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