

IT Sicherheit im Umfeld mit unerfahrenen Usern

Dataspace Switzerland
22.06.2022

Agenda

- Personas
- Security
 - Einflussfaktoren bei der Entwicklung
 - Kontrollierbare Faktoren
 - Key Takeaways
- Empfehlenswerte Tools

Personas



Bettina Künzle

Alter: 35-45 Jährig

Beruf: Bäcker / Konditorin

Hobbies: dekorieren, reisen, backen

Technik im Einsatz: Samsung S10, Acer

Notebook

IT Erfahrung:

MS Office, Youtube, Instagram



Hans Müller

Alter: 50-55 Jährig

Beruf: Elektroinstallateur

Hobbies: Velo- und Skitouren, Feuerwehr

Technik im Einsatz: Pager, iPhone 6s, iPad

IT Erfahrung:

Gelegentliches Surfen, Youtube und eine @swissonline.ch eMail-Adresse

Security in der Entwicklung

Einflussfaktoren der Personas bei der Entwicklung von Web-Apps / PWA

- Keine Kontrolle über die Endgeräte der Benutzer
- Schulungen nur mit erheblichem Aufwand möglich (online tutorials, FAQs, etc.)
- Oftmals kein Interesse an "dem ganzen online Zeugs"
- Möglichst wenige Berührungspunkte in Bezug auf Sicherheit





Security in der Entwicklung

Key takeaways für Startups und Kleinfirmen

- Sicherheit auch bei headless devices (z.B. Signage Player)
- Funktionalität und Sicherheit > Design
- PWs sind zu keiner Zeit für backend user oder admins sichtbar
- Passwort reset geschieht immer durch den Enduser
- Unterschiedliche SSH Keys im Einsatz und PW geschützt
- Client input = dirty data
- "Bis jetzt ist ja auch nichts passiert" < "Wir sind bisher verschont geblieben"
- Autorisierter User ≠ keine Gefahr

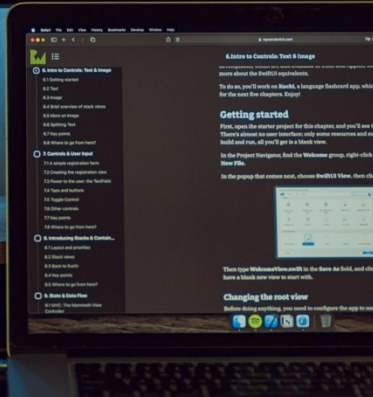
```
import SwiftUI

enum Operator {
    case none
    case add
    case subtract
    case multiply
    case divide
}

extension View {
    public func addOperator(operator: Operator) {
        ...
    }
}

struct CalculatorView: SwiftUIView {
    ...
}

struct CalculatorView_Preview: SwiftUIView_Preview {
    ...
}
```





Empfehlenswerte Tools

- Package vulnerability scanner (z.B. [snyk.io](https:// snyk.io))
- Sensibilisierung der Entwickler und Entscheidungsträger (z.B. Security Academy von [oneconsult.com](https:// oneconsult.com))
- Teleport infrastructure access control ([goteleport.com](https:// goteleport.com))
- Passwort Manager (on-prem [Bitwarden](https:// Bitwarden))
- Log alerts ([grafana loki](https:// grafana loki), [grayscale](https:// grayscale))
- Interne reverse proxy für gültige SSL Zertifikate (z.B. [NGINX Proxymanager](https:// NGINX Proxymanager))
- Dokumentation Infrastruktur ([netbox.dev](https:// netbox.dev))
- Zero Trust, Access, etc. ([cloudflare.com](https:// cloudflare.com))
- Intranet Dashboard für Systeme ([bastienwartz/homer on github](https:// bastienwartz/homer on github))



SimplyConnect

Kontakt: office@simplyconnect.ch

