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

Geschäftsmodell Ohnmacht

Security News

Bad Barcode

Zweckbindung der Meldebehörde

OWASP ASVS 3.0

Secure Messaging reloaded

Deserialisierung

Einer geht noch ...

Nmap 7 wird volljährig

Secorvo News

Hacking pur

Seminare 2016

24 Tage, 24 Krypto-Rätsel

Veranstaltungshinweise

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