IAM – Circle

Trade off zwischen Usability und Security bei der Authentifizierung

Sicheres IAM für Bürger & Juristische Personen

Bern, Januar 2024

ti&m

Speaker / Workshopleitung

Jan Ramseyer

PM ti&m Authentication

Fabian Dobler

Head Security Integration, ti&m

Chris Turtschi

Lead Interaction Designer, ti&m

Unser Unternehmen

Digital Trust Center – Vertrauen, Kompetenz und Technologie

Fokus: Sichere Authentifizierung

Workshop & Diskussion

ti&m

ti&m steht für technology, innovation & management.

Wir sind Leader für Digitalisierungs-, Security-, Innovationsprojekte und -produkte in der Schweiz und streben dasselbe in weiteren internationalen Wirtschaftszentren an.

Wir digitalisieren Ihr Unternehmen.

600+

Experten

Consultants, Analysts, Designers, System- & Software-Engineers.

No. 1

In der Schweiz

für Digitalisierungs-, Security-, Innovationsprojekte und -produkte.

100 %

Vertikale Integration

der gesamten IT-Wertschöpfungskette.

6

Standorte

Zürich, Bern, Basel, Frankfurt am Main, Düsseldorf und Singapur.

20 %

Wachstum pro Jahr

Expertise in Digital Banking & Finance, Insurance, E-Government & Public, Transport & Logistics, Life Science & Industry, Retail und Cyber Defense macht uns zum richtigen Partner.

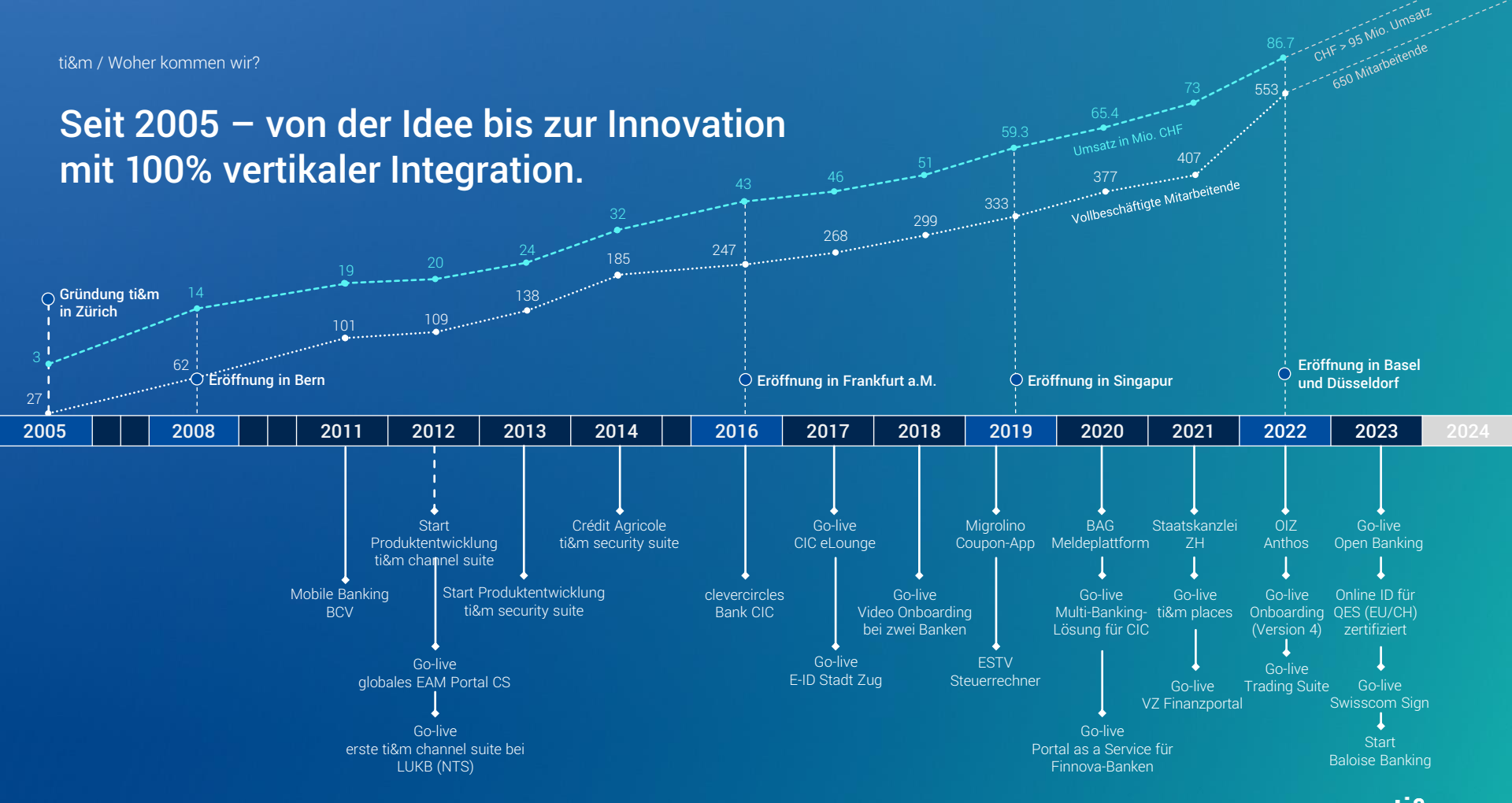
Top 10

Der grössten, inhabergeführten Schweizer IT-Firmen

2005 gegründet und seitdem zu 100 % inhabergeführt.

ti&m

Seit 2005 – von der Idee bis zur Innovation mit 100% vertikaler Integration.

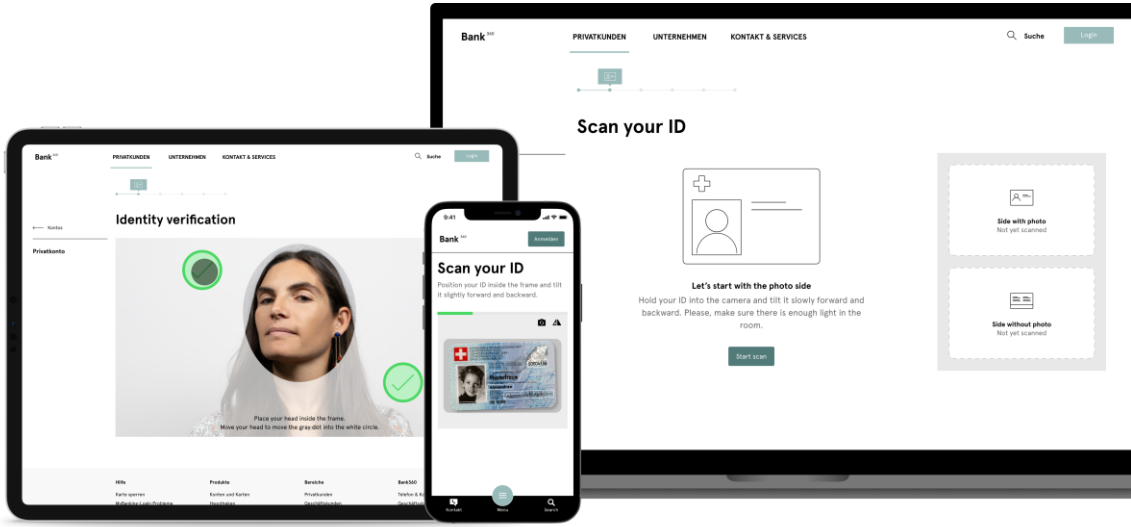


ti&m

Onboarding Suite

Kunde zu werden ist keine Aufgabe. Sondern ein Erlebnis.

ti8m.com/products/onboarding



Die Eröffnung eines Bankkontos ist viel schwieriger, als es sein sollte. Compliance-Prüfungen, alte Softwaresysteme und Medienbrüche schrecken Ihre digitalaffinen Kunden ab, die ihr Konto mit nur wenigen Klicks eröffnen wollen. Schaffen Sie ein reibungsloses, nutzerorientiertes Onboarding-Erlebnis, das selbst Ihre jüngsten Besucher beeindruckt. Machen Sie Webseitenbesucher zu Bankkunden. Mit einem Klick.

01 Effizient und flexibel
Passen Sie den Identifikationsprozess an die speziellen Anforderungen Ihres Geschäfts an.

02 24/7 Verfügbarkeit
Rund um die Uhr parat für Ihre Kunden.

03 Anbindung an Ihr Kernbankensystem
Automatischer Übertrag der Neukundendaten inklusive Doublettencheck.

04 Innovative Technologie
Unschlagbar in Verbindung mit unseren innovativen und patentierten ti&m onlineID und/oder ti&m videoID Services.

Security Suite

«Sicher» als Standard. Ohne Kompromisse.

ti8m.com/products/security

Security Consulting
Ob Beratung, Projektbegleitung, Entwicklung oder Betrieb – wir bieten Sicherheit aus einer Hand.

Security Engineering
Komplexe Technologie für sichere Benutzererlebnisse

ti&m security suite
Sichere Authentifizierung für all Ihre digitalen Services

Unternehmen aller Branchen und jeder Grösse haben die gleichen Erwartungen, wenn es um die Sicherheit ihrer digitalen Assets geht – keine Kompromisse! Unsere Security Produkte und unser Know-how in allen Bereichen der Informationssicherheit sorgen dafür, dass Ihr Unternehmen jederzeit sicher auf Kurs bleibt. Von der Idee bis zum Betrieb sind wir der ideale Partner für alle Ihre Sicherheitsbedürfnisse.

01 Holistische Security Strategien
Umfassende Sicherheitsberatung unter Berücksichtigung Ihrer speziellen Anforderungen.

02 Umfassendes Security Engineering
Sichere Infrastrukturen und Netzwerktopologien, Entwicklung von sicherheitskritischen Applikationen.

03 Schweizer Authentisierungslösung
Schützen Sie, was Ihnen wichtig ist. Ohne Kompromisse bei der Sicherheit und im Benutzererlebnis.

04 Starke Partnerschaften
Strategische Partnerschaften ermöglichen einen lückenlosen Schutz vor Cyberbedrohungen.

ti&m

ti&m swiss eGov cloud

Sichere Digitalisierung. Aus der Schweiz, für die Schweiz.

ti8m.com/services/cloud/swiss-egov-cloud

Die ti&m swiss eGov cloud kombiniert das Bedürfnis der öffentlichen Verwaltung nach Lokalität und Privatheit der anvertrauten Daten mit der Effizienz, Skalierbarkeit und Sicherheit eines professionellen Cloud-Angebotes. Wir betreiben Ihre individuellen Applikationen und Services in zertifizierten Schweizer Rechenzentren – skalierbar, flexibel und jederzeit bestens geschützt.

01 Lokale, vertikal organisierte Teams erarbeiten in enger Abstimmung mit den Institutionen echt schweizerische Lösungen.

02 Unsere ti&m swiss eGov cloud verwaltet die Daten in der Schweiz und unter Schweizer Recht.

03 Standard Sicherheitskomponenten des öffentlichen Dienstes «out-of-the-box».

04 Von Strategie und Governance bis zu Entwicklung und Betrieb.

Unser Unternehmen

Digital Trust Center – Vertrauen, Kompetenz und Technologie

Fokus: Sichere Authentifizierung

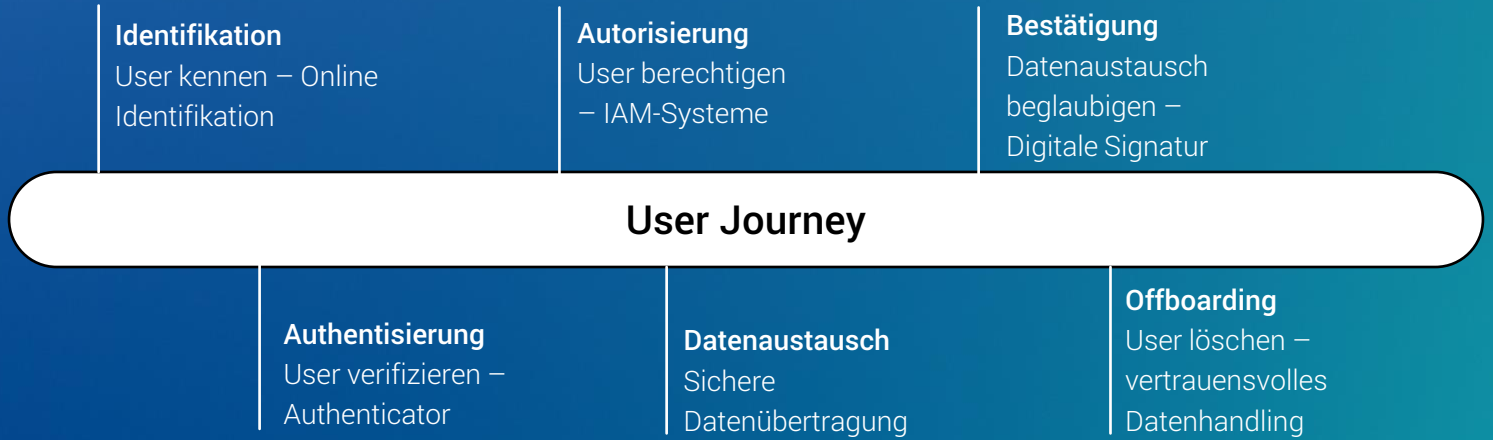
Workshop & Diskussion

ti&m

Security Services von ti&m –
Der Weg hin zum Digitalen Trust.

ti&m Digital Trust Center

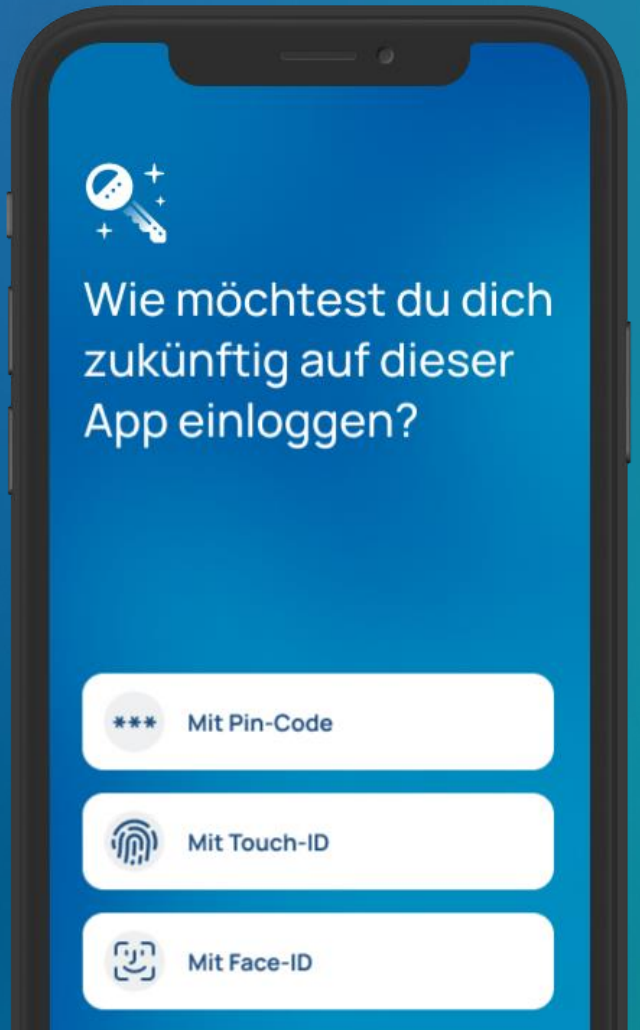
Kompetenz entlang des gesamten User Journey



ti&m

Mehr Sicherheit durch Multifaktor-Authentisierung

Der perfekte zusätzliche Faktor zu Benutzername und Passwort.



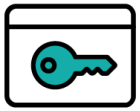
ti&m

Passwortloser Zugang
die sichere Alternative mit unschlagbarer Usability

Face ID oder Fingerabdruck ermöglichen eine einfache Authentifizierung ohne Login-Daten.

ti&m

ti&m security suite Übersicht



Multi Factor Authentication

Erhöhen Sie die Sicherheit drastisch, indem Sie zusätzlich zu Username und Passwort einen weiteren Authentisierungsfaktor bspw. Eine Authentisierung via ti&m secure app verlangen.

Passwortlose Authentisierung

Ersetzen Sie Usernamen und Passwörter durch stärkere Authentisierungsfaktoren wie Fingerabdrücke oder Facemaps. Keine verlorenen Passwörter, kein administrativer Aufwand.

Transaktionsbestätigung

Mit Transaction Signing können User wie beim Bezahlen mit Kreditkarten eine Transaktion bestätigen, ohne einen Code eingeben zu müssen. Für mehr Sicherheit und Usability.

ID-Check 2nd Factor Recovery

Unsere KI-basierte Personenidentifikations-Technologie ermöglicht eine automatisierte, kostengünstige Kontowiederherstellung bei einem Wechsel des 2. Faktors wie dem Smartphone.

ti&m

Unser Unternehmen

Digital Trust Center – Vertrauen, Kompetenz und Technologie

Fokus: Sichere Authentifizierung

Workshop & Diskussion

ti&m

Password Sniffing

Link zum Video

Passwörter sind unsicher

81%

der Sicherheitsverletzungen sind auf die Verwendung schwacher oder gestohlener Zugangsdaten zurückzuführen

4 von 5

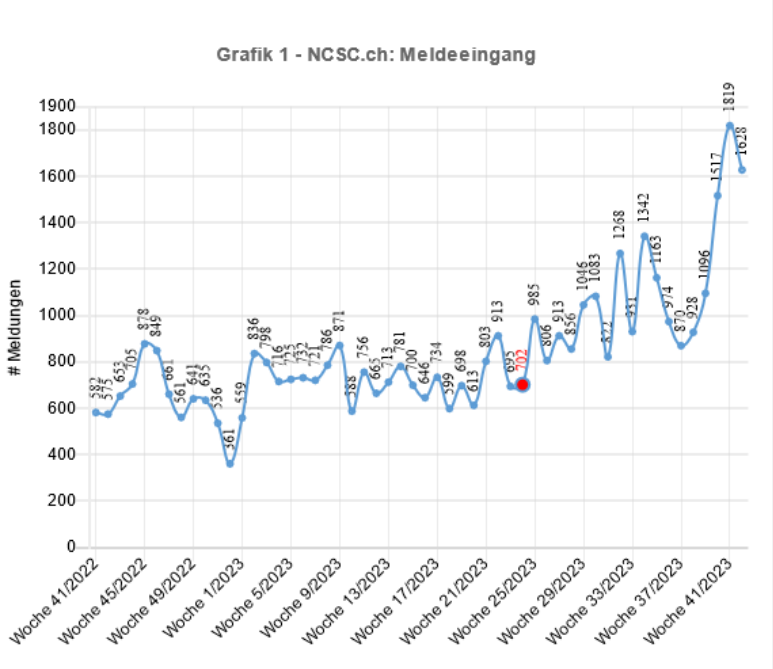
verwenden das identische Passwort für unterschiedliche Anmeldungen bzw. Dienste

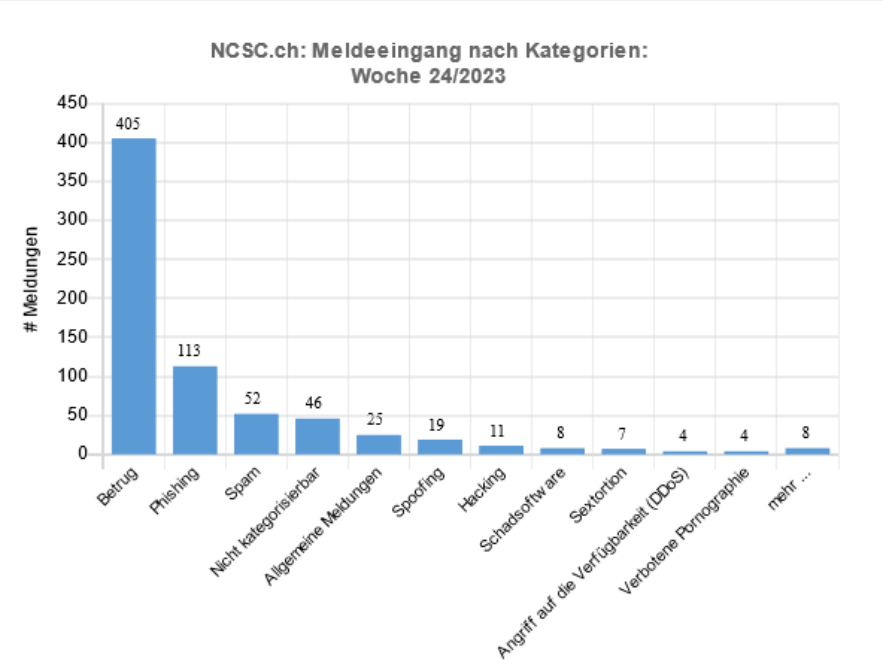
«123456»
«passwort»

gehören immer noch zu den beliebtesten Passwörtern

2.2 Milliarden Benutzernamen und Passwörter wurden 2019 veröffentlicht.

Die Zahlen dazu aus der Schweiz

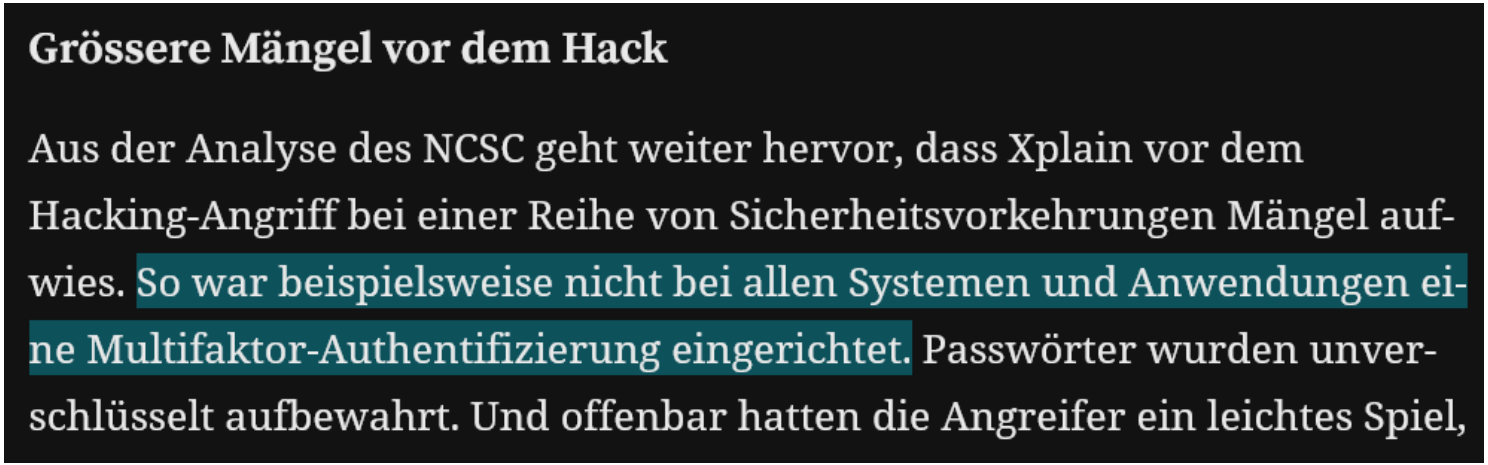




Der Mensch ist die grösste Schwachstelle

Quelle: https://www.ncsc.admin.ch/ncsc/de/home/aktuell/aktuelle-zahlen.html

Datensicherheit



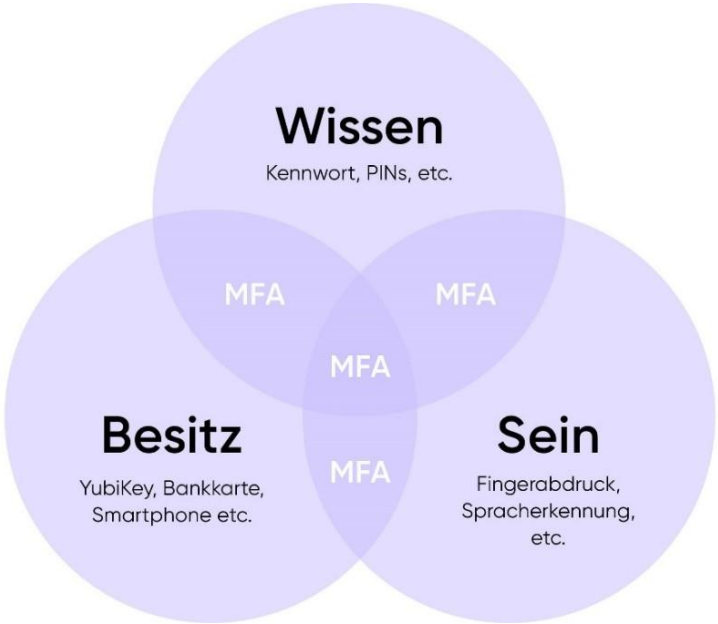
Grössere Mängel vor dem Hack

Aus der Analyse des NCSC geht weiter hervor, dass Xplain vor dem Hacking-Angriff bei einer Reihe von Sicherheitsvorkehrungen Mängel aufwies. So war beispielsweise nicht bei allen Systemen und Anwendungen eine Multifaktor-Authentifizierung eingerichtet. Passwörter wurden unverschlüsselt aufbewahrt. Und offenbar hatten die Angreifer ein leichtes Spiel,

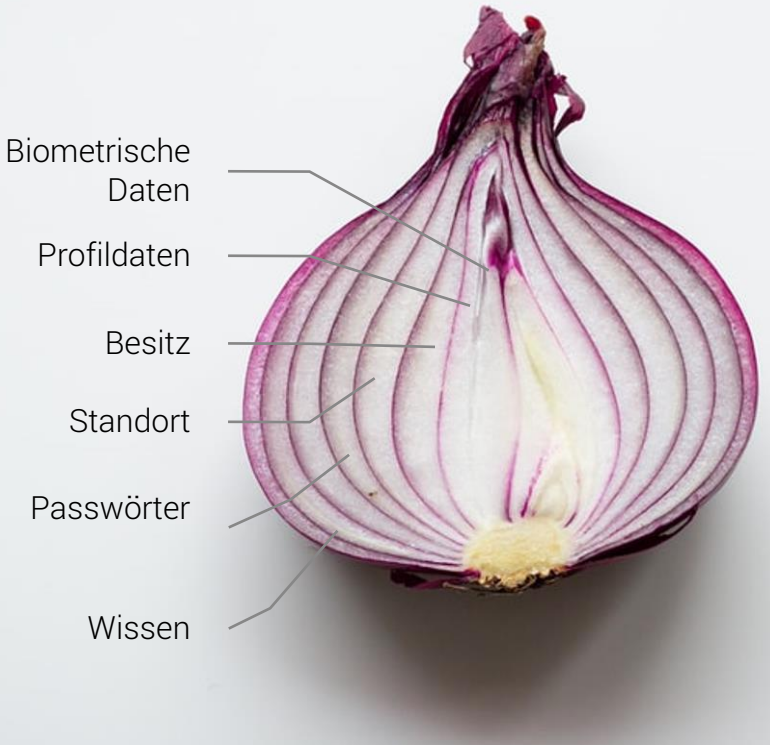
Quelle: https://www.bernerzeitung.ch/gehackt-schweiz-haelt-an-it-firma-xplain-fest-464556309188

Multi Factor Authentication (MFA)

- Zwei-Faktor Authentisierung oder Multi Faktor Authentisierung
- Verschiedene Faktoren:
  - Etwas, das Sie kennen, wie eine PIN oder Antwort auf eine Sicherheitsfrage
  - Etwas, das Sie haben, wie ein Gerät, ein Einmalcode/-passwort oder Hardware-/Software-Token.
  - Oder etwas, das Sie ausmacht, wie biometrische Merkmale (Fingerabdruck oder Gesichts-ID) oder kontextuelle Signale wie ein Standort.



Quelle: https://www.bizfactory.tech/blog/2fa-vs-mfa-was-ist-der-unterschied



Nicht jeder Faktor ist gleich sicher. Wie bei einer Zwiebel sind die äussersten Schichten am einfachsten zu entfernen.

Nicht jeder Faktor ist allerdings gleich userfreundlich.

Usability von MFA im Detail

– **Aufgabeneffizienz** – Die Zeit für die Registrierung und Zeit für die Authentifizierung mit dem System ist möglichst kurz.
– **Aufgabeneffektivität** – die Anzahl der Anmeldeversuche zur Authentifizierung mit dem System ist möglichst tief.
– **Benutzer:innenpräferenz** – es sollte berücksichtigt werden, ob die Benutzer:innen ein bestimmtes Authentifizierungsverfahren gegenüber einem anderen bevorzugen.

– Lässt sich einfach aber sicher wiederherstellen (Bsp. Gerätewechsel oder Geräteverlust).

– Verschiedene Usergruppen berücksichtigen bspw. auch Betrieb / interne IT.

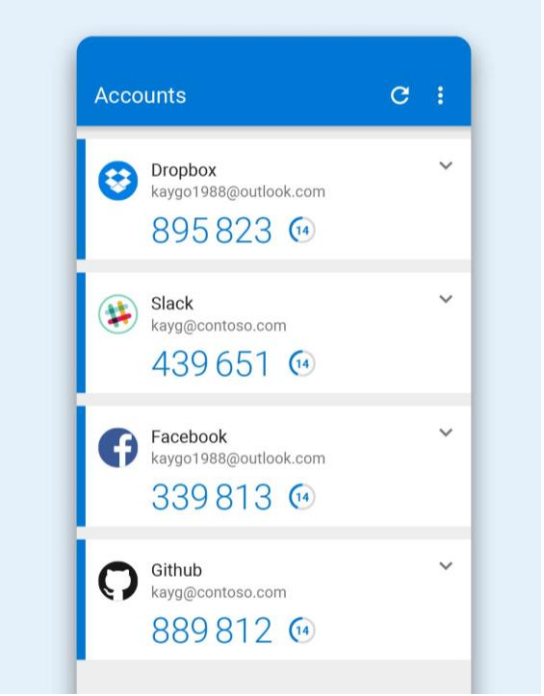
Sichere MFA-Lösungen

- Sicher vor Phishing
  - Keine Codes werden irgendwo eingegeben
- Sicher vor Fatigue Attacks
  - Keine Push-Funktion
- Einsatz von Geräte-Login
  - Geräteauthentifizierungsschnittstelle einsetzen
- Same Device MFA
  - PIN oder Biometrie funktioniert nur auf dem lokalen Gerät
  - Keine Schlüssel in der Cloud

Quelle: https://www.security-insider.de/wie-sicher-ist-multi-faktor-authentifizierung-wirklich-a-4f9ea0b2a4217b49cffdbb5cef91f798/

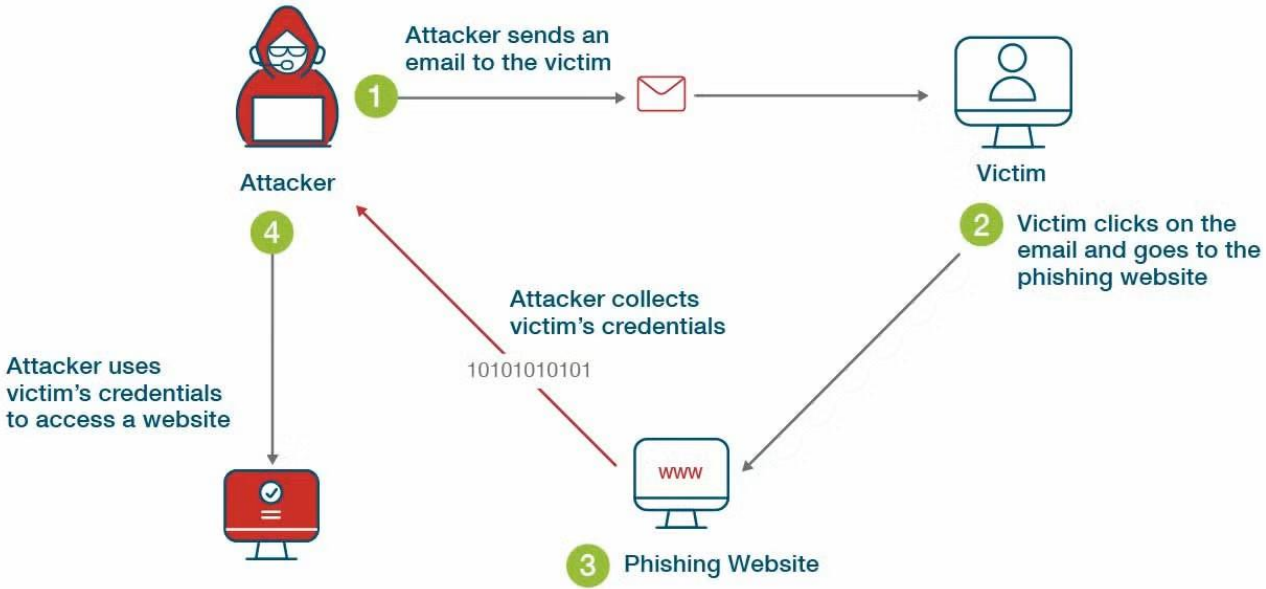
MFA Methoden (Auswahl)

- **Hardware Token**
  - Sicherheitsschlüssel, die laufend Codes generieren.
- **Push-Benachrichtigung**
  - Signal an Endgerät (meist Smartphone), um den Zugriff zu bestätigen resp. abzulehnen.
- **SMS-Verifizierung**
  - Nachricht mit an eine vertrauenswürdige Telefonnummer, mit Code, welcher bspw. auf Website eingegeben werden kann.
- **OTP-App**
  - Die App generiert einen einmaligen Passcode (OTP) für jede Website oder jeden Dienst, den die User mit dem Authentifikator registriert hat.



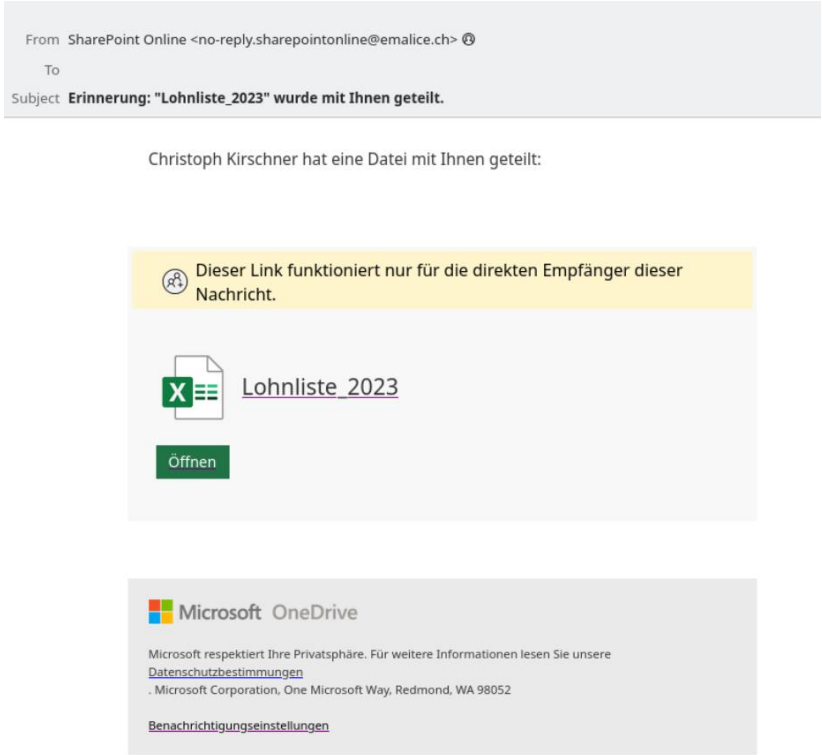
Quelle: https://www.bizfactory.tech/blog/2fa-vs-mfa-was-ist-der-unterschied

Wie können Angreifer vorgehen?



Quelle: https://www.yubico.com/resources/glossary/phishing-resistant-mfa/

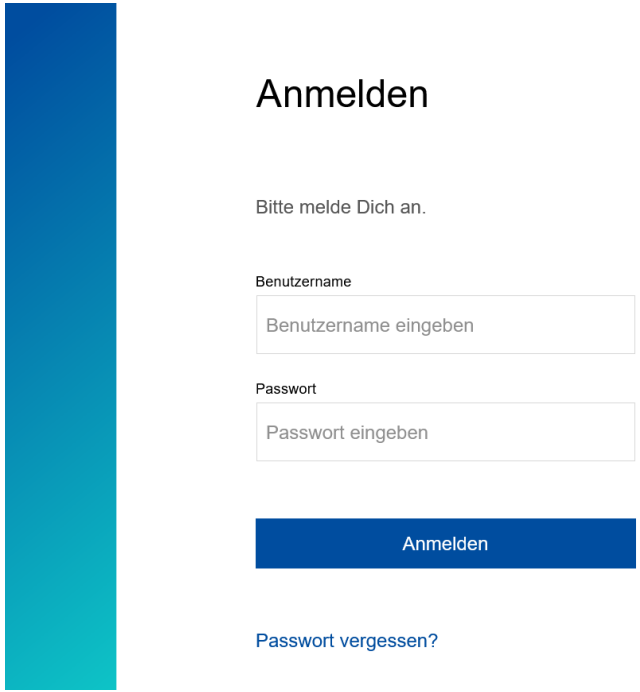
Phishing Beispiel: ti&m MA-Test



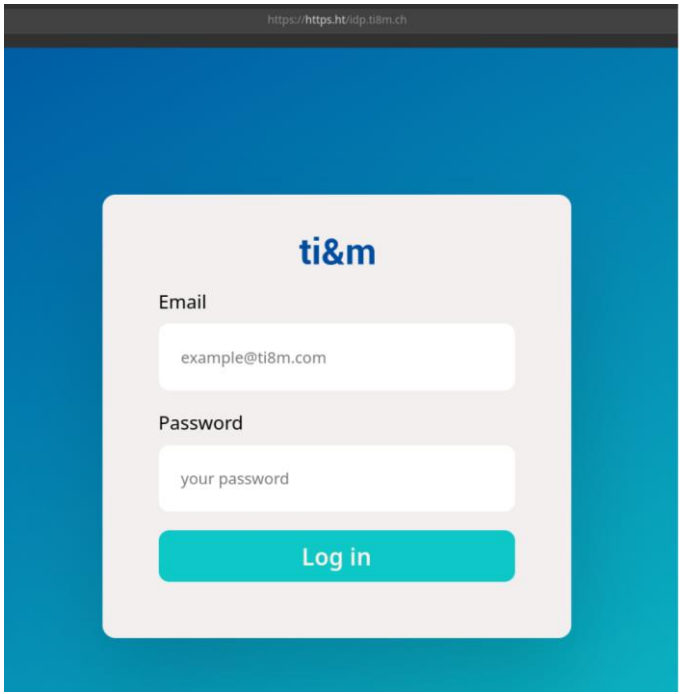
Quelle: ti&m

Schwachstellen Beispiel: ti&m MA-Test

Original



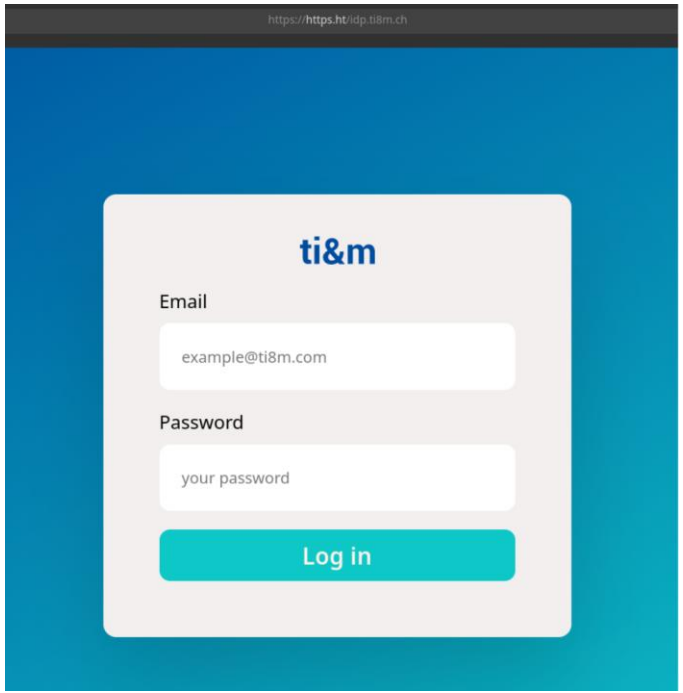
Fake



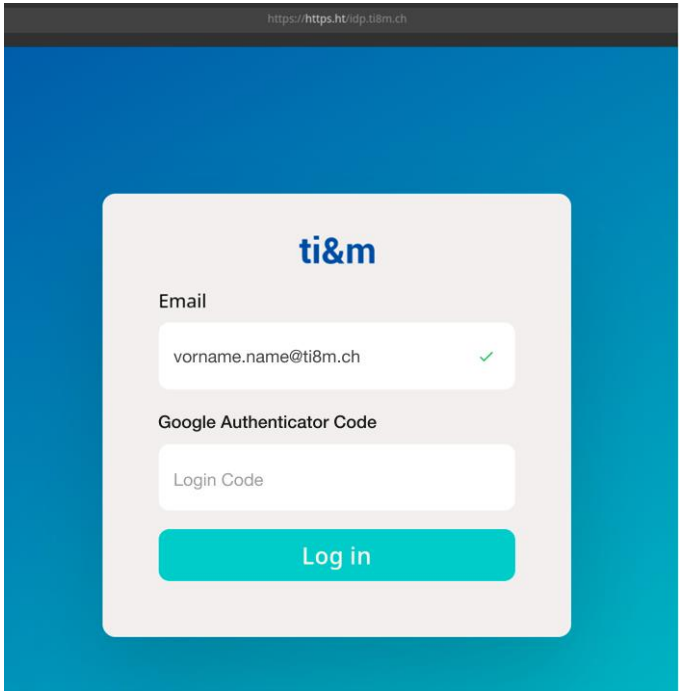
Quelle: ti&m

Schwachstellen Beispiel: ti&m MA-Test

Fake

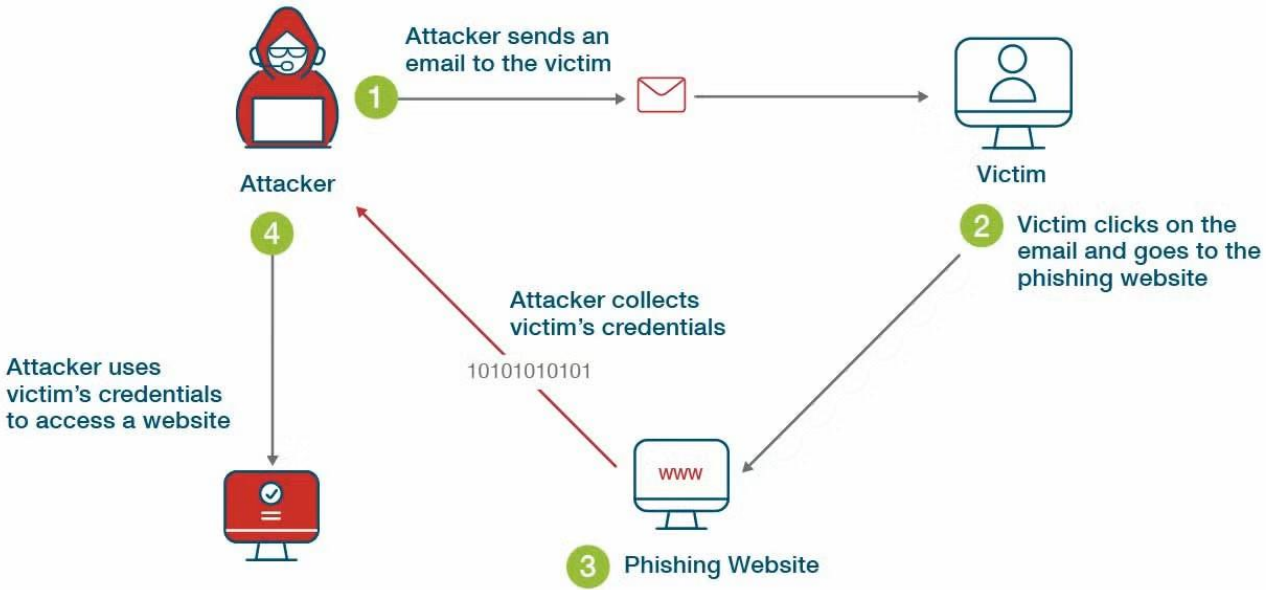


Fake



Quelle: ti&m

Schwachstellen

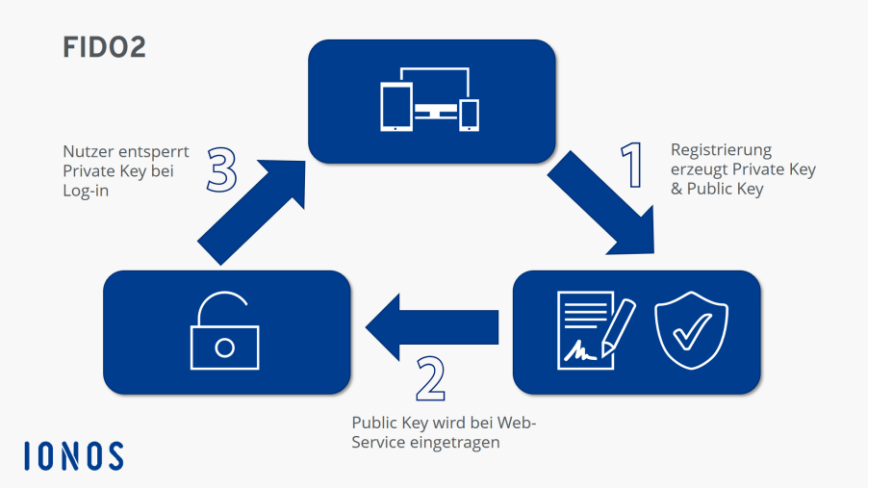


Quelle: https://www.yubico.com/resources/glossary/phishing-resistant-mfa/

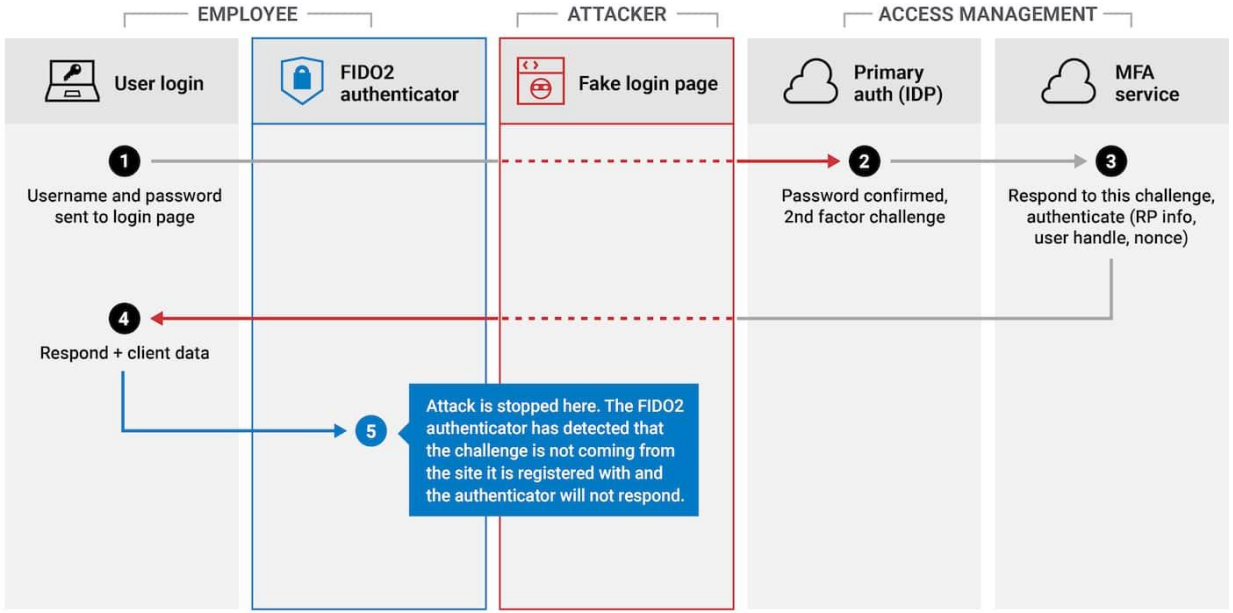
Kryptographie / FIDO2

- Entwickelt von der FIDO-Allianz und W3C
- **F**ast **Id**entity **O**nline
- Challenge Response Verfahren
- Asymmetrische Verschlüsselung
- Biometrie (auf Handy oder PC), Hardware-Token, Smartcards etc.

- Der Authenticator fragt **das Secret** der User:innen ab und erzeugt eine Signatur der Challenge.
- Der Webdienst überprüft die Signatur und authentifiziert den Client.
- Wichtig: die vom Authenticator verwendeten Faktoren wie beispielsweise der PIN, verlassen das lokale Endgerät nie.
- «Nachteil»: Immer an **genau ein Gerät** gebunden.



Sichere MFA-Lösungen Bsp.: mit FIDO2

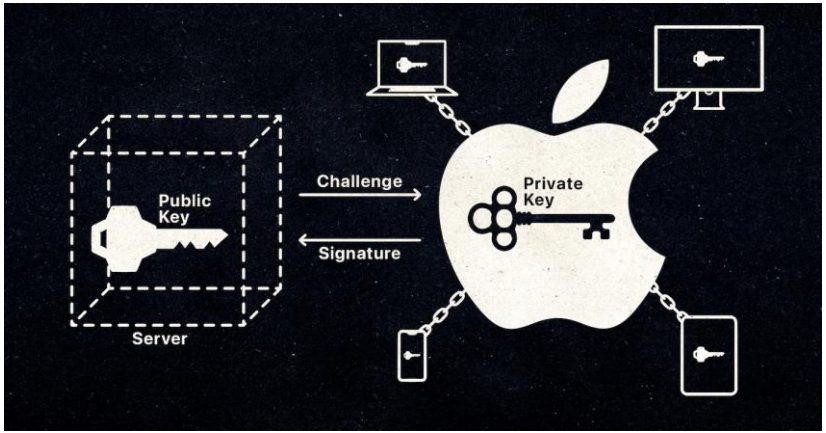


How FIDO2 blocks a fake login page

Quelle: https://www.akamai.com/de/glossary/what-is-multifactor-authentication

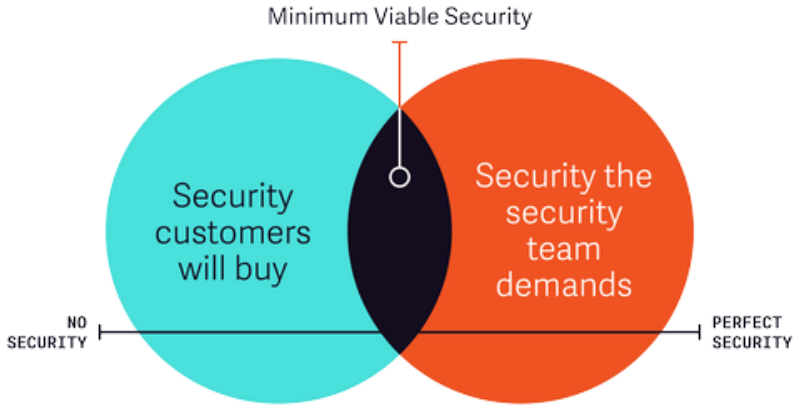
Passkeys

- Die FIDO-Alliance hat zusammen mit Google die sogenannte «Passkey»-Technologie entwickelt.
- Damit sollen Passwörter abgeschafft und Logins einfacher gemacht werden.
- Ebenfalls mit private und public Key
- Basiert auf WebAuthn
- **Unterschied zu FIDO2:** Der private Schlüssel kann zwischen mehreren Geräten synchronisiert werden.
  - User können sich bspw. mit allen Geräten, welche die selbe Apple-ID haben für einen Dienst anmelden.
- Weit verbreitet und vergleichsweise einfache Implementierung.
- Apple und Google speichern die Schlüssel in der Cloud, was eine gewisse **Abhängigkeit resp. Sicherheitslücke** bedeutet.



Fazit

- WICHTIG: Der Einsatz von MFA ist immer noch besser als kein MFA
- Es gibt aber auch bei MFA Sicherheitsunterschiede
- Wahl der Lösung muss unter Berücksichtigung verschiedener Faktoren getroffen werden:
  - Sämtliche Anspruchsgruppen berücksichtigen
  - Usability aus Sicht der Anspruchgruppen beurteilen
  - Sensibilität der Daten abwägen
  - Sicherheit der gewählten Lösung evaluieren
  - Sicherheitskosten mit Incidentkosten vergleichen
  - Risikoabwägung machen



Quelle: https://www.akamai.com/de/glossary/what-is-multifactor-authentication

Unser Unternehmen

Digital Trust Center – Vertrauen, Kompetenz und Technologie

Fokus: Sichere Authentifizierung

Workshop & Diskussion

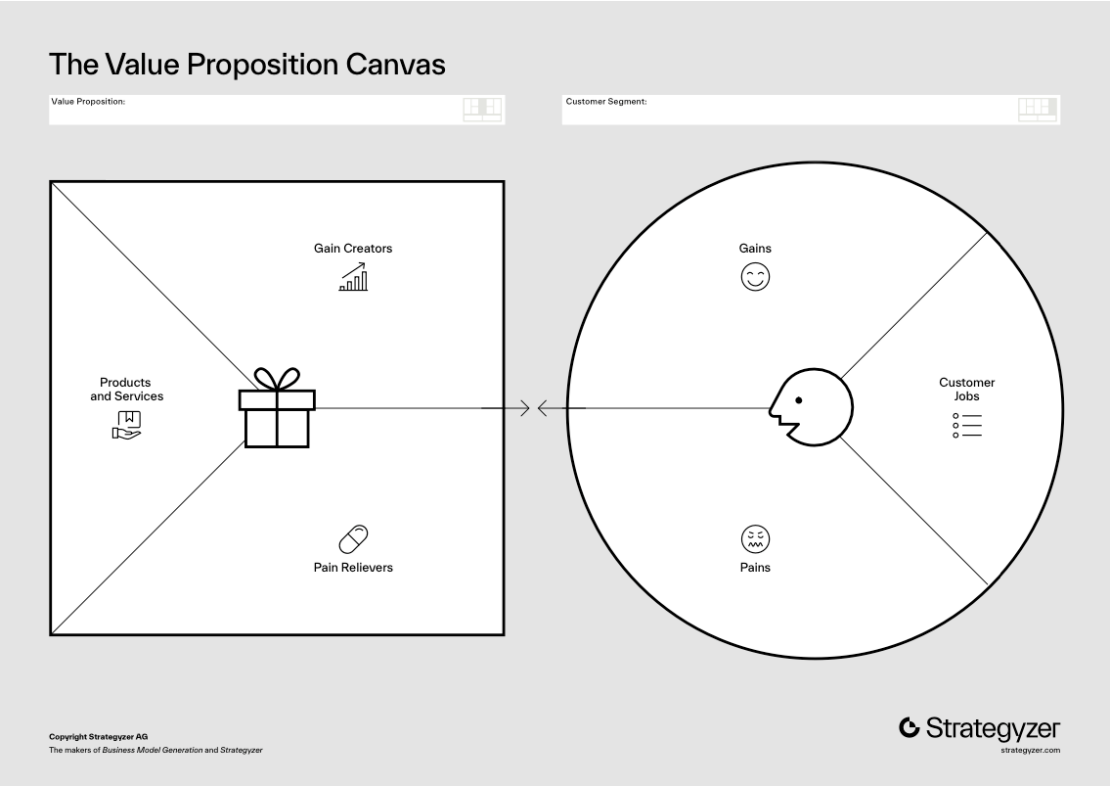
ti&m

Ziele

- Die Teilnehmenden wissen, worauf zu achten ist.
- Die Teilnehmenden kennen die verschiedenen Perspektiven:
  - Sicherheit
  - Usability
  - Implementierung
  - Betrieb
  - Etc.
- Die Teilnehmenden können anhand ihrer eigenen Beispiele grob abschätzen, welche MFA-Methode für sie passend sein könnte.

Quelle: https://www.akamai.com/de/glossary/what-is-multifactor-authentication

Value Creation Canvas von Osterwalder



Quelle: https://www.strategyzer.com/library/the-value-proposition-canvas

Wir digitalisieren Ihr Unternehmen.

Herzlichen Dank!

Kontakt:
Jan Ramseyer
jan.ramseyer@ti8m.ch

Kontakt:
Fabian Dobler
fabian.dobler@ti8m.ch

ti8m.com

ti&m AG
Buckhauserstrasse 24
8048 Zürich
SCHWEIZ
+41 44 497 75 00

ti&m AG
Helvetiastrasse 17
3005 Bern
SCHWEIZ
+41 31 960 15 55

ti&m AG
Elisabethenanlage 9
4051 Basel
SCHWEIZ
+41 61 501 29 99

ti&m GmbH
Schaumainkai 91
60596 Frankfurt am Main
DEUTSCHLAND
+49 69 24745268-0

ti&m GmbH
Kesselstraße 3
40221 Düsseldorf
DEUTSCHLAND
+49 211 90989580

ti&m Pte. Ltd.
18 Robinson Road #15-01
Singapore 048547
SINGAPORE
+65 6983 9530

ti&m