Digitalisierung und Du! - Mach den Schulen -

- Daten sind das Gold des digitalen Zeitalters.
- Wenn Du Dich im Internet bewegst, hinterlässt Du bei jedem Klick Spuren!
- Daten sind rückwärts verbreitert und es gibt viele Goldgräber mit verschiedensten Absichten!
- Das Internet ist schnell, Daten sind leicht zu finden und auszuwerten! Losen ist fast unmöglich.
- Trotz Verschlüsselung gibt es viele Möglichkeiten, Dich zu erkennen und deine Aktivitäten auszuspionieren!
- Wie Du anderen Goldgräbern das Handwerk legst!
- In zehn Schritten zur Sicherung des Daten-Goldes!
- Beuge dem Eigenleben Deiner Daten und dem Datenklaue vor!

Das Problem

Es gibt manche, die im Internet surfen und dabei an ihrer Identität interessiert sind. Du solltest wissen, dass du ein digitaler Akteur bist und deine Spuren im digitalen Raum hinterlassen kannst. Diese Spuren können dazu genutzt werden, um dir Schaden zuzufügen. Dazu gehören all deine Daten, die du beim Internet-Browsing oder im Social-Media-Bereich hinterlassen hast.

(1) Betriebssysteme

- Betriebssysteme kennen Dein Gerät und alles, was sich darauf befindet.

allgemein Tipps:

- Nutze das Lieblingsprogramm, das dir gefällt!
- Kein Systemanpassen ohne Rücksprache mit dem IT-Team!
- Keine Software ohne Updates installieren!!
- Nur Programme mit Lizenzen verwenden!

Hundertz prozentige Sicherheit gibt es leider nicht, aber wer durchdacht, dem eröffnen sich neue Chancen! Beachte den Hinweis auf die Komponente von Windows 10!


(2a) Internetbrowser

- Browser wissen viel über Dich und sind die Tür zum Internet.

Tipps zur Grundversicherung:

- Achte bei Browserwahl auf datenarme Konfiguration. Erweiterbarkeit und Updatefähigkeit. Startseite des Browsers und neue Tabs auf leere oder lokale Seite setzen! (abdenkt)
- Kennst Du z.B. Firefox http://www.mozilla.org/de/ @Mozilla.de!
- Waterfox: Pale Moon, Brave http://www.mozilla.org/de/ @Mozilla.de!

Achtsamer Konfigurationsbedarf und auf aktuelle Erkennungen. Prüfe Konfiguration der Einstellungen nach Update

Umgebungsvariable SSLKEYLOGFILE keinen entfernen!

(2b) Internetbrowser

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

- Konfigurieren, aktualisieren und nutzen Browser Addons: http://www.mozilla.org/de/ @Mozilla.de

Tipps zu speziellen AddOns:

- Panopticlick zeigt, wie man Dich erkennt. Lightbeam zeigt Verbindungen
- Erweiterung: informiere Dich über Suchmaschinen bezog Da Du sie nutzt, Trage Dir eine datensparsame Suchmaschine als Default ein!
- Erweiterung: track-er.de sucht nach Transparenz von Datenpapier und -verwertung am Beispiel von Facebook

http://www.mozilla.org/de/ @Mozilla.de


(3) Apps

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

Tipps:

- Überprüfe App-Zugriff und Verbindungen vor dem Einsatz z.B. erweitert.privacy.org
- Konfigurieren Apps datensparsam http://www.mozilla.org/de/ @Mozilla.de
- bevorzuge lokale Apps (Need-to-know)
- Blockiere Zugriffe bei App-Einstellungen auf dem Telefon (z.B. auf Mikrofon, Kamera, Speicher)
- Verwende z.B. BLOKADA zur Sperrung von Trackern http://www.mozilla.org/de/ @Mozilla.de
- Blockiere Zugriffe auf Positionsdienste (WLAN, IP, GPS)
- Kennst Du offene App-Downloads wie F-Droid? http://f-droid.org

(4) Suchmaschin

Die meisten Suchmaschinen (durch-)suchen auch Dich.

Tipps:

- Kennst Du die Suchmaschinen? http://lite.qwant.com
- MetaGer.de
- YoC.net

- schau doch mal unter http://www.mozilla.org/de/ @Mozilla.de

(5) E-Mail

E-Mails sind elektronische Postkarten, die ohne Gegenmaßnahmen von jedermann gelesen werden können.

Tipps:

- Interesse an sicheren E-Mail Anbietern? Dann findest Du Infos hier: http://www.mozilla.org/de/ @Mozilla.de
- Kennst Du extra E-Mail Programme mit Verschlüsselung (z.B. Thunderbird mit Enigma)?
- Kannst Du offene E-Mail-Programme wie Privacyfox.org nutzen?
- Verwende einen sicheren Nutzernamen
- Nutze nur E-Mail-Adressen, die nicht von Dritten interagieren
- Verwende Verschlüsselung (z.B. PGP)
- Verwende verschlüsselte E-Mails an Dich, wann immer möglich!
- Lass Dir immer den langen E-Mail-Briefkopf (Header) anzeigen und überprüfe die Adressen!
Schulwebauftritt (6)

Mit Deinem Webauftritt überrasst Du

Analysen- und -Entwicklung von IT-Sicherheit
und Datenschutz für Dich und Deine Nutzer.

Tipps:
- Nutze lokale Suchfunktionen
- Kennst Du Open Data-Karten- und Navigationsdienste? Bsp. Opendatastreemap
  (pdf)
- Prüfe bei Webbaukasten auf integrierte Verbindungsaufbauten an Dritte und deaktiviere sie
- Informiere dich zu datensparsamen Terminplanern z.B. unfold https://www.fbm-kleinspiegel.de/shop.html
  (pdf)
- Binde Vorlesendienste, Clouddienste, Übersetzungen lokal ein
- Verweise eine Kombination von Drittanbietern bei Verwendung von anonymisierten Diensten z.B.
  anonymisierte Analytics und Webfonts

Soziale Netzwerke, Chat, Messenger, Navigationsdienste (7)


Tipps:
- Kennst Du dezentrale, Open Source basierte soziale Netzwerke? z.B. aus dem Feedvddiere
  https://digitalstrategie-badenwurttemberg.de/2019/05/02/kerne-um-das-open-source-sozialen-netzwerk-ethereums-aktivitaet-
  de/index.html
- Erkenne und blockiere Zugriffs- und Trackingtechniken z.B. über Webfonts und APIs, nütze die Hilfsmittel aus (2a), (2b) und (4) z.B. Privacy Badger, webbkoll.datensicht.de zur Erkennung und BLOKADA zur Unterbindung
- Kennen Sie zum Beispiel datensparsame Messenger (z.B. Jabber/XMPP)

Internet-Gateway/Firewall (8)

Das Gateway ist das Tor zum Internet und die letzte Verteidigungslinie für die Systeme des Nutzers.

Tipps:
- Über DNS kannst Du unerwünschte Dienste ausblenden, deshalb konfigu-
  riere und betriebe eigene DNS Server oder den des Providers, keine Drittan-
  biet, verwenden und sichere DNS Anfragen (DNS over HTTPS)
- Unterdrücke Telemetrie: apps.google.com
  (online) https://developers.google.com/analytics/devguides/datastream/telemetry
- Konfigurieren und verwenden Sie Firewalls zum Filtern ins Netzwerk
- Konfigurieren und betriebe Intrusion Prevention Systeme zum Schutz vor Schadcode
- Prüfe und konfiguriere App-Zugriffe z.B. bei exodus-privacy.eu (u.a.)

Passwort (9)

Passwörter sind eine wichtige Maßnahme zur Sicherung der digitalen Identität.

Tipps:
- Verwende lange Passwörter (mind. 10 Zeichen) mit Sonderzeichen und Zahlen ohne bekannte Wörter
- Verwende jedes Passwort nur für einen Dienst/Account
- Bilde und merke Dir einen geheimen Satz und erzeuge daraus das Passwort anhand z.B. der Anfangsbuchstaben und Zahlen, Beispiel: Jm Urlaub 2018 hatte ich einen blauen Badeanzug mit 17 Straffen und 8 Punkten? (IU28bM1Su8P)
- Verwende lokale Passwortgeneratoren und lokale OpenSource Passwortmanager siehe auch
  https://web.de/infos/karten/qvegt/fund/04.php

Bürowerfahren (10)

Die Bürowerfahren kennen alle Daten, die sie verarbeiten.

Tipps:
- Kennst Du lokai installierte Open Source Anwendungen? z.B. in
  https://www.kunter.blog.de/2017/03-meine-verschiedenen-open-source-datenmuster/ (pdf)
- LibreOffice, GIMP
- Verwende lokale Rechtschreib- und Übersetzungsunterstützung
- Kennst Du digitale Medienschränke? Achte bei Cloud-basierten Anwen-
  dungen mit Abo-Modell (u.a. Office 365) und Microsoft Office auf die Datenschutzanalyse

Konsequenzen

Mit Privacy-by-Design unterstützt Du

Die Datenschutz-Grundverordnung fordert den besonderen Schutz für Kinder für Werbezwecke, für die Erstellung von Persönlichkeits- oder Nutzerprofilen und bei der Nutzung von Diensten, die Kindern direkt angeboten werden.

Tipps:
- Kennst Du das Beispiel datensparsame IRC Klienten (z.B. Chat?)
  (online) https://www.privacyproject.ch/form/irc/

Achtung: Die Datenschutzgrundverordnung fordert den besonderen Schutz für Kinder für Werbezwecke, für die Erstellung von Persönlichkeits- oder Nutzerprofilen und bei der Nutzung von Diensten, die Kindern direkt angeboten werden.

Wichtig:
Die Informationen und Referenzen stellen einen ersten Einstieg zum Thema dar. Die Inhalte sind vor dem Hintergrund der Infotainment erstellt und mit größter Sorgfalt recherchiert. Es kann dennoch keine Haftung für die Richtigkeit, Vollstän-

gigkeit und Aktualität der bereitgestellten Informa-


Hinweis

Beachten Sie die angegebenen Links, die bewusst gekürzt und sollten im Digitale nachgeschlagen werden.

"When you shop, your data may be the most valuable thing for sale."