Sicherheitsrisiken von QR-Codes

Markus Diller, Manuel Hatzl, Rico Schneider, Lukas Wachter

Universität Salzburg

3. Februar 2021

Überblick

1. Grundlegendes und Aufbau (Rico Schneider)
2. Sicherheit und Manipulationsmöglichkeiten (Markus Diller)
3. Angriffsarten (Lukas Wachter)
4. Sicherheitsrisiken im Alltag (Manuel Hatzl)
5. Quellen

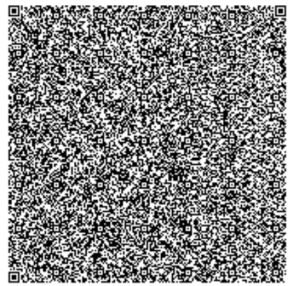
Allgemein

- „Quick Response“
- 1994 von japanischer Firma „Denso Wave“ entwickelt
- Repräsentiert binäre digitale Daten in analoger Form
- Quadratische Matrix aus schwarzen und weißen Kästchen
  - schwarz $\rightarrow$ 1
  - weiß $\rightarrow$ 0
- Variation (Bsp.: Designer-QR-Code)
- Verschiedene Größen

(Foundata, 2019)

Allgemein

- „Quick Response“
- 1994 von japanischer Firma „Denso Wave“ entwickelt
- Repräsentiert binäre digitale Daten in analoger Form
- Quadratische Matrix aus schwarzen und weißen Kästchen
  - schwarz $\rightarrow$ 1
  - weiß $\rightarrow$ 0
- Variation (Bsp.: Designer-QR-Code)
- Verschiedene Größen



(Techspot, 2021)

Grundgerüst

- Erkennungsmuster
  - Position detection patterns (gelb)
  - Alignment patterns (hellblau)
  - Timing patterns (rot)
- Informationsbereiche
  - Versionsinformationen (grün)
  - Formatinformationen (blau)

(MST, 2020)

Kodierung des Textes

- Je nach Zeichen → verschiedene Zeichensätze verwendet
  - Ziffern (0-9)
  - Alphanumerisch (0-9, A-Z, $%*+-/:)
  - ISO-8859-1 (0-9, a-Z, viele Satzzeichen, kombinierte Buchstaben)
  - Kanji (japanische Schriftzeichen)
- Jeder Zeichensatz hat eigene Kennnummer

w w w . g o o g l e . c o m

↓

77 77 77 2E 67 6F 6F 67 6C 65
2E 63 6F 6D

↓

1110111 1110111 1110111 0101110 1100111
1101111 1101111 1100111 1101100 1100101
0101110 1100011 1101111 1101101

Inhalt

(MST, 2020)

Inhalt

- Kennzeichnung des Zeichensatzes

(MST, 2020)

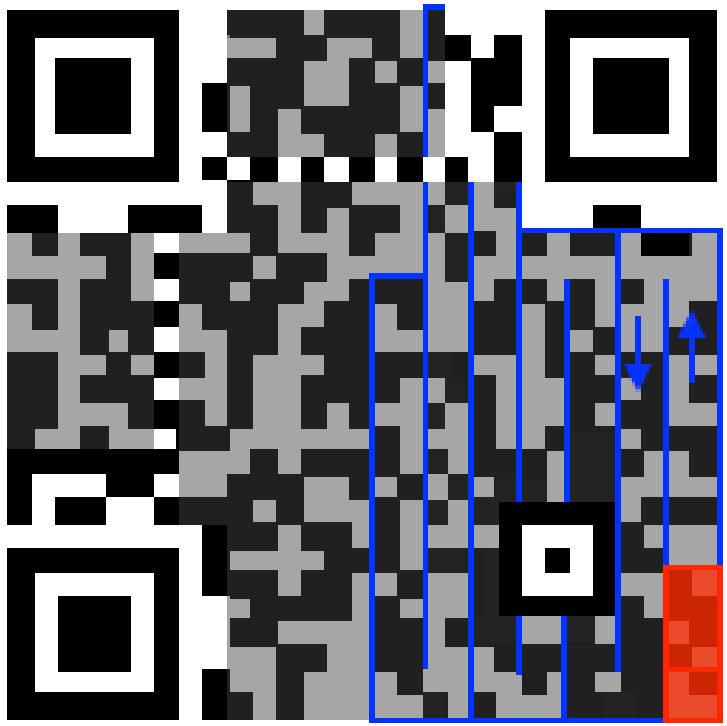
Inhalt

- Kennzeichnung des Zeichensatzes
- Kennzeichnung der Anzahl an Zeichen

(MST, 2020)

Inhalt

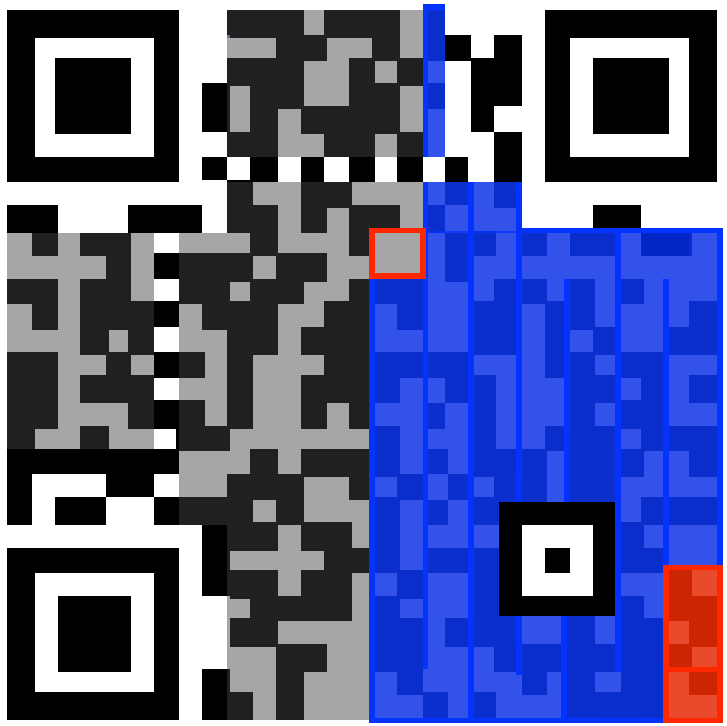
- Kennzeichnung des Zeichensatzes
- Kennzeichnung der Anzahl an Zeichen
- Kodierter Text



(MST, 2020)

Inhalt

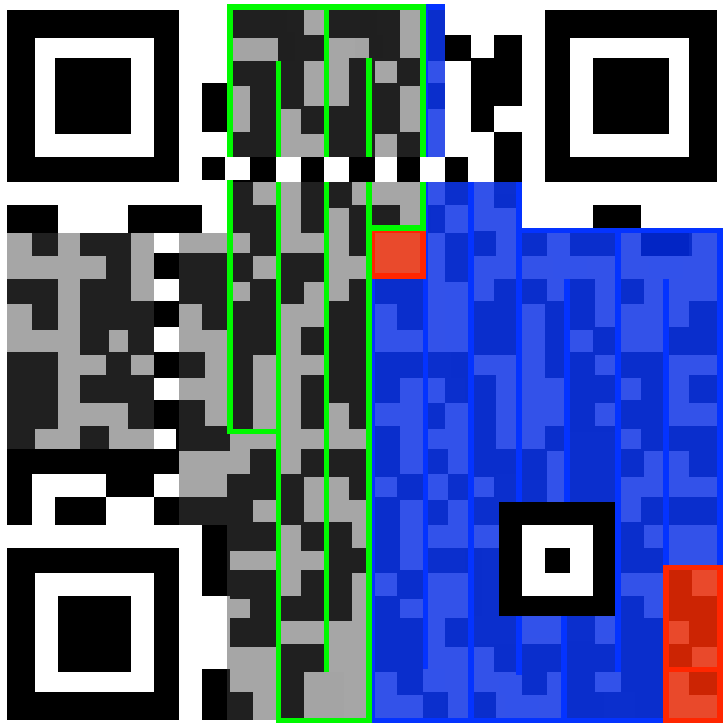
- Kennzeichnung des Zeichensatzes
- Kennzeichnung der Anzahl an Zeichen
- Kodierter Text
- Ende-Kennzeichnung



(MST, 2020)

Inhalt

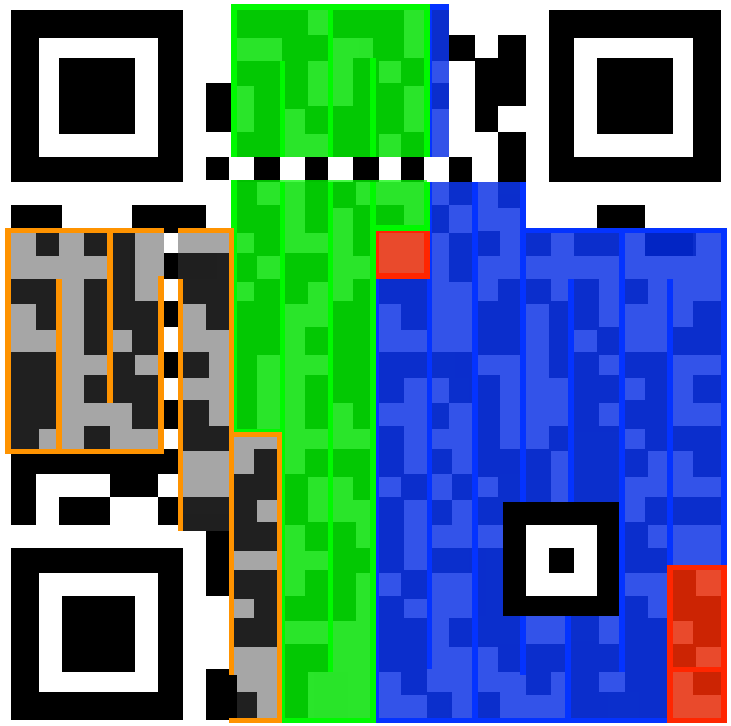
- Kennzeichnung des Zeichensatzes
- Kennzeichnung der Anzahl an Zeichen
- Kodierter Text
- Ende-Kennzeichnung
- Code für Fehlerkorrektur



(MST, 2020)

Inhalt

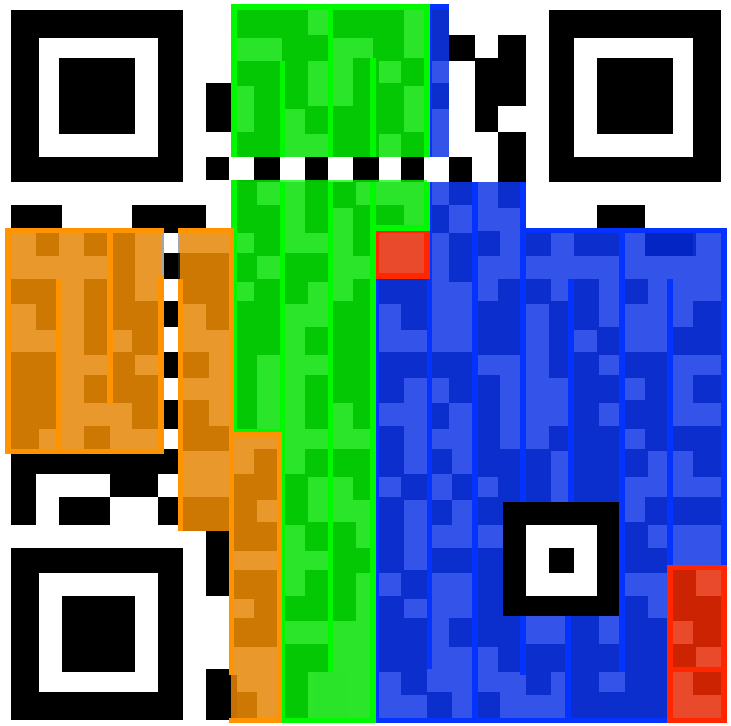
- Kennzeichnung des Zeichensatzes
- Kennzeichnung der Anzahl an Zeichen
- Kodierter Text
- Ende-Kennzeichnung
- Code für Fehlerkorrektur
- Code als Lückenfüller



(MST, 2020)

Inhalt

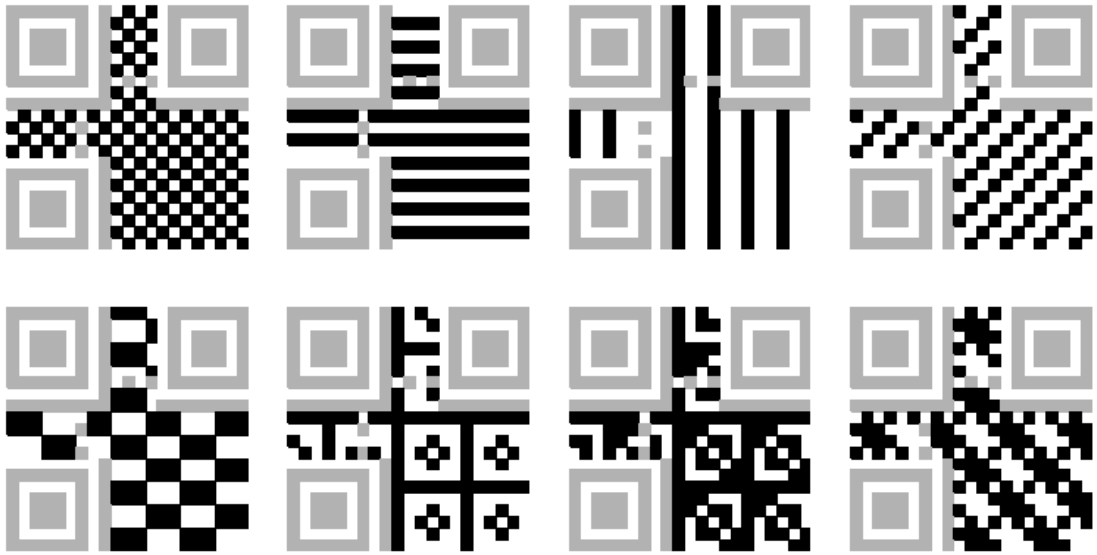
- Kennzeichnung des Zeichensatzes
- Kennzeichnung der Anzahl an Zeichen
- Kodierter Text
- Ende-Kennzeichnung
- Code für Fehlerkorrektur
- Code als Lückenfüller



(MST, 2020)

Masken

- Schablone
- Gut lesbaren QR-Code erhalten
- Kennnummer in Formationformationen gespeichert



(MST, 2020)

Sicherheit und Manipulationsmöglichkeiten

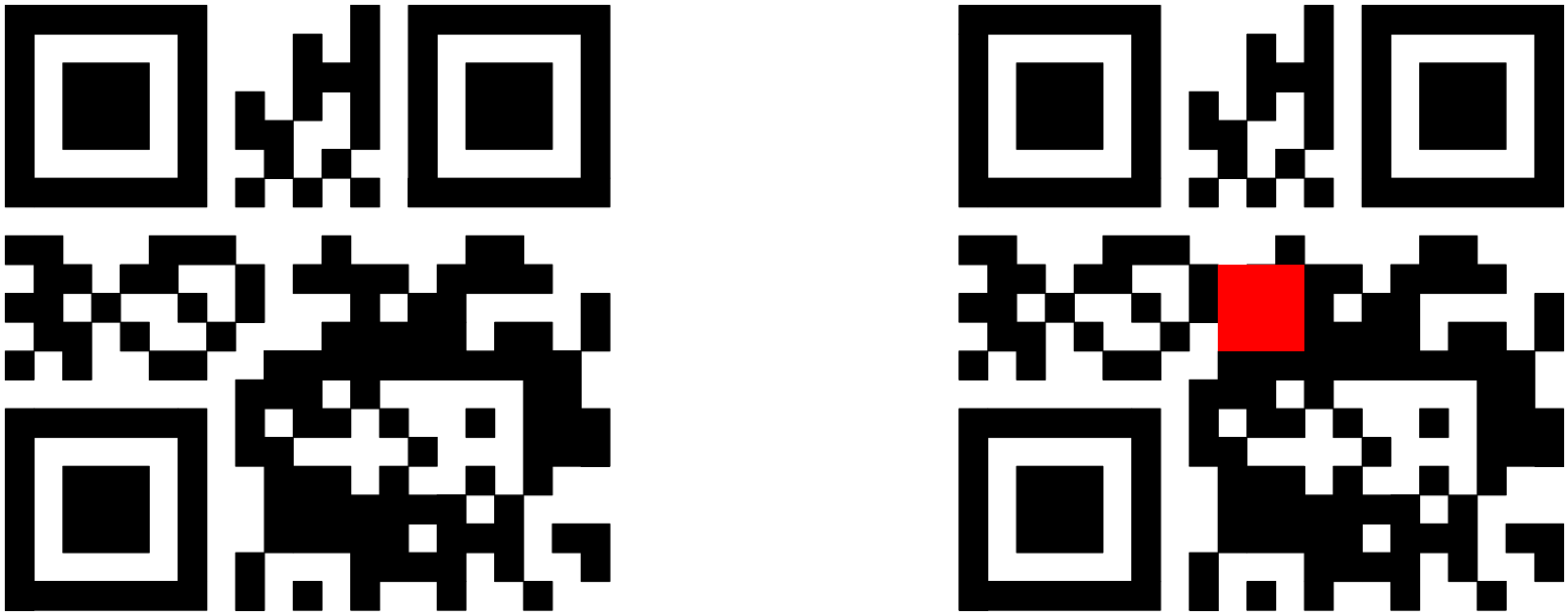
Fehlerkorrektur

- Erlaubt Rekonstruktion beschädigter Daten
- Mittels Reed-Solomon-Code realisiert
- Vier Stufen der Fehlertoleranz
- Höhere Stufe bedeutet weniger Platz für Daten

Low	7%
Medium	14%
Quartile	25%
High	30%

(Kieseberg, 2010)

Beispiel zur Fehlerkorrektur



Trotz rotem Quadrat ist die korrekte Dekodierung möglich

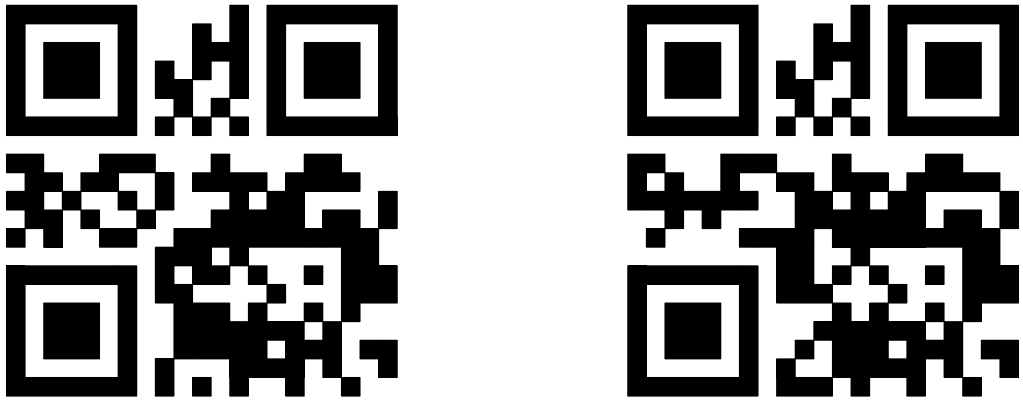
Design QR-Codes

- Zweckentfremdung der Fehlerkorrektur
- Teile des Codes mit Bild oder Logo überlagern
- Echte Lesefehler können nicht mehr ausgeglichen werden
- Meist Korrekturlevel „High“ angewandt

(Foundata, 2019)

Sicherheit

- Fehlerkorrektur sichert Integrität
- Für einen Menschen nicht leicht entzifferbar

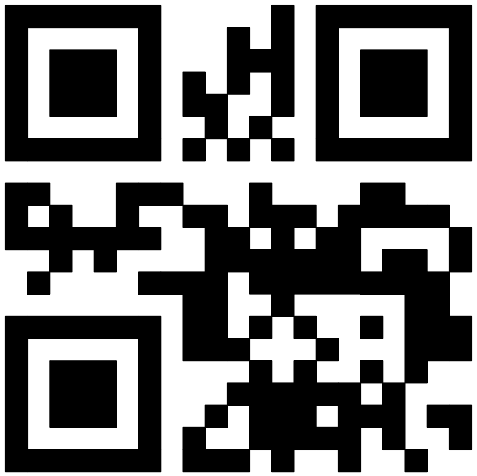


Welcher ist der böswillige QR-Code?

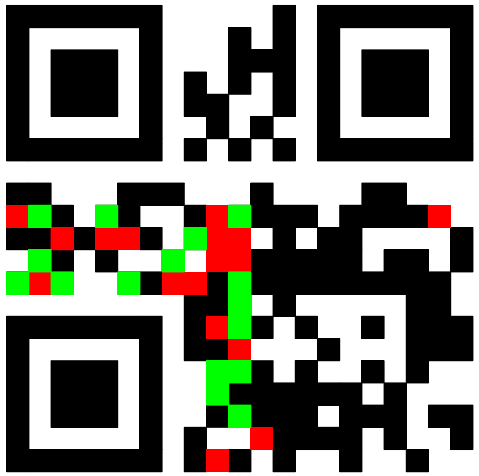
Beispiel eines abgeänderten QR-Codes

WAP kodiert

WBP kodiert



Unterschied



Gezielte Brute Force Methode

Strategien:

- Maske ändern
- Zeichenkodierung verändern
- Länge der Nachricht anpassen:
  - Buffer Underflow
  - Buffer Overflow
- Eine von mehreren Nachrichten modifizieren
- Versuchen die Fehlerkorrektur zu überlisten

Angriff auf die Binärdarstellung

- Dekodieren, Anpassen, Enkodieren
- Teile der Nachricht abändern
- In Binärdarstellung umwandeln
- Mit der originalen Darstellung vergleichen
- Erstrebenswert ist eine niedrige Hamming-Distanz

Angriffsarten

Angriffsbereiche

Automatisierte Interaktion

- SQL-Injection
- Command-Injection

Menschliche Interaktion

- Phishing
- Betrug

Phishing

- Verbreitetste Angriffsart
- Benutzer unvorsichtig

SSL-Stripping = Angreifer greift in Weiterleitung von HTTP ein
Benutzer $\rightarrow$ Angreifer $\rightarrow$ Server

Erstellung QR-Codes

- Erfolgt mittels Tools
- Zu kodierende Information kann angegeben werden
- Viele Auswahlmöglichkeiten

QRGen

Python Skript, schnell bei der Erstellung von QR-Codes

Vordefinierte WordLists

```
C:\Users\lukas\Desktop\Programme\QRGen>python qrgen.py

  e88 88e   888 88e    e88'Y88
 d888 888b  888 888D  d888  'Y   ,e e,  888 8e
C8888 8888D 888 88"  C8888 eeee d88 88b 888 88b
 Y888 888P  888 b,    Y888 888P 888   , 888 888
  "88 88"   888 88b,   "88 88"   "YeeP" 888 888
      b
      8b,    QRGen ~ v0.1 ~ by h0nus

usage: qrgen.py -l [number]
usage: qrgen.py -w [/path/to/custom/wordlist]

Payload lists:
0 : SQL Injections
1 : XSS
2 : Command Injection
3 : Format String
4 : XXE
5 : String Fuzzing
6 : SSI Injection
7 : LFI / Directory Traversal

Tool to generate Malformed QRCodes for fuzzing QRCode parsers/reader

optional arguments:
  -h, --help            show this help message and exit

Options for QRGen:
  --list {0,1,2,3,4,5,6,7}, -l {0,1,2,3,4,5,6,7}
                        Set wordlist to use
  --wordlist WORDLIST, -w WORDLIST
                        Use a custom wordlist

Pay attention everywhere, even in the dumbest spot
```

Beispiel: SQL-Payload

- Payload = jener Teil der Schaden verursacht
- Inhalt WordList wird kodiert
- Kann automatisch ausgeführt bzw. verarbeitet werden

Ergebnis Code, Interpretation

and (select substring(@@version,3,1))=‘S’

Sicherheitsrisiken im Alltag

Verwendung von QR-Codes im Alltag

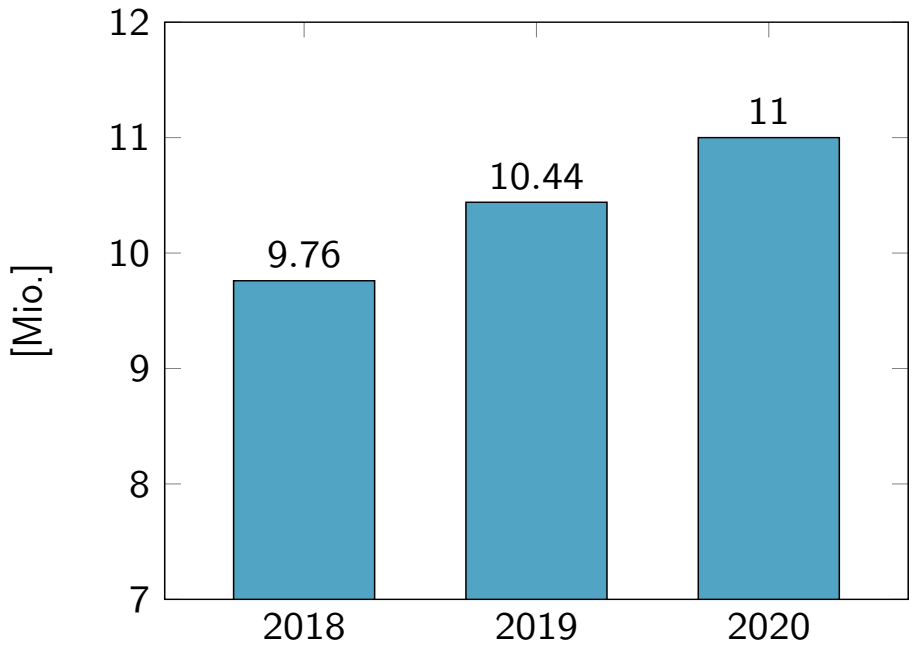
Nimmt seit Jahren stark zu

Hoher Zuwachs in China und Indien

Gründe dafür sind:

- Technologischer Fortschritt bei Smartphones
- Kontaktlose Interaktion werden bevorzugt
- Passive Verbindung zwischen analoger und digitaler Welt (Bsp.: Rabattcodes in Printmedien)

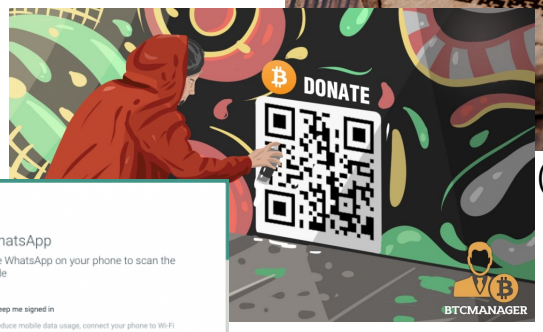
Anzahl an Haushalte in den USA, die QR-Codes gescannt haben [in Millionen] (Scanova, 2020)



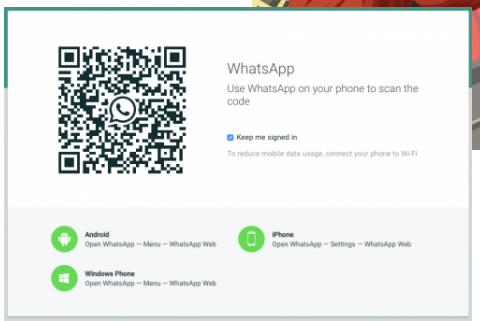
Verwendung von QR-Codes im Alltag

- Produktidentifikation in der Industrie
- In Restaurants als digitales Menü
- Bargeldloses bezahlen
- Passwortlose Anmeldung
- Marketing
- Identifikation
- Uvm.

(Menury, 2020)



(Btcmanager, 2018)



(Gautam, 2015)

Hackerangriffe im Zusammenhang mit QR-Codes

- Erster bekannte Angriff wurde 2011 von Kaspersky SecurityLab entdeckt (Kumar, 2011)
- Unbemerkte Nutzerdatenabfrage bei Google Glass (Kumar, 2013)
- Sicherheitslücke bei der URL-Anzeige in iOS 11 (Khandelwal, 2018)
- Phishing von Daten bei Webseiten mit QR basierten Loginsystemen (Khandelwal, 2016)
- Zutritt zu VIP-Lounges von Fluggesellschaften verschaffen (Greenberg, 2016)

Zusammenfassung

Vorteile von QR-Codes

- Große Datenmenge auf geringer Fläche
- Mehrere Stufen der Fehlerkorrektur
- Im Alltag bereits gut integriert und akzeptiert
- Gute Softwareunterstützung in den meisten Geräten

Nachteile von QR-Codes

- Kodierte Daten schwer lesbar
- Sicherheit stark abhängig von QR-Code-Scanner
- Kein Standard verfügbar, um validierte QR-Codes zu kennzeichnen

Angriffsarten mithilfe von QR-Codes

Angriffe erfolgen meist durch

- URLs die auf schädliche Webseiten zeigen

  Hier werden Schwachstellen in
  - QR-Code-Scannern
  - Web-Browsern

  ausgenützt.
- Spezielle Befehlssätze welche böswillige Aktionen ausführen

  Hier werden Schwachstellen in
  - Betriebssystemen
  - Datenbanken
  - „InternetOfThings“-Geräten

  ausgenützt.

Schutz vor böswilligen QR-Codes

- Vertrauenswürdige QR-Code-Scanner verwenden
  (z.B.: Kaspersky QR-Scanner)
- Überprüfen von gescannten URLs
  URL aus gescannten Daten und im Browser angezeigte muss übereinstimmen
- Automatisches Ausführen von Aktionen deaktivieren
  Dekodierte Daten sollten zuvor manuell überprüft werden
- Verwendung von Zertifikaten in proprietären Lösungen
  Selbst entwickelte Scanner so entwerfen, dass diese nur QR-Codes mit gültigem Zertifikat akzeptieren

Quellen

MST (2020), Fachkonzept – Struktur von QR-Codes. Verfügbar unter: https://www.inf-schule.de/content/1_information/2_darstellunginformation/5_qrcodes/1_struktur/2_strukturelemente/QRCodeBunt.png (bearbeitet)

Foundata (2019), QR-Code-Generator. Verfügbar unter: http://goqr.me/de/qr-code-logo/

TechSpot (2021), QR Codes Explained. Verfügbar unter: https://www.techspot.com/guides/1676-qr-code-explained/

MST (2020), Fachkonzept – Struktur von QR-Codes. Verfügbar unter: https://www.inf-schule.de/content/1_information/2_darstellunginformation/5_qrcodes/1_struktur/2_strukturelemente/QRCodeBunt.png (bearbeitet)

MST (2020), Fachkonzept – Struktur von QR-Codes. Verfügbar unter: https://www.inf-schule.de/content/1_information/2_darstellunginformation/5_qrcodes/1_struktur/2_strukturelemente/QRCodeBunt.png (bearbeitet)

MST (2020), Anwendung von Masken auf einen QR-Code. Verfügbar unter: https://www.inf-schule.de/information/darstellunginformation/qrcodes/masken/anwendung

Kieseberg (2010), QR Code Security. In Proceedings of the 8th International 76 Conference on Advances in Mobile Computing and Multimedia, MoMM '10, Seite 430-435, New York, NY, USA, 2010. Association for Computing Machinery. (bearbeitet)

Quellen

Scanova (2020). QR Code Statistics 2020: Up-To-Date Numbers On Global QR Code Usage. Verfügbar unter: https://scanova.io/blog/qr-code-statistics/ (Angesehen: 07.01.2021)

Kaspersky (2020). Kaspersky QR Code Scanner. Verfügbar unter: https://www.kaspersky.com/qr-scanner (Angesehen: 07.01.2021)

Kumar, M. (2011). QR codes - Next way for Android Malware. Verfügbar unter: https://thehackernews.com/2011/10/qr-codes-next-way-for-android-malware.html (Angesehen: 07.01.2021)

Kumar, M. (2013). Hacking Google Glass with QR Code to sniff user data. Verfügbar unter: https://thehackernews.com/2013/07/Hacking-Google-Glass-QR-Code.html (Angesehen: 07.01.2021)

Khandelwal, S. (2018). QR Code Bug in Apple iOS 11 Could Lead You to Malicious Sites. Verfügbar unter: https://thehackernews.com/2018/03/ios-qr-code-camera.html (Angesehen: 07.01.2021)

Khandelwal, S. (2016). QRLJacking - Hacking Technique to Hijack QR Code Based Quick Login System. Verfügbar unter: https://thehackernews.com/2016/07/qrljacking-hacking-qr-code.html (Angesehen: 07.01.2021)

Greenberg, A. (2016). Fake Boarding Pass App Gets Hacker Into Fancy Airline Lounges. Verfügbar unter: https://www.wired.com/2016/08/fake-boarding-pass-app-gets-hacker-fancy-airline-lounges/ (Angesehen: 07.01.2021)

Menury (2020). Restaurant Menü als QR Code. Verfügbar unter: https://menury.de/img/OwnerImg/Menury_Sticker_QR_wood_preview.jpg (Angesehen: 08.01.2021)

Btcmanager (2018). QR Code in Streetart. Verfügbar unter: https://btcmanager.com/wp-content/uploads/2018/05/Street-Artist-Makes-0.11-BTC-Incorporating-Bitcoin-QR-Code-in-Artworks-1120x669.jpg (Angesehen: 08.01.2021)

Gautam Garg (2015). WhatsApp Web QR Code. Verfügbar unter: https://scanova.io/blog/blog/2015/03/05/whatsapp-qr-code/ (Angesehen: 08.01.2021)

Fragen?

Danke für eure Aufmerksamkeit