Thematic Insights: Robotik, Schutz und Sicherheit

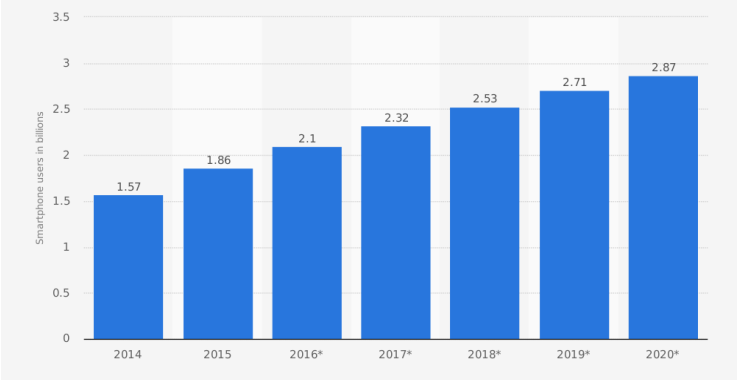
Die Gefahr in Ihrer Tasche

Davide Mascolo, Analyst, Credit Suisse

> ***«App-Stores und Mobile-Apps sind die gefährlichsten Quellen für Schadcode und Malware, die jemals entwickelt wurden»*** [1]
>
> ***Winn Schwartau, Chairman von MobileActiveDefense.com***

Die Anzahl der Menschen, die aktuell Smartphones nutzen, wird auf fast zwei Milliarden geschätzt. Sie soll bis 2020 auf 2,9 Milliarden wachsen, was rund 40 % der Weltbevölkerung entspricht (siehe Abb. 1). Da die Leistungsfähigkeit von Smartphones immer weiter zunimmt, sind sie demzufolge in der Lage, mehr und mehr Funktionen zu erfüllen. Es könnte daher eventuell passieren, dass sie den traditionellen Desktop-PC Schritt für Schritt ablösen werden.

Abbildung 1: Anzahl der weltweiten Smartphone-Nutzer zwischen 2014 und 2020



Quelle: Statista 2017

Ausserhalb der Büronutzung ist das für viele Menschen bereits Alltag. Mit Ihrem Smartphone können Sie kontaktlos für Güter und Dienstleistungen bezahlen, Finanztransaktionen durchführen, zielsicher Ihren Weg durch unbekannte Städte finden und Sprachen übersetzen, die Ihnen nicht vertraut sind. Es kann als Schlüssel für Ihr Hotelzimmer dienen oder Ihre Körperfunktionen überwachen. Es ist Videoplayer, Musikanlage und Spielkonsole zugleich. Und das alles ist nur ein Bruchteil der Funktionen, die es erfüllen kann. Es überrascht also nicht, dass der Markt für Desktop-PCs und Laptops von 363 Millionen verkauften Einheiten im Jahr 2011 auf nur noch 260 Millionen im Jahr 2016[2] geschrumpft ist, was einem dramatischen Umsatzeinbruch von 29 %[3] über diesen 5-Jahres-Zeitraum entspricht.

Neben den Auswirkungen auf die Lebens- und Arbeitsweise von Millionen Menschen ergeben sich durch diese Verschiebung der Nutzung technischer Geräte auch neue Gefahren für die Sicherheit der auf Smartphones gespeicherten vertraulichen Informationen. Aufgrund der zunehmenden Leistungsfähigkeit und Fülle an Funktionen, die sie für uns übernehmen können, speichern wir eine immer grössere Menge persönlicher Informationen, Passwörter und Benutzernamen auf unseren Handys. Das macht sie zum unwiderstehlichen Ziel für Cyberkriminelle, die genau wissen, dass sie – wenn es ihnen erst einmal gelingt, unbefugt auf ein Gerät zuzugreifen – möglicherweise einen wahren Schatz nützlicher Informationen vorfinden werden. Die Tatsache, dass Smartphones ein wesentlicher Bestandteil unseres Lebens geworden sind und dass wir im Alltag stets damit konfrontiert werden, kann dazu führen, dass wir die Gefahren von Cyberangriffen unterschätzen.

Mobile Malware

[1] Quelle: TechNewsWorld «The Ultimate Jailbreaker», 7. September 2010.
URL: http://www.technewsworld.com/story/70769.html?wlc=1283868974

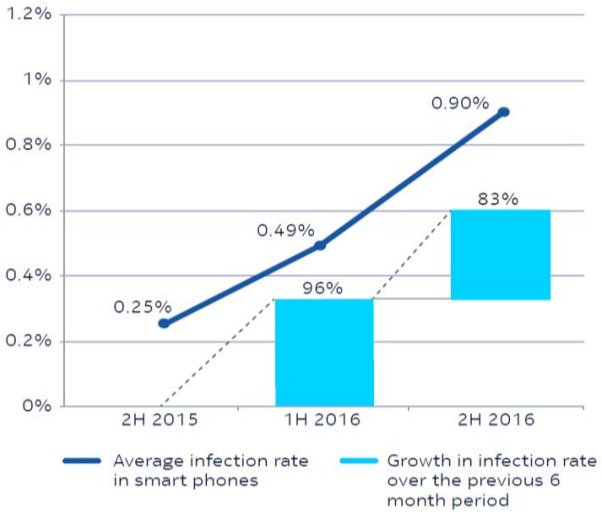
[2] Quelle: Statista (2017): «Shipment forecast of tablets, laptops and desktop PCs worldwide from 2010 to 2021».

[3] Quelle: Bloomberg, Industry Primer «Computer Hardware & Storage».

Dem Threat Intelligence Report von Nokia vom März 2017 zufolge wurden in der zweiten Jahreshälfte 2016 nur 0,9 % aller Smartphones mit Malware infiziert. Obwohl diese Zahl für sich genommen wenig beunruhigend wirkt, markiert sie dennoch einen massiven Anstieg von 83 % im Vergleich zur ersten Jahreshälfte 2016. Diese verzeichnete ihrerseits einen deutlichen Anstieg von 96 % im Vergleich zu dem Halbjahr davor, wo die Infektionsrate noch lediglich 0,25 % betrug.

Abbildung 2 veranschaulicht den rasanten Anstieg der Infektionsrate über den Zeitraum der vergangenen 18 Monate. Schätzungen zufolge sind Smartphones verantwortlich für rund 85 % aller Virus- und Malware-Infektionen in den globalen Mobilnetzwerken.

Abbildung 2: Infektionsrate von Smartphones durch Viren



Quelle: Nokia Threat Intelligence Report, 27. März 2017

Die Tore stehen weit offen

Was ist der Grund für den rasanten Anstieg der Infektionsraten? Da Smartphones immer leistungsfähiger werden und in der Lage sind, zunehmend anspruchsvollere Softwareanwendungen zu unterstützen, bilden ihre schnelleren Prozessoren und umfangreicheren Speicherressourcen sowie das breite Spektrum verwendeter Apps ein sehr viel grösseres und komplexeres Ökosystem, das Hacker nutzen können, um darin Schadcode zu verstreuen. Auch die Anzahl möglicher Zugriffspunkte hat sich stark erhöht. Viele Menschen melden sich in kostenlosen WLAN-Netzwerken an und stellen unbekannten Dritten ihre E-Mail-Adressen oder Telefonnummern zur Verfügung, ohne genau zu wissen, wem der WLAN-Router tatsächlich gehört. Auch öffentliche Ladestationen erlauben skrupellosen Betreibern, auf die Daten unserer Smartphones zuzugreifen, und der Download extern entwickelter Apps eröffnet Cyberkriminellen einen weiteren potenziellen Kanal, um auf unsere Handydaten zuzugreifen.

Ende März 2017 standen Android-Anwendern 2,8 Millionen und Apple-Usern 2,2 Millionen Apps zur Verfügung. Im Jahr davor waren es noch rund 500'000.[4] Bei Milliarden von Smartphone-Nutzern und Millionen von Apps, die nicht selten kostenlos sind oder lediglich ein bis zwei Dollar kosten, überrascht es wenig, dass die Zahl der Apps, die jeden Monat heruntergeladen werden, schwindelerregend hoch ist: Allein für Juni 2016 vermeldete Apple den Download von 130 Milliarden Apps.

Zudem hat Apple den Einstiegspreis für App-Entwickler auf nur noch 99 US-Dollar pro Jahr gesenkt und den hauseigenen App Store damit selbst für den kleinsten Hobbyentwickler erschwinglich gemacht. Dadurch ist die Zahl der verfügbaren Apps erheblich angestiegen, während zeitgleich der Qualitätsstandard erwartungsgemäss gesunken ist – sowohl im Hinblick auf die Apps selbst, als auch auf eingebaute Sicherheitsmerkmale und Verteidigungsmechanismen. Es stellte sich heraus, dass viele Apps, die Benutzerdaten speichern, eine nur sehr schwache Verschlüsselung verwenden.[5]

Angesichts der niedrigen Preise, zu denen Apps auf Smartphones verkauft werden, überrascht es wenig, dass einer Schätzung von Gartner Inc zufolge 2018 vermutlich weniger als 0,01 % aller Verbraucher-Apps ein finanzieller Erfolg sein werden[6]. Diese wirtschaftlich unattraktiven Aussichten bieten Entwicklern wenige Anreize dafür, in wasserdichte Sicherheitsmassnahmen zu investieren. Im Gegensatz dazu ist für PCs entwickelte Software heutzutage oft weitaus profitabler – insbesondere dann, wenn sie in Verbindung mit einem sich automatisch erneuernden Abonnement erworben wird. Diese Softwareprodukte werden in der Regel von renommierten Unternehmen entwickelt, die ihr Markenimage schützen müssen und über eine breite Abonnentenbasis verfügen.

[4] Quelle: Apple Keynote, 13. Juni 2016.

[5] Siehe auch arsTechnica-Artikel (2012): «iOS app success is a ‹lottery›: 60% (or more) of developers don't break even», 5. April 2012. URL: https://arstechnica.com/gadgets/2012/05/ios-app-success-is-a-lottery-and-60-of-developers-dont-break-even/

[6] Quelle: Gartner Inc. Report (2014): «Predicts 2014: Mobile and Wireless».

Für diese Unternehmen ist die Investition in solide Sicherheitsprotokolle ein wesentlicher Bestandteil ihrer Produktentwicklung.

Es ist daher nachvollziehbar, dass niedrige Qualitätsstandards, die wachsende Zahl verfügbarer Apps und die Blauäugigkeit der Benutzer, die sich bei der Speicherung wichtiger Daten blindlings auf ihre Apps verlassen, reiche Jagdgründe für Cyberkriminelle eröffnen.

Pokémon GO

Pokémon GO ist ein kostenloses, standortbasiertes Augmented-Reality-Spiel für iOS- und Android-Geräte, das im Juni 2016 veröffentlicht wurde. Zugleich ist es eines der aktuellsten Beispiele für die Risiken, die wir durch die Nutzung unserer Smartphones jeden Tag unbewusst eingehen.

Nur wenige Stunden nach der Veröffentlichung von Pokémon GO fand das Threat Intelligence Lab von Nokia zahlreiche, mit Malware infizierte Klone des Spiels in regionalen App-Stores. Für Endbenutzer war es nahezu unmöglich, die Malware aufzuspüren, da sich die geklonte, infizierte App praktisch genau so verhielt wie das tatsächliche Spiel. Die in diesem Fall bestehenden Risiken wurden durch die Tatsache noch erschwert, dass das Spiel ursprünglich nur in den USA, Australien und Neuseeland veröffentlicht worden war. Dies führte dazu, dass Pokémon-Fans in anderen Ländern sich in ihren regionalen App-Stores auf die Suche nach dem Spiel machten, in dem sie jedoch nur die infizierten Klone finden konnten.

Diese App war schon allein aufgrund der Tatsache umstritten, dass in ihrer ersten Version das Spielen nur möglich war, nachdem man eine Vereinbarung unterzeichnet hatte, in der man den vollen Zugriff auf die Daten des eigenen Google-Kontos gewährte. Dadurch eröffnete sich die Möglichkeit, diese Informationen beliebig zu manipulieren. Der Schöpfer der App meinte dazu, dass *«der Kontoerstellungsprozess von Pokémon GO für iOS fälschlicherweise nach dem vollen Zugriff auf das Google-Konto des Benutzers frage. Dabei greift Pokémon GO aber nur auf grundlegende Daten des Google-Profils zu (genauer gesagt, auf die Benutzererkennung und die E-Mail-Adresse). Es erhält keinen Zugriff auf andere Google-Kontoinformationen und fragt diese auch nicht ab.»*

Quelle: Nokia Threat Intelligence Report, 27. März 2017

Fazit

Da Mobilgeräte in ihrer Funktion als Unterhaltungsmedium, Mittel zur Komfort- und Effizienzsteigerung und Kontaktpunkt zur Verknüpfung mit Familienmitgliedern und Freunden eine zunehmend wichtige Rolle im Leben vieler Leute spielen, ist es wahrscheinlich, dass sie künftig immer stärker ins Visier von Cyberangriffen rücken werden.

Die Bedrohung beschränkt sich dabei nicht auf den persönlichen Bereich, in dem Cyberkriminelle Daten abschöpfen, das Nutzerverhalten überwachen, Textnachrichten versenden, Telefonanrufe tätigen und Bankdaten stehlen können. Die bereits stark verbreitete «Bring Your Own Device»-Politik in vielen Unternehmen erhöht die Bedrohungslage über den persönlichen Raum hinaus und stellt Unternehmen vor neue Probleme. Laut einer Umfrage von IDG Research Services[7] gaben 74 % aller befragten Unternehmen an, dass es bereits zu Datenschutzverletzungen aufgrund der mangelnden Sicherheit von Mobilgeräten gekommen sei. Die Hauptursachen dafür waren Malware in Mobile-Apps, Apps mit Sicherheitslücken und unsichere WLAN-Verbindungen.

Es macht daher definitiv Sinn, dass Einzelpersonen, Unternehmen und möglicherweise auch staatliche Akteure sich für bessere Datensicherheit einsetzen sollten, um solchen Risiken mit möglicherweise sehr weitreichenden Folgen vorzubeugen. Vielen scheint bereits bewusst zu sein, dass die Sicherheit für die mobile Kommunikation noch mehr in den Fokus rücken muss. Tatsächlich geniessen Investitionen in mobile und Endpunktsicherheit in den kommenden 12 Monaten für 90 % der von IDG befragten Unternehmen die höchste Priorität. Trotz einiger Ähnlichkeiten zwischen der PC-Sicherheit und der mobilen Sicherheit müssen Unternehmen sich über die Eigenheiten der Bedrohungen aus dem mobilen Bereich im Klaren sein: verstehen, dass diese spezifische Sicherheitsrahmenbedingungen erfordern und nicht einfach durch eine Überarbeitung der bestehenden Risikomanagement-Strategie entschärft werden können. Der zunehmenden Komplexität der mobilen Cybersicherheit kann durch die steigende Leistungsfähigkeit des maschinellen Lernens und durch künstliche

[7]Siehe auch das bei Lookout erhältliche IDG-White-Paper «IT Leaders Buying into Mobile Security»

Intelligenz (KI) möglicherweise entgegengewirkt werden. Diese Technologien bieten Potenzial für intelligentere Sicherheitslösungen und Überwachungssysteme.

Auch Einzelpersonen müssen verantwortungsvoller mit dem Thema umgehen. Wir alle profitieren von den Vorteilen und Annehmlichkeiten unserer Smartphones. Doch vielleicht sollten wir diesen Geräten mit etwas mehr Respekt begegnen. Letztendlich führen wir nämlich ein Gerät mit uns, das ständig eingeschaltet ist und unter Umständen ohne unser Wissen vertrauliche Informationen an unbekannte Personen weitergibt. Der allererste Schritt zur Reduzierung der Risiken ist es, bei der Bevölkerung ein Bewusstsein für die Gefahren zu schaffen, die Smartphones mit sich bringen.

Erfahren Sie mehr zu unseren thematischen Aktienanlagen.

CREDIT SUISSE (DEUTSCHLAND) AKTIENGESELLSCHAFT
Taunustor 1
D-60310 Frankfurt am Main

Service-Line:
Telefon: +49 (0) 69 7538 1111
Telefax: +49 (0) 69 7538 1796
E-Mail: investment.fonds@credit-suisse.com