secorvo
security consulting

Secorvo Security News

März 2018

Der Kern des Problems

Werbung hat Streuverluste. Niemand hat das so treffend auf den Punkt gebracht wie *Henry Ford* (1863-1947) in dem ihm zugeschriebenen Bonmot: „Ich weiß, die Hälfte meiner Werbung ist hinausgeworfenes Geld. Ich weiß nur nicht, welche."

Folgerichtig ist eines der zentralen Ziele im Marketing, diese Verluste zu reduzieren. Das gelingt allerdings nur, wenn der Werber möglichst präzise weiß, *wen* er erreichen muss und *wie* er diese Zielgruppe wirksam anspricht.

In beiderlei Hinsicht ist das Internet der Heilige Gral. Denn anders als bei einer Zeitschriftenanzeige, einer Plakatwerbung oder einem TV-Spot weiß jede Webseite, wer sie gerade besucht – und kann die zum Besucher passende Werbung einblenden.

Und zugleich, noch wertvoller, ist „im Netz" weit mehr über den Besucher bekannt, als anonyme Zuschauer- oder Leserbefragungen verraten – obendrein personalisiert. Dabei sind es sind nicht die „klassischen" personenbezogenen Daten wie Name, Geburtsdatum oder E-Mail-Adresse, die den eigentlichen Wert darstellen, sondern von vielen Betroffenen als wenig relevant eingestufte „Meta-Informationen": Zu welchen Zeiten wurden welche Seiten besucht? Welche Personen werden wie oft kontaktiert? Wie oft wurde wann nach was gesucht? Diese vermeintlich harmlosen Daten entblößen jedoch mit zunehmender Internet-Nutzung nahezu alles: die tatsächlichen Interessen (Suchziele), typische Verhaltensmuster (Nutzungszeiten, Verweildauern und Standortverläufe), Neigungen (Kontaktintensität) bis hin zur sexuellen Orientierung – und bei automatischer Auswertung von Nachrichteninhalten auch die persönlichsten Überzeugungen. Und mit jeder neuen App werden es mehr.

Ihre Analyse zielt dabei nicht auf Überwachung. Sondern darauf, die Unterschiede zu finden – bis zur Vorhersage des Verhaltens. Anders formuliert: Sie will die Persönlichkeit. Und genau deshalb ist nicht der Datenmissbrauch das Problem. Sondern diese Daten selbst.

Inhalt

secorvo
security consulting

Security News

Illegalisierte Blockchain

Wie in den SSN 2/2018 thematisiert, hat wohl nicht jeder, der die Blockchain als Lösung verschiedenster Probleme propagiert, das Konzept und seine Eigenschaften komplett durchdrungen. Einige „Nutzer" scheinen aber zumindest ein wesentliches Feature erfasst zu haben: Etwas, das einmal gültig in der Blockchain verzeichnet ist, kann nie wieder daraus verschwinden, allenfalls mit einem späteren Eintrag wieder rückabgewickelt werden.

Am 12.03.2018 veröffentlichten Forscher aus Frankfurt und Aachen eine Untersuchung von Dateninhalten, die bei vergangenen Transaktionen unauslöschlich in die Bitcoin-Blockchain aufgenommen wurden. Unter knapp 150 auffindbaren Bild-Dateien ist auch eine, die mutmaßlich den Tatbestand der Kinderpornographie erfüllt; dazu kommen mehrere Dutzend Links zu entsprechendem Material im sogenannten Darknet.

Damit sind die Beschaffung und der Besitz einer Kopie der kompletten Bitcoin-Blockchain, wie sie für das Bitcoin-Mining grundsätzlich erforderlich ist, in Deutschland und vielen anderen Ländern vermutlich illegal – ganz unabhängig vom rechtlichen Status der Bitcoin als Zahlungsmittel.

Man in the ISP

Citizen Lab beschreibt in einer Veröffentlichung vom 09.03.2018, wie die Internet Service Provider (ISP) Türk Telekom und Telecom Egypt Deep-Packet-Inspection-Technologien (DPI) nutzen, um ihren Kunden Schadsoftware oder Krypto-Miner unterzuschieben. DPI erlaubt es, nicht nur Metadaten von Datenpaketen zu durchsuchen, sondern auch deren Inhalte. Diese Möglichkeit wurde vor allem zur Erkennung und Filterung von Schadsoftware und Spam im Netzwerkverkehr entwickelt, lässt sich jedoch auch für Zensur und Einschränkung der Netzneutralität nutzen.

Offenbar werden von Türk Telekom unverschlüsselte Programmdownloads bekannter Programme wie VLC, Skype oder Opera mit einer Schadsoftware infiziert, die es erlaubt, die Computer der Benutzer auszuspähen. In Ägypten werden Teile des Verkehrs auf Affiliate-Programme und Krypto-Miner geleitet, um zusätzliche Einnahmen zu generieren.

Auch der Download von Programmen sollte wie jede andere sensible Kommunikation über einen TLS geschützten Kanal stattfinden. Mechanismen wie HSTS verhindern dabei ungewollte Downgrades auf HTTP. Manipulationsangriffe muss man dabei offenbar nicht mehr nur bei offenen WLANs unbekannter Anbieter befürchten, sondern sollte auch besser Providern keinen Vertrauensvorschuss mehr gewähren. Leider gibt es noch immer zahlreiche Softwareanbieter und andere Hersteller, die ihre Downloads unverschlüsselt bereitstellen.

Darf's ein bisschen mehr sein?

Weltweit gültige TLS-Serverzertifikate bekommt man nach den Richtlinien des CA/Browser-Forums in den Geschmacksrichtungen DV, OV und EV. Die EV (Extended Validation) Zertifikate enthalten über den oder die Servernamen hinaus weitere Angaben zum dahinter stehenden Unternehmen. In einem für Antragsteller und Trustcenter gleichermaßen aufwändigen Validierungsprozess wird sichergestellt, dass alle enthaltenen Angaben korrekt sind, das Unternehmen die fragliche Internet-Domain besitzt und die Erstellung des Zertifikats auch tatsächlich veranlasst hat. EV-Zertifikate werden eingesetzt, wo dies regulatorisch verlangt ist, bspw. beim Online-Banking, oder wo immer der Serverbetreiber Wert auf den „grünen Balken" legt, mit dem Browser besondere Vertrauenswürdigkeit anzeigen.

OV (Organization Validation) Zertifikate vereinen die Nachteile der beiden anderen Typen: Bei der Ausstellung werden zwar ähnlich wie bei EV Angaben zum Unternehmen geprüft, vom Browser wird jedoch kein Unterschied zu DV-Zertifikaten angezeigt.

Bei der einfachsten Kategorie, den DV (Domain Validation) Zertifikaten, wird vor der Ausstellung lediglich geprüft, ob der Antragsteller Kontrolle über die Internet-Domain hat, in der der zu zertifizierende Servername liegt. Dieser Check ist gut automatisierbar. Genau das macht sich die gemeinnützige CA Let's Encrypt zunutze, die kostenfrei DV-Zertifikate ausstellt.

Am 13.0.3.2018 aktivierte Let's Encrypt ACMEv2, die neue Version ihres Protokolls zum automatischen Zertifikatsbezug. Damit sind nun auch Wildcard-DV-Zertifikate für alle Server einer bestimmten Subdomain kostenfrei erhältlich.

Seither gibt es kaum noch Gründe, bei einem kommerziellen Trustcenter zu kaufen, wenn es kein EV-Zertifikat sein soll. Interne Serverzertifikate der eigenen PKI kann jedoch auch Let's Encrypt nicht komplett ersetzen – rein intern genutzte Server- bzw. Domain-Namen oder IP-Adressen sind für öffentliche DV-Zertifikate tabu.

Schwachstellensuche bei LTE

Am 06.03.2018 veröffentlichten Forscher der Universitäten Purdue und Iowa Details zu dem von ihnen entwickelten Tool LTEInspector. Ähnlich wie der bekannte IMSI-Catcher zu GSM-Zeiten setzt sich

dieses Tool als Emulation eines Access Points und eines Endgeräts zwischen LTE-Endgerät und Providernetz und erlaubt es, Analysemethoden für Kryptoprotokolle automatisiert auf reale LTE-Netze anzuwenden. Damit wurden auch gleich zehn neue und neun bereits bekannte Angriffe gegen den LTE-Verbindungsaufbau (wieder-)entdeckt und in echten LTE-Netzen durchgespielt.

So hoch der Wert des Tools für Analyse und Validierung von Sicherheitsprotokollen einzuschätzen ist, muss man doch die Tragweite der Schwachstellen relativieren. Ein Angreifer muss sich in Funkreichweite des Opfers befinden: Dadurch sind bspw. eine grobe Lokalisation des Opfers und die Möglichkeit, dessen Funknetz-Aktivitäten zeitlich zu erfassen, auch ohne elaborierten Protokollangriff gegeben. Auch ein Denial-of-Service wäre protokollunabhängig durch einen Störsender möglich.

Einer der Angriffe erlaubt, unautorisiert für Erdbeben oder Tsunamis gedachte Warnmeldungen abzusetzen. Dies scheint im Sinne einer Risikoabwägung plausibel – dass Sicherheitshürden im Katastrophenfall fatal sein könnten, hat sich u. a. bei der verzögerten Entwarnung nach dem Raketen-Fehlalarm auf Hawaii im Januar bestätigt.

Verblüffend ist, dass bei einem großen US-Provider unverschlüsselte LTE-Verbindungen möglich waren. Warum Handys nicht – wie jeder WWW-Browser – dem Anwender den Verschlüsselungsstatus seiner Verbindung anzeigen, bleibt nach wie vor ein Rätsel.

Orientierungspunkte

Die Art. 29 Gruppe beschloss am 06.02.2018 eine Reihe neuer Orientierungshilfen zur DSGVO. Mehrere beziehen sich auf den Datenverkehr mit Drittstaaten, u. a. mit Bezug die einschlägige EuGH-Rechtsprechung und Art. 44 ff DSGVO. Sie beschäftigen sich mit der Feststellung eines angemessenen Datenschutzniveaus (WP 254 rv.01), den Ausnahmeregelungen des Art. 49 (WP261/262) und mit den notwendigen Elementen von *Corporate Binding Rules* (BCR, WP 257 rev.01). Zur Feststellung des angemessenen Datenschutzniveaus sei nur die Umsetzung der Kerninhalte der Europäischen Gesetzgebung zu prüfen; dabei wird jedoch sehr weitgehend auf die bestehenden Instrumente wie Zweckbindung, Betroffenenrechte und Transparenz zurückgegriffen. Daneben werden eine unabhängige Aufsicht und eine wirkungsvolle Beschränkung staatlicher Eingriffsbefugnisse gefordert. Die Ausführungen zu BCR umfassen eine Tabelle mit kommentierten Inhaltsanforderungen, darunter direkte Ansprüche des Betroffenen als Drittbegünstigtem. Der Art. 49 schließlich sei als Ausnahmeregelung zu verstehen und sehr eng auszulegen.

Weiter passte die Art. 29 Gruppe die Richtlinien zur Meldung von Datenschutzvorfällen (WP250rev.01), zu automatisierten Einzelentscheidungen (WP251-rev.01) und zur Bußgeldbemessung (WP253) an.

WP250 setzt sich umfangreich mit dem Zusammenspiel von Auftragsverarbeiter und Verantwortlichem, dem Meldeinhalt und dem Ablauf zur Vorfallsklärung auseinander. Am Ende steht eine Liste mit Beispielvorfällen. Eine Meldung wird regelmäßig innerhalb von drei Tagen erwartet; Prozesse zur technischen Vorfallserkennung und –untersuchung werden nach Art. 32 DSGVO vorausgesetzt.

WP251 zu automatisierten Einzelfallentscheidungen fasst in einer Liste am Ende konkrete Umsetzungsanforderungen als *best practice* zusammen. Das Papier zur Bußgeldfestsetzung (bereits vom Oktober 2017) enthält zahlreiche Bemessungskriterien, eine sehr weite, Art. 4 Nr. 19 DSGVO ignorierende Unternehmensdefinition zur Erfassung ganzer Konzerne, allerdings keine konkreten beispielhaften Bemessungen. Intensiv diskutiert werden jedoch alternative Maßnahmen wie Verwarnungen.

Insgesamt tragen die Orientierungshilfen dazu bei, das künftige Vorgehen der Aufsichtsbehörden besser einschätzen zu können. Teilweise tendieren die Papiere allerdings zu einer eher restriktiven Auslegung der einzelnen Bestimmungen.

Secorvo News

Für Kurzentschlossene

Noch wenige freie Plätze können wir für unser nächstes T.I.S.P.- (**16.–20.04.2018**) und das PKI-Seminar (**23.–26.04.2018**) anbieten. Programme, weitere Termine und Online-Anmeldung unter https://www.secorvo.de/seminare

Sesam, öffne Dich – nicht.

Dass der Betreiber der hausinternen IT gerne eigenständig kontrolliert, was in seinem Rechenzentrum vorgeht und wie die dortigen Betriebsbedingungen sind, ist bekannt. Doch um das Ziel einer möglichst hohen Verfügbarkeit zu erreichen, muss auch immer der Gefahrenfaktor Mensch betrachtet werden. Bei unserem kommenden KA-IT-Si-Event am **12.04.2018** werden Ihnen von Fabian Schäfer (Rittal) an Anwendungsbeispielen die technischen Einsatzmöglichkeiten automatisierter Zutrittskontrollsysteme im IT-Umfeld vorgestellt.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

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

April 2018	
10.-11.04.	Datenschutztage 2018 (FFD Forum für Datenschutz, Wiesbaden)
19.-20.04.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
23.-26.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
24.-26.04.	3rd IEEE European Symposium on Security and Privacy (IEEE Computer Society, London/UK)
25.-27.04.	GI SICHERHEIT 2018 (Gesellschaft für Informatik e.V., Konstanz)
25.-26.04.	BvD Verbandstage 2018 (BvD e.V., Berlin)
29.04.-03.05.	Eurocrypt 2018 (IACR, Tel Aviv/ISR)
Mai 2018	
02.-03.05.	Security Forum 2018 (Hagenberger Kreis zur Förderung der digitalen Sicherheit, Hagenberg/AT)
07.-09.05.	11th International Conference on IT Security Incident Management & IT Forensics (GI, SIDAR, DFN-Cert, Hamburg)
15.-18.05.	European Identity & Cloud Conference 2018 (KuppingerCole Ltd., München)
16.-18.05.	19. Datenschutzkongress (EUROFORUM Deutschland SE, Berlin)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Hans-Joachim Knobloch, 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