Der Zitmo-Virus und worauf man achten sollte

Bei den Computernutzern war der Zitmo-Virus schon länger bekannt, bevor er auch Smartphones befiel. Denn die Betrüger, welche dieses Virus nutzen, haben ihre kriminelle Arbeit dem Nutzerverhalten der User angepasst. Es wird inzwischen ja immer häufiger das Smartphone auf für das Online-Banking genutzt und genau darum geht es. Der ZeUS-in-the-Mobile-Virus kann die Betriebssysteme:

Android
iOs
Blackberry
Windows Phone

befallen. Nach der Installation werden die Passwörter und mTans für das Online-Banking gestohlen.

So arbeitet Zitmo

Der User lädt sich den Virus selbst herunter und installiert. Das geschieht dann, wenn er, bei der Suche nach einer Anti-Virus-App auf eine mit dem Namen *TrustMobile* stößt. Diese gibt es auf illegalen Webseiten oder auch auf Fake-App-Stores. Da der User denkt, er bekommt eine sichere Antivirensoftware, lädt er sie sich herunter und schon ist sein Smartphone mit dem Virus Zitmo befallen. Für eine ganze Weile gab es TrustMobile sogar im Android Market. Erst nach Entdecken der Schadsoftware darin wurde diese App aus dem Programm genommen. Ist das Virus auf dem Smartphone installiert, fängt er eingehende SMS ab und lädt diese dann auf einen Remote Server. Nutzt ein User Online-Banking, dann schickt die Bank auf Wunsch des Kunden, mobile Tans oder auch Passwörter, die zurückgesetzt wurden, per SMS zu. Diese werden dann von Zitmo auf den Remote Server geleitet und:

die mTans und Passwörter landen in den Händen der Betrüger
die Betrüger führen Online-Buchungen durch
anschließend wird der gesamte Vorgang wieder deinstalliert
so werden alle Spuren vernichtet

Durch die selbstständige Deinstallation ist es nur sehr schwer möglich, den Betrügern auf die Spur zu kommen.

Was wichtig wäre

Es gibt sehr viele verschiedene Apps, so ist es kaum möglich, alle diese Programme zu überprüfen. Möchte man eine App herunterladen, sollte man vorher die Berichte von anderen Usern lesen. Diese werden am meisten darüber sagen können, wie die App funktioniert und welche Probleme es vielleicht gibt. Auch sollte jedes Smartphone einen Virenscanner besitzen, der auch regelmäßig eingesetzt werden muss. Diese kann die Software-Updates kontrollieren und Schadware entdecken. Allerdings sollte man eben auch beim Herunterladen von Virensoftware aufpassen. Es empfiehlt sich, auf bekannte Anbieter zurückzugreifen. Eine Liste finden Sie hier: Virenscanner Test. Wenn eine Virenapp sehr viele Daten abfragt, sollte man lieber die Finger davon lassen, denn es kann sich eben auch dahinter eine Schadware

verstecken. Leider ist es nicht sicher möglich, Zitmo vom Smartphone zu entfernen. Denn es ist nicht bekannt, inwieweit diese Schad-App in das Betriebssystem eingreift und sich dort einnistet. Die sicherste Methode ist es daher, das Smartphone auf die Werkseinstellung zurückzusetzen und dann das Betriebssystem neu zu installieren. Informationen darüber, wie die geht, kann man dem Servicehandbuch des Smartphones entnehmen oder bei der Servicehotline nachfragen. Bild: ©Uli Carthäuser / pixelio.de