendeckenden Einsatz erfordert die Technik zwar ausgemessene „Landkarten". Die Sperrung der GPS-Daten im Smartphone lässt sich damit jedoch umgehen. Wegen des geringen Verbrauchs ist ein Verschleiern der Werte durch das Starten vieler Apps keine wirksame Gegenmaßnahme; helfen würde allein eine Ausdehnung des Rechtemanagements auf die Stromverbrauchsdaten.

Kompatibilitätsbug

2010 patchte Microsoft gegen Stuxnet und Fanny – nur leider fehlerhaft. Das belegt die nach Hinweisen von Michael Heerklotz vom Januar initiierte Untersuchung von HP, deren Ergebnisse Dave Weinstein am 10.03.2015 veröffentlichte.

So missbrauchte Stuxnet CPL-Dateien (DLLs mit anderem Namen, also ausführbaren Code), indem er über Icons für Windows-Verknüpfungen (.lnk) eigenen Code aus mitgebrachten CPLs zur Ausführung brachte. Seit dem Patch im Jahr 2010 lädt Microsoft diese Windows-Urgesteine nur noch aus einer CPL-Whitelist. Der Schutz lässt sich allerdings durch geschickte Änderungen des Dateinamens der .lnk-Datei aushebeln: Das Icon wird zusammen mit dem Angriffscode in einen Speicherbereich mit Ausführberechtigung geladen – und Stuxnet ist fünf Jahre nach dem Patch wiederbelebt.

Die kompatibilitätserhaltende Pflege von Architekturschwächen (wie das Laden von Icons in Executable Memory) ist immer wieder ein Einfallstor. Eine ernsthafte Erhöhung des Sicherheitsniveaus erfordert es jedoch, gelegentlich die Rückwärtskompatibilität auf dem Altar der Sicherheit zu opfern.

Sozialadäquate Straftat

In den SSN 2/2015 wiesen wir darauf hin, dass Berufsgeheimnisträger wie Ärzte, Rechtsanwälte und Steuerberater grundsätzlich keine Dienstleister mit der Verarbeitung personenbezogener Daten beauftragen dürfen: Sie müssen die ihnen anvertrauten Geheimnisse schützen (§ 203 Abs. 1 StGB).

Diese (zugegebenermaßen betagte) strafrechtliche Vorschrift empfanden die Anwaltskammern als nicht zeitgemäß und versuchten sie mit dem am 11.11.2014 (sic!) beschlossenen Entwurf zur neuen Berufsordnung (BORA) auszuhebeln: Um künftig Aktenvernichter, Schreib- und Clouddienste einsetzen zu dürfen, soll ein Rechtsanwalt sich nicht mehr strafbar machen, wenn das Outsourcing „im Rahmen der Arbeitsabläufe der Kanzlei einschließlich der Inanspruchnahme von Leistungen Dritter erfolgt und objektiv einer üblichen, von der Allgemeinheit gebilligten Verhaltensweise im sozialen Leben entspricht (Sozialadäquanz)." Auf Deutsch: Alle schieben ihre Daten in die Cloud – dann muss das der Rechtsanwalt doch auch dürfen.

Dieser eigenmächtigen Strafbefreiung schob der Bundesjustizminister jetzt einen Riegel vor und stellte am 04.03.2015 klar, dass die Berufsordnung das Strafgesetzbuch nicht aufweichen kann. Nicht alles, was technisch machbar ist, darf auch zulässig sein: Schließlich verarbeiten Berufsgeheimnisträger besonders schützenswerte Daten.

Angriffsanalyse

Auf dem USENIX Security Symposium wurden am 21.08.2014 die Ergebnisse einer Analyse gezielter, systematischer Angriffe auf eine China kritische Nichtregierungsorganisation vorgestellt, die Rückschlüsse auf typische Angriffsmethoden erlauben – das dürfte auch der Grund für die Einladung der Autoren als Keynote der diesjährigen 22. DFN-Konferenz gewesen sein.

In der Analyse wurden 1.500 verdächtige E-Mails von ca. 700 unterschiedlichen Absenderadressen untersucht; bei über 1.100 wurde Schadsoftware gefunden. Alle betroffenen E-Mails waren mit für die Empfänger plausiblem individuellen Kontext versehen. Bemerkenswert sind die folgenden Erkenntnisse: Es handelte sich um einen Langzeitangriff, der mindestens von 2009 bis 2013 dauerte und ggf. weiter andauert. Die meisten Empfänger, die Opfer der Angriffe wurden, erhielten erst nach dem Eintritt von Praktikanten in die Organisation infizierte E-Mails. Genutzt wurden keine Zero-Day-Exploits, sondern frei verfügbare Schadsoftware, wobei die Zeitspanne zwischen Veröffentlichung des Exploits und der maliziösen E-Mail meist sehr kurz war. Als „Wirtsdatei" wurden zunächst meist PDF-

Dokumente verwendet, die nach Einführung von Sandboxing in Acrobat Reader (ab 2010) von Microsoft Office-Dokumenten abgelöst wurden.

Daraus können wir Verschiedenes lernen. Erstens: Angreifer haben einen langen Atem. Zweitens: Schnelles Patchen von Sicherheitslücken wird immer wichtiger – „Aufpassen" schützt nicht. Und Drittens: Bei einer Häufung von Schadsoftware-Vorfällen könnte ein gezielter Angriff dahinterstecken – daher ist eine systematische Auswertung wichtig.

Rechts(un)sicherer WLAN-Betrieb

Das Bundesministerium für Wirtschaft und Energie hat am 11.03.2015 einen Gesetzesentwurf für ein zweites Gesetz zur Änderung des Telemediengesetzes vorgelegt. Damit will das Ministerium Rechtssicherheit für WLAN-Anbieter schaffen. Bislang drohen diesen bei missbräuchlicher Nutzung Unterlassungsansprüche (SSN 6/2014). Gleichzeitig will man die Störerhaftung von Plattformanbietern erleichtern, deren Plattformen hauptsächlich für rechtswidrige Handlungen genutzt werden, und das bisherige telemedienrechtliche Haftungsprivileg einschränken.

Diese Ziele soll eine Definitionsergänzung in § 2 TMG für drahtlose lokale Funknetze (= WLAN) ermöglichen. In drei neuen Absätzen des § 8 TMG, dem Haftungsprivileg für Access-Provider, wird klargestellt, dass auch die Störerhaftung ausgeschlossen sein soll. Voraussetzung ist, dass die Anbieter bestimmte Sorgfaltspflichten erfüllen: die Verschlüsselung des Zugangs zum Ausschluss unberechtigter Nutzer und die Beschränkung auf Nutzer, die zuvor erklären, keine Rechtsverletzungen über den Zugang zu begehen. Nicht geschäftsmäßige Anbieter sollen zudem den Zugang auf namentlich bekannte Nutzer beschränken.

Entgegen der in der Rechtsprechung zuletzt erkennbaren Tendenz, das Haftungsprivileg endlich uneingeschränkt auf WLAN-Anbieter anzuwenden, werden nun mit den Sorgfaltspflichten europarechtswidrige, wirkungslose Einschränkungen geschaffen. Erklärungen allein werden Rechtsverletzungen nicht verhindern, das Abmahnrisiko bei einer unzureichenden Umsetzung der Sorgfaltspflichten steigt dagegen. Im Interesse der Rechtssicherheit und einer Verbesserung der WLAN-Verfügbarkeit ist zu hoffen, dass dieser Entwurf gar nicht erst den Bundestag erreicht.

Secorvo News

Sichere Systeme

Für die Entwicklung sicherer Systeme genügt es nicht, nur die Sicherheit der einzelnen Komponenten zu betrachten – in deren Zusammenspiel und an der Schnittstelle zum Benutzer können unerwartet neue Risiken entstehen. Wie sich auch in komplexen Systemen Security by Design erreichen lässt, erfahren Sie auf unserem Seminar T.E.S.S. – Sichere Systeme dank System Security Engineering vom 14. bis 19.06.2015 mit anschließender Zertifizierung als T.E.S.S. (TeleTrusT Engineer for System Security).

Der T.I.S.P., das deutsche Personenzertifikat für Informationssicherheit, umfasst alle grundlegenden Themenbereiche der Informationssicherheit. In unseren T.I.S.P. Schulungen erhalten Sie in fünf Tagen einen kompakten Überblick – und vorab unser T.I.S.P.-Begleitbuch zur Vorbereitung. Für die Schulung vom 22. bis 26.06.2015 gibt es noch wenige freie Plätze. Die nächste Möglichkeit zur Zertifizierung bieten wir im September und November. Alle Termine und Seminarangebote sowie die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/college.

7. Tag der IT-Sicherheit

Der Tag der IT-Sicherheit am **19.05.2015** in Karlsruhe, eine Kooperationsveranstaltung der KA-IT-Si mit der IHK Karlsruhe, dem CyberForum und KASTEL, beschäftigt sich mit aktuellen IT-Sicherheitsherausforderungen für Unternehmen. Das Landesamt für Verfassungsschutz Baden-Württemberg informiert in einer Keynote über die aktuelle Bedrohungslage. Es folgen Fachvorträge zu den Themen Netzwerksicherheit, Datenschutz und Mobile Computing. Die Veranstaltung schließt mit einem Live-Hacking, das Sicherheitslücken von Webseiten aufzeigt. Zwischendurch gibt es Gelegenheit zum fachlichen Gedanken- und Erfahrungsaustausch mit Referenten, Teilnehmern und Ausstellern. Wir freuen uns auf Ihre Anmeldung!

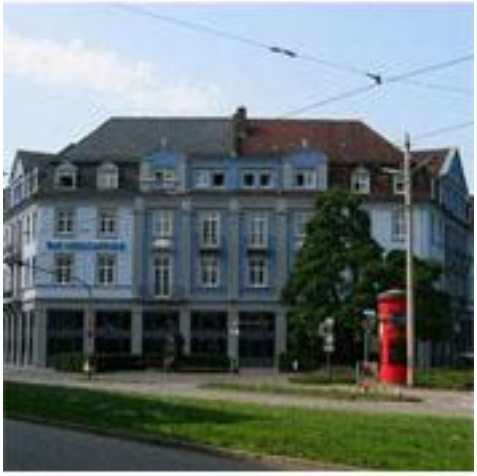
„No Blackout"

Am **12. und 13.05.2015** veranstaltet Secorvo anlässlich der bevorstehenden Verabschiedung des IT-Sicherheitsgesetzes und der daraus folgenden Verpflichtungen von Betreibern kritischer Infrastrukturen das Symposium „No Blackout – IT-Sicherheit für die Energieversorgung" in der Buhlschen Mühle in Ettlingen. Die Veranstaltung richtet sich nicht nur an Unternehmen und Institutionen aus dem Bereich der kritischen Infrastrukturen – sie bietet wertvolle Informationen für alle Unternehmen, die den Aufbau eines ISMS planen oder vorbereiten. Unter anderem werden die Stadtwerke Ettlingen über den „fx-Hack" und die Folgen berichten, und wir werden etwas über die IT-Sicherheit in Kernkraftwerken erfahren. Wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

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

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)
23.-24.04.	8. GDD-Fachtagung "Datenschutz International" (GDD e.V., Berlin)
26.-30.04.	Eurocrypt 2015 (IACR, Sofia/BG)
Mai 2015	
04.-07.05.	CPSSE (Certified Professional for Secure Software Engineering) (Secorvo, Karlsruhe)
06.-07.05.	16. Datenschutzkongress (EUROFORUM, Berlin)
11.-12.05.	BvD Verbandstag 2015 (BvD e. V., Berlin)
12.-13.05.	No Blackout – Symposium IT-Sicherheit für die Energieversorgung (Secorvo, Ettlingen)
18.-20.05.	IMF 2015 (Fraunhofer IAO, Magdeburg)
18.-21.05.	OWASP AppSec EU 2015 (OWASP Foundation, Amsterdam/NL)
19.-21.05.	14. Deutscher IT-Sicherheitskongress (BSI, Bonn)
19.05.	7. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
20.-22.05.	Entwicklertag 2015 (VKSI, ObjektForum, Karlsruhe)



Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Michael Knopp, Sven Köhler, Christoph Schäfer, Jochen Schlichting

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

April 2015

Maßlos

Angenommen, wir besäßen ein riesiges Stück Papier mit einer Materialstärke von 0,09 mm. Wie oft müssten wir dieses Papier falten, um den Abstand zwischen Erde und Mond (ca. 384.400 km) zu überbrücken? Den Rechenweg kennen wir aus der Schule:

$$2^n \cdot 0{,}09 \text{ mm} = 384.400 \text{ km},$$
$$\text{also: } n = \log_2 (42{,}71 \cdot 10^{11}) \approx 42.$$

Ein überraschend kleiner Wert, den wir – Douglas-Adams-Fans ausgeschlossen – eher nicht erwartet hätten. Die kleine Rechnung zeigt, wie schwer wir uns exponentielles Wachstum vorstellen können.

Und das hat Folgen. Im Januar 1997 lobte die Firma RSA eine *Crypto Challenge* aus: Eine mit RC5 und einem 56 bit langen Schlüssel verschlüsselte Nachricht sollte durch eine Brute-Force-Attacke entschlüsselt werden. Das gelang einem riesigen Netzwerk von Freiwilligen, die die Leerlaufzeiten ihrer PCs für die Schlüsselsuche zur Verfügung stellten, in 270 Tagen. Einer dieser Freiwilligen war ein Student, den ich betreute. Nachdem der Schlüssel gefunden war, erklärte er mir freudestrahlend, jetzt wolle er mit den Institutsrechnern an der RC5-64 bit-Challenge teilnehmen. Als ich ihn fragte, wer ihm denn ein so langes Studium bezahle, sah er mich mit großen Augen an – und ich musste ihm vorrechnen, dass die Challenge die 2^8-fache Rechenleistung benötigt, seine 4.000 Teams ohne schnellere Rechner fast 190 Jahre suchen müssten.

So verleitet uns unsere mangelnde Vorstellungskraft, es bei Schlüssellängen ständig zu übertreiben. Denn ein 256 bit-AES-Schlüssel ist nicht doppelt, sondern 2^{128}-mal so sicher wie ein 128 bit-Key. Das ist, als wolle man ein Haus mit einer gepanzerten Tür dadurch sicherer machen, dass man nicht eine zweite, sondern gleich $3{,}4 \cdot 10^{38}$ zusätzliche Türen montiert. Die würden übrigens nicht in unser Universum passen – das hat lediglich einen Durchmesser von 93 Milliarden Lichtjahren (etwa $8{,}8 \cdot 10^{26}$ m), wir benötigten also 387 Milliarden weitere Universen gleicher Größe dafür.

Inhalt

secorvo
security consulting

Security News

Nächster Persilschein

Gerade ein Jahr ist es her, dass Microsoft einen vermeintlichen Persilschein der europäischen Datenschutz-Aufsichtsbehörden (Art.-29-Gruppe) für Microsoft Office 365 erhielt (SSN 04/2014). Nun hat auch Amazon den Datenschutz als Schlüssel zum europäischen Markt entdeckt und am 06.03.2015 ein ähnliches Dokument der luxemburgischen Datenschutzaufsicht (CNPD), stellvertretend für die Art.-29-Gruppe, für seinen Cloud-Service AWS erhalten. Wie zuvor Microsoft verkündet Amazon seitdem vollmundig, AWS sei damit datenschutzkonform einsetzbar. Tatsächlich schreibt die CNPD genau das Gegenteil: Sie habe lediglich gemäß dem Cloud-Leitfaden der Art.-29-Gruppe die Vertragsstruktur geprüft und will das positive Prüfergebnis gerade nicht als Freigabe für AWS verstanden wissen.

Derweil kämpfen die amerikanischen Cloud-Anbieter weiter um den europäischen und insbesondere den deutschen Markt und setzen dabei zunehmend auf nationale Niederlassungen, wie den AWS Marketplace in Frankfurt. Doch die augenscheinlich lokal angebotenen Dienste sind weiterhin in die globale Infrastruktur des Anbieters eingebunden. Cloud-Willige sollten daher nicht den Fehler machen, sich ohne eine gründliche (datenschutz-) rechtliche und (sicherheits-)technische Prüfung auf die Marketing-Aussagen der Anbieter zu verlassen.

Car to go

Das Keyless-System PKES entriegelt Fahrzeugtüren automatisch, wenn der Besitzer naht. Oder auch ein geschickter Dieb: Am 06.04.2015 musste der Reporter Nik Bilton zusehen, wie zwei Teenager mit seinem Toyota Prius davonfuhren. Wahrscheinlich nutzten die beiden einen simplen Signalverstärker, der die Reichweite der Kommunikation zwischen Token und Fahrzeug vergrößerte.

Der Fehler liegt nicht im verwendeten kryptografischen Protokoll - denn Kryptografie hilft nicht gegen diese Art von Angriffen. Ein weiteres Beispiel dafür, dass mancher Komfortgewinn nur auf Kosten der Sicherheit erhältlich ist.

Zur Prävention können betroffene Autobesitzer ihr Token mit Schutzhüllen vor Funksignalen abschirmen – oder besser gleich wieder auf herkömmliche Schlüssel mit Knopfdruckentriegelung umsteigen.

Ende des Passworts?

Die unter anderem von Paypal initiierte FIDO-Alliance, der inzwischen weitere Größen wie Alibaba oder die Bank of America beigetreten sind, engagiert sich neben der 2-Faktor-Authentifikation (U2F, siehe SSN 10/2014) verstärkt für biometrische Authentifikationsverfahren (Fingerabdruck-, Herzrhythmus- und Venenerkennung) und hat am 09.12.2014 Version 1.0 ihres Universal Authentication Framework (UAF) veröffentlicht.

Doch Biometrie hat bekannte Schwächen. Jüngst zeigten das der Vortrag von starbug auf dem 31. Chaos Communication Congress am 27.12.2014, der u. a. über Kameras in Mobiltelefonen biometrische Merkmale ausspähte, und der Hack des iPhone-Fingerabdrucksensors von Ben Schlabs, dem es im September 2014 gelang, den Sensor mit einem Holzleim-Fingerimitat zu täuschen.

Ein grundsätzliches Problem ist, dass sich biometrische Merkmale, wenn sie einmal gestohlen wurden, nicht einfach wie ein Passwort ändern lassen – lediglich der Fingerabdruck erlaubt bis zu neun Wechsel. Das wiegt umso schwerer, als dieselben biometrischen Merkmale unvermeidlich für die Authentifikation in zahlreichen unterschiedlichen Anwendungen zum Einsatz kommen werden.

Mit Passwörtern werden wir daher wohl noch eine Weile leben und sollten uns mit Verfahren beschäftigen, die zu sichereren Passwörtern führen. So lassen sich Anwender möglicherweise zu Wahl stärkerer Passwörter bewegen, wenn sie von Passwort-Managern unterstützt werden. Und Anwendungen könnten die Stärke eines gewählten Passworts mit Passwort-Metern bei der Eingabe messen und zu schwache Passwörter zurückweisen.

XP lebt!

Totgesagte leben länger. Dies belegen Anfragen der Grünen und der Piratenpartei zum Einsatz von Windows XP in der Berliner Stadtverwaltung anlässlich des bevorstehenden Ablaufs der teuer bezahlten Supportverlängerung von Microsoft: Ab April 2015 werden keine Aktualisierungen mehr geliefert. Tatsächlich ist Berlin nicht die einzige Stadtverwaltung, bei der ältere Anwendungen die Ablösung von Windows XP bisher verhindert haben. Auch werden noch eine Vielzahl von Geldautomaten unter Windows XP betrieben. Wie groß aber ist die Gefährdung durch Windows XP wirklich?

Werden neu entdeckte Sicherheitslücken von XP nicht mehr behoben, steigt das Risiko, dass Schadsoftware durch Ausnutzung dieser Lücken Systeme befällt. Dagegen hilft eine strikte Entkopplung der produktiven Anwendungen von „Malwarezugängen“ wie dem Internet, den lokalen Datenschnittstellen (vulgo USB-Anschlüsse) und dem Einfallstor E-Mail-Anhang.

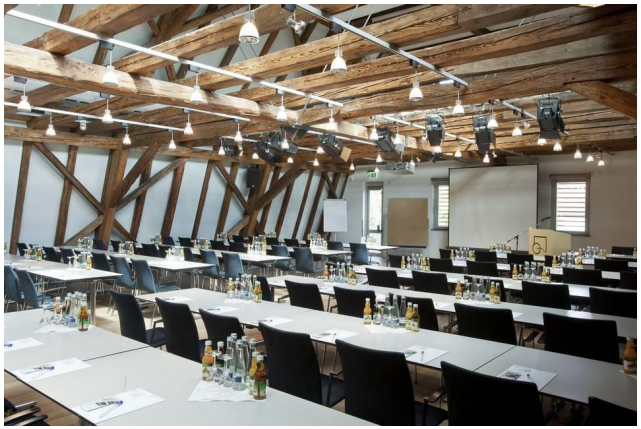
Realisieren lässt sich das, indem man z. B. den Internet- und E-Mail-Zugang über einen Terminalserver bereitstellt oder, noch besser, die alte Software in eine virtuelle Maschine mit XP verfrachtet – und diese auf aktuellen Windows-Clients betreibt.

Dass Abschalten keine Lösung, sondern „friendly fire" ist, dürfte auch dem Berliner Datenschutzbeauftragten Dix klar sein. Mit einer besonnenen und differenzierten Analyse lassen sich Lösungen finden, XP-abhängige Anwendungen mindestens für eine Übergangszeit und mit vertretbaren Komforteinbußen für die Benutzer weiter zu betreiben, ohne damit einen Sicherheits-Gau zu riskieren.

Secorvo News

Symposium „No Blackout"

Anlässlich der bevorstehenden Verabschiedung des IT-Sicherheitsgesetzes und der daraus folgenden Verpflichtungen von Betreibern kritischer Infrastrukturen veranstaltet Secorvo am **12.** und **13.05.2015** das Symposium „No Blackout – IT-Sicherheit für die Energieversorgung" in der Buhlschen Mühle in Ettlingen.



Die Veranstaltung richtet sich nicht nur an Unternehmen und Institutionen aus dem Bereich der kritischen Infrastrukturen – sie bietet wertvolle Erfahrungen für alle Firmen, die den Aufbau eines Information Security Managements (ISMS) planen oder bereits vorbereiten.

Unter anderem werden die Stadtwerke Ettlingen über den „fx-Hack" und die Folgen berichten, und wir werden etwas über die IT-Sicherheit in Kernkraftwerken erfahren. Gelegenheit zur Diskussion bieten das gemeinsame Dinner in der Villa Hartmaier's am 12.05. und die Networking-Pausen.

Wir freuen uns auf Ihre Teilnahme.

7. Tag der IT-Sicherheit

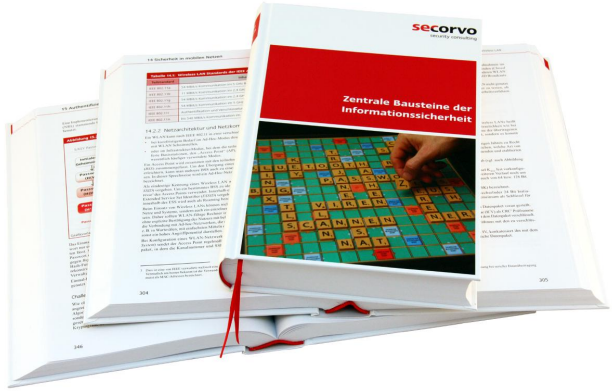
Beim 7. Tag der IT-Sicherheit am **19.05.2015**, einer Kooperationsveranstaltung der KA-IT-Si mit der IHK Karlsruhe, dem CyberForum und KASTEL, informiert das Landesamt für Verfassungsschutz über die aktuelle Bedrohungslage und die Risiken „Mensch" und „Technik". Es folgen Fachvorträge zu den Themen Netzwerksicherheit, Datenschutz und Mobile Computing. Das Programm schließt mit einem Live-Hacking, in dem gezeigt wird, welche Sicherheitsschwächen zahlreiche Webanwendungen aufweisen.

Gelegenheit zum fachlichen Gedanken- und Erfahrungsaustausch mit Referenten, Teilnehmern und Ausstellern bieten die „Networking-Pausen". Wir freuen uns auf Ihre Anmeldung.

Mit Brief und Siegel

Seit vielen Jahren setzt Secorvo College auf Seminare, bei denen die Teilnehmer ihre Qualifikation durch eine anschließende Prüfung und ein Zertifikat nachweisen können.

Dazu zählt insbesondere der T.I.S.P. (TeleTrusT Information Security Professional), ein inzwischen deutschlandweit anerkanntes Expertenzertifikat für Informationssicherheit. In unseren T.I.S.P.-Schulungen erhalten Sie in fünf Tagen einen kompakten Überblick zu allem, was in der Informationssicherheit zählt – unterstützt vom T.I.S.P.-Buch „Zentrale Bausteine der Informationssicherheit". Auf dem Seminar vom **22.** bis **26.06.2015** gibt es noch wenige Plätze; weitere Gelegenheiten zur Zertifizierung Ihrer Expertise bieten wir im September (**21.–25.09.2015**) und November (**23.–27.11.2015**) in unseren Seminarräumen in Karlsruhe.



Die Zertifikatsschulung T.E.S.S. – Sichere Systeme dank System Security Engineering zeigt Wege auf, wie ganze Systeme mit allen Komponenten, Schnittstellen und Prozessen mit angemessener Sicherheit gestaltet werden können. Der T.E.S.S. (TeleTrusT Engineer for System Security) steht für interdisziplinäre Sicherheitskompetenz. Termine: **14.–19.06.2015** und **10.–13.11.2015** in Karlsruhe.

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

Veranstaltungshinweise

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

Mai 2015	
06.-07.05.	16. Datenschutzkongress (EUROFORUM, Berlin)
12.-13-05.	Symposium „No Blackout“ – IT-Sicherheit für die Energieversorgung (Secorvo, Karlsruhe)
18.-21.05.	OWASP AppSec EU 2015 (OWASP Foundation, Amsterdam/NL)
18.-20.05.	IMF 2015 (Fraunhofer IAO, Magdeburg)
19.-21.05.	14. Deutscher IT-Sicherheitskongress (BSI, Bonn)
19.05.	7. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si; Karlsruhe)
20.-22.05.	Entwicklertag 2015 (VKSI, GI, ObjektForum; Karlsruhe)
26.-28.05.	IFIP SEC 2015 (IFIP, Hamburg)
Juni 2015	
08.-12.06.	Audit Challenge 2015 (Frankfurt School of Finance & Management, Frankfurt)
15.-16.06.	DuD 2015 (COMPUTAS, Berlin)

Fundsache

Am 02.04.2015 wurden vom Open Crypto Audit Project die Ergebnisse des TrueCrypt-Audits (v7.1a) veröffentlicht. Mängelfrei ist die Software nicht, aber Hintertüren oder einfach ausnutzbare Angriffsmöglichkeiten wurden nicht gefunden. Trotz der Einstellung der Weiterentwicklung spricht also derzeit nichts gegen die Nutzung dieser Version – oder auf TrueCrypt aufbauender Lösungen wie VeraCrypt.

Impressum

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

ISSN 1613-4311

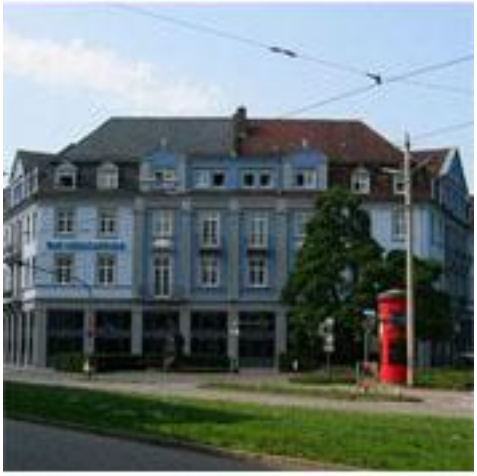
Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Sven Köhler, Christoph Schäfer

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Mai 2015

Wir regulieren uns zu Tode

Nicht immer kommt die Bürokratie so unübersehbar daher wie beim Mindestlohngesetz. Dokumentationspflichten, Erklärungen gegenüber Auftraggebern und Verpflichtungen von Auftragnehmern – 99% aller Unternehmen werden wegen einzelner schwarzer Schafe in kollektive Misstrauenshaft genommen.

Ganz Ähnliches ereilt Deutschland in Folge des Sarbanes-Oxley-Act: Die Skandale bei Enron und Worldcom hatten 2002 in den USA eine Welle der Compliance-Regulierung losgetreten. Seitdem sickern regulatorische Kontrollen unternehmerischen Wohlverhaltens in deutsche Unternehmen ein. Wirtschaftsprüfer stellen in wachsendem Umfang auch Anforderungen an den sicheren IT-Betrieb. Mit teilweise skurrilen Resultaten: Keine Prüfung, in der nicht für zentrale IT-Systeme ein regelmäßiger Passwortwechsel spätestens alle 90 Tage gefordert wird. Von dem eigentlichen Zweck (Begrenzung des Schadens, sollte ein Passwort kompromittiert sein) hat sich diese Regelung längst befreit – denn Benutzer wählen Passwörter, denen sie eine einfache Bildungsregel mitgeben, wie z. B. eine Ziffer am Ende. Ein Angreifer kennt daher mit einem Passwort auch alle folgenden – und wir quälen alle 90 Tage eine wahrscheinlich 8stellige Zahl von IT-Nutzern mit einem Sinn entleerten Ritual, das sogar die Passwortkomplexität senkt. Ähnliches könnte uns nun mit dem IT-Sicherheitsgesetz bevorstehen – und auch die Vorratsdatenspeicherung wird nicht ohne Auswirkungen auf die Compliance-Anforderungen in Unternehmen bleiben (siehe die Beiträge in diesen SSN).

Manchmal ist es unvermeidlich, dass politisch oder gesellschaftlich gewünschtes Verhalten gesetzlich erzwungen wird. Die durch Detailregulierung entstehenden Bürokratiekosten dürften jedoch – bei aller Sympathie für die IT-Sicherheit – die verhinderten Schäden um ein Vielfaches übersteigen. Wer in erster Linie wirtschaftlichen Schaden von Unternehmen abwenden will, sollte die IT-Sicherheit daher besser der Selbstregulierung und Haftung überlassen.

Inhalt

secorvo
security consulting

Security News

Das BAG und die Einwilligung

Dass die Einwilligung nur in speziellen Ausnahmefällen als Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten taugt ist herrschende Meinung unter Datenschützern.

Das Bundesarbeitsgericht hat sich nun in einem Urteil vom 11.12.2014 – eher beiläufig – zu dieser Frage geäußert. So gebe der Arbeitnehmer mit Eingehen des Arbeitsvertrags nicht seine Persönlichkeitsrechte auf. Eine Benachteiligung aufgrund einer Einwilligungsverweigerung stelle einen groben arbeitgeberseitigen Nebenpflichtverstoß und einen Verstoß gegen das Maßregelungsverbot aus § 612a BGB (Verbot der Benachteiligungen wegen einer zulässigen Rechteausübung) dar. Arbeitnehmer könnten sich auch im Arbeitsverhältnis frei entscheiden, wie sie ihr Grundrecht auf informationelle Selbstbestimmung ausüben.

Eine Revolution steht trotzdem nicht bevor: Zwar stellt das BAG auch die Widerruflichkeit einer Einwilligung unter den Vorbehalt einer Interessensabwägung. Es verleiht damit aber der Einwilligung trotzdem nicht die praktisch notwendige Stabilität.

Zudem sind an der Argumentation des BAG Zweifel angebracht: Bereits die Befürchtung, der Arbeitgeber könne aufgrund der Verweigerung benachteiligen, ohne dass der Zusammenhang nachweisbar ist, kann die Freiwilligkeit einer Einwilligung im Arbeitsverhältnis erheblich einschränken. Der Verweis auf späteren Rechtsschutz ist sehr formal und verkürzt den Schutz der Informationellen Selbstbestimmung erheblich.

Seiteneffekt der Vorratsspeicherung

Am 27.05.2015 hat das Bundeskabinett den Gesetzentwurf zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten – kurz: die Vorratsdatendatenspeicherung – beschlossen. Die Diskussion über die Verfassungsmäßigkeit des neuen Anlaufs ist nun in vollem Gange.

Aus Sicht der Informationssicherheit ist jedoch von Interesse, wie die Bundesregierung die Mahnung des Bundesverfassungsgerichts umgesetzt hat, den Schutz der Daten zu regeln. Der Entwurf kommt dieser Anforderung in den vorgeschlagenen §§ 113d ff TKG nach. Vorgesehen sind – in Ergänzung zu § 109 TKG – u. a. der Einsatz eines „besonders sicheren Verschlüsselungsverfahrens“, die Speicherung in getrennten Speichereinrichtungen, das „Vier-Augen-Prinzip“ für den Zugriff und eine Zugriffsprotokollierung von einem Jahr über Zeitpunkt, Akteure, Zweck und Art des Zugriffs.

Die Bundesnetzagentur soll in Abstimmung mit dem BSI und der Bundesdatenschutzbeauftragten einen ergänzenden Anforderungskatalog erstellen. Das Sicherheitskonzept der Provider nach § 109 Abs. 4 TKG ist entsprechend zu ergänzen. Ein mangelnder Schutz soll Geldstrafen bis zu 500.000 € nach sich ziehen.

Sollte der Entwurf Gesetz werden, könnte dies weit reichende Auswirkungen auf andere Verarbeitungen besonders schutzwürdiger Daten haben: Die Sicherheitsvorgaben setzen hier einen neuen Maßstab. Mit Spannung darf man daher den Anforderungskatalog der BNetzA erwarten – vor allem in Bezug auf die in § 113b Abs. 8 TKG n.F. geforderte irreversible Löschung oder die Kriterien für ein „besonders sicheres Verschlüsselungsverfahren“.

Wirkungen von Datensicherheit

Häufig sind es die Nebenfolgen, der die wahre Bedeutung eines Urteils ausmachen. So auch bei einem Urteil des Landesarbeitsgerichts Schleswig-Holstein vom 04.03.2015, das die Aufhebung einer Kündigung bestätigt, die gegen ein Betriebsratsmitglied wegen des Verstoßes gegen die Verschwiegenheitspflicht ausgesprochen worden war. Das Betriebsratsmitglied hatte Rechtsanwaltsrechnungen zu betriebsverfassungsrechtlichen und individualarbeitsrechtlichen Beratungen an den betroffenen Betriebsrat eines verbundenen Unternehmens weitergegeben.

Das Landesarbeitsgericht sah hierin keinen die fristlose Kündigung rechtfertigenden Verstoß. Denn die Zugriffsrechte des Gekündigten waren nicht eingeschränkt und es fehlte eine Kennzeichnung des Geheimhaltungsbedarfs an den Dokumenten.

Das Urteil verdeutlicht die rechtliche Bedeutung von IT-Sicherheitsmaßnahmen: Sie begründen bereits durch ihre Existenz rechtlichen Schutz und erzeugen auch rechtliche Wirkungen. Aus diesem Grund sollte selbst auf überwindbare technische und organisatorische Maßnahmen und eine Geheimhaltungsklassifizierung nicht verzichtet werden.

Schriftform bei Mitarbeiterfotos

Wollen Arbeitgeber Fotos oder Videos ihrer Mitarbeiter veröffentlichen, bedarf dies nach § 22 Kunsturhebergesetz (KUG) in der Regel der Einwilligung der Arbeitnehmer. Das Gesetz sieht für diese Einwilligung keine besondere Form vor. Tatsächlich setzen Unternehmen oft auf ein „lautes Nicken“ – die für einen Werksausweis angefertigten Fotos werden so oft wie selbstverständlich in das elektro-

nische Telefonverzeichnis aufgenommen und auf die Webseite gestellt.

Das Bundesarbeitsgericht (BAG) hat nun mit Urteil vom 11.12.2014 (Az. 8 AZR 1010/13) schärfer als die Forderung des KUG entschieden, dass eine ausdrückliche – also in der Regel schriftliche – Einwilligung der betroffenen Arbeitnehmer erforderlich ist. Anlass war ein Werbefilm im Internet, in dem Mitarbeiter einige Sekunden lang gezeigt wurden. Gleichzeitig stellte das BAG fest, dass eine formal korrekte Einwilligung nicht automatisch mit Beendigung des Arbeitsverhältnisses erlischt, sondern der Widerruf vielmehr eines plausiblen Grundes bedarf – zumindest dann, wenn nicht die Person des Mitarbeiters im Vordergrund steht.

Für die Fotos auf Werksausweisen wird man auch weiterhin von überwiegenden Sicherheitsinteressen des Unternehmens ausgehen können. In den meisten anderen Fällen der Veröffentlichung müssen Unternehmen schriftliche – und zweckbezogene – Einwilligungen einholen. Dies gilt für das Internet gleichermaßen wie für das Intranet. Eine unspezifische Generaleinwilligung in Arbeitsverträgen scheidet aus – solche Klauseln scheitern meist am AGB-Recht.

Security-Adventure

Die Spieler von „Gezielter Angriff – Das Spiel“, einem am 05.05.2015 veröffentlichten kostenlosen Online-Lernspiel des japanischen IT-Sicherheitsanbieters Trend Micro, schlüpfen in die Rolle des CIOs der fiktiven Firma „The Fugle“. Er hat ein beschränktes Budget und muss im Spiel das Geld in sinnvolle und angesichts der aktuellen Risiken angemessene Projekte investieren.

Seine Entscheidungen beeinflussen den weiteren Verlauf der Spiels, bis es schließlich zu einem gezielten Angriff kommt. Spieler, die den Angriff nicht mehr verhindern können, erhalten eine Analyse ihrer Handlungsschritte und Hinweise, wie sie das Spiel beim nächsten Mal in die richtige Richtung lenken können.

Ein interessanter Ansatz, um die Sensibilität für IT-Sicherheit zu steigern und zugleich ein gesundes Verständnis für angemessene Schutzmaßnahmen zu vermitteln. Das Spiel ist kostenlos, die Spieler müssen keine persönlichen Daten preisgeben.

Secorvo News

Kompetenz darf sich auszahlen

In diesen Tagen wird das 750ste T.I.S.P.-Zertifikat ausgestellt. Es belegt neben der mindestens dreijährigen Berufserfahrung im Gebiet IT-Sicherheit vertiefte Kenntnisse in allen relevanten Teilgebieten der Informationssicherheit – von rechtlichen Anforderungen über Public Key Infrastrukturen bis zur Sicherheit mobiler Endgeräte.

In unseren fünftägigen T.I.S.P. Schulungen erhalten Sie einen kompakten Überblick über alle für die Zertifizierung relevanten Wissensgebiete. Zur Vorbereitung schicken wir Ihnen vorab das von uns verfasste 700seitige Begleitbuch zum T.I.S.P. („Zentrale Bausteine der Informationssicherheit“, 2. Auflage 2014).

2015 geben wir Ihnen noch drei Mal die Gelegenheit das T.I.S.P.-Zertifikat zu erwerben: im Juni (**22.–26.06.**), September (**21.–25.09.**) und November (**23.–27.11.**). Sichern Sie sich Ihren Platz!

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

Mehr Sicherheit im Mittelstand

Über 100 Verantwortliche für Datenschutz und IT-Sicherheit aus Unternehmen der TechnologieRegion Karlsruhe folgten am 19.05.2015 den Praxisberichten und Expertenvorträgen auf dem 7. Tag der IT-Sicherheit in Karlsruhe. Wer die Veranstaltung verpasst haben sollte, findet die Pressemitteilung und die Vortragsunterlagen (zu den Themen Risiko Mensch und Technik, Aktuelle Entwicklungen zu ‚Privacy by Design‘, Sicherheit im Always-On, Designprinzipien für sichere Systeme, Intrusion Prevention Systeme) ab sofort auf http://www.tag-der-it-sicherheit.de.

Das nächste Event der Karlsruher IT-Sicherheitsinitiative findet statt am **16.07.2015** im Panoramasaal der IHK Karlsruhe. Dort wird Dominik Schadow über Java-Security sprechen – wer ‚Java‘ sagt, sollte auch ‚sichere Softwareentwicklung‘ meinen …

Veranstaltungshinweise

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

Juni 2015	
08.-12.06.	Audit Challenge 2015 (Frankfurt School of Finance & Management, Frankfurt)
15.-16.06.	DuD 2015 (COMPUTAS Gisela Geuhs GmbH, Berlin)
19.06.	Workshop: Social Media Security (Fachgruppe SECMGT der Gesellschaft für Informatik e.V., Frankfurt)
22.-26.06.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)>
August 2015	
01.-06.08.	Blackhat USA 2015 (Blackhat, Las Vegas/US)
06.-09.08.	DEF CON 23 (DEFCON, Las Vegas/US)
09.-13.08.	15th Annual DFRWS Conference 2015 (DFRWS, Philadelphia/US)
12.-14.08.	24th USENIX Security Symposium (Usenix, Washington D.C./US)
16.-20.08.	Crypto 2015 (IACR, Santa Barbara/US)
31.08.	Sommerakademie (ULD, Kiel)

Fundsache

Am 12.01.2015 hat die ENISA einen 78seitigen Report „Privacy and Data Protection by Design" veröffentlicht. Darin versuchen die Autoren, die rechtlichen Anforderungen und technischen Möglichkeiten in Überdeckung zu bringen. Lesenswert sind die „Eight Privacy by Design Strategies" und der profunde Überblick über aktuelle Privacy Enhancement Technologies. 211 Referenzen belegen die breite fachliche Abdeckung.

Impressum

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

ISSN 1613-4311

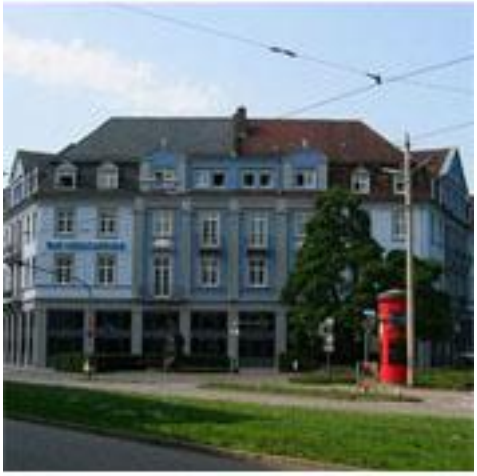
Autoren: Dirk Fox (Editorial), Dr. Yun Ding, Michael Knopp, Christoph Schäfer

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Juni 2015

Von Medizinern lernen

Dass eine gesetzliche Immunität nicht vor Trojanerangriffen schützt mussten jüngst auch die Abgeordneten des Deutschen Bundestages schmerzlich erfahren. Und sie sind in guter Gesellschaft: Die Zahl der Fälle, in denen Angreifer über gut gemachte E-Mail-Anhänge und unveröffentlichte Sicherheitslücken (Zero-Day-Attacken) in Unternehmen eindringen, nehmen nachweislich zu.

Dabei sind die bekannten Fälle möglicherweise nur die Spitze eines (großen) Eisbergs: Wie im Bundestag bleiben die Angriffe häufig lange unentdeckt. Denn komplexe Angriffssoftware kümmert sich auch um den eigenen Schutz: Mit herkömmlichen Tools ist sie meist nicht aufzuspüren, und wenn die Aktivitäten des Trojaners unterhalb der Wahrnehmungsschwelle des Benutzers bleiben, schöpft dieser auch keinen Verdacht.

Gegen Angriffe dieser Art ist unser etabliertes Instrumentarium – ein Sicherheitskonzept plus präventive Schutzsysteme – schnell mit seinem Latein am Ende. Da hilft auch kein ‚fingerpointing' auf das Risiko vor dem Bildschirm – denn bei einem sorgfältig vorbereiteten, gezielten Angriff ist ‚Aufpassen' keine adäquate Schutzmethode. Wenn schon der Virenscanner die Schadsoftware nicht erkennen kann, wie soll dies dann dem Anwender glücken?

Vielleicht müssen wir angesichts dieser Herausforderungen den Beruf des Informations-Sicherheitsbeauftragten neu denken. Denn es geht uns inzwischen ähnlich wie den Medizinern: Auch wenn wir die Zusammenhänge immer besser verstehen, werden Krankheiten komplexer, Therapien spezialisierter, entwickeln Viren Resistenzen gegen bislang wirksame Medikamente und suchen sich neue Infektionswege. Neue Medikamente haben wiederum unbekannte Nebenwirkungen – damit steigt die Unübersichtlichkeit. Mediziner haben darauf mit Diversifizierung und Spezialisierung reagiert. Dabei haben sie gegenüber uns Technikern einen uneinholbaren Vorteil: Ihre Patienten heilen meist von selbst. Auch trotz der Therapie.

Inhalt

secorvo
security consulting

Security News

Der Chirurg

Der unvermeidliche ‚Trade-off' zwischen erzielbarer Sicherheit und Benutzerakzeptanz kann gelegentlich den Chirurgen erfordern. Denn manchmal geht es nicht ohne operativen Eingriff.

So benötigen Trojaner einen Kommunikationsweg, um von einem Endsystem aus mit dem Angreifer zu kommunizieren. Schneidet man das Unternehmensnetz in mehrere Teilnetze, so kann man die externe und interne Kommunikation entkoppeln. Das Surfen im Internet lässt sich beispielsweise über einen Terminalserver mit Browser realisieren, während das Endsystem nur auf das interne Netz zugreifen kann. Hat der Browser eine Malware eingefangen, kann diese nicht auf interne Daten zugreifen. Der Download von Daten aus dem Internet funktioniert dann allerdings nicht mehr ganz so bequem über einen Quarantänebereich.

Der Internist

Die aktuellen Infektionswege zwingen zu einer genaueren Beschäftigung mit den inneren Organen. So können durch eine Separierung von Anwendungen deren Daten vor anderen, möglicherweise infizierten ‚Organen' geschützt werden. Technisch realisierbar ist so etwas über Virtualisierungslösungen wie Qubes OS oder Docker. Dabei läuft jede Anwendung in einem eigenen Kontext, damit bei einem Sicherheitsproblem nur die jeweilige virtuelle Plattform betroffen ist, nicht aber das Gesamtsystem oder weitere Anwendungen. Der Datenaustausch zwischen diesen Plattformen sollte restriktiv gehandhabt werden.

Leider ist dieser hochinteressante Ansatz ab Werk bisher nur für eine Handvoll Anwendungen wie Firefox, Thunderbird und Libreoffice verfügbar. Für eigene Anwendungen muss ggf. eine Windows-VM etabliert werden.

Der Infektionsschutz kann durch die Innere Medizin erheblich gesteigert werden. Risiken und Nebenwirkungen sollten jedoch mit den betroffenen Benutzern abgestimmt werden.

Der Psychologe

Der Psychologe kümmert sich um den Menschen, darum, was dieser denkt und fühlt. Ihn interessieren weniger technische Lösungen sondern Maßnahmen, die auf das Verhalten der Menschen zielen. Er greift da ein, wo es in ungesunder Weise von der gesetzten Norm abweicht.

Eines seiner Instrumente ist die Durchführung wirksamer Awareness-Kampagnen, die mit Wahrnehmungs- und Verhaltensgewohnheiten brechen und einprägsam wesentliche Kernbotschaften vermitteln. Statistiken und Messungen helfen ihm, den Erfolg seiner Maßnahmen zu überprüfen.

Der Labordiagnostiker

Die Labordiagnostik untersucht Proben auf Befunde und versucht, aus den Ergebnissen zusammen mit der Bewertung anderer Symptome eine Diagnose zu erstellen. Auch in der Informationssicherheit sollte man die Diagnose nicht allein auf Symptome wie Anzeichen für Schwächen oder Berichte über Vorfälle stützen. Ein Labordiagnostiker solle regelmäßig Proben analysieren, um Infektionsgefahren frühzeitig zu erkennen. Die Ergebnisse von Schwachstellenscans und Penetrationstest können Handlungsbedarf aufzeigen.

Wie in der Medizin sind auch hier Erfahrung und die richtigen Werkzeuge der Schlüssel zur zutreffenden Diagnose. Konkrete Ansätze findet man z. B. bei PCI, beim BSI, beim NIST sowie im OWASP OTG und OWASP ASVS.

Der Notarzt

Gelegentlich sind akut lebensrettende Maßnahmen für die Versorgung eines Notfallpatienten erforderlich. Treten eine Störung des Bewusstseins, der Atmung, des Kreislaufes oder Lähmungen, Verbrennungen, Vergiftungen, Schuss-, Stich- oder Hiebverletzungen lebenswichtiger Organe auf, sollte spätestens 10 bis 15 Minuten nach Eingang des Notrufs der Notarzt seinen Einsatzort erreichen. Kommt er zu spät, können auch Fachwissen und Reanimation dem Notfallpatienten meist nicht mehr helfen.

Zwar ist auch der Notarzt der Informationstechnik gelegentlich von einem Fehlalarm betroffen. Oft aber stößt er auf zunächst unerklärliche Effekte auf der Ebene der Betriebssysteme oder im Netzwerkverkehr, die Symptome einer getarnten Schadsoftware sein können.

Die Auswertung von zusammengeführten Logdaten und Netflows bringt ihn, manchmal mit Unterstützung des »*Labodiagnostikers* oder, wenn er zu spät gekommen ist, des »*Pathologen*, auf die Spur des Krankheitsbilds und erlaubt ihm eine Einschätzung, wie kritisch der Grad der Verletzung bzw. der Infektion für das einzelne System und die gesamte Infrastruktur ist. Wird er zu spät gerufen, lassen sich betroffene Infrastrukturbereiche nicht mehr isolieren und es bleibt ihm nur, der IT eine Totenbescheinigung auszustellen.

secorvo
security consulting

Der Anästhesist

Der Anästhesist sorgt dafür, dass die Vitalfunktionen des Patienten während operativer und diagnostischer Eingriffe aufrechterhalten werden. Ein medizinischer Eingriff ist eine Krise – und der Anästhesist ihr Manager. Egal ob sich ein Hackerangriff, ein Systemausfall oder eine sonstige Krise im Unternehmen ereignet: es bedarf eines Krisenmanagers, der den Überblick und den Puls des Unternehmens im Auge behält, der mit allen Beteiligten in Kontakt steht und sie bei Bedarf beruhigt. Das gilt gleichermaßen für interne Beteiligte wie für interessierte Dritte, etwa die Presse.

Vor allem aber muss er den Patienten im Blick behalten, damit der Eingriff, die Säuberung der IT-Systeme und der Tausch von Hard- und Software, trotz des Zeitdrucks in geordneten Bahnen verläuft.

Der Anästhesist muss sich in vielen Disziplinen wenigstens grundsätzlich auskennen, er muss Situationen einschätzen, entscheiden und moderieren können. Vor allem aber muss er für Ruhe und Gelassenheit sorgen, damit der Patient die Operation gut übersteht.

Der Pathologe

Auch nach einer erfolgreichen (Not-) Operation gibt es noch offene Fragen. Wie konnte es dazu kommen? Was waren die Ursachen? Wie lässt sich so etwas in Zukunft vermeiden?

Der Pathologe unterstützt die Bewertung und Behandlung von Notfällen und Infektionen durch die Analyse von Gewebeproben (Biopsie) und Obduktionen. Er untersucht sowohl funktionierende IT-Systeme, bei denen Auffälligkeiten festgestellt wurden, als auch Systeme, die ohne erkennbaren Grund ihre Funktionen eingestellt haben.

Dabei gewinnt er Metadaten aus Hauptspeicherabzügen und Festplattenduplikationen und wertet diese zielgerichtet aus. Kann er die Infektion eines Systems feststellen, veranlasst er Quarantänemaßnahmen zur Eingrenzung der Ansteckungsgefahr. Sollte es zu einem Abfluss von Vitaldaten gekommen sein, werden die Nachweise so dokumentiert, dass sie im Streitfall gerichtsverwertbar sind.

Das Gesundheitsamt

Die Gesundheitsämter wachen über Hygiene und Epidemien. Eine wesentliche Säule sind Meldepflichten, die auch in der IT-Sicherheit langsam Einzug in Gesetze halten. Beispiele sind § 109a TKG, § 42a BDSG, § 15a TMG oder § 83a SGB X. Hinzu kommt die Einführung von Meldepflichten in dem vor der Verabschiedung stehenden IT-Sicherheitsgesetz: § 8b Abs. 4 BSIG-E wird künftig die Betreiber kritischer Infrastrukturen zur Meldung verpflichten.

Empfänger der Meldungen sind die Datenschutzaufsichtsbehörden, die Bundesnetzagentur und künftig das Bundesamt für Sicherheit in der Informationstechnik (BSI). Ähnlich den Datenschutzaufsichtsbehörden kann auch das BSI bald Auflagen zur Beseitigung von Sicherheitsmängeln erteilen.

Damit entsteht eine staatliche, auf Informationssicherheit bezogene Aufsicht. Im Gesundheitswesen wurde mit den Gesundheitsämtern der Grundstein für eine erfolgreiche Epidemiebekämpfung gelegt.

Secorvo News

Secorvo ist ‚Top Consultant'

Am vergangenen Freitag, den 26.06.2015, wurde Secorvo in Essen als eines der besten deutschen Beratungsunternehmen für den Mittelstand ausgezeichnet. Das Urteil der Jury ist das Ergebnis einer Bewertung der Professionalität von Secorvo in elf Dimensionen durch zehn mittelständischen Referenzkunden, die wissenschaftlich ausgewertet wurde. Die Auszeichnung überreichte Bundespräsident a. D. Christian Wulff.

Wer ‚Java' sagt, sollte auch sichere Softwareentwicklung meinen.

Die Sicherheit von Java-Webanwendungen hatte lange Zeit einen guten Ruf. Tatsächlich ist Java jedoch nicht sicherer oder unsicherer als andere Programmiersprachen. Spätestens mit den zahlreichen Java-Sicherheitsproblemen der vergangenen Jahre hat sich diese Erkenntnis herumgesprochen. Auf dem nächsten KA-IT-Si-Event am **16.07.2015** stellt Dominik Schadow (BridgingIT) in seinem Vortrag Sichere Webanwendungen mit Java typische Fallstricke bei der Planung, Entwicklung und Wartung von Java-Webanwendungen vor und zeigt, wie man diesen wirkungsvoll in allen Phasen eines Entwicklungsprojekts zu Leibe rücken kann (zur Anmeldung).

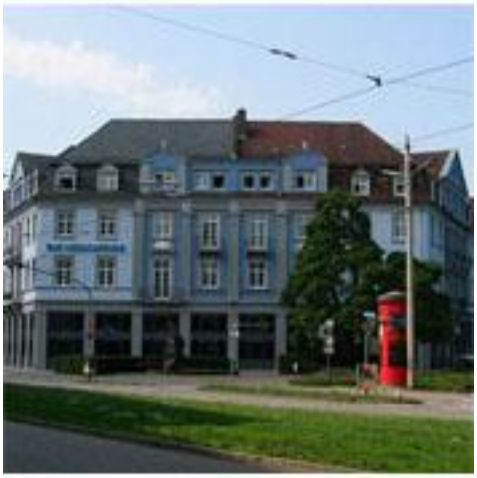
Veranstaltungshinweise

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

Juli 2015	
16.07.	Wer 'Java' sagt, sollte auch sichere Softwareentwicklung meinen. (KA-IT-Si, Karlsruhe)
August 2015	
01.-06.08.	Blackhat USA 2015 (Blackhat, Las Vegas/US)
06.-09.08.	DEFCON 23 (DEFCON, Las Vegas/US)
09.-13.08.	15th Annual DFRWS Conference 2015 (DFRWS, Philadelphia/US)
12.-14.08.	24th USENIX Security Symposium (Usenix, Washington D.C./US)
16.-20.08.	Crypto 2015 (IACR, Santa Barbara/US)
31.08.	Sommerakademie (ULD, Kiel)
September 2015	
08.-09.09.	D•A•CH Security (Gemeinsame Arbeitskonferenz GI OCG BITKOM SI TeleTrusT, Sankt Augustin)
15.-17.09.	Future Security 2015 (Fraunhofer VVS, Berlin)
17.09.	Informationstag "Elektronische Signatur" 2015 (TeleTrust, Berlin)
21.-25.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Fundsache

Wer schon immer wissen wollte wie Gedankenlesen funktioniert - im folgenden 2,5minütigen Video wird dieses Mysterium aufgelöst.



Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Michael Knopp, Christoph Schäfer, Jochen Schlichting

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Juli 2015

… denn sie wissen nicht, was sie tun.

Siebzig Jahre ist es her, dass James Dean in kürzester Zeit die unbekümmerte Ungezügeltheit der Jugend salonfähig machte. Daran konnten auch die Umstände seines frühen Todes nichts ändern. Und sein Vermächtnis wirkt offenbar bis heute fort.

So ist es in den vergangenen 20 Jahren endlich Schritt für Schritt gelungen, Sicherheit als eine wesentliche Eigenschaft eines IT-Systems zu verankern. Kaum ein Anbieter, der sich der Frage der Sicherheit eines neuen IT-Produkts nicht widmen würde – und sei es auf den letzten Metern vor der Produktivschaltung. Das ist das Ergebnis eines mühsamen, oft von unangenehmen (und vermeidbaren) Lernerfahrungen begleiteten Prozesses.

Doch kaum ist es so weit, konterkariert das „Internet der Dinge" diese Entwicklung auf erschreckende Weise: Elektrische Skateboards lassen sich via Bluetooth unter fremde Kontrolle bringen, kontaktlose „Smart-Keys" schalten das Fahrzeug einfach aus, wenn Mitfahrer sie während der Fahrt aus dem Fenster werfen. Ein Automobilhersteller liefert Autos mit Internet-Zugang, die sich während der Fahrt von unberechtigten Dritten steuern und manipulieren lassen – und bittet anschließend seine Kunden, einen Patch über das Internet herunterzuladen und via USB-Stick zu installieren (siehe diese SSN). Schließlich kommt ein 13.000 US$ teures Präzisionsgewehr auf den Markt, bei dem Unberechtigte die Zieleinrichtung via WLAN umkonfigurieren können.

In Fragen der Sicherheit scheint ungezügelte, von Kompetenz unbelastete Produktentwicklung im Internet der Dinge wieder „En Vogue" zu sein – ungeachtet der um ein Vielfaches größeren Gefahren, die dabei für Leben und Gesundheit drohen. Wir können nur hoffen, dass die Lernkurve diesmal steiler und kürzer ausfällt.

Inhalt

secorvo
security consulting

Security News

Mit Daten bezahlen

Was lange von Datenschützern befürchtet wurde, wird nun wahr: Ab 2016 werden unsere Gesundheitsdaten zur Währung. Die Generali plant die Einführung ihres Tarifs „Vitality“ in 2016. Per Smartphone-App können Versicherte Fitnessdaten an Generali übermitteln und werden für einen gesunden Lebensstil mit Rabatten belohnt. Derweil hat Apple am 16.07.2015 ein Verfahren zum Patent angemeldet, mit dem Nutzern eines Smartphones oder Tablets nur dann bestimmte Werbeanzeigen eingeblendet werden, wenn sie sich die beworbenen Produkte oder Dienste auch leisten können. Festgestellt wird das anhand von Bank- oder Prepaid-Guthaben.

Noch sind solche Angebote die Ausnahme, und nur eine Minderheit von freiwilligen „First Movern“ wird sie nutzen. Irgendwann aber wird sich das Blatt wenden. Wer seine Daten dann nicht als Zahlungsmittel einsetzt, wird unter Rechtfertigungsdruck geraten. Mit Freiwilligkeit hat die Datenpreisgabe dann nichts mehr zu tun.

Clipper reloaded

Vor gut 22 Jahren, am 16.04.1993, löste die US-Regierung mit einer Pressemitteilung zum Clipper-Chip eine heftige Debatte über Verschlüsselung aus. Sie plante damals die Einführung einer Telefonie-Verschlüsselung mit einer Zugriffsmöglichkeit für die Strafverfolgungsbehörden. Die öffentliche Diskussion mündete schließlich 1997 in einer öffentlichen Stellungnahme führender Kryptologen mit dem Titel „*The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*“, die dazu beitrug, dass in den USA und Europa die Regulierung von Verschlüsselung aufgegeben wurde.

Aber Geschichte wiederholt sich. Begehrlichkeiten von Ermittlungsbehörden, wie sie von FBI-Direktor James B. Comey am 16.10.2014 ausgesprochen wurden, haben eine Kryptodebatte 2.0 losgetreten. Daher haben nun die Autoren der Stellungnahme von 1997 erneut Position bezogen. In ihrem Papier „*Keys Under Doormats*“ vom 06.07.2015 machen sie deutlich, dass Zugriffsmöglichkeiten für Strafverfolgungsbehörden auf verschlüsselte Daten die Fortschritte bei der Sicherheit im Internet konterkarieren: durch höhere Komplexität, zentrale Angriffspunkte und Hintertüren, die von Dritten ausgenutzt werden können. Es ist zu hoffen, dass das Papier den Gegnern offener Kryptografie den Wind genauso aus den Segeln nehmen wird wie die Stellungnahme 19 Jahre zuvor.

Ferngesteuert in den Graben

Chris Valasek und Charlie Miller sorgten am 21.07.2015 mit der Veröffentlichung eines Hacks, den sie auf der diesjährigen BlackHat vorstellen werden, bei Autofahrern für Gänsehaut: Es gelang ihnen, mittels einer Schwachstelle im Uconnect-Bordsystem über das Internet direkt auf Fahrzeuge verschiedener Marken des Konzerns Fiat-Chrysler (unter anderen Jeep, Fiat und Alfa Romeo) zuzugreifen. So konnten sie bei einem gekaperten Jeep Cherokee nicht nur die Bordelektronik (Klimaanlage, Radio) fernsteuern, sondern bekamen auch sicherheitskritische Komponenten unter ihre Kontrolle: Sie konnten Hupen, Bremsen deaktivieren und in die Lenkung eingreifen. Auch beim Umgang mit der Schwachstelle schwächelte Chrysler – und bot über die Uconnect-Webseite ein Executable zum Download für die Installation via USB-Stick an.

Die Schwachstelle ist kein Einzelfall, wie Valasek und Miller bereits 2014 in einer 100seitigen Studie belegten. Sie beweist aber überdeutlich, dass durch die für die Vernetzung von Auto und Smartphone erforderliche Anbindung an das Internet neue Bedrohungen entstehen – und sich auch traditionelle Industriezweige ernsthaft mit Security Engineering befassen sollten.

Sozialadäquanz als Erlaubnistatbestand?

Schon in den SSN 3/2015 berichteten wir über die geplante Neufassung von § 2 BORA (Berufsordnung der Rechtsanwälte), die das Outsourcing bei Berufsgeheimnisträgern legalisieren sollte. Der Bundesjustizminister hatte den Beschluss mit Verweis auf die mangelnde Regelungsbefugnis am 04.03.2015 aufgehoben. Auf Intervention der Bundesrechtsanwaltskammer wurde die Aufhebung am 31.03.2015 wieder rückgängig gemacht und die Neuregelung trat am 01.07.2015 in Kraft.

Damit ist die Inanspruchnahme von Leistungen Dritter nun auch bei Gefahr einer möglichen Offenbarung von geheimen Inhalten zulässig, wenn sie „objektiv einer üblichen, von der Allgemeinheit gebilligten Verhaltensweise im sozialen Leben entspricht (Sozialadäquanz)“. Bisher machte sich ein Berufsgeheimnisträger durch unbefugte Offenbarungen strafbar, wenn er bspw. externe IT-Dienstleistungen in Anspruch nahm, bei denen er mit eigenen Mitteln einen unberechtigten Zugriff auf die Daten kaum verhindern konnte.

Bei allem Verständnis für das Dilemma: Die Argumentation der Rechtsanwaltskammer ist angesichts des hohen Schutzgutes gefährlich. Soll ein ungenügender Schutz, der üblich wird, künftig als Legitimationsgrundlage taugen?

Weisungsfreiheit externer DSBs

Das Landesarbeitsgericht Düsseldorf hat in einem jüngst veröffentlichten Urteil vom 04.03.2015 wichtige Standpunkte zur Stellung eines in einem Drittunternehmen angestellten, persönlich bestellten externen Datenschutzbeauftragten ausgeführt. Darunter sind für externe Datenschutzbeauftragte die folgenden Aussagen besonders interessant:

Die arbeitsvertragliche Weisungsgebundenheit des zum externen DSB persönlich bestellten Unternehmensmitarbeiters steht der Weisungsfreiheit gegenüber der verantwortlichen Stelle nicht entgegen. Auch das Benachteiligungsverbot betrifft nur das Vertragsverhältnis zur verantwortlichen Stelle. Eine persönliche Bestellung darf allerdings dem Angestellten eines dritten Unternehmens nicht aufgedrängt werden, es sei denn, dies ist Teil der arbeitsvertraglichen Leistung.

Tatsächlich ist die BDSG-konforme Bestellung eines externen Datenschutzbeauftragten unter Experten umstritten. Durch diese Entscheidung wird die Bestellung von Angestellten aufgewertet – ein bislang eher kritisch betrachteter Weg. Zu empfehlen ist er wegen des Auseinanderfallens von Bestellung und Leistungsvertrag dennoch nicht.

Einjährige Hackerin

Am 18.07.2015 gelang einem einjährigen Mädchen ein unfreiwilliger Hack des VW Passat ihrer Mutter: Es warf auf der A1 den Schlüsselbund mitsamt dem Smart-Key des Passat aus dem Fenster. Sofort schaltete sich der Motor aus – die Mutter konnte den Wagen glücklicherweise noch unfallfrei auf den Standstreifen lenken.

Offenbar ist der Hersteller hier bei der Bedrohungsanalyse zu kurz gesprungen. Bequemlichkeit sollte besser nicht vor Sicherheit gehen, schon gar nicht, wenn dadurch Leib und Leben in Gefahr geraten können. Auch bei Automobilzulieferern sollte man besser Security Engineering praktizieren.

Side-Channel in der Cloud

Auf der diesjährigen Recon stellte Sophia D'Antoine am 19.06.2015 einen sehr interessanten Side-Channel Angriff auf virtuelle Maschinen (VM) vor. VMs nutzen Hardware-Ressourcen gemeinsam; die virtuellen Instanzen und die darauf verarbeiteten Daten werden über einen Hypervisor getrennt. D'Antoines Angriff liest über den gemeinsamen Zugriff zweier VMs auf die Level-3-Caches des Prozessors Daten der VMs untereinander aus. Yuval Yarom und Katrina Falkner zeigten bereits am 05.07.2013 in „aFLUSH+Reload: A High Resolution, Low Noise, L3 Cache Side-Channel Attack", wie von einer Angreifer-VM aus z. B. auf den privaten PGP-Schlüssel in einer zweiten VM zugegriffen werden kann.

Wer vertrauliche Daten in der Cloud verarbeitet sollte nicht nur seinen Provider, sondern auch seine unmittelbaren Nachbarn auf Vertrauenswürdigkeit prüfen: Auch Hardware sollte man besser nicht unbesehen mit jedermann teilen.

Secorvo News

Secure Coding

Kaum ein Angriff, der zu seiner Durchführung nicht auf eine Software-Schwachstelle angewiesen wäre. Daher gilt: Wer das Übel an der Wurzel packen möchte, muss dafür sorgen, dass Software sicherer wird. Seit einigen Jahren engagiert sich Secorvo deshalb für sichere Software-Entwicklung und unterstützt Unternehmen mit entsprechenden Trainings.

Neben dem Seminar „Certified Professional for Secure Software Engineering" (CPSSE) sind daraus nun zwei Seminare speziell für Softwareentwickler entstanden: Für Java- und für C/C#-Entwickler bietet Secorvo College ab Oktober zwei Schulungen, die vermitteln, wie Sicherheit „programmiert" werden kann. Java Security findet statt am 13.-16.10.2015, und Secure Coding C/C# bieten wir an am 01.-03.12.2015.

T.I.S.P., PKI und aktuelle Fragen

Ende September (21.-25.09.2015) und Ende November (23.-27.11.2015) können Sie Ihre Kenntnisse und Erfahrungen mit dem T.I.S.P.-Zertifikat krönen – beim „Seminar zum Buch".

Schon einige hundert Teilnehmer haben sich mit unserem laufend aktualisierten Hands-on-Seminar „PKI – Grundlagen, Vertiefung, Realisierung" mit CAs, CRLs und OCSP vertraut gemacht. Die nächste Gelegenheit für die Teilnahme an diesem PKI-Steilkurs bietet sich Ihnen am 20.-23.10.2015 (schnelle Buchung empfohlen).

Mit der Neuauflage unseres Seminars IT-Sicherheit heute – das Schlaglicht auf die Informationssicherheit setzen wir auf aktuelle Themen mit hoher Relevanz für die Praxis – und auf eine Kombination auf konzentrierter Wissensvermittlung, Erfahrungsaustausch und Diskussion. Nächster Termin: 29.09.-01.10.2015.

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

Veranstaltungshinweise

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

August 2015	
01.-06.08.	Blackhat USA 2015 (Blackhat, Las Vegas/US)
06.-09.08.	DEF CON 23 (DEFCON, Las Vegas/US)
09.-13.08.	15th Annual DFRWS Conference 2015 (DFRWS, Philadelphia/US)
12.-14.08.	24th USENIX Security Symposium (Usenix, Washington D.C./US)
16.-20.08.	Crypto 2015 (IACR, Santa Barbara/US)
31.08.	Sommerakademie (ULD, Kiel)
September 2015	
08.-09.09.	D·A·CH Security (Gemeinsame Arbeitskonferenz GI OCG BITKOM SI TeleTrusT, Sankt Augustin)
15.-17.09.	Future Security 2015 (Fraunhofer VVS, Berlin)
17.09.	3. Deutscher Rechenzentrumstag (proRZ Rechenzentrumsbau GmbH, Freiburg)
21.-25.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
21.-22.09.	OWASP AppSec USA 2015 (OWASP Foundation, San Fransisco/CA)

Fundsache

Am 23.07.2015 veröffentlichte Google die Ergebnisse der Studie *Comparing Expert and Non-Expert Security Practices*. Die Befragung von über 500 Experten und Laien zeigt Aufklärungsbedarf: Während Experten Software-Updates für die wichtigste Maßnahme halten, setzen Laien auf Antivirus-Software – bei Experten nicht unter den fünf wichtigsten.

Impressum

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

ISSN 1613-4311

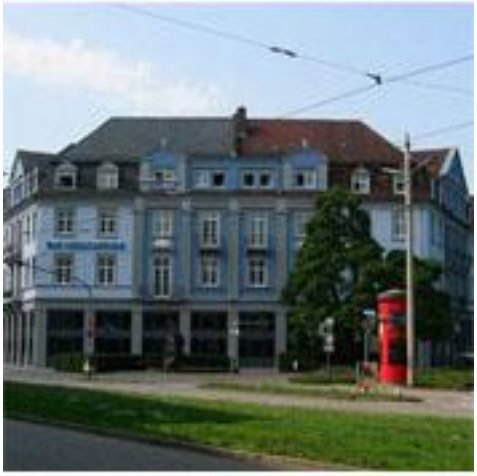
Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Christoph Schäfer

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

August 2015

Das bislang beste Windows?

Was ein unaufgefordert erschienenes hartnäckiges Windows-Symbol wochenlang angekündigt hatte, stand am 29.07.2015 endlich zum Download bereit: Windows 10. Microsoft hat von Apple gelernt: Upgrades verteilen sich einfach besser, wenn sie nichts kosten. Und, man muss es Microsoft lassen, das Upgrade klappt schnell und problemlos. Bei Windows 8 fühlt es sich eher wie ein Update an, bei dem der nervige Metro-Screen abgeschaltet wird.

Nachdem Microsoft sich mit Windows 8 – einer komplett am Bedarf von Windows-Nutzern vorbeigegangenen Entwicklung – eine blutige Nase geholt hatte, sollte nun alles besser werden. Und eigentlich hatte man bisher das Gefühl, Microsoft hätte im Rahmen von Office 365 gelernt, dass – zumindest in Europa und speziell in Deutschland – der Datenschutz ein entscheidendes Kriterium ist.

Die Ernüchterung folgt nach der Installation, denn die nächste Stunde benötigt man dafür, die Datensammelwut – inklusive der Vergabe einer eindeutigen Werbe-ID – in unzähligen Einstellungen zu begrenzen. Vollständig abstellen lässt sie sich nicht. Dass man zur Installation ein Microsoft-Live-Konto benötigt, daran hatten sich Windows 8-Nutzer schon gewöhnt. Man konnte (und kann) anschließend immerhin den Offline-Modus aktivieren. Karl Klammers Nachfolgerin heißt nicht Siri, sondern Cortana und sammelt alles, was sie zu lesen oder hören bekommt.

Überflüssig zu erwähnen, dass ein Aufschrei zur Datensammelwut folgte. In Russland prüft der Generalbundesanwalt bereits Anzeigen. Microsofts Selbstwahrnehmung ist hingegen eine andere – und natürlich ist man unheimlich transparent.

Microsoft scheint das Prinzip „Lernen durch Schmerzen“ fest in seinen Entwicklungsprozessen verankert zu haben. Das bislang beste Windows? Funktional mag das stimmen, dennoch bleibt XP ungeschlagen. Vielleicht lernen sie es ja noch ...

Inhalt

secorvo
security consulting

Security News

Websites im Fokus

Bereits im Juni haben die Datenschutzaufsichtsbehörden von Hamburg, Bayern und Baden-Württemberg bekanntgegeben, gezielt Webportale auf Datenschutz und Datensicherheit zu prüfen. Derzeit prüfen die Aufsichtsbehörden die Datensicherheit noch auf der Grundlage von § 13 Abs. 4 TMG anhand von Fragebögen.

Nun sind die gesetzlichen Sicherheitspflichten aus dem TMG durch das am 25.07.2015 in Kraft getretene IT-Sicherheitsgesetz verschärft worden. Es ergänzt § 13 TMG um weitere Pflichten: Geschäftsmäßige Anbieter von Telemedien haben nun technisch-organisatorische Maßnahmen zu ergreifen, um unerlaubte Zugriffe auf die genutzten technischen Einrichtungen zu verhindern. Außerdem sind die Angebote gegen Störungen, auch durch Angriffe, und unbefugte Zugriffe auf personenbezogene Daten nach dem Stand der Technik zu schützen. Eine Maßnahme hierzu sollen anerkannte Verschlüsselungsverfahren sein. Bei Verstößen können die Datenschutz-Aufsichtsbehörden Bußgelder von bis zu 50.000 € verhängen.

Bei Vorfällen wie dem Ashley Madison Hack müssen deutsche Anbieter künftig neben allem anderen ein Ordnungswidrigkeitsverfahren wegen unzureichender Sicherheitsmaßnahmen fürchten. Dabei werden sich dokumentierte Sicherheits-Maßnahmen und Sicherheitskonzepte auszahlen. Damit steigt der Druck auf Anbieter, sich systematisch mit Sicherheitsfragen auseinanderzusetzen. Der pauschale Verweis des Gesetzes auf Verschlüsselungstechnik wirkt allerdings ein wenig naiv.

Automatisierbare Bedrohungen

Am 31.07.2015 stellte Colin Watson das OWASP-Projekt „OWASP Automated Threat Handbook v1.00“ vor. Mit diesem Handbook will die Projektgruppe auf relevante, automatisierbare Bedrohungen von Webanwendungen hinweisen, die bisher höchstens am Rande betrachtet wurden. Wir empfehlen dieses Dokument jedem Entwickler, um geeignete Schutzmechanismen gegen solche weniger bekannten Bedrohungen zu implementieren. Entscheidern und Architekten sei zumindest ein Blick in die zweiseitige Zusammenfassung angeraten.

Experten und Laien

Google-Mitarbeiter publizierten am 23.07.2015 die Ergebnisse einer Studie, in der vergleichend untersucht wurde, welche IT-Sicherheitsmaßnahmen 230 befragte Security-Experten für wirksam halten und an welche Maßnahmen 290 interviewte Laien glauben. Von den zahlreichen detaillierten Ergebnissen der Studie überrascht vor allem die Erkenntnis, dass nur der „Umgang mit Passwörtern“ bei beiden Gruppen zu den fünf wirkungsvollsten Sicherheitsmaßnahmen zählt. Während Laien an die Wirksamkeit von Virenschutz glauben, setzen Experten darauf, ihre Systeme auf einem möglichst aktuellen Stand zu halten. Statt eines regelmäßigen Passwort-Wechsels bevorzugen Experten komplexe und einmalige Passwörter, die sicher aufbewahrt werden, oder Mehrfaktorauthentifizierung. Und nur Laien glauben daran, dass man einer Webseite ihre Vertrauenswürdigkeit ansehen kann.

Die Ergebnisse machen deutlich, dass eine verbesserte Aufklärung von Laien über wirksame IT-Sicherheitsmaßnahmen notwendig ist, wenn man nicht immer mehr Jessicas riskieren will.

Recht auf Vergessen? Vergiss es...

Das so genannte „Recht auf Vergessen“, das der Europäische Gerichtshof in seiner Google Spain-Entscheidung vom 13.05.2014 (SSN 5/2014) geprägt hat, bleibt weiter umstritten. Eine Anordnung der französischen Datenschutzaufsichtsbehörde CNIL vom 12.06.2015, beantragte Sperrungen weltweit auf alle Google-Domains zu erstrecken, beantwortete Google am 30.07.2015 in einem Blog-Beitrag: Das durch den EuGH formulierte „Recht auf Vergessen“ sei auf Europa beschränkt. Es sei keinem Land erlaubt, zu bestimmen, was in einem anderen Land zugänglich gemacht werde. Ansonsten drohe das restriktivste nationale Recht weltweit zum Maßstab der Freiheit im Internet zu werden. Dass Google dabei staatliche Zensurbestrebungen und Daten- oder Persönlichkeitsschutz in einen Topf wirft, zeigt deutlich das andauernde Unverständnis für europäisches Recht.

Derweil hat das OLG Hamburg über die Löschpflicht der Anbieter der Ursprungsseiten entschieden. Es bejaht einen Unterlassungs-Anspruch auch gegen den veröffentlichenden Website-Anbieter. Hintergrund war die Berichterstattung über ein eingestelltes Strafverfahren auf der Seite einer Tageszeitung. Da jedoch auch die Pressefreiheit der Beklagten zu berücksichtigen war, beschränkt sich der Anspruch in Fortsetzung der Google Spain-Rechtsprechung darauf, dass der Anbieter die Auffindbarkeit durch Suchmaschinen anhand des Namens verhindert.

Selbst wenn es gelänge, die Rechtsauffassungen dies- und jenseits des Atlantik anzugleichen, zeigt die OLG-Entscheidung, wie stark beim „Recht auf Vergessen“ das Persönlichkeitsrecht mit anderen Rechten wie bspw. der Pressefreiheit kollidieren kann. Das letzte Wort ist bei diesem Thema sicher noch lange nicht gesprochen.

secorvo
security consulting

Kali 2.0

Am 11.08.2015 erschien die rundum erneuerte Version 2.0 der *Penetration Testing Destribution Kali Linux*. Seit dem Schritt von Backtrack zu Kali Linux im Jahr 2013 konnte die Distribution ihre Stellung als de facto-Standard für Penetrationstests noch weiter ausbauen. Die neue Version bringt neben etlichen aktualisierten Tools, die das Herz eines jeden Testers höher schlagen lassen, auch einen Linux Kernel der Version 4.0 und diverse grafische Benutzerumgebungen mit.

Ab dieser Version erscheint Kali als Rolling-Release mit ständig aktuellen Paketen auf Basis von Debian Testing. Neben den typischen Plattformen stehen auch Versionen für ARM, die mobile Penetration Testing Plattform Nethunter und spezielle Images für den RaspberryPi 2 bereit. Ein Blick auf die neue Version lohnt also auf jeden Fall.

Pseudonyme Nutzung

Der Streit um die Klarnamenpflicht bei Facebook geht mit einer Anordnung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, Prof. Dr. Johannes Caspar, vom 28.07.2015 in eine neue Runde. Darin wird Facebook Ireland Ltd. erneut verpflichtet, die pseudonyme Nutzung seines Dienstes zuzulassen und Sperrungen pseudonymer Accounts aufzuheben. Außerdem wird Facebook untersagt, Ausweiskopien zur Identitätsbestätigung zu verlangen. Anlass ist die Beschwerde einer Nutzerin, die von Facebook zur Angabe ihres echten Namens unter Vorlage einer Personalausweiskopie aufgefordert wurde und deren gesperrtes Profil Facebook gegen ihren Willen auf den Klarnamen umgestellt hatte, allerdings ohne das Profil freizuschalten.

Die Anordnung folgt in den Fußstapfen der im April 2013 durch das OVG Schleswig-Holstein kassierten Anordnung des Unabhängigen Landeszentrums für Datenschutz (ULD) Schleswig-Holstein. Caspar beruft sich erneut auf § 13 Abs. 6 TMG und bzgl. des Personalausweises auf § 20 Abs. 2 PAuswG. Durch die Google Spain-Entscheidung des EuGH vom 13.05.2014 (SSN 5/2014) ist das Hauptargument des OVG-Urteils von 2013 jedoch entfallen: Aufgrund der wirtschaftlichen Tätigkeit der in Hamburg niedergelassenen Facebook Germany GmbH kommt nun sehr wohl deutsches Datenschutzrecht zur Anwendung. Die Erfolgsaussichten von Caspers erneuter Anordnung sind damit erheblich gestiegen.

Secorvo News

Für Kurzentschlossene

Nutzen Sie noch im September die Möglichkeit, Ihre Erfahrungen und Kenntnisse zu vertiefen und mit einem Zertifikat zu krönen: Die T.I.S.P.-Schulung (**21.–25.09.2015**) bereitet auf die anschließende T.I.S.P.-Prüfung am 26.09.2015 vor und hilft, durch einen umfassenden Einblick in alle Gebiete der Informationssicherheit verbliebene Wissenslücken zu schließen. Zur Vorbereitung erhalten Sie nach Ihrer Anmeldung das Begleitbuch „Zentrale Bausteine der Informationssicherheit".

Der ständigen Weiterentwicklung des Themas IT-Sicherheit trägt das Seminar IT-Sicherheit heute (**29.09.–01.10.2015**) mit der Behandlung aktueller Fragestellungen Rechnung. Hier erfahren Sie das Wesentliche über die aktuellen Entwicklungen und Bedrohungen und lernen Best Practice-Vorgehensweisen kennen, mit denen Sie Ihr Unternehmen wirksam schützen können.

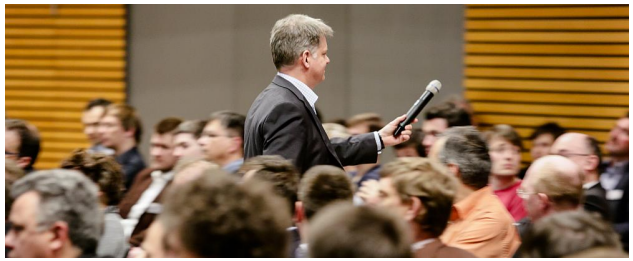
Alle Termine und das komplette Seminarangebot finden Sie unter www.secorvo.de/college.

Eine kurze Geschichte der Überwachung

Im Rahmen der Ausstellung „Globale Überwachung und Zensur" des ZKM | Zentrum für Kunst und Medientechnologie Karlsruhe geben Prof. Dr. Müller-Quade und Dirk Fox am **08.10.2015 um 18 Uhr** im Vortragssaal des ZKM | Karlsruhe einen Rück- und Ausblick auf die Geschichte und Entwicklung geheimdienstlicher Überwachung. Zur Einstimmung bietet das ZKM | Karlsruhe ab 17 Uhr für interessierte Teilnehmer eine Führung durch die Ausstellung an. Da die Zahl der Plätze beschränkt ist, bitten wir um rechtzeitige Anmeldung.

Führung und Vortragsveranstaltung finden auf Einladung des ZKM | Karlsruhe in Zusammenarbeit mit dem KIT und der Karlsruher IT-Sicherheitsinitiative statt. Sie sind **kostenfrei** – und setzen auch keine Fachkenntnisse voraus. Bringen Sie also gerne interessierte Freunde, Kollegen und Bekannte mit!

Im Anschluss an den Vortrag haben Sie die Möglichkeit, den Abend gemütlich im „mint - bistro.café.bar.catering" im Foyer des ZKM ausklingen zu lassen.



Weitere Informationen und die Möglichkeit zur Anmeldung zur Führung finden Sie auf www.ka-it-si.de. Wir freuen uns auf Ihr Kommen!

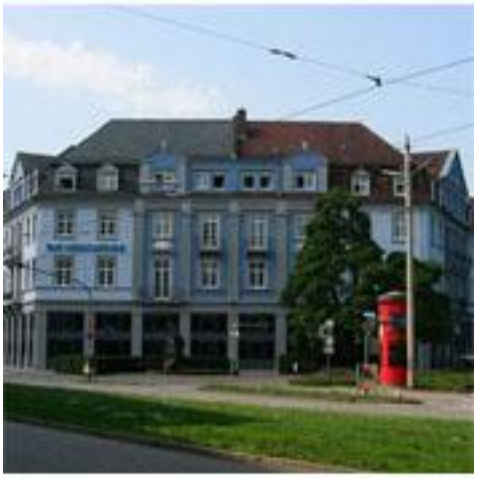
Veranstaltungshinweise

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

September 2015	
08.-09.09.	D•A•CH Security (Gemeinsame Arbeitskonferenz GI OCG BITKOM SI TeleTrusT, Sankt Augustin)
15.-17.09.	Future Security 2015 (Fraunhofer VVS, Berlin)
17.09.	3. Deutscher Rechenzentrumstag (proRZ Rechenzentrumsbau GmbH, Freiburg)
21.-25.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
21.-22.09.	OWASP AppSec USA 2015 (OWASP Foundation, San Fransisco/CA)
29.09.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
29.09.-01.10.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen & Schutzmechanismen (Secorvo, Karlsruhe)
Oktober 2015	
06.-08.10.	it-sa 2015 (NürnbergMesse GmbH, Nürnberg)>
12.-16.10.	Conference on Computer and Communications Security (CCS) (CASED/Fraunhofer SIT, Denver/USA)
13.-15.10.	15. IDACON 2015 (WEKA-Akademie, München)
13.-16.10.	Java Security (Secorvo, Karlsruhe)

Fundsache

Auf der diesjährigen 23. Konferenz DefCon präsentierten am 08.08.2015 Dan Petro und Oscar Salazar, wie sich die „Smart Safes“ Galileo des Herstellers Brink mit einem USB-Stick öffnen lassen. Auch hier hätte die Empfehlung „Schuster, bleib‘ bei deinem Leisten“ geholfen.



Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, André Domnick, Kai Jendrian, Michael Knopp, Christoph Schäfer (Editorial).

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

September 2015

Eingebettetes Vertrauen

Kaum ein Gerät, das heute nicht von Software gesteuert wird. Die wenigen verbliebenen rein mechanischen Lösungen (wie batteriefreie Armbanduhren) genießen bereits Kult-Status.

Zwar wissen wir, dass Software fehlerhaft sein kann. Aber Fehler fallen auf: Abweichendes Systemverhalten zeigt sich bei Tests, und bei unspezifischen Fehlern stürzt das System meist ab. Daher ist unser Vertrauen in ursprünglich mechanische, aber zunehmend von Software gesteuerte Geräte meist unbeeinträchtigt geblieben. In der Regel ist das auch vernünftig: Eine Waschmaschine, die zu heiß wäscht, erkennen wir an eingelaufener Wäsche. Eine Uhr, die die falsche Zeit anzeigt, erkennen wir beim Vergleich mit anderen Zeitanzeigen. Und ein Auto, bei dem die Motorsteuerung schwächelt, erkennen wir am Fahrverhalten.

Allerdings gibt es auch Systeme, bei denen Fehler weniger offensichtlich sind und eine Überprüfung schwierig ist. Wie sollten wir die Korrektheit eines Taxameters prüfen? Oder die des Kilometerzählers im Gebrauchtwagen? Und wie sollten wir bei einem Spielautomaten feststellen, dass das Gerät auch die gesetzlich vorgeschriebene Menge an Gewinnausschüttungen einhält? Genau aus diesen Gründen hat das Bundesverfassungsgericht 2009 dem Einsatz von Wahlcomputern bei Bundestagswahlen einen Riegel vorgeschoben.

Üblicherweise werden solche Geräte unabhängig geprüft. Aber wie gut kann eine solche Prüfung sein, deren Umfang weit unter dem einer „Common Criteria"-Zertifizierung liegt? Prüft der Prüfer den Source-Code? Und was ist, wenn Schadcode über die Programmierumgebung in den ausführbaren Code gelangt (siehe diese SSN)?

Die Entwicklung effizienter Verfahren, mit denen die Vertrauenswürdigkeit solcher Systeme sichergestellt und transparent gemacht werden kann, wird eine große Herausforderung der Zukunft sein.

Inhalt

secorvo
security consulting

Security News

Komplexität killt Sperrbildschirm

Ein YouTube-Video vom 20.09.2015 legte eine gravierende Schwachstelle der neuen Version 9 von Apples iOS offen: Sie ermöglicht es, den Sperrbildschirm zu umgehen und auf Kontakte und Bilder zuzugreifen. Dabei werden lediglich auf dem Sperrbildschirm verfügbare Funktionen wie der Sprachassistent Siri und die eingebaute Uhr verwendet.

Diese Verwundbarkeit reiht sich ein in zahlreiche gleichartige Schwachstellen, beispielsweise für iOS 7, Android 5 oder Windows 8. Die Ursache aller dieser Schwachstellen liegt darin, dass der Sperrbildschirm um immer mehr Funktionen erweitert wird. Wenn man aber erlaubt, dass ausgewählte Aktionen schnell und bequem durchgeführt werden können, ohne das Gerät zu entsperren, so vergrößert man zugleich die Angriffsfläche. Hersteller sollten den Sperrbildschirm nicht weiter als Platz zum Abladen von Apps oder als Schnellstartseite missverstehen, sondern als ein essentielles Sicherheitsfeature, das man besser nicht aufweicht.

Kamera-Attrappen

Nach einer kürzlich veröffentlichten Entscheidung des Landesarbeitsgerichts (LAG) Mecklenburg-Vorpommern vom 12.11.2014 (Az. 3 TaBV 5/14) unterliegt das Anbringen von Kamera-Attrappen im Außenbereich nicht der Mitbestimmung des Betriebsrats. In seiner grammatischen Auslegung des § 87 Abs. 1 Nr. 6 BetrVG stellt das LAG fest, dass eine Attrappe nicht zur Überwachung der Arbeitnehmer geeignet ist. Dass auch die Vorschriften des Bundesdatenschutzgesetzes (BDSG) keine Anwendung finden, hat der Bundesgerichtshof in einem Nachbarschaftsstreit bereits am 16.03.2010 entschieden (Az. VI ZR 176/09). Allerdings bestätigte er gleichzeitig, dass dennoch ein „Überwachungsdruck“ und damit ein Eingriff in das allgemeine Persönlichkeitsrecht vorliegen kann. Folglich kann ein zivilrechtlicher Unterlassungsanspruch gemäß §§ 1004, 823 BGB geltend gemacht und damit die Beseitigung der Kamera-Attrappe verlangt werden.

Anders als Datenschutzaufsichtsbehörden teilweise behaupten sind Attrappen demnach nicht wie echte Kameras zu behandeln. Unzulässig können sie im Einzelfall dennoch sein.

Passworttipps der Spione

Am 08.09.2015 hat der englische Geheimdienst GHCQ Hinweise zum Umgang mit Passwörtern veröffentlicht. Auch wenn man nach den Skandalen um die Geheimdienste einem solchen Dokument erst mal skeptisch gegenüber stehen mag, finden sich dort doch sinnvolle und angemessene, wenn auch nicht sonderlich überraschende Hinweise zum Umgang mit Passwörtern – gut dargestellt auf 13 Seiten. Anscheinend beschäftigen sich einige Mitarbeiter des GHCQ auch mit für die Sicherheit wertvollen Tätigkeiten.

DIN-Norm Löschkonzept

Der zuständige Arbeitskreis des DIN verabschiedete am 10.09.2015 eine weiterentwickelte Fassung der Leitlinie Löschkonzept als DIN-Norm 66398 – passend zur DIN 66399, die die Vernichtung von Datenträgern regelt. Seit Ende 2013 hatten die Deutsche Bahn, DATEV, Blancco, Secorvo und Toll Collect an diesem Projekt gearbeitet (siehe SSN 2/2014 und SSN 1/2015). Die neue DIN 66398 hilft bei der Entwicklung passender Löschkonzepte, insbesondere für personenbezogene Daten. Sie beschreibt die Elemente eines Löschkonzepts und stellt dar, wie mit Hilfe von Löschklassen Löschregeln für unterschiedliche Datenarten festgelegt werden können. Die Norm wird voraussichtlich Ende November im Beuth-Verlag erscheinen; eine englische Übersetzung ist geplant.

Für den Datenschutz ist die neue Norm ein großer Gewinn: Sie kann helfen, das Vollzugsdefizit beim Löschen personenbezogener Daten abzubauen.

Der Geist im iPhone

Am 20.09.2015 gestand die Firma Apple einen erfolgreichen Angriff auf den Appstore ein. Eine bisher unbekannte Anzahl von Apps (FireEye spricht von über 4000) ist durch Verwendung einer modifizierten XCode-Entwicklungsumgebung mit Schadsoftware infiziert worden. Apple arbeitet an der Bereinigung. Der Vorfall zeigt, dass selbst ein stark reguliertes Anwendungsökosystem anfällig für Angriffe sein kann. Dass modifizierte Compiler ein Sicherheitsproblem sein können, hat Ken Thompson schon 1984 in seinem berühmten Artikel „Reflections on Trusting Trust“ angesprochen. Sollten Software-Entwicklungswerkzeuge zum Einfallstor für Schadsoftware werden, wird dies die Entwicklung sicherer Software vor ganz neue Herausforderungen stellen.

Finger in die Wunde

Die Auftragsdatenverarbeitung (ADV) ist eines der wichtigsten Instrumente des Datenschutzes, wenn es um das Outsourcing der Verarbeitung personenbezogener Daten geht. Braucht man hierfür normalerweise einen Erlaubnistatbestand, ermöglicht es die gesetzliche Fiktion der ADV, diese durch einen Vertrag zu ersetzen. Dadurch wird der Auftragnehmer datenschutzrechtlich zum Teil des Auftrag-

gebers (verantwortliche Stelle), sodass keine – erlaubnispflichtige – Datenübermittlung an einen Dritten vorliegt.

Mit einer Pressemitteilung vom 20.08.2015 und einem Bußgeldbescheid in fünfstelliger Höhe legte das Bayerisches Landesamt für Datenschutzaufsicht (BayLDA) den Finger tief in die Wunde der praktischen Umsetzung: Oft machen es sich Auftraggeber allzu leicht und verwenden ADV-Vertragsmuster aus dem Internet, ohne dass diese auf den konkreten Fall angepasst werden. So sollte man beispielsweise mit einem Aktenvernichtungsunternehmen keine Rückgabe der Datenträger nach Erfüllung des Auftrags vereinbaren.

Insbesondere mangelt es häufig an konkret vereinbarten technischen und organisatorischen (Sicherheits-) Maßnahmen (TOM) – stattdessen werden nur allgemeine Floskeln angeführt oder eine Ankreuz-Liste beigefügt, die meist nur geringe Aussagekraft besitzt. Eine individuelle Vereinbarung und Prüfung der Auftragnehmer ist aber unumgänglich, um als Auftraggeber den gesetzlichen Aufsichts- und Kontrollpflichten zu genügen.

Datenschutzniveau der USA

Wir erinnern uns: Der österreichische Datenschutz-Aktivist Max Schrems hatte gegen die irische Datenschutzaufsichtsbehörde wegen der Speicherung der Daten europäischer Facebook-Nutzer in den USA und die damit einhergehende Überwachung durch US-Behörden vor dem irischen High Court geklagt. Dieser hatte unter Berufung auf die Safe Harbor-Entscheidung der EU-Kommission die Prüfung der Beschwerde abgelehnt. Im daraufhin von Max Schrems eingeleiteten Verfahren gegen den irischen Data Protection Commissioner hat der EuGH nun nach Ansicht des Generalanwalts zu prüfen, ob die Kommissionsentscheidung die nationalen Aufsichtsbehörden an eigenen Maßnahmen und Prüfungen hindert und ob unter Anwendung der Safe-Harbor-Grundsätze von einem angemessenen Datenschutzniveau in den USA ausgegangen werden kann. Angesichts der nicht bestrittenen massiven und nicht zielgerichteten Überwachungspraxis sowie des fehlenden gerichtlichen Rechtsschutzes wird letzteres von Generalanwalt Bot in seinen Schlussanträgen vom 23.09.2015 verneint.

Folgt man dieser Begründung steht jedoch nicht nur das Safe-Harbor-Abkommen auf dem Prüfstand, sondern indirekt auch die Wirksamkeit der Standardvertragsklauseln. Denn die staatliche Überwachungspraxis kann auch durch diese nicht ausgeschlossen werden. Bezogen auf deutsche Unternehmen wäre die Folge, dass Datenübermittlungen in die USA nur noch mit Genehmigung der Aufsichtsbehörden, mit Einwilligung des Betroffenen oder in den Ausnahmefällen aus § 4c Abs. 1 BDSG zulässig blieben. Für die betroffenen Unternehmen würde das zu gravierenden Problemen führen, da ein Großteil der Datenverarbeitungen mit US-Unternehmen faktisch rechtswidrig wären.

Secorvo News

Eine kurze Geschichte der Überwachung

Im Rahmen der Ausstellung GLOBAL CONTROL AND CENSORSHIP. Weltweite Überwachung und Zensur des ZKM | Zentrum für Kunst und Medientechnologie Karlsruhe geben Prof. Dr. Müller-Quade (Karlsruher Institut für Technologie) und Dirk Fox (Secorvo) am **08.10.2015** um **18 Uhr** im Vortragssaal des ZKM | Karlsruhe einen Rück- und Ausblick auf die Geschichte und Entwicklung geheimdienstlicher Überwachung.

Zur Einstimmung bietet das ZKM | Karlsruhe ab 17 Uhr für interessierte Teilnehmer eine Führung durch die Ausstellung an. Da die Zahl der Plätze beschränkt ist, bitten wir um rechtzeitige Anmeldung zur Führung – eine Anmeldung zur Veranstaltung ist nicht erforderlich. Führung und Vortragsveranstaltung finden auf Einladung des ZKM Karlsruhe in Zusammenarbeit mit dem KIT und der KA-IT-Si statt. Sie sind kostenfrei und setzen auch keine Fachkenntnisse voraus. Bringen Sie also gerne interessierte Freunde, Kollegen und Bekannte mit!

Im Anschluss an den Vortrag haben Sie die Möglichkeit, den Abend gemütlich im „mint – bistro.café.bar.catering“ im Foyer des ZKM ausklingen zu lassen.

Softwaresicherheit

Sicherheitsrelevante Schwachstellen in Software lassen sich durch systematisches Vorgehen bei der Softwareentwicklung vermeiden. Mit zwei Seminaren führen wir in die Sichere Softwareentwicklung (CPSSE, **16.–19.11.2015**) und das System Security Engineering (T.E.S.S., **09.–11.11.2015**) ein und bieten Ihnen anschließend die Möglichkeit, sich als *Certified Professional for Secure Software Engineering* (CPSSE) bzw. als *TeleTrusT Engineer for System Security* (T.E.S.S.) zu zertifizieren.

Alle weiteren Seminarangebote und den Seminarkalender für 2016 finden Sie jetzt auf unserer Webseite.

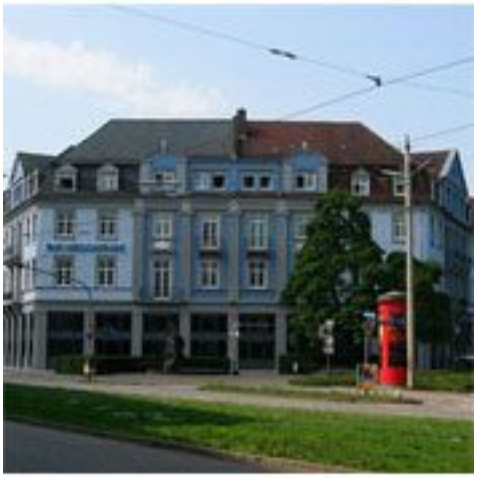
Veranstaltungshinweise

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

Oktober 2015	
06.-08.10.	it-sa 2015 (NürnbergMesse GmbH, Nürnberg)
08.10.	Eine kurze Geschichte der Überwachung (KA-IT-Si, Karlsruhe)
12.-16.10.	Conference on Computer and Communications Security (CCS) (CASED/Fraunhofer SIT, Denver/USA)
13.-15.10.	15. IDACON 2015 (WEKA-Akademie, München)
20.-23.10.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
21.10.	Swiss Cyber Storm 6 (Swiss Cyber Storm Association)
November 2015	
02.-03.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
10.-11.11.	ISSE 2015 (TeleTrusT e.V./eema, Berlin)
10.-13.11.	T.E.S.S. - Sichere Systeme dank System Security Engineering (Secorvo, Karlsruhe)
10.-13.11.	Blackhat Europe 2015 (Blackhat, Amsterdam/NL)
16.-19.11.	CPSSE (Certified Professional for Secure Software Engineering) (Secorvo, Karlsruhe)
23.-27.11.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)

Fundsache

Das BSI hat eine FAQ zum IT-Sicherheitsgesetz veröffentlicht, in der der Geltungsbereich des Gesetzes präzisiert und die Verpflichtungen der betroffenen Unternehmen zusammengefasst werden.



Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Kai Jendrian, Michael Knopp, 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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.

secorvo
security consulting

Secorvo Security News

Oktober 2015

Datenschutzdomino

Elf Jahre lang, von 1998 bis 2009, fand jährlich der Domino-Day statt. Seine Spannung bezog er aus der Ungewissheit, wie viele Steine der erste Stein zum Fallen bringen würde.

Dieselbe Spannung befällt nun Unternehmen und Datenschützer angesichts des Realitäts-checks für Safe Harbor durch den EuGH. Allein bewirkt dieser erste gefallene Stein wenig, stehen doch u. a. mit Standardvertrags-klauseln und Corporate Binding Rules noch andere Wege für die rechtskonforme Übermittlung personen-bezogener Daten an US-Unternehmen bereit.

Doch die nächsten Steine wackeln. Die im Urteil festgestellten Schutzlücken gegenüber staatlicher Datenerhebung können auch Standardvertragsklauseln nicht beheben. Selbst die Einwilligung des Betroffenen wird, mangels Transparenz, als unwirksam angesehen. Solche Defizite sind nicht auf die USA beschränkt – die Urteilsfolgen werden es langfristig auch nicht sein. Andere Bausteine wie die Auf-tragsdatenverarbeitung bspw. im Konzern oder in der Cloud könnten bei konsequenter vergleichbarer Spruchpraxis wanken – hier hat der Auftraggeber häufig weder die Weisungshoheit noch effektive Kontrollmöglichkeiten.

Das Datenschutzrecht hat ein Problem mit der Schutzgewährleistung bei der kooperativen, vor allem internationalen Datenverarbeitung. Instrumente wie Safe Harbor versprachen Rechtssicherheit; die reale Umsetzung des europäischen Datenschutzes war jedoch schon lange und erkennbar reine Fiktion. Da kann auch ein auf die Schnelle verabschiedetes US-Gesetz nicht helfen.

Informationelle Selbstbestimmung durch Isolation der Daten in der EU ist unrealistisch. Laissez faire allerdings auch keine Lösung.

Beim Domino Day entstanden aus den umgefallenen Steinen neue Bilder. Genauso braucht das Datenschutzrecht neue Instrumente, die einen effektiven Schutz personenbezogener Daten nicht untergraben.

Inhalt

secorvo
security consulting

Security News

Chrome will weniger verwirren

Am 13.10.2015 hat Google in einem Blogpost angekündigt, mit Wechsel von der Version 45 auf 46 die Darstellung von HTTPS-Verbindungen in Chrome, die die Überprüfung nicht vollständig bestehen, zu vereinfachen. Das bisherige gelbe Symbol, mit dem auf kleinere Probleme bei einer HTTPS-Verbindung hingewiesen wurde, fällt weg. Dieser Status wird zukünftig mit dem Status „HTTP“ gleichgesetzt. Dadurch reduziert Google die Anzeige auf drei Status.

Das ist aus unserer Sicht ein begrüßenswerter Ansatz, denn bisher konnte die Vermutung aufkommen, dass HTTPS mit kleineren Problemen (gelb) unsicherer sei als reines HTTP (keine Farbe). Für Benutzer ist es schon schwierig genug, HTTPS zu verstehen – daher ist jeder Gewinn an Klarheit bei der Darstellung ein Gewinn für die Sicherheit.

Still und Heimlich

Mit dem eilig verabschiedeten neuen Gesetz zur Vorratsdatenspeicherung – offiziell Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten – ist, kaum wahrgenommen, auch ein neuer Straftatbestand der „Datenhehlerei“ im Strafrecht (§ 202d StGB) eingeführt worden.

Danach soll bestraft werden, wer sich oder Dritten Daten verschafft, verbreitet oder zugänglich macht, die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat. Ausgenommen sind lediglich Handlungen, die ausschließlich der Erfüllung beruflicher Pflichten dienen. Laut Entwurfsbegründung sollen so Lücken im Schutz vor dem Handel mit illegal erlangten Daten geschlossen werden.

Befürchtet wird jedoch, dass der Tatbestand auch Whistleblower oder Blogger erfasst, die Informationen veröffentlichen, ohne deren illegale Beschaffung ausschließen zu können. Die subjektiven Voraussetzungen schränken den Straftatbestand jedoch ein, denn es muss eine Bereicherungs- oder Schädigungsabsicht vorliegen. Journalisten sind nur dann ausgenommen, wenn ihr Status anerkannt wird – das dürfte mindestens zu Verunsicherung führen. Dabei drängt sich tatsächlich der Eindruck auf, dies könnte angesichts zahlreicher Leaks das primäre Ziel der Regelung sein.

DANE ist RFC 7672

Mit der Standardisierung von DANE for SMTP als RFC 7672 hat die Internet Engineering Task Force (IETF) im vergleichsweise kurzen Zeitraum von nur zwei Jahren einen neuen Standard für den sicheren E-Mail-Transport geschaffen. Auch das BSI fordert mittlerweile in seiner technischen Richtlinie Sicherer E-Mail-Transport den Einsatz von DANE.

Im Gegensatz zur Ende-zu-Ende-Verschlüsselung (wie S/MIME oder PGP) zielt DANE darauf ab, einen sicheren Transport zwischen den Mailservern mittels SSL/TLS zu gewährleisten. Hierzu publizieren die E-Mail-Server einen über DNSSEC gesicherten Eintrag mit dem Fingerprint ihres X.509 Zertifikats. Der sendende E-Mail-Server kann diesen Fingerprint zum Schutz vor manipulierten Zertifikaten beim Verbindungsaufbau prüfen.

Der schnellen Verbreitung von DANE steht derzeit noch entgegen, dass alle beteiligten E-Mail-Server für DANE konfiguriert sein müssen und das noch nicht sehr weit verbreitete DNSSEC-Protokoll benötigen.

Audit Fails

Am 07.10.2015 veröffentlichte Guido Vranken gleich acht Schwachstellen, die er bei seiner Analyse des Quellcodes der freien SSL/TLS Bibliothek ARM mbed TLS / PolarSSL gefunden hatte. Damit lässt sich PolarSSL teilweise sogar über das Netzwerk angreifen. Die Ursache sind überwiegend Buffer-Overflows auf Stack und Heap – typische Fehler der 90er Jahre des vergangenen Jahrhunderts. Pikant wird diese Entdeckung vor dem Hintergrund, dass PolarSSL im Auftrag des niederländischen Geheimdienstes AIVD durch die Firma Fox-IT einem Code-Audit unterzogen wurde, bei dem diese Schwachstellen nicht gefunden wurden.

Der Fall weist eine gewisse Ähnlichkeit zu Truecrypt auf: Forscher des Google-Projekts Zero veröffentlichten am 18.09.2015 eine kritische Schwachstelle von Truecrypt (Incorrect Impersonation Token Handling EoP), die bei der Prüfung im Rahmen des Open Crypto Audit Project (siehe SSN 04/2015) offenbar nicht aufgefallen war. Ein Fehler im Truecrypt-Treiber ermöglicht den unberechtigten Zugriff auf Truecrypt-Container anderer Nutzer auf derselben Maschine. Auch wenn die Schwachstelle nur unter bestimmten Voraussetzungen ausgenutzt werden kann, ist ein Umstieg auf Alternativen wie den Truecrypt-Nachfolger Veracrypt (Fehler gefixt) oder Ciphershed zu empfehlen.

Auch ein Code-Audit ist keine Garantie für die Abwesenheit von Schwachstellen. Denn erstens kann aufgrund der Komplexität heutiger Anwendungen meistens nur ein Teil intensiv durchleuchtet werden; das sollte von den Auditoren sauber dokumentiert werden. Und zweitens ist trotz der

Unterstützung durch ausgefeilte Tools am Ende immer der Auditor gefragt. Dabei kann leicht der eine oder andere kleine Fehler übersehen werden – mit fatalen Folgen für die Sicherheit des Produkts.

Threat Modelling Tool 2016

Am 07.10.2015 hat Microsoft eine verbesserte Version des Microsoft Threat Modelling Tool angekündigt. Das Tool hat sich in der Praxis für die Erstellung von Bedrohungsmodellen bewährt, hatte aber bisher einige Schwächen bei der Anpassung der Vorlagen für Modelle. Wir begrüßen es sehr, dass Microsoft sich genau dieser Punkte angenommen hat und mit der neuen Version einen Template-Editor liefert, auf den wir sehr gespannt sind. Bedrohungsmodelle sind ein wichtiger Teil von Sicherheitsanalysen. Nach unserer Erfahrung lohnt es, das (kostenlose) Werkzeug für die Durchführung von Bedrohungsanalysen in Betracht zu ziehen.

Secorvo News

Ritterschlag

Mit der zunehmenden Sensibilität für IT-Sicherheit wachsen Penetrationstester wie Pilze aus dem Boden. Wenn ein Penetrationstest keine relevanten Schwachstellen findet, liegt das daher manchmal nicht nur an der Absicherung.

Mit dem Zertifikat „Offensive Security Certified Professional“ (OSCP) haben die Urheber von Kali-Linux und der Exploit-DB vor knapp fünf Jahren eine Qualifikation für Pentester geschaffen, die es in sich hat: Nach intensiven Live-Hacking-Lektionen über mehrere Monate (von der Informationssammlung über die Nutzung von Exploit-Code bis zur Übernahme von Windows-Domänen) folgt eine praktische Prüfung, in der die Kandidaten innerhalb von 24 Stunden in einer Laborumgebung ein vorgegebenes Hacking-Ziel erreichen und anschließend dokumentieren müssen.

Im Oktober haben **Dr. Safuat Hamdy** und **André Domnick** diese derzeit anerkannteste Pentester-Zertifizierung bestanden – ein Ritterschlag.

T.I.S.P., CPSSE und mehr...

Zwei Gelegenheiten zur Zertifizierung Ihrer Qualifikation bietet Secorvo College noch in diesem Jahr: Ein CPSSE- (**16.–19.11.2015**) und ein T.I.S.P.-Seminar (**23.–27.11.2015**) mit anschließender Zertifikatsprüfung.

Im kommenden Jahr bieten wir wieder zahlreiche interessante und lehrreiche Schulungen an. Neu im Programm ist der D'Day – Datenschutz Deep Impact, der sich an Datenschutzbeauftrage richtet: Ausgewähltes aktuelles Erfahrungswissen, konzentriert an einem Tag. Die erste Gelegenheit für eine Teilnahme bietet sich am **25.02.2016**.

Den Schwerpunkt Sichere Software- und Systementwicklung haben wir ausgebaut. Mit den Seminaren Java Security und Secure Coding C/C++ vertiefen wir die Sicherheitsaspekte von der Projektierung bis zum Coding. Das Seminar spricht nicht nur Entwickler, sondern alle Beteiligte im Lifecycle der Softwareentwicklung an.

Auch die Zertifikatsseminare T.I.S.P., T.E.S.S. und CPSSE bieten wir im kommenden Jahr zu mehreren Gelegenheiten an, ebenso das Seminar IT-Sicherheit heute – praxisnah, zielsicher, kompakt mit den neuesten Entwicklungen in Informationssicherheit und Datenschutz. Am **26.–28.01.2016** können Sie sich auf den neusten Stand bringen lassen.

Globale Überwachung

Beim KA-IT-Si-Event „Eine kurze Geschichte der Überwachung“ am 08.10.2015 füllten knapp 200 Teilnehmer das Medientheater des ZKM | Karlsruhe. Den ersten 80 angemeldeten Teilnehmern konnten wir eine Sonderführung durch die sehr empfehlenswerte Ausstellung "GLOBALE: GLOBAL CONTROL AND CENSORSHIP. Weltweite Überwachung und Zensur" anbieten. Zahlreiche Exponate bieten einen interessanten Einblick in digitale Überwachung und Zensur, wie beispielsweise ein Live-Ticker der aktuell in China gesperrten Websites, eine Visualisierung aller gerade eingeschalteten Smartphones im ZKM (und der von diesen gesuchten WLANs) und eine Wand voller „Überwachungsmonitore“, die Live-Bilder von im Internet frei erreichbaren Webcams zeigen. Die Ausstellung kann noch **bis zum 01.05.2016** besucht werden. (Museums-) Eintritt: 10 €; freitags von 14-18 Uhr ist der Eintritt frei.

Eat, Sleep, Pwn, Repeat

Sicherheitslücken in Protokollen, Systemen und Anwendungen sind die zentrale Ursache erfolgreicher Angriffe auf moderne IT-Systeme. Dennoch gibt es nur wenige Möglichkeiten, tiefergehendes Wissen in diesem Bereich zu erlernen. Capture-The-Flag-Wettbewerbe (CTF) bieten dafür einen spielerischen Rahmen. Dabei treten über den Zeitraum eines Wochenendes mehrere Teams gegeneinander an und lösen anspruchsvolle Aufgaben aus den Bereichen Binary Exploitation, Kryptologie, Reverse Engineering, Web-Sicherheit und Forensik.

Beim nächsten KA-IT-Si-Event am **03.12.2015, 18 Uhr** berichten **Samuel Groß** und **Niklas Baumstark** (KITCTF Team) von ihren Erfahrungen und stellen ausgewählte Beispiele von Aufgaben aus CTFs vor (zur Anmeldung).

Veranstaltungshinweise

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

November 2015	
02.-03.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
10.-13.11.	T.E.S.S. – Sichere Systeme dank System Security Engineering (Secorvo, Karlsruhe)
10.-11.11.	ISSE 2015 (TeleTrust e.V./eema, Berlin)
10.-13.11.	Blackhat Europe 2015 (Blackhat, Amsterdam/NL)
12.-13.11.	Smart Energy 2015 (Fachhochschule Dortmund)
16.-19.11.	CPSSE (Certified Professional for Secure Software Engineering) (Secorvo, Karlsruhe)
17.-20.11.	DeepSec ISDC 2015 (DeepSec GmbH, Wien/AT)
19.-20.11.	39. Datenschutzfachtagung (DAFTA) (GDD, Köln)
23.-27.11.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
24.-25.11.	3. DFN-Konferenz "Datenschutz" (DFN-Cert Services GmbH, Hamburg)
25.-26.11.	Die Zukunft der IT im Digital Business (Management Circle AG, München)
30.11.-01.12.	IsSec/ZertiFA 2015 (COMPUTAS Gisela Geuhs GmbH, Berlin)
Dezember 2015	
03.12.	Eat, Sleep, Pwn, Repeat, (KA-IT-Si, Karlsruhe)

Impressum

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

ISSN 1613-4311

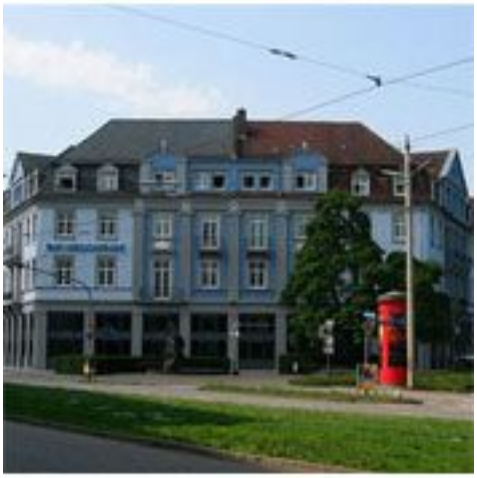
Autoren: Dirk Fox, André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp (Editorial).

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

November 2015

Geschäftsmodell Ohnmacht

Wir wissen: So genannte „Soziale“ Netzwerke und Kommunikationsdienste sammeln zu viele Nutzerdaten, in den meisten Fällen ohne (europäische) Rechtsgrundlage und damit rechtswidrig. Jetzt wissen wir auch, dass alle deutschen Verbraucher es wissen: In einer Ende Oktober veröffentlichten Emnid-Studie im Auftrag des Bundesverbands der Verbraucherzentralen (vzbv) haben dieser Aussage 84% der Befragten beigepflichtet. Und sie machen sich Sorgen – 63% weil sie nicht wissen, wer ihre persönlichen Daten nutzt. Allerdings glauben 75% der Befragten, dass ein „vorsichtiger Umgang mit persönlichen Daten“ wirkungsvoll schützt: Wer sich eingehender mit dem Thema beschäftigt wird wohl eher zu den 22% gehören, die „Aufpassen“ für wirkungslos halten.

Immer mehr Menschen sind jedoch skeptisch, dass Maßnahmen zur Eindämmung der Datensammelei fruchten: So wären 51% (!) aller Befragten bereit, für Datenschutz und Werbefreiheit im Internet zu bezahlen – vor zwei Jahren lag deren Anteil erst bei 35%. Und das nicht zu knapp: 54% dieser Personengruppe ist Datenschutz bis zu 5 € im Monat wert, ein Drittel würde eine noch höhere Gebühr akzeptieren.

Das klingt nach einem viel versprechenden Geschäftsmodell: Daten sammeln, um sich anschließend das selektive Löschen vergolden zu lassen. Das Modell lässt sich verallgemeinern: Wie wäre es mit einem monatlichen Entgelt an Einbrecher, damit sie die Wohnung unangetastet lassen (Art. 13 GG)? Oder einer Gebühr, damit die Polizei öffentliche Versammlungen zulässt (Art. 8 GG)? Denkbar wäre auch, die Gleichheit vor dem Gesetz durch eine monatliche Gerichtsabgabe sicherzustellen (Art. 3 GG).

Warum also nicht gleich eine monatliche Menschenrechts-Abgabe? Klingt verrückt? Jedenfalls nicht für die Verbraucher, wenn es um die freie Entfaltung der Persönlichkeit geht (Art. 2 GG). So weit kann Ohnmacht den Menschen bringen.

Inhalt

secorvo
security consulting

Security News

Bad Barcode

Der am 11.11.2015 von Hyperchem Ma auf der PacSec in Tokyo vorgestellte Angriff mit dem griffigen Namen BadBarcode zeigt, wie verbreitet Designfehler beim Umgang mit Benutzereingaben auch bei etablierten Funktionen sind. Der Angriff nutzt aus, dass viele Barcode-Leser als Tastatur (HID) via USB angebunden sind und auch nicht als ASCII darstellbare Steuerzeichen ungefiltert als Tastaturangaben an das System weiterleiten. Da das Betriebssystem nicht zwischen einer Tastatur und einem solchen HID-Barcode-Scanner unterscheiden kann, kann ein Angreifer via Barcode eine Kommandozeile im Kontext des Benutzers öffnen und beliebige Befehle ausführen. Den Forschern gelang es mittels eines präparierten Amazon Kindle derartige Angriffe auch automatisiert durchzuführen. Aufgrund der weiten Verbreitung von Barcode-Scannern (Kassensystem, Hochregallager etc.) sind die konkreten Auswirkungen dieser Design-Schwachstelle schwer abzusehen - und vor allem schwer zu verhindern.

Zweckbindung der Meldebehörde

Am 01.11.2015 trat das bereits am 03.05.2013 beschlossene Bundesmeldegesetz (BMG) in Kraft, das die Landesmeldegesetze ersetzt. Datenschutzrechtlich relevante Änderungen ergeben sich vor allem für die gewerbliche Nutzung und Auskünfte zum Zweck der Werbung und des Adresshandels (§ 44 BMG). So sind Auskünfte nur noch möglich, wenn der Betroffene generell gegenüber der Meldebehörde oder gegenüber dem Anfragenden eingewilligt hat. Eine Prüfung müssen die Meldebehörden immerhin stichprobenartig durchführen. Gegenüber der bisherigen Widerspruchslösung hat sich damit die Position der Betroffenen aus Datenschutzsicht verbessert. Bemerkenswert ist, dass das BMG auf strenge Zweckbindung setzt: Der Zweck ist bei Auskunftsverlangen zu benennen und nach Zweckerreichung sind die Daten zu löschen. Verletzungen der Zweckbindung werden als Ordnungswidrigkeit mit Geldbußen bis zu 50.000 € sanktioniert.

OWASP ASVS 3.0

OWASP veröffentlichte am 09.10.2015 den Application Security Verification Standard (ASVS) in der Version 3.0. Der ASVS ist eine Sammlung von Anforderungen zur systematischen Prüfung der Sicherheitsmaßnahmen in Webanwendungen. In der Praxis hat sich dieser Standard sowohl als Grundlage für Audits als auch für die Ausgestaltung von Sicherheitsmechanismen in Anwendungen bewährt. In der neuen Version wurden Anforderungen an die Konfiguration und Web-Services ergänzt. Neben weiteren Aufräumarbeiten erhielt der Standard Verweise auf passende Cheat Sheets, die Hilfestellungen bei der Umsetzung bieten. Wir empfehlen den Standard wärmstens allen Prüfern und Entwicklern von Webanwendungen.

Secure Messaging reloaded

Zwar werben Dienste wie iMessage oder WhatsApp mit (teilweiser) Absicherung durch Verschlüsselung – letztlich muss man bei beiden Diensten aber dem Betreiber vertrauen, da es sich nicht um eine Ende-zu-Ende-Verschlüsselung handelt.

Messenger mit echter Ende-zu-Ende-Verschlüsselung sind Threema, Signal und Jabber mit OTR. In einem am 02.11.2015 veröffentlichten Auditbericht hat die Schweizer Security AG die Sicherheitsfunktionen von Threema für gut befunden; Threema dokumentiert seine Sicherheitsmechanismen in einem detaillierten Whitepaper und beschreibt, wie man die Verschlüsselung validieren kann. Am selben Tag hat Open Whisper Systems die Veröffentlichung seiner quelloffenen Lösung für Android verkündet, die schon länger für iOS verfügbar ist. Und schon am 05.11.2014 haben Sicherheitsexperten der Ruhr Universität Bochum das Ergebnis ihrer Untersuchung der Sicherheit von TextSecure publiziert, dem Vorgänger von Signal. Eine Alternative zu Messengern mit Store-and-Forward ist Jabber mit dem Off-the-Record-Protokoll (OTR).

Deserialisierung

Am 06.11.2015 sorgte eine Zero-Day-Schwachstelle in der verbreiteten Java-Bibiothek Commons Collections für Schlagzeilen: Viele Server (z. B. WebLogic, WebSphere, JBoss und Jenkins) sind von ihr betroffen. Die Lücke und das Werkzeug „ysoserial" zu ihrer Ausnutzung wurden bereits Ende Januar 2015 auf der OWASP AppSec Konferenz vorgestellt.

Ursache der Schwachstelle ist die ungesicherte Verwendung der Java-Deserialisierung – ein Problem, das nicht spezifisch für Java ist: Für die Kommunikation mit Java-Anwendungen werden Objekte als Bytefolge abgespeichert und übertragen, die ein Angreifer modifizieren kann – indem er beispielsweise ausführbaren Code hinzufügt. Ein Empfänger (im Fall der Bibliothek Commons Collections ein Server), der die Bytefolge nicht sorgfältig überprüft, generiert bei der Deserialisierung Java-Objekte, bei denen es im schlimmsten Fall zur Ausführung des vom Angreifer eingespielten Programmcodes kommt.

Das Apache Commons Team arbeitet daran, die Deserialisierung mit der verwundbaren Klasse

InvokerTransformer zu unterbinden. Die Hersteller Oracle, Red Hat und Jenkins haben Patches angekündigt bzw. Workarounds bereitgestellt. Bis zur Verfügbarkeit der Patches sollten Administratoren die Klasse *InvokerTransformer* manuell aus allen commons-collections-Jar-Files entfernen.

Einer geht noch …

Spätestens seit dem EuGH-Urteil zu Safe Harbor vom 06.10.2015 sind gesetzlich angeordnete oder erlaubte Weitergaben personenbezogener Daten ohne ausreichende Transparenz und Rechtsschutz in den USA konfliktgeladen. Mit dem Cybersecurity Information Sharing Act of 2015 (CISA) befindet sich nun ein weiteres US-Gesetz in der Endphase des Gesetzgebungsprozesses, das Unternehmen die Weitergabe von personenbezogenen Daten zum Austausch über IT-Security-Bedrohungen gestattet.

Das Gesetz verpflichtet die Sicherheitsbehörden, Berichte und Strategien z. B. für kritische Infrastrukturen oder den Gesundheitssektor zu erstellen und Unternehmen zur Verfügung zu stellen. Die entscheidenden Art. 104, 105 regeln, sehr unbestimmt, die Erlaubnis zum Informationsaustausch zwischen Unternehmen. Die auszutauschenden „Cyber threat indicators" dürfen ausdrücklich auch personenbezogene Daten enthalten. Richtlinien für den Umgang mit diesen Daten sollen erst nach Beschluss des Gesetzes festgelegt werden.

Auch wenn die Ziele legitim sind, Privacy behandelt und sogar eine Art Zweckbindung geregelt wird: Für ein angemessenes Datenschutzniveau fehlen weiter die Transparenz für Betroffene und der Rechtsschutz. Zudem wird auch diese Erlaubnis über vertraglichen Einschränkungen des Datenumgangs mit europäischen Datenexporteuren stehen.

Nmap 7 wird volljährig

Am 19.11.2015 wurde Nmap 7 veröffentlicht – dreieinhalb Jahre nach dem letzten Release und mehr als 18 Jahre seit der ersten Version. Die Verbesserungen betreffen vor allem die Erweiterung der Skript-Bibliothek: Hier wurden u. a. viele Schwachstellen-Scans, Skripte für Webanwendungen und SSL/TLS sowie für eine detaillierte Informationsbeschaffung ergänzt. Außerdem gibt es Verbesserungen bei der IPv6-Unterstützung und bei der Performanz; auch die Datenbank zur System- und Diensterkennung ist kräftig gewachsen.

Mittlerweile ist Nmap 7 auch als Paket für viele Betriebssystem-Distributionen verfügbar, so dass es unmittelbar genutzt werden kann.

Secorvo News

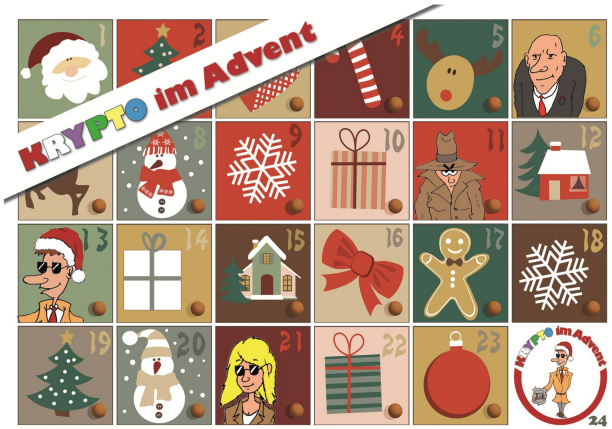
Hacking pur

Auf dem KA-IT-Si-Event „Eat, Sleep, Pwn, Repeat" am **03.12.2015** im Fraunhofer IOSB berichten Samuel Groß und Niklas Baumstark (KITCTF) von ihren Erfahrungen aus Capture-The-Flag-Wettbewerben (CTF). Dabei treten mehrere Teams über ein Wochenende gegeneinander an und müssen anspruchsvolle Aufgaben aus den Bereichen Binary Exploitation, Kryptologie, Reverse Engineering, Web-Sicherheit und Forensik lösen.

Nach dem Vortrag gibt es – wie immer – die Gelegenheit zum „Buffet-Networking". Anmeldung unter www.ka-it-si.de.

Seminare 2016

Gleich zum Jahresanfang bietet Secorvo College zwei spannende Veranstaltungen: Aktuelle Entwicklungen und Fragestellungen in der Informationssicherheit beleuchtet das Dreitagesseminar IT-Sicherheit heute (**26.–28.01.2016**). Die Veranstaltung D'Day – Datenschutz Deep Impact vertieft am **25.02.2016** ausgewählte und aktuelle Themen des Datenschutzes. Das nächste T.I.S.P.-Seminar findet vom **29.02.** bis **04.03.2016** statt. Details und weitere Seminare finden Sie auf unserer Webseite.



24 Tage, 24 Krypto-Rätsel

Um Schülerinnen und Schüler spielerisch an die Kryptologie heranzuführen, startet die KA-IT-Si dieses Jahr gemeinsam mit der Pädagogische Hochschule Karlsruhe das Adventsrätsel „Krypto im Advent". Daran können Schülerinnen und Schüler der Klassen 3 bis 7 teilnehmen; den Siegern winken zahlreiche Sachpreise. Auch ältere Interessierte sind herzlich eingeladen mitzumachen – allerdings außer Konkurrenz.

Veranstaltungshinweise

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

Dezember 2015	
03.12.	Eat, Sleep, Pwn, Repeat (KA-IT-Si, Karlsruhe)
Januar 2016	
15.-17.01.	ShmooCon 2016 (The Shmoo Group, Washington/US)
19.-21.01.	Omnicard 2016 (in TIME berlin, Berlin)
26.-28.01.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
Februar 2016	
09.-10.02.	23. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
17.-18.02.	25. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)>
25.02.	D'Day – Datenschutz Deep Impact (Secorvo, Karlsruhe)
29.02.-04.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
März 2016	
07.-11.03.	Audit Challenge 2016 (Frankfurt School of Finance & Management, Frankfurt)
08.-11.03.	Java Security (Secorvo, Karlsruhe)
14.-15.03.	9. GDD-Fachtagung "Datenschutz International" (Gesellschaft für Datenschutz und Datensicherung e.V., Berlin)

Impressum

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

ISSN 1613-4311

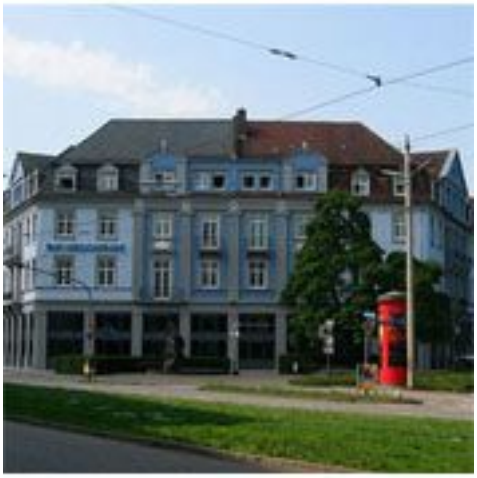
Autoren: Dirk Fox (Editorial), Dr. Yun Ding, André Domnick, Dr. Safuat Hamdy, Kai Jendrian, Michael Knopp.

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.



secorvo
security consulting

Secorvo Security News

Dezember 2015

Würdelos

Sie werden es vernommen haben: „In Zeiten, in denen nahezu alle Bereiche von Wirtschaft und Gesellschaft digitalisiert werden, muss das Konzept der Datensparsamkeit überdacht werden." (Bitkom-Präsident Thorsten Dirks am 20.07.2015). Und: Datenschutz dürfe „nicht die Oberhand über die wirtschaftliche Verarbeitung gewinnen" (Angela Merkel, Bundeskanzlerin, am 02.11.2015). Die „Minimierung [der Verarbeitung personenbezogener Daten] als oberstes Ziel ist das Gegenteil des Geschäftsmodells von Big Data" (Sigmar Gabriel, Stellvertreter der Bundeskanzlerin, am 19.11.2015).

Kaum hat der letzte Politiker verstanden, dass Informationstechnik zum Wirtschaftsfaktor geworden ist und das Silicon Valley die Nase vorn hat (beides seit der Einführung des Apple II im Jahr 1977 absehbar), ertönt der Ruf nach ungehemmter Datenverarbeitung.

Sind „Informationelle Selbstbestimmung" und „Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten" (Volkszählungsurteil des BVerfG, 1983) Konzepte von gestern? Weil amerikanische Internet-Konzerne wie Google, Amazon oder Facebook unsere Persönlichkeitsrechte mit Füßen treten, indem sie (europa-)rechtswidrig Nutzungsdaten unbegrenzt speichern und so ihre Geschäftsmodelle optimieren? Wie frei ist ein Leben, in dem Bewegungsprofile (SmartPhone), Internet-Nutzung (GoogleAnalytics), Kommunikation (WhatsApp, Skype, GMail), Vitaldaten (AppleWatch), TV-Konsum (SmartTV) und Fahrverhalten (iCar) unbegrenzt protokolliert werden?

Was ist das für ein Staat, dessen Repräsentanten ungerügt die Säge an Grundrechte anlegen? Würden wir auch unser Strafrecht ‚modernisieren', wenn Körperverletzung in Mode käme? „Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt." (Grundgesetz Artikel 1, Absatz 1). Lesen bildet.

Inhalt

secorvo
security consulting

Security News

SmartToys mit Schwachstellen

Interaktive, netzfähige SmartToys erfreuen zur Weihnachtszeit nicht nur Kinder, sondern auch Hacker und Datendiebe: Anfang November griffen sie auf die Datenbanken des Lernspielzeug-Anbieters VTech zu. Bei dem am 14.11.2015 entdeckten Einbruch wurden Kontodaten von rund 4,8 Millionen Kunden und Profile von 6,3 Millionen Kindern erbeutet. Sie enthalten Namen, Geschlecht, E-Mail-Adressen, Geburtsdaten, verschlüsselte Passwörter, Sicherheitsabfragen und Antworten zur Kennwortwiederherstellung, IP-Adressen sowie Postanschriften und Download-Chroniken. Auf der Webseite „Have I been pwned?“ des Sicherheitsforschers Troy Hunt können VTech-Kunden prüfen, ob auch ihre Daten den Hackern in die Hände gefallen sind. VTech hat eine ausführliche, regelmäßig aktualisierte FAQ zum Vorfall veröffentlicht. Die betroffenen Webseiten sind derzeit wegen eines gründlichen Security Assessments außer Betrieb.

Auch bei „Hello Barbie“, der interaktiven Barbie-Puppe, die sich in Echtzeit unterhalten kann, wurden – erneut – Schwachstellen in der App und in der Server-Konfiguration gefunden. Die Puppe schickt Tonaufzeichnungen via WLAN zur Beantwortung in die Cloud – und speichert sie dort für zwei Jahre. Dafür erhielt sie im Oktober den Negativ-Preis „Big Brother Awards Austria“.

Mode und Recht

Der Bundesgerichtshof hat mit zwei Urteilen vom 26.11.2015 die Internetsperre wiederbelebt – diesmal zum Schutz von Urheberrechten: Wenn gegen den Störer oder Host-Provider nicht vorgegangen werden kann, soll der Access-Provider auf Grundlage der Störerhaftung zur Sperrung rechtsverletzender Seiten verpflichtet werden können.

Die GEMA hatte gegen die Deutsche Telekom auf Unterlassen der Zugangsvermittlung geklagt, da über Telekom-Zugänge die Urheberrechte verletzenden Seiten „3dl.am“ und „goldesel.to“ erreichbar waren. Das Vorgehen gegen Seitenbetreiber und Host-Provider gelang wegen falscher Adressen nicht. Zwar scheiterte die GEMA vor dem BGH, weil weitere Anstrengungen gegen die Verursacher hätten nachgewiesen werden müssen; den Anspruch bejahte der BGH aber grundsätzlich, da ein adäquat-kausaler Tatbeitrag des Access-Providers bestehe. Umgehungsmöglichkeiten stünden der Verhältnismäßigkeit nicht entgegen.

Die Idee der Internetsperre galt eigentlich seit dem gescheiterten Zugangserschwerungsgesetz von 2010 als tot. Aber offenbar haben Recht und Schlaghosen eines gemeinsam: beide können eine modische Wiederauferstehung erleben. Von der Entscheidung sind alle Unternehmen betroffen, die Internet-Zugänge für die Öffentlichkeit bereitstellen. Dabei verursacht die Prüfung von Sperranforderungen Aufwand – denn irrtümliches Sperren kann als wettbewerbswidrige Handlung gelten.

Freie Zertifikate für alle

Am 03.12.2015 begann die CA Let's Enrypt mit der weitgehend automatischen Bereitstellung kostenloser TLS-DV-Zertifikaten im Testbetrieb. Die Initiative Internet Security Research Group (ISRG) finanziert den Betrieb der CA mit Hilfe von Sponsoren. Jeder Interessierte kann mit Hilfe des auf Github bereitgestellten Clients Zertifikate installieren oder erneuern.

Der Client implementiert den aktuellen Draft des geplanten IETF-Standard ACME. In Praxistest gelang es, Apache manuell zu konfigurieren und Zertifikate automatisiert per Webroot-Challenge zu beantragen oder zu verlängern. Automatische Konfigurationsänderungen von Apache schlugen jedoch fehl.

Die automatische Bereitstellung und Verlängerung freier TLS-DV-Zertifikate ist sehr zu begrüßen; sie wird die Verbreitung verschlüsselter Services befördern. Allerdings weist die aktuelle Implementierung noch Schwächen auf: Im Standalone-Modus muss kurzzeitig der eigentliche Webserver heruntergefahren werden – das ist nicht für alle Anbieter eine Option. Auch werden sich viele Betreiber scheuen, die Client-Software als root laufen zu lassen, was erforderlich ist, um Konfigurationsdateien anzupassen oder einen Service auf Port 80 zu starten. Nicht zuletzt dürfte die Nutzung von HTTP Public Key Pinning zu Problemen in der Praxis führen, da Let's Encrypt zur Zeit noch bei jeder Verlängerung das Schlüsselpaar erneuert.

Für Privatpersonen oder kleine Unternehmen, denen die manuelle Verwaltung von Zertifikaten eine Last ist, bietet Let's Encrypt schon heute eine Erleichterung. Man darf aber nicht zu viel erwarten: Ohne ein solides Verständnis der Funktionsweise von TLS ist es derzeit noch eine Herausforderung, die Software in Betrieb zu nehmen.

TLS-Chaos

Anders als gelegentlich kolportiert herrscht keineswegs ein Mangel an sicheren kryptografischen Verfahren – wohl aber an deren korrektem Einsatz in der Praxis. Dies bestätigen erneut zwei aktuelle Vorfälle.

Am 23.11.2015 hatte auf der Diskussionsplattform reddit ein Benutzer namens „robotercowboy“ berichtet, dass auf seinem XPS-Notebook von Dell die eDellRoot-CA als vertrauenswürdige Stammzertifizierungsstelle im Windows Zertifikatspeicher installiert sei. Der harmlose Hinweis wurde zum Skandal, als bekannt wurde, dass Dell nicht nur sein eigenes Root-CA-Zertifkat, sondern gleich auch den zugehörigen geheimen Schlüssel vorinstalliert hatte. Damit konnte jedermann Zertifikate für beliebige Namen ausstellen, die von Dell-Systemen als vertrauenswürdig akzeptiert wurden. Nicht der erste Fall dieser Art: Lenovo leistete sich Ähnliches erst Anfang 2015.

Andere kompromittieren in voller Absicht: Am 30.11.2015 forderte Kazakhtelecom ihre Kunden unter dem Vorwand der Internetsicherheit und mit Verweis auf die Gesetzgebung dazu auf, ein neues „national security certificate“ auf ihren Geräten zu installieren – das dem kasachischen Staat letztlich das unbemerkte Aufbrechen von TLS-Verbindungen seiner Bürger ermöglicht.

Doch auch bei anderen TLS-Protokollen (POP3S, IMAPS, SMTPS, IRCS) sieht es düster aus. Das zeigt eine am 02.11.2015 publizierte Untersuchung von Forschern der Universitäten Sydney, Berkeley und München, in der der gesamte IPv4-Adressraum analysiert und mehr als 110 Mio. TLS-Verbindungen ausgewertet wurden. Nur bei rund 31 % aller SMTP-Server war eine Verbindung mittels STARTTLS möglich, und von diesen Servern setzten nur rund 30 % ein vertrauenswürdiges X.509-Zertifikat ein. Bei (je nach Dienst) bis zu 30 % der Server war das Zertifikat abgelaufen, und 10-20 % der TLS-Verbindungen waren mit RC4 verschlüsselt.

Secorvo News

Ich bereue immer noch nichts

Wer das Snowden-Theaterstück „Ich bereue nichts“ des Badischen Staatstheaters Karlsruhe noch nicht gesehen hat, kann das am **29.01.2016** und **05.02.2016** nachholen. Der Darsteller Thomas Halle wurde am 30.03.2015 bei der Woche junger Schauspieler in Bensheim für seine schauspielerische Leistung in diesem Stück mit dem Günther-Rühle-Preis ausgezeichnet.

Am **29.01.2016** gestaltet Secorvo ab 19:30 Uhr das Rahmenprogramm: Christoph Schäfer führt in das Stück ein („NSA: Der Skandal im Zeitraffer“), und Kai Jendrian geht im anschließenden Publikumsgespräch auf die Möglichkeiten des Selbstschutzes ein. Beide Experten stehen anschließend für Fragen zur Verfügung. Sichern Sie sich jetzt eine Platzkarte!

Spotlight: D'Day

Das eintägige Seminar D´Day – Datenschutz Deep Impact für Datenschutzbeauftragte am 25.02.2016 wird aktuelle Herausforderungen im Datenschutz diskutieren und bewerten. Nach einer einführenden Betrachtung von Dirk Fox über vermeintliche und tatsächliche Datenschutz-Highlights diskutiert Karin Schuler mit Ihnen Aufbau und Gestaltung einer Datenschutz-Stellungnahme. Michael Knopp und Christoph Schäfer zeigen Fallstricke und Lösungswege beim Cloud-Outsourcing auf. Über die Möglichkeiten der Ausgestaltung eines Security Information and Event Managements (SIEM) berichtet Dr. Safuat Hamdy; Michael Knopp übernimmt die datenschutzrechtliche Einordnung. Abschließend stellt Ihnen Dr. Volker Hammer (Editor der DIN 66398) vor, wie Sie das systematische Löschen personenbezogener Daten in den Griff bekommen.

T.I.S.P. und Java Security

Unsere erste T.I.S.P.-Schulung im neuen Jahr – vom **29.02. bis 04.03.2016** – lädt Sie ein, Ihre Berufserfahrung und Qualifikation im Gebiet Informationssicherheit durch ein T.I.S.P.-Zertifikat bestätigen zu lassen. Zur Vorbereitung erhalten Sie vorab unser T.I.S.P.-Begleitbuch.

Dass viele Bedrohungen durch sicher programmierte Software erst gar nicht entstehen würden, muss an dieser Stelle nicht betont werden. Wie Sie das in Java erreichen, erfahren Sie in unserer „Hands-On“-Schulung Java Security vom **08. bis 11.03.2016**.

Alle Seminarangebote mit detaillierter Beschreibung finden Sie auf unseren Webseiten.

Wer druckt, der bleibt

Drucker und Kopierer sind heute keine dummen Ausgabegeräte mehr, sondern haben sich zu smarten Netzwerkteilnehmern gemausert. Mit ihnen werden tagtäglich personenbezogene und vertrauliche Informationen gedruckt, kopiert, gescannt und gelegentlich auch gefaxt. Damit sind sie ein Angriffsziel für Innen- und Außentäter – nicht nur Geräte mit Festplatte.

Beim nächsten KA-IT-Si-Event am **02.02.2016** um 18 Uhr zeigt Hendrik Herberger (MODOX – Modern Documents GmbH) in den Räumen des CyberForum e.V. die Gefährdungslage auf und gibt konkrete Empfehlungen, wie sich bestehende Risiken minimieren lassen. Anschließend haben Sie wie gewohnt die Gelegenheit zum „Buffet-Networking“. Anmeldung unter www.ka-it-si.de.

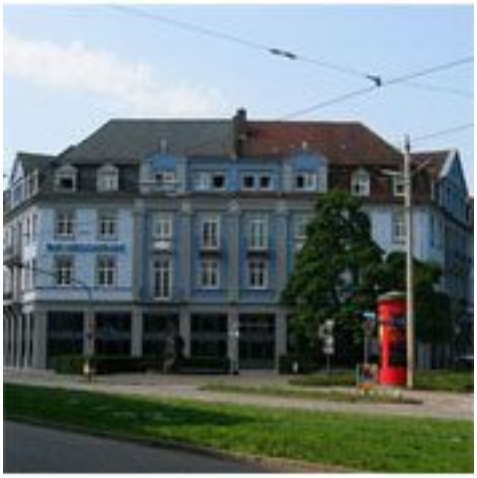
Veranstaltungshinweise

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

Januar 2016	
15.-17.01.	ShmooCon 2016 (The Shmoo Group, Washington/US)
19.-21.01.	OmniSecure 2016 (inTIME, Berlin)
Februar 2016	
09.-10.02.	23. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
17.-18.02.	25. SIT-SmartCard Workshop (SIT, Darmstadt)
25.02.	D'Day – Datenschutz Deep Impact (Secorvo, Karlsruhe)
29.02.-04.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
März 2016	
07.-11.03.	Audit Challenge 2016 (Frankfurt School of Finance & Management, Frankfurt)
08.-11.03.	Java Security (Secorvo, Karlsruhe)
14.-15.03.	9. GDD-Fachtagung "Datenschutz International" (GDD e.V., Berlin)
29.03.-01.04.	2nd DFRWS EU Conference (DFRWS, Dublin/IE)

Fundsache

Mozilla hat Ende November in Hamburg die Bedrohung unserer Privatsphäre durch Internet-Konzerne mit einem Glashaus-Experiment veranschaulicht – dokumentiert in einem Youtube-Video.



Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Yun Ding, André Domnick, Kai Jendrian, Michael Knopp, 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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.