Digitalisierung und Ich! - Mach den Schulen -

- Daten sind das Gold des digitalen Zeitalters.
- Wenn Sie sich im Internet bewegen, hinterlassen Sie bei jedem Klick Spuren!
- Daten sind rückvordernebt und es gibt andere Gläubiger mit verschiedensten Absichten.
- Das Internet ist schnell, Daten sind leicht zu finden und auszuwerten! Löschen ist nicht möglich!
- Trotz Verschlüsselung gibt es viele Möglichkeiten, Sie zu erkennen und Ihre Aktivitäten auszuspionieren!
- Wie Sie anderen Gläubigern das Handwerk legen!
- In zehn Schritten zur Sicherung des Daten-Goldes!
- Sie können dem Eigenleben Ihrer Daten und dem Datenklaue vor!

Das Ziel

(1) Betriebssysteme

Betriebssysteme kennen Ihr Gerät und alles, was sich darauf befindet.

allgemeine Tipps:
- https://www.young-penguins.de/beitragsarchiv/2019/05/12/der-lustige-faxer/ 
- Nutzen Sie datensparsame Betriebssysteme!
- Anfragen Sie, ob sie so tun, dass:
  - kein Mikrofon/Kamera aktiv ist
  - keinerlei Telemetriedaten erhoben und versendet werden
  - keine Clouddienste verwendet werden
  - keine exterior Sprach- und Sprechерerkennung erfolgt
- Verwenden Sie Anti-Virus-Programme
- Die digitale Selbstverteidigung ist die Lösung für unbekannte Probleme.

Spezielle Tipps:
- Kennen Sie Linux? – PC (z.B. Debian/Edu)
  https://www.macs.de/laptop-software-free-software-for-the-laptop/edu/ 
  https://digital-souveraen.de/digitale-souveraen-betriebssysteme/meineUARIO-Mobile (z.B. LineageOS, Ubuntu Touch)
  https://www.sicheres-browsen.de/digitale-souveraen-betriebssysteme/meineUARIO-Mobile/ 
- Falls Sie Windows 10 benutzen müssen – erhabliche Konfigurationsbedarf
  https://www.sicheres-browsen.de/digitale-souveraen-betriebssysteme/meineUARIO-Mobile/ 
- benutzerdefinierte Installation
- bereitgestellte Datenschutzoptionen (u.a. zu WerbeID, Schreibverhalten, Nutzer-/App Protokollierung)
- lokale Konten (kein Microsoft-Konto)
- Apps Dritter (z.B. Browser, E-Mail)
- niedrigstes Telemetrieniveau (basics, trotzdem keine vollständige Sperrung)
- Beenden Sie Desaktivierungshinweise zu Cortana, Spracherkennung, Verbindungs- und Fehlerberichterstattung, Clouddienste als Datenspeicher
- Überprüfen Konfiguration nach Update!

(2a) Internetbrowser

Browser wissen viel über Sie und sind die „Tür zum Internet“.

Tipps zur Grundsicherung:
- Achten Sie bei Browerswahl auf datenmäßige Konfigurierbarkeit, Erweiterbarkeit und Updatefähigkeit
- https://www.young-penguins.de/beitragsarchiv/2019/05/12/der-lustige-faxer/ 
- https://digital-souveraen.de/digitale-souveraen-betriebssysteme/meineUARIO-Mobile/ 
- Schauen Sie mal bei den Anregungen: 
  - Anfragen Sie, ob Sie für die Einstellungen der Systeme auf Ihrem Computer Zugriff haben?
  - Waterfox, Pale Moon, Brave

(2b) Internetbrowser

Browser-URLs sind Postkarten (http) bzw. Briefe (https) der Abendpost, Der Empfänger und die Form des Briefumschlags sind immer erkennbar.

Tipps zu speziellen AddOns:
- Panoplick zeigt Ihnen, ob man Sie erkennt. Lightbeam zeigt Verbindungen.
- Anonymisierungsdienste können die eigene Präsenz verschleieren helfen:
  https://www.young-penguins.de/beitragsarchiv/2019/05/12/der-lustige-faxer/ 
- Schauen Sie mal bei den Anregungen: 
  - Anfragen Sie, ob Sie für die Einstellungen der Systeme auf Ihrem Computer Zugriff haben?

(3) Apps

Die Apps kennen alle Daten, auf die sie Zugriff haben.

Tipps:
- Überprüfen Sie App Zugriffe und Verbindungen vor dem Einsatz z.B. https://www.privacypolicies.org
- Konfigurieren Sie Apps datensparsam https://www.sicheres-browsen.de/digitale-souveraen-betriebssysteme/meineUARIO-Mobile/
- Vorzug für lokale Apps (Need-to-know)
- Blockieren Sie Zugriffe durch Einstellungen auf dem Telefon (z.B. Mikrofon, Kamera, Speicher)
- Verschieden B. BLOKADA zur Sperrung von Trackern:
  - https://www.peerblock.de/ 
  - Blockieren Sie Zugriffe auf Positionsdaten (WLAN, IP, GPS)
- Benutzer können die privacy.de App verwenden, um Apps nachzufahren
- Benutzer können die privacy.de App verwenden, um Apps nachzufahren

(4) Suchmaschine

Die meisten Suchmaschinen (durchschn) aushalten auch Sie.

Tipps:
- Kennen Sie die Suchmaschinen?
- https://www.yandex.de/ 
- http://www.meta.de/
- Suchen Sie doch mal unter https://digital-souveraen.de/digitale-souveraen-betriebssysteme/meineUARIO-Mobile/ 
- Blockieren Sie Zugriffe durch Einstellungen auf dem Telefon (z.B. Mikrofon, Kamera, Speicher)

(5) E-Mail

E-Mails sind elektronische Postkarten, die von jedermann gelesen werden können, wenn Sie nichts dagegen unternehmen.

Tipps:
- Interesse an sicheren E-Mail Anbietern? Dann finden Sie Infos hier: https://www.privacy.de/e-mail-privatsphäre
- Kennen Sie extra E-Mail Programme mit Verschlüsselung (z.B. Thunderbird mit Enigmail? https://enigmail.org/) 
- Lassen Sie sich immer den langen E-Mail Briefkopf (Header) anzeigen und überprüfen die E-Mail-Adressen
- Verwenden Sie Virenscanner!
- Empfohlen: kein automatisches Nachladen von Bildern und Öffnen von Links im Webbrowser, keine html Mails
**Schulwebaufftritt (6)**
Mit Ihrem Webaufftritt übernehmen Sie Verantwortung für IT-Sicherheit und Datenschutz für sich und Ihre Nutzer.

**Tipps:**
- Nutzen Sie lokale Schriftarten, Übersetzungs-, Vorlesedienste
- Geben Sie Löschrätseln für gespeicherte Daten an und halten Sie sie ein
- Prüfen Sie auf voreingestellte, ungewollte Analytics-Funktionen der Software
- Verwenden Sie Opt-In statt Opt-Out
- Verwenden Sie IP-Adressenverwendung auf Metaebene -mehr Details im Artikel
- Vermeiden Sie Webfonts, Analytics
- Testen Sie Ihren Webaufftritt unter PrivacyScore.org
- Nutzen Sie Videos nur vom genutzten Server bzw. lokal gespeichert

**Soziale Netzwerke, Chat, Messenger, Navigationsdienste (7)**

**Tipps:**
- Kennen Sie dezentrale, Open Source basierte soziale Netzwerke? z.B. aus dem Fediverse
- Erkennen und blockieren Sie Zugriffs- und Trackingtechniken z.B. über Webfonts und APIs, nutzen Sie die Hilfsmittel aus (2a), (2b) und (4) z.B. Privacy Badger zur Erkennung und BLOKAD zur Unterbindung

**Internet-Gateway/Firewall (8)**
Das Gateway ist das Tor zum Internet und die letzte Verteidigungslinie für die Systeme des Nutzers.

**Tipps:**
- über DNS können Sie unerwünschte Dienste ausblenden, deshalb konfigurieren und betreiben Sie eigene DNS Server oder den des Providers, keine Drittanbieter
- Konfigurieren und verwenden Sie Firewall zur Filterung des Netzwerks
- Konfigurieren und betreiben Sie Intrusion Prevention Systeme zum Schutz von schadcode
- Prüfen und konfigurieren Sie App-Zugriffe z.B. bei exodus-privacy.eu.org (u.a. Zugriffe auf Smartphone-Dienste)

**Passwort (9)**
Passwörter sind eine wichtige Maßnahme zur Sicherung der digitalen Identität.

**Tipps:**
- Verwenden Sie lange Passwörter (mind. 10 Zeichen) mit Sonderzeichen und Zahlen ohne bekannte Silben
- Verwenden Sie jedes Passwort nur für einen Dienst/Account
- Verwenden Sie lokale Passwortgeneratoren und lokale OpenSource Passwortmanager oder:
- Bilden und merken Sie sich einen geheimen Satz und erzeugen daraus das Passwort anhand z.B. der Anfangsbuchstaben und Zahlen. Beispiel: „Im Urlaub 2018 hatte ich einen blauen Badeanzug mit 7 Streifen und 8 Punkten!“
- Führen Sie keine Sicherheitssanfage aus!

**Konsequenzen**
Wenn Privacy-by-Design nicht umgesetzt wird, ergeben sich direkte und spürbare Konsequenzen:

- Profitbildung
- Neuro Marketing
- verhaltensbasiertes Marketing
- algorithmische Entscheidungsfindung
- Kreditwürdigkeit von Personen
- personenbezogene Preisermittlung

Bereits im Einsatz: dynamische, personalisierte Preisgestaltung
Also besonders gut eignet sich all die Produkte, wo der Käufer kein Gefühl dafür hat, was sie kosten. Ich denke, dass nicht nur die absolute Höhe des Preises entscheidend ist, sondern die Preissensibilität eine wichtige Rolle spielt.

**Wichtig:**

**Büroanwendungen (10)**
Die Büroanwendungen kennen alle Daten, die sie verarbeiten.

**Tipps:**
- Kennen Sie lokal installierte Open Source Anwendungen z.B. eine in https://www.kontakt.de/dgin/1598.html?event magnet=servenummer
- LibreOffice
- GIMP
- Verwenden Sie lokale Rechtschreib- und Übersetzungsunterstützung

Achten Sie bei Cloud-basierten Anwendungen mit Abo-Modell (u.a. Office 365) und Microsoft Office auf die Datenschutzanalyse

**Hinweis**
Die angegebenen Links sind bewusst kleindruckt und sollten im Digitalen nachgeschlagen werden.


**Beispiel für die Nutzung von Outlook
durch einen Mitarbeiter**

**Hinweis**
Die angegebenen Links sind bewusst kleindruckt und sollten im Digitalen nachgeschlagen werden.