SocietyByte
Wissenschaftsmagazin des BFH-Zentrums Digital Society
https://www.societybyte.swiss

Unsicheres Smartphone und warum wir es trotzdem fürs Bezahlen verwenden...

Autoren : Reto E. Koenig, Gerhard Hassenstein

Datum : 28. Juli 2017

Irgendwie wissen wir es, aber durch die vollmundigen Anpreisungen und einer Unmenge von 'sicheren' Apps, mit welchen viele Unternehmen uns umgarnen, schlagen wir unsere Bedenken bezüglich der verlangten Sicherheit an das Smartphone in den Wind. So bleibt uns nur der subjektive Eindruck: "Das muss ja sicher sein…“

Aber wie steht es wirklich um die Sicherheit von mobilen Anwendungen, die von Unternehmen, wie Banken, Versicherungen, Telekommunikationsanbieter, Transportwesen angeboten werden? Der nachfolgende Text soll Denkanstösse über die objektive Sicherheit von Smartphone-Apps geben.

Was ist eigentlich „Sicherheit“?

Die etwas sperrige aber übliche Definition von 'Sicherheit' besagt, "dass das grundsätzliche Ziel einer sicheren Lösung in der Informatik die korrekte Verwaltung eines virtualisierten Gutes

(engl. "Asset") nach Willen des Eigners ist. Kein Dritter soll sich an den Gütern in irgendeiner Form bereichern können, ohne dass dies der Wille des Eigners ist". Diese Beschreibung erscheint wie selbstverständlich in einer perfekten Welt, in der es keine "Böses-im-Sinn-habenden Personengruppen" (= Angreifer) gibt. In der realen Welt aber erzeugt der Besitz von Gütern ein Begehren durch Dritte. Je grösser der Wert der verwalteten Güter, desto stärker wird dieses Begehren, welches so lange auf die Schwächen der angebotenen Lösung einwirkt, bis über den schwächsten Punkt ein Angriff erfolgt. Zwei scheinbar unabhängige Beispiele untermauern das:

- Die sichere Lösung beim E-Banking garantiert die korrekte und fehlerfreie Verwaltung des monetären Vermögens des Kunden. Das Ziel des Angreifers ist demnach, sich am Vermögen der Kunden unberechtigt zu bereichern.
- Eine sichere Lösung im E-Health (Verwaltung von Patientendaten) garantiert die korrekte und fehlerfreie Verwahrung der Vitaldaten, sowie die gezielte Bekanntgabe von privaten Daten an Dritte (sofern vom Patienten erwünscht). Das Ziel des Angreifers ist das Erlangen des Wissens bzgl. der Vitaldaten oder sogar deren fatale Manipulation im eigenen Interesse.

Unsichere Kommunikationskanäle

Durch die vollmundigen Versprechen der einzelnen Unternehmen ist man geneigt zu akzeptieren, dass eine gut geschriebene und fehlerlose App dem Druck eines Angreifers standhalten kann und man so sicherheitskritische Aktionen auf dem Smartphone durchführen darf. Doch genau das ist nicht der Fall. Betrachten wir dazu den unwahrscheinlichen Fall, dass ein Unternehmen eine 100% fehlerfreie Lösung bereitstellt, welche sie als App ihren Kunden zur Verfügung stellt und lassen diese auf einem beliebigen Smartphone laufen. Auch in diesem Falle muss die App für die Kommunikation mit dem Menschen zwei Kanäle anbieten:

- Der Ausgabekanal zum Benutzer, damit dieser die Verwaltung der Daten (z.B. Geld oder Vitaldaten) einsehen kann und zudem erkennen kann, welche Aktionen die Sicherheitslösung damit ermöglicht. Dafür wird typischerweise das Display des Smartphones genutzt.
- Der Eingabekanal zur Sicherheitslösung, damit diese die Anweisungen des Benutzers verstehen und ausführen kann. Eingaben werden zumeist über den Touchscreen realisiert.

Es sind aber genau diese beiden Kanäle, welche durch das Smartphone in keiner Weise abgesichert werden können. Dieser "Showstopper" gilt nicht nur für Smartphones im Speziellen, sondern auch für PC, Notebooks etc. Der Benutzer kann sich nie sicher sein, ob er der Ausgabe des Displays vertrauen kann, da eine böswillige App des Angreifers (= Malware) die Ausgabe der App auf dem Display überlagern kann (= Overlay-Attack). Aus der Ausgabe für ein 'Nein' wird so plötzlich ein 'Ja', ein falscher Empfänger für eine Transaktion wird durch den vermeintlich richtigen Empfänger ersetzt. Ähnliches gilt für die Eingaben, welche der Benutzer tätigt. Obwohl der Benutzer beispielsweise die Passworteingabe nur der richtigen App überlassen will, wird diese notgedrungen auch gleich der Tastatur-App mitgeteilt, welche möglicherweise vom Angreifer kontrolliert wird. Auch hier ist wieder ein Angriffspotenzial

vorhanden, welches weder vom System noch vom Benutzer erkannt werden kann.

Offen für Malware

Doch wie kommt die App des Angreifers auf ein Smartphone? Ein Smartphone ist wie jeder Computer per Definition offen für neue Software (engl. software open). Das ist genau die Eigenschaft, welche dem Smartphone zum Durchbruch gereicht hat. Es ist aber auch genau diese 'Offenheit', welche es verunmöglicht zu wissen, ob eine böswillige Software (=Malware) installiert ist oder nicht. Diese grundlegende Erkenntnis wurde bereits in den 1940er Jahren durch Alain Turing bewiesen. Ein Angreifer kann seine Malware in fast beliebig kleinen Teilen über mehrere Apps (und deren Berechtigungen) verteilt auf ein Smartphone bringen, sodass weder vermeintliche Malware-Filter noch der Benutzer selber diese je erkennen können.

Kalkuliertes Risiko für die Unternehmen

Wenn dem so ist, warum gibt es denn aber die vielen „sicheren“ Apps, insbesondere im Finanzbereich (E-Banking / Twint / etc.)? Der grösste Schaden für ein Unternehmen ist eine Dezimierung des Kundenstamms. Dies bringt die Unternehmen dazu, dem Kunden die Interaktion mit dem angepriesenen Produkt so einfach und angenehm wie möglich zu machen, am besten mit einer sexy Smartphone-App. Der mögliche Schaden, der dem Kunden durch einen Angriff über das Smartphone entstehen kann, ist kalkuliert und wird weitestgehend auf den Kunden abgewälzt. Um das Risiko möglichst tief zu halten, wird dem Kunden die Sorgfaltspflicht überlassen, ihm also die bewiesenermassen unmögliche Aufgabe auferlegt, das Smartphone Malware-frei zu halten. Passiert dennoch ein Schaden, welcher erwiesenermassen auf einen Angriff zurückzuführen ist, verhält sich die Bank dann kulant?

Weil wir es so wollen

Sämtliche Dienstleister, die Apps für ihre Produkte über das Smartphone anbieten, machen dies (laut deren Aussage), weil wir als Kunden das so verlangen. Für mögliche Schäden kommt in erster Linie der Kunde auf. Im Gegensatz zu monetären Verlusten, die evtl. noch rückführbar sind, ist beim Bruch der Privatsphäre der Schaden maximal und kann auch nicht rückgängig gemacht werden. So liegt es am Benutzer, das beschriebene Risiko abzuwägen. Dafür wird von jedem einzelnen von uns eine a priori Mündigkeit in diesen Belangen erwartet, womit sich die ganze Angelegenheit als gesellschaftliches Problem manifestiert, welches es zu lösen gilt.