secorvo
security consulting

Secorvo Security News

Juli 2018

Falsche Baustelle

Seit Jahren geistert das Bild der E-Mail als „Postkarte“ unausrottbar durch Gazetten und Datenschutzempfehlungen: Wer E-Mails unverschlüsselt versende, der müsse damit rechnen, dass sie mitgelesen werden. Tatsächlich übermitteln Mailserver die ihnen anvertrauten Nachrichten heute meist wirksam verschlüsselt: Als Reaktion auf Edward Snowdens Veröffentlichungen stellten 2014 im Projekt „E-Mail made in Germany“ mehrere Provider und immer mehr Unternehmen ihre Mailserver auf eine TLS-Verbindungsverschlüsselung um, und Zugriffe auf das Postfach werden sowohl von Web-Clients als auch unternehmensintern schon längst verschlüsselt. Ein Mitlesen von E-Mails erfordert daher heute einen erfolgreichen DNS-Angriff – oder den direkten Zugriff auf die Postfächer.

Genau dort lauert in Wirklichkeit die reale Bedrohung: Amerikanische Anbieter kostenloser E-Mail-Dienste wie insbesondere GMail geben Drittfirmen, die Apps mit E-Mail-Anbindung realisieren, großzügig den Zugriff auf Kundenpostfächer frei, sofern diese dafür eine Zustimmung der Benutzer einholen. Und dann wird, automatisiert oder manuell, die persönliche Nachrichtenablage durchwühlt – z. B. um Spam-Diensten die Optimierung der Empfängeransprache zu ermöglichen (wie Return Path), passende Werbung zu generieren oder Testdaten für die Verbesserung der eigenen App zu gewinnen. Immerhin: Wer wissen will, welchen Apps er bereits Zugriff auf sein GMail-Konto eingeräumt hat, kann dies in den Privacy-Einstellungen seines Google-Accounts nachprüfen.

Dass es so etwas wie ein Fernmeldegeheimnis gibt und persönliche Kommunikationsinhalte nicht in Testumgebungen gehören hat sich offenbar noch nicht bei allen Anbietern herumgesprochen. Und für Anwender ist es noch immer nicht selbstverständlich, dass man Datenschutzerklärungen von Apps sehr genau lesen sollte, bevor man ihnen zustimmt – allen Datenschutzskandalen zum Trotz.

Inhalt

secorvo
security consulting

Security News

WPA ... zum Dritten

Nicht nur das TLS-Protokoll (SSN 06/2018), sondern auch das als WPA2 bekannte und ebenfalls in die Jahre gekommene Sicherheitsverfahren hat ein Facelifting erhalten: Die WiFi Alliance veröffentlichte am 09.04.2018 eine Zusammenfassung der neueren Sicherheitsmechanismen, die in 802.11s, 11w bzw. 11ac standardisiert wurden, unter der Bezeichnung WPA3:

- das Passwort-basierte Schlüsselaustauschverfahren SAE, das Sicherheit gegen Offline-Wörterbuchattacken auf das WLAN-Passwort verspricht,
- die Absicherung von Management-Frames, wie bspw. Deauthentication, die Angreifer zum Abmelden einer angegriffenen Station missbrauchen konnten und
- die durchgängige Nutzung von Kryptoalgorithmen, die einer 192-bit-Stärke nach aktuellen US-Behördenstandards entsprechen.

Dass dabei recht sorgfältig gearbeitet wurde, zeigt sich u. a. daran, dass nicht nur die Stärke der WLAN-Verschlüsselung selbst, sondern auch die TLS Cipher Suites festgelegt wurden, die bei einer vorangegangenen EAP-Authentifikation zum Einsatz kommen dürfen.

1:0 für 802.11 vs. Bluetooth SIG

Ordentlich implementierte WPA3-Produkte sollten auch gegen die Schwachstelle vieler Bluetooth-Implementierungen gefeit sein, die am 24.07.2018 publiziert wurde – die Bluetooth SIG hingegen muss ihre Spezifikation um einen Schritt zur Prüfung der übergebenen Elliptische-Kurven-Punkte nachbessern, um von Angreifern konstruierte Punkte zuverlässig zu verwerfen. Für SAE ist eine solche Prüfung bereits in Abschnitt 12.4.5.4 von IEEE 802.11-2016 beschrieben – siehe Seite 1942.

Framing 4.0

Bisher waren für einen kritischen, mit den Möglichkeiten der Bildmanipulation und Bildsynthese vertrauten Beobachter Fälschungen durch Video-Rewriting meist mit bloßem Auge erkennbar. Diese Zeiten sind nun allerdings vorbei: Am 29.05.2018 wurde von einer Forschergruppe um das Max-Planck-Institut für Informatik ein Verfahren veröffentlicht, welches dreidimensionale Kopfmodelle erstellt und die Qualität der Fälschung durch einen KI-Gegenspieler prüfen lässt.

Ob die von den Autoren der Studie in den Vordergrund gestellte Lippenkorrektur bei synchronisierten Filmen zukünftig der bevorzugte Anwendungsfall sein wird, darf bezweifelt werden – Fake News und Fake Porn erscheinen da viel wahrscheinlicher. Auch der Aufwand wird eine breite Anwendung kaum verhindern: Diese Hoffnung war schon vor 35 Jahren trügerisch, als erste Warnungen vor digitaler Foto-Fälschung ausgesprochen wurden. Hardware für rund 2.000 € und eine Rechenzeit von einigen Stunden bis wenigen Tagen sind bereits heute kein unüberwindliches Hindernis.

1000 x T.I.S.P.

Das deutsche Schwergewicht der Personenzertifizierung für Informationssicherheit T.I.S.P. (TeleTrusT Information Security Professional) wurde am 10.04.2018 zum 1.000sten Mal verliehen – an Herrn Kai Riecke, CTO der Hubert Burda Media Holding.

Prof. Dr. Norbert Pohlmann, Vorstand von TeleTrusT, äußert sich stolz: „Der T.I.S.P. hat eine Anerkennung erreicht, die den Vergleich mit ähnlichen Personen-Zertifikaten im deutschsprachigen Raum nicht scheuen muss."

Mit der erfolgreich abgelegten Prüfung zum T.I.S.P. belegt ein IT-Sicherheits-Spezialist seine umfassenden Kenntnisse im IT-Sicherheitsumfeld auf technischem, rechtlichem und strategischem Gebiet. Das Zertifizierungsprogramm umfasst eine fünftägige Schulung, an die sich eine intensive Prüfung anschließt. Die Schulungsanbieter Secorvo, isits und Fraunhofer SIT freuen sich bereits auf die Ausstellung von Zertifikat Nr. 2.500...

Löschkonzept goes ISO

Die englische Fassung der von den Unternehmen Deutsche Bahn, Blancco, DATEV, Secorvo und Toll Collect geförderten „Leitlinie Löschkonzept", die am 08.04.2016 als DIN 66398 verabschiedet worden ist (siehe SSN 4/2016), wurde jetzt bei der ISO als Grundlage eines internationalen Standards eingereicht.

Nach den bisherigen Rückmeldungen wird sich an der darin beschriebenen Vorgehensweise nichts ändern. Anpassungen sind notwendig, weil die Beispiele in der Norm noch auf das alte BDSG und nicht auf die DSGVO oder andere internationale Vorschriften abstellen und einige Begriffe an die ISO-Terminologie angepasst werden sollen.

Das Standardisierungsprojekt soll in den kommenden Wochen vom zuständigen Gremium beschlossen werden. Ein ISO-Standard könnte dann Ende 2021 verabschiedet werden und die in Deutschland bereits genormte Vorgehensweise für Löschkonzepte sich auch international durchsetzen.

Informationspflicht

Nach der Datenschutz-Grundverordnung (DSGVO) entsteht zum Zeitpunkt der Erhebung personenbezogener Daten eine Informationspflicht des verantwortlichen Datenverarbeiters gegenüber dem Betroffenen (Art. 13 DSGVO). Dabei können sich in der praktischen Umsetzung zahlreiche Problemfälle ergeben:

- das Unternehmen erhält spontan zugesandte Informationen (z. B. eine Initiativbewerbung),
- es laufen Hintergrundprozesse ab (wie eine automatisierte Erhebung z. B. bei Bonitätsprüfungen),
- es sind gar keine Interaktionen vorgesehen oder
- ein Dienstleister erhebt die Informationen.

Meist liegt die Hauptschwierigkeit darin, einen geeigneten Kommunikationskanal zu finden, der den Betroffenen erreicht und die Anforderungen der DSGVO erfüllt – auch in Bezug auf den Inhalt der Information: So lassen sich komplexe Verarbeitungen oft nicht ohne weiteres in zugleich präziser, transparenter, verständlicher und leicht zugänglicher Form darstellen.

Bleibt zu hoffen, dass die Aufsichtsbehörden eine pragmatische Auslegung dieser Anforderungen vornehmen, die noch etwas einfacher ausfällt als die derzeitigen Vorschläge zur Ausweisung der Videoüberwachung. Denn es wird immer wieder Fälle geben, in denen die Daten verarbeitende Stelle ihren Informationspflichten entweder nicht unmittelbar oder nicht zugleich präzise und verständlich nachkommen kann.

Facebook unter Druck

Nachdem der Europäische Gerichtshof in seinem Urteil vom 05.06.2018 die grundsätzlich gemeinsame Verantwortlichkeit für die Verarbeitung der Nutzerdaten von Unternehmensauftritten bei Facebook („Fanpages“) geklärt hat, haben auch die deutschen Datenschutzaufsichtsbehörden erste Stellungnahmen abgegeben.

Die Pflichten gemeinsam Verantwortlicher regelt die DSGVO in Art. 26. Danach müssen die Zuständigkeiten insbesondere bezüglich der Betroffenenrechte und Informationspflichten in einer transparenten Vereinbarung festgelegt werden. Dementsprechend fordern die Aufsichtsbehörden, dass dem Fanpage-Besucher diese Informationen beim Besuch zugänglich gemacht werden müssen. Für das Tracking soll Facebook grundsätzlich eine Einwilligung einholen; die Seitenbetreiber müssen sich vergewissern, dass Facebook die Pflichten erfüllt.

Bislang hat Facebook den Seitenbetreibern keine entsprechende Vereinbarung zur Verfügung gestellt. Für Seitenbetreiber ist damit auch nach dem Urteil unklar, womit sie zu rechnen haben und in wieweit sie derzeit ihre Pflichten bezüglich der Informationspflichten auf der Fanpage erfüllen.

Secorvo News

Weiterbildung

Schon im Sommer an den Herbst denken: Im Oktober starten wir unsere Seminarserie mit den beiden Zertifizierungsseminaren T.I.S.P. (**15.–19.10.2018**) und T.P.S.S.E. (**12.–15.11.2018**). Wir freuen uns, sie in unserem frisch renovierten Seminarbereich begrüßen zu dürfen – und empfehlen für das T.I.S.P.-Seminar eine baldige Anmeldung, da uns schon zahlreiche Anmeldungen vorliegen.

Programm und Online-Anmeldung unter https://www.secorvo.de/seminare

Digitale Mülltrennung

Die DSGVO fordert das Löschen personenbezogener Daten. Wie aber organisiert man diese Aufgabe für eine Organisation effizient und systematisch? Die DIN 66398 „Leitlinie Löschkonzept“, an deren Entwicklung Secorvo maßgeblich beteiligt war, gibt zahlreiche Hilfestellungen dafür.

Dr. Volker Hammer (Secorvo) war Editor der Norm und gibt beim kommenden **KA-IT-Si-Event** am **13.09.2018** im Panoramasaal der IHK Karlsruhe einen Überblick über die Inhalte aus erster Hand (Beginn: 18 Uhr). Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ (zur Anmeldung).

Secorvo@itsa

In diesem Jahr werden wir vom 09. bis 11.10.2018 auf der IT-Security-Messe it-sa in Nürnberg vertreten sein und dort am Stand 10.1-628 unsere Datenschutz- (DSMSready2go) und Informationssicherheits-Management-Lösungen (ISMSready2go) zeigen. Sie sind herzlich eingeladen, bei Interesse vorab einen Termin mit uns zu vereinbaren.

Veranstaltungshinweise

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

August 2018	
04.-09.08.	Blackhat USA 2018 (Blackhat, Las Vegas/US)
09.-12.08.	DEF CON 26 (DEFCON, Las Vegas/US)
14.08.	SOUPS 2018 (usenix, Baltimore/US)
15.-17.08.	27th USENIX Security Symposium (usenix, Baltimore/US)
15.-18.08.	DFRWS USA 2018 (DFRWS, Providence/US)
19.-23.08.	Crypto 2018 (IACR, Santa Barbara/US)
September 2018	
04.-05.09.	D • A • CH Security (GI, OCG, TeleTrusT, Gelsenkirchen)
10.09.	Sommerakademie 2018: Beschäftigtendatenschutz im digitalen Zeitalter (ULD, Kiel)
13.09.	Digitale Mülltrennung (KA-IT-Si, Karlsruhe)
Oktober 2018	
01.-03.10.	ISSE 2018 (EEMA, Rom/IT)
08.-12.10.	OWASP AppSec USA 2018 (OWASP Foundation, San Jose/US)

Fundsache

Studien zur IT-Sicherheit gibt es viele – aber nur wenige liefern statistisch belastbare Aussagen und sind deutlich mehr als eine willkürliche Befragung zufällig ausgewählter Unternehmen. Daher hebt sich die wik-Studie „Aktuelle Lage der IT-Sicherheit in KMU“ vom 18.05.2018 erfreulich vom sonstigen Einerlei der Kaffeesatzerkenntnisse ab.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Dr. Volker Hammer, Hans-Joachim Knobloch, Michael Knopp, Thomas Maus, Sarah Niederer, 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