Aus 2FA wird 1FA(ch)

2023-07-29 21:56 (Kommentare: 0)

Benutzername und Passwort reichen bei einigen Diensten und Webseiten aus.
Doch man wird mehr und mehr zum "2FA/MFA" überredet. Und das ist gar nicht schwer oder teuer, aber dafür schon ziemlich sicher ...

Machen wir ab heute Betrügern und Hackern doch einfach das Leben schwer.

2FA? MFA?

Benutzername und Passwort kennt jeder. Immer mehr Dienste nutzen jedoch zusätzlich einen "zweiten Faktor" (also ein zweites Sicherheitsmerkmal zusätzlich zum Passwort).
Dadurch soll erreicht werden, dass - wenn das Passwort zu einfach ist oder geknackt wurde - es trotzdem immer noch nicht möglich ist sich an dem jeweiligen Konto an zu melden. So wie z. B. das PIN/TAN Verfahren beim Onlinebanking.

Siehe Wikipedia 2FA und MFA.

Beliebt, bekannt, besonders einfach: TOTP

Einer der weit verbreiteste 2FA ist das TOTP.
Das Prinzip dabei ist sehr einfach: alle 30 Sekunden gibt es eine neue, sechsstellige Zahl wie z. B. 259 367, 774 189, 468 229, 328 979, ...
Diese Reihenfolge ist aber nur insoweit zufällig, dass nur der jeweilige Dienst (z. B. der Online-Shop, bei dem man einkaufen möchte) und man selbst die richtige Reihenfolge der Zahlen kennt. Die Wahrscheinlichkeit, dass irgendjemand innerhalb von 30 Sekunden die gerade aktuell richtige Zahl erraten kann tendiert schon recht Nahe gegen Null.
Natürlich muss man sich die Zahlen nicht selbst merken, dass macht z. B. eine App auf dem Smartphone für einen.

Und wie komme ich an meinen 2FA TOTP?

Erst einmal muss der Dienst (z. B. der Onlineshop) ein solches Sicherheitsmerkmal anbieten.
Wenn man dann das "2FA" Merkmal aktiviert, kommt man irgendwann an den Punkt, wo ein solcher QR-

Code anbietet:


Anmerkung: die Abbildung des QR-Codes habe ich natürlich verfremdet, da es sich um MEINEN Code handelt!

Gut, den QR-Code möchte man natürlich nicht abmalen, also sollte man sich tunlichst vorher eine entsprechende (vertrauenswürdige!) App auf sein Smartphone laden.
Da wären dann z. B. der Microsoft Authenticator oder aber auch der Google Authenticator.
Mit der jeweiligen App scannt man dann den QR-Code ab und schon hat man auf dem Display einen sechsstelligen Code, der alle 30 Sekunden wechselt.

Diesen Vorgang kann man dann mit jedem Dienst wiederholen, bei dem man TOTP als 2FA einrichten möchte.

Ja, aber ...

Natürlich gibt es einige Bedenken, die wir hier auch mal betrachten werden.

Wir benötigen den Zugang zu einem Dienst mit mehreren Personen

- Kein Problem. Den QR-Code kann man auch mit mehreren Geräten fotografieren. Dabei hat jedes Gerät, welches den QR-Code fotografiert einen Zugang.

Was ist, wenn ich mein Smartphone verliere oder es defekt ist?

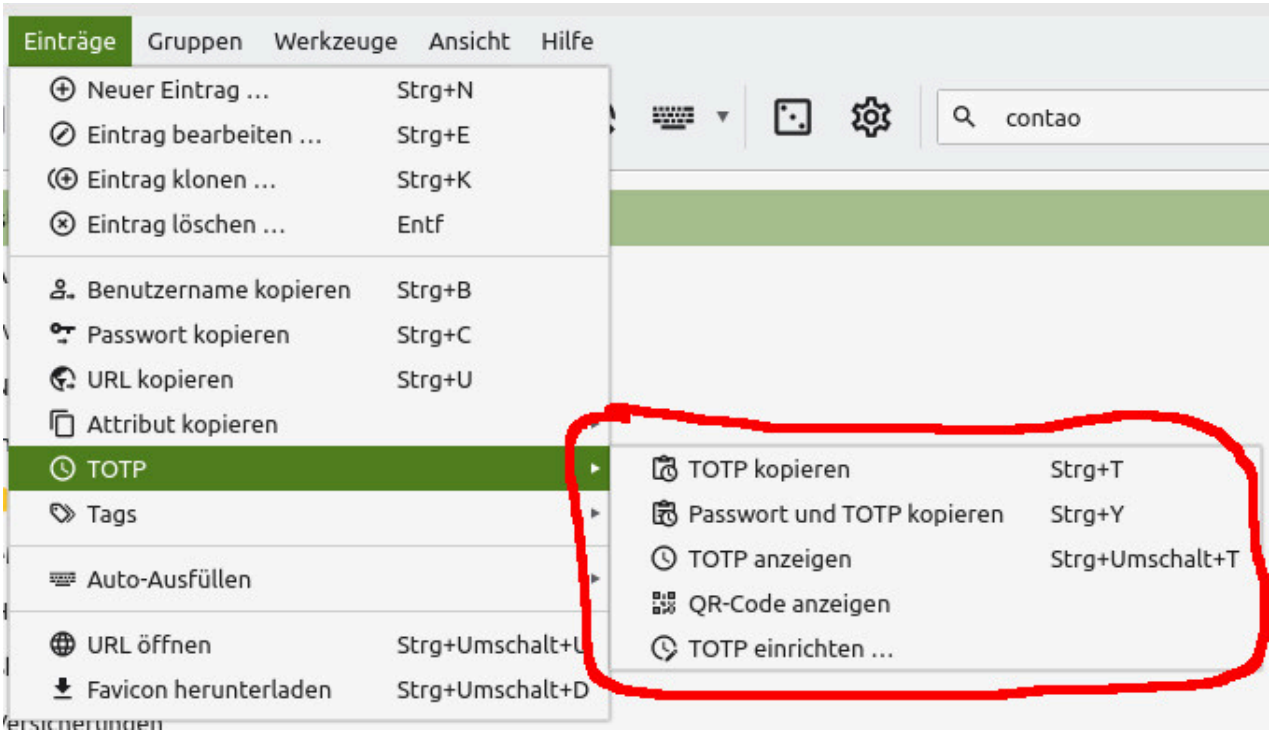
- Dann gilt das, was für alle Daten gilt: es sollte eine Datensicherung geben. Doch das ist sehr einfach. Denn wenn man den QR-Code scannt, steht darunter i. d. R. ein Text wie etwa "Can't scan it?" oder "Sie können den Code nicht lesen?":

  
  Can't scan it?

  Ein Klick auf diesen Link zeigt den Code an, der von der Kamera als QR-Code gescannt würde, in etwa so wie z. B. DCVOQUCNRRWXNQXPWERQXMZF. Diesen Code kann man kopieren und - wie man es mit allen Passwörter machen sollte - in den kostenlosen Programmen KeePass

(KeePass benötigt das ebenfalls kostenlose Plugin KeyTrayTOTP) oder KeePassXC automatisch verschlüsselt speichern.

Diese Programme können dann sowohl den QR-Code erneut als auch den jeweils aktuell gültigen sechsstelligen Code dann jederzeit wieder anzeigen lassen.



Beispiel: Anzeige eines TOTP Codes in KeePassXC

Wer das nicht kann oder möchte, kann immer noch den QR-Code als Bildschirm "Hardcopy" ablegen. Doch auch dieses Hardcopy sollte - aus Sicherheitsgründen - verschlüsselt und möglichst auch noch "offline" auf z. B. einem USB-Stick außerhalb des Rechners abgespeichert werden.

Tipp: aus Sicherheitsgründen sollte man die TOTP QR-Codes nicht in derselben KeePass Datei speichern, in der man auch seine "normalen" Passwörter gespeichert hat. Ansonsten hätte jemand, der in den Besitz der KeePass Datei gelangt direkt Zugriff auf die normalen Passwörter UND die TOTP QR-Codes.
Da man die TOTP QR-Codes nur beim Ersetzen eines Gerätes durch Verlust oder Neukauf benötigt (also eigentlich so alle paar Jahre), kann die Datei mit diesen Codes mit einem sehr, sehr starken Passwort verschlüsselt werden.

Was ist mit dem QR-Code, wenn ich ein neues Gerät kaufe?

- Einige der Authenticator-Apps können die QR-Codes über die Cloud auch auf weitere und/oder neue Geräte synchronisieren. Unabhängig davon, ob die alten Geräte defekt sind oder gestohlen wurden. Außerdem kann man sich die abgespeicherten QR-Codes in KeePass bzw. KeePassXC (siehe oben) jederzeit neu anzeigen lassen um weitere und / oder neue Geräte hinzuzufügen.

Mein erstes Gerät ist gestohlen, das zweite defekt, das dritte habe ich nicht dabei und ich habe keine Sicherungskopie in KeePass erstellt

- Nun, es gibt den Spruch "kein Datensicherung - kein Mitleid" sowie "keine Arme, keine Kekse". Bei vielen Diensten kann man sich für den Notfall noch alternativ an eine zuvor registrierte E-Mail auch einen temporären Schlüssel senden lassen. Aber diesen Service unterstützen nicht alle Dienste.

Ich habe keine Möglichkeit mehr meinen TOTP Code generieren zu lassen, wie kann ich ihn umgehen?

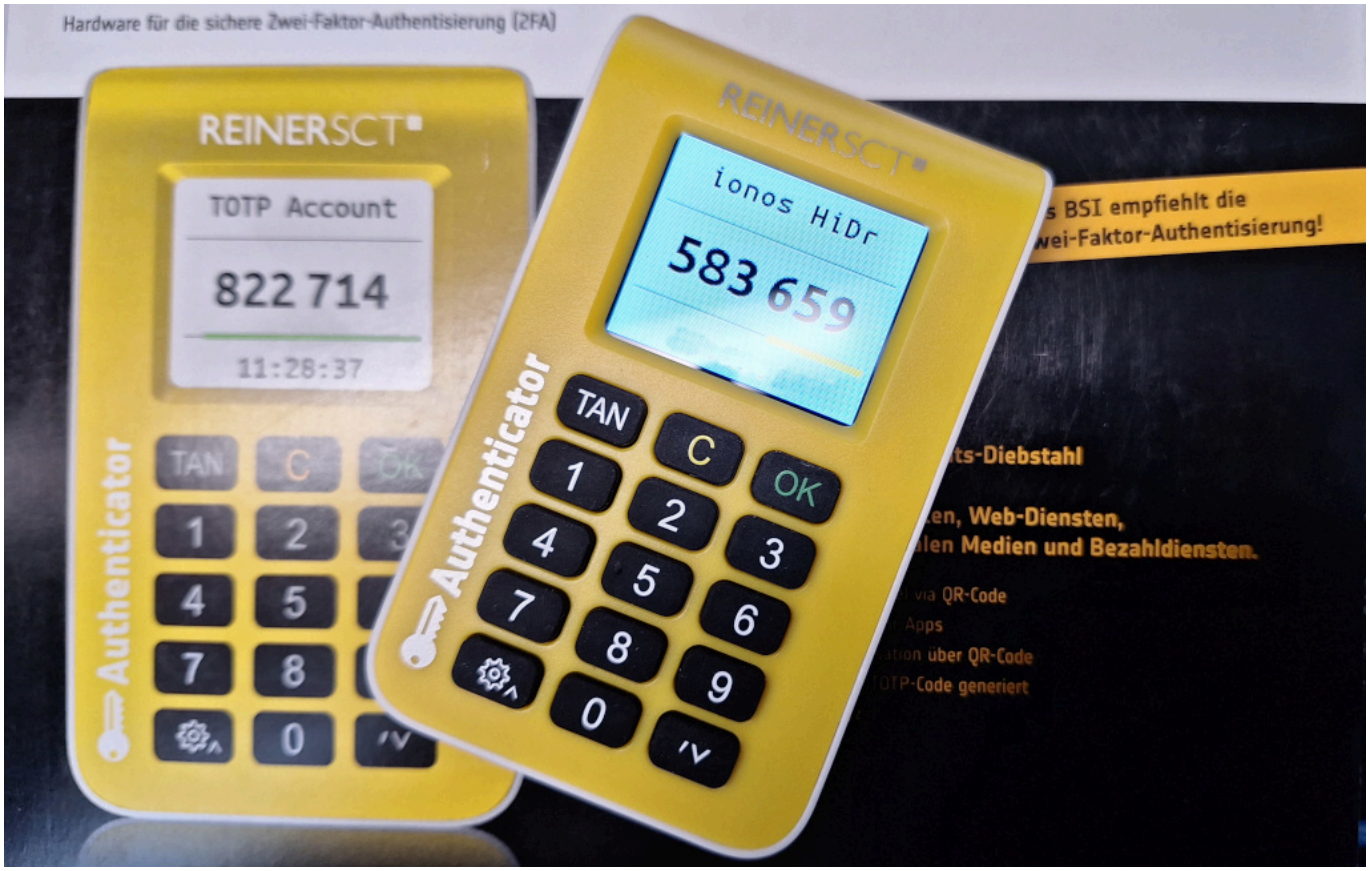
- Jetzt kommen wir zu einer wirklich schlechten Nachricht: gar nicht. Denn wäre es ganz einfach möglich die Haustüre ohne Schlüssel zu öffnen, wozu sollte man dann überhaupt noch Türen abschließen.
  Da hilft nur noch eines: den Anbieter des Dienstes wie z. B. den Onlineshop kontaktieren.

Ist 2FA bzw. TOTP auch sicher?

- Also sicher ist nur eines. Alles andere ist nicht so sicher. Aber brauchte ein Angreifer bisher "nur" Benutzername und Passwort, so muss er nun auch noch innerhalb von 30 Sekunden die richtige sechsstellige Zahl finden. Wie groß die Wahrscheinlichkeit möge jeder bitte selbst probieren.

Geht es denn noch sicherer?

- Aber latürnich. Ein möglicher Angriffsvektor ist dann immer noch das Smartphone. Es hat eine Verbindung zum Internet und könnte einen Virus / Trojaner haben, der den jeweils aktuell gültigen Code kopiert und per Internet versendet.
  Aber auch dagegen gibt es eine Waffe: ein eigener Authenticator wie z. B. den Reiner-SCT Authenticator, der keinen USB- oder Internetanschluss hat. Somit unknackbar. Und sollte es doch jemand versuchen: wer beim Einschalten des Gerätes 5x den (optionalen!) 5-12 stelligen PIN falsch eingibt löscht mit der letzten, fünften Falscheingabe alle im Gerät gespeicherten PINs. Das Gerät befindet sich dann wieder im Auslieferungszustand.



Quanta Costa?

Achtung, Spoiler: dieses Plus an Sicherheit ist prinzipiell kostenlos.
Nachdem jetzt klar ist, dass es ziemlich sicher ist und auch nicht besonders schwer ein zu richten, kommen wir nun zur Wurzel aller Fragen, nämlich die des Preises.
Die Dienste bieten den TOTP 2FA eigentlich immer kostenlos an. Mir ist nicht ein einziger Dienst bekannt, der Geld dafür nimmt.
Wer sowieso schon ein Smartphone sein eigen nennt, kann die Authenticator Apps von z. B. Microsoft oder Google kostenlos herunterladen.
Zur Dokumentation von Passwörtern und den QR-Codes ist sowohl die Software KeePass (mit dem notwendigen Plugin) als auch KeePassXC ebenfalls kostenlos.

Und wer auf Nummer sicher gehen möchte und sich den Reiner SCT Authenticator zulegt, muss je nach Angebot irgendwas zwischen 40 und 50 Euro auf den Tisch legen. Wer sich das Gerät als Backup für das Smartphone zulegt, spart letztendlich trotzdem Geld, denn günstiger (und sicherer) als ein 2. Smartphone als Backup ist er allemal.

Zusammenfassung

1. TOTP als 2FA beim gewünschten Dienst aktivieren und sich den QR-Code anzeigen lassen
2. Mit einem oder mehreren Smartphone und / oder Authenticator Gerät den QR-Code scannen
3. Den auf dem Bildschirm angezeigten QR-Code als Hardcopy abspeichern, oder noch besser: den jeweiligen QR-Code als Buchstabenfolge anzeigen lassen und in KeePass/KeePassXC abspeichern

Wer Fragen hat, kann diese gerne unten in den Kommentaren posten ...

Kommentare

Einen Kommentar schreiben