Bild: Archiv

Die grössten Chancen, sich einen Virus auf Ihr Smartphone zu holen, haben Sie über die Installation zweifelhafter Apps.

Die mobile Gefahr

Mit unseren Daten lässt sich viel Geld verdienen. Allein das «kostenlose» Facebook erzielt einen Quartalsgewinn von $ 2 Milliarden. Das Handy spielt dabei eine wichtige Rolle. Es ist zu einem ständigen Begleiter geworden.

Egal ob beim Warten auf den Bus, unterwegs oder zu Hause, es ist immer bei uns. Auch den Sport, unseren Puls oder den Schlaf können damit aufgezeichnet werden. Doch wo lauern die Gefahren und was kann dagegen unternommen werden?

Madware

Viele Apps sind kostenlos herunterladbar. Sie locken mit spannenden Beschreibungen und Trailern. Doch nach der Installation zeichnen sie alles auf, was wir machen. Ständig im Hintergrund laufend überwachen sie jede Tätigkeit und schicken es an die Entwickler oder darauf spezialisierte Firmen. Im Minimum bekommen wir auf uns zugeschnittene Werbung. Daher der Name Madware – Mobile Adware, Werbung auf Mobilgeräten. Dabei gehen diese Apps oft sehr aggressiv vor und können sogar ungewollt Einstellungen verändern. Was aber sonst alles mit unseren Daten passiert, bleibt das Geheimnis der jeweiligen Firmen.

Malware

Viren, Würmer und andere Schädlinge haben längstens den Weg auf unsere ständigen Begleiter gefunden. Klar, dass Hacker dieses lukrative Ziel nicht aussen vorlassen und ihre Schädlinge angepasst haben. Es gibt verschiedene Studien, die von 10'000 neuen Android- Schad-Apps pro Tag ausgehen, alle acht Sekunden kommt eine neue dazu. Während Malware (Malicous Software) auf herkömmlichen PCs gemäss Symantec abnimmt, werden die mobilen Geräte regelrecht überschwemmt. Auch Erpressungsviren, sogenannte Ransomware, verbreiten Angst, in dem sie alle Daten verschlüsseln und nur gegen Bezahlung einer gewissen Anzahl Bitcoins diese wieder freigeben.

Drive-by

Diese Art der Infizierung ist nicht neu. Seit Jahren versuchen Hacker seriöse Webseiten so zu manipulieren, dass bereits ein Besuch darauf einen Schädling installiert. Daher der Name Drive-by, beim Vorbeisurfen, ohne einen Klick zu tätigen, wird die unerwünschte Software installiert. Dass nun auch mobile Geräte infiziert werden, war eine Frage der Zeit. Es kursiert momentan das Gerücht, dass beispielsweise iPhones über Jahre so manipuliert wurden. Die Experten streiten nicht ob, sondern wie viele iPhones davon betroffen sind.

Phishing

Auch Phishing ist nichts neues und beschäftigt uns seit vielen Jahren (siehe Maschinenbau 2/2020, Seite 28). Die Qualität dieser Manipulationen haben aber zugenommen. Während früher in schlechtem Deutsch nach dem Passwort gefragt wurde, sind diese heute perfekt auf ein Unternehmen oder eine Person abgestimmt (Spear Phishing). Die Anrede ist korrekt, der Inhalt könnte sein, der Absender ist wirklich der eigene Chef. Solche gefälschten E-Mails zu erkennen wird immer schwieriger.

Schutzmöglichkeiten

- Nutzen Sie einen Pin anstelle des Wischmusters. Damit ist aber nicht 1-2-3-4 gemeint, sondern mindestens acht Stellen sollten es schon sein, am besten alphanummerisch, mit Buchstaben, Zahlen und Sonderzeichen. Was spricht gegen das Wischmuster? Zum ersten kann es einfacher abgeschaut werden als die Pin-Eingabe. Zum anderen hinterlassen wir Talgspuren auf dem Display. So kann es leicht «abgelesen» und wiederholt werden.
- Nutzen Sie die Sicherheitsfunktionen des Handys. Damit sind beispielsweise der Fingerprint, aber auch FaceID gemeint. Klar gibt es für beide Funktionen Anleitungen im Internet, wie diese überlistet werden können. Doch der Aufwand ist sehr gross. Ein Gelegenheitsdieb wird kaum die Möglichkeit haben, diese Sperre zu umgehen. Und die «Profis» haben sicherlich bereits einen anderen Weg gefunden, um an unsere Daten zu kommen.
- Bleiben Sie aktuell. Schwachstellen sind kaum zu vermeiden. Der Leistungsdruck nach neuen Versionen wird immer grösser. Früher oder später werden die Schwächen gefunden und mittels Updates geschlossen (sogenannte Patches). Installieren Sie diese daher zeitnah. Hacker greifen vornehmlich bekannte Schwachstellen an, als sich den enormen Aufwand zu machen, neue noch unbekannte Fehler zu finden. Handy-Hersteller veröffentlichen in der Regel genaue Hinweise, was gefunden wurde. Somit können auch weniger gewiefte Hacker das Problem eruieren und eine Schad-Software dafür schreiben.

- Bleiben Sie anonym. Gerade in Hotels, aber auch am Bahnhof oder Flughafen, laden kostenlose WLANs zum Surfen ein. Doch diese Verbindungen sind unverschlüsselt. Jede Person am gleichen Hotspot kann mit den richtigen Tools zuschauen, welche Informationen Sie im Internet abrufen. Auch Passwörter können dabei aufgefangen werden. VPN ist eine gute Möglichkeit sich davor zu schützen. Jeglicher Verkehr wird dabei verschlüsselt über einen zuvor definierten Punkt umgeleitet. Viele Schweizer Provider bieten diese Funktion in ihren Routern an. So können Sie Ihren Internetverkehr über den Anschluss zu Hause umleiten. Niemand sieht dann die übertragenen Daten.
- Sichern Sie Ihre Daten. Dies ist Ihre Lebensversicherung. Sollte ein Problem mit dem Handy auftreten, sind die Daten unwiederbringlich verloren. Führen Sie daher regelmässig ein Backup Ihrer Daten durch. Es wäre schade, wenn die einmaligen Fotos und Erinnerungen weg sind. Wenn Sie sich überlegen, das Backup in der Cloud abzulegen, muss es zwingend verschlüsselt sein.
- Verschlüsseln des Handys. Gelangt das Handy in die falschen Hände, kann es unter Umständen mit entsprechenden Tools ausgelesen werden. Daher gilt es, die Verschlüsselung des Gerätes zu aktivieren. Unter iPhone ist dies seit vielen Versionen aktiviert, bei anderen Anbietern muss dies der Benutzer selbst noch einrichten.
- Einfallstor Sperrbildschirm. Diverse Apps ermöglichen Informationen auch auf dem Sperrbildschirm anzuzeigen. Dies ist zwar praktisch, kann doch ohne Aufwand auf die wichtigsten Informationen zugegriffen werden. Doch sollte eine Schwachstelle genau in dieser Option vorhanden sein, ist im schlimmsten Fall ein Zugriff auf alle Daten möglich.
- Apps einschränken. Egal ob beim Android oder beim iPhone, viele Apps verlangen beinahe uneingeschränkten Zugriff auf das Gerät. Das ist aber in den meisten Fällen gar nicht notwendig. Schränken Sie die Apps auf ein Minimum ein. Eventuell gibt es sogar Alternativen, die es nicht so auf unsere Daten abgesehen haben. Gerade Sensoren, Kamera, Mikrofon und die Funk-Schnittstelle sind mit Bedacht freizugeben. Auch die Standortfreigabe sollte im Auge behalten werden. Einige Apps fragen nach, ob diese auch bei Nichtbenutzung auf unseren Standort zugreifen dürfen. Dies ist in den wenigsten Fällen notwendig. Richten Sie die Standortfreigabe so ein, dass diese nur bei Benutzung der entsprechenden App erlaubt ist. Google und Co. müssen nicht jeden unserer Schritte kennen.
- Auch wenn das Handy zu unserem ständigen Begleiter geworden ist, sollten wir vorsichtig sein. Poppt eine suspekte Meldung auf dem Display auf, sollte nicht einfach auf «Ja» geklickt werden. Zudem muss nicht jede App sofort installiert werden. Lesen Sie zuerst, auf welche Daten die App zugreifen möchten und entscheiden Sie nachher, ob Sie dies wirklich möchten.

Unsere Daten gehören uns und sollten nicht mit unbekannten Firmen geteilt werden. Wenn wir mit gesunder Skepsis handeln, können wir auch in Zukunft sicher kommunizieren und unsere Daten vor Missbrauch schützen.

INFOS | KONTAKT

goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch