TikTok, Wechat & Co: Wie kommt die Spyware ins Smartphone?

Freitag, 21.08.2020, 15:52

TikTok, WeChat und tausende weitere Apps aus China sehen harmlos aus, sind aber in Wirklichkeit Schadsoftware. Sie verschleiern geschickt ihre Herkunft. Wie kann ich mich davor schützen?

Die Vorwürfe gegen die chinesische App TikTok sowie gegen unzählige weitere chinesische Apps wiegen schwer: Die Programme sollen eine Fülle von Informationen über ihre Nutzer abschöpfen. Das sind Daten, die nichts mit der eigentlichen Funktion der App zu tun haben und für deren Erfassung es keinerlei vernünftige Begründung gibt.

"Bei TikTok und den anderen Malware-Apps ist die App nicht unschuldig und wird kompromittiert", sagt IT-Sicherheitsexperte Stefan Strobel, "sondern der Entwickler der App hat von vornherein Hintertüren, Spionagefunktionen und andere Dinge in seine App eingebaut und sich auch noch Mühe gegeben, dass das keiner bemerkt."

Der Gründer und CEO des IT-Sicherheitsunternehmens CIROSEC berät deutsche mittelständische Unternehmen in Sachen IT-Sicherheit. Einige von ihnen sind selbst in China tätig. Und so hat Strobel einschlägige Erfahrungen mit chinesischen Apps gesammelt. Die populären chinesischen Apps TikTok und WeChat bilden aus seiner Sicht nur die Spitze des Eisberges.

WeChat ist eine universal-App, die Messaging mit Bezahlfunktionen und weiteren Social-Media-Anwendungen verknüpft. Sie ist in China sehr populär und unter IT-Experten gibt es kaum Zweifel, dass alle Daten, die darüber fließen, durch das chinesische Regime nahezu komplett erfasst werden.

Warum verschleiert mir die App etwas? Es geht um Tausende oft kostenloser, aber auch um kommerzielle Apps. "Immer wieder merkt man, dass da aus seltsamen Gründen viel investiert wurde, um die Analyse der Apps zu erschweren", sagt IT-Sicherheitsexperte Strobel. "Und wenn man sich dann noch mehr Mühe macht und versucht, diese Schutzfunktionen zu umgehen, damit man überhaupt einmal nachvollziehen kann, wie die App programmiert wurde, dann stellt man fest, dass da jede Menge Daten gesammelt werden, nach China geschickt werden. Daten, die eigentlich gar nicht notwendig sind."

Viele Apps geben sich anfangs unscheinbar und harmlos. Dann ist erst einmal nur eine kleine Hintertür eingebaut. Die kann der Angreifer später nutzen. "Selbst wenn man die App jetzt anschaut, und sie macht nur harmlose Dinge, dann ist der chinesische Hersteller oft in der Lage, zur Laufzeit die Funktionalität zu erweitern," sagt Strobel. "Auf einmal macht die App ganz andere Sachen, ohne dass das irgendwo neu aus dem App-Store geladen wird."

"Ist ja nicht so schlimm, das machen doch alle so" - stimmt nicht!

Das sei keineswegs vergleichbar mit regelmäßigen Live-updates, wie sie etwa westliche Softwareentwickler ihren Kunden anbieten. So dürfe man die Laufzeit-Updates der chinesischen Spionage-Apps nicht mit Updates vergleichen, wie sie etwa von Microsoft Office durchgeführt werden. "Bei MS Office kann ich als Endanwender zustimmen, dass ein Update eingespielt wird", sagt Strobel. "Die chinesischen Apps machen das völlig unbemerkt vom Endanwender, ohne dass er irgendetwas davon merkt, dass da was upgedatet wird – möglicherweise sogar während er mit der App arbeitet."

TikTok ist ein Beispiel dafür, dass die Angreifer sehr geschickt vorgehen. Anfangs als harmlose Spielerei getarnt, wächst der Datenappetit mit der Zeit und dem Erfolg der App. Erst wenn eine große Zahl Anwender damit arbeitet, entsteht eine Sogwirkung. "Und wenn die App einen Coolheits-Status erreicht und viral wird, und die Leute sagen: 'Hey, das muss man haben!', dann kann der Hersteller irgendwann die Rechte erweitern

und dann muss derjenige, der es installiert, noch mehr zustimmen," beschreibt der IT-Experte die Strategie der Angreifer.

Auf diese Weise wächst die Liste der Berechtigungen, die der Nutzer der App einräumt. Viele Nutzer verstehen auch nicht, was die App alles von ihnen verlangt. Kommt ein entsprechendes Dialogfenster, stimmen sie einfach zu. Und auf einmal hat die App Zugriff auf die aktuelle Position des Nutzers, kann jederzeit abfragen, wo er sich befindet, hat vielleicht Zugriff auf die Kontakte und den Kalender. Wer die App nutzen will, muss das dann akzeptieren.

Keine Chance bei vorinstallierten Spionage-Apps

Dabei geht es nicht nur um Apps, die man selbst aktiv aus dem App-Store herunterlädt. Oft ist die Schadsoftware schon beim Kauf schon auf dem Smartphone installiert.

"Viele Smartphone-Vertreiber nutzen Software, die von Dritten entwickelt wurde, ohne zu wissen, woher sie eigentlich stammt oder wer es programmiert hat. Dabei wird die Malware zum Teil der Produktionskette, die dadurch sehr schnell verseucht werden kann," sagt Angelos Stavrou.

Er hat mit seiner Firma Kryptowire aus den USA Ende letzten Jahres 146 Fälle von vorinstallierter Schadsoftware gefunden, auf Android Mobiltelefonen von 26 verschiedenen Anbietern – das können etwa Telekommunikationsunternehmen, Elektronikmärkte oder andere sein. Mittlerweile sind hunderte weitere Fälle dazugekommen, sagte Stavrou am Rande der IT-Defense Konferenz 2020 gegenüber der DW.

Sein Kollege Ryan Johnson nennt als Beispiel zwei kleine Programme namens "Lovelyfonts" und "LovelyHighFonts", die 2019 aufgeflogen sind. Sie gaben sich als reine Schriftfonts aus, um die Darstellung auf dem Smartphone Bildschirm ansprechender und verspielter zu gestalten.

In Wirklichkeit starteten beide Programme - vom Nutzer unerkannt - einen Angriff auf das Smartphone, schnürten verschlüsselte Datenpakete und schickten sie unerkannt, wenn das Telefon nicht genutzt wurde, an einen Server in Shanghai.

"Einige dieser von uns entdeckten Programme verschaffen sich Systemprivilegien, die Teil des Betriebssystems sind. Der Nutzer kann sie nicht abschalten. Falls es also eine Schwachstelle in einer solchen App gibt, kann der Nutzer nichts dagegen tun," sagt Johnson

Zersplitterte Software-Entwicklung als Risikofaktor

Android ist etwas anfälliger für solche bösartige Software als das Apple Betriebssystem IOS. Das hat damit zu tun, dass bei Apple die Entwicklung der Smartphones und der App-Store mit der Software in nur einer Hand sind. Deshalb kann Apple auch schneller reagieren und Schadsoftware entfernen, wenn sie entdeckt wird.

Bei Android dauert das meist länger. Dort gibt es das Android Open Source Project (ASOP), wo di e vielfältigen Software Entwickler ihre Produkte anbieten können. Wer ein Smartphone auf den Markt bringt, bedient sich dort und sucht sich die Software-Komponenten zusammen, von denen er glaubt, dass sie dem Kunden gefallen. Und es gibt fast so viele App-Stores wie Telefon-Anbieter. "Jede Sicherheitslücke, die im ASOP enthalten ist, wird von dort an die Smartphone Anbieter weitergegeben," warnt Johnson.

Auch der deutsche IT-Sicherheitsexperte Stefan Strobel sieht in der unübersichtlichen Hersteller-, Entwickler- und Händler-Landschaft ein Sicherheitsrisiko. "Es gibt viele verschiedene Parteien, ein zersplitterter Markt, weil es ganz verschiedene Hardware-Hersteller gibt, die Modifikationen am Betriebssystem durchführen und ihren eigenen Stempel aufdrücken und all das führt dazu, dass es nicht sicherer wird."

Malware bereits in den Werkzeugen für Programmierer versteckt

Dabei ist auch Apple nicht völlig vor derartigen Angriffen geschützt. Ebenfalls aus China stammte etwa 2015 der XcodeGhost. Dabei handelte es sich um eine manipulierte und illegale Kopie des Apple Programmierwerkzeugs XCode. Programmierer brauchen es, um Apps für MacOS oder IOS schreiben zu können.

"Wenn man offiziell das Xcode von Apple bezogen hat und damit entwickelt hat, war alles gut. Wenn man aber ohne zu bezahlen, sich diese Umgebung über graue Kanäle besorgt hat und die Schadcodes automatisch in die App integriert hat, dann hatte man ein Problem," beschreibt Strobel die Strategie der Hacker.

Etwa 4000 Apps hatten Software Entwickler nichts ahnend seinerzeit mit der gehackten Software programmiert und ihre Produkte mit Malware verseucht. Das scheint auf den ersten Blick viel, ist aber relativ wenig, verglichen mit den fast zwei Millionen Apps, die etwa derzeit im App-Store von Apple verfügbar sind. Dennoch muss selbst IT-Sicherheitsexperte Stefan Strobel anerkennen, dass der XCodeGhost echte Profiarbeit war: "Der Trick, über die Entwicklungsumgebung den Schadcode bei der Entwicklung schon in die App einzuschleusen, ist natürlich aus Angreifersicht genial."

Smartphones sind aber immer noch sicherer als PCs

Was kann ich als Nutzer eigentlich tun, um mit meinem Smartphone sicher unterwegs zu sein? Die gute und vielleicht auch überraschende Nachricht: So unsicher wie es scheint, sind Smartphones eigentlich gar nicht.

"Das Grundkonzept der Betriebssysteme von Smartphones – sowohl Android als auch IOS – ist , dass eine App in einer Sandbox, einem Sandkasten abläuft und zunächst nur sehr begrenzte Rechte hat," sagt Sicherheitsfachmann Strobel.

Selbst eine Malware App kann - wenn das Betriebssysteme keine offenen Sicherheitslücken hat – also nicht so einfach auf das zugreifen, was ich in anderen Apps tue – oder gar auf mein Betriebssystem. Insofern sind Smartphones meist sicherer als normale Computer. "Zum Beispiel ist IOS sicherer als das, was ich auf einem normalen Windows10 PC vorfinde. Das beginnt schon damit, dass ich auf einem IOS Smartphone keine administrativen Rechte habe – auch als Anwender nicht –, während ich die auf meinem PC natürlich habe."

Vieles hängt vom Nutzer ab

Wichtig ist allemal, misstrauisch zu sein. Nicht jede Spielerei muss man auch unbedingt auf dem eigenen Smartphone installieren. Man sollte die Berechtigungen der Apps im Blick haben und ihnen nicht alles erlauben. Eine Übersicht, sicherer Apps haben wir hier für Sie zusammengestellt.

Letztlich muss der Kunde entscheiden, ob es angesichts der vielfältigen Hinweise auf chinesische Spionage-Apps und die vorherrschende Intransparenz einiger Hersteller unbedingt ein Smartphone eines chinesischen Herstellers sein muss.

Ansonsten können insbesondere Unternehmen ihre dienstlich ausgegebenen Smartphones gut gegen Angreifer schützen, über das zentrale Management der Unternehmensgeräte – die sogenannte MDM-Funktion. Dort können sie etwa festlegen, dass nur freigegebene Apps installiert werden können. Sie können auch vorgeben, mit welchen Netzen sich die Nutzer verbinden dürfen, wie die Bluetooth-Einstellungen sind und weiteres mehr.

Das macht dann zwar nicht so viel Spaß wie TikTok, aber wenigsten bleiben die Daten da, wo sie hingehören.

Autor: Fabian Schmidt

*Der Beitrag "TikTok, Wechat & Co: Wie kommt die Spyware ins Smartphone?" wird veröffentlicht von Deutsche Welle. Kontakt zum Verantwortlichen hier.

Deutsche Welle

Fotocredits: