secorvo
security consulting

Secorvo Security News

Juni 2016

Glückliche Sklaven

Während sich der von der Safe-Harbor-Entscheidung des EuGH vom 06.10.2016 aufgewirbelte Staub langsam legt, die ersten Aufsichtsbehörden Bußgeld-Bescheide verschicken und sich die EU beeilt, via Privacy Shield-Abkommen eine neue Rechtsgrundlage für die Übermittlung personenbezogener Daten in die USA zu zimmern, erreicht die heimliche Überwachung neue Dimensionen.

Anfang der 2000er Jahre schossen sich Datenschützer auf die Nutzung von Cookies als Tracking-Instrument ein. Darauf reagierte die EU am 25.11.2009 mit der Verabschiedung einer (wenig universellen) „Cookie-Richtlinie“, die eine Einwilligung der Benutzer fordert. Sie ist bis heute in vielen EU-Staaten nicht umgesetzt; Verstöße werden nicht geahndet. Derweil wichen Google & Co. auf andere, weit ergiebigere Methoden zur Gewinnung von Internet-Nutzungsdaten aus: Mit „kostenlosen“ Service-Angeboten spannten sie Webseitenbetreiber vor ihren Karren. Mit Erfolg: Das Webseiten-Analysetool Google Analytics erreichte einen Marktanteil von über 90%, bevor es in den Fokus von Datenschützern geriet, denen die Datensammelei von Marketingabteilungen ohnehin ein Dorn im Auge war.

Während sich Datenschützer an Google Analytics und Social Media Plugins festbissen, zündeten Google & Co. ein Feuerwerk an Angeboten für Webentwickler, die diese bereitwillig in ihren Code einbetteten. Kaum eine Webseite, die kein Javascript- oder CSS-Framework und keinen Web-Font nachlädt – und dabei die Nutzerdaten bei Facebook, Google oder Twitter abliefert. Schließlich erfand Google die Safe Browsing-API, die jeden Seitenaufruf anhand einer Google-Blacklist auf enthaltene Schadsoftware prüft. Inzwischen Teil von Firefox, Safari und Chrome meldet die API jeden Webseitenaufruf von einer Milliarde Nutzern an Google. Microsoft wollte da nicht zurückstehen führte im IE8 den SmartScreen-Filter ein. Ein genialer Coup. Denn die erbittertsten Feinde der Freiheit sind bekanntlich die glücklichen Sklaven.

Inhalt

secorvo
security consulting

Security News

Heimlich, still und leise

Google Analytics und Social-Media-Plugins sind immer wieder für eine Aufregung gut – wie zuletzt anlässlich der Bußgeldbescheide der Datenschutz-Aufsichtsbehörde Hamburg vom 06.06.2016. Technisch sind beide inzwischen Nebenkriegsschauplätze der großflächigen Erhebung von Metadaten. Die erfolgt mittlerweile – heimlich, still und leise – durch Web-Entwickler-Tools, die sich bisher weitgehend der Wahrnehmung von Datenschützern und Aufsichtsbehörden entziehen:

Bootstrap: Das von Twitter angebotene CSS-Framework erfreut sich großer Beliebtheit bei Webseitenbetreibern. Wird es jedoch nicht auf dem eigenen Server installiert, bekommt Twitter beim Online-Download die Nutzerdaten (IP-Adresse, besuchte Webseite und Zugriffszeitpunkt) frei Haus.

jQuery/Ajax: Eine Webseite zu finden, die ohne den Einsatz der freien JavaScript-Bibliothek auskommt, gleicht schon fast einem Wunder. Werden dabei die jQuery-Bibliotheken von Google nachgeladen, erhält Google die Nutzerdaten.

AngularJS: Genauso verhält es sich mit Googles JavaScript-Webframework. Eine lokale Installation ist aus Datenschutzgründen anzuraten, doch welcher Webdesigner macht das schon?

React: Facebook bietet mit React eine Alternative zu Angular – ein Webframework, das beim Nachladen die Nutzerdaten an Facebook übermittelt.

Web-Fonts: Annähernd jede moderne Webseite nutzt Web-Fonts von Google oder Adobe. In der Regel werden die Fonts dabei erst beim Seitenbesuch nachgeladen. Dabei wäre eine lokale Installation der Fonts problemlos möglich.

Kartendienste: Beliebt ist es auch, auf der Kontakt-Seite die Kartendienste von Google oder Bing Maps einzubinden. Auch hier liefert man dem Anbieter die Nutzungsdaten seiner Seitenbesucher. Mangels einer ähnlichen Lösung wie für die Social-Media-Plugins würde hingegen ein Link zum Kartendienst genügen – sofern man nicht gleich auf die freie Alternative OpenStreetMap setzen möchte.

No CAPTCHA reCAPTCHA: In den SSN 12/2014 berichteten wir über die Google-Version des Turing-Tests, bei der die IP-Adresse übermittelt und Mausbewegungen ausgewertet werden. Zumindest die DENIC setzt nach harscher Kritik im Netz inzwischen wieder auf eine alternative Lösung.

Viele Webseiten-Entwickler erliegen heute den Verlockungen kostenfreier Frameworks, Schriften etc. Die Übermittlung der Nutzungsdaten der Webseitenbesucher in die USA ist nach der Entscheidung des EuGH (SSN 10/2015) jedoch ohne einen Vertrag nach EU-Standardvertragsklauseln oder eine wirksame Einwilligung der Betroffenen rechtswidrig. Zumindest eine lokale Installation der Dienste ist daher geboten – auch wenn man sich anschließend selbst um das Patching kümmern muss.

Versteckter Tracing Code

Dank eines Beitrags im Diskussionsforum reddit wurde am 10.05.2016 bekannt, dass der C++-Compiler von Visual Studio 2015 ungefragt *Tracing Code* in kompilierte Anwendungen einbaut. Dabei handelt es sich um Telemetriedaten wie bestimmte Events und Zeitstempel, die an die Systemkomponente ETW (*Event Tracing for Windows*) weitergeleitet werden. Daraufhin sah sich Microsoft zu einer Stellungnahme gezwungen, in der angekündigt wurde, diese Funktion mit dem nächsten Update zu entfernen.

Auch wenn diese Daten nur lokal auf dem System gespeichert werden und nicht unmittelbar abfließen, ist es schon bedenklich, dass derartige Funktionen im Verborgenen injiziert werden. Schließlich ist es nahezu unmöglich nachzuvollziehen, ob das kompilierte Programm tatsächlich nur die gewünschte Funktionalität enthält. Beim Vertrauen in die eigesetzten Werkzeuge ist besondere Vorsicht geboten, wie schon Ken Thompson in seinem 1984 erschienenen Paper „Reflections on Trusting Trust“ aufzeigte.

Smart Spy

Groß war die Aufregung, als heise am 25.01.2014 SmartTVs als potentielle Spione im Wohnzimmer entlarvte. Über den Datendienst HbbTV können TV-Sender den Fernseher anweisen, eine bestimmte URL abzurufen – und zwar genau dann, wenn man den Sender einschaltet: Der Zählpixel der TV-Welt, mit dem sich das Fernsehverhalten der Nutzer protokollieren lässt. Eine senderübergreifende Auswertungsmöglichkeit mit Google Analytics versteht sich von selbst – Cookies finden nicht nur im PC, sondern auch im Fernseher Verwendung.

Neben den TV-Sendern lassen sich inzwischen auch die Hersteller smarter Fernsehgeräte mit Daten über den Nutzer beglücken. In einem Musterklageverfahren gegen die deutsche Samsung-Tochter konnte nun die Verbraucherzentrale Nordrhein-Westfalen am 10.06.2016 einen kleinen Sieg beim Landgericht Frankfurt am Main erringen (Az. 2-03 O 364/15): Auch wenn man die AGB und die über 56 Bildschirmseiten lange Datenschutzerklärung gele-

sen und abgelehnt hat, übermittelt ein Samsung-SmartTV die IP-Adresse des Nutzers an Samsung.

Das LG akzeptierte die Datenschutzbestimmungen wegen ihrer Länge und Unübersichtlichkeit nicht als wirksame Einwilligung. Da die Datenübermittlung jedoch nicht an die beklagte deutsche Samsung-Tochter, sondern an die Muttergesellschaft erfolgt, muss Samsung Deutschland nur seine AGB nachbessern. „Ob die Datenübermittlung in der konkreten Art und Weise rechtmäßig war, hatte die Kammer (...) nicht zu entscheiden" – schließlich gilt das BDSG nicht für Südkorea.

Unsichere Updates

Automatische Updates von Software beugen der Ausnutzung von Schwachstellen in veralteten und verwundbaren Programm-Versionen vor und stellen damit eine immer wieder empfohlene Schutzmaßnahme dar. Allerdings setzen viele Software-Hersteller ihre Nutzer durch automatische Update-Mechanismen unnötigen Gefahren aus, wenn der sensitive Update-Prozess über unverschlüsselte HTTP-Verbindungen erfolgt. So geschehen z. B. bei Intels Driver Update Utility (19.01.2016), ebenso bei Dell (23.11.2015) und bei Lenovo (31.05.2015). Sogar Sicherheitssoftware wie Keepass 2 (02.03.2016) ist verwundbar.

Erfolgt der Download nicht über TLS, können Angreifer mit einem Man-in-the-Middle-Angriff die übermittelten Updates *on the fly* mit Schadsoftware „anreichern". Die dafür benötigten Werkzeuge sind frei im Web verfügbar. Für die Nutzer ist die Manipulation eines Updates praktisch nicht zu erkennen. Wirksam schützen kann man sich davor nur, indem man unverschlüsselte Updates ausschließlich im eigenen, vertrauenswürdigen Netz zulässt.

Seitenkanäle im PC

Angriffe über so genannte Seitenkanäle, also nicht intendierte Informationswege wie das physische Verhalten eines Systems (Zeit, Stromverbrauch oder Arbeitsgeräusche), sind nichts grundsätzlich Neues. So wurden in der Vergangenheit Funker an der „Handschrift" ihrer Morsezeichen identifiziert oder Inhalte von Röhrenmonitoren über deren elektromagnetische Abstrahlung rekonstruiert.

Neu ist, dass über die Auswertung des Stromverbrauchs, des elektromagnetischen Felds oder der Geräuschentwicklung nicht nur geheime Schlüssel einer SmartCard (Paul Kocher, 1996), sondern auch aus einem modernen PC gewonnen werden können. Das belegen Daniel Genkin, Lev Pachmanov, Itamar Pipman, Adi Shamir und Eran Tromer in ihrem am 04.06.2016 in der Juni-Ausgabe der Communications of the ACM erschienenen Beitrag am Beispiel von Angriffen auf GnuPG – zwar unter optimierten Bedingungen, aber mit preiswertem Equipment aus gut 10 m Entfernung.

Will man Krypto-Software wirksam vor solchen Seitenkanalangriffen schützen, führt kein Weg an den bei Krypto-Hardware bereits üblichen Schutzmechanismen wie „Blinding" vorbei. Eine neue Herausforderung für Softwareentwickler.

Secorvo News

IT-Sicherheit heute

Für das Herbstseminar „IT-Sicherheit heute" sind noch letzte Plätze frei. Vom **27. bis 29.09.2016** bringen wir Sie auf den aktuellen Stand in den Bereichen Informationssicherheit, IT-Sicherheit und Datenschutz.

Neben Themen wie dem IT-Sicherheitsgesetz und der EU-Datenschutz-Grundverordnung stehen aktuelle Bedrohungen im Fokus: Gleich zu Seminarbeginn schlüpfen Sie in die Rolle von Angreifer und Verteidiger. Am dritten Seminartag (Hacking Day) zeigen Ihnen unsere Experten in Live-Hacks Angriffe mit Ransomware und PowerShell. Auch klassische Angriffsmethoden wie Spoofing und Man-in-the-Middle werden vorgestellt und es wird auf die Sicherheitslücken von Web-Anwendungen eingegangen. Zum Abschluss des Seminares dürfen Sie selbst Hand anlegen: Im WebGoat-Workshop nähern Sie sich Schritt für Schritt der Web-Security.

Wichtig für alle T.I.S.P.-Absolventen: Das Seminar wird als Weiterbildung für die Re-Zertifizierung anerkannt. Wir freuen uns auf Ihre Anmeldung.

Who is who?

Bei der Anmeldung an Ihrem Arbeitsplatzrechner müssen Sie sich authentisieren, d. h. Ihre Identität gegenüber dem System nachweisen. Das erfolgt heute in den meisten Fällen über die Eingabe Ihres Passworts.

Doch sind Passwörter noch zeitgemäß? Immer mehr Unternehmen setzen auf eine Zwei-Faktor-Authentifizierung (2FA). Bei unserer kommenden KA-IT-Si-Veranstaltung am **14.07.2016**, diesmal in den Räumen der Nexus Technology GmbH in Ettlingen, stellen Petra Barzin (Secorvo), Sandra Bialinski und Michael Leuchtner (Nexus) vor, welche 2FA-Alternativen es gibt und welche Stärken und Schwächen diese Lösungen besitzen.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking". Weitere Infos und die Möglichkeit zur Anmeldung auf www.ka-it-si.de.

Veranstaltungshinweise

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

Juli 2016	
14.07.	Who is who? (KA-IT-Si, Karlsruhe)
30.07.-04.08.	Blackhat USA 2016 (Blackhat, Las Vegas/US)
August 2016	
04.-07.08.	DEF CON 24 (DEFCON, Las Vegas/US)
07.-10.08.	16th Annual DFRWS Conference 2016 (DFRWS, Philadelphia/US)
10.-12.08.	25th USENIX Security Symposium (Usenix, Austin/US)
14.-18.08.	Crypto 2016 (IACR, Santa Barbara/US)
September 2016	
07.-08.09.	Annual Privacy Forum 2016 (ENISA, EC DG Connect, Goethe Universität, Frankfurt)
13.-15.09.	Future Security 2016 (Fraunhofer VVS, Berlin))
19.09.	Sommerakademie (ULD Schleswig-Holstein, Kiel)
26.-27.09.	D • A • CH Security (Gemeinsame Arbeitskonferenz von GI, OCG, BITKOM, SI, TeleTrusT, Klagenfurt)
27.-29.09.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)

Fundsache

Wer angesichts der zahlreichen Passwort-Leaks auf einen Passwort-Manager umsteigen will, dem sei dieser am 22.06.2016 veröffentlichte ausführliche Vergleich der wichtigsten Lösungen empfohlen.

Impressum

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

ISSN 1613-4311

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