Zwischen Komfort und Katastrophe - wenn Usability auf Security trifft.

SWISS MADE IAM

ITSENSE

GoHack25 I 08.11.2025 I public

Zu meiner Person

Silvan Grüter

CTO
Product Owner
Software Engineer
Uvm.

ITSENSE – IAM made by Experts.

Mission - Als Schweizer Experten für moderne Identity und Access Management schaffen wir einfache, effiziente und skalierbare IAM Lösungen für den internationalen Markt.

23
Jahre Erfahrung

250
IAM Projekte

100%
SwissMade

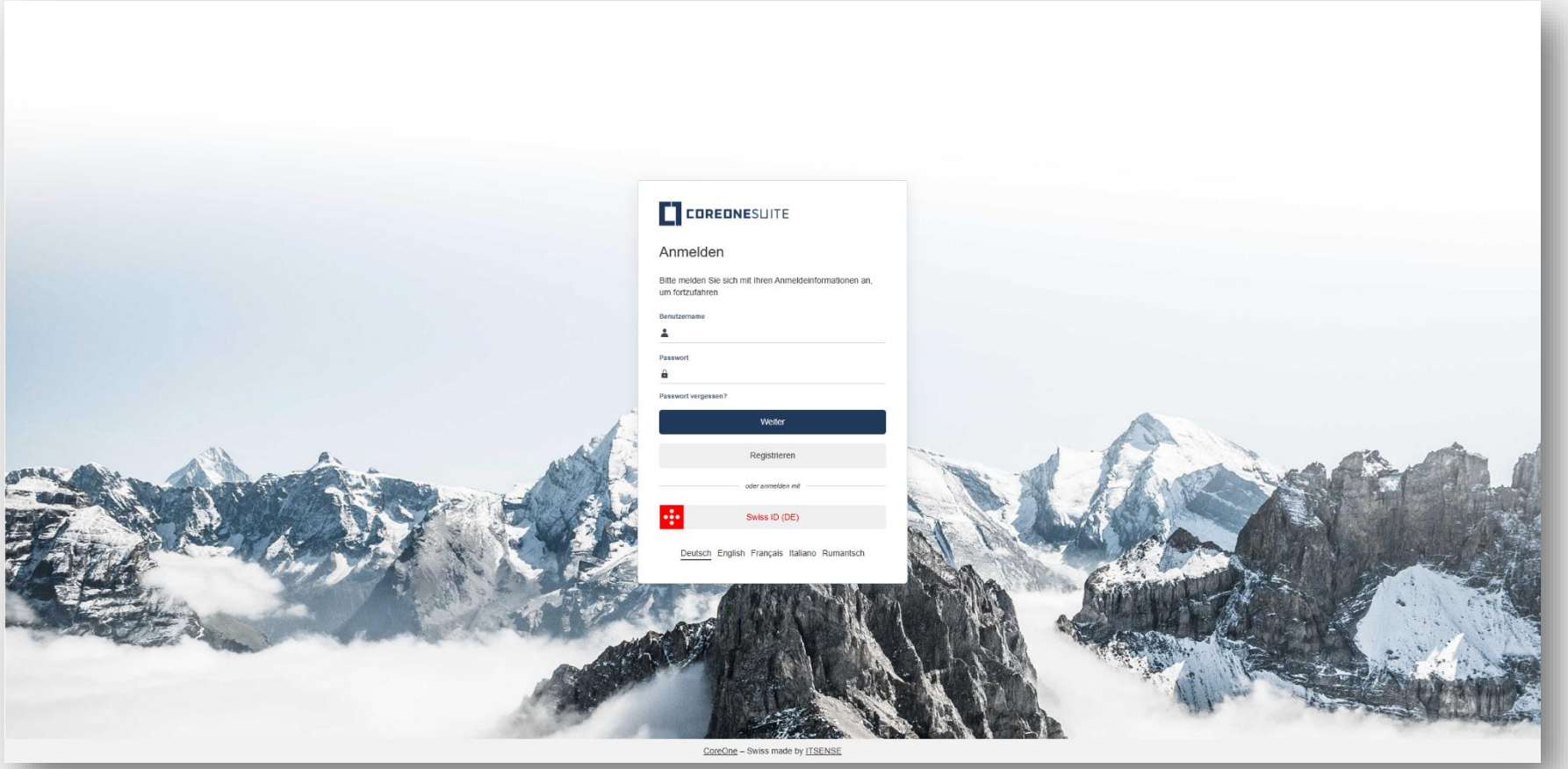
ITSENSE

Ausgangslage & Theorie

ITSENSE

GoHack25 I 08.11.2025 I public

CoreOne Authentication Services



ITSENSE

CoreOne Authentication Services

- Identitätsanbieter für viele Kantonale Logins, Webshops und andere Applikationen
- Benutzer können sich ein Konto anlegen und dieses verwalten
- Das Konto ermöglicht, digitale Services zu nutzen oder deren Nutzung an andere zu delegieren
  - Bsp.: Mein Treuhänder macht für mich die Steuern
- Applikation wird regelmässig
  - auf WCAG 2.1 Konformität geprüft → Usability
  - Penetrationtests unterzogen → Security
  - in Bug Bounty Programmen geprüft → Security
  - von UX-Experten gereviewed → Usability
- 💥 Spannungsfeld Usability vs. Security

Usability

- ISO 9241-210:
  - „Usability ist das Ausmass, in dem ein Produkt durch bestimmte Benutzer in einem bestimmten Nutzungskontext **effektiv**, **effizient** und **zufriedenstellend** genutzt werden kann, um bestimmte Ziele zu erreichen.“
- Anders gesagt:
  - Kann der Benutzer tun, was er will, ohne sich zu ärgern oder aufzugeben?

Wie Gestalten wir Usability?

- Ziel definieren
  - Was will der Benutzer erreichen?
- Personas
  - Personas helfen, verschiedene Nutzergruppen mit klaren Zielen und Frustrationen zu verstehen
- User Journey modellieren
  - Welche Schritte durchläuft ein Benutzer?
  - Wo entstehen Friktionen?
  - Typische Fragen, welcher sich ein Benutzer stellen könnte?
- Testen & Messen
  - Wir lassen Benutzer die Prozesse durchlaufen und dokumentieren, wo sie anstehen

Key Punkte

- Don’t make me think – alles sollte selbsterklärend sein.
- Feedback & Sichtbarkeit – Systemzustand immer klar (z. B. „E-Mail gesendet“).
- Konsistenz – gleiche Logik, Labels, Icons in allen Flows.
- Fehlervermeidung statt Fehlerbehandlung.
- Progressive Disclosure – nur zeigen, was jetzt relevant ist.
- Default Secure Choices – sichere Optionen als Voreinstellung.
- Empathie – verstehen, was Benutzer denken („Warum wollen die das?“).
- Mobile-first – viele IAM-Prozesse laufen heute über Smartphones.

Use Cases 1
Level Easy

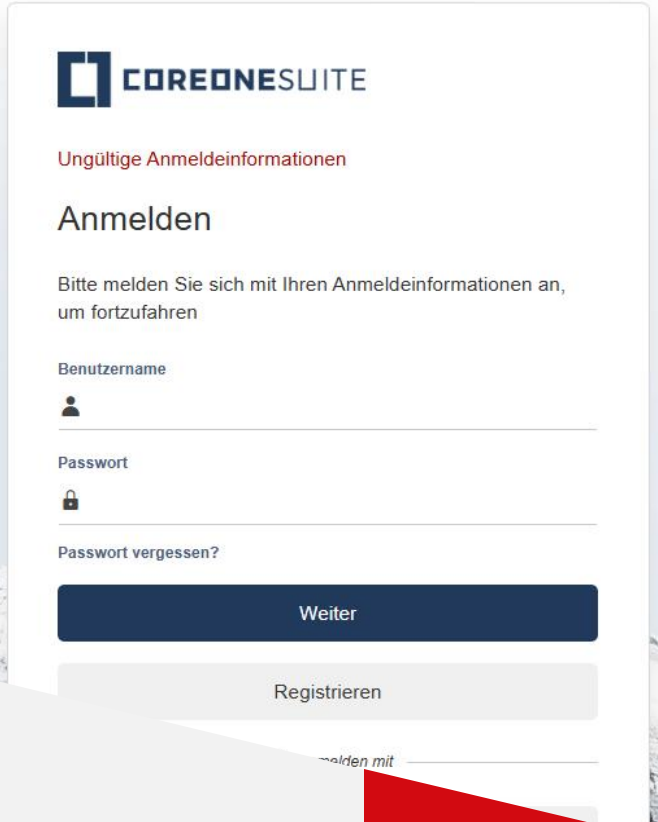
ITSENSE

GoHack25 I 08.11.2025 I public

Level Easy – Anmeldung

- Ziel
  - Benutzer möchte sich anmelden, um Steuern einzureichen

- Personas
  - Ruby Müller, 84
    - Kann gerade so den Computer bedienen
    - «Was ist ein Benutzername?»
  - Sven Security, 42
    - CSO Kantonale Verwaltung
    - Starke Authentisierung mit MFA
    - Regulatorische Anforderungen müssen erfüllt sein

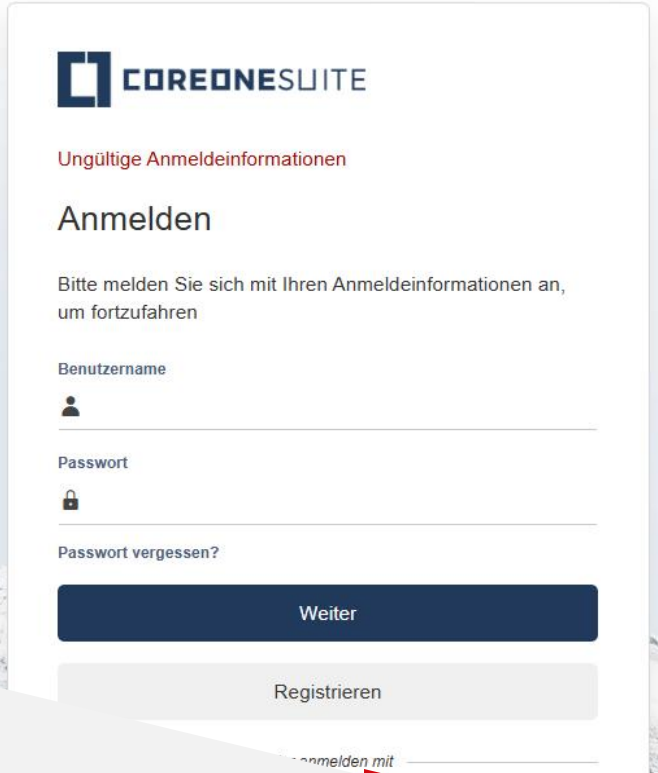


ITSENSE

Level Easy – Anmeldung

- Usability – User Journey
  - Benutzername und Passwort eingeben und ich will angemeldet sein
  - Einfachheit – Keine unnötigen Schritte, keine App installieren, keine MFA, etc.
  - Schnelligkeit – Kein Warten auf OTP oder Push Authentication
  - Klarheit – Was habe ich falsch gemacht?
    - «Ihr Passwort ist falsch» oder «Der Benutzername ist nicht vergeben»
  - Kontinuität – Am besten einmal Anmelden und für 30 Tage SSO
  - Uvm.

- ❓Doch was meint Sven Security dazu?



ITSENSE

Level Easy – Anmeldung

- Security
  - Kurzlebige Session – Keine langlebigen Tokens
  - Starke Authentisierung – Am Liebsten mit verifizierten Hardware Tokens und DNA-Tests
  - Brute-Force-Protection – Rate Limiting
  - Account-Locking – Source Sperren nach 3 Fehlversuchen
  - Re-Authentifizierung – Für sensible Aktionen
  - Uvm.

Level Easy – Anmeldung

- Usability vs. Security
  - ⚡Erste Spannungsfelder
    - Keine klaren Entscheidungen ohne Impact
- Usability & Security (not vs.)
  - Kontextabhängiger MFA / Risk-Based-Authentication
    - Anmelden mit Benutzername & Passwort (Neue Steuererklärung ausfüllen)
    - Sensible Aktionen mit Step-up-authentication (Alte Steuererklärungen einsehen)
  - Neutrale Fehlermeldungen
    - «Ihr Benutzername oder Passwort ist falsch»
  - Passkey-Unterstützung

Use Cases 2
Level Easy

ITSENSE

GoHack25 I 08.11.2025 I public

Level Easy – Account Linking

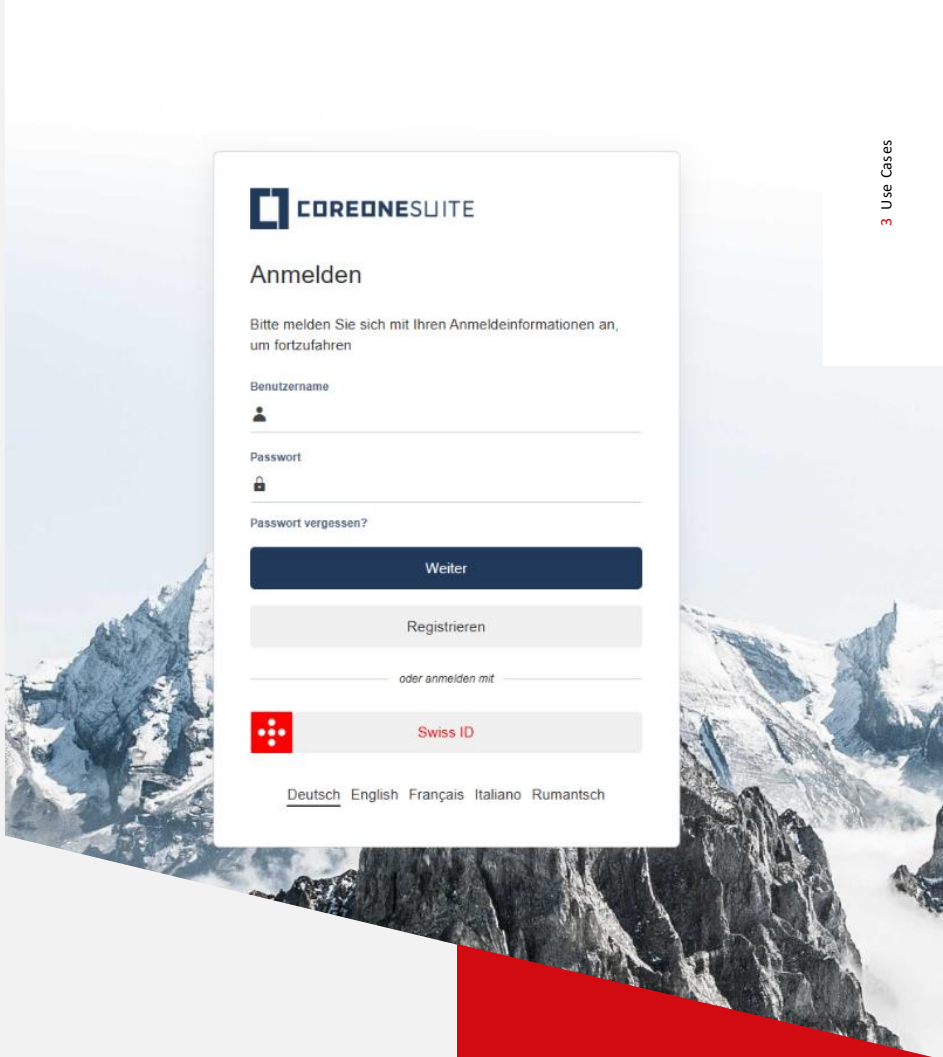
- Ziel
  - Benutzer hat sich registriert mit silvan.grueter@itsense.ch
  - Benutzer hat auch ein Swiss ID Konto mit dieser E-Mail Adresse
  - 🖇 Er möchte die beiden Konten verknüpfen

- Personas
  - Silvan Grüter
    - Kennt sich etwas mit Computer aus
    - Kennt den Unterschied zwischen dem Swiss ID und CoreOne Suite Konto
  - Michael Schläpfer
    - Security Nerd
    - Alles muss perfekt sicher sein

Level Easy – Account Linking

- Usability – User Journey
  - Es sollen so wenig Schritte wie möglich sein
  - Klick auf Swiss ID
  - Anmelden
  - Wenn E-Mail Adresse mit einem CoreOne Konto übereinstimmt, sollte das die Konten automatisch verlinken

- ❓Doch was meint Michael Schläpfer dazu?



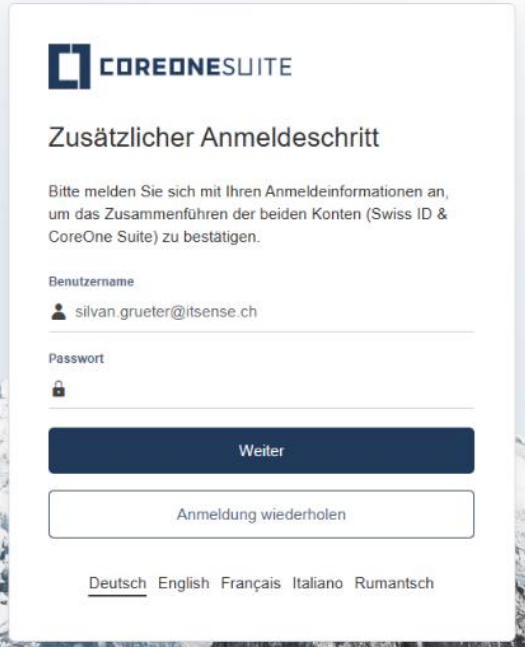
ITSENSE

Level Easy – Account Linking

- Security
  - A1: Broken Authentication / Account Takeover
    - Durch ein kompromittiertes Mail Konto kann sich ein Angreifer ein Swiss ID Konto erstellen und das CoreOne Konto “übernehmen”
  - A3: Insufficient Verfication of User Identity
    - Ohne Re-Authentication weiss das System nicht, ob der Benutzer wirklich der korrekte Benutzer ist
  - Etc.

Level Easy – Account Linking

- Usability & Security (not vs.)
  - Durch Eingabe des Lokalen (CoreOne Suite) Passwortes muss das Zusammenführen bestätigt werden.
  - Security wird erfüllt
  - Die Usability ist nicht merklich beeinträchtigt
  - Einfache technische Massnahme bringt Win – Win Situation



ITSENSE

Use Cases 3
Level Medium

ITSENSE

GoHack25 I 08.11.2025 I public

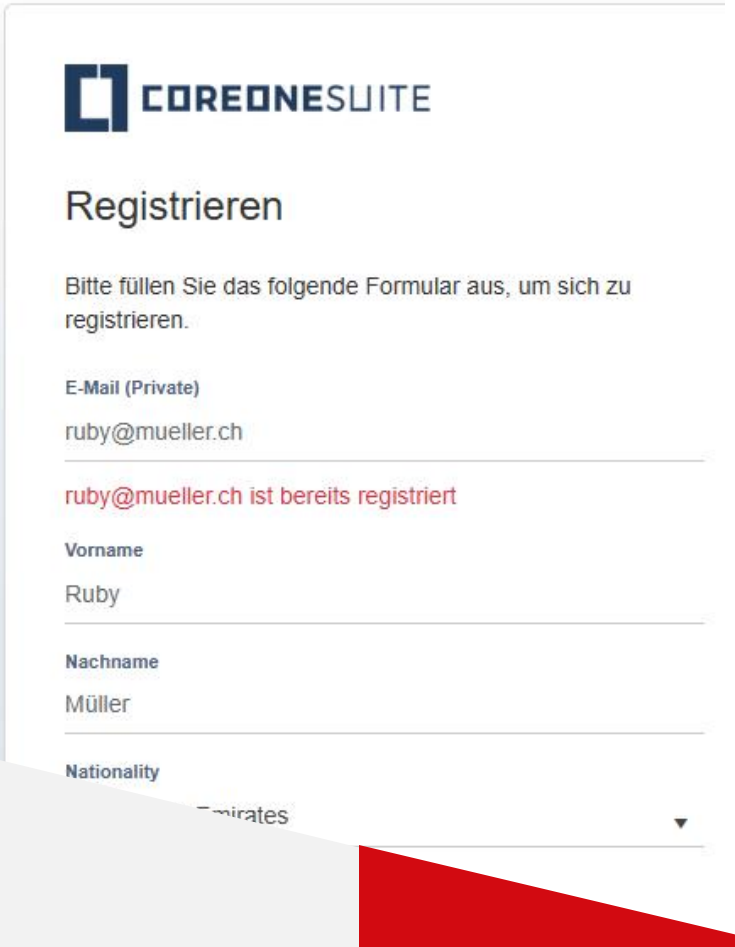
Level Easy – Registration

- Ziel
  - Benutzer will die Steuern im darauffolgenden Jahr wieder machen, weiss aber nicht mehr, ob er bereits ein Konto erstellt hat

- Personas
  - Ruby Müller, 84
    - Kann gerade so den Computer bedienen
    - «Was ist ein Benutzername?»
  - Sven Security, 42
    - CSO Kantonale Verwaltung
    - Starke Authentisierung mit MFA
    - Regulatorische Anforderungen müssen erfüllt sein

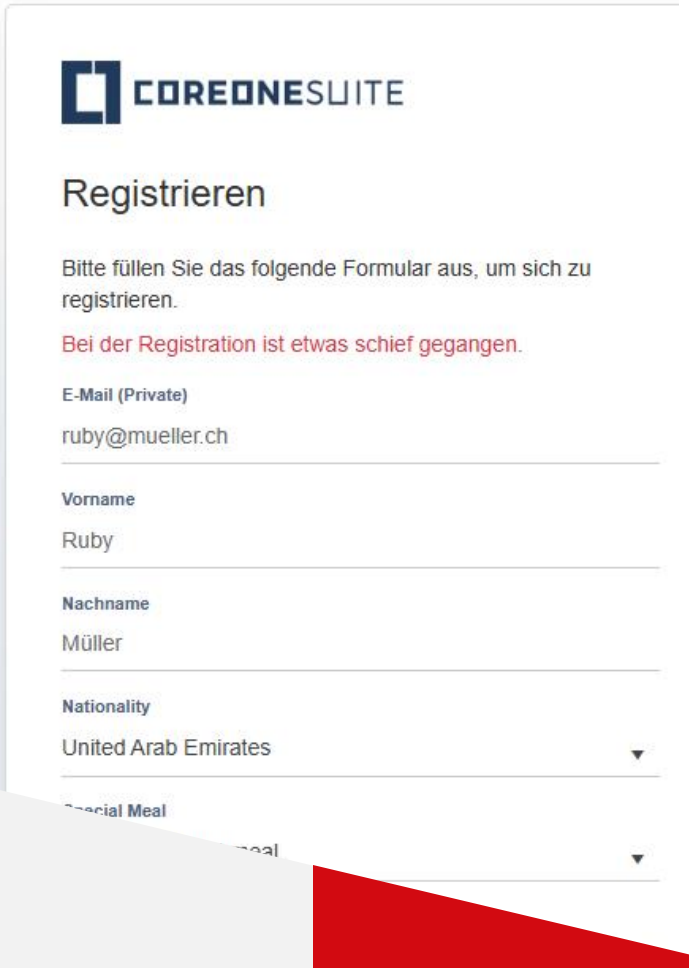
Level Medium – Registration

- Usability – User Journey
  - Benutzer klickt auf «Registrieren» und gibt eine E-Mail-Adresse ein, welche bereits verwendet wird
  - Klarheit – Klare Feedback Meldungen
    - E-Mail ist bereits registriert
  - Hilfestellung – Direkte Hilfe im UI
    - Wenn E-Mail bereits vergeben, direkt Weiterleitung zu Password vergessen



Level Medium – Registration

- Security
  - Das System bestätigt, das es ein Account mit dieser E-Mail gibt
  - Angreifern können massenhaft E-Mails testen
  - OWASP
    - A01 (2021) – Broken Access Control
      → Fehlende Zugriffsbeschränkung auf Benutzerinformationen
    - A07 (2021) – Identification and Authentication Failures
      → Account Enumeration durch differenzierte Fehlermeldungen
    - A09 (2021) – Security Logging and Monitoring Failures
      → Fehlende Erkennung und Alarmierung bei Enumeration-Versuchen
    - OWASP Testing Guide v4 – OTG-IDENT-004 („Testing for User Enumeration“)



Level Medium – Registration

- Usability & Security (not vs.)
  - Generische Fehlermeldung ist nicht benutzerfreundlich
  - Benutzer gibt E-Mail-Adresse ein und wir lassen ihn durch
  - E-Mail-Adresse muss per OTP bestätigt werden
    - Benutzer ist im Besitz der E-Mail-Adresse
      - ✅ Wir weisen im Mail und nach der Eingabe des OTPs auf das existierende Konto hin
    - Benutzer ist nicht im Besitz der E-Mail-Adresse
      - ✅ «Angreifer» bleibt an diesem Punkt hängen
  - 🥳 Lösung erfüllt Usability und Security

Use Cases 4
Level Hard

ITSENSE

GoHack25 I 08.11.2025 I public

Level Hard – Delegation

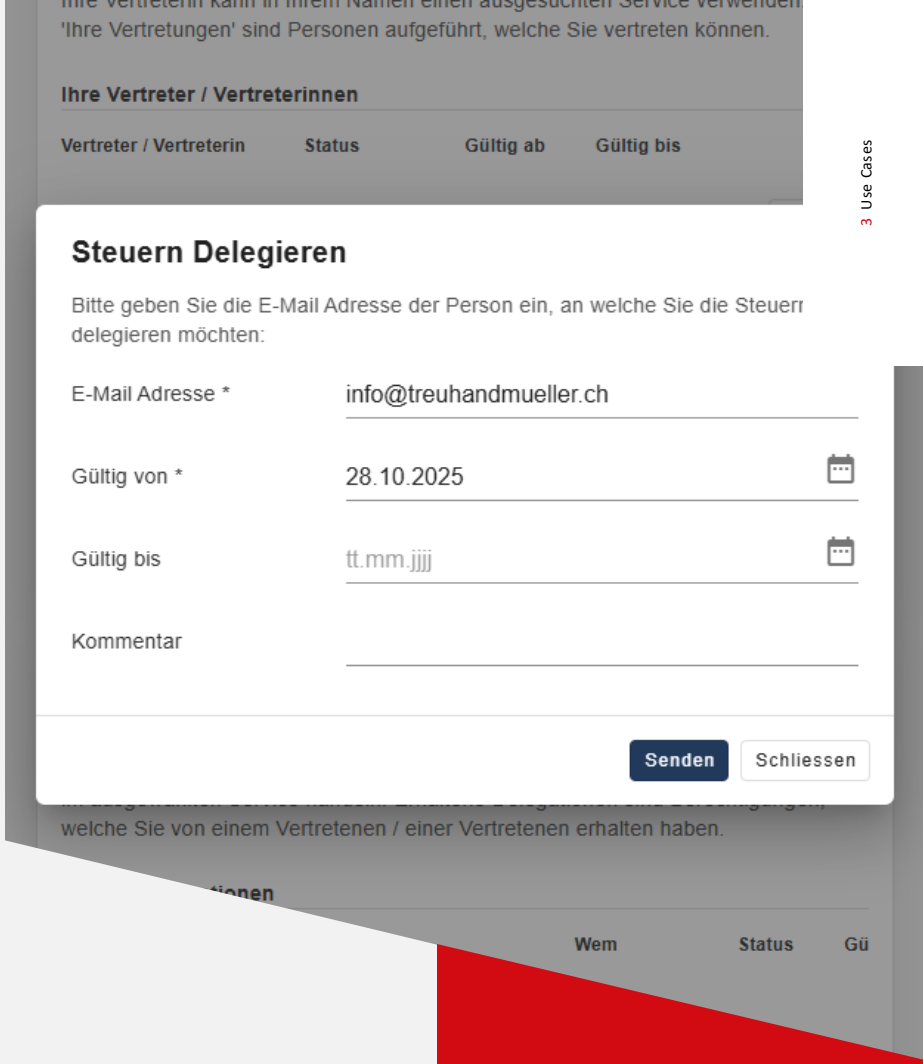
- Ziel
  - Benutzer möchte die Steuern an Peter Sträussle von Treuhandbüro Müller delegieren

- Personas
  - Ruby Müller, 84
  - Peter Sträussle, 31
    - Computerversiert
    - Hat ein Konto, das er mit peter@treuhandmueller.ch registriert hat
    - Mitarbeiter von Treuhand Müller
  - Sven Security, 42
    - CSO Kantonale Verwaltung

Level Hard – Delegation

- Usability – User Journey
  - Ruby
    - Ich melde mich an, wähle den Steuer Service an und klicke «Delegieren»
    - Ich gebe die E-Mail von Peter ein, die ich jedoch nicht kenne, daher gebe ich einfach info@treuhandmueller.ch an
  - Peter
    - Ich kriege eine E-Mail, das ein Bestätigungslink enthält
    - Ich klicke darauf und erhalte die Rechte (aka Session-Link)

- ❓Doch was meint Sven Security dazu?



ITSENSE

Level Hard – Delegation

- Usability & Security (not vs.)
  - Vorschlag 1
    - Session-Link ist an E-Mail gebunden und muss nach Anmeldung bestätig werden
    - 💥 Benutzer hat aber info@treuhandmueller.ch eingegeben
  - Vorschlag 2
    - Session-Link ist nicht an E-Mail gebunden, muss aber rückbestätigt werden
    - ⚖️ Ich kann mir immer noch ein Fake-Konto machen
  - Vorschlag 3
    - Session-Link ist nicht an E-Mail gebunden, kann nur unter verifizierten Benutzern durchgeführt werden
    - ❓ Schafft Ruby ein Video-Ident verfahren?
  - Vorschlage 4
    - Session-Link ist nicht an E-Mail gebunden, kann nur von verifizierten Benutzern angenommen werden

Level Hard – Delegation

- Usability vs. Security
  - Generische Fehlermeldung ist nicht benutzerfreundlich
  - Benutzer gibt E-Mail-Adresse ein und wir lassen ihn durch
  - E-Mail-Adresse muss per OTP bestätigt werden
    - Benutzer ist im Besitz der E-Mail-Adresse
      - ✅ Wir weisen im Mail auf das existierende Konto hin
    - Benutzer ist nicht im Besitz der E-Mail-Adresse
      - ✅ «Angreifer» bleibt an diesem Punkt hängen
  - 🤩 Lösung erfüllt Usability und Security

Conclusion

ITSENSE

Key Takeaways

- Usability und Security sind keine Gegensätze.
  - → Gute Security fühlt sich einfach an.
  - → Schlechte Usability führt zu Unsicherheit.
- Design für Vertrauen, nicht für Kontrolle.
  - → Wenn der Benutzer versteht, warum etwas sicher ist, akzeptiert er auch Reibung.
  - → Kommunikation ist Teil der Security.
- Context beats Policy.
  - → Eine 84-Jährige braucht keine Hardware-MFA.
  - → Ein CSO braucht Nachvollziehbarkeit – nicht Klickfreundlichkeit.
  - → Sicherheit muss sich am Risiko orientieren, nicht am Ideal.

Key Takeaways

- Security by Design = Usability by Design.
  - → Wenn Security „by default“ integriert ist, wirkt sie unsichtbar.
  - → Jede Sicherheitsmassnahme muss auch „UX-tauglich“ sein.

- Das Ziel ist Vertrauen.
  - → Nur Systeme, die sicher und benutzbar sind, werden wirklich genutzt.
  - → Adoption = der wahre Security-Erfolg.

Vielen Dank

ITSENSE

GoHack25 I 08.11.2025 I public

SWISS MADE IAM