Zu den wichtigsten vermeidbaren Fehlern zählen der Download von Apps aus nicht offiziellen Quellen.

Cyber-Erpressung: Jeder dritte Befragte in Deutschland fürchtet mobile Ransomware-Programme.

Mobile Bedrohung

Laut einer Studie von *Kaspersky Lab* werden mobile Nutzer in Deutschland immer öfter von Ransomware attackiert. Jeder dritte deutsche Mobilnutzer fürchtet Cyber-Erpressung.

Mobile Geräte werden vermehrt für sensible Transaktionen wie Mobile-Banking oder zur Steuerung von intelligenten Geräten und Systemen wie smarte Lautsprecher oder Häuser verwendet. Nutzer mobiler Geräte stehen damit verstärkt im Visier Cyber-Krimineller. *Kaspersky Lab* veröffentlichte eine Studie über die mobilen Cyber-Gefahren in Deutschland. Der Bericht informiert über hochentwickelte Schadprogramme, warnt vor kriminellen Trends und liefert Sicherheitstipps für den Schutz von Smartphones und Tablets. Die Studie ist downloadbar unter *http://newsroom.kaspersky.eu*.

Im Untersuchungszeitraum September 2016 bis August 2017 gab es mehr als eine Million Angriffe auf Nutzer mobiler Kaspersky-Lösungen in Deutschland. Das entspricht einer Zunahme von über 70 % gegenüber dem Vergleichszeitraum 2015/16; und einer Steigerung von über 240 % im Vergleich zu 2014/15. 2017 um 16 % mehr deutsche Smartphone-Nutzer mittels Ransomware-Attacken erpresst als vor drei Jahren; die Anzahl mobiler Banking-Trojaner stieg seit September 2014 um 68 % an. Je mehr Smartphone- oder Tablet-Nutzer sensible Transaktionen wie Online-Shopping tätigen, desto mehr heikle Informationen speichern sie auf ihren mobilen Geräten – und desto interessanter werden sie für mobilen Betrug, Spionage oder Erpressung.

Mobile Schädlinge. *Kaspersky-Lab* kennt derzeit über 28 Millionen APK-Dateien *(Android Installation Packets)* – dabei handelt es sich um Programme/Apps, über die mobile Schädlinge/Malware heimlich auf die Geräte der Nutzer geschleust werden sollen. Von den bei *Kaspersky-Lab* bekannten fünf Millionen mobilen Schädlingsdateien haben es 99,88 Prozent auf das Android-Betriebssystem abgesehen. „Gründe für den Anstieg an Malware liegen im riesigen Markt für Apps und den damit verbundenen massiven Downloads“, sagt Christian Funk, Leiter des deutschen Forschungs- und Analyse-Teams bei *Kaspersky Lab*. „Die Malware wird dabei in vermeintlich legitimen Apps versteckt, die Reputation populärer Apps damit missbraucht.“

Finanzdaten. Im Untersuchungszeitraum September 2014 bis August 2017 nahmen die Angriffe durch mobile Banking-Trojaner um 78 % zu. „Mobile-Banking-Trojaner haben es auf Finanzdaten wie Kreditkarteninformationen oder Zugänge zu Banking-Accounts abgesehen, insbesondere Online-Payment-Systemen“, erklärt Funk. Es sollten zusätzliche Sicherheitsmerkmale wie die Zwei-Faktoren-Authentifizierung genutzt werden. Die Zwei-Faktoren-Authentifizierung besteht aus zwei unterschiedlichen Sicherheitsmaßnahmen, um sich zu identifizieren – etwa PIN- und Passwort-Abfrage.

Erpressung. Jeder dritte Befragte fürchtet mobile Ransomware-Programme (Cybererpressung). Die Qualität der Ransomware-Schädlinge bei mobilen Geräten habe sich laut Funk verbessert. Die Variante „Trojan-Ransom.AndroidOS.Fusob.h“ wurde bei 12 % der in Deutschland mobil attackierten *Kaspersky*-Nutzer registriert und abgewehrt.

Unerwünschte Werbung. Zwei Drittel der deutschen Nutzer fühlen sich durch unerwünschte Werbung (Adware) auf dem Smartphone und Tablet gestört. *Kaspersky Lab* kennt weltweit über 24 Millionen Adware-Programme. Auf der Top-40-Liste der 2016/17 grassierenden mobilen Schadprogramme wurden 35 % dem Typ Adware zugeordnet.

Spionage und Datenklau. Die Experten von *Kaspersky Lab* kennen derzeit weltweit 840.500 mobile Schädlinge des Typs „Trojan Spy“. Auch auf *Google Play* gibt es mit Malware kompromittierte Apps. 2016/17 registrierten die Experten von *Kaspersky Lab* mobile Trojaner (Spyware), die in der Lage sind, Login-Daten zu stehlen, und über kompromittierte Apps in *Google Play* verbreitet wurden, wie die Version „Trojan-Spy.AndroidOS.Instealy.a“ – ein mobiler Trojaner, der Login-Daten und Passwörter von *Instagram*-Accounts stehlen kann – oder „Trojan-

Fotos: Carballo/Fotolia, Jampedion/Fotolia

PSW.AndroidOS.MyVk.a“, ein Schädling, der es auf Zugangsdaten der Social-Networking-Seite *VKontakte* abgesehen hat.

Einfallstore auf mobile Geräte. 85 % der Befragten laden Apps von offiziellen App-Stores (zum Beispiel *Google Play, Apple App Store, Microsoft Windows App)* herunter. Nur 5 % behaupten, Apps von unbekannten Quellen oder Seiten herunterzuladen; 4 % wissen es nicht genau.

Der Download von Apps aus nicht offiziellen Quellen ist der Hauptinfektionsweg für Smartphones und Tablets. Cyber-Kriminelle tarnen schädliche Installationspakete als populäre Apps im legitim erscheinenden Gewand, um sie auf mobile Geräte einzuschleusen und aktiv zu werden“, warnt Christian Funk.

2016 gab es einen Hype um das mobile Spiel „Pokémon Go“. Cyber-Kriminelle nutzten den Hype für ihre illegalen Machenschaften aus, indem sie Installationsdateien des Spiels mit Malware kompromittiert zum App-Download angeboten hatten; nach der Installation hatten die Angreifer Zugriff auf das Smartphone.

Nutzungsrechte. Wenn es um App-Berechtigungen geht, gehen viele Nutzer in Deutschland sorglos um. 32 % stimmen den von der App eingeforderten Nutzungsrechten erst zu, wenn sie die Berechtigungen gelesen hat. 38 Prozent stimmen den angefragten Berechtigungen zu, ohne sie zu lesen. 20 Prozent sind unentschlossen.

Christian Funk empfiehlt, dass „ab Android 6 Berechtigungen von Apps individuell verwaltet und geändert werden können. Nutzer können App-Berechtigungen ändern und beispielsweise nachträglich entziehen, was im Sinne von Privatsphäre und besserem Datenschutz zu begrüßen ist“.

Rooten von Geräten. Fast jeder fünfte Befragte in Deutschland gab an, er habe schon einmal beim eigenen Smartphone oder Tablet die vom Hersteller vorgegebenen Nutzungsbeschränkungen entfernt (das Gerät gerootet beziehungsweise einen Jailbreak durchgeführt), um zum Beispiel die Systemeinstellungen verändern oder vorinstallierte Apps löschen zu können. 40 Prozent haben dies noch nie getan. 39 Prozent gaben zu, dass sie nicht so genau wissen, was mit dem Entfernen von Nutzerbeschränkungen gemeint ist.

WLAN aktiv. 55 % der Befragten haben die WLAN-Funktion auf dem Handy durchgehend aktiviert. „Zu den wichtigsten vermeidbaren Fehlern zählen der Download von Apps aus nicht offiziellen Quellen und das Rooten von Geräten.

Es sollte jedem Nutzer klar sein: Wer unsichere WLAN-Netze und zweifelhafte Bezugsquellen verwendet, oder auf seinen Geräten die voreingestellten Beschränkungen manipuliert, der sollte ein hohes Sicherheitsverständnis haben und wissen, welche Konsequenzen das mit sich bringen kann“, sagt Christian Funk.

CYBERSICHERHEIT

Sicherheitstipps

Auf die Umgebung achten: Wer unterwegs mobile Geräte benutzt, sollte nicht jeden Sitznachbarn in Bahn oder Bus mitlesen oder mithören lassen. Mobile Kommunikation ist grundsätzlich nicht abhörsicher. Mobile Geräte sollte man niemals unbeaufsichtigt liegen lassen.

Gerätesperren nutzen: Die Tasten- oder Display-Sperre mobiler Geräte sollte immer aktiviert sein. PIN- und Passwort-Abfragen sind als Authentifizierung besser geeignet, als der scheinbar sichere Fingerabdruck-Scan. Denn die Fingerabdrücke des rechtmäßigen Nutzers lassen sich vom Display des Geräts abnehmen. Kennwörter und -nummern sollten nicht als getarnte Telefonnummern auf dem Gerät hinterlegt werden, denn viele Apps haben Zugriff auf die Kontaktdaten der Anwender.

Vorsicht bei der Weitergabe von Geräten: Wer ein Gerät verschenkt oder verkauft, sollte alle Daten löschen. Das Zurücksetzen auf die Werkseinstellungen reicht nicht aus.

Betriebssystem aktuell halten: Nur die aktuellsten Betriebssysteme sind einigermaßen sicher.

Daten regelmäßig sichern: Die beste Möglichkeit sich gegen Erpressungsversuche mit mobiler Ransomware zu schützen ist, regelmäßig Daten des mobilen Geräts zu sichern. Lösegeld-Forderungen sollte man niemals nachkommen, sondern den Fall der Polizei melden.

SMS-Dienste sperren: Damit Trojaner auf dem Smartphone nicht unbemerkt Nachrichten an Premium- oder Abo- Dienste versenden, sollte man entsprechende Dienste bei seinem Mobilfunk-Anbieter sperren lassen.

Geräte niemals „rooten“: Nutzer sollten genau wissen, was sie tun, und mit Bedacht Apps installieren und sie nur aus vertrauenswürdigen Quellen downloaden.

Die Verbindung im Auge behalten und verschlüsseln: Vor der Nutzung heikler Anwendungen wie Mobile-Banking muss die aktuelle Netzverbindung des mobilen Geräts geprüft werden. Auf keinen Fall sollte man unsichere WLAN-Verbindungen nutzen, es sei denn, es wird darüber eine eigene, sichere VPN-Verbindung hergestellt. Sensible Daten sollten – wann immer möglich – nur in verschlüsselter Form übertragen werden.

Sicherheitslösung installieren: Es gibt kostenlose, gute Sicherheitslösungen und Tools für mobile Geräte, mit denen sich deren Sicherheit verbessern lässt.

Vorsicht bei der Installation neuer Apps: Keinesfalls sollte man Apps installieren, die als Anhang oder Link einer E-Mail propagiert werden. Apps sollten von vertrauenswürdigen Quellen und Entwicklern bezogen werden, am besten aus den offiziellen App-Stores. Vorsicht ist geboten, wenn Apps Rechte verlangen. Etwa die Weitergabe von Standort-Daten, Zugriff auf Kontakte oder das Recht zum Versenden von SMS.

App-Liste von Zeit zu Zeit durchforsten: Nicht jede App auf jedem mobilen Gerät wird wirklich noch genutzt, viele sind längst überholt. Das regelmäßige Löschen unsinniger oder unnötiger Apps verschafft nicht nur mehr Speicherplatz, sondern erhöht auch die allgemeine Sicherheit.

Apps immer aktuell halten: Alle Anwendungen auf den Geräten sollten wie das Betriebssystem selbst immer auf dem aktuellen Stand gehalten werden. Das gilt besonders für sicherheitsrelevante Apps.