secorvo
security consulting

Secorvo Security News

Mai 2022

Behind the Scenes

Die meisten Internet-Nutzer werden wissen, dass Webseiten, die sie besuchen, ihre Seitenaufrufe tracken – nicht selten ohne rechtswirksame Einwilligung. Weniger Internet-Nutzer werden wissen, dass die auf der Seite angezeigte Werbung meist von Dritten eingespielt wird. Doch die wenigsten Internet-Nutzer wissen, dass und wie die Werbung auf sie persönlich zugeschnitten wird.

Tatsächlich versteigern die meisten Portalseiten die Werbeplätze erst beim Aufruf der Seite über „Real Time Bidding“ (RTB) innerhalb weniger Millisekunden. Dazu schickt ein Werbeplatz-Anbieter (oder dessen Broker) über das OpenRTB-Protokoll einen „Ad Request“ an einen RTB-Exchange-Server, der daraus einen „Bid Request“ erzeugt und per Broadcast an alle Werbetreibenden verteilt. Dieses Datenpaket enthält alle bekannten Angaben über das die Seite aufrufende Gerät (u. a. Hersteller und Modell, Betriebssystem, IP-Adresse, Hash der MAC-Adresse und aktuelle GPS-Koordinaten) und den Nutzer (User ID, Geschlecht, Geburtsjahr, Keyword-Liste der Interessen und GPS-Daten des „Heimatstandorts“).

Nach einer am 14.05.2022 veröffentlichten Studie des Irish Council for Civil Liberties (ICCL) werden allein von Google Bid Requests an über 4.500 Unternehmen in den USA und über 1.000 in Europa geschickt – bei jedem deutschen Surfer im Schnitt im Minutentakt. Jeder Empfänger kann darüber benutzerbezogene Surf- und (bei mobilen Devices) Bewegungsprofile erstellen – eine Quelle, die in den USA auch bereits Sicherheitsbehörden nutzen.

Jeder Entwickler weiß, dass Real-Time-Bidding auch ohne die Verteilung der Anfragen funktioniert – ein Schelm, wer Arges dabei denkt. Vielleicht sollten wir uns ab und zu Immanuel Kants 1785 in der „Grundlegung der Metaphysik der Sitten“ formulierten praktischen Imperativ in Erinnerung rufen: „Handle so, dass du die Menschheit, sowohl in deiner Person, als in der Person eines jeden andern, jederzeit zugleich als Zweck, niemals bloß als Mittel brauchest.“

Inhalt

secorvo
security consulting

Security News

GPS-Tracking

In einem erst jetzt veröffentlichten Urteil vom 17.01.2022 hat das VG Wiesbaden Kriterien für den Einsatz von GPS-Tracking im Logistikbereich aufgestellt. Das klagende Unternehmen hatte Geo-Tracking in den Fahrzeugen verbaut, wodurch der Live-Standort der Fahrzeuge und der Benzinverbrauch feststellbar waren. Die Daten wurden mittels Fahrerkarte einzelnen Fahrern zugewiesen und 400 Tage in der Cloud gespeichert.

Begründet wurde das Tracking mit Effizienzsteigerung sowie Schutz vor Missbrauch und Diebstahl. Einwilligungen der betroffenen Arbeitnehmer lagen nicht vor, auch waren keine Maßnahmen ergriffen worden, um eine verdeckte Arbeitnehmerüberwachung zu verhindern. Das Gericht bestätigte die Einschätzung der zuständigen Aufsichtsbehörde: Eine Einwilligung der Arbeitnehmer sei als Rechtsgrundlage nicht ausreichend, da diese in der Regel von Arbeitnehmern nicht wirksam erteilt werden kann. In Betracht käme nur die Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO) nach sorgfältiger Interessensabwägung. Ohne Prüfung, ob es keine weniger einschneidenden Mittel zur Zweckerfüllung gibt, sei das Tracking rechtswidrig.

25-jähriger Bug in cmd.exe

Na, wenn das kein Geburtstagsgeschenk ist: Auf full disclosure wurde am 10.05.2022 eine Denial-of-Service-Schwachstelle im 25 Jahre alten, noch aus Windows-NT-Zeiten stammenden Kommandozeilen-Interpreter cmd.exe gemeldet. Auch wenn die Auswirkung sich auf das „Abschießen" einer eigenen Instanz des Interpreters beschränkt und eine gezielte Ausnutzung oder Angriffe gegen andere Benutzer darüber nicht möglich sind, bleibt die Frage, wie ein so offensichtlicher Fehler so lange unbemerkt bleiben konnte.

Merke: Software reift nicht über die Jahre bei ruhiger Lagerung (wie Whisky oder guter Wein), sondern sollte (wie Champagner) regelmäßig gerüttelt (sprich: untersucht) werden. Auch jahrelang bewährte Software ist nicht automatisch fehlerfrei. Der Fall zeigt, wie wichtig Aktivitäten zur systematischen Untersuchung von Software sind, wie z. B. die der Open Source Security Foundation, sowie die regelmäßige Durchführung von Penetrationstests. Im konkreten Fall besteht kein weiterer Handlungsbedarf – die eigene Kommando-Zeile kann man auch ohne Crash schließen.

Videokonferenzen ohne AV-Vertrag

In der DuD 05/2022 diskutieren Friederike Schellhas-Mende, Nils Wiedemann und Nicolas Blum die Auswirkungen des am 01.12.2021 in Kraft getretenen TTDSG und des neuen TKG auf Videokonferenzsysteme. So wechselt nicht nur die datenschutzrechtliche Zuständigkeit zum BDfI, sondern führt die Einordnung als „nummernunabhängiger interpersoneller Telekommunikationsdienst" dazu, dass für Videokonferenzdienste i.d.R. kein Auftragsverarbeitungsvertrag zu schließen ist.

Datenschutz-Bußgeldbemessung

Am 12.05.2022 hat der Europäische Datenschutzausschuss (EDSA) Leitlinien für die einheitliche Sanktionierung von Bußgeldern bei Datenschutzverstößen veröffentlicht und damit die Leitlinien vom 03.10.2017 (WP 253) präzisiert. Die Datenschutzkonferenz der deutschen Aufsichtsbehörden (DSK) hatte bereits am 14.10.2019 ein abgestimmtes Verfahren veröffentlicht (SSN 10/2019), das nun mit der Veröffentlichung der EDSA-Leitlinien seine Gültigkeit verliert.

Das Konzept des EDSA unterscheidet sich wesentlich von dem der DSK. Zwar betont es ebenfalls, dass Bußgelder auf die spezifischen Bedingungen des Einzelfalls zugeschnitten sein müssen. Doch es bleibt deutlich abstrakter als das deutsche Konzept, das aus dem Jahresumsatz des Unternehmens einen „Grundwert" (Umsatz pro Tag) ermittelte und diesen abhängig von dem Schweregrad des Verstoßes mit einem Faktor belegte.

Ausgangspunkt des EDSA-Konzepts ist eine Bewertung der Art, Dauer und Schwere des Verstoßes, in die u. a. die Zahl der Betroffenen, der Zweck der Verarbeitung und die Größe des verursachten Schadens einfließen. Daraus wird ein „Startwert" als prozentualer Anteil des maximal möglichen Bußgelds abgeleitet. Aus dem Jahresumsatz des Unternehmens errechnet sich dann das minimal aufzuerlegende Bußgeld zu 0,2% (Kleinst-) bis 50% (Großunternehmen) des zuvor bestimmten Startwerts. Je nach Ernsthaftigkeit des Verstoßes und den Bedingungen des Einzelfalls, wie z. B. ergriffene Gegenmaßnahmen oder frühere Verstöße, wird von der zuständigen Aufsichtsbehörde dann das Bußgeld zwischen Minimal- und Startwert festgelegt.

Ob dieses Verfahren geeignet ist, die Höhe der verhängten Bußgelder europaweit zu vereinheitlichen und deren Bestimmung transparenter zu machen, darf bezweifelt werden: Als „Bußgeldrechner" eignet es sich noch weniger als das Konzept der DSA. Die Angemessenheit der europäischen Bußgelder wird also weiterhin vom Augenmaß der zuständigen Behörden (und ggf. der Gerichte) abhängen.

Klagerecht für Verbraucherschutzverbände

Am 28.04.2022 hat der EuGH Verbraucherschutzverbänden ein ähnliches Klagerecht eingeräumt wie schon bei Wettbewerbsfragen. Die Verbände dürfen demnach in Form von Verbandsklagen Unterlassungsklagen gegen Verletzungen des Schutzes personenbezogener Daten erheben. Damit erhalten auch diejenigen Verbraucherinnen und Verbraucher eine Stimme, die aus mangelnder Kenntnis ihrer Rechte nicht gegen Datenschutzverstöße vorgehen.

Cookie-Walls

Die französische CNIL hat am 16.05.2022 erste Empfehlungen für Cookie-Walls veröffentlicht. Cookie-Walls stellen Nutzer beim Aufruf einer Webseite vor die Wahl, entweder alle Cookies für Werbezwecke zu akzeptieren oder eine Gebühr für die werbefreie Nutzung zu zahlen. Zwar sei die Einwilligung freiwillig, jedoch müsse den Nutzern eine „echte und faire Alternative" angeboten werden, die sich an der Angemessenheit der Vergütung bemisst. Die CNIL gibt dafür keinen Schwellenwert an, sondern verlangt, dass diese begründbar ist und ermutigt zu einer transparenten Kostenfestsetzung.

Stimmt der Nutzer der kostenpflichtigen Alternative zu, dürfen nur für den Betrieb der Webseite erforderliche Cookies hinterlegt werden. Der Anbieter kann davon abweichen, wenn z. B. auf Webseiteninhalte von Dritten zugegriffen werden muss. Dafür wird wiederum eine Einwilligung benötigt. Umstritten ist, ob die CNIL als Datenschutzbehörde nicht ihre Kompetenzen überschreitet, indem sie sich zur Vergütung äußert. In ihren Leitlinien hatte die CNIL bereits 2019 Cookie-Walls als unzulässig bezeichnet, woraufhin ihr das oberste französische Verwaltungsgericht diesbezüglich die Zuständigkeit absprach. Die Datenschutzkonferenz (DSK) verweist in ihrer Orientierungshilfe für Anbieter von Telemedien vom 20.12.2021 hinsichtlich Cookie-Walls auf die Leitlinien zur Einwilligung der EDPB. Danach sind Cookie-Walls nur dann unzulässig, wenn sie keine echte Wahlmöglichkeit anbieten („is not presented with a genuine choice").

ISO 27002 – neu und sortiert

Im Februar 2022 wurde die dritte Überarbeitung der ISO 27002 veröffentlicht; eine neue Version der ISO 27001 ist wohl in Kürze zu erwarten. Die ISO 27001 legt die prüfbaren Anforderungen eines Informationssicherheitsmanagementsystems (ISMS) fest und listet im Annex A die Maßnahmen der ISO 27002 auf. Daher sollte die Anpassung des unternehmenseigenen ISMS an die überarbeiteten und neuen Maßnahmen frühzeitig eingeplant werden.

Neu sind elf der nunmehr 93 Maßnahmen; weitere wurden zusammengefasst oder um neue Inhalte wie Bezüge zum Datenschutz angereichert. Eine Hilfe ist die Einführung von Eigenschaften zu jeder Maßnahme. Darüber können Unternehmen die Maßnahmen nach fünf unterschiedlichen Kriterien sortieren: Art der Risikosteuerung, Informationssicherheitsziele, Cybersecurity-Methoden, Managementziele (wie in der ISO 27002:2013) oder Handlungsfelder nach der NIS-Richtlinie. Eine Übersicht der Änderungen und einen Vorschlag für den schrittweisen Umstieg von Version 2013 hat Milan Burgdorf in der DuD 05/2022 zusammengestellt.

Digital Services Act

Am 23.04.2022 haben sich Europäischer Rat und Parlament über den Digital Services Act (DSA) als Nachfolger der 20 Jahre alten E-Commerce-Richtlinie geeinigt. Dieser wird neben der DSGVO weitere Vorgaben für Online-Dienste wie Vermittlungsdienste, Hosting-Dienste und Online-Plattformen enthalten. So werden beispielsweise „Dark Patterns" und irreführende Benutzeroberflächen bei der Auswahl der Cookies verboten. Sensible Daten wie politische Ansichten, religiöse Überzeugungen und sexuelle Vorlieben dürfen in Zukunft nicht mehr für personalisierte Werbung verwendet werden. Auch dürfen über Minderjährige keine Daten mehr gesammelt und diesen auch keine personalisierte Werbung mehr angezeigt werden. Zudem schafft der DSA u. a. für Nutzer eine einfache Meldemöglichkeit, infolge derer die Online-Dienste illegale Inhalte wie Hassrede, Gewaltaufrufe oder Terrorpropaganda entfernen müssen.

Bußgelder bei Verstößen gegen den DSA fallen mit bis zu 6 % des weltweit erzielten Jahresumsatzes noch höher aus als bei der DSGVO. Betreiber von Online-Diensten müssen sich bald auf die Vorgaben des DSA einstellen, da die Verordnung nach einer nur dreimonatigen Übergangsfrist unmittelbar in allen EU-Staaten gelten wird.

Secorvo News

13. Tag der IT-Sicherheit

Wir freuen uns sehr, den 13. Karlsruher Tag der IT-Sicherheit am **14.07.2022** wieder als Präsenzveranstaltung durchführen zu können. Die Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, dem Kompetenzzentrum für angewandte Sicherheitstechnologie am KIT (KASTEL) und dem CyberForum e.V. hat die Förderung des Erfahrungsaustauschs unter IT-Sicherheitsverantwortlichen (nicht nur) in der TechnologieRegion Karlsruhe zum Ziel. Das Programm und die Möglichkeit zur Anmeldung finden Sie unter www.tag-der-it-sicherheit.de.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juni 2022	
06.-10.06.	7th IEEE European Symposium on Security and Privacy (IEEE, Genua/IT)
06.-08.06.	OWASP Global AppSec (OWASP Foundation, virtuell)
16.-17.06.	AREA41 Security Conference (DEFCON, Zürich/CH)
20.-21.06.	DuD 2022 (COMPUTAS, Berlin)
21.-23.06.	Omnisecure 2022 (in TIME, Berlin)
23.-24.06.	Annual Privacy Forum 2022 (ENISA, DG Connect Católica University of Portugal, Warschau/POL)
Juli 2022	
11.-15.07.	PETS 2022 (University of Minnesota, hybrid)
14.07.	13. Tag der IT-Sicherheit (KA-IT-Si, IHK, Cyberforum, KASTEL, Karlsruhe)
August 2022	
06.-11.08.	Blackhat USA 2022 (Blackhat, Las Vegas/US)
10.-12.08.	31st USENIX Security Symposium (usenix, Boston/US)
11.-14.08.	DEF CON 30 (DEFCON, Las Vegas/US)

Fundsache

Neben dem Bericht des BSI zur Lage der IT-Sicherheit sollte man auch einen Blick in das Bundeslagebild Cybercrime 2021 des BKA werfen: Sehr kompakt und übersichtlich wird darin über typische Angriffsziele und -methoden von Cyberkriminellen berichtet. Die erfassten Fälle nehmen zwar stetig zu, die aufgeklärten Fälle jedoch ebenfalls.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Milan Burgdorf, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, 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