SWITCH-CERT Report zu aktuellen Trends im Bereich IT-Security und Privacy

Juli / August 2018

SWITCH

I. Eigentor und grobes Foul: Android-App der spanischen Fussball-Liga macht 10 Millionen Nutzer unfreiwillig zu Spionen

Ein Foul der ganz groben Art hat sich die spanische Fussball-Liga «La Liga» geleistet: Die offizielle App des Fussballverbandes aktiviert während Live-Übertragungen von Fussballspielen Mikrofon und GPS-Modul, um herauszufinden, ob im Umfeld des jeweiligen Smartphones eine öffentliche Übertragung der Spiele stattfindet. Für eine solche brauchen z.B. Gaststätten, Tankstellen oder Campingplätze eine spezielle Pay-TV-Lizenz der Liga. Zeigen sie ein Spiel, ohne die Lizenz gekauft zu haben, geht die Liga gegen sie vor. Sie begründet das mit Schäden von bis zu 150 Millionen Euro durch entgangene Lizenzgebühren. Dennoch muss die Spionage im Dienste des Geschäfts der Liga ohne Wissen der Nutzerinnen und Nutzer der App als grobes Foul gewertet werden, das nicht durch einen Schiedsrichter, sondern durch die neue Datenschutzgrundverordnung DSGVO aufgedeckt wurde.

Vor deren Inkrafttreten war in seitenlangen Nutzungsbedingungen der Hinweis untergebracht, dass die App das Mikrofon zu «Pubikumsanalysen» nutze. Nun weist die aktuelle, DSGVO-konforme und deutlich knappere Datenschutzerklärung explizit drauf hin, dass die App nach unlizenzierten Übertragungen der Liga-Spiele fahnde – Eigentor!

© SWITCH 2018

Dass der spanische Fussballverband mit seiner neugierig-mitteilsamen App nicht alleine in der Sportwelt dasteht, belegt z.B. auch Eurosport. Die App des Senders nimmt im Hintergrund Kontakt zu zahlreichen Servern auf und sendet den Standort des Android-Mobilgeräts an 18 verschiedene Empfänger. Auch im Security Report hatten wir über das Thema der Spionage via Mikrofon in vernetzten Geräten mit GPS-Modul immer wieder berichtet (u.a. in der letzten Ausgabe). Und das Open Web Application Security Project OWASP führt solche Spionageattacken auf seiner Liste von mehr als 60 Schwachstellen (Vulnerabilities)

Wer die Exponierung seiner Daten verhindern möchte, dem bleibt nur die Möglichkeit, Kamera, Mikrofon und Ortungsdienste zumindest bei Nichtgebrauch in den Systemeinstellungen zu deaktivieren oder der Spionage verdächtigte bzw. überführte Apps vom Gerät zu entfernen.

Nachzulesen unter:

https://www.heise.de/newsticker/meldung/Spanien-App-der-Fussball-Liga-sucht-uebers-Mikro-unlizenzierte-Uebertragungen-4075636.html

https://www.blick.ch/news/ausland/handy-mik-sucht-nach-illegalen-uebertragungen-spanische-liga-spioniert-fussball-fans-aus-id8483984.html

https://www.golem.de/news/dsgvo-la-liga-app-ueberwacht-umfeld-per-mikrofon-1806-134887.html

https://www.owasp.org/index.php/Category:Vulnerability

II. Amazon Rekognition – Nützliches Sicherheits- und Convenience-Tool oder totale Überwachung zum Discountpreis?

Für die einen ist Gesichtserkennung ein wichtiges und nützliches Instrument, um z.B. Identifikation und Zugangslegitimation zu vereinfachen, Sicherheitsbedarfe besser zu bedienen und Straftäter effektiver ausfindig zu machen. Für die anderen läutet sie das Ende des Rechts auf informationelle Selbstbestimmung ein und führt schnurstracks in den totalen Überwachungsstaat. Weil Amazon Rekognition weit mehr kann als «nur» Gesichter erkennen, verwundert es nicht, dass die Meinungen darüber weit auseinander gehen.

Denn Amazon Rekognition erkennt nicht nur Gesichter, sondern kann nach eigenen Angaben «Tausende von Objekten (z.B. Fahrrad, Telefon, Gebäude) und Szenen (z.B. Parkplatz, Strand, Stadt) identifizieren, inklusive Aktivitäten in Frames, wie etwa das Betanken eines Fahrzeugs oder die Zustellung eines Pakets».

© SWITCH 2018

Es ist ein KI-Programm, das auf Deep-Learning-Technologien basiert, die dafür entwickelt wurden, Milliarden von Bildern und Videos täglich zu analysieren. Amazon wirbt dafür mit dem Slogan «Ein Gesicht unter Millionen wiedererkennen».

Wie umfassend die Software Erkennung in allen Lebensbereichen und für zahlreiche Einsatzzwecke verwendet werden kann, ist auf Amazons aws-Website nachzulesen. Für Bürgerrechtsorganisationen gleicht denn auch die Anleitung zum Gebrauch der Software einer «Gebrauchsanweisung für autoritäre Überwachung». Was den Verdacht naheläge, so die Amazon-Kritiker, dass Rekognition förmlich auf «den Missbrauch durch die Regierung» hin konzipiert sei.

Wer wenigstens im Social Web unerkannt bleiben und Gesichtserkennung und bildbasierte Suche blockieren will, sollte den unten zitierten Artikel auf mimikama.at lesen. Dort ist beschrieben, wie kanadische Forscher der Universität Toronto künstliche Intelligenz in zwei sich bekämpfenden neuronalen Netzen einsetzen: das eine verfeinert ständig seine Fähigkeiten zur Gesichtserkennung; das andere will genau die verhindern. Als Ergebnis dieser Art von KI-Wettrüsten ist ein kaum wahrnehmbarer Filter entstanden, der sich über die Bilder legt und dadurch nicht nur die Gesichtserkennung deaktiviert, sondern auch automatische Bildsuchprozesse blockiert.

Nachzulesen unter:

https://www.nzz.ch/digital/das-gesicht-ist-das-ticket-ld.1410493

https://www.welt.de/regionales/bayern/article177883974/Gesichtserkennung-Muenchner-Polizei-setzt-jetzt-Super-Recogniser-ein.html

http://www.spiegel.de/netzwelt/netzpolitik/singapur-will-gesichtserkennung-testen-kameras-an-strassenlaternen-a-1202769.html

https://aws.amazon.com/de/rekognition

https://meedia.de/2018/04/26/datenschuetzer-caspar-die-technik-der-gesichtserkennung-birgt-unabsehbare-risiken-fuer-die-gesellschaft

https://www.tagesschau.de/ausland/amazon-gesichtserkennung-rekognition-101.html

https://eu.usatoday.com/story/tech/2018/07/09/orlando-police-decide-keep-testing-amazon-facial-recognition-program/768507002

https://www.mimikama.at/allgemein/filter-schuetzt-user

© SWITCH 2018

III. Unterschätzte Gefahr: Malware-Angriffe auf Smartphones und Tablets mit gigantischen Wachstumsraten

54 Prozent plus von 2016 auf 2017, 240 Prozent plus seit 2014 – von solchen Zahlen können Wirtschaftslenker nur träumen. Vielen Smartphone- und Tabletbesitzern bereiten sie dagegen Alpträume. Denn das 54-Prozent-Wachstum beschreibt die Entwicklung der Malware Varianten für Mobilgeräte. Die 240 Prozent zeigen die steile Aufwärtskurve der Zahl der Angriffe auf Smartphones und Tablets. Die meisten davon sind für Hacker leichte Beute. Denn anders als Lap- und Desktop-Computer sind viele Android- als auch IOS-Geräte nur mangelhaft gegen Angriffe geschützt. Mobile-Security-Experten fanden heraus, dass täglich ca. 24.000 bösartige Apps auf ihrem Weg auf Smartphones und Tablets blockiert werden – 1.000 pro Stunde! Alleine 2017 wurden über 27.000 (!) neue Varianten von Schadsoftware für Mobile Devices registriert. Und auch wenn viel mehr davon für Android-Geräte entwickelt wurden – iPhones sind gleichermassen beliebte Angriffsziele. Und je mehr Funktionen Nutzer ihrem Gerät anvertrauen, desto lohnenswerter wird für Hacker der Angriff darauf. Denn Mobile ist der Schlüssel zum Leben der Nutzer, ihrer Freunde und allen Menschen und Institutionen, mit deren Netzen sich das Gerät verbindet: Persönliche Daten, Zugang zum e-Banking, zur Steuerung smarter Umgebungen vom Auto übers Haus bis zum Arbeitsplatz und private wie auch unternehmerische Netzwerke werden ausspioniert, abgefischt bzw. für teilweise spektakuläre Einbrüche oder Diebstähle sowie zur Industriespionage und -sabotage genutzt.

Im unten zitierten Artikel werden 6 Hauptgruppen mobiler Malware unterschieden. Zudem wird dargestellt, wie diese Malware auf die Geräte kommt. Zum Schutz der eigenen Geräte sollten Nutzer die nachstehenden Regeln beachten:

- Apps nur aus den offiziellen Stores der Anbieter herunterladen
- Sofort nach dem Laden prüfen, welche Rechte sich die App einräumt. Vorsicht ist geboten, wenn der angeforderte Zugang in keinem erkennbaren Zusammenhang mit der Funktion der App besteht (etwa, wenn eine App zur Aufzeichnung des eigenen Körpergewichts Zugriff auf Kamera und Ortungsdienste oder gar auf das Adressbuch verlangt).
- Betriebssystem und Browser immer auf dem neuesten Stand halten

© SWITCH 2018

- WLAN-Angebote unbekannter Betreiber meiden und stattdessen die offiziellen Hotspots der Provider oder seriöse Angebote von Hotels und anderen Anbietern nutzen.
- Ein Virtual Private Network (VPN) einrichten, um den eigenen Netzverkehr zu verschlüsseln.

Nachzulesen unter:

https://www.heise.de/security/solutions/telekom/malware-angriffe-auf-smartphones-die-unterschaetzte-gefahr/?source=nat_teas

IV. Phishing with the Proms: Betrüger nutzen Promiwahn und Krypto-Gier zum Schaden der User

Werbung mit prominenten Persönlichkeiten funktioniert 2018 so gut wie nie zuvor. Tennisasse, Fussballgötter, Musik-, Internet- und Börsenstars verdienen Millionen, weil Menschen gerne so wären wie sie und deshalb die Produkte kaufen, für die ihre Idole werben. Da war es eigentlich nur eine Frage der Zeit, bis Cyberkriminelle die Idee aufgriffen und ihrerseits mit Promibonus phishen gingen. So ist seit kurzem auf bluewin.ch nachzulesen, mit welcher Raffinesse Betrüger auf Twitter unter der Vorgabe, Elon Musk zu sein, arglosen Nutzern Kryptowährungen aus dem Account zogen. Mit leicht abgeändertem Accountnamen (elohnmusk) schalteten sie sich in ein Twittergespräch des echten Tesla-Gründers ein. Nach ein, zwei täuschend echt wirkenden Fake- oder Mal-Tweets verkündeten sie, dass sie in einer spontanen Marketingaktion Ethereums und Bitcoins verschenken würden, wenn die User einem Link folgen und einen kleinen «Verifizierungsbeitrag» in Kryptowährung zahlen würden.

Die Opfer solcher kriminellen Machenschaften finden sich sowohl auf Seiten der Nutzer als auch auf der der Promis, weil deren Vertrauenswürdigkeit durch den Betrug massiv untergraben wird.

Nachzulesen unter:

https://www.bluewin.ch/de/digital/betrueger-phishen-ueber-elon-musks-twitter-account-nach-bitcoins-124106.html

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis und Michael Fuchs verfasst.

Der Security Report spiegelt nicht die Meinung von SWITCH wider, sondern ist eine Zusammenstellung verschiedener Berichterstattungen in den Medien. SWITCH übernimmt keinerlei Gewähr für die im Security Report dargelegten Inhalte, Meinungen oder deren Richtigkeit.

© SWITCH 2018