secorvo
security consulting

Secorvo Security News

April/Mai 2018

Der Spion, den ich liebe

Tim Berners-Lees Vision des World Wide Web war die eines freien Informationszugangs und der virtuellen Zusammenarbeit. Aber schon Mitte der 90er Jahre änderte sich der Charakter des WWW: Zwischen die Informationsquellen mischten sich die ersten Shops, die neben Besuchsdaten (IP-Adresse, Herkunft, Verweildauer) auch Kontaktdaten (Adresse, Kreditkartendaten oder die Bankverbindung) erfragten und Käuferprofile erstellten. Seither fordern immer mehr Dienste Daten, wie Sport-Coaches, Tourenplaner oder Gesundheitsberater. Dank Social Networks werden sie immer persönlicher: Fotos, Lebensläufe und Chatinhalte landen nun auch im Netz. Mit Smartphones wurden die Dienste mobil und werten jetzt auch Ortsinformationen aus, und inzwischen liefert das Internet of Things (IoT) Daten unserer smarten Fahrzeuge (Geschwindigkeit, Fahrverhalten) und smarten Homes (Kameraaufzeichnungen, Stromverbrauch, Steuerbefehle).

Was noch fehlte, war die Sprache. Nur auf den ersten Blick sind Alexa, Siri und Cortana lediglich eine Sprachsteuerung. Denn die Internet- und KI-basierten Sprachdienste funktionieren nur, wenn sie viel über uns wissen – unseren Geschmack, unsere Gewohnheiten und unseren Haushalt kennen. Und hemmungsbefreit beginnen wir, ihnen bereitwillig so viel wie möglich mitzuteilen: welche Musik wir präferieren, über welche Steckdose die Kaffeemaschine angeschaltet werden kann und wann wir das Haus verlassen oder betreten. Wir machen unsere Stimme, unsere Wünsche, unseren Tagesablauf, unsere Vorlieben, unseren Geschmack und sogar die Stimmen unserer Gäste zugänglich – weil wir möchten, dass Alexa & Co. verstehen, was wir wollen: Dass der Morgenkaffee fertig ist, wenn Alexa uns weckt und die Wohnung beleuchtet ist, wenn wir nach Hause kommen.

Und wenn sie das erste Mal das Badezimmer vorheizt, bevor wir selbst wissen, dass wir gleich ein Bad nehmen wollen, werden wir sie wirklich lieben.

Inhalt

secorvo
security consulting

Security News

Netflix schnorren mit Gmail

Ein schönes Beispiel, wie durch die Kombination zweier unabhängiger Internet-Dienste eine neue Angriffsmöglichkeit entsteht, beschreibt James Fischer in seinem Blogeintrag vom 07.04.2018: Warum Punkte in E-Mail-Adressen wichtig sind ("dots do matter"). Hintergrund ist, dass Googles Gmail-Dienst die Punkte in E-Mail-Adressen nicht auswertet – james.hfisher@gmail.com wird also genauso behandelt wie jameshfisher@gmail.com. Eine Ergonomiefunktion.

Dies kann bei der Netflix-Registrierung ausgenutzt werden. Durch einen Rateangriff lässt sich feststellen, ob für eine Gmail-Adresse bereits ein Konto existiert. Da Netflix die Punkte in der E-Mail-Adresse auswertet, kann ein zweiter Netflix-Account zu einem existierenden angelegt werden, indem bei der E-Mail-Adresse die Punkte verwendet respektive weggelassen werden. Die E-Mail-Adresse wird nicht überprüft, eine weitere Ergonomiefunktion: Warum auch, schließlich ist die Nutzung für vier Wochen kostenfrei. Die E-Mail-Adresse wird nur zur Benachrichtigung z. B. über neue Serien verwendet.

Was passiert aber, wenn man für das künstlich geschaffene Zweitkonto eine Kreditkarte mit sehr kurzer Laufzeit hinterlegt? Dann wird jameshfisher@gmail.com benachrichtigt, seine Kreditkartendaten zu aktualisieren. Die Nachricht geht, Google-intern, an james.hfisher@gmail.com. Kommt von Netflix, ist original Netflix. Wenn James Fisher dann die Daten aktualisiert, bestehen auf einmal zwei Netflix-Konten – dass doppelt abgebucht wird, fällt frühestens bei der nächsten Abrechnung auf.

Stutzig wurde James Fischer nur, weil die zu aktualisierenden Kreditkartendaten überhaupt nicht zu seiner echten Kartennummer passten. Unser Tipp, wie im Straßenverkehr: Augen auf – und mit dem Fehlverhalten anderer rechnen. Auch wenn im konkreten Fall keine der Parteien wirklich etwas falsch gemacht hat, gehen Sie einfach nicht davon aus, dass sich ein Internet-Dienst so verhält, wie Sie das erwarten.

Efail – HTMLfail?

Als am 13.05.2018 die Entdecker der Efail-Angriffe und die EFF die ersten Hinweise und Warnungen veröffentlichten, war die Rede von Schwachstellen in der PGP- und S/MIME-Verschlüsselung. Wenn man jedoch auf die Website schaut, die ein Forschungsergebnis – ebenso wie ein mehr oder weniger eingängiges Logo – in der heutigen Aufmerksamkeitsökonomie offenbar braucht, dann sieht man schnell den eigentlichen Schuldigen an der Misere: HTML.

Was anfänglich eine Möglichkeit war, die ursprünglich spartanischen reinen Text-E-Mails ansprechender zu formatieren, zieht einen Rattenschwanz an Missbrauchsmöglichkeiten nach sich. Angefangen mit Aufrufen externer URLs, die Efail nutzt, um entschlüsselte E-Mail-Inhalte zu exfiltrieren, könnte das bis zur Echtzeit-Übertragung von Bildschirm-Inhalten oder Kamera-Bildern gehen, falls denn die HTML-„formatierten" Inhalte über einen WebRTC-fähigen Browser gerendert werden.

Mit PDF/A wurde eine Teilmenge von PDF standardisiert, die keine externen Referenzen oder aktiven Inhalte erlaubt und zur Darstellung der meisten üblichen Dokumente völlig ausreicht. Es wird Zeit, über ein vergleichbares statisches HTML/A-Format nachzudenken, das es ermöglicht, bspw. E-Mails wesentlich gefahrloser aufzuhübschen, als über unbeschränktes HTML mit allen zwischenzeitlich definierten Erweiterungen inklusive JavaScript. Auch oder gerade, wenn damit ein Tracking von Mail-Empfängern über Web-Bugs o. ä. ebenfalls nicht mehr möglich wäre.

Facebook-Nachlese

In seiner Anhörung vor dem US-Repräsentantenhaus hat Mark Zuckerberg, CEO von Facebook, am 11.04.2018 die weltweite Anwendung der im neuen europäischen Datenschutzrecht vorgesehenen Kontrollen angekündigt. Falls das kein Lippenbekenntnis bleibt, könnte dies ein wichtiger Schritt zu einer amerikanisch-europäischen Annäherung beim Datenschutzverständnis sein. Immerhin: Anders, als sein Statement aus dem Jahr 2010 vermuten lässt, Privatheit sei nicht länger eine „social norm", ist Zuckerberg zumindest um seine eigene Privatsphäre sehr besorgt: Im Jahr 2013 kaufte er die vier an sein Haus angrenzenden Grundstücke in Palo Alto – für 30 Mio. US$.

Während sich die Facebook-Aktie nach dem 18% Einbruch vom 17.03.2018 inzwischen wieder erholt hat, hat die Aufregung um die Nutzung der Daten von 87 Mio. Facebook-Nutzern für den britischen Datenanalysedienstleister Cambridge Analytica nun handfeste Konsequenzen: Am 02.05.2018 musste das Unternehmen Insolvenz anmelden. Offensichtlich gibt es eine große Diskrepanz zwischen den Erwartungen der Nutzer an den Umgang mit ihren Daten – und der tatsächlichen Rechtslage in Teilen der Welt.

Hoteltüren-Crack

Am 25.04.2018 veröffentlichten Tomi Tuominen und Timo Hirvonen, Mitarbeiter des finnischen Sicherheitsunternehmens F-Secure, dass es ihnen bereits 2017 gelungen ist, durch die Kombination mehrerer kleiner Schwachstellen den Master-Key für das Türschließsystem von Assa Abloy aus einer einzigen Schlüsselkarte abzuleiten. Inzwischen hat der schwedische Hersteller ein Update für das in mehr als 42.000 Hotels weltweit eingesetzte Schließsystem bereitgestellt – das allerdings manuell in jedes einzelne Schloss eingespielt werden muss.

Der Angriff ist ein Beispiel für die latente Gefahr, die in allen digitalen Zutrittssystemen lauert: Jede entdeckte Schwachstelle, die den Zutrittsschutz aushebelt, skaliert sofort, da sie alle bereits installierten Einheiten betrifft. Und da die Installation von Updates – anders als bei PCs oder Smartphones – weder üblich ist noch automatisiert erfolgt, ist eine erfolgreiche Ausnutzung einer solchen Lücke sogar sehr wahrscheinlich.

APT-Simulation

Am 30.04.2018 erweiterte MITRE sein vor ziemlich genau einem Jahr veröffentlichtes ATT&CK-Framework über auftretende Angriffsklassen, -typen und -techniken von 188 auf 219 Angriffstypen, verständlich gruppiert in einer technischen Angriffs-Matrix. Nicht erst seitdem fragen sich viele CISOs, ob ihr Netzwerk nicht bereits Opfer eines Advanced Persistent Threat-Angriffs geworden ist.

Mit dem APT Simulator von Florian Roth, der seit dem 09.04.2018 in einer stabilen Version 0.80 verfügbar ist, kann das eigene Red Team die Erkennung von APT-Angriffen trainieren: Damit lassen sich Windows-Enterprise-Clients per *.bat-Script mit derzeit bis zu 25 Testfällen aus den Bereichen Antivirus, Network Intrusion Detection, Endpoint Detection, Security Monitoring und Compromise konfrontieren – und jede zweite Kalenderwoche einen vermeintlichen Incident simulieren. Noch vielversprechender ist die Möglichkeit, auch eigene Testfälle zu ergänzen.

Simple DSGVO-Compliance

Für alle, bei denen Weihnachten jedes Jahr ganz überraschend kommt und der Datenschutz erst seit der DSGVO (General Data Protection Regulation, GDPR) ein Thema ist, gibt es eigenwillige Angebote wie https://gdpr-shield.io.

Falls die Seite wegen Überlastung nicht erreichbar sein sollte, kann man dem Suchmaschinen-Cache die Zielsetzung entnehmen: „Making your website GDPR compliant can take thousands in legal fees ...“. Die Idee des Angebotes: Man sperre EU-Besucher von den eigenen Webseiten aus – was wäre auch einfacher? Geo-IP-Filterung als Compliance-Maßnahme...

Secorvo News

ISO-zertifiziertes ISMS

Anfang 2017 hat das Kirchliche Rechenzentrum Südwestdeutschland (KRZ-SWD), einer der führenden IT-Dienstleister für Kirche, Diakonie und Caritas begonnen, sich mit dem Information Security Management System ISMS ready2go von Secorvo auf eine ISO 27001-Zertifizierung vorzubereiten.

Mit dem Auditbericht vom 02.05.2018 wurde dem Rechenzentrum nun nach wenig mehr als einem Jahr Vorbereitung die Erfüllung der Anforderungen der ISO 27001 bestätigt – ohne eine einzige Abweichung: der „Proof of Concept“, dass ein ISMS „out of the box“ den Weg zum Zertifikat erheblich beschleunigen kann. Wir gratulieren herzlich und bedanken uns für die hervorragende Zusammenarbeit!

Secorvo Seminare

Vor der Sommerpause bieten wir Ihnen noch einmal die Möglichkeit, sich Ihre Kenntnisse und Erfahrungen in der IT-Sicherheit mit einem T.I.S.P.-Zertifikat bestätigen zu lassen: Das T.I.S.P.-Seminar findet statt vom **11. bis 15.06.2018**. Wir freuen uns auf Ihre Anmeldung.

10. Tag der IT-Sicherheit

Auf dem diesjährigen zehnten Karlsruher „Tag der IT-Sicherheit“, einer Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe und dem CyberForum e. V., werden aktuelle Herausforderungen der IT-Sicherheit für Unternehmen diskutiert und Präventionsmöglichkeiten vorgestellt. Als Keynote-Speaker konnten wir in diesem Jahr Stefan Krebs gewinnen, den CIO Baden-Württemberg, Beauftragter der Landesregierung für Informationstechnologie. Er verfügt über vieljährige Erfahrung im IT-Sicherheitsbereich, im Bankensektor und der Verwaltung.

Die Veranstaltung findet am **07.06.2018** im Saal Baden der IHK Karlsruhe statt. Das Programm sowie die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite www.tag-der-it-sicherheit.de.

Veranstaltungshinweise

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

Juni 2018	
07.06.	10. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
11.-12.06.	DuD 2018 (COMPUTAS, Berlin)
11.-15.06.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
13.-14.06.	Annual Privacy Forum 2018 (ENISA, EC DG Connecct, Universität Wien, Barcelona/ES)
15.-16.06.	AREA41 Security Conference (DC4131 DEFCON Switzerland, Zürich/CH)
17.-21.06.	OWASP AppSec EU 2018 (OWASP Foundation, Tel Aviv/ISR)
20.-22.06.	Entwicklertag 2018 (VKSI, GI, ObjektForum, Karlsruhe)
26.-27.06.	EssoS 2018 (EssoS Organization, Paris/FR)
Juli 2018	
24.-27.07.	PETS 2018 (University of Minnesota, Barcelona/ES)

Fundsache

Unter dem Titel „Human Rights under Surveillance“ veröffentlichte Amnesty International einen spannenden und betroffen machenden Bericht über IT-Angriffe auf Menschenrechts-Aktivisten in Pakistan. Langfristig geplante Attacken, unter anderem über Spearfishing-E-Mails und gefakte Social-Media Seiten sowie gefakte Personen, werden im Detail beschrieben. Lesenswert.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Hans-Joachim Knobloch, 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