secorvo
security consulting

Secorvo Security News

September 2019

Das Vermächtnis

Vor exakt 2.300 Tagen erwirkte das FBI einen Haftbefehl gegen Edward Snowden – seitdem ist er auf der Flucht. Ein großes Opfer für den damals knapp 30-Jährigen. Jetzt hat er seine Geschichte veröffentlicht – auf Anhieb ein Bestseller. Was aber hat Snowden tatsächlich bewirkt?

Auf den ersten Blick wenig. Ende 2013 stellte die NSA ihr Utah Data Center fertig, mit einer Speicherkapazität, die die Archivierung und Analyse der gesamten weltweiten Datenkommunikation ermöglicht. Über den US Cloud Act sicherten sich die amerikanischen Geheimdienste am 06.02.2018 den Zugriff auf die Daten ausländischer Kunden von amerikanischen Unternehmen – ein (bislang folgenloser) Affront gegen das Privacy Shield-Abkommen mit der EU vom 02.02.2016. Derweil versucht das Bundesinnenministerium, deutschen Nachrichtendiensten „technische Datenerhebungen aus Wohnungen" zu ermöglichen – schließlich verfügen immer mehr Haushalte über freiwillig installierte Abhöranlagen: Alexa, Cortana, Siri und andere Sprachassistenten lassen grüßen.

Aber es gibt auch die andere Seite. So warnen Browser inzwischen vor Webseiten, die HTTP nicht oder mit veralteten TLS-Versionen schützen – rund 90% der Webkommunikation wird inzwischen verschlüsselt. Auch dank der Initiative „E-Mail made in Germany", einer Reaktion der deutschen E-Mail-Provider auf Snowdens Veröffentlichungen, schützen heute nur noch wenige E-Mail-Server die Kommunikation nicht via TLS vor dem Zugriff Dritter. Mehrere Messenger bieten vor Geheimdiensten sichere Ende-zu-Ende-Verschlüsselung. Sogar Microsoft und Apple versuchen die Daten ihrer Kunden dem NSA-Zugriff zu entziehen, indem sie die Schlüsselgenerierung in Kundenhand legen.

Jetzt gilt es, die Spurensammlung von Google und Co. zu begrenzen – sie sind inzwischen der Ansaugstutzen der NSA im Netz. Wenn uns das nicht gelingt ist Snowdens Vermächtnis verspielt.

Inhalt

secorvo
security consulting

Security News

Sichere(re)s DNS?

Gelingt es einem Angreifer die Namensauflösung einer Domäne zu manipulieren, kann er Nutzern gefälschte Webseiten „unterschieben". Eine wirksame Gegenmaßnahme ist die Einführung von DNS over TLS oder DNS over HTTPS (DoH), doch die läuft bislang zögerlich. Am 06.09.2019 kündigte Mozilla an DoH zum Default zu machen. Der Firefox-Browser enthält bereits einen DoH-Resolver, der künftig standardmäßig alle DNS-Anfragen verschlüsselt an einenn Resolver von Cloudflare senden soll.

Für komplexere Netzkonfigurationen sind allerdings Nebenwirkungen zu erwarten, bspw. bei Split-DNS (hier wird immer die externe Namensauflösung geliefert) oder Content-Filtering Blacklists. Firefox setzt Heuristiken ein, um solche Konfigurationen zu erkennen: Beim Start versucht Firefox, eine „Canary"-Domain aufzulösen; gelingt das nicht, wird DoH abgeschaltet. Schlägt später eine DOH-Anfrage fehl, wird das Betriebssystem befragt, und ist eine Enterprise Policy im Einsatz, ist DoH standardmäßig inaktiv. Vorsicht gilt auch, falls interne Domainnamen nicht offengelegt werden sollen. Administratoren sollten DOH in Firefox erforderlichenfalls deaktivieren.

Dubiose Hotspots oder Zensur betreibende Länder können mittels der Canary-Domain die DOH-Auflösung einfach „abschalten". Und beunruhigen kann auch, dass künftig Cloudflare alle DNS-Anfragen erhält, selbst wenn der Betreiber angibt, die Daten nur für 24 Stunden zu speichern. Monopolstellungen sind immer ein Risiko – in verschiedener Hinsicht.

Identitätsdiebstahl via Auskunft

Auf der Black Hat-Konferenz stellte der Sicherheitsforscher James Pavur am 08.08.2019 einen Social Engineering-Angriff vor, der sich Fehler bei der Umsetzung der datenschutzrechtlichen Auskunftspflicht von Unternehmen zu Nutze macht. Mittels einer selbst angelegten E-Mail-Adresse gab sich Pavur gegenüber mehr als 150 Unternehmen als seine Mitautorin Casey Knerr aus und bat um Auskunft über alle zu „ihr" verarbeiteten personenbezogenen Daten. Von den Unternehmen reagierten 72%; 23% antworteten gar nicht und 5% verweigerten jede Auskunft. Von den reagierenden Unternehmen übersandten 24% die Daten ohne jede Identitätsprüfung, weitere 16% verlangten leicht zu fälschende Identitätsnachweise (wie das Ausfüllen einer schriftlichen Erklärung, tatsächlich die betroffene Person zu sein).

Dabei sollte selbstverständlich sein, dass einem datenschutzrechtlichen Ersuchen erst nach hinreichend sicherer Identitätsprüfung nachgekommen wird, z. B. durch Versand an eine authentisierte Zustelladresse, ein Login in einem bestehenden Benutzerkonto oder die Vorlage eines von einer vertrauenswürdigen Instanz ausgestellten Identitätsnachweises.

De-Anonymizer

Personenbezogene Daten sind Informationen, die sich auf eine identifizierbare natürliche Person beziehen. Dabei sind für die Identifikation in der Regel weder Name noch Adresse erforderlich: Nach einer am 23.07.2019 in „nature" veröffentlichten Studie genügen bereits 15 demografische Attribute, um 99,98% der US-Bürger zu re-identifizieren. Für eine Anonymisierung reicht es daher in der Regel nicht, in einem Datensatz lediglich den Namen und die Adresse zu löschen. Mehr noch: Je aussagekräftiger die statistischen Angaben über eine Gruppe von Personen, desto höher ist die Wahrscheinlichkeit, dass eine Re-Identifizierung Einzelner möglich ist. Mit dem wachsenden Einsatz von künstlicher Intelligenz bei Big-Data-Auswertungen dürften zukünftig vermehrt vermeintlich anonyme Datensammlungen als Verarbeitung personenbezogener Daten zu bewerten sein.

SIM-Jack

Am 12.09.2019 veröffentlichte Cathal McDaid von AdaptiveMobile Security im firmeneignen Blog einen Post über die Schwachstelle Simjacker. Darüber können sich Angreifer mittels einer präparierten SMS in der SIM-Karte einnisten. Von dort können Informationen ausgelesen oder unbemerkt Telefonverbindungen aufgebaut werden, die das Gerät in eine Wanze verwandeln. Offenbar nutzen diese Schwachstelle Angreifer mehrerer Länder schon seit mindestens zwei Jahren. Die Schwachstelle bedroht jedes mobile Endgerät, auf dessen SIM-Karte (UICC) der Netzbetreiber die Software S@T Browser, eine Alternative zum klassischen SIM Toolkit, installiert hat. Sie soll in 30 Staaten mit insgesamt über einer Milliarde Einwohnern im Einsatz sein. Immerhin: Die Netzbetreiber Telekom, Vodafone und Telefónica teilten übereinstimmend mit, dass auf ihren Karten der S@T Browser nicht installiert ist.

Die Erfahrung zeigt, dass es in komplexen IT-Systemen selten nur einen einzigen Sicherheitsbug gibt. Daher gilt (nicht nur aus diesem Grund): Gelegentliches Ausschalten hilft.

Unzulässige Kekse

Cookie-Banner finden sich inzwischen auf fast allen Webseiten – oft sind sie jedoch datenschutzrecht-

lich unzureichend. Erst am 18.09.2019 wies der Landesbeauftragte für Datenschutz- und Informationsfreiheit (LfDI) Baden-Württemberg darauf hin, dass die Nutzung der Webseite keine rechtswirksame Einwilligung darstellt. Eine Studie der Ruhr-universität Bochum zeigt, dass die meisten untersuchten Cookie-Banner nicht nur nicht DSGVO-konform sind (86%), sondern auch psychologische Tricks anwenden, um Nutzer dazu zu bringen die gewünschte Einwilligung zu erteilen. Oft wird zudem nicht darüber informiert, dass die Daten an Dritte weitergegeben werden. Das LG Dresden urteilte am 11.01.2019, dass es nicht ausreicht, die Nutzer aufzufordern, Einstellungen im Browser vorzunehmen, die das Speichern von Cookies und die Übertragung von personenbezogenen Daten verhindern – auch dies eine verbreitete Unsitte.

Bereits im Cookie-Banner muss die Möglichkeit gegeben werden, die Verwendung von Cookies abzulehnen. Hier hilft eine kurze Beschreibung, welche Cookies was an wen übermitteln. Ausführliche Hinweise und Informationen können dann in einem gesonderten Cookie-Hinweis oder in der Datenschutzerklärung folgen. Eine gute Hilfe bei der Gestaltung bieten die FAQ des LfDI Baden-Württemberg.

Renitenter Sündenbock

Ransomware-Autoren haben ein neues Angriffsziel: US-amerikanische Kleinstädte, die nicht ausreichend gegen derartige Angriffe gewappnet sind. In der Not sind sie oft bereit, das geforderte Lösegeld zu zahlen. Am 10.06.2019 wurde Lake City (Florida) Angriffsopfer – und verlor 460.000 USD (42 BTC). Daraufhin entließ man am 21.06.2019 den IT-Direktor. Brian Hawkins jedoch verklagte am 09.08.2019 die Stadt: Er habe bereits 2017 gewarnt und auf die Anschaffung eines Cloud-basierten Backup-Systems gedrängt, was aus Kostengründen abgelehnt worden sei. Nach Überzeugung von Hawkins habe die Stadt damit entschieden, das Risiko eines Cyberangriffs zu akzeptieren. Solche essentiellen Entscheidungen sind im Rahmen des Risikomanagements zu dokumentieren, sonst kann man sich später nicht darauf berufen. Im Fall von Hawkins ist dies nicht geschehen – was ihn nun in Beweisnot bringt.

Secorvo News

Secorvo@it-sa

Besuchen Sie uns vom 08. bis 10.10.2019 auf der deutschen IT-Sicherheits-Leitmesse it-sa in Nürnberg. Unseren Stand finden Sie in Halle 10, Standnummer 10.1.-630. Wir zeigen unsere „ready2go"-Managementlösungen für Informationssicherheit (ISMSr2g), Datenschutz (DSMSr2g) und die Zertifikatsverwaltung (Easy). Am 09.10.2019 spricht um 10:45 Uhr Jörg Völker im Forum M10-Management über „Die Rückkehr der ISMS-Ritter".

Sie haben noch kein Ticket? Registrieren Sie sich mit unserem Gutscheincode **A411787** und Sie erhalten ein kostenfreies Tagesticket.

3. Auflage des T.I.S.P.-Buchs

Jetzt ist sie verfügbar – die gründlich überarbeitete und ergänzte dritte Auflage des T.I.S.P.-Begleitbuchs „Informationssicherheit und Datenschutz", ein Gemeinschaftswerk des gesamten Secorvo-Teams. Wir freuen uns sehr, dass der dpunkt.verlag die Herausgabe übernommen hat. Auf der Verlagswebseite finden sich ausgewählte Leseproben des 824 Seiten umfassenden Grundlagenwerks, das nun für 84,90 € im Buchhandel erhältlich ist.

Nächste Seminare

Die letzte Gelegenheit, bei der Sie sich in diesem Jahr Ihre Qualifikation und Erfahrung in der IT-Sicherheit zertifizieren lassen können, bieten wir Ihnen in der 48. Woche mit dem nächsten T.I.S.P.-Seminar (**25.–29.11.2019**) – von über 250 Teilnehmern mit 4,35 von 5 Punkten bewertet. In der Woche davor kommen PKI-Interessierte zum Zug: In nur vier Tagen vom Einsteiger zum Experten bei unserem PKI-Seminar (**18.–21.11.2019**), Rating: 4,3. Wir freuen uns auf Ihre Teilnahme!

Alle Programme, die Seminartermine 2020 und die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Möge das ISMS mit dir sein

Die Etablierung von Informationssicherheit im Unternehmen gleicht oft dem Kampf der Star-Wars-Rebellen gegen die dunkle Seite der Macht – hier dem allzu sorglosen Umgang mit schützenswerten Informationen. Dabei hilft ein Informationssicherheits-Managementsystem (ISMS).

Damit sich der Aufbau und die Zertifizierung des ISMS jedoch nicht ähnlich lange hinziehen wie der Kampf gegen das Imperium empfiehlt es sich zielstrebig vorzugehen. Der Vortrag beim kommenden KA-IT-Si-Event am **24.10.2019** fasst die grundlegenden Anforderungen der ISO 27001 zusammen und stellt die konkrete Umsetzung und Zertifizierung beim Kirchlichen Rechenzentrum Südwestdeutschland (KRZ-SWD) vor.

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

Veranstaltungshinweise

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

Oktober 2019	
08.-10.10.	it-sa 2019 (NürnbergMesse GmbH, Nürnberg)
14.-18.10.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
14.10.	Night of the Living Labs (FZI Forschungszentrum Informatik, Karlsruhe)
15.10.	Swiss Cyber Storm 2019 (Swiss Cyber Storm Association, Bern/CH)
22.-24.10.	IDACON 2019 (WEKA-Akademie, München)
November 2019	
05.-06.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
05.-06.11.	9. Handelsblatt Jahrestagung - Cybersecurity (Handelsblatt/EUROFORUM, Berlin)
11.-15.11.	ACM CCS 2019 (ACM/SIGSAC, London/UK)
18.-21.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
20.-22.11.	43. DAFTA (GDD, Köln)
25.-29.11.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
26.-29.11.	DeepSec In-Depth Security Conference Europe (DeepSec, Wien/AT)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Benjamin Faller, Hans-Joachim Knobloch, Friederike Schellhas-Mende, Christian Titze

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