SOPHOS
Cybersecurity made simple.

25 Jahre QR-Code – Braucht die beliebte Pixel-Matrix ein neues Sicherheitskonzept?

QR-Codes gibt es seit 1994, doch ihr Entwickler ist besorgt und der Meinung, dass sie ein Sicherheitsupdate benötigen. Der Ingenieur Masahiro Hara entwickelte mit seinem Team die 2D-Codes für den Einsatz in der japanischen Automobilherstellung. Aber wie bei vielen anderen Technologien auch, nahm die Verbreitung schnell zu, da der Code auch für weitere Zwecke sinnvoll einzusetzen ist. Masahiro Haras Arbeitgeber Denso stellte das Design damals kostenlos zur Verfügung und heute sind QR-Codes überall zu finden – vom Werbeplakat über Zeitschriften, Restaurants und Museen bis hin zum Login auf dem Bestätigungsfeld einer Webseite.

Insbesondere in China sind QR-Codes sehr beliebt und es werden Zahlungen in Billionenhöhe über das System getätigt. Hongkong hat kürzlich ein auf QR-Code basierendes und zugleich schnelleres Zahlungssystem eingeführt. Dieser Code weckte so viel Interesse, dass Apple ihn nativ in der Kamera-Applikation von iOS 11 unterstützt, wodurch die Notwendigkeit von QR-Scan-Anwendungen von Drittanbietern entfällt. Hara ist ein wenig erschrocken über all diese neuen Einsatzgebiete für ein Design, das ursprünglich nur zur Produktionskontrolle in Betrieben entwickelt wurde. In einem Interview Anfang August äußerte er angeblich seine Bedenken und meinte, dass er sich dafür verantwortlich fühle, QR-Codes sicherer zu machen.

Security-Experten teilen sein Bedenken: „Cyberkriminelle können QR-Codes auf vielfältige Weise für Angriffe nutzen, wie beispielsweise durch Quick Response Code Login Jacking", so Michael Veit, Security-Experte bei Sophos. Dieser Angriff ist möglich, wenn ein Nutzer den QR-Code als Einmalpasswort verwendet und auf einem Bildschirm anzeigt. Das Open Web Application Security Project (OWASP) listet diese Attacke als Angriffsvektor und warnt, dass ein Angreifer den QR-Code von einer legitimen Website auf eine Phishing-Site klonen und dann an das Opfer senden könnte. Eine weitere Angriffsmöglichkeit entsteht durch gefälschte QR-Codes. Kriminelle können ihre eigenen QR-Codes über legitime stellen. Anstatt das Smartphone des Benutzers auf die vorgesehene Webseite zu leiten, führt der gefälschte Code den Benutzer zu Phishing-Websites oder zu Seiten, die auf JavaScript basierende Malware bereitstellen. Cyberkriminelle könnten auch die zunehmende Verwendung von QR-Codes für Zahlungen nutzen. Sie ersetzen dabei den QR-Code, der den Anwender zu einer legitimen Zahlungsadresse führt, mit einer eigenen URL für gefälschte Zahlungen.

Forscher des MIT (Massachusetts Institute of Technology) haben in einem Bericht bereits einige Vorschläge für Sicherheitsmaßnahmen aufgeführt. So könnte beispielsweise der QR-Code eine Verschlüsselung verwenden, um zu verhindern, dass ein Dritter diesen Code ausspioniert und klont. Dazu sendet eine Online-App einen verschlüsselten QR-Code an ein bereits angemeldetes (und damit vertrauenswürdiges) mobiles Gerät. Nur das angemeldete Gerät kann den QR-Code entschlüsseln und zeigt ihn dann für das zweite Gerät zum Lesen an. Der QR-Code enthält eine URL, die den Nutzer in die App einloggt – ähnlich dem Prinzip der Zwei-Faktor-Authentisierung. Es gibt auch mehrere verschlüsselte QR-Code Login-Systeme, die derzeit in Entwicklung sind. Ein weiterer Vorschlag besteht darin, digitale Signaturinformationen in den Code einzubetten, um seine Authentizität zu bestätigen. „Das sind alles sehr gute Ideen, aber die Forscher sollten sich besser beeilen", so Veit. „Denn mit zunehmender Verbreitung von QR-Codes wird es immer schwieriger, das Design zu ändern."

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
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