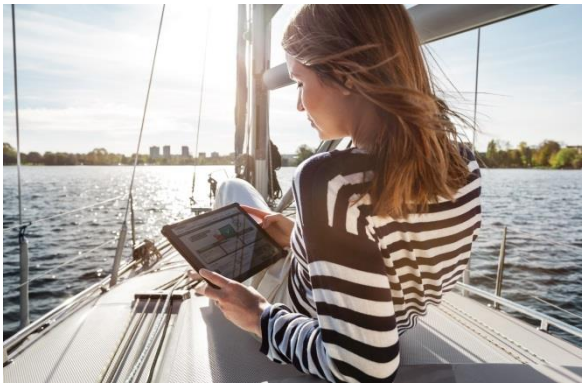
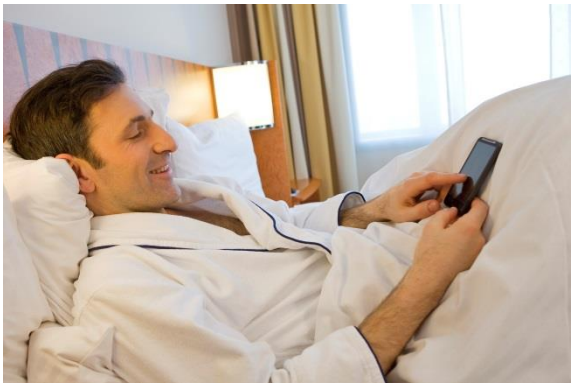
Mobile Schadprogramme in Deutschland – Panikmache oder echte Gefahr?

Kaspersky-Studie der mobilen Bedrohungssituation in Deutschland – eine Jahresanalyse (September 2016 bis August 2017)

Inhalt





Laut Statista-Prognose[1] soll sich die Anzahl der Smartphone-Nutzer in Deutschland im Jahr 2022 auf rund 65 Millionen belaufen. Mobile Geräte werden bereits heute nicht ausschließlich zum Telefonieren und Surfen, sondern vermehrt für sensible Transaktionen verwendet. So meldet etwa der Branchenverband Bitkom[2], dass die Deutschen zunehmend vom stationären Online-Banking auf Mobile-Banking umsteigen. Smartphone und Tablet entwickeln sich immer mehr zum Mittelpunkt des digitalen Lebens.

Nutzer mobiler Geräte stehen damit jedoch auch verstärkt im Visier Cyberkrimineller. Die 20-jährige Erfahrung im Kampf gegen Cyberkriminalität hat Kaspersky Lab gezeigt, dass Kriminelle ihre Ziele gerne nach einem bestimmten Muster aussuchen:

Große Zielgruppe + Aussicht auf Gewinne = Attraktives Ziel

Die Informationen und Daten, die wir vermehrt mit unserem mobilen Verhalten preisgeben, sind zudem für weitere Gruppen interessant, bei denen weniger kriminelles Verhalten als vielmehr wirtschaftlicher Nutzen im Vordergrund steht.

Grund genug für Kaspersky Lab, erstmals eine Studie[3] über die mobilen Cybergefahren in Deutschland zu veröffentlichen. Der Bericht beschreibt Lage und Entwicklung, informiert über hochentwickelte Schadprogramme, warnt vor aktuellen kriminellen Trends, und liefert Sicherheitstipps für den Schutz von Smartphones und Tablets.

Methodik

Die Studie von Kaspersky Lab zur mobilen Bedrohungssituation in Deutschland besteht aus drei Teilen:

- *Teil 1 – Daten-Analyse der mobilen Gefahren in Deutschland:* Unter der Leitung von Christan Funk, Leiter des deutschen Forschungs- und Analyse-Teams bei Kaspersky Lab, wurden im Zeitraum September 2016 bis August 2017 die auf mobilen Geräten deutscher Kaspersky-Nutzer identifizierten und blockierten Attacken (Virenalarme) analysiert. Um Tendenzen bezüglich der mobilen Bedrohungssituation in Deutschland aufzeigen zu können, werden die Daten im genannten Untersuchungszeitraum mit denen der beiden Vorjahreszeiträume verglichen (September 2015 bis August 2016 und September 2014 bis August 2015). Die Untersuchung basiert auf Daten, die aus dem cloudbasierten Kaspersky Security Network (KSN)[4] gewonnen wurden. Am KSN können Kaspersky-Kunden auf freiwilliger Basis teilnehmen. Die von Kaspersky Lab erhobenen Daten werden anonym und vertraulich behandelt.

- *Teil 2 – Umfrage unter 500 deutschen mobilen Nutzern:* Zudem wurde im August/September 2017 im Auftrag von Kaspersky Lab eine Befragung von Arlington Research[5] durchgeführt. Dabei wurden 500 deutsche Smartphone- und/oder Tablet-Nutzer ab 18 Jahre online über mobile Sicherheitsthemen befragt.

[1] https://de.statista.com/statistik/daten/studie/500579/umfrage/prognose-zur-anzahl-der-smartphonenutzer-in-deutschland/
[2] https://www.bitkom.org/Presse/Presseinformation/Mobile-Banking-wird-zum-Standard.html
[3] https://kas.pr/mobile_report
[4] http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/Kaspersky_Lab_Whitepaper_KSN_DE_1709.pdf
[5] http://www.arlingtonresearch.global/de/

- *Teil 3 – Sicherheitstipps für Smartphone- und Tablet-Nutzer:* Was sollte man sicherheitstechnisch bei der mobilen Nutzung des Internets beachten? Welche Programme schützen? Und wie gehe ich sicher mit Apps um? Diese Fragen werden praxisnah durch Experten von Kaspersky Lab beantwortet.

Auf einen Blick: Schlüsselergebnisse und Trends

Im Folgenden finden sich die interessantesten Ergebnisse der Datenanalyse sowie der Umfrage. Die Datenanalyse gibt Aufschluss über die Verbreitung mobiler Angriffe in Deutschland. Die Umfrage bildet die Wahrnehmung hinsichtlich Sicherheit und erlebter Gefahren der Nutzer mobiler Geräte in Deutschland ab.

Die Schlüsselergebnisse werden nach folgenden Themenbereichen beleuchtet:

- Betrug
- Erpressung
- Unerwünschte Werbung
- Spionage und Datenklau

BETRUG

Mobile Schädlinge stehen ihren Vorbildern aus dem Desktopbereich in nichts nach. Vor allem Trojaner haben es darauf abgesehen, ihre Opfer zu betrügen.

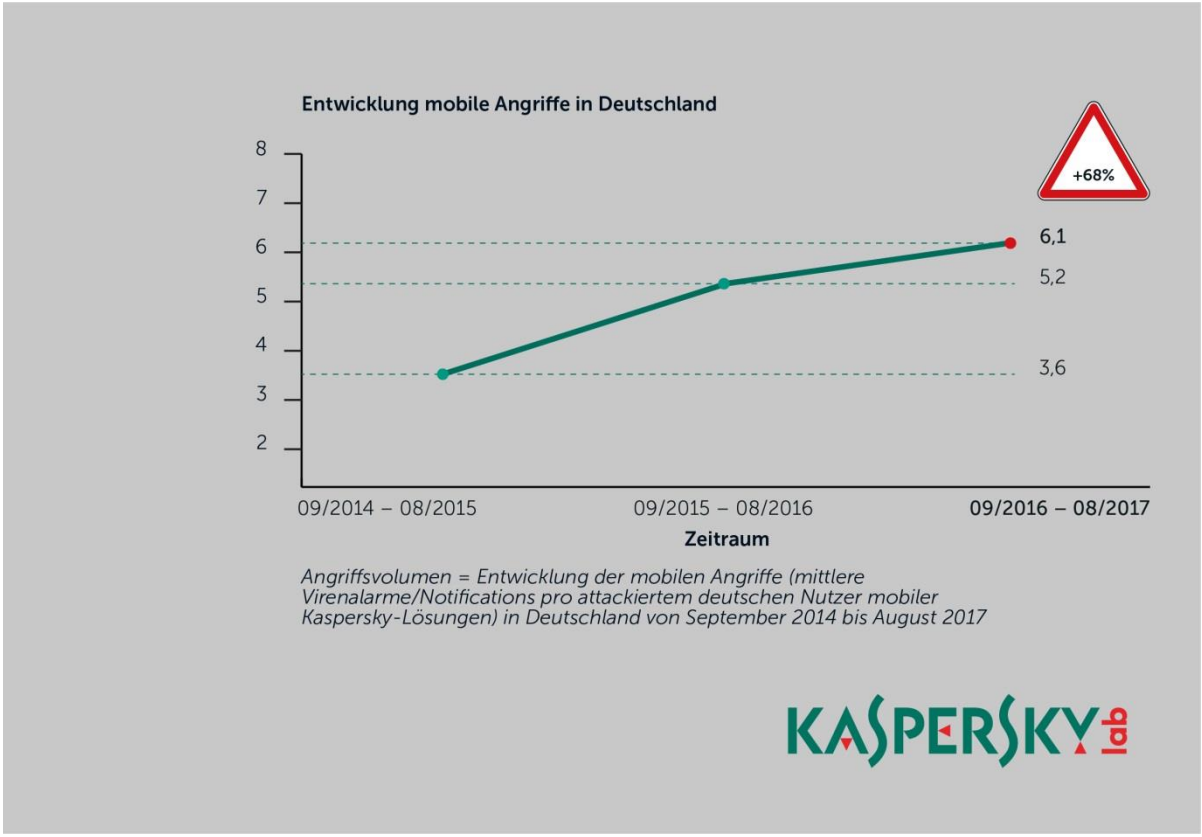
Die weltweite Ausgangslage: Kaspersky Lab kennt derzeit über 28 Millionen APK-Dateien (Android Installation Packets) – dabei handelt es sich um Programme/Apps, über die mobile Schädlinge/Malware heimlich auf die Geräte der Nutzer geschleust werden sollen. Von den bei Kaspersky Lab bekannten 5.405.053 einzelnen mobilen Schädlingsdateien haben es 99,88 Prozent auf das Android- Betriebssystem abgesehen.

Christian Funk, Leiter des deutschen Forschungs- und Analyse-Teams bei Kaspersky Lab, erklärt: *„Gründe für den Anstieg liegen im riesigen Markt für Apps und den damit verbundenen, massiven Downloads. Die Malware wird dabei in vermeintlich legitimen Apps versteckt, die Reputation populärer Apps damit missbraucht. Eine Methode, die auch deshalb so gut funktioniert, weil 50 Prozent der Android-Geräte nicht gepatchte Schwachstellen aufweisen, die beispielsweise zur Erlangung höherer Rechte benutzt werden.“*

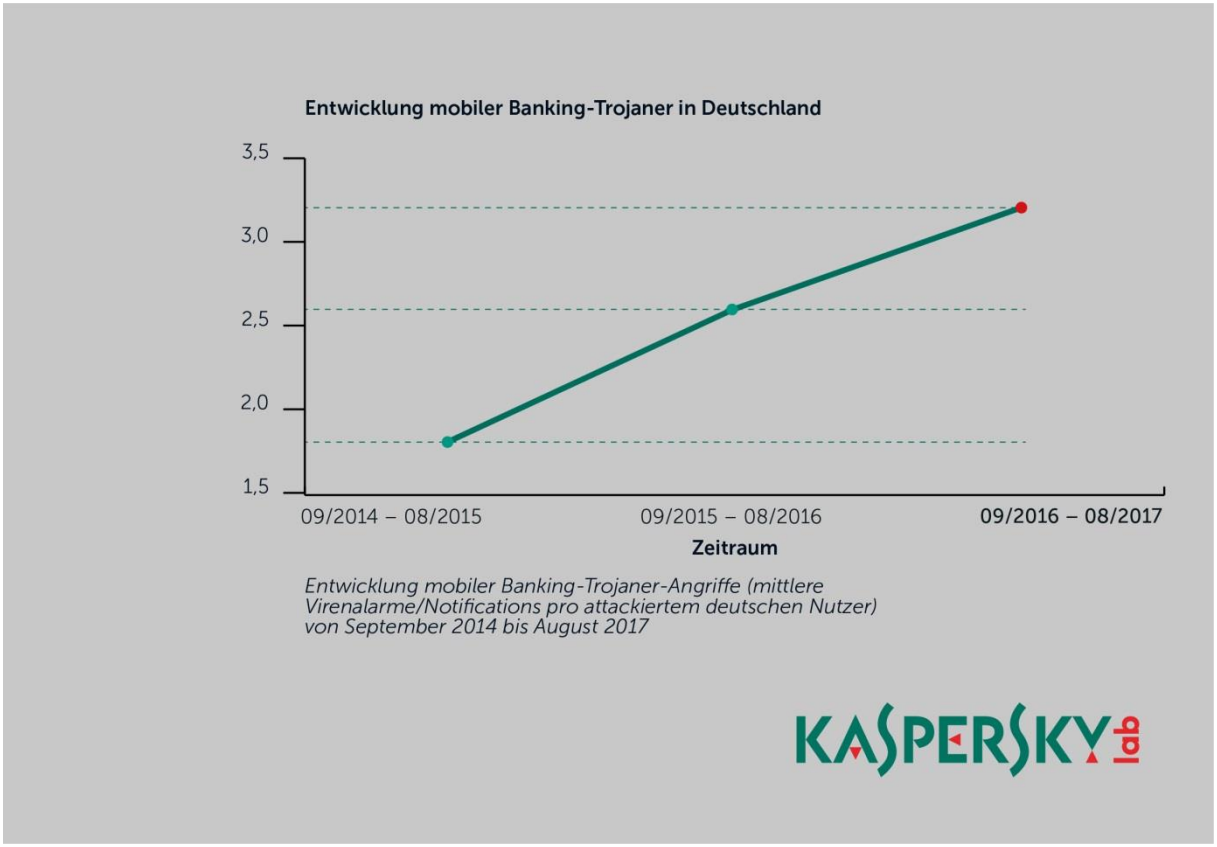
Die Bedrohungssituation in Deutschland: Im Untersuchungszeitraum September 2016 bis August 2017 gab es mehr als eine Million Angriffe auf Nutzer mobiler Kaspersky-Lösungen in Deutschland. Das entspricht einer Zunahme von über 70 Prozent gegenüber dem Vorjahreszeitraum (September 2015 bis August 2016); und einer Steigerung von über 240 Prozent im Vergleich zu zwei Jahren zuvor (September 2014 bis August 2015).

Die folgende Grafik 1 bezieht sich auf die von Kaspersky Lab durchschnittlich gemessenen Angriffsversuche gegen Android bei deutschen Smartphone- und Tablet-Nutzern. Auch hier verzeichnet Kaspersky Lab einen kontinuierlichen Anstieg – von 3,6 Schädlingsalarmen (Notifications), die zwischen September 2014 und August 2015 durchschnittlich bei den Nutzern mobiler Kaspersky-Lösungen registriert wurden, über 5,2 (September 2015 bis August 2016) auf

6,1 zwischen September 2016 und August 2017. In Grafik 2 wird dieselbe Methodik in Bezug auf Angriffe durch mobile Banking-Trojaner angewendet.



Grafik 1: Entwicklung mobiler Angriffe (mittlere Virenalarme/Notifications pro attackiertem deutschen Nutzer mobiler Kaspersky-Lösungen) in Deutschland von September 2014 bis August 2017



Grafik 2: Entwicklung mobiler Banking-Trojaner-Angriffe (mittlere Virenalarme/Notifications pro attackiertem deutschen Nutzer) von September 2014 bis August 2017

Trend 1 – mehr Angriffe generell: Im mobilen Bereich ist die Gesamtzahl der Attacken gegen deutsche Nutzer seit September 2014 bis August 2017 um 240 Prozent angestiegen. Auch die durchschnittlichen Virenalarme/Notifications, die auf die attackierten Nutzer mobiler Kaspersky-Lösungen entfallen, sind signifikant gestiegen – seit September 2014 um mehr als 68 Prozent.

Trend 2 – mehr Angriffe auf Finanzdaten: Im Untersuchungszeitraum September 2014 bis August 2017 nahmen ebenfalls die Angriffe durch mobile Banking-Trojaner – auch hier die durchschnittlichen Virenalarme (Notifications) pro attackiertem Nutzer – in Deutschland signifikant zu: von 1,8 (September 2014 bis August 2015) auf 3,2 (September 2016 auf August 2017) und damit um 77,8 Prozent.

IT-Sicherheitsexperte Christian Funk: *„Mobile Banking-Trojaner haben es auf Finanzdaten wie Kreditkarteninformationen oder Zugänge zu Banking-Accounts, insbesondere Online-Payment-Systemen, abgesehen. Bei zunehmender Nutzung sensibler Transaktionen über Smartphones und Tablets müssen wir auch mit einer Zunahme von mobilem Banking-Betrug in Deutschland rechnen. Schon jetzt Grund genug, zusätzliche Sicherheitsmerkmale wie Zwei-Faktor Authentifizierung zu nutzen."*

Wahrnehmung der deutschen Nutzer: Befragt man die deutschen Nutzer selbst nach den für sie größten mobilen Cybergefahren (Mehrfachnennungen waren möglich, 500 Befragte) ergibt sich folgende Top-3:

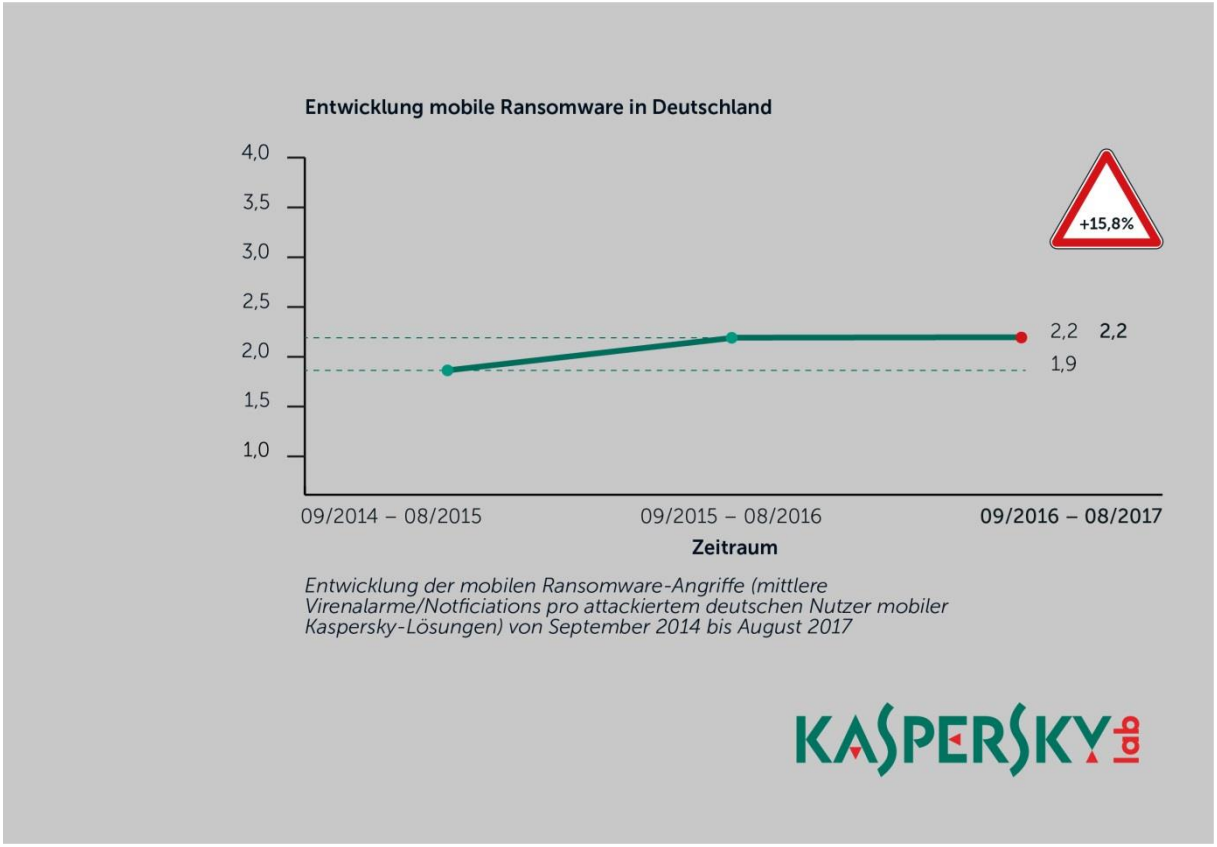
1. Mobile Schadprogramme wie Viren oder Trojaner (65,8 Prozent)
2. Phishing (53,6 Prozent)
3. Heimlicher Datenklau (48,2 Prozent)

Im Übrigen sind laut der Kaspersky-Umfrage 68 Prozent der deutschen Nutzer der Meinung, von ihrem primär genutzten Smartphone oder Tablet seien bisher noch keine Daten gestohlen worden.

ERPRESSUNG

Die Umfrage unter mobilen Nutzern in Deutschland zeigt außerdem, dass jeder Dritte (33,4 Prozent) mobile Ransomware-Programme (also Cybererpressung) fürchtet.

Trend: Nach den Zahlen von Kaspersky Lab ging die durchschnittliche Anzahl der Alarme (Notifications) durch Ransomware auf den Geräten mobiler Kaspersky-Lösungen pro Jahr von September 2014 bis August 2017 um 15,8 Prozent nach oben (von 1,9 auf 2,2 mittlere Virenalarme pro Kaspersky-Nutzer). Im Vergleich zur Steigerung bei den allgemeinen Attacken durch mobile Schädlinge oder Banking-Trojanern ist die Steigerung im mobilen Ransomware-Bereich weniger signifikant, doch sind die genutzten Erpresserprogramme mittlerweile besonders raffiniert.



Grafik 3: Entwicklung mobiler Ransomware-Angriffe (mittlere Virenalarme/Notficiations pro attackiertem deutschen Nutzer mobiler Kaspersky-Lösungen) von September 2014 bis August 2017

Fusob in Deutschland aktiv: Der Ransomware-Schädling Fusob ist in Deutschland besonders aktiv. Die Variante „Trojan-Ransom.AndroidOS.Fusob.h“ wurde bei 11,61 Prozent der in Deutschland mobil attackierten Kaspersky-Nutzer im Untersuchungszeitraum September 2016 bis August 2017 registriert und abgewehrt, wenn man sich das Angriffsaufkommen der Top-20 der mobilen Malware (ohne Adware und Riskware) in Deutschland ansieht (mehr zu Fusob siehe unten).

Christian Funk bestätigt den Trend hin zu mehr Qualität: *„Auch im mobilen Bereich gibt es Ransomware. Die Qualität der Schädlinge hat sich stark verbessert. Versionen wie Fusob und Svpeng holen mit großen Schritten zu ihren Verwandten im PC- und Mac-Bereich auf und grassieren auch in Deutschland.“*

Ein großes Problem beim Thema Erpressung: Laut Kaspersky-Umfrage führen 40,6 Prozent Backups ihrer mobilen Daten (Fotos, Musik, Kontakte, Dokumente) durch. Ebenso viele (40,6 Prozent) machen jedoch keine Backups der auf ihrem Smartphone oder Tablet gespeicherten Daten. Die übrigen 18,8 Prozent können dazu keine Aussage treffen. Mögliche Konsequenzen: Wenn das Gerät verloren geht, gestohlen wird oder nach einem Ransomware-Befall nicht mehr hergestellt werden kann, sind auch alle dort gespeicherten Daten weg.

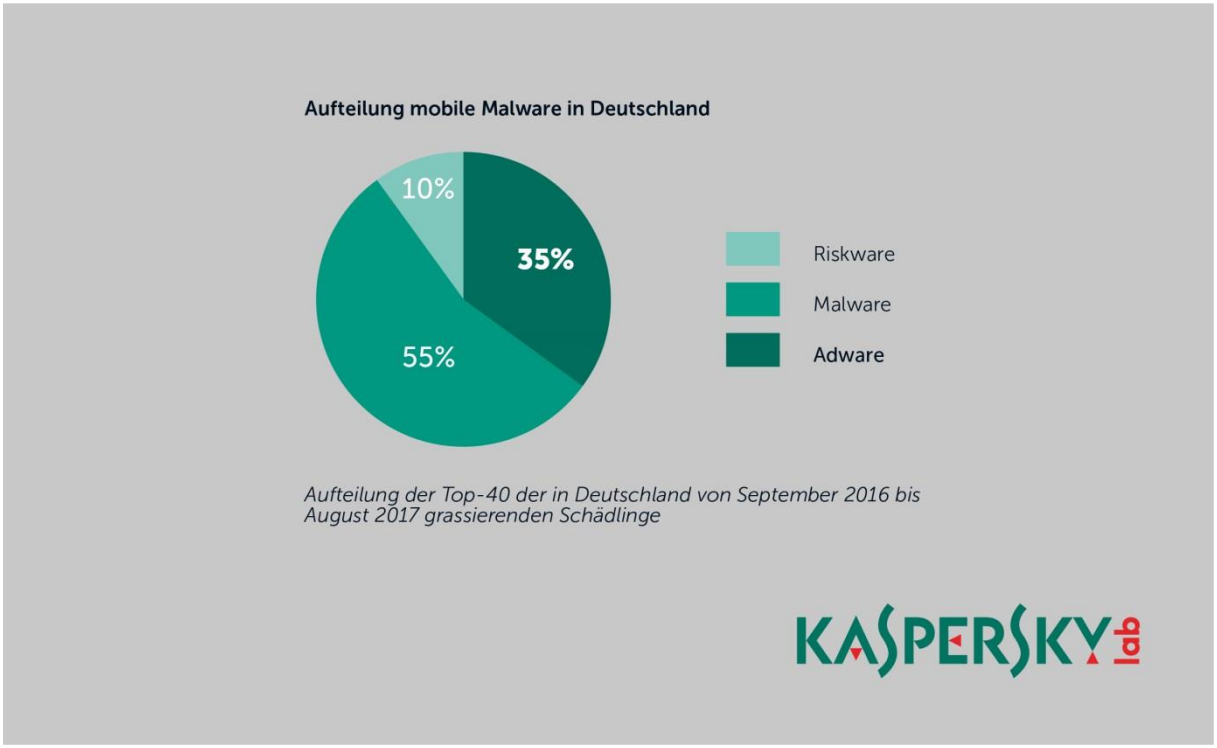
UNERWÜNSCHTE WERBUNG

65,8 Prozent der deutschen Nutzer stören sich laut der Kaspersky-Umfrage zunehmend an unerwünschter Werbung (Adware) auf dem eigenen Smartphone und Tablet.

Das spiegeln auch die Zahlen von Kaspersky Lab zum Aufkommen von Adware-Programmen wieder:

- **Weltweit** kennt Kaspersky Lab über 24 Millionen Adware-Programme.
- Sieht man sich die Top-40-Liste der zwischen September 2016 bis August 2017 grassierenden mobilen Schadprogramme inklusive Adware für **Deutschland** an, können 35 Prozent dem Typ Adware zugeordnet werden.

Christian Funk erklärt: *„Wenn Adware die Nutzer nicht über die Informationserfassung informiert, gilt sie bei Kaspersky Lab als schädlich, weil sie das Verhalten eine Trojaner-Spyware imitiert.“*



Grafik 4: Aufteilung mobiler Malware (nach den Typen Adware, Riskware und Malware); Top-40 für Deutschland von September 2016 bis August 2017

SPIONAGE UND DATENKLAU

Die Experten von Kaspersky Lab kennen derzeit weltweit 840.495 mobile Schädlinge des Typs ‚Trojan Spy' – also Spyware-Programme.

Trend 1 – Auch auf Google Play gibt es mit Malware kompromittierte Apps (APKs): Im Untersuchungszeitraum September 2016 bis August 2017 sahen die Experten von Kaspersky Lab mobile Trojaner (Spyware)[6], die in der Lage sind, Login-Daten zu stehlen, und über kompromittierte Apps in Google Play verbreitet wurden, beispielsweise die Version „Trojan-Spy.AndroidOS.Instealy.a" – ein mobiler Trojaner, der Login-Daten und Passwörter von Instagram-Accounts stehlen kann – oder „Trojan-PSW.AndroidOS.MyVk.a" – ein Schädling, der es auf Zugangsdaten der Social-Networking-Seite VKontakte abgesehen hat.

Trend 2 – SMS immer noch im Visier: Im ersten Quartal 2017 belegte die Kategorie „Spyware-Trojaner"[7] den zweiten Platz, wenn man sich die weltweite Verbreitung der unterschiedlichen mobilen Malware-Arten ansieht. Vor allem die mobilen Malware-Familien „Trojan-Spy.AndroidOS.SmForw" und „Trojan-Spy.AndroidOS.SmsThief" waren hier aktiv – Programme, die es auf den Diebstahl von SMS-Nachrichten abgesehen haben – meist mit dem Ziel, Zwei-Faktor Authentifizierungen auszuhebeln.

Wie denken die Deutschen über mobile Spionage? Die von Kaspersky Lab durchgeführte Umfrage zeigt auch die Skepsis der Deutschen gegenüber Abhör- und Trackingmöglichkeiten mobiler Geräte. So befürchtet die Mehrheit (56,4 Prozent), über das eigene Smartphone oder Tablet von

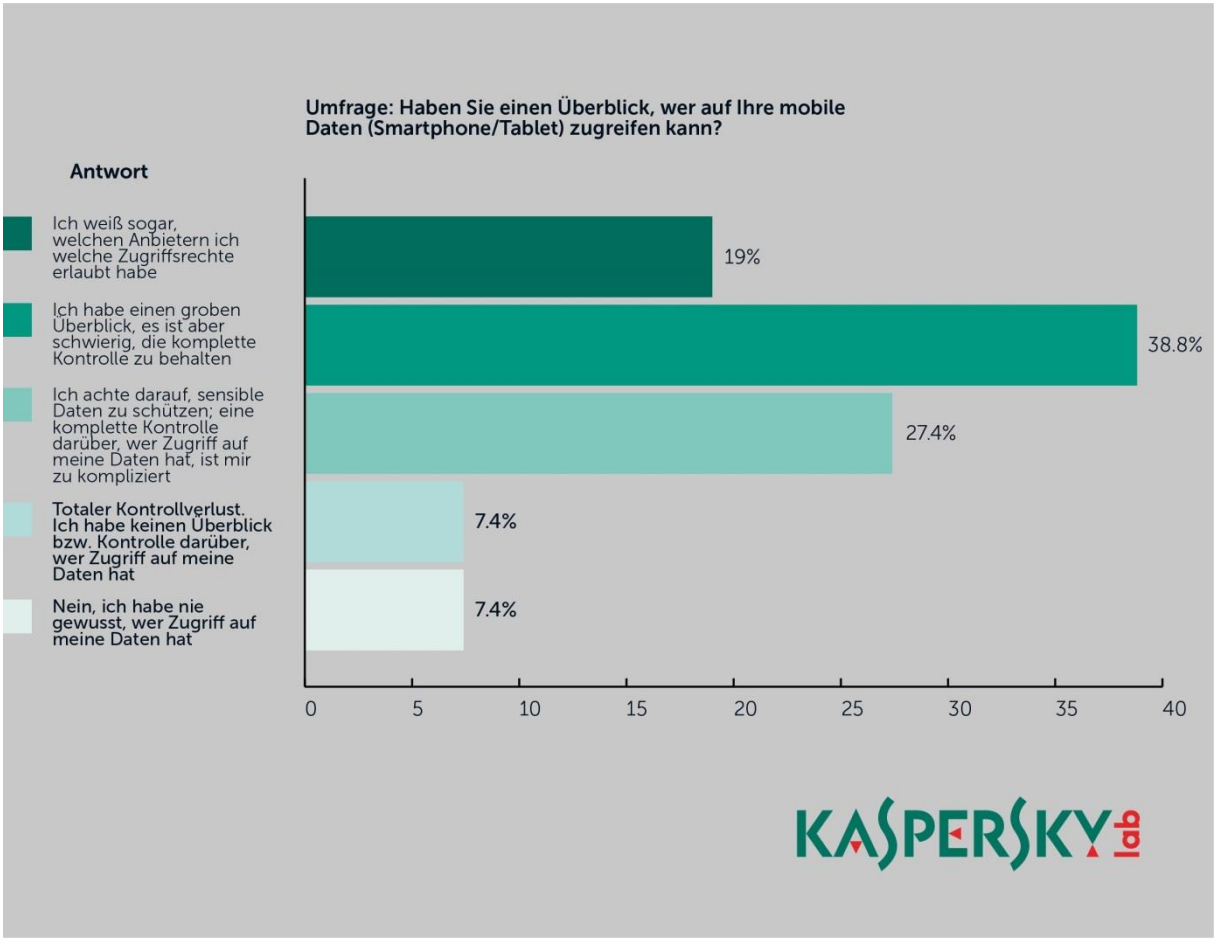
[6] https://securelist.com/mobile-malware-evolution-2016/77681/
[7] https://securelist.com/it-threat-evolution-q1-2017-statistics/78475/

anderen ausspioniert werden zu können. Zudem haben 40,8 Prozent Angst davor, dass Hacker oder andere Unbefugte ihr Smartphone oder Tablet in eine Wanze umfunktionieren.

Wer hat alles meine Daten? Interessant wird es auch, wenn man sich die Ergebnisse zu folgender Frage ansieht: „Haben Sie einen Überblick beziehungsweise die Kontrolle darüber, wer alles auf Ihre mobilen Daten (Smartphone/Tablet) zugreifen kann?“.

Demnach glaubt etwa nur jeder Fünfte (19 Prozent), noch volle Kontrolle über erteilte Zugriffsrechte zu besitzen. Zwei Drittel (66,2 Prozent) geben jedoch an, dass es ihnen trotz aller Bemühungen schwer falle oder schlicht unmöglich sei, hier den vollständigen Überblick zu behalten. Und 14,8 Prozent haben die Kontrolle über erteilte Zugriffsrechte vollständig verloren beziehungsweise noch nie besessen (siehe auch Grafik 5).

Christian Funk erklärt: *„Die Erteilung von Zugriffsrechten ist oftmals eine der Voraussetzungen für die erfolgreiche Infektion mit mobiler Malware bei der Installation einer legitim erscheinenden App – bei der Erfragung von Geräteadministrator-Rechten sollten immer die Alarmglocken schrillen und die Vertrauenswürdigkeit der App sowie der Quelle überprüft werden.“*



Grafik 5: Kaspersky-Umfrage unter 500 deutschen Smartphone- und/oder Tablet-Nutzern, ob sie einen Überblick darüber haben, wer Zugriff auf die mobilen Daten hat

EXKURS: Einfallstore auf mobile Geräte

Laut der von Kaspersky Lab durchgeführten Umfrage lädt die überwiegende Mehrheit (84,6 Prozent) Apps von offiziellen App-Stores (zum Beispiel Google Play, Apple App Store, Microsoft Windows App) herunter. Nur 4,8 Prozent behaupten, Apps von unbekannten Quellen/Seiten herunterzuladen. 4,4 Prozent wissen es nicht genau.

„Vorsicht! Der Download von Apps aus nicht offiziellen Quellen ist der Hauptinfektionsweg für Smartphones und Tablets. Cyberkriminelle tarnen schädliche Installationspakete als populäre Apps im legitim erscheinenden Gewand, um diese so auf mobile Geräte einzuschleusen und anschließend aktiv zu werden“, warnt Christian Funk.

„Pokémon Go“ als Beispiel für die Verbreitung mobiler Schädlinge: Im Jahr 2016 war der Hype um das Mobile-Spiel „Pokémon Go“[8] ungebrochen. Allerdings nutzen auch Cyberkriminelle den Hype für ihre illegalen Machenschaften aus, indem sie Installationsdateien des Spiels (Android Application Package Datei, kurz APK) mit Malware kompromittiert zum App-Download angeboten hatten; nach Installation hatten die Angreifer Zugriff auf das Smartphone.

Nutzungsrechte werden nur überflogen: Wenn es um App-Berechtigungen geht, gehen viele Nutzer in Deutschland allerdings sehr sorglos um. So stimmt weniger als die Hälfte (41,8 Prozent) den von der App eingeforderten Nutzungsrechten erst zu, wenn sie die Berechtigungen gelesen hat. 38,4 Prozent stimmen den angefragten Berechtigungen zu, ohne sie zu lesen. 19,8 Prozent sind unentschlossen.

Christian Funk empfiehlt: „Ab Android 6 können Berechtigungen von Apps individuell verwaltet und geändert werden. Der Vorteil: 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 (20,8 Prozent) aller Befragten in Deutschland sagt, er oder sie habe schon einmal beim eigenen Smartphone oder Tablet die vom Hersteller vorgegebenen Nutzungsbeschränkungen entfernt (also das Gerät gerootet beziehungsweise einen Jailbreak durchgeführt), um zum Beispiel die Systemeinstellungen verändern oder vorinstallierte Apps löschen zu können. 40,4 Prozent haben dies noch nie getan. 38,8 Prozent geben zu, dass sie gar nicht so genau wissen, was mit dem Entfernen von Nutzerbeschränkungen gemeint ist.

WLAN aktiv: Über die Hälfte (55,2 Prozent) der Befragten hat die WLAN-Funktion auf dem Handy durchgehend aktiviert.

Christian Funk resümiert: *„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.“*

[8] http://www.spiegel.de/netzwelt/games/pokemon-go-jetzt-auch-in-deutschland-gestartet-vorerst-nur-fuer-android-a-1102754.html und https://threatpost.com/malicious-pokemon-go-app-installs-backdoor-on-android-devices/119174/

ZWISCHENFAZIT: Mobile Schadprogramme in Deutschland – Panikmache oder echte Gefahr?

Fakt ist, dass es heute mehr Attacken gibt, die es auf mobile Nutzer in Deutschland abgesehen haben, als noch im September 2014 (mit einer Steigerung um 240 Prozent). Zudem hat sich die Qualität deutlich verbessert. Es geht mehr denn je um die Finanzdaten der Nutzer. So werden heute mehr deutsche Smartphone-Nutzer mittels Ransomware-Attacken erpresst; auch die Anzahl mobiler Banking-Trojaner stieg seit September 2014 um 68 Prozent 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, Erpressung sowie Dritte. Das zeigen die Analysedaten von Kaspersky Lab deutlich auf.

Auch wenn man sich das Stimmungsbild unter den Deutschen ansieht, wie sie ihre mobile Nutzung in punkto Sicherheit und Privatsphäre erleben und einschätzen, zeigt sich: die großen Gefahren sind bekannt, allerdings weiß die Mehrheit, dass sie durchaus mehr für die Cybersicherheit ihrer mobilen Geräte tun könnte. Immerhin gab jeder Zehnte (10,4 Prozent) der von Kaspersky Lab befragten Deutschen zu, dass schon einmal Daten von seinem Smartphone oder Tablet abhanden kamen; 21,6 Prozent können dies nicht einschätzen.

Die mobile Cyberbedrohung ist auch in Deutschland real. Mit steigender Nutzung dürfte sie weiter zunehmen. Es gilt, Nutzern zu verdeutlichen, dass das eigene Smartphone der heutige zentrale Computer ist, den es vor Viren, Würmern und Trojanern sowie heimlichen Mitlesern zu schützen gilt. Vor allem, wenn man bedenkt, dass sich Smartphone und Tablet als zentrale Steuerungskonsole für immer mehr intelligente Geräte und Systeme (wie smarte Lautsprecher oder Häuser) etablieren. Auch hier scheint das Sicherheitsbewusstsein der Nutzer vorhanden zu sein: so stimmten 49,6 Prozent der deutschen Befragten der Aussage zu: „Immer mehr smarte Geräte und ständige Verbindung zum Internet machen mein Leben unsicher“.

TEIL 1 – DATENANALYSE

Statistik

Mobile Malware - weltweite Bedrohungssituation

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. Allein im Jahr 2016 waren es 8.526.221 schädliche Installationspakete[9]. Im Jahr 2015 waren es 2.961.727[10].

Von den bei Kaspersky Lab bekannten 5.405.053 einzelnen mobilen Schadcodes haben es 99,88 Prozent auf das Android-Betriebssystem abgesehen. Um die Effizienz und Streuwirkung zu erhöhen, wird in der Regel ein Schadcode in mehrere APK-Dateien implantiert, die dann als Vehikel für die Infizierung eines mobilen Geräts benutzt werden.

[9] https://de.securelist.com/mobile-malware-evolution-2016/72443/
[10] https://de.securelist.com/mobile-malware-evolution-2015/71008/

„Wir sehen in den vergangenen Jahren einen rapiden Anstieg mobiler Schädlinge gegen Android. Kein Wunder, wenn man bedenkt, dass sich die mobile Nutzung des Internets über Smartphones und Co. weltweit etabliert hat. Entsprechend ist auch Malware für mobile Endgeräte endgültig der Kinderstube entwachsen“, sagt Christian Funk.

Exkurs: Wie gefährdet ist iOS?

Für iOS-Geräte existieren nur vereinzelt mobile Schädlinge. Dennoch gibt es Angriffe auf das mobile Betriebssystem von Apple. Dabei handelt es sich zum einen um zielgerichtete und sehr aufwendige Attacken gegen Unternehmen und Organisationen – ein Beispiel hierfür ist die iOS-Spyware Pegasus[11]. Andererseits ist auch der Apple-Normal-Nutzer betroffen. Beispielsweise hat Ende des Jahres 2016 ein Windows-Schädling neben Android- auch iOS-Nutzer angegriffen: der Trojaner „DualToy“[12] war in der Lage, weitere Schädlinge auf iOS-Geräte zu laden und Systemdaten zu exfiltrieren. Auch weitere iOS-basierte Geräte waren betroffen. Ebenfalls im Jahr 2016 konnte in China der Schädling „AceDeceiver“ nicht gejailbreakte iOS-Geräte infizieren[13]. Auch hier lief der Angriff über die Verbindung mit Windows-PCs.

Dank des geschlossenen Ökosystems von Apple sind iOS-Geräte vor Schädlingen besser geschützt als Android-Geräte. Gefährlich wird es aber, wenn Nutzer ihre iOS-Geräte jailbreaken (rooten). Damit ist gemeint, dass Nutzer die vom Hersteller vorgegebenen Nutzungsbeschränkungen bewusst umgehen, um beispielsweise die Systemeinstellungen zu verändern, vorinstallierte Apps löschen oder Apps außerhalb offizieller Pfade installieren zu können.

Bedrohungssituation für Deutschland

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 Prozent gegenüber dem Vorjahreszeitraum (September 2015 bis August 2016); und einer Steigerung von über 240 Prozent im Vergleich zu zwei Jahren zuvor (September 2014 bis August 2015).

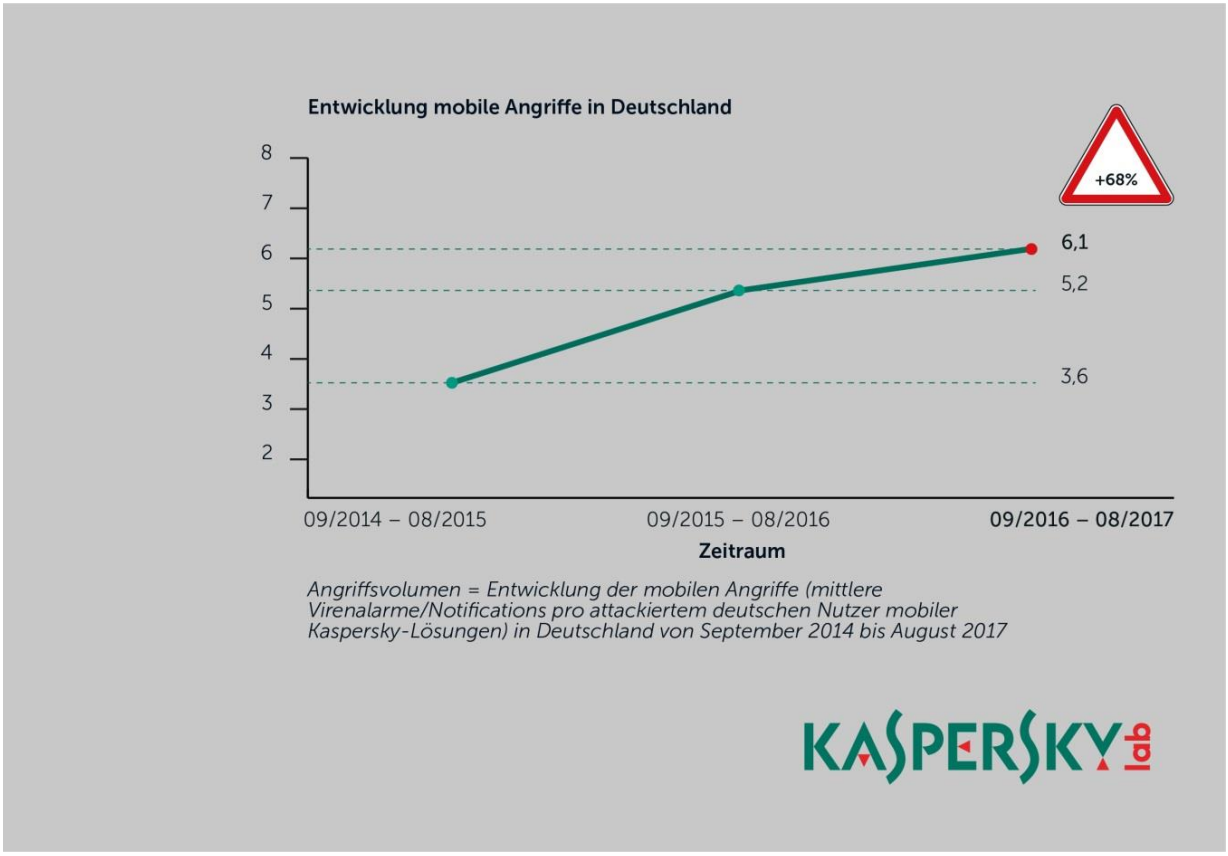
Im Folgenden werden allerdings nicht die Gesamtattacken oder die Anzahl der angegriffenen Nutzer analysiert, sondern die mittleren Schädlingsalarme im jeweiligen Untersuchungszeitraum. Dabei handelt es sich um die durchschnittlichen Virenalarme (Notifications), die auf die attackierten deutschen Nutzer mobiler Kaspersky-Lösungen in den jeweiligen Jahreszeiträumen entfallen.

So verzeichnete Kaspersky Lab 6,1 Schädlingsalarme pro Nutzer im Untersuchungszeitraum September 2016 bis August 2017. Das bedeutet: Mobile Nutzer wurden in Deutschland im Durchschnitt mehr als sechs Mal innerhalb eines Jahres von einem mobilen Schädling attackiert.

Im Zeitraum September 2015 bis August 2016 lag diese Zahl bei 5,2 Alarmen und zwischen September 2014 und August 2015 wurden 3,6 mittlere mobile Schädlingsalarme verzeichnet.

Der Durchschnittswert mobiler Attacken auf deutsche Nutzer ist damit seit September 2014 bis August 2017 um 68 Prozent angestiegen.

[11] https://de.securelist.com/kaspersky-security-bulletin-predictions-for-2017/72225/
[12] https://de.securelist.com/windows-trojaner-dualtoy-greift-android-und-ios-an/72024/
[13] https://de.securelist.com/trojaner-ladt-schadlinge-unter-ausnutzung-eines-bugs-im-drm-auf-ios/71172/



Grafik 6: Entwicklung der mobilen Angriffe (mittlere Virenalarme/Notifications pro attackiertem deutschen Nutzer mobiler Kaspersky-Lösungen) in Deutschland von September 2014 bis August 2017

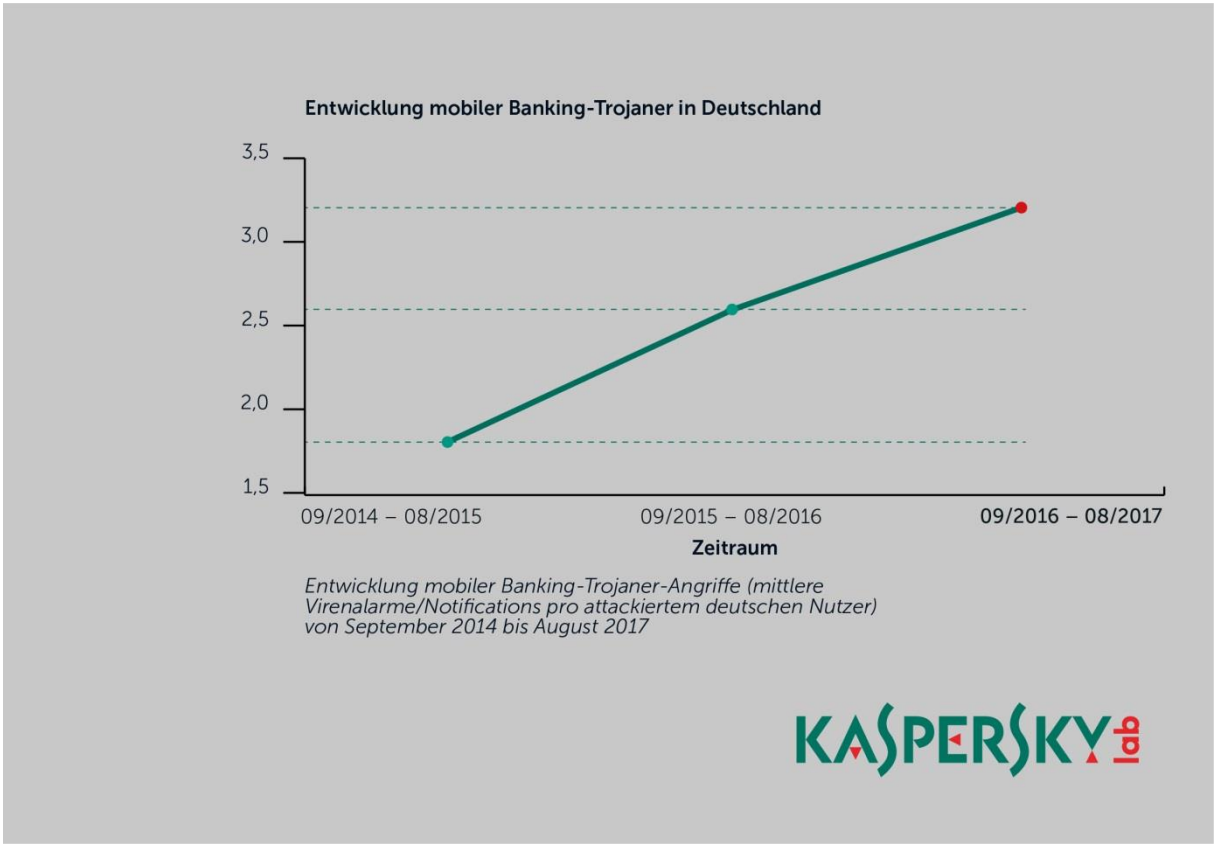
Die Entwicklung im Monatsverlauf: Sieht man sich die mobilen Attacken auf deutsche Nutzer genauer an, lässt sich erkennen, dass vor allem in den Monaten um die Jahreswende 2016/2017 sowie im März die meisten Angriffe stattfanden. Im Sommer, insbesondere im Juni/Juli 2017 gab es in Deutschland dagegen signifikant weniger Angriffe.

Mobile Bank-Trojaner

Online-Banking wird auch in Deutschland mobil. Laut einer Studie des ITK-Branchenverbandes Bitkom[14] hat derzeit mehr als die Hälfte der Smartphone- und Tablet-Nutzer eine App für Mobile-Banking installiert. Besitzer mobiler Geräte werden damit als potenzielle Opfer für Cyberkriminelle zunehmend interessant.

Im Untersuchungszeitraum September 2014 bis August 2017 nahmen die mobilen Banking-Trojaner-Angriffe gegen deutsche Nutzerinnen und Nutzer signifikant zu: Die durchschnittliche Zahl der Angriffe auf deutsche Nutzer mobiler Kaspersky-Lösungen stieg seit September 2014 bis August 2017 von 1,8 auf 3,2 um 77,8 Prozent.

[14] https://www.bitkom.org/Presse/Presseinformation/Mobile-Banking-wird-zum-Standard.html

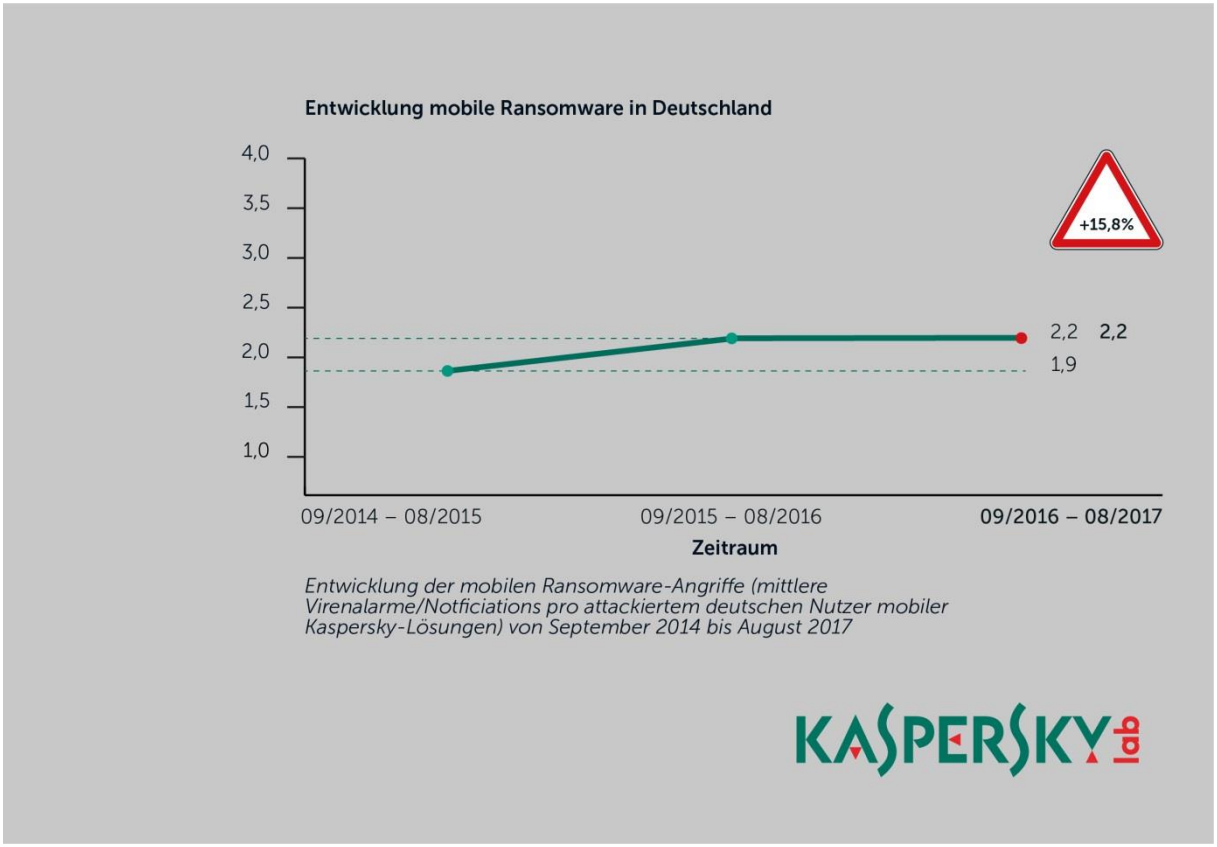


Grafik 7: Entwicklung mobiler Banking-Trojaner-Angriffe (mittlere Virenalarme/Notficiations pro attackiertem deutschen Nutzer mobiler Kaspersky-Lösungen) von September 2014 bis August 2017

Mobile Ransomware

Hinter mobiler Ransomware verbergen sich Erpressungsprogramme, die Geräte sperren oder Daten verschlüsseln können, um im Anschluss für deren Freigabe Lösegeld von den Opfern zu verlangen. Im Gegensatz zur Ransomware, die sich gegen stationäre Rechner richtet, ist der Anteil der gerätesperrenden Schädlinge im mobilen Bereich höher.

Sieht man sich die Entwicklung der durchschnittlichen Virenalarme/Notifications im Bereich Ransomware-Angriffe auf Nutzer mobiler Kaspersky-Lösungen in Deutschland genauer an, zeigt sich im Zeitraum September 2014 bis August 2017 eine Steigerung um 15,8 Prozentpunkte (von 1,9 auf 2,2 mittlere Ransomware-Alarme pro Nutzer im Jahresdurchschnitt). Das ist nur ein kleines Plus im Vergleich zur generellen mobilen Cyberbedrohungssituation. Allerdings nimmt die Qualität der Angriffe zu. Mit den mobilen Erpressern Fusob und Svpeng grassieren auch zwei besonders fortschrittliche Exemplare in Deutschland. Mehr zu Fusob und Svpeng siehe unten.



Grafik 8: Entwicklung mobiler Ransomware-Angriffe (mittlere Virenalarme/Notficiations pro attackiertem deutschen Nutzer mobiler Kaspersky-Lösungen) von September 2014 bis August 2017

Adware

Neben den mobilen Schadprogrammen (Trojaner, Exploits, Spyware, Backdoor und sonstige Schadprogramme) stuft Kaspersky Lab auch Adware und Riskware als gefährlich ein.

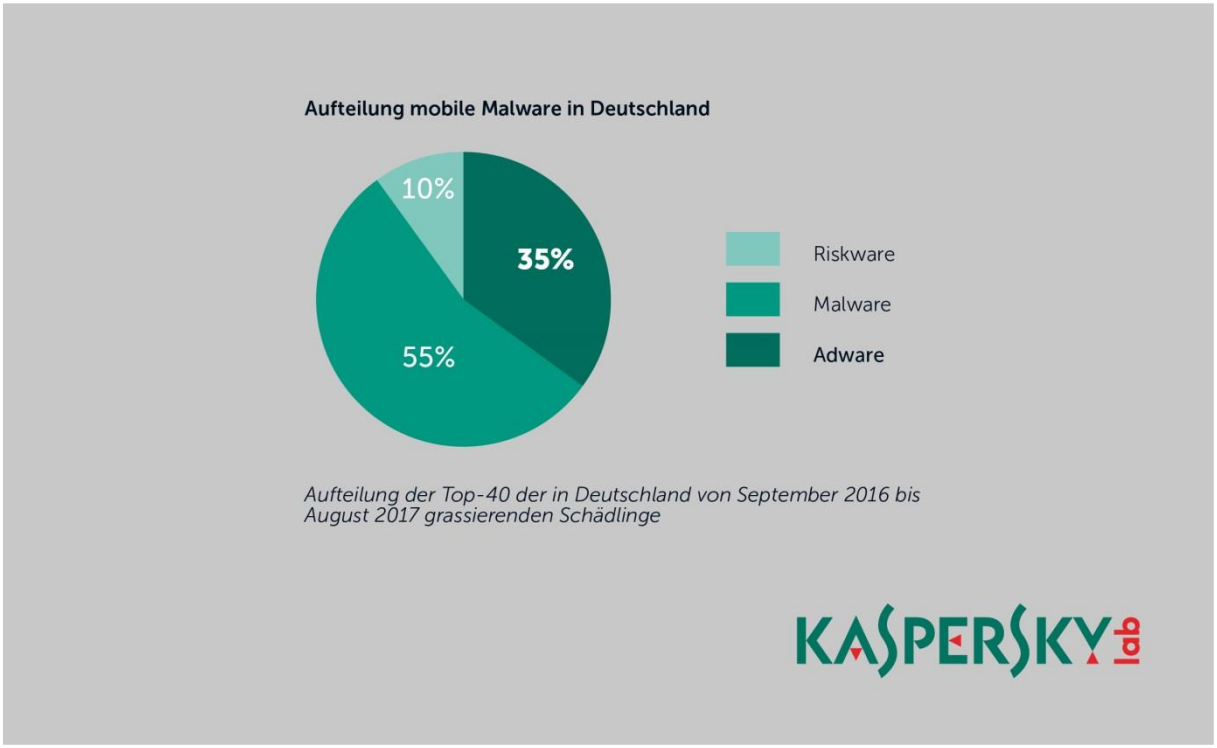
Unter Adware versteht man Programme, die Werbung anzeigen, Suchanfragen an Werbewebseiten umleiten und Marketing-Daten für individuelle Werbung sammeln. Wenn Adware die Nutzer nicht über die Informationserfassung informiert, gilt sie bei Kaspersky Lab als schädlich, weil sie eine Trojaner-Spyware imitiert.

Als Riskware werden legitime Programme bezeichnet, die Schäden anrichten können, wenn sie von Hackern ausgenutzt werden. Zum Beispiel indem sie Daten löschen, blockieren, verändern oder kopieren und die Leistung des Geräts beeinträchtigen. Im Android-Bereich zählt dazu auch ein großer Teil an Tools zum Rooten des Geräts. Diese Tools werden als Riskware eingestuft, weil diese Programme vom Nutzer gewollt oder auch ungewollt zur Ausführung gebracht werden können.

Weltweit kennt Kaspersky Lab über 24 Millionen Adware-Programme.

Sieht man sich die Top-40 der im Zeitraum September 2016 bis August 2017 in **Deutschland** grassierenden mobilen Schädlinge (Malware, Adware und Riskware) genauer an, dann entfallen

- 55 Prozent auf mobile Schädlinge,
- 35 Prozent auf Adware
- und 10 Prozent auf Riskware.



Grafik 9: Aufteilung mobiler Malware (nach den Typen Adware, Riskware und Malware); Top-40 für Deutschland von September 2016 bis August 2017

Die mobilen Schädlinge gegen deutsche Nutzer

Analysiert man ausschließlich die mobilen Schädlinge (ohne Adware und Riskware), die in Deutschland im Untersuchungszeitraum September 2017 bis August 2017 besonders aktiv waren, findet man zu 70 Prozent Trojaner (Ransomware-, Banking-Trojaner, Spionage-Trojaner); der Rest entfällt auf Exploit-Programme, Backdoors oder Hacking-Tools.

DangerousObject.Multi.Generic	70.71%
UFO:Blocked	17.31%
Trojan-Ransom.AndroidOS.Fusob.h	11.61%
Trojan.AndroidOS.Boogr.gsh	7.26%
Trojan.AndroidOS.Hiddad.v	7.02%
Trojan.AndroidOS.Hiddapp.ao	3.39%
Trojan-Ransom.AndroidOS.Fusob.pac	3.07%
Trojan.AndroidOS.Hiddad.ax	3.00%
Trojan-Banker.AndroidOS.Hqwar.jck	2.84%
Trojan-Dropper.AndroidOS.Wroba.san	2.38%

Tabelle 1: Top-10 der mobilen Schädlinge (ohne Adware und Riskware) in Deutschland im Zeitraum September 2016 bis August 2017; Prozentwert: Nutzer mobiler Kaspersky-Lösungen, auf deren Gerät der Schädling registriert wurde

Achtung! In Deutschland sind die folgenden mobilen Schädlinge unterwegs

‚DangerousObject.Multi.Generic' – die große Masse

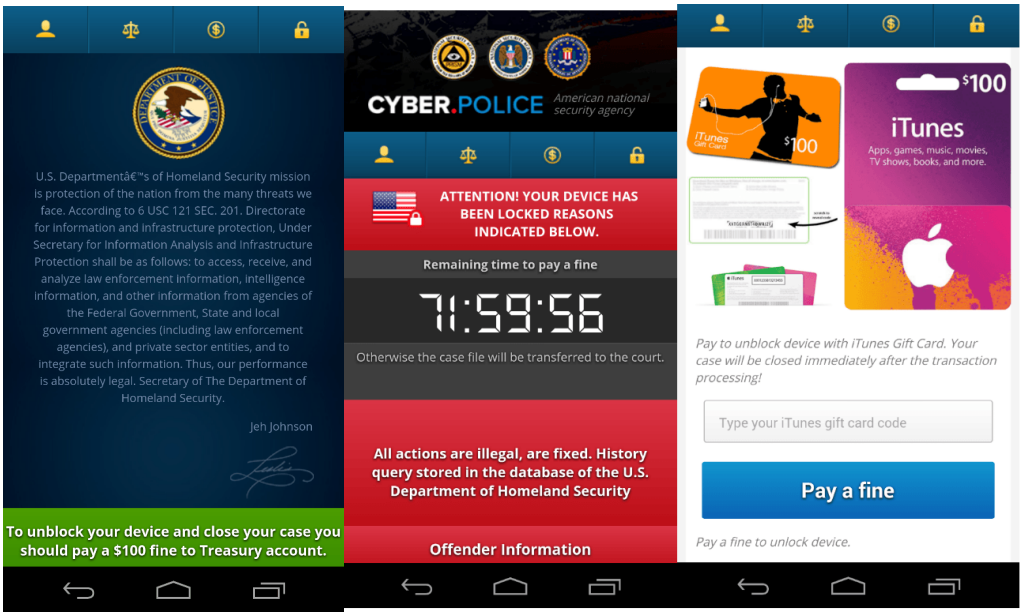
Den ersten Platz der Liste mobiler Schädlinge in Deutschland für den Zeitraum September 2016 bis August 2017 belegen Objekte des Typs „DangerousObject.Multi.Generic". Bei 70,71 Prozent der Nutzer mobiler Kaspersky-Lösungen wurde ein Schädling dieser Kategorie gefunden. Hierbei handelt es sich nicht um eine einzelne Schädlingsversion, sondern um ein ganzes ‚Sammelbecken' an mobiler Malware, das mit Hilfe von Cloud-Technologien aufgespürt wird. Diese Technologie wird genutzt, wenn es in den Antiviren-Datenbanken noch keine Signaturen gibt und auch keine Heuristiken zur Erkennung von Schadprogrammen zur Verfügung stehen. Dann können in der Cloud von Kaspersky Lab bereits Informationen über derartige Objekte abgerufen werden, um einer Infizierung vorzubeugen. Auf diese Weise werden die neuesten Schadprogramme erkannt. Dazu kann alles zählen, was das mobile Schädlingsrepertoire derzeit zu bieten hat: Trojaner, Ransomware, Spyware, Adware und Co.

Fusob – der Erpresser (Trojaner)

Die Schädlingsversion der Fusob-Familie ist eine Ransomware-Variante, die das Gerät seines Opfers sperrt, einen eigenen Bildschirm mit der Lösegeldforderung einblendet und es so unmöglich macht, das Gerät weiter zu nutzen[15]. Die Variante „Trojan-Ransom.AndroidOS.Fusob.h" wurde bei 11,61 Prozent der in Deutschland mobil attackierten Nutzern im Untersuchungszeitraum registriert und von Kaspersky Lab abgewehrt, wenn man sich das Angriffsaufkommen der Top-20 der mobilen Malware (ohne Adware und Riskware) in Deutschland im Untersuchungszeitraum September 2016 und August 2017 ansieht (siehe auch Tabelle 1). Die Version „Trojan-Ransom.AndroidOS.Fusob.pac" wurde im Untersuchungszeitraum bei 3,07 Prozent der mobilen Nutzer in Deutschland registriert und blockiert. Interessant ist, dass dieser Trojaner Nutzer aus Deutschland, den USA und Großbritannien angreift, Anwender aus der GUS (Gemeinschaft Unabhängiger Staaten) und einigen angrenzenden Staaten allerdings meidet, indem er nach dem Start die Systemsprache überprüft, und dann seine Arbeit abbricht[16]. Für das Entsperren fordert der Trojaner ein Lösegeld in Höhe von 100 bis 200 US-Dollar in Form von Codes von Prepaid-iTunes-Karten.

[15] https://kasperskycontenthub.com/securelist-germany/files/2016/02/mobile_vir_2015_de_2.png

[16] https://de.securelist.com/mobile-malware-evolution-2016/72443/



Screenhots: Fenster, die der Erpressungs-Trojaner Fusob öffnet

Boogr – der Superuser-Rechteinhaber (Trojaner)

Der Schädling „Trojan.AndroidOS.Boogr.gsh“ wurde bei 7,26 Prozent der zwischen September 2016 und August 2017 in Deutschland mobil attackierten Nutzer registriert und von Kaspersky Lab abgewehrt (siehe Tabelle 1). Zu dieser Schädlingsversion gehören beispielsweise Trojaner, die den Nutzer bei zahlungspflichtigen Services registrieren, sowie Werbetrojaner, die Superuser-Rechte nutzen[17].

Hiddad – der aggressive Werber (Trojaner)

Der mobile Trojaner verbirgt sich in beliebten Spielen (oftmals für Kinder) oder Programmen. Die Version „Trojan.AndroidOS.Hiddad.v“ wurde bei 7,02 Prozent der zwischen September 2016 und August 2017 in Deutschland mobil attackierten Nutzern registriert (siehe Tabelle 1), die Variante „Trojan.AndroidOS.Hiddadapp.ao“ bei 3,39 Prozent und „Trojan.AndroidOS.Hiddad.ax“ bei 3,0 Prozent der attackierten Nutzer. Interessant ist, dass sich Hiddad[18] nach dem Start auch als die vorgegebene Anwendung (zum Beispiel als Spiel) lädt und installiert. Dabei fordert der Trojaner Administratorenrechte auf dem Gerät an, um zu verhindern, gelöscht zu werden. Das Hauptziel ist das aggressive Anzeigen von Werbung.

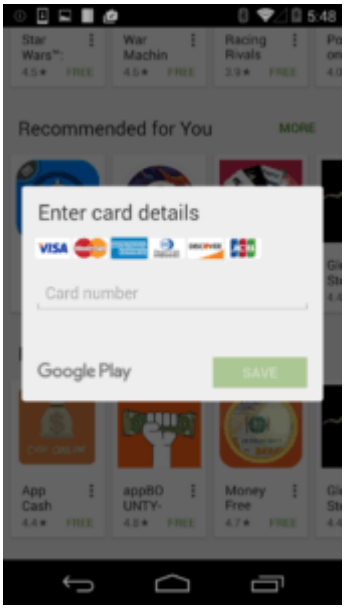
Ausblick – welche Schädlinge auf uns in Zukunft warten könnten

Faketoken – der Wandlungsfähige (Trojaner)

Dieser Trojaner hat viele Gesichter. Ursprünglich griff der mobile Banking-Trojaner – getarnt als Spiele-App oder Adobe Flash – Finanz- und Bankdaten bei Reise- und Hotelbuchungen oder der Zahlung von Verkehrsbußgeldern ab. Auch hatte er sich bereits in Apps versteckt, die in Android

[17] https://de.securelist.com/it-threat-evolution-q2-2017-statistics/72915/b
[18] https://de.securelist.com/it-threat-evolution-q2-2017-statistics/72915/

Play und dem Google Play Market registriert waren. Jüngst hat er es eher auf Nutzer von Taxi- und Mitfahrgelegenheiten-Apps[19] abgesehen.



Screenshot: Phishing-Seite, die Faketoken nutzt, um direkt Kreditkartedaten abzugreifen

„Die neue Version von Faketoken gegen Taxifahrer hat überwiegend russische Nutzer zum Ziel. Dennoch kann sich die Geografie der Attacken schnell ausweiten, so wie es auch bei den Vorgängerversionen von Faketoken und anderer Finanzmalware bereits der Fall war“, warnt in diesem Zusammenhang Christian Funk, Leiter des deutschen Forschungs- und Analyse-Teams bei Kaspersky Lab.

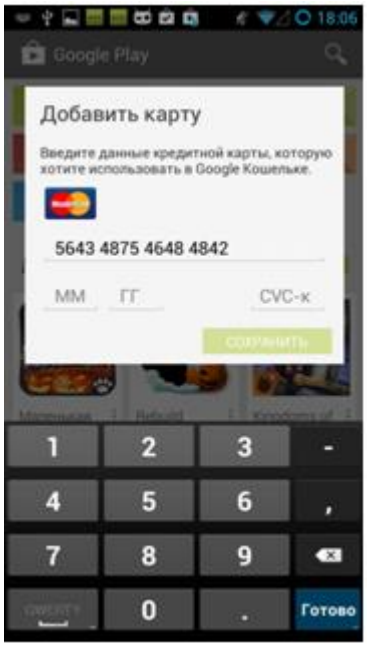
Svpeng – das Schweizer Taschenmesser (Trojaner)

Die aktuelle Version von Svpeng greift mittels Keylogger-Funktion in Smartphones und Tablets eingegebenen Text und damit auch Banking-Zugangsdaten ab, indem die Zugangsdienste von Android missbraucht werden. Zugangsdienste (Accessibility Services) sind Erweiterungen der Benutzeroberfläche, um jene Nutzer, die mit dem Gerät interagieren müssen, zu unterstützen. Der Trojaner wird über gefährliche Webseiten, als Flash-Player-App getarnt, verbreitet und erfragt die Erlaubnis zur Nutzung der Zugangsdienste. Dadurch erhält er Zugriff auf die Benutzeroberfläche anderer Apps und kann so bei Tastendruck Screenshots erstellen und Daten wie Banking-Zugangsdaten mitprotokollieren. Darüber hinaus kann er sich selbst Administratorenrechte für das Gerät verschaffen und andere Apps überdecken. Das hilft dem Trojaner dabei, das Unterbinden der Screenshot-Erstellung durch einige Apps zu umgehen. Im Sommer 2017 war Svpeng[20] auch in Deutschland aktiv.

„Die Svpeng-Malware-Familie ist bekannt für ihre Innovationsfreude und macht sie damit zu einer der interessanten Familien“, erläutert Funk. „Sie war als eine der ersten an Angriffen auf SMS-Banking beteiligt, bei denen Phishing-Webseiten verwendet wurden, um Apps zu überlagern und so Zugangsdaten abzugreifen, um dann die Geräte zu blocken und Geld zu verlangen.“

[19] http://newsroom.kaspersky.eu/de/texte/detail/article/android-trojaner-faketoken-hat-jetzt-taxi-nutzer-im-visier

[20] http://newsroom.kaspersky.eu/de/texte/detail/article/neue-version-von-svpeng-mobiler-banking-trojaner-mit-keylogger-funktion-greift-bankkunden-an



Screenshot: Gefahr Svpeng – vom Anwender eingegebenen Daten werden umgehend an die Cyberkriminellen gesendet

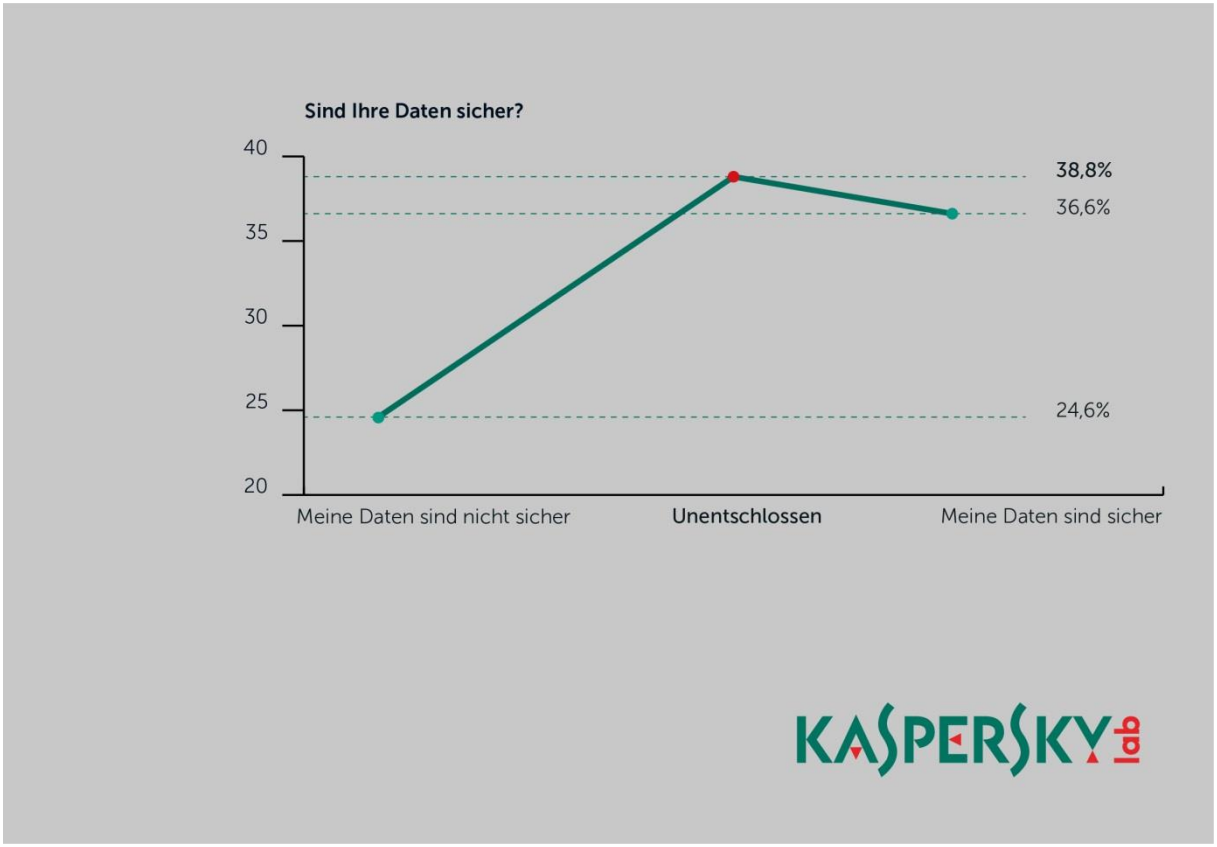
TEIL 2 – UMFRAGE

Die von Kaspersky Lab beauftrage Umfrage unter 500 deutschen Smartphone- und/oder Tablet-Nutzern wurde im August/September 2017 durchgeführt (siehe Methodik). Die Befragung zeichnet ein Bild über die Wahrnehmung mobiler Gefahren, aber auch über das eigene Sicherheitsverhalten mobiler Nutzer in Deutschland.

Datenschutz und Sicherheit

Die Deutschen hätten gerne mehr Datenschutz und sehen in der allgegenwärtigen Vernetzung, auch mit Hinblick auf das Internet der Dinge, eine zunehmende Cybergefährdung für ihren Alltag.

So glaubt nur ein gutes Drittel (36,6 Prozent) der in Deutschland befragten Nutzer mobiler Geräte, dass ihre Daten generell sicher seien. 38,8 Prozent zeigen sich hier unentschlossen und jeder Vierte (24,6 Prozent) meint, seine Daten seien nicht sicher.



Grafik 10: Kaspersky-Umfrage unter 500 deutschen Smartphone- und/oder Tablet-Nutzern, ob ihre Daten sicher sind

Zudem hätten drei von vier Befragten (72 Prozent) gerne mehr Datenschutz.

Fast die Hälfte (49,6 Prozent) stimmt der Aussage zu: „Immer mehr smarte Geräte und ständige Verbindung zum Internet machen mein Leben unsicher“. 29,6 Prozent sind bei dieser Frage unentschlossen und nur 20,6 Prozent widersprechen hier.

Speziell im mobilen Bereich scheinen die Deutschen bereits zu vermuten, dass sie mehr für den Cyberschutz ihrer digitalen Begleiter tun könnten. So haben 66,4 Prozent das Gefühl, sie könnten ihr primär genutztes Smartphone oder Tablet und die darauf befindlichen Daten noch besser schützen.

WLAN und App-Berechtigungen

Wenn es um App-Berechtigungen geht, gehen viele Nutzer in Deutschland damit sehr sorglos um. So stimmen weniger als die Hälfte (41,8 Prozent) den von der App eingeforderten Nutzungsrechten erst zu, wenn sie die Berechtigungen gelesen haben. 38,4 Prozent stimmen den angefragten Berechtigungen zu, ohne sie zu lesen. 19,8 Prozent sind unentschlossen.

Über die Hälfte (55,2 Prozent) hat die WLAN-Funktion auf ihrem Handy durchgehend aktiviert. 32 Prozent nicht und 12,8 Prozent sind unentschlossen.

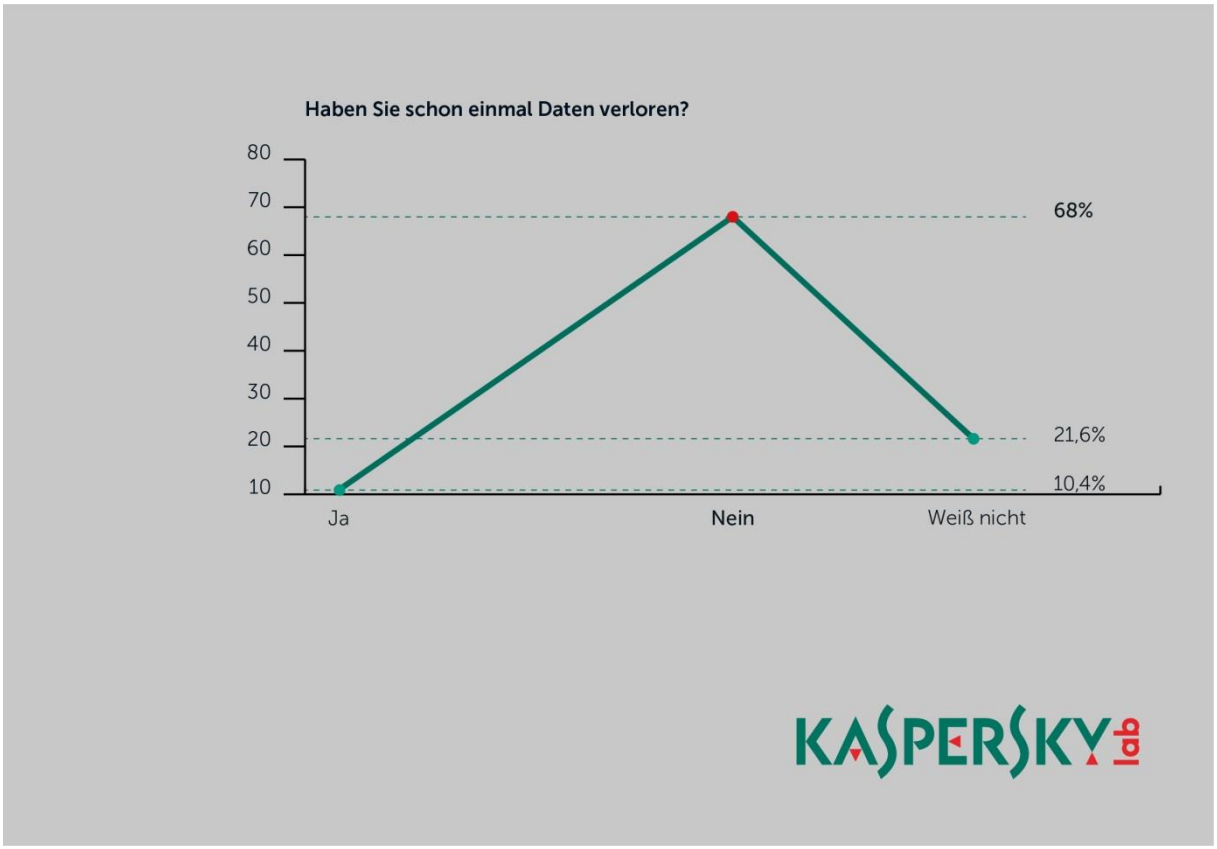
Betrug, Datendiebstahl und Erpressung

68 Prozent der deutschen Befragten sind der Meinung, von ihrem primär genutztem Smartphone oder Tablet seien bisher noch keine Daten gestohlen worden. Das war allerdings bei fast jedem

Zehnten (10,4 Prozent) bereits der Fall. Zudem sagen 21,6 Prozent, dass sie gar nicht in der Lage sind, einzuschätzen, ob bereits Daten von ihren mobilen Geräten gestohlen wurden.

40,6 Prozent machen keine Backups der auf ihrem Smartphone oder Tablet gespeicherten Daten (Fotos, Musik, Kontakte, Dokumente). Das kann schwerwiegende Konsequenzen haben: Wenn das Gerät verloren geht oder gestohlen wird, sind auch alle dort gespeicherten Daten weg – oder können nach einem Ransomware-Befall nicht mehr hergestellt werden.

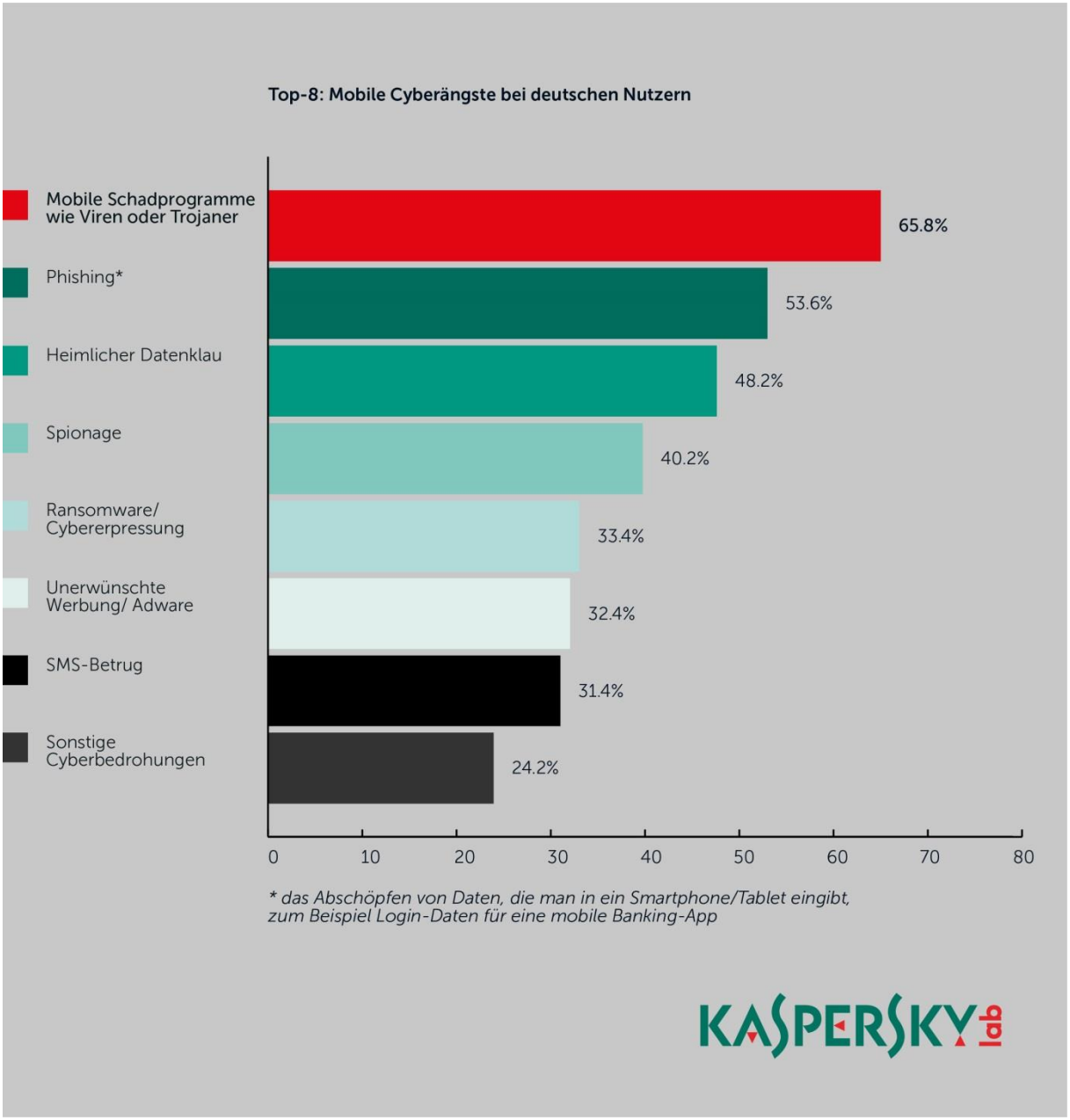
Ebenso viele Befragte (40,6 Prozent) führen dagegen Backups durch.



Grafik 11: Kaspersky-Umfrage unter 500 deutschen Smartphone- und/oder Tablet-Nutzern, ob sie schon einmal Daten verloren haben

Gibt es eine „German Angst“ vor mobilen Cybergefahren?

Die Frage nach den größten Cybergefahren (Mehrfachnennungen waren möglich) ergab folgende Reihenfolge der Antworten:



Grafik 12: Top-8 Cyberängste der deutschen Nutzer

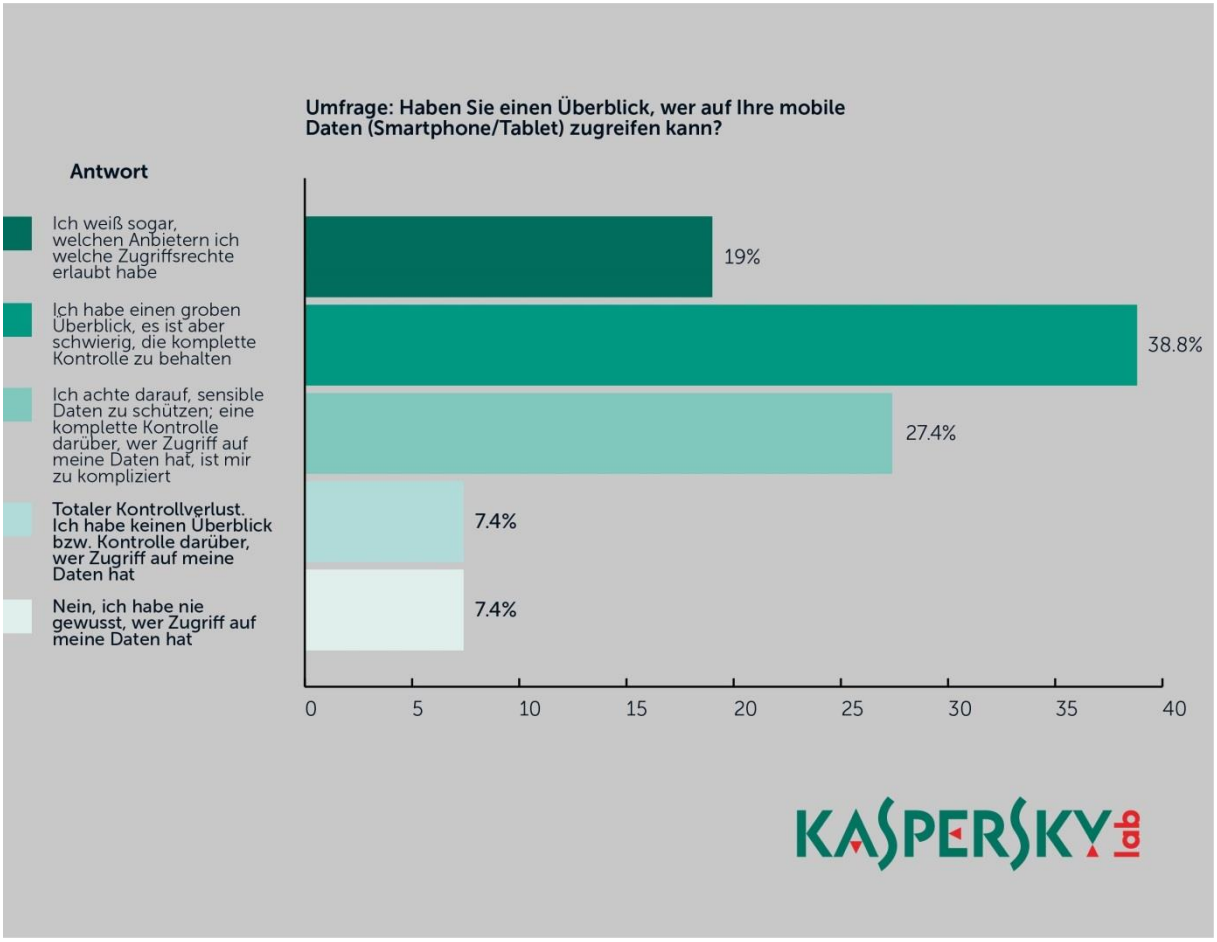
Nur zehn Prozent behaupten, sie hätten überhaupt keine Angst vor mobilen Cyberbedrohungen. Ansonsten fürchten die deutschen Nutzer vor allem mobile Schädlinge, Phishing-Angriffe auf ihre Daten, heimlichen Datenklau sowie Spionage und Erpressung.

Angst vor Spionage

Eine Mehrheit (56,4 Prozent) befürchtet, über das eigene Smartphone oder Tablet von anderen ausspioniert werden zu können.

Zudem haben 40,8 Prozent Angst davor, dass Hacker oder andere Unbefugte ihr Smartphone oder Tablet in eine Wanze umfunktionieren. Knapp ein Drittel (32,2 Prozent) kann sich dazu keine Meinung bilden.

Interessant wird es auch, wenn man sich die Ergebnisse zu folgender Frage ansieht: „Haben Sie einen Überblick beziehungsweise die Kontrolle darüber, wer alles auf Ihre mobilen Daten (Smartphone/Tablet) zugreifen kann?“



Grafik 13: Kaspersky-Umfrage unter 500 deutschen Smartphone- und/oder Tablet-Nutzern, ob sie einen Überblick darüber haben, wer Zugriff auf die mobilen Daten hat

Unerwünschte Werbung (Adware) stört die Nutzer

Die deutschen Nutzer sind sich laut der Kaspersky-Umfrage mehrheitlich einig: 65,8 Prozent stören sich zunehmend an unerwünschter Werbung (Adware) auf dem eigenen Smartphone und Tablet. 19 Prozent sind hier unentschlossen und 14,4 Prozent sind Aktivitäten von Adware egal.

Download von Apps – welche Quellen werden genutzt?

Die überwiegende Mehrheit (84,6 Prozent) lädt Apps von offiziellen App-Stores (zum Beispiel Google Play, Apple App Store, Microsoft Windows App) herunter. Nur 4,8 Prozent behauptet, Apps von unbekannten Quellen/Seiten herunterzuladen beziehungsweise 4,4 Prozent wissen es nicht genau. Weitere Downloadkanäle (Mehrfachnennungen waren möglich) für mobile Nutzer in Deutschland sind: App-Entwickler-Seiten (15,6 Prozent), Telekommunikationsanbieter (17 Prozent), Mobiltelefonanbieter (18 Prozent) oder Downloadcenter (16,8 Prozent).

Rooten von Geräten – wenn Nutzer das eigene Smartphone für Cyberkriminelle aufbrechen

Fast jeder fünfte (20,8 Prozent) der deutschen Befragten sagt, er oder sie habe schon einmal beim eigenen Smartphone/Tablet die vom Hersteller vorgegebenen Nutzungsbeschränkungen

entfernt (also das Gerät gerootet beziehungsweise gejailbreakt), um zum Beispiel die Systemeinstellungen verändern oder vorinstallierte Apps löschen zu können. 40,4 Prozent haben dies noch nie getan. 38,8 Prozent geben zu, dass sie gar nicht genau sagen können, was mit dem Entfernen von Nutzerbeschränkungen gemeint ist.

TEIL 3 – SICHERHEITSTIPPS

DIE BASICS

Auf die Umgebung achten: Wer unterwegs mobile Geräte benutzt, sollte nicht jeden Sitznachbarn in Bahn oder Bus mitlesen lassen. Gleiches gilt natürlich für Telefonate in der Öffentlichkeit. Grundsätzlich ist die mobile Kommunikation nicht abhörsicher. Und selbstverständlich sollte man mobile Geräte niemals unbeaufsichtigt liegen lassen, zumal das auch als Einladung zum Diebstahl verstanden werden könnte.

Gerätesperren nutzen: Die Tasten- beziehungsweise Display-Sperre mobiler Geräte mag für ihre rechtmäßigen Besitzer lästig sein, doch sinnvoll ist sie allemal. Daher nie die PIN-Abfrage der SIM-Karte deaktivieren! PIN- und Passwort-Abfragen sind als Authentifizierung übrigens besser geeignet als der scheinbar so sichere Fingerabdruck-Scan. Denn die passenden Fingerabdrücke des rechtmäßigen Nutzers lassen sich im Zweifelsfall direkt vom Display des Geräts abnehmen. Dass Notizen zu PIN und Passwörtern nichts auf den Geräten oder deren Hüllen zu suchen haben, versteht sich von selbst. Kennwörter und -nummern sollten auch 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: Viele Menschen neigen dazu, ihre mobilen Geräte arglos an Dritte weiterzugeben. Da aber in der Regel dort viele sensible Daten gespeichert sind, sollte man lieber darauf verzichten. Möchte man ein Gerät dauerhaft verschenken, verleihen oder verkaufen, sollten alle Daten explizit gelöscht werden. Das Zurücksetzen auf die Werkseinstellungen reicht hier nicht aus.

Betriebssystem möglichst aktuell halten: Nur die aktuellsten Betriebssysteme sind einigermaßen sicher. Bereits bei der Anschaffung eines Geräts ist daher zu prüfen, ob das Betriebssystem dem neuesten Stand entspricht, und ob der Hersteller Aktualisierungen zulässt oder zukünftig Sicherheits-Updates zur Verfügung stellen will.

Daten regelmäßig sichern: Der beste Schutz gegen Erpressungsversuche mit mobiler Ransomware ist eine aktuelle Sicherungskopie der Daten des mobilen Geräts. Dann laufen Lösegeld-Forderungen ins Leere, wobei man diesen grundsätzlich niemals nachkommen sollte, stattdessen sollte der Fall der Polizei gemeldet werden.

SMS-Dienste sperren: SMS-Betrug ist nach wie vor ein lukratives Geschäftsfeld für Cyberkriminelle. Damit die nächste Mobilfunk-Abrechnung keine unangenehmen Überraschungen bereit hält, weil Trojaner auf dem Smartphone unbemerkt Nachrichten an Premium- oder Abo-Dienste versenden, sollte man entsprechende Dienste vorsorglich bei seinem Mobilfunk-Anbieter sperren lassen.

Geräte niemals „rooten“: Nutzer sollten genau wissen was sie tun, und mit Bedacht Apps installieren sowie ausschließlich 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 dafür unsichere WLAN-Verbindungen nutzen, es sei denn, es wird darüber eine eigene, sichere VPN-Verbindung etabliert. Sensible Daten sollten – wann immer möglich – nur in verschlüsselter Form übertragen werden.

WLAN-, Bluetooth- und Ortungsdienste nur bei Bedarf aktivieren: Die WLAN-, Bluetooth- und Ortungsdienst-Funktion sollte deaktiviert bleiben, solange sie nicht wirklich benötigt wird. So mindert man die Hackbarkeit des Gerätes und schont gleichzeitig noch den Akku.

Sicherheitslösung installieren: Es gibt auch kostenlose, gute Sicherheitslösungen und weitere Tools für mobile Geräte, mit denen sich deren Sicherheit verbessern lässt. Jede dieser Lösungen ist besser, als das Gerät vollkommen ungeschützt zu lassen. Bei der Auswahl sollte man allerdings zu robusten Lösungen greifen. Und es kann sinnvoll sein, für wenige Euro weitere Bequemlichkeiten und zusätzlichen Schutz zu genießen. Informationen zu den anerkannt robusten Sicherheitslösungen und Tools von Kaspersky Lab sind unten in einem eigenen Kapitel aufgelistet.

SICHERER UMGANG MIT APPS

Vorsicht bei der Installation neuer Apps: Mobile Schädlinge gelangen nicht ohne Zutun des Anwenders auf Smartphone und Co. Wer Apps aus dubiosen Quellen und Stores bezieht, darf sich nicht wundern, neben scheinbar sinnvollen Anwendungen oder unterhaltsamen Spielen gleich den passenden Trojaner mitgeliefert zu bekommen. Keinesfalls darf man Apps installieren, die als Anhang oder Link einer E-Mail propagiert werden. Vielmehr sollten Apps grundsätzlich von vertrauenswürdigen Quellen und Entwicklern bezogen werden, also am besten aus den offiziellen App-Stores. Doch Vorsicht: Es haben sich auch in Google Play schon ein paar schwarze Android-Schafe eingeschlichen.

Nicht jede App muss alles können: Besondere Vorsicht ist auch geboten, wenn Apps bestimmte Rechte verlangen. Etwa die Weitergabe von Standort-Daten, Zugriff auf Kontakte oder das Recht zum Versenden von SMS. Hier sollte man kritisch prüfen, ob die gewünschte Anwendung diese Möglichkeiten wirklich benötigt und sie gegebenenfalls ablehnen, beziehungsweise ganz auf die App verzichten. Ab Android 6[21] können Berechtigungen von Apps individuell verwaltet und geändert werden. Der Vorteil: Nutzer können App-Berechtigungen ändern und beispielsweise nachträglich entziehen.

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 erhöt 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 natürlich besonders für sicherheitsrelevante Apps.

App oder Browser, mobil oder stationär? Nicht alles muss immer sofort und überall per App erledigt werden. Gerade bei sehr sensiblen Anwendungen wie Online-Banking oder Bezahlvorgängen sollte sich jeder überlegen, ob er den Vorgang unbedingt via App und Smartphone durchführen muss. Es kann sicherer sein, die Transaktion am gut gesicherten,

[21] https://www.androidpit.de/app-berechtigungen-aendern

heimischen Rechner durchzuführen. Wer unbedingt Finanztransaktionen mit mobilen Geräten erledigen möchte, sollte zumindest auf Zwei-Faktoren-Authentifizierung achten, also zum Beispiel via Passwort und PIN. Das mTAN-Verfahren beim Mobile-Banking muss hinterfragt werden, es sei denn die TAN wird an ein separates Gerät geschickt (etwa ein älteres Einfach-Handy), welches ansonsten nicht zum Online-Banking genutzt wird.

Privatsphäre-Einstellungen beachten: Die am häufigsten genutzten Apps sind wohl die von Sozialen Netzwerken. Damit nicht jede Nachricht, jedes Foto oder Video sofort von aller Welt eingesehen werden kann, sollte man sich vor der Nutzung eingehend mit den Möglichkeiten befassen, die die App zum Schutz der eigenen Privatsphäre bietet.

MOBILE SICHERHEITSLÖSUNGEN

Kaspersky Internet Security for Android[22]: Freemium-Schutz und Komfort gewährt Kaspersky Security for Android. Die App bietet automatische Schadsoftware-Scans für Apps und Gerät sowie Schutz vor Phishing-Seiten und SMS-Links. Bei Smartphones mit bestimmten Android-Versionen können damit zudem unerwünschte Anrufe und SMS unterdrückt und dank Privatsphäre-Modus Kontakte, Anrufe, Nachrichten und Protokolle verborgen werden. Neu ist auch die praktische App-Locker-Funktion für die sichere Nutzung sensibler Anwendungen. Die vielfach ausgezeichnete Sicherheitslösung liefert auch zahlreiche Funktionen, die dem Nutzer im Falle eines Diebstahls oder Verlustes seines Geräts unterstützen.

Und iOS?

Für iOS-Geräte hat Kaspersky Lab zwei weitere, kostenlose Produkte im Angebot.

Der **Kaspersky AdCleaner**[23] blockiert unerwünschte Werbeanzeigen auf iPhone und iPad, schützt die Privatsphäre der Nutzer und sorgt für mehr Geschwindigkeit beim Surfen.

Der ebenfalls kostenlose, über iTunes beziehbare **Kaspersky Safe Browser**[24] erkennt und blockiert Phishing-Webseiten auf iPhones und iPads, warnt vor gefährlichen Links und blockiert Webseiten mit bestimmten unerwünschten Inhalten.

Der kostenlose Kaspersky Safe Browser ist übrigens auch für die Windows-Plattform im Microsoft-Store verfügbar.

Das höchste Maß an plattformübergreifendem Schutz und Komfort für alle stationären und mobilen Geräte der ganzen Familie bietet schließlich die ultimative Lösung **Kaspersky Total Security**[25] – inklusive Passwortverwaltung, mobilem Kinderschutz und Verschlüsselung.

[22] https://www.kaspersky.de/android-security
[23] https://www.kaspersky.de/adcleaner
[24] https://itunes.apple.com/de/app/kaspersky-safe-browser/id723879672?mt=8
[25] https://www.kaspersky.de/total-security