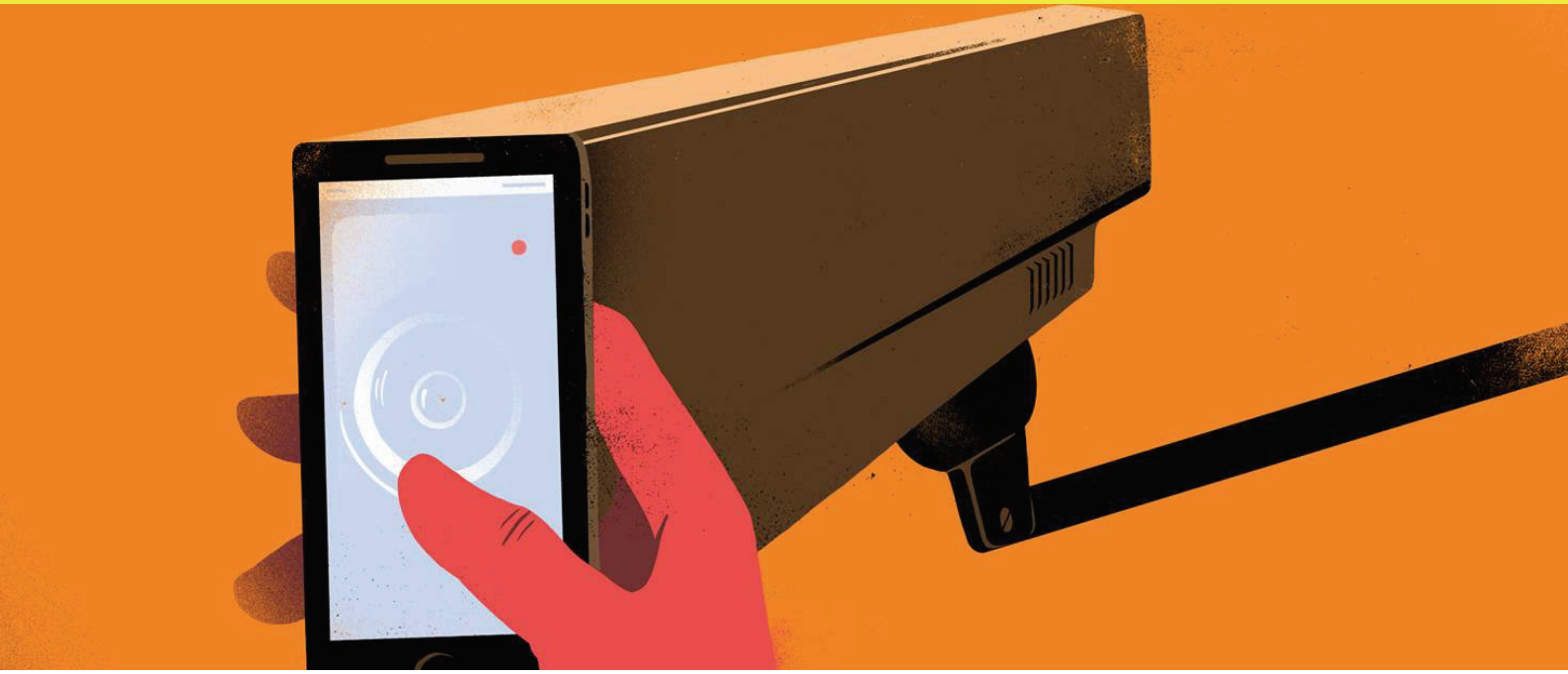
AMNESTY
INTERNATIONAL



https://www.amnesty.org/en/latest/news/2020/01/digital-surveillance-threats-for-2020/

# GEFAHREN DIGITALER ÜBERWACHUNG IM JAHR 2020

15. Januar 2020, 12:43 UTC

Die Palette und Reichweite von Bedrohungen für Menschenrechtsverteidiger durch Übergriffe vonseiten hochentwickelter Spionagesoftware bis hin zu massenhaftem Datendiebstahl via Smartphone und durch den Aufstieg von Gesichtserkennungstechnologie nimmt stetig zu.

Für die Sicherheitsteams, die sich mühen, den Schutz für die Aktivisten aufrechtzuerhalten, ist es ein Katz-und-Maus-Spiel, weil sich die Angreifer sehr schnell an Entwicklungen von Schutzmechanismen anzupassen wissen.

*„Wenn digital agierende Angreifer mitbekommen, dass die Nutzer etwa verstärkt zu Signal (einer Messaging App) überwandern, dann versuchen sie Signal zu attackieren. Werden verstärkt VPN-Technologien eingesetzt, beginnt man, diese zu blockieren. Verwenden Nutzer immer öfter den Tor-Browser, dann werden die Angriffe auf den Tor-Verkehr gerichtet,"* sagt Ramy Raoof, Experte für taktische Technologie bei Amnesty Tech.

Ramy Raoof zufolge wird es einer der Hauptschwerpunkte für Amnesty Tech im Jahr 2020 sein, gegen die maßgeschneiderten Übergriffe auf Smartphones vorzugehen, die 2019 in die Schlagzeilen gelangten. Im Oktober 2019 Jahr strengte die zu Facebook gehörende Messaging App *WhatsApp* wegen Spionageangriffen auf über Tausend ihrer Nutzer ein Gerichtsverfahren gegen die Überwachungsfirma NSO Gruppe an, das von großem öffentlichem Interesse begleitet war.

Deren schädliche digitale Übergriffe werden auch diese Woche wieder im Rampenlicht stehen, wenn ein von Amnesty International und anderen Menschenrechtsgruppen angeregtes Gerichtsverfahren in Tel Aviv zur Verhandlung kommt. Die Aktivisten wollen das israelische Verteidigungsministerium dazu zwingen, der NSO Gruppe, deren Produkte weltweit für Übergriffe auf Aktivisten benutzt werden, die Exportlizenz zu entziehen.

Wie der Amnesty Tech Sicherheitsexperte Etienne Maynier erklärte, ist es bei fortgeschritten Überwachungstechnologien heute nicht mehr nötig, dass Betroffene auf einen Link klicken, um ihr Gerät zu infizieren. Bei einem Übergriff mit der NSO-Spionagesoftware auf einen Aktivisten in Marokko wurden die Aktivitäten seines

Internetbrowser verdeckt umgeleitet, um sein Telefon mit Spionagesoftware zu infizieren. *„Man wartet nicht mehr darauf, dass jemand einen Link anklickt, sondern hackt sich stattdessen in den Internetverkehr seines Browsers ein und leitet diesen auf eine Schadwebseite um, die dann heimlich versucht, die Spionagesoftware zu installieren,“* so Etienne Maynier.

Es kommt immer häufiger vor, dass auch gut geschützte Telefone erfolgreich attackiert werden, während die Sicherheitsteams durch eine aufstrebende Industrie unter zusätzlichem Druck stehen, die sich sogenannter Zero-Day-Exploits bedient. Dabei versuchen skrupellose Hacker, unbekannte Sicherheitslücken zu finden, um ihr Wissen zu verkaufen. Da diese Sicherheitslücken nicht gemeldet werden, bleibt den Softwareentwicklern keine Zeit, die Lücke zu schließen. Daher der Name Zero Day.

Im Mai 2019 nutzte die NSO-Gruppe eine bis dahin unbekannte Sicherheitslücke in WhatsApp, um mehr 100 Menschenrechtsaktivisten auf der ganzen Welt mit Spionagesoftware zu infizieren.

# DATENKLAU

Amnesty Tech versucht auch solche Cyberattacken in den Griff zu bekommen, die zwar mit weniger hoch entwickelter Technik arbeiten, die aber dennoch äußerst wirksam sind und innerhalb von Minuten eine große Anzahl von Nutzern treffen können.

Der massenhafte Datenklau (Phishing) via SMS oder über Anwendungssoftware (Apps) auf Smartphones ist eine dieser Methoden, die wenig kosten und allzu oft zum Erfolg führen.

Beim Phishing wird versucht, Menschen zur Herausgabe persönlicher Informationen wie Passwörter zu bewegen. Die Angriffe finden oft in Form einer Aufforderung zum Zurücksetzen eines Passworts auf einer Seite statt, die der des Telefonanbieters oder eines Dienstes in den sozialen Medien zum Verwechseln ähnlich sieht. Es kommt auch vor, dass Angreifer als Freunde oder Kontakte der Opfer auftreten und mit diesen einen Link teilen wollen, in den bereits ein Schadcode eingebettet ist.

Etienne Maynier fügt hinzu, dass Angreifer wie diese häufig eine Art "soziale Manipulation" einsetzen und Nutzer drängen, einen Link anzuklicken oder ein Dokument zu öffnen, indem sie zum Beispiel als Vertreter einer vertrauten Organisation auftreten und vorgeben mit den Betroffenen zusammenarbeiten zu wollen.

*„Eine äußerst kostengünstige und sehr effiziente Methode, die sich zudem auch noch sehr leicht ausweiten lässt,“* sagt Ramy Raoof, der voraussagt, dass die im Jahr 2020 kommende Phishing-Welle für Menschenrechtsverteidiger weltweit eine Bedrohung sein wird, weil sie immer mehr von ihren Mobiltelefonen abhängen.

# WEGE ZUR ABSICHERUNG DER KOMMUNIKATION

*Hier sind daher einige einfache Tipps vom Amnesty Tech Experten für taktische Technologie Ramy Raoof.*

### *Grundlagen für das Telefonieren mit iPhone- oder Android-Systemen*

Um zu verhindern, dass gegen Ihren Willen Zugriff auf Ihre persönliche Daten genommen wird und um die Gefahr von Angriffen möglichst gering zu halten, sollten Sie nur Apps von offiziellen App-Stores herunterladen. Aktualisieren Sie Ihr System und Ihre Apps regelmäßig, um sicherzustellen, dass die letzten Sicherheitsupdates installiert sind. Aktivieren Sie "Kontowiederherstellung (Account Recovery)", für den Fall, dass der Zugangscode für Ihr Telefon verloren geht. Und schließlich sollte man durch ein Passwort, das sich nicht leicht erraten lässt (z.B. eine achtstellige Zahl, ein alphanumerischer Code) eine mobile Bildschirmsperre einrichten.

### *Vom Umgang mit Passwörtern*

Durch die Verwendung eines Passwort-Managers, muss man sich keine Sorgen über vergessene Passwörter mehr machen und kann vermeiden, immer dieselben Passwörter zu verwenden. Der Passwort-Manager ist ein Werkzeug, das sicher abgespeicherte und starke Passwörter erstellt, so dass auf verschiedenen Webseiten und für die vielen unterschiedlichen Dienste zahlreiche und immer wieder andere Passwörter eingesetzt werden können. Aktuell verfügbare Passwort-Manager wären z.B. KeePassXC, 1Password oder Lastpass. Allerdings sollte man nie vergessen, ein Backup der Datenbank des gewählten Passwort-Managers einzurichten.

### *Messenger Apps*

Wenn wir Menschenrechtsverteidiger zu Messenger Apps beraten, dann beurteilen wir jede App anhand ihrer Firmenpolitik (wie Nutzungsbedingungen, Datenschutzvereinbarungen etc.), ihrer Technologie (Handelt es sich um ein Open-Source-System? Sind Überarbeitungen möglich? Wurde die App getestet? Wie sieht es mit der Sicherheit aus?), und schließlich anhand der Ausgangssituation (Stellt die App wirklich die Eigenschaften und Funktionen bereit, die dem Bedarf und dem Bedrohungspotential des Gerätes entsprechen?). So stellten wir fest, dass die beiden Messenger-Apps Signal und Wire über insgesamt starke Datenschutz-Eigenschaften verfügen. **ANMERKUNG:** Signal verlangt für die Registrierung eine SIM-Karte, bei Wire kann man sich mit einem Benutzernamen/einer Email-Adresse registrieren.

### *Die Nutzung öffentlicher Wi-Fi-Schnittstellen und VPNs*

Verbindungen zu Wi-Fi-Hotspots in Cafés oder Flughäfen werden über ein Netzwerk ins Internet geleitet. Wenn in diesem Netzwerk Angreifer lauern, können diese Ihre persönlichen Daten abgreifen. Durch die Nutzung einer VPN-App auf Ihrem Gerät, können Sie Ihre Online-Aktivitäten bei der Nutzung öffentlicher Verbindungen schützen und vor den Augen anderer Teilnehmer, die im Netzwerk unterwegs sind, verbergen. Potentiell empfehlenswerte VPN-Apps sind z.B. NordVPN und TunnelBear.