QR-Code als Sicherheitsfalle?
„Ich würde die Finger davon lassen.“

QR-Codes auf Verpackungen, Plakaten oder in Bars verlocken, einfach das Smartphone daran zu halten. Trotz vieler Vorteile für Unternehmen und Konsumenten, rät Chester Wisniewski, Sicherheitsprofi bei Sophos, zu Vorsicht und Einzelfallprüfung.

Der Mensch neigt bekanntlich zur Bequemlichkeit. Warum noch extra den Browser mit dem kleinen Smartphone-Display bemühen – da kommt ein QR-Code doch goldrichtig. Informationen, die auf der Stelle gebraucht werden, sind so schnell zur Hand. Diese Vorteile setzen immer mehr Unternehmen ein, beispielsweise um Kunden Zusatzinformationen zu Produkten oder deren Nutzung zu bieten. Und wie das immer so ist, sind Cyberkriminelle nicht weit, sobald sich eine Technik im Alltag durchgesetzt hat. „Quishing“ heißt die Betrugsart mit QR-Codes. Den Trend hat Sophos in diesem Beitrag beschrieben.

Chester Wisniewski, Director, Global Field CTO von Sophos, gibt Antworten auf die wichtigsten Fragen zur Sicherheit von QR-Codes.

1. QR-Codes erweisen sich wachsender Beliebtheit in Verkauf, Marketing und Bezahlsystemen. Wie kam es zu dieser Entwicklung und inwieweit verbessern sie das Kundenerlebnis?

Chester Wisniewski: Niemand spricht gern in Computer-Art. Der Vorteil, ein Smartphone für schnelle Informationen oder Aktionen nutzen zu können, ist eine starke Motivation sowohl für die Anbieter als auch die Nutzer von QR-Codes. Das in Kombination mit den ökologischen Vorzügen des Nicht-Ausdruckens von Dokumenten und der Tatsache, dass viele Unternehmen komplexe Tracking-Tokens in die URLs einbauen können, trägt zur Verbreitung von QR-Codes zusätzlich bei.

2. Während QR-Codes einen großen Mehrwert bieten, wachsen die Bedenken zu ihrer Sicherheit. Welche Arten von Betrug oder schadhaften Aktivitäten sind in den letzten Jahren aufgetaucht, die Nutzer via QR-Codes ins Visier genommen haben?

Chester Wisniewski: Jeder kann QR-Codes herstellen und es ist nicht möglich, sie zu authentifizieren. Es erfordert einen hohen Grad an Vertrauen beim Konsumenten, dass der QR-Code, den er am Parkscheinautomat oder auf dem Kaffeetisch sieht, echt ist. Wir haben von Vorfällen gehört, speziell in denen Zahlungen beteiligt waren, bei denen Betrüger QR-Codes ausgedruckt haben und diese auf echte QR-Codes aufklebten, um die Leute auf eine Phishing-Webseite zu lenken und hier ihre Kreditkarten-Daten und persönliche Informationen abzugreifen.

3. Welche Schritte können beispielsweise Händler unternehmen, um sicherzustellen, dass die QR-Codes, die sie in den Geschäften oder Online einsetzen, sicher und legitimiert sind? Wie können sie ihre Kunden vor potentiellem Betrug oder Phishing-Angriffen schützen?

Chester Wisniewski: Geschäfte, Händler, Gastronomie usw., die QR-Codes nutzen, sollten sie regelmäßig kontrollieren – insbesondere, wenn die QR-Codes öffentlich aushängen. Das wird zu einer größeren Herausforderung bei verteilten Systemen wie Parkscheinautomaten. Konsumenten sind gut beraten, keine QR-Codes zu scannen, denen sie nicht wirklich vertrauen und lieber ein anderes Zahlungsmittel mit weniger Risiken verwenden.
Ich persönlich meide Geldautomaten, die zweifelhafte Tastaturen haben oder sich ersichtlich

nicht im Originalzustand befinden – das gleiche könnte man für QR-Sticker anwenden. QR-Codes sollten wirklich niemals online genutzt werden, denn die meisten sind nur eine visuelle Form einer URL. Wenn man möchte, dass jemand auf einen Link klickt, dann sollte man auch einen Link benutzen. Es gibt Ausnahmen, aber im Allgemeinen bestätigen sie die Regel.

4. Vor welchen „red Flags“ sollten sich Konsumenten in Acht nehmen, wenn sie QR-Codes in der Öffentlichkeit oder auf Produkten scannen, um nicht zum Opfer von Kriminellen zu werden?

Chester Wisniewski: QR-Codes übertragen ein Bild in eine Webseiten-Adresse. Wenn der Code im Browser öffnet, sollte man auf die Adressleiste sehen und prüfen, wohin man als Nutzer gelenkt wurde. Gefällt einem dieses Ziel nicht, ist es klug, die Anwendung zu beenden. Der sicherste Weg für den Konsumenten? Den QR-Code nicht scannen. Stattdessen lieber die Lieblingssuchmaschine nutzen. Es existieren jedoch auch Applikationen für mobile Geräte wie Sophos Intercept X, die QR-Codes Scanner beinhalten, die auf schadhafte Links aufmerksam machen.

5. Ein Blick in die Zukunft: Wie wird sich die Rolle von QR-Codes in Verkauf und anderen Branchen weiterentwickeln? Werden sie sicherer werden mit neuen Technologien oder wird die Sicherheit eine Herausforderung bleiben?

Chester Wisniewski: Ich sehe die Sicherheit von QR-Codes nicht besser werden. Sie sind ursprünglich für Maschinen entwickelt worden und nicht dafür, dass Menschen sie im Alltag nutzen. Eine Authentifizierung von QR-Codes stellt ein Aufgabe dar, die sich nicht so simpel lösen lässt. Im Idealfall sollten QR-Codes in Plakate, Produktverpackung etc. fest und ersichtlich eingebettet sein und nicht nur ein Sticker, der irgendwo draufgepappt wurde.
Die Verantwortung liegt beim Konsumenten: Wenn ein QR-Code komisch erscheint, lieber die Finger davon lassen und auf eine bewährte, sichere Informationsgewinnung oder Zahlung setzten.

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/
X/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