heise online

Brauche ich auf dem iPhone einen Virenscanner?

14.05.2020 09:38 Uhr Anna Kalinowsky

Wie können Sie sich auf dem iPhone vor Viren schützen? Gibt es überhaupt Virenscanner für das iPhone? Wir zeigen, worauf Sie achten müssen.

Jeder PC-Nutzer weiß, wie wichtig ein Virenscanner ist. Schließlich bedrohen Sicherheitslücken und Angreifer, die Schadsoftware einschmuggeln, den Rechner tagtäglich. Erpressungstrojaner wie Locky sperren Rechner und erpressen die Nutzer, andere Schädlinge fügen Dateien oder dem Computer selbst Schaden zu. Dementsprechend logisch scheint es zu sein, Virenscanner auch auf dem iPhone oder iPad einzusetzen. Das ist jedoch nicht nötig. Warum? Nun, es gibt mehrere Gründe:

Darum brauchen Sie keinen Virenschutz auf Ihrem iPhone:

1. **Apple sagt, dass Sie keinen Virenscanner brauchen:** Apple geht offiziell gegen Virenscanner im App Store vor. 2015 gab es eine große Löschwelle, bei der alle vorgeblichen Antivirus-Lösungen von Apple aus dem Store geschmissen wurden. Seither tauchen zwar immer wieder namhafte Produkte im Store auf – etwa Norton oder McAfee – doch die sind keine Virenscanner, sondern „Sicherheitstools“ mit geringem Mehrwert.
2. **Das iOS-Betriebssystem ist nicht für Virenscanner geeignet:** Aber warum hat Apple etwas gegen Virenscanner? Das liegt daran, dass sie bestenfalls einen Placebo-Effekt erzielen können, sprich: keinen Sicherheitsbonus bieten. Eine Erklärung bietet ein Blick auf die Konstruktion des iOS-Betriebssystems: Jede App läuft in einer geschützten eigenen Umgebung, einer

sogenannten Sandbox. Auch Virenscanner arbeiten dementsprechend in einer Sandbox, sodass sie dadurch nicht auf andere Apps und das Betriebssystem zugreifen können. Das macht sie nutzlos.

3. **Es gibt nur den App Store als Software-Quelle:** Außerdem hat Apple von vornherein einen der Haupt-Übertragungswege von Schadsoftware ausgemerzt: Viren und Trojaner kommen in den allermeisten Fällen durch die Installation von Software auf den Windows-PC: Das kann ein als Dokument getarnter Installer sein oder eine manipulierte Setup-Datei aus einer Download-Website oder Filesharing-Börse. Alles Dinge, die auf dem iPhone nicht möglich sind – weil nur der App Store Software bereitstellt. Und zwar nach Prüfung durch Apple. Android-Geräte können hingegen auf eine Vielzahl von deutlich schlechter geprüften App-Stores zugreifen – das Risiko, dass sich hier irgendwo ein Schädling einnistet, ist ungleich höher. Virenscanner für Android können also durchaus sinnvoll sein.
4. **Der iPhone-Marktanteil ist zu klein:** Befällt ein Schädling eine Monokultur, hat er leichtes Spiel – das ist bei Computern nicht anders als in der Landwirtschaft. Dementsprechend waren die großen Virenwellen der Vergangenheit zumeist mit Windows-PCs verknüpft: Das Windows-System bietet mit 90 Prozent Marktanteil ideale Ausbreitungsmöglichkeiten und ist damit für Angreifer besonders interessant: Die installierte Basis hat einen ähnlichen Update-Stand, nicht gepatchte Sicherheitslücken stehen sperrangelweit offen – und es ist ein Leichtes, schnell eine große Zahl von Rechnern zu infizieren. Bei iOS liegt der Marktanteil weltweit bei ca. 20 Prozent – Android ist da ein deutlich dankbareres Ziel.
5. **Apples iOS besitzt zusätzliche Sicherheitsmechanismen:** All diesen Sicherheitsvorteilen zum Trotz gibt es immer wieder App-Entwickler, die versuchen, Schadsoftware im kleinen Umfang zu integrieren. In der Vergangenheit gab es zum Beispiel Apps, die unerlaubt auf die Kamera zugriffen oder Adressdaten kopierten. Inzwischen hat iOS hierfür Sicherheitsmechanismen: Jede App muss erst um Erlaubnis fragen, um auf bestimmte Systemfunktionen oder Informationen zuzugreifen – bei Schädlingen aus dem App Store ist das nicht anders.
6. **Ein Virus würde auffallen:** Doch selbst, wenn ein Virus es zum Beispiel über eine Website und eine Sicherheitslücke im Safari-Browser schaffen würde, würde dieser vermutlich auffallen: Heutige Angreifer versuchen in aller Regel, Daten zu stehlen, Botnetze zu etablieren oder Bitcoins zu ernten – und das kann auf Smartphones durchaus auffallen, weil die Systemlast und der Akkuverbrauch steigen. Zudem sprechen sich alle Apple-bezogenen News schnell herum: Würde eine App oder Website tatsächlich Schadsoftware ausliefern, wäre das ein gefundenes Fressen für die zahllosen Apple-Blogs und News-Seiten. Apple reagiert zudem schnell auf solche Sicherheitslücken.

Gilt nicht für iPhones mit Jailbreak

Apples Behauptung, dass iOS ein sicheres Betriebssystem sei, ist also durchaus berechtigt. Angreifer haben zumindest auf dem klassischen Wege der Installation einer Schadsoftware kaum Chancen, einen Virus oder Trojaner auf dem iPhone zu hinterlegen. Was im Umkehrschluss Antivirensoftware unnötig macht. Allerdings gilt das nur für iPhones und iPads im Originalzustand. Wer einen Jailbreak durchführt, kann sich durchaus einen Schädling einfangen: Einerseits, weil der Jailbreak konzeptbedingt zahlreiche Sicherheitsmechanismen von iOS umgeht, andererseits, weil der Cydia-Store im Grunde jedem Entwickler offen steht und es hier keine Kontrollmechanismen gibt. Zusätzlich

können Jailbreak-iPhones nicht immer sofort auf die neueste Software-Version aktualisiert werden – ein weiterer Risikofaktor. Der lässt sich jedoch nur durch Vorsicht umgehen, denn Virenscanner gibt es schließlich trotzdem nicht für das iPhone.

Die Gefahren liegen woanders

Doch der klassische Virus ist auf dem iPhone ohnehin nicht das bedeutendste Problem: Vielmehr drohen Phishing-Attacken, Scareware-Werbung, falsche Gewinnspiele und Rückruf-Abzocke – alles Dinge, gegen die das iPhone keine Handhabe hat. So sind entsprechende Websites meist nur wenige Stunden online: Falsche Paypal-, Ebay-, Amazon- oder Onlinebanking-Seiten verlangen die Eingabe der Zugangsdaten, meist über die per Mail oder SMS angedrohte Sperrung des Kontos – sogenannte Phishing-Attacken. Oder falsche Gewinnspiele greifen Kontaktdaten ab, die später für den Identitätsdiebstahl verwendet werden. Scareware-Werbung bringt Sie dazu, eine App zu installieren, die Sie gar nicht wollten oder Daten abzugeben, die eigentlich bei Ihnen bleiben sollten (etwa Passwörter) und Anruf-Abzocker kassieren bei Rückruf mehrere Euros pro Minute, während Sie in einer Warteschleife hängen.

Die einzige Lösung: Aufmerksamkeit

Gegen diese Art der Angriffe ist leider derzeit kein Kraut gewachsen: Fake- und Phishing-Websites sind nur selten länger online, weshalb Warnsysteme (zu aktivieren unter Einstellungen -> Safari -> Betrugswarnung) oft zu spät greifen. Hier hilft nur gesunder Menschenverstand und eine Überprüfung der verlinkten URL, wenn eine E-Mail zur Neueingabe der Kontodaten aufruft: Seriöse Anbieter wie Amazon, Paypal oder Ebay gehen ohnehin nicht so vor, sie „verlieren" keine Kontodaten, müssen dementsprechend auch keine Mails versenden, die zur Neueingabe auffordern. Bei Scareware hilft oft (aber nicht immer) die Deaktivierung von Pop-ups (Einstellungen -> Safari -> Pop-ups blockieren). Wenn Sie diese Maßnahmen berücksichtigen, sollten Sie immer auf der sicheren Seite sein.

MEHR INFOS

- **Security-Checklisten: Die richtigen Handgriffe für mehr Sicherheit [1]**
- **Virenscanner für Android – brauche ich das? [2]**
- **Virenschutz für Ihren Windows-PC [3]**

(anka)

URL dieses Artikels:

`https://www.heise.de/-3853961`

Links in diesem Artikel:

[1] `https://www.heise.de/ratgeber/Security-Checklisten-Die-richtigen-Handgriffe-fuer-mehr-`

Sicherheit-4886774.html

[2] https://www.heise.de/tipps-tricks/Virenscanner-fuer-Android-brauche-ich-das-3872867.html

[3] https://www.heise.de/tipps-tricks/Virenschutz-fuer-Ihren-Windows-PC-3841400.html