# QR-Codes – Pac-Man lässt grüssen

Ein wenig erinnert ein QR-Code an das Pac-Man-Labyrinth. In diesem bewegte man sich rund wie ein Puck und mit aufgerissenem Mund vorwärts, konnte fressen und gefressen werden. Es gibt Werbekampagnen, Stadtparcours und Kunstprojekte mit Codes. Und Sicherheitsrisiken, über die man diskutieren sollte. Oliver Bendel

Bild: Fotolia

QR-Codes gehören wie Data-Matrix- und Aztec-Codes zu den 2-D-Codes. Sie wurden in den 90er-Jahren von der japanischen Firma Denso Wave (einer Tochter von Toyota) entwickelt. Man hatte nach einer einfachen und günstigen Möglichkeit gesucht, die Autoteile in den Produktionsstätten zu markieren und automatisch ihre Position und ihre Art zu ermitteln. Das Labyrinth, einst von Dädalus für den Minotaurus erschaffen und in den 80er-Jahren für Puck Man (den späteren Pac-Man) eingesetzt, wurde also für die Verbesserung der Logistik eines Autoherstellers wiederentdeckt. Die Abkürzung «QR» steht für «Quick Response» («schnelle Antwort» oder «schnelle Reaktion») und meint die Anzeige von Informationen beziehungsweise den Aufruf von (Online-)Ressourcen. In QR-Codes können unter anderem Webadressen, Telefonnummern, SMS und freier Text enthalten sein.

Der QR-Code ist international standardisiert und weltweit verbreitet. Er wurde von den japanischen Entwicklern freigegeben, und man darf ihn lizenz- und kostenfrei herstellen und verwenden. So wie jeder Benutzer die Muster mit Handys, Smartphones oder Tablets, die mit einem QR-Code-Reader ausgestattet sind, einscannen kann, kann er auch seine eigenen produzieren. Voraussetzung hierfür ist ein QR-Code-Generator, den es als Webanwendung und lokal installierbare Anwendung für den Computer oder das Smartphone gibt. Wer einen Generator anbietet, kann über dessen Gebrauch bestimmen. Prinzipiell kann man QR-Codes auch mit Klebeband oder Legosteinen anfertigen oder sich eintätowieren lassen; aber es führt kaum ein Weg an der vorherigen maschinellen Generierung vorbei.

**Oliver Bendel** lehrt und forscht als Professor für Wirtschaftsinformatik an der Hochschule für Wirtschaft (Fachhochschule Nordwestschweiz), mit den Schwerpunkten Wissensmanagement, Social Media, Mobile Business und Informationsethik.

## Sicherheitsrisiken von QR-Codes

Im Labyrinth der QR-Codes muss man aufmerksam sein. Wie Pac-Man kann man fressen, etwa einen Mitbewerber. Man kann Plakate, Zeitschriften und Bücher anreichern und so Mehrwert schaffen und Kosten sparen. Man kann aber auch, wenn man nicht aufpasst, gefressen werden. Im Folgenden werden einige Sicherheitsrisiken beschrieben, geordnet nach den QR-Codes selbst, den Readern und den Generatoren für QR-Codes. Bei den Readern wird auf Anwendungen für das Handy eingeschränkt, bei den Generatoren zwischen Online- und Offlineprogrammen unterschieden.

- Das grundsätzliche Problem der QR-Codes ist, dass man ihnen nicht ansieht, was sie enthalten. Peter Kieseberg und seine Mitautoren heben einen Aspekt hervor: Weil das Auslesen der Daten und Informationen nur Maschinen möglich ist, vermag ein Mensch nicht zwischen einem originären und einem manipulierten Code zu unterscheiden. Die Autoren tragen in ihrem wissenschaftlichen Artikel mehrere Möglichkeiten von Attacken zusammen. Wie Kai Biermann auf «Zeit online» erläutert, kann in einem QR-Code etwa Javascript verschlüsselt werden; wenn der Programmcode ausgeführt wird, wird beispielsweise der Reader gekapert. Der QR-Code kann zudem zu einer Website mit Malware führen. Die Malware befällt das Handy und richtet dort Schaden an oder spioniert Informationen aus. Nicht zuletzt kann der QR-Code – wie auch Kieseberg und Biermann erläutern – auf eine Phishing-Website verweisen. Mittels dieser ist es möglich, Daten des Benutzers abzugreifen, beispielsweise Passwörter oder Kreditkartennummern.
- Die Reader können dazu missbraucht werden, Daten von Benutzern einzusammeln und weiterzugeben. Betroffen sind

verschiedene Arten von Daten und ihre Aggregationen. Der Scan an sich generiert Bildinformationen; ein bestimmter Code wird als visuelles Element erfasst (mitsamt Logo, wenn vorhanden), vielleicht auch ein Teil des Trägers und der Umgebung (wobei heutige Reader in allen bekannten Fällen auf den Code fokussieren). Weiterhin wird der Code ausgelesen, was mit Fehlern verbunden sein kann. Die Daten kann man mit dem Standort des Benutzers und mit den persönlichen Daten auf dem Handy in Verbindung bringen. Erstellen liesse sich zum Beispiel ein Bewegungs- und ein Interessenprofil. QR-Code-Reader können auch unerbetene Daten auf dem Handy oder Smartphone ablegen, unerwünschte Installationen auf dem mobilen Gerät vornehmen oder den Benutzer mit Werbung belästigen.

- Bei den Generatoren muss man Online- und Offlineprogramme unterscheiden. Beide Arten haben spezifische Sicherheitsrisiken. Mithilfe der Onlinegeneratoren können die Anbieter die online eingegebenen Daten auslesen und weiterverwenden. Sie können zudem den Daten mindestens die IP-Adresse des Benutzers zuordnen. Offlinegeneratoren werden über lokal abgelegte Dateien aufgerufen oder auf dem Gerät installiert. Beim Produzieren von QR-Codes über Offlinegeneratoren ist, wie der Name verrät, in der Regel keine Onlineverbindung notwendig. Manche Offlinegeneratoren unterstützen eine Vielfalt von Codes, darunter auch 1-D-Codes wie EAN-Barcodes und andere 2-D-Codes wie Data-Matrix-Codes, und stellen damit eine «All-in-One»-Lösung für Unternehmen dar. Sie weisen die generellen Sicherheitsrisiken von lokal ausgeführten beziehungsweise installierten Programmen auf.

Ein weiteres Sicherheitsproblem ist, dass QR-Codes überklebt und ausgetauscht werden können; darauf geht auch das Connecticut Better Business Bureau ein. Auf diese Weise kann ein Benutzer auf Websites mit fragwürdigen Informationen oder mit Malware gelockt und dem Anbieter auf unterschiedliche Weise geschadet werden. Der Vorteil für die «Vandalen» ist, dass sie auf einer bestehenden Kampagne aufzusetzen vermögen. Auch in der Schweiz wurde der eine oder andere Fall bekannt, etwa das Überkleben eines QR-Codes bei einem Plakat eines Lokalpolitikers im Sommer 2012.

Derzeit besteht kein Anlass zur Hysterie, doch genügt bereits ein kleiner Missbrauch, um das Vertrauen in QR-Codes bei den Anwendern zu beschädigen. Und natürlich kann sich die Situation schlagartig ändern. Gerade noch hat man einen Mitbewerber gefressen und plötzlich macht sich ein hungriges Gespenst über einen her.

## Sicherheitsmassnahmen und Lösungsansätze

Vereinzelt werden von (Wirtschafts-)Informatikern, IT-Spezialisten und Marketern Sicherheitsrisiken diskutiert, selten jedoch Sicherheitsmassnahmen. Die folgende Auflistung entspringt ersten Überlegungen.

- Inhaltlicher Zusammenhang und «physische Umgebung» eines QR-Codes können Hinweise darauf liefern, ob Vertrauen gerechtfertigt oder Vorsicht angebracht ist. Immer mehr Produkte, Broschüren und Bücher werden mit Codes angereichert. Produzenten, Händler und Verleger garantieren mit ihrem guten Namen dafür, dass sich keine unerwünschten Effekte einstellen.
- Ist der QR-Code fest auf dem Produkt oder Träger aufgebracht und mit einer zusätzlichen Folie gesichert, ist eine missbräuchliche Verwendung unwahrscheinlich. Wenn der QR-Code nur aufgeklebt ist oder sich auf einem austauschbaren Etikett befindet, sollte man die Echtheit prüfen. Bei einem offensichtlich überklebten Code ist zu erhöhter Wachsamkeit zu raten.
- Um die seriöse Herkunft des Codes garantieren zu können, kann auch ein Sicherheitsmerkmal entwickelt werden. Dieses wird in den Code integriert oder an dessen Seite angebracht. Das Merkmal sollte schwer zu imitieren sein, ähnlich wie bei Geldscheinen. Man muss untersuchen, wie man Codes auszeichnen kann, ohne die Kosten zu stark zu erhöhen und die Einfachheit der Erstellung und Nutzung zu sehr zu beeinträchtigen.
- Von Bedeutung ist die Auswahl der Reader. Wenn die Adresse vor dem Aufruf einer Website angezeigt wird, kann man entscheiden, ob man dorthin navigieren will. Allerdings gelten Reader als komfortabel, die direkt Ressourcen aufrufen. Auch Adressen sieht man nicht unbedingt an, ob die damit verknüpften Inhalte vertrauenswürdig sind, insbesondere verkürzten nicht; nützlich sind Vorschaufunktionen.
- Neutrale Personen und Einrichtungen können Reader dahingehend testen, ob diese fehlerhaft arbeiten, Informationen weitergeben, unerbetene Daten auf dem Handy, Smartphone oder Tablet ablegen oder unerwünschte Installationen auf dem Gerät vornehmen. Natürlich ist es zu begrüssen, wenn die Anbieter auch selbst informieren und den Code des Programms offenlegen.
- Nicht zuletzt ist die Verwendung von geeigneten Generatoren wichtig. Man sollte sich an Anbieter halten, die die Funktionsweise des Programms und – bei Onlinegeneratoren – die Datenverwendung transparent darstellen. Und man sollte die AGB auf den Websites und in den Handbüchern lesen und sich daran halten. Eine kommerzielle Verwendung der QR-Codes wird nicht von jedem Anbieter erlaubt.

Damit sind längst noch nicht alle möglichen Ansätze und Massnahmen benannt, und ohne Zweifel werden sich auch Technologien, Umsetzungen und Umfeld immer wieder ändern.

## Resümee

Der QR-Code ist eine faszinierende und sich hierzulande rasch etablierende Technologie mit enormen Chancen und riesigem Potenzial. Man kann mit Trägern und Substanzen experimentieren und sich in kreativer Weise betätigen. Das Labyrinth ist omnipräsent wie in den Spielhallen der 80er-Jahre das Pac-Man-Spielfeld. Und wie in diesem lauern im 2-D-Code gewisse Gefahren. Mit dem 3-D- und 4-D-Code werden weitere (Offline-)Anwendungen möglich, mit denen man gewisse Probleme eliminieren kann, mit denen aber auch neue entstehen. So kann man durch die höhere Speicherkapazität verschiedene Formen von Malware direkt im Code unterbringen. Es lohnt sich auf jeden Fall sowohl für die Anbieter und Unternehmen als auch die Benutzer und Kunden, sich einen Überblick über mögliche Sicherheitsrisiken von heutigen und künftigen Anwendungen zu verschaffen. <

### LITERATUR

**Bendel, Oliver.** Gutenbergs Rückkehr: Codes als Erweiterungen gedruckter Bücher. In: B.I.T.online, Zeitschrift für Bibliothek, Information und Technologie, 1/14. 2011.

**Biermann, Kai.** QR-Code: Böse Pixelmuster. In: «ZEIT ONLINE», www.zeit.de/digital/datenschutz/2011-09/qr-code-hack. 21.9.2011.

**Connecticut Better Business Bureau.** New Uses for Old Technology are Revolutionizing Marketing but Prone to Abuse. Über http://ct.bbb.org/article/new-uses-for-old-technology-are-revolutionizing-marketing-but-prone-to-abuse-28431. 2011.

**Kieseberg, Peter; Leithner, Manuel; Mulazzani, Martin et al.:** QR Code Security. In: TwUC 10, www.sba-research.org/wp-content/uploads/publications/QR_Code_Security.pdf. 2010.