VIRENSCHUTZ FÜR DAS SMARTPHONE

Das Smartphone ist heute längst weit mehr als nur ein Mobiltelefon. Mit dem kleinen Computer in der Hosentasche gehen wir täglich wie selbstverständlich online, rufen über Browser oder Apps Informationen unterschiedlichster Art ab. Doch nicht alle Seiten und Anwendungen sind seriös und vertrauenswürdig. Cyberkriminelle nehmen zunehmend Smartphones ins Visier, da hier doch die eine oder andere Sicherheitslücke vorhanden ist. Es gilt also, Vorsicht walten zu lassen. Wir zeigen in diesem Ratgeber auf, welches Betriebssystem besonders betroffen ist, welche Vorsichtsmaßnahmen ergriffen werden können und beschäftigen uns mit der Frage, inwieweit Security-Apps eine Hilfe gegen Schädlingsangriffe aus dem Netz sein können.

Wenn es um das Thema Virenschutz für das Smartphone geht, sollte zunächst einmal geklärt werden, wie groß eigentlich das individuelle Risiko einer solche Bedrohung ist. Denn je nachdem, welches Betriebssystem auf dem eigenen Gerät installiert ist, stellt sich die Gefahrenlage durchaus unterschiedlich dar. So müssen sich iPhone-Nutzer kaum Sorgen machen, dass Viren ihr Telefon befallen könnten. Das hat insbesondere damit zu tun, dass unter dem Betriebssystem iOS lediglich Apps aus dem offiziellen iTunes Store installiert werden können. Diese werden vorher genauestens von Experten überprüft. Aufatmen können auch alle Nutzer eines Windows-Smartphones. Da die Verbreitung dieses mobilen Betriebssystems so marginal ist, wird es von Cyberkriminellen eher links liegen gelassen.

Auf der Hut sein sollten also allen voran Besitzer eines Smartphones mit Android an Bord. Dieses Betriebssystem ist heute mit Abstand führend auf dem Markt. Da hier das sogenannte „Open Source“-Konzept verfolgt wird, ist es deutlich anfälliger für Malware als iOS. Denn bei Android ist es grundsätzlich auch möglich, Anwendungen aus anderen Quellen als Google Play zu installieren. Und selbst dort ist es schon vorgekommen, dass schädliche Apps hochgeladen, hinterher jedoch wieder vom Portal entfernt wurden. Für Android-Nutzer gilt also: Augen auf in Sachen Virenschutz für das Smartphone, damit es gar nicht erst zu einem Befall des Geräts kommt.

Auch vollkommen unabhängig von einem Virenschutz für das Smartphone in Form spezieller Apps lässt sich einiges unternehmen, um es den finsteren Gestalten des World Wide Webs so schwer wie möglich zu machen. Wichtig ist vor allem für Android-Nutzer, dass sie niemals Anwendungen aus Quellen installieren, die nicht vertrauenswürdig erscheinen. Am besten sollten nur Apps heruntergeladen werden, die schon seit einigen Wochen bei Google Play gelistet werden und bereits überwiegend positive Bewertungen von anderen Nutzern erhalten haben. Bei einer solchen Vorgehensweise dürfte die Gefahr, dass auf diesem Wege Viren oder Trojaner auf das eigene Smartphone gelangen, gegen Null tendieren.

Aber nicht nur in Sachen Apps ist es wichtig, besonnen zu handeln. So sollte auch jeder Smartphone-Nutzer sich genau überlegen, welche Webseiten er über seinen mobilen Browser wirklich aufrufen möchte. Je häufiger unbekannte oder eher unseriöse Seiten besucht werden, desto größer ist die Gefahr, dass im Verborgenen Schädlinge auf das Gerät gelangen. Bei empfangenen E-Mails sollte ebenfalls nicht achtlos auf die enthaltenen Links geklickt werden. Viele Phishing-Mails sind heutzutage erstaunlich professionell erstellt. Jedoch hilft in den meisten Fällen dennoch das Einschalten des gesunden Menschenverstandes. So wird beispielsweise die Hausbank niemals per E-Mail nach PINs oder TANs fragen. Auch seltsame Absender-Adressen und Rechtschreibfehler sollten stutzig machen. Hinzu kommen einige Einstellungen, die Nutzer unter Android vornehmen können, um den Virenschutz für das Smartphone zu verbessern:

In den Einstellungen sollte unter „Sicherheit“ im Untermenü „Unbekannte Quellen“ der Haken nicht gesetzt sein

- Regelmäßig durchgeführte Updates des Betriebssystems halten dieses auch im Hinblick auf die Sicherheit auf dem neuesten Stand
- Um Trojaner daran zu hindern, teure Premium-SMS zu versenden, kann beim Mobilfunk-Anbieter eine sogenannte „Drittanbietersperre“ beantragt werden
- PIN oder klassisches Passwort zum Eingeben bieten den besten Schutz für das Gerät

Selbst unter ausgewiesenen Experten gibt es keine einhellige Meinung dazu, ob Security-Apps nun Pflicht sein sollten auf jedem mobilen Endgerät oder ob es ausreicht, die bereits beschriebenen Vorkehrungen im Hinblick auf den Virenschutz für das Smartphone zu treffen. Die entsprechenden Anbieter der Apps listen selbstverständlich jede Menge Vorteile auf und schwören auf den Mehrwert, den das eigene Produkt dem Nutzer bietet. Doch welche Punkte sprechen nun tatsächlich für die Installation solcher Anwendungen? Welche dagegen? Beginnen wir mit den Pro-Argumenten:

•Vielfältige individuelle Sicherheitseinstellungen möglich
•Security-Apps laufen in der Regel unauffällig im Hintergrund
•Warnungen vor Klicks auf Links in E-Mails oder bei Besuchen unbekannter Websites
•Eine Firewall gehört zum Bestandteil der meisten Apps
•Integrierte Ortungs- und Sperrfunktionen für gestohlene Smartphones
•

Diesen Argumenten stehen einige Kritikpunkte gegenüber, denen im Folgenden ebenfalls Raum gegeben werden soll, damit sich jeder sein eigenes Urteil bilden kann:

•Manche Security-Apps verbrauchen viel Speicherplatz
•Akkuleistung und Performance des Geräts können beeinträchtigt werden
•Teils schlechtes Kosten-Nutzen-Verhältnis bei kostenpflichtigen Apps
•Einige Funktionen der Apps sind auch schon in Android selbst gegeben
•Die verwendeten Datenbanken sind nicht immer auf dem neuesten Stand

Ist die persönliche Entscheidung pro Security-Apps ausgefallen, gilt es als nächstes herauszufinden, welche dieser Anwendungen wirklich den besten Virenschutz für das Smartphone bietet. Auf dem Markt gibt es sowohl kostenlose als auch kostenpflichtige Apps. Ein Test der Fachzeitschrift „CHIP“ hat ermittelt, dass nur eine einzige App wirklich 100 Prozent der auf das Gerät losgelassenen Schadsoftware erkannt hat. Bitdefender Mobile Security ging keine der 2545 getesteten Malware-Apps durch die Lappen. Doch auch die folgenden Security-Apps erzielten sehr gute Werte von 99,9 bis 99,8 Prozent:

•Trend Micro Mobility Security
•Micro World eScan Mobile Security
•avast
•Symantec
•Comodo

Bei all diesen Lösungen kann der Anwender im Prinzip bedenkenlos zugreifen und erhält ein sehr gutes Produkt, das den Virenschutz für das Smartphone auf ein neues Level bringt.

Auch der vorsichtigste Nutzer kann einmal in die Situation geraten, dass sämtliche vorbeugenden Maßnahmen ins Leere gelaufen sind und ein Schädling sich auf dem Smartphone ausbreiten konnte. Was sollte man nun am besten tun? Wer nun eine gute Security-App installiert hat, dem wird diese bereits entsprechende Lösungsvarianten präsentieren. Ist dies nicht der Fall, ist das Zurücksetzen

des Smartphones auf die Werkseinstellungen immer eine gute Maßnahme. So wird der Virus zuverlässig entfernt. Vorab sollten allerdings alle wichtigen Daten beispielsweise in einer Cloud gesichert worden sein, da diese sonst ebenfalls verloren sind. Sollte das Zurücksetzen durch den Virus nicht möglich sein, gilt es den Recovery-Modusaufzurufen. Dazu bedarf es einer besonderen Tastenkombination, die sich in der Bedienungsanleitung des Smartphones finden lassen sollte. Fordert ein Virus den Nutzer beispielsweise zur Überweisung eines Geldbetrages auf, sollte auch das Konsultieren der Polizei nicht gescheut werden.

Letztendlich lässt sich sagen, dass auch die beste Security-App natürlich keinen tausendprozentigen Schutz vor Schädlingen aus dem Netz bieten kann. Denn schließlich entstehen immer wieder neue Schlupflöcher, die sich Kriminelle zunutze machen. Wer eine gute App installiert, erhält dennoch ein weitestgehend zuverlässiges und vor allem auch sehr komfortables Schutzsystem. Der wichtigste Virenschutz für das Smartphone bleiben aber die eigene Wachsamkeit und ein kritisches Nutzungsverhalten, das mögliche Gefahren frühzeitig erkennt.