secorvo
security consulting

Secorvo Security News

Juli 2014

Verdeckte Profilbildung

Mit Erfolg haben sich Datenschützer gegen die Speicherung der IP-Adresse (als ein oft auf eine natürliche Person beziehbares Datum) und von Cookies gewehrt, die eine Verknüpfung von zeitlich auseinanderliegenden Nutzungsvorgängen ermöglichen. Der EU waren letztere sogar die wenig technikneutrale „Cookie-Richtlinie“ (RL 2009/136/EG) wert.

Tatsächlich aber handelt es sich dabei um ein Randthema. Denn das Kernproblem ist nicht Identifikation, sondern Profilbildung: Gelingt es einem Webseitenanbieter, Nachrichtendienst oder – schlimmer noch – Werbungs-Vermittler (wie Google oder Facebook), Seitenzugriffe zu einem eindeutigen Profil zu verdichten, so entwickelt sich daraus ein äußerst aussagekräftiger „Schattenriss“ eines, wenn auch zunächst anonymen, Benutzers.

Dieses Internet-Verhaltensprofil wird dabei mehr und mehr zum Abbild unserer Identität. Für den Anbieter kommt es dabei nur auf die Wiedererkennung an – und die gelingt ihm auch ohne Cookies und IP-Adressen, z. B. durch *Canvas Fingerprinting*. Dabei werden mittels versteckter HTML5-Kommandos Unterschiede im Zeichensatz-Rendering identifiziert, die von Grafikkarte, Treiber-Versionen und installierten Zeichensätzen abhängen. Kombiniert mit anderen Browser-Spezifika wie aktiven PlugIns oder Konfigurationseinstellungen ist heute so eine nahezu eindeutige Rechner-Wiedererkennung möglich – unbemerkt vom Nutzer und nur durch ständigen Rechnerwechsel zu verhindern.

Daher springt das jüngst gefeierte „Recht auf Vergessen“ gegenüber Suchmaschinen (SSN 5/2014) zu kurz. Denn was ist das Wissen aus Veröffentlichtem gegenüber einem vollständigen Profil unserer Internet-Nutzung? Wenn technische Mechanismen eine solche Profilbildung gegen den Willen der Betroffenen nicht verhindern, mutiert das Internet – ganz ohne NSA und BND – unweigerlich von einer Informations- zu einer verdeckten Überwachungsinfrastruktur.

Inhalt

secorvo
security consulting

Security News

Google-Projekt Zero

In der Vergangenheit haben Google-Mitarbeiter zahlreiche Sicherheitslücken in Software gefunden, die im Zusammenhang mit Google-Produkten zum Einsatz kommen. Dazu gehören die OpenSSL Heart-Bleed-Schwachstelle und Schwachstellen in der Open-Source HTML-Engine WebKit (siehe SSN 04/2014). Motiviert durch diese Erfolge kündigte Google am 15.07.2014 an, unter dem Projekt-namen Zero ein Team mit Sicherheitsexperten auf-zubauen, das sich in Vollzeit um Internetsicherheit kümmern soll. Ihr Ziel: Zero-Day-Schwachstellen finden, bevor sie von Kriminellen oder staatlichen Behörden genutzt werden, um Rechner zu infizie-ren, sensible Daten zu stehlen oder Kommunikation zu überwachen. Die Bug-Suche ist dabei nicht auf Google-Produkte beschränkt, da deren Sicherheit oft von der Sicherheit fremder Software abhängt.

Google will die gefundenen Lücken ausschließlich an die betroffenen Hersteller melden und mit ihnen gemeinsam an einem Fix arbeiten. Anschließend werden alle Lücken in einer Datenbank veröffent-licht; dazu existiert bereits eine eigene Blogseite. Eine löbliche Initiative, die der Sicherheit von Soft-ware erneut Auftrieb geben könnte.

Telefonwerbung

Telefonwerbung unterliegt spätestens seit der Ein-führung des § 7 Abs. 2 Nr. 2 UWG im Jahr 2004 erheblichen Beschränkungen. Neben dem wettbe-werbsrechtlichen Einwilligungserfordernis ist auch die Verwendung der Telefonnummer zu Werbe-zwecken ein Fallstrick. Das Verwaltungsgericht Berlin hat in einem Urteil vom 07.05.2014 die anzulegenden Maßstäbe klargestellt.

Das Gericht wies die Klage gegen eine Anordnung des Berliner Beauftragten für Datenschutz und Informationsfreiheit ab, nach der die Klägerin die Praxis ihres Call-Centers beenden sollte, im Rahmen von telefonischen Kundenzufriedenheitsbefragun-gen eine Einwilligung in Werbeanrufe zu erbitten. Das Verwaltungsgericht bestätigt, dass dabei eine Verwendung der Telefonnummer für zwei unter-schiedliche Zwecke vorliegt. Während die Frage nach der Kundenzufriedenheit nach § 28 Abs. 1 Nr. 1 BDSG zulässig sei, habe die Frage nach einem Opt-In für Werbeanrufe bereits Werbecharakter. Hierfür sei § 28 Abs. 3 BDSG eine abschließende Spezialregelung. Erforderlich sei eine Einwilligung des Betroffenen vor dem Anruf.

Das sehr klare, wenn auch noch nicht rechtskräftige Urteil stärkt die Bedeutung der sorgsamen Diffe-renzierung von Einzelzwecken in einem Verfahren und stellt klar, dass Datenschutzrecht nicht durch eine Vermengung mit einem im Vordergrund stehenden Zweck umgangen werden darf.

Mit Licht ins WLAN

Das „Internet der Dinge“ hält noch viele Über-raschungen mit Sicherheitsimplikationen bereit. Eine davon hat Alex Chapman am 04.07.2014 in seinem Blog-Post „Hacking into Internet Connected Light Bulbs“ aufgedeckt: Bei der Analyse des Zu-sammenspiels von über das Internet verbundenen Lampen stellte er fest, dass das Wi-Fi-Passwort des Netzwerks, in dem sich die Lampen befinden, bei der Kommunikation zwar mit AES verschlüsselt wird, der verwendete Schlüssel aber in der Firmware der Lampen fest verdrahtet ist. Damit öffnen die Leuchten die Tür zum heimischen WLAN. Wer über Wi-Fi verbundene Geräte nutzt, sollte stutzig werden, wenn es an einer Eingabemöglichkeit für das WLAN-Passwort mangelt…

Europas großer Wurf

Vor gut zwei Jahren, am 04.06.2012, hatte die Europäische Kommission einen Verordnungsent-wurf zu Diensten der elektronischen Identifizierung und Vertrauensdiensten für elektronische Transak-tionen im Binnenmarkt vorgestellt. Nun wurde die Verordnung am 16.07.2014 vom Europäischen Rat angenommen. Sie tritt nach Veröffentlichung im Amtsblatt in Kraft und gilt ab dem 01.07.2016; zu diesem Zeitpunkt hebt sie die Signaturrichtlinie auf.

Die Verordnung regelt als unmittelbar geltendes Recht den Rechtsrahmen für elektronische Signa-turen, Siegel, Zeitstempel, Dokumente, Zustel-lungs- und Zertifizierungsdienste für die Webseiten-authentifizierung. Außerdem legt sie die Voraussetzungen für die Anerkennung von elektro-nischen Identifizierungssystemen fest und enthält Vorschriften für die Anbieter der genannten Dienste. Ohne Berücksichtigung geltender nationaler Regelungen legt die Verordnung Beweisregeln fest.

Dabei verweist fast jeder Artikel der Verordnung auf von der Kommission noch zu erlassende Rechtsakte zu technischen Spezifikationen, Verfahren, Maßnah-men, Meldeinhalten und intereuropäischen Abstim-mungen, ohne dass es hierfür klare Vorgaben gäbe. Für Deutschland wird nun die Anpassung einer Reihe von Gesetzen anstehen: Signaturgesetz, De-Mail-Gesetz, Personalausweisgesetz, Verwaltungs-verfahrensgesetze und viele weitere Regelungen sind von der Verordnung betroffen. Zu den Vertrau-ensdiensten gehören auch die in Deutschland bislang aus systematischen Gründen ausgeschlos-senen Fremdsignaturen, bei denen die Signaturer-

stellungseinheit Dritten überlassen wird. Umgekehrt entfällt die deutsche Sonderform der qualifizierten Signatur mit Anbieterakkreditierung.

Damit stehen dem elektronischen Rechtsverkehr nicht nur in Deutschland erhebliche Veränderungen bevor – ohne erkennbare Vertrauenssteigerung. Wie dabei die unvermeidliche Rechtsunsicherheit und die in einigen Bereichen erheblichen Umstellungskosten zu einer größeren Akzeptanz elektronischer Signatur- oder Identifikationstechniken führen sollen, bleibt das große Geheimnis des Verordnungsgebers. Offenbar wähnt sich dieses Paralleluniversum frei von der Geltung profaner Marktmechanismen.

Einfallstor Virenschutz

Virenschutz-Software soll vor Viren schützen – und schafft dabei neue Angriffsflächen, denn sie besitzt höchste Berechtigungen, die sie für Angreifer besonders interessant macht. Außerdem öffnet sie jede Schadsoftware – besitzt sie Schwachstellen, lassen diese sich daher besonders leicht ausnutzen.

Und tatsächlich ist es mit der Sicherheit von Anti-Viren-Software bei weitem nicht so gut bestellt, wie man erwarten könnte: Am 23.07.2014 veröffentlichte Joxean Koret die Ergebnisse seiner Analyse von 17 AV-Lösungen, die er eine Woche zuvor auf der SyScan360 in Singapur vorgestellt hatte. Seine Erkenntnisse machen sprachlos: die meisten Produkte laden Updates via HTTP, in 14 fand er klassische Schwachstellen wie *Heap Overflows*, *Remote Command Injection* und Fehler in Entpacker-Routinen – Ansätze wie ASVS sind den Herstellern offenbar unbekannt. Angesichts dieser Schwachstellen gehört der zentrale Virenscanner im Netz auf ein isoliertes System.

Passwords are dead – again...

Online-Passwortdienste füllen Passwortfelder aus, arbeiten plattformübergreifend, verwalten Passwörter von Millionen Nutzern – und stellen daher attraktive Angriffsziele dar. Im August werden Forscher der Universität Berkeley auf dem 23. Usenix Security Symposium eine Untersuchung zur Sicherheit von Online-Passwortmanagern vorstellen, die Schwachstellen in der Implementierung aller fünf untersuchten Produkte aufdeckte. So war das automatische Einloggen auf Webseiten via Bookmarklets angreifbar, drei Lösungen hatten XSS- oder CSRF-Schwachstellen, zwei prüften die Autorisierung beim *credential sharing* nicht, zwei waren über die Benutzeroberfläche angreifbar. Seit August 2013 sind die Hersteller informiert; LastPass und RoboForm haben die beanstandeten Schwachstellen nach eigenen Angaben inzwischen beseitigt.

Grundsätzlich sind Passwörter aber auch im Kopf nicht sicher und verursachen Kosten durch Passwort-Rücksetzungen und -Wechsel. Die Alternative sind lokal speichernde Passwortmanager – bei denen man sich allerdings selbst um die Verfügbarkeit kümmern muss.

Secorvo News

Know-How-Update

Der ständigen Weiterentwicklung des Themas IT-Sicherheit versuchen wir mit unserem Seminar „IT-Sicherheit heute“ Rechnung zu tragen: Das Programm unterziehen wir einer ständigen Aktualisierung und Überarbeitung. Besonders zu empfehlen als Auffrischung Ihres Basiswissens – die nächste Möglichkeit zur Teilnahme bieten wir vom **30.09.–02.10.2014** (anrechenbar mit 21 CPEs).

Wie sich sichere Softwareentwicklung in die Entwicklungsprozesse integrieren lässt, vermittelt unser Zertifikatslehrgang Certified Professional for Secure Software Engineering (CPSSE) vom **20.–24.10.2014**. Für Ihre T.I.S.P.-Zertifizierung bieten wir in diesem Jahr noch zwei Termine: vom **22.–26.09.2014** und vom **10.–14.11.2014** jeweils mit anschließender Prüfung – und der aktualisierten und überarbeiteten Neuauflage des T.I.S.P.-Buchs. Alle Termine und Seminarangebote dazu sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

3. Staffel der Anti-Prism-Party

Zwei Auflagen der größten Cryptoparty Europas mit 650 bzw. 900 Teilnehmern gab es bereits. Doch aller guten Dinge sind drei – daher veranstaltet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) anlässlich der Uraufführung des Edward-Snowden-Stücks „Ich bereue nichts“ am Badischen Staatstheater am **Samstag, 11.10.2014** eine dritte Staffel der Anti-Prism-Party. Dort erfahren Sie alles, was Sie schon immer über Verschlüsselung wissen wollten, aber bisher nicht zu fragen wagten.

Auf Bühnen und an Stationen in den Foyers des Staatstheaters zeigen Karlsruher IT-Sicherheits- und Datenschutzexperten in Live-Vorführungen, wie man Tracking verhindert, seine Passwörter wählt und geschützt aufbewahrt, E-Mails vor fremdem Zugriff schützt, Chats verschlüsselt und wie File-Sharing in der Cloud sicher wird. Derweil können sich Ihre Kinder zum Verschlüsselungsexperten ausbilden lassen. Krönender Abschluss ist ein **Anti-Prism-Plenum** im Kleinen Haus.

Aktuelle Informationen zum Programm der Anti-Prism-Party gibt es in einem eigenen Newsletter und auf Twitter.

Veranstaltungshinweise

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

August 2014	
02.-07.08.	Blackhat USA 2014 (Blackhat, Las Vegas/US)
03.-06.08.	14th Annual DFRWS Conference 2014 (DFRWS, Denver/US)
07.-10.08.	DEF CON 22 (DEFCON, Las Vegas/US)
17.-21.08.	Crypto 2014 (IACR, Santa Barbara/US)
20.- 22.08.	23rd USENIX Security Symposium (Usenix, San Diego/US)
25.- 25.08.	Sommerakademie (ULD Schleswig-Holstein, Kiel)
September 2014	
16.-17.09.	D • A • CH Security (GI, OCG, BITKOM, SI, TeleTrusT, Graz/AT)
16.-19.09.	OWASP AppSec USA 2014 (OWASP Foundation, Denver/Colorado)
22.-27.09.	T.I.S.P.-Schulung und Prüfung (Secorvo, Karlsruhe)
30.09.	Anwendertag IT-Forensik (Fraunhofer, Darmstadt)
30.09.-02.10.	IT-Sicherheit heute (Secorvo, Karlsruhe)

Fundsache

Am 30.06.2014 veröffentlichte die KPMG eine Studie zu den Auswirkungen des von der Bundesregierung geplanten IT-Sicherheitsgesetzes. Danach werden im Bereich der kritischen Infrastrukturen knapp 18.500 (Groß-)Unternehmen von den Meldepflichten erfasst, deren Bürokratiekosten sich auf 1,1 Mrd. € summieren werden – ein teures Vergnügen.

Impressum

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

ISSN 1613-4311

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

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