QR-Codes – Sicherheitsprobleme

Gefahr im Bithaufen

QR-Codes: Sicherheitsproblem oder nicht?

QR-Codes können ähnlich wie Phishing-Mails Träger gefährlicher URLs sein. Wir erklären, welche Tricks sich Kriminelle ausgedacht haben und worauf Sie beim Scan von QR-Codes achten müssen.

Von Wilhelm Drehling

Die quadratischen Codes sind im Alltag nützliche Helfer: Mit einem Scan können Sie eine URL aufrufen, einen Kontakt hinzufügen oder dem Gast zu Hause das Abtippen des WLAN-Passworts ersparen. Weil sie praktisch sind und auch mal leichtfertig gescannt werden, haben auch Angreifer ihre Freude an QR-Codes gefunden. Denn das Aussehen des QR-Codes verrät nichts über dessen Inhalt, so kann sich in dem Pixelhaufen ein gefährlicher Link zu einer täuschend echten Anmeldeseite einer Fake-Bank oder zu einem Trojaner verbergen. In den vergangenen Jahren haben Kriminelle originelle Methoden erfunden – denen man aber zum Glück nicht schutzlos ausgeliefert ist.

Quishing

Das erste Angriffsszenario gehört in die Kategorie der Phishing-Angriffe: Vermutlich kommen Ihnen dubiose Mails wie „PayPal: Ihr Konto ist vorübergehend eingeschränkt“ bekannt vor. Mit solchen Mails versuchen die Angreifer häufig, an Ihre

Anmeldedaten heranzukommen, indem sie Sie auf eine gefälschte Webseite mit gewohntem Anmeldefenster weiterleiten. Enthält die Mail einen QR-Code, der zur Phishing-Seite führt, spricht man von Quishing.

Der große Unterschied zu den üblichen Mail-Betrügereien: Es hat sich bereits herumgesprochen, dass man nicht einfach so auf Links in Mails klicken sollte, die möglicherweise obendrein in schlechtem Deutsch verfasst sind. Bei QR-Codes ist das nicht der Fall. Ergo schenkt man QR-Codes mehr Vertrauen, scannt sie ein und landet dann womöglich auf einer Phishing-Seite oder Ärgerem.

Diese Masche tritt häufig in unterschiedlichen Varianten auf: Die Volksbank warnte im Dezember 2021 vor Mails und sogar Briefen mit QR-Codes, die Kunden dazu aufforderten, eine neue App herunterzuladen und sich dort zu registrieren. Ähnliche Angriffe mit QR-Codes häuften sich in letzter Zeit so sehr, dass die Polizei eine Warnung vor QR-Codes in Mails aussprach (sämtliche Warnungen haben wir Ihnen unter ct.de/yrf5 verlinkt).

Ob diese Warnungen wirklich etwas bringen, lässt sich diskutieren. Der c’t-Security-Experte Jürgen Schmidt geht in seinem Kommentar im Kasten rechts dieser Frage auf den Grund.

QR-Codes sind nicht das Problem

Ein Kommentar von Jürgen Schmidt (Leiter heise Security)

Die Krypto-Börse Coinbase platzierte in der Halbzeitpause des Superbowls einen Werbespot, der die Zuschauenden dazu verleiten sollte, einen über den Fernseher hüpfenden QR-Code

mit der Handy-Kamera einzufangen. Auf der dann angezeigten Website erwartete sie nur eine Meldung, dass der Dienst nicht erreichbar ist – vermutlich wegen Überlastung. Aber das ist eine andere Geschichte.

Es folgte ein Aufschrei der um die Sicherheit besorgten Experten, dass man den Anwendern unsichere Verhaltensweisen antrainiere und somit Phishing-Betrügern in die Karten spiele. Schließlich könne sich hinter dem QR-Code doch auch eine bösartige Phishing-Webseite verbergen, die es auf ihre Zugangsdaten abgesehen hat. Ich halte diesen Ansatz für falsch.

Das World Wide Web beruht darauf, dass Anwender Links öffnen. Auch solche, bei denen sie vorher nicht wissen, was genau sich dahinter verbirgt, schließlich will man ja Dinge entdecken. Es ist deshalb unsere (uns hier im Sinne von all denen, die im weitesten Sinne das Web mitgestalten) Aufgabe, den Anwendern Werkzeuge bereitzustellen, mit denen sie das tun können. Sprich: Anwender sollten einen Link ohne unmittelbare Gefahr öffnen können. Wenn allein durch das Öffnen eines Links etwas Böses passiert, dann ist das ein Fehler im Browser, den dessen Hersteller zu verantworten und zu beseitigen hat.

Die Verantwortung des Anwenders beginnt, wenn er mit der Seite interagiert. Bevor er dort persönliche Daten oder sogar ein Passwort eingibt, sollte er sich die Frage stellen, ob und wie weit er der Seite vertrauen kann. Da spielt primär der Kontext eine wichtige Rolle. Das ist in der analogen Welt nicht anders: Dem Hotel-Angestellten beim Check-in gibt man seine Kreditkarte; einem Unbekannten am Bahnhof eher nicht.

In der digitalen Welt zeigt sich da schon das erste Problem: Browser zeigen immer öfter gar nicht mehr an, wo sich der Anwender gerade befindet und machen es damit schwer, die Vertrauenswürdigkeit einer Passwortabfrage zu beurteilen oder gar zu überprüfen. Immerhin können sich Anwender fragen: Wie bin ich hierher gelangt? Über ein gespeichertes Lesezeichen

oder einen QR-Code in einem eher zweifelhaften Zusammenhang? Der Vertrauens-Check ist nicht trivial – aber etwas, was man Anwendern beibringen kann und sollte. „Klicke nicht auf Links“ oder „Verwende keine QR-Codes“ hingegen sind keine sinnvollen Lernziele. Darüber hinaus kann man Anwender zu Multifaktor-Authentifizierung und insbesondere FIDO2 ermuntern, weil sie konzeptionell vor Phishing schützen.

Eine Verteufelung von QR-Codes hingegen führt nur zu noch mehr angeblichen „Best Practices der Security“, die zwar gebetsmühlenartig wiederholt werden, an die sich niemand wirklich hält, weil sie praxisfern sind. Ich scanne den QR-Code im Restaurant, um mir die Speisekarte anzuschauen und ich würde mir wünschen, dass auch meine Bank Girocodes einführt [1], weil ich es satthabe, ständig gefühlt 100-stellige IBANs von Hand einzutippen. Ich werde also auch anderen Menschen, die sich von mir Sicherheitstipps erhoffen, nicht erzählen, dass sie keine QR-Codes benutzen dürfen, sondern lieber zur Zweifaktor-Authentifizierung raten.

Überklebt

Ein deutlich gefährlicherer und unscheinbarer Angriffsvektor geht von öffentlichen QR-Codes aus, die Sie in Broschüren, Werbeplakaten oder Speisekarten finden. Angreifer können die Codes überkleben und die Opfer somit auf gefälschte Webseiten locken. Die Idee hinter dem Angriff ist nicht neu, schon 2013 warnte das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor überklebten QR-Codes.

Das passiert nicht unbedingt bei Speisekarten; vorsichtig müssen Sie bei QR-Codes sein, die „alternative Bezahlmöglichkeiten“ anpreisen. Das FBI warnt in den USA zum Beispiel davor, keine QR-Codes bei Parkplätzen zu scannen, die zu einem Bezahldienst weiterleiten: Anstatt zum Parkautomat zu laufen, könne man so bequem die Rechnung für die Parkdauer bezahlen. Doof nur, wenn das Geld dann nicht an den Parkplatzbetreiber fließt, sondern direkt in die Taschen der

Betrüger.

Überklebte QR-Codes verheißen auch bei Außenwerbung Unheil, die dazu einlädt, eine App herunterzuladen oder Webseiten zu besuchen. In solchen Fällen greifen die Angreifer erneut nach Ihren Daten und im schlimmsten Falle versuchen sie, über eine App einen Trojaner auf Ihr Smartphone herunterzuladen (zugegebenermaßen ist das leichter beim Google Play Store zu bewerkstelligen als über den App Store auf iOS).

Genauso kritisch sind leicht zugängliche QR-Codes in Zügen oder Einkaufszentren, die einen einfachen Zugang zum WLAN anbieten: Ein solcher QR-Code kann von Angreifern überklebt worden sein. Mit einem Klick verbinden Sie sich mit einem von Angreifern eingerichteten gleichnamigen Hotspot.

Gegenmaßnahmen

Hersteller von Smartphones haben schon früh reagiert: Kamera-Apps folgen nicht mehr direkt einer gescannten URL. Ein Großteil aller modernen Kamera-Apps zeigt den Link stattdessen auf dem Bildschirm an. Danach ist es an Ihnen, zu entscheiden, ob Sie darauf klicken oder nicht. Dabei ist der gesunde Menschenverstand gefragt: Sieht die URL merkwürdig aus, dann sollten Sie den QR-Code genauso wie eine Phishing-Mail in den Papierkorb befördern.

Wenn Sie zusätzlich auf Nummer sicher gehen wollen (oder Familienangehörigen einen Gefallen tun wollen), weichen Sie unter Android auf eine App wie zum Beispiel Trend Micro QR-Scanner aus (siehe ct.de/yrf5), die den Inhalt des QR-Codes prüft und Sie vor potenziell gefährlichen Links warnt. iOS-Nutzer nehmen die App Intercept X von Sophos (siehe ct.de/yrf5). Die sichere Scanfunktion für QR-Codes ist aber nur ein kleiner Teil der Antiviren-App: Mit der App laden Sie leider noch viele weitere Funktionen herunter, deren Sinn mindestens zweifelhaft ist.

Mit der App QR-Scanner von Trend Micro bekommen Sie eine Einschätzung, ob die URL hinter dem QR-Code potenziell gefährlich ist.
Tipp für ganz harte Tüftler: Alternativ können Sie Ihr Smartphone beiseitelegen und den QR-Code per Hand dekodieren [2]. Das ist zwar mühsam, aber Sie fangen sich auf diese Art und Weise definitiv kein Virus ein.

Fazit

Wie bei vielen der vorgestellten Szenarien spielt der Kontext

eine wichtige Rolle: Ein QR-Code mit WLAN-Daten bei Ihnen zu Hause genießt ein höheres Vertrauen als ein QR-Code auf einem Laternenmast, der für ein öffentliches WLAN wirbt. Im Zweifel sollten Sie die Entscheidung, eine fragwürdige URL anzuklicken, dem gesunden Menschenverstand überlassen oder bei noch größeren Zweifeln eine QR-Überprüfungs-App konsultieren. *(wid@ct.de)*

1. Literatur
2. Jan Mahn, Schöner zahlen, Rechnungen schneller überweisen mit QR-Codes, c't 7/2022, S. 138
3. Wilhelm Drehling, Bithaufen, QR-Codes verstehen und ohne technische Hilfsmittel per Hand dekodieren, c't 17/2022, S. 142

Warnungen und Scanner-App: ct.de/yrf5