Die Sperrfunktion des Handys umgehen? Das kann teuer werden. Aktuelles Beispiel: Apple Pay „Express Transit“-Funktion

Komfort und Sicherheit verhalten sich in der IT oft ähnlich in ihrem Verhältnis zueinander wie Freiheit und Sicherheit. Das eine geht nur auf Kosten des anderen. Ein aktuelles Beispiel bietet die Apple Pay „Express Transit“-Funktionalität: kleine Beträge lassen sich bequem bezahlen, trotz Sperrcode. Doch das lässt sich nach jüngsten Berichten fatal ausnutzen. Paul Ducklin, Sophos Security-Experte, erklärt das Problem.

Ein noch nicht veröffentlichtes Papier von Forschern aus dem Vereinigten Königreich hat Ende September wegen seiner dramatischen Behauptungen über Apple Pay Schlagzeilen gemacht: Demnach ermögliche es eine offensichtliche Schwachstelle, Geld von einem gesperrten iPhone zu stehlen, wenn eine Visa-Karte mit Apple Pay Express Transit eingerichtet ist.

Noch nie von Express Transit gehört? Es handelt sich um eine dieser cleveren Ideen, bei der Cybersicherheit zugunsten der Bequemlichkeit geopfert wird.
Einfach ausgedrückt, lassen sich mit dieser Funktion einige Arten von Touch-to-Pay-Transaktionen durchführen, auch wenn das Telefon gesperrt ist – sofern Express Transit aktiviert ist.

Das Prinzip des digitalen Zahlens ohne gesonderte Freigabe
Mit Express Transit funktionieren Apple Pay und das iPhone ein bisschen wie eine normale Kreditkarte, die bei Transaktionen mit geringem Wert nicht mit einem PIN-Code freigegeben werden muss. In den meisten Ländern Europas liegt dieses Limit zwischen 25 und 50 Euro.

Ähnlich einfach ist die Bezahlung via Express Transit über das Smartphone. Wird eine Transaktion angefordert, genügt ein einfacher Klick auf dem gesperrten Smartphone und schon ist das Geld beim Empfänger. Dieser eine letzte Klick kann leicht ungewollt passieren, wenn der Nutzer schnell etwas „wegklickt“, weil er gerade an etwas anderem interessiert ist oder wenn dieser eine Klick von einem Fremden unbemerkt ausgelöst wird, beispielsweise im Cafe oder in der überfüllten Bahn. Denn im Gegensatz zur Kreditkarte, die man meist in seinem Portemonnaie aufbewahrt und nur dann herausholt, wenn die Zahlung am Terminal tatsächlich ansteht, ist das Handy viel öfter und sichtbar präsent, beispielsweise auf einem Tisch.

Damit das Smartphone nicht missbraucht werden kann, sperren wir es gemeinhin mit einem Pincode oder einem alternativen Authentifizierungsmechanismus wie Fingerabdruck oder Gesichtserkennung. Doch leider schalten Nutzer immer wieder Telefonfunktionen auf dem Sperrbildschirm frei und verringern so die Sicherheit, die der Sperrbildschirm in erster Linie ja bieten soll – ganz gleich, ob es darum geht, dass Benachrichtigungen und persönliche Nachrichten angezeigt werden, während das Telefon gesperrt ist, oder um die Verwendung der Apple Pay Express Transit-Funktion zu nutzen.

Die Forscher, die hinter der noch zu veröffentlichenden Arbeit stehen, behaupten nun, dass sie in der Lage waren, iPhones unter sorgfältig vorbereiteten Umständen zu betrügerischen Zahlungen zu verleiten. Sie stellten ihr eigenes Zahlungsterminal auf und tarnten es als das öffentliche Verkehrsunternehmen, das Teil des Express-Transit-Zahlungssystems war.
Offenbar gelang ihnen der Diebstahl nur mit Visa-Kartenkonten (vermutlich waren andere Zahlungsanbieter strenger bei der Entscheidung, ob Zahlungsterminal X wirklich zu Unternehmen Y gehörte), und noch viel schlimmer: die Zahlungen waren nicht durch das übliche Limit von rund 50 Euro begrenzt. Die Forscher behaupten, dass sie durch die

Verwendung eines betrügerischen Zahlungsterminals Transaktionen von bis zu über 1000 Euro vornehmen konnten.

Was ist zu tun?
Trotz dieses dramatischen Ergebnisses müssen iPhone-Besitzer nun nicht in Panik verfallen, der Bericht ist allerdings Anlass, sich erneut mit der Nutzung des eigenen Smartphones auseinanderzusetzen. Nutzer sollten die Ausnahmen, die sie auf dem gesperrten Handy zulassen, generell gründlich überdenken. Ist es wirklich eine Belastung, bei jeder Aktion den Sperrcode eingeben zu müssen? Wenn man das mit Ja beantwortet, muss man mit den Risiken leben. Für alle anderen, die sich mit einem Entsperrvorgang sicherer fühlen, gibt es hier noch ein paar Tipps:

- Verzicht auf Express Transit und alle anderen Funktionen, die auf dem Sperrbildschirm aktiv sind. Diese Optionen opfern unweigerlich die Sicherheit zugunsten der Bequemlichkeit.

- Express Transit in Verbindung mit einer Visa-Karte sollte vorerst vermieden werden. Um Visa gegenüber fair zu sein, gehen wir davon aus, dass mit genügend Aufwand ähnliche Umgehungstricks auch für andere Zahlungsanbieter gefunden werden könnten. Ist man wirklich besorgt und kann ohne Express Transit nicht leben, sollte eine Prepaid-Debitkarte mit einem moderaten Guthaben eingerichtet werden. Zumindest ist dann ein Diebstahl nur für das Guthaben und nicht für den Kreditrahmen einer Kreditkarte möglich.

- Niemals das Telefon unbeaufsichtigt liegen lassen und nur herausholen, wenn es gerade benutzt wird. Ansonsten, in der Hand halten oder in der Tasche haben.

- Man sollte den bestmöglichen Sperrcode nutzen und die kürzeste Zeitspanne für die automatische Sperre. Ein gesperrtes Telefon ist eine kleine Unannehmlichkeit, aber eine große Hürde für Betrüger, sogar für die technisch Versierten. Ein ungesperrtes Telefon hingegen ist ein offenes Ziel für jeden, auch für schlichte Gelegenheitsverbrecher.

- Bank- und Zahlungskartenabrechnungen regelmäßig prüfen. Wenn man Express Transit für regelmäßige und vorhersehbare Zahlungen, beispielsweise im öffentlichen Verkehr nutzt, fallen unnormale Buchungen schnell ins Auge.

Neu: Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de