Tipps für die Umsetzung geeigneter IT-Sicherheitsmaßnahmen

Jürgen Schüler

Kompetenzzentrum SMART SERVICES
Innovative Dienstleistungen aus Baden-Württemberg

Kompetenzzentrum SMART SERVICES Innovative Dienstleistungen aus Baden-Württemberg

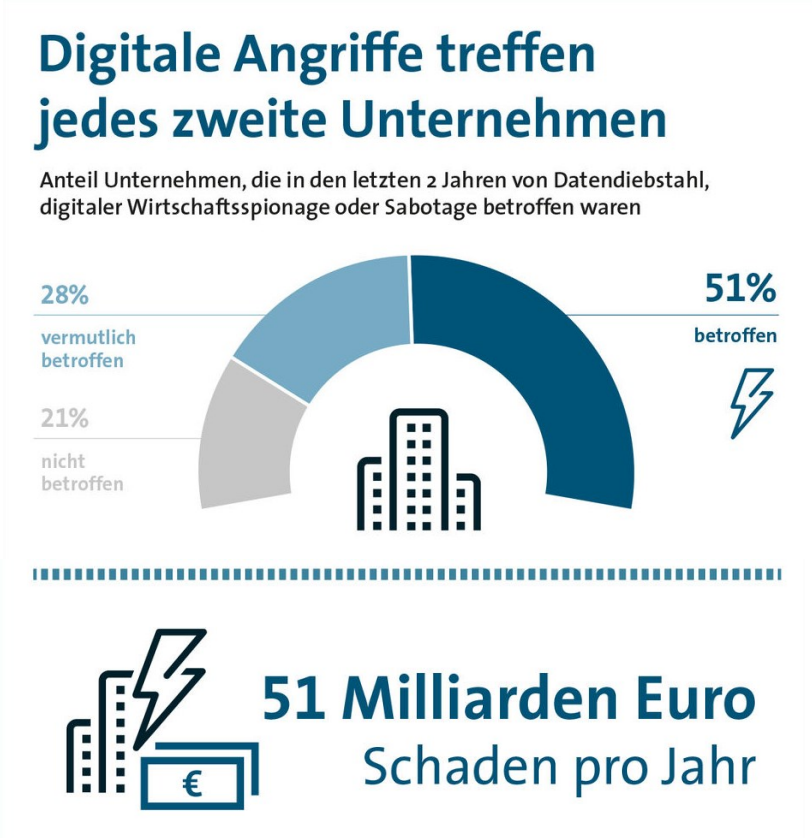
itb Institut für Betriebsführung im Handwerk
UNIVERSITÄT SIEGEN

Störungen des Geschäftsbetriebes

Das Risiko wird meist verdrängt

Stromausfall, Vandalismus, Cyberangriffe Ausfälle von Server, Internet oder Outsourcing-Dienstleister/innen können zu erheblichen Störungen oder Ausfällen von Geschäftsprozessen führen.

Folge: enorme Schäden



Wie sich Betriebe schützen können

10 Wege

1. Authentifizierungsverfahren
2. Umgang mit Passwörtern
3. E-Mail-Sicherheit
4. Browserschutz
5. Router-Sicherheit
6. Verschlüsselung
7. Hotspot-Nutzung und VPN
8. Anti-Malware-Software
9. Software-Updates
10. Visuelle Hacker*innen

1. Multi-Faktor-Authentifizierung

Erhöhte digitale Sicherheit durch vielschichtige Verifizierung

Identitätsnachweis durch zwei oder mehr unabhängige Faktoren (Anmeldedaten), z.B.:

- **geheimes Wissen**: Passwörter oder PINs
- **physischer Besitz:** Bluetooth®-Telefone, Smartcards oder Token
- **physische oder biometrische Daten:** Gesichts- oder Fingerabdruck

https://www.globalsign.com/de-de/blog/was-versteht-man-unter-multi-faktor-authentifizierung

2. Umgang mit Passwörtern

Best Practices für die sichere Passwortverwaltung

- Einen einprägsamen Satz überlegen, Zahlen und Buchstaben durch Sonderzeichen ersetzen
- Masterpasswort mit unterschiedlichen Zusätzen pro Zugang
- Passwort-Manager nutzen

„Alle meine Entchen schwimmen auf dem See.“
= AmEad.....

Top Ten deutscher Passwörter

1. 123456	6. hallo123
2. 12345	7. hallo
3. 123456789	8. 123
4. ficken	9. passwort
5. 12345678	10. master

Tipps zur Passwortwahl

Bei der Passwortwahl empfiehlt das Hasso-Plattner-Institut daher:

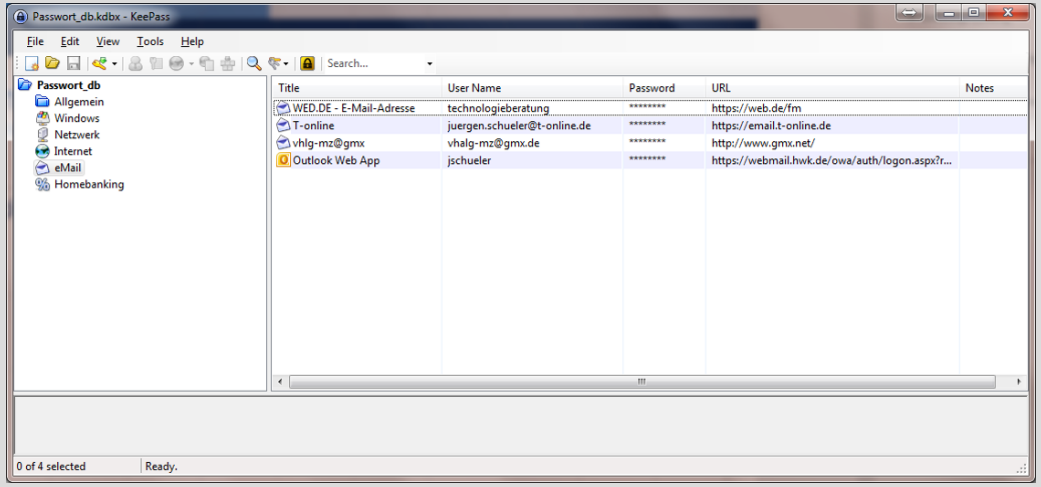
> Lange Passwörter (> 15 Zeichen)
> Alle Zeichenklassen verwenden (Groß-, Kleinbuchstaben, Zahlen, Sonderzeichen)
> Keine Wörter aus dem Wörterbuch
> Keine Wiederverwendung von gleichen oder ähnlichen Passwörtern bei unterschiedlichen Diensten
> Verwendung von Passwortmanagern
> Passwortwechsel bei Sicherheitsvorfällen und bei Passwörtern, die die obigen Regeln nicht erfüllen
> Zwei-Faktor-Authentifizierung aktivieren

2. Umgang mit Passwörtern

Passwort-Safe nutzen

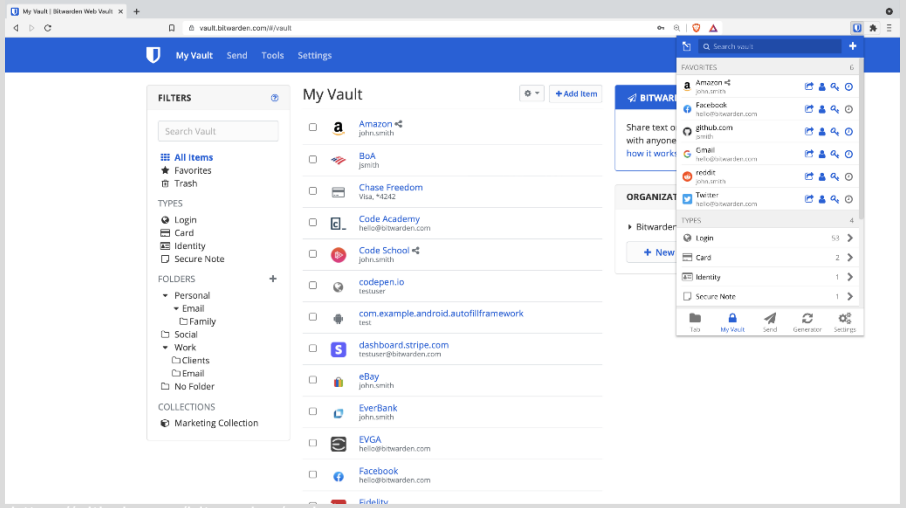
KeyPass

KeyPass ist eine Open-Source-Passwortverwaltungssoftware, die es Nutzer/innen ermöglicht, ihre Passwörter sicher und zentralisiert zu speichern



Bitwarden

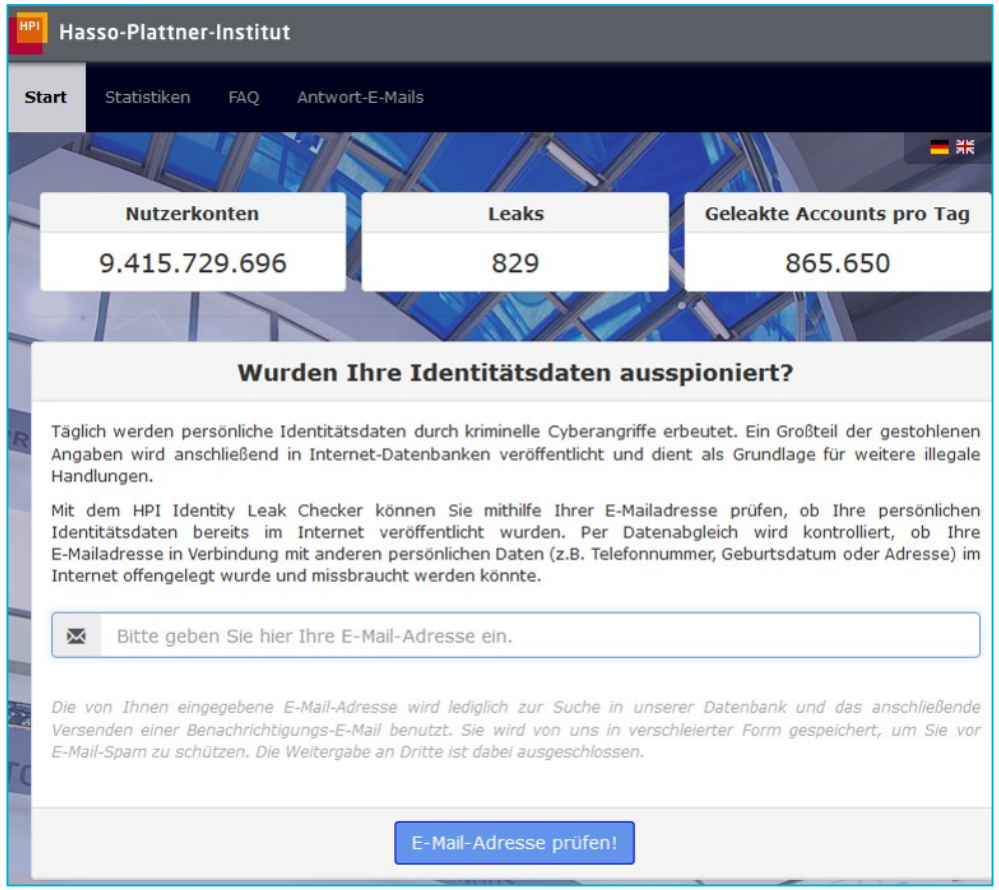
Bitwarden ist eine Open-Source-Passwortverwaltungslösung, die sowohl Einzelpersonen als auch Teams eine sichere und synchronisierte Aufbewahrung ihrer Anmeldedaten bietet



https://github.com/bitwarden/web

3. E-Mail-Sicherheit

Wurde Ihre Identität ausspioniert?



HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

3. E-Mail-Sicherheit

Umgang mit unsicheren E-Mails

https://www.netzwelt.de/news/158678-spam-e-mails-so-ermittelt-wahren-absender-gefaelschten-mails.html

Gefälschte Absenderadresse
Überprüfung der E-Mail-Adresse des Absenders durch Vergleich. Möglichkeit des persönlichen oder telefonischen Kontakts zum Absender.


https://www.storage-insider.de/vertrauliche-daten-in-der-cloud-schuetzen-a-870680/

Vertrauliche Daten
Vorsicht bei Anfragen nach persönlichen Daten, Geheimnummern oder Passwörtern.


https://www.cpm-bg.de/aktuelles/dringender-handlungsbedarf-in-der-arbeitszeiterfassung-kontakt-nun-die-stechuhr-4-0/

Dringender Handlungsbedarf
Betrügerische E-Mails können falschen Druck durch angebliche Fristen erzeugen. Überlegung, ob eine solche Nachricht erwartet wurde.

https://www.kaspersky.de/resource-center/preemptive-safety/scam-websites

Gefälschte Websites
Verlinkungen in E-Mails, die zu unbekannten Webseiten führen. Ziel-URL beim Überfahren des Links mit der Maus überprüfen.

4. Browserschutz

Sicher surfen

Automatische Browser-Updates aktivieren

Schutz vor betrügerischen Webseiten

Inhalte und Plugins beschränken

https://www.juraforum.de/news/sind-ankervpns-und-browserschutz-etwa-legal_257950

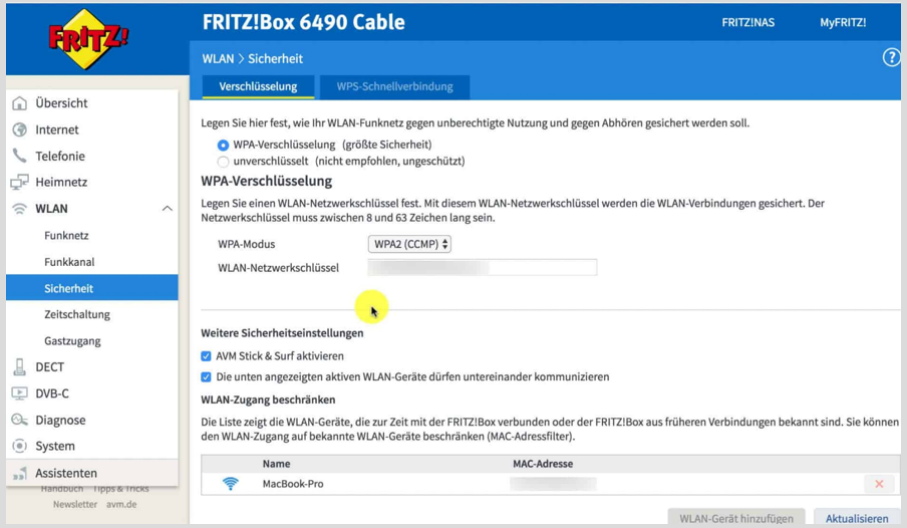
5. Router-Sicherheit

Schutz und Optimierung des zentralen Knotenpunkts im Heimnetzwerk

WLAN-Verschlüsselung

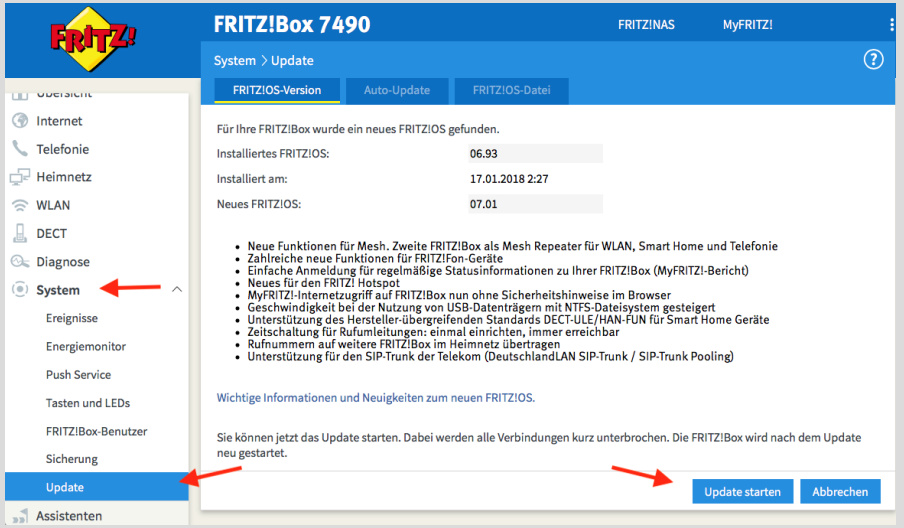
Höchsten Verschlüsselungs-standard wählen (**WPA3**)

Router immer mit personalisiertem **Administrator-Passwort** sichern



Firmware aktualisieren

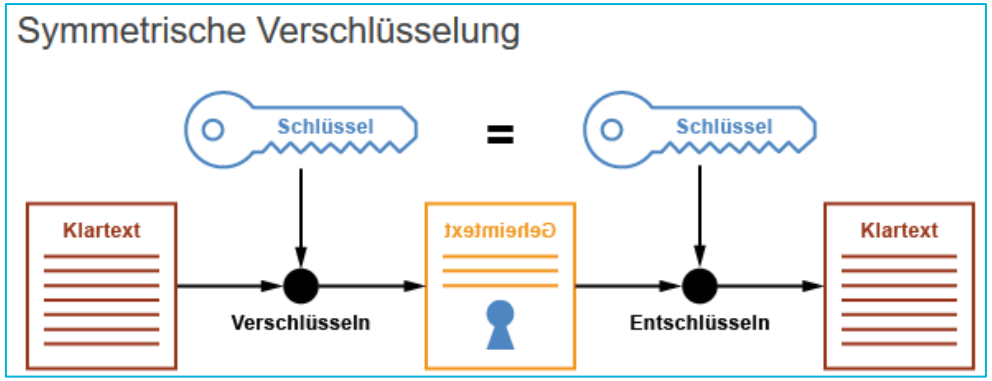
Regelmäßige Firmware-Aktualisierungen sind essenziell, um Router vor aktuellen Sicherheitslücken zu schützen. Sie gewährleisten eine optimierte Leistung und schließen potenzielle Einfallstore für Cyberangriffe



6. Verschlüsselung

Der Schlüssel zum Schutz digitaler Daten und Kommunikation

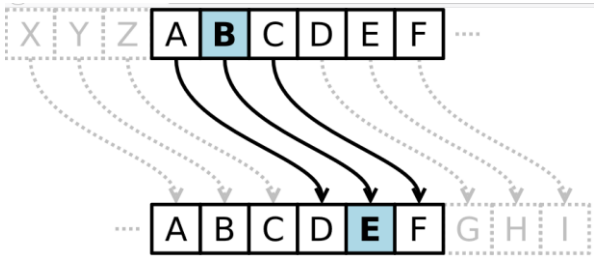
- **Symmetrische Verschlüsselung:** Ein Verfahren, bei dem derselbe Schlüssel zum Verschlüsseln und Entschlüsseln verwendet wird
- **Schlüssel:** Einheitliches geheimes Element, das für beide Prozesse (Verschlüsseln und Entschlüsseln) genutzt wird
- **Verschlüsseln:** Prozess, bei dem der Klartext mit Hilfe des Schlüssels in einen unleserlichen Code (Chiffretext) umgewandelt wird
- **Entschlüsseln:** Prozess, bei dem der Chiffretext mithilfe desselben Schlüssels wieder in den ursprünglichen Klartext zurückverwandelt wird
- **Sicherheit:** Abhängig von der Geheimhaltung des Schlüssels; wenn der Schlüssel kompromittiert wird, sind sowohl die Verschlüsselung als auch die Entschlüsselung gefährdet



6. Verschlüsselung

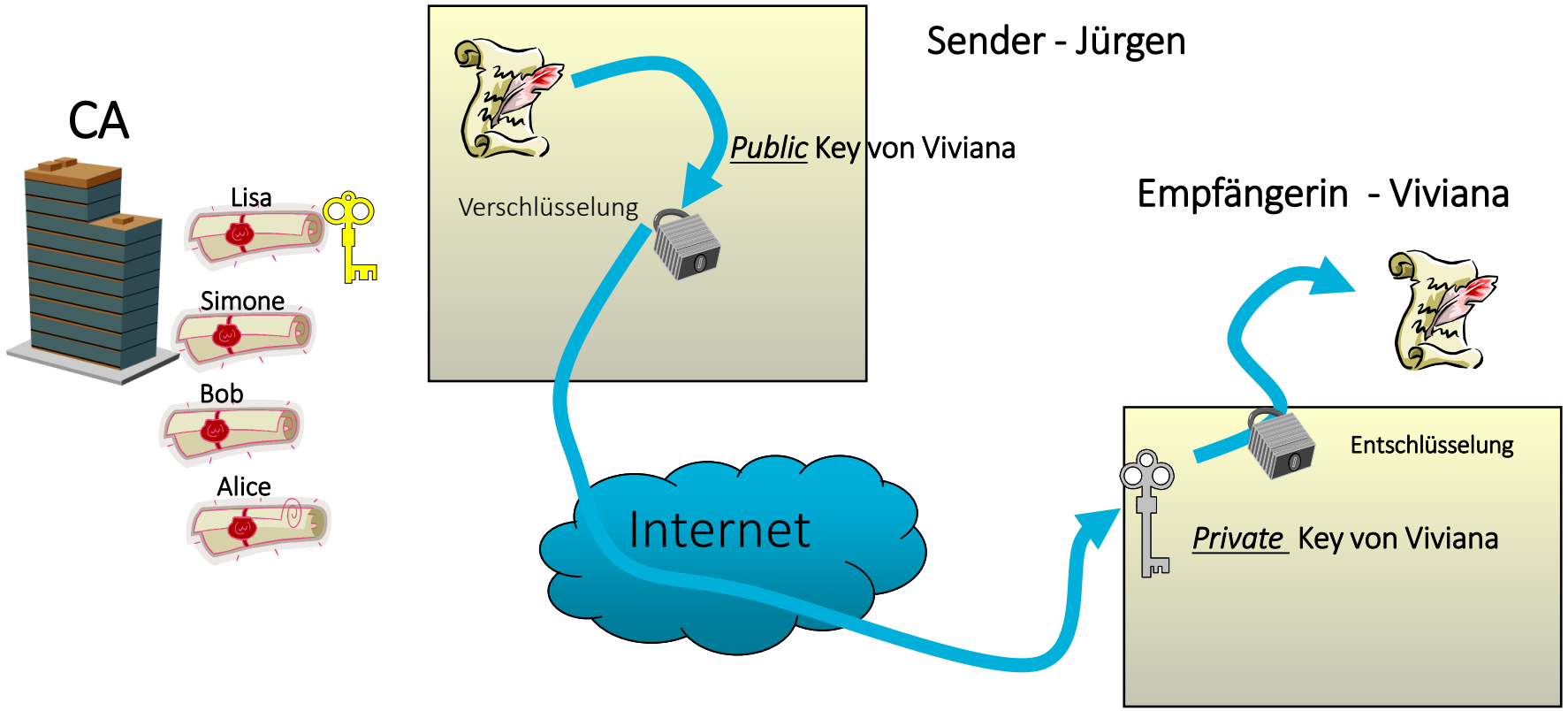
Der Schlüssel zum Schutz digitaler Daten und Kommunikation

- **Caesar-Verschlüsselung:** Ein Verschlüsselungsverfahren, bei dem jeder Buchstabe im Klartext um eine feste Anzahl von Stellen im Alphabet verschoben wird
- **Verschiebung:** Die Anzahl der Positionen, um die ein Buchstabe verschoben wird, bezeichnet man als den Schlüssel der Verschlüsselung
- **Beispiel:** Bei einer Verschiebung um 3 wird "A" zu "D", "B" zu "E" usw.
- **Zyklisch:** Am Ende des Alphabets wird wieder von vorne begonnen, z. B. wird "Z" bei einer Verschiebung um 3 zu "C"
- **Entschlüsselung:** Durch eine Verschiebung um die entgegengesetzte Anzahl von Positionen wird der Klartext wiederhergestellt



6. Verschlüsselung

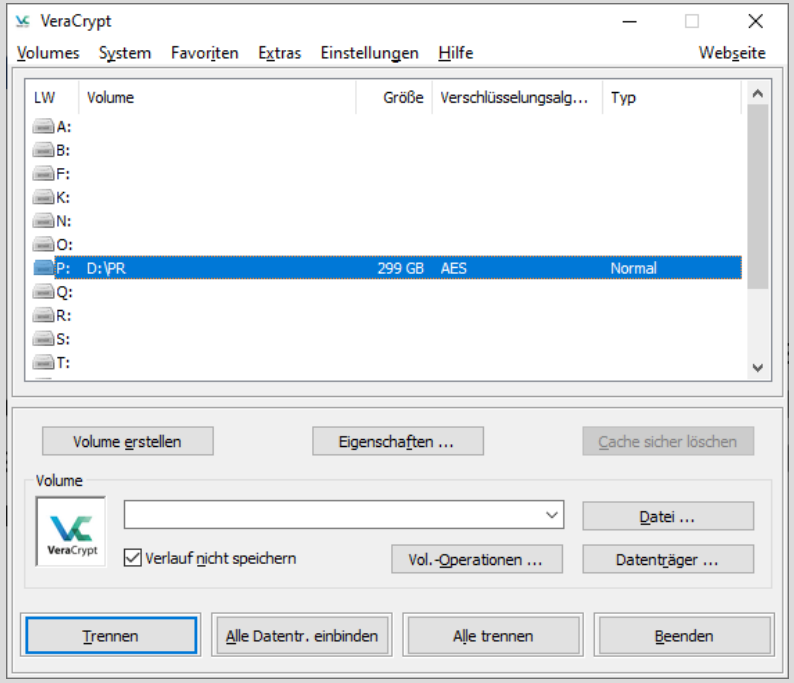
Der Schlüssel zum Schutz digitaler Daten und Kommunikation



6. Verschlüsselung

Verschlüsselung mit Software

VeraCrypt



BitLocker

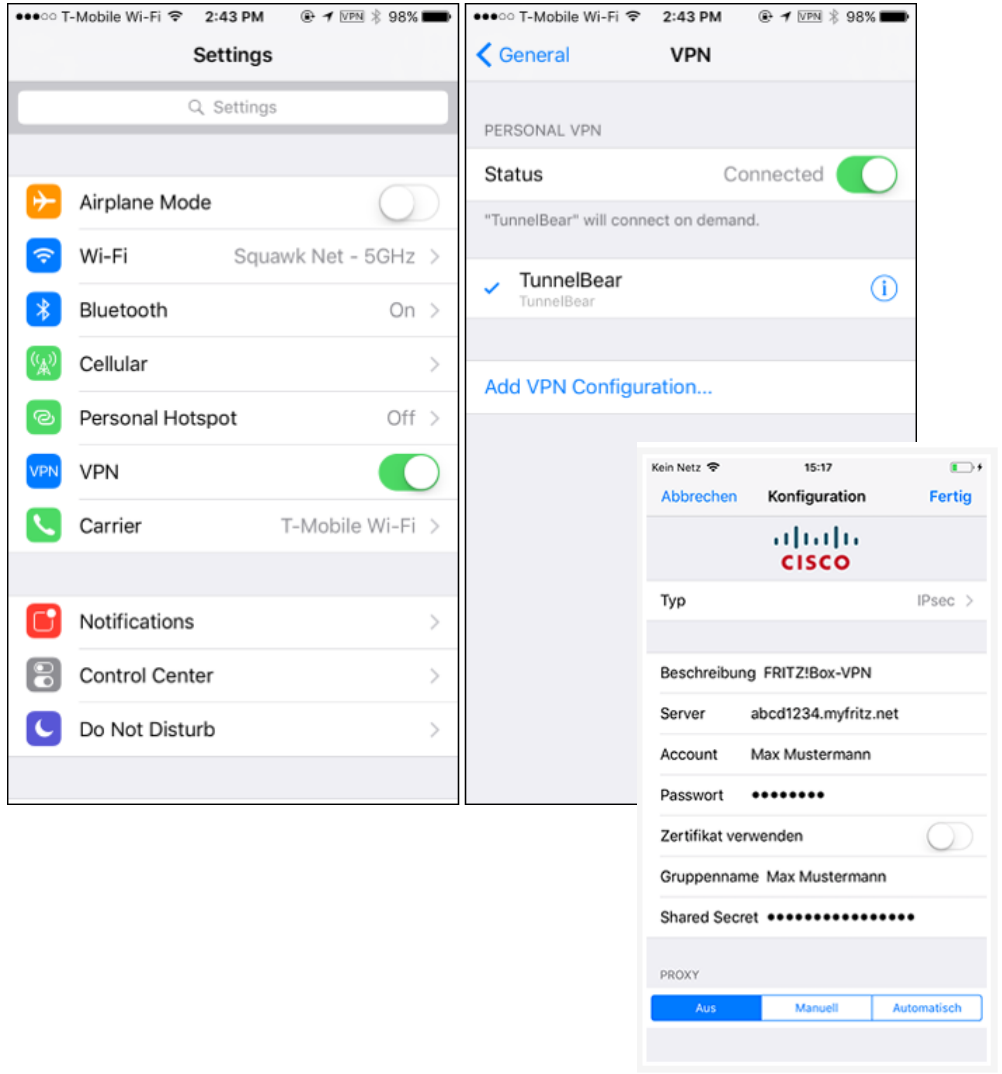
7. Hotspot-Nutzung und VPN

Sicher im öffentlichen Netz

In offenen Netzwerken (Hotspots, z. B. Wifi@DB) ist jede Kommunikation ungesichert und öffentlich.

Bei fehlenden Alternativen VPN (Virtual Private Network) nutzen.

Tipp:
Kostenlosen Fernzugang zur eigenen (falls vorhanden) FRITZ!Box einrichten und mit Heimnetz-Einstellungen surfen



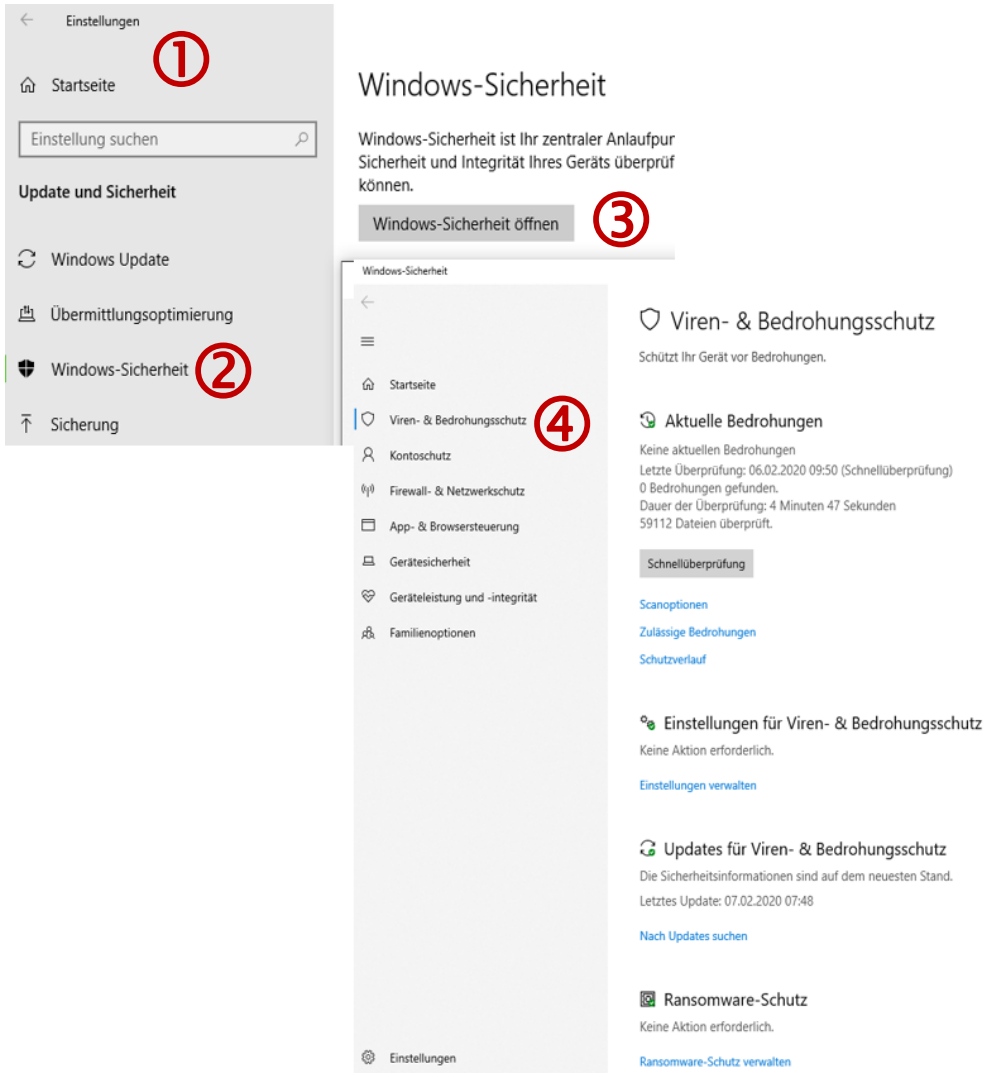
8. Anti-Malware-Software

Schutz vor unerwünschten Bedrohungen

Für Windows 10 Pro-Nutzer/innen ein kostenloses Antivirus-Programm

Anti-Malware-Software sollte niemals deaktiviert werden!

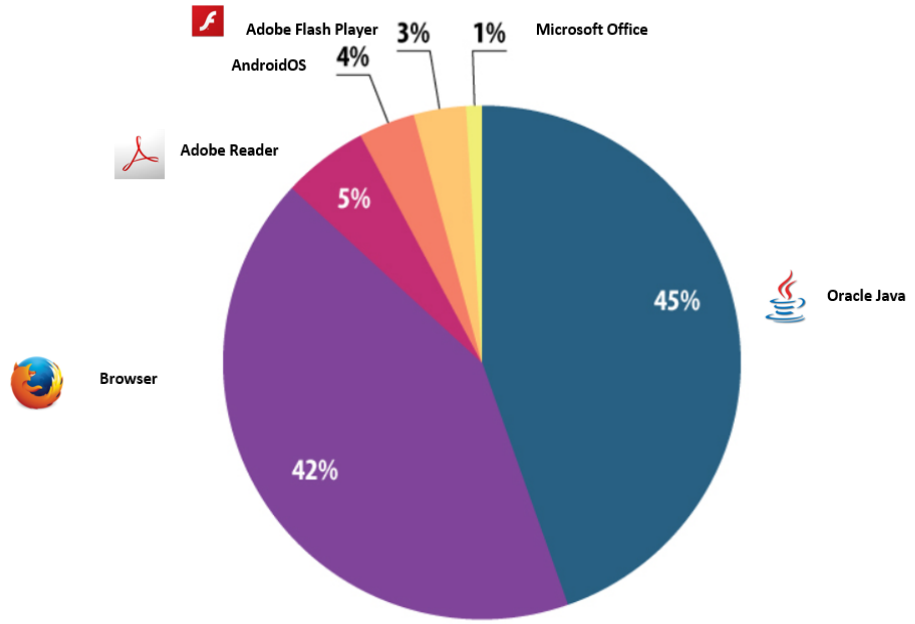
z.B. Windows Defender nutzen



9. Software-Update

Software-Updates für maximale Performance und Sicherheit

- **Versionsnummern auf Hersteller/in-Webseite prüfen**
- **Software aktualisieren**
- **Evtl. Update-Manager nutzen (z. B. SUMO)**

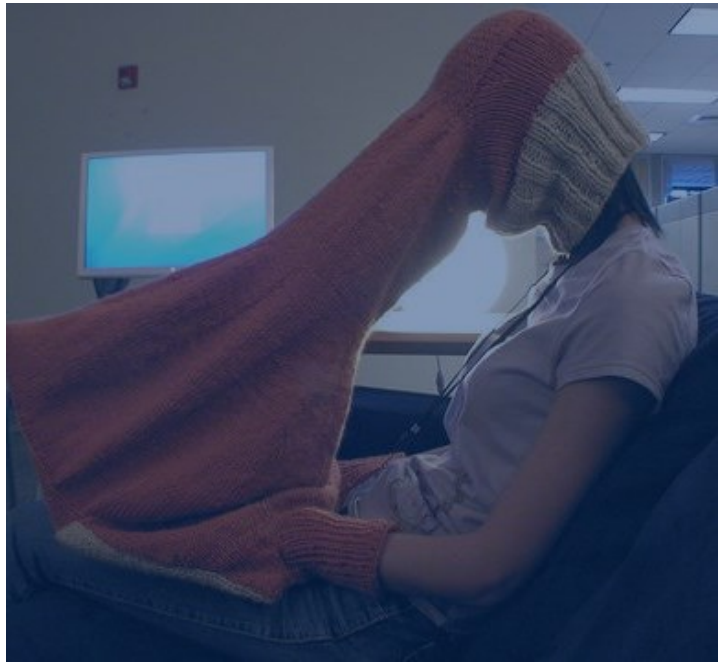


10. Visuelle Hacker*innen stoppen

z.B. Sichtschutzfolie

Sichtschutz verwenden, der den Betrachtungswinkel des Bildschirmes reduziert

Potenziellen visuellen Hacker*innen Sicht versperren



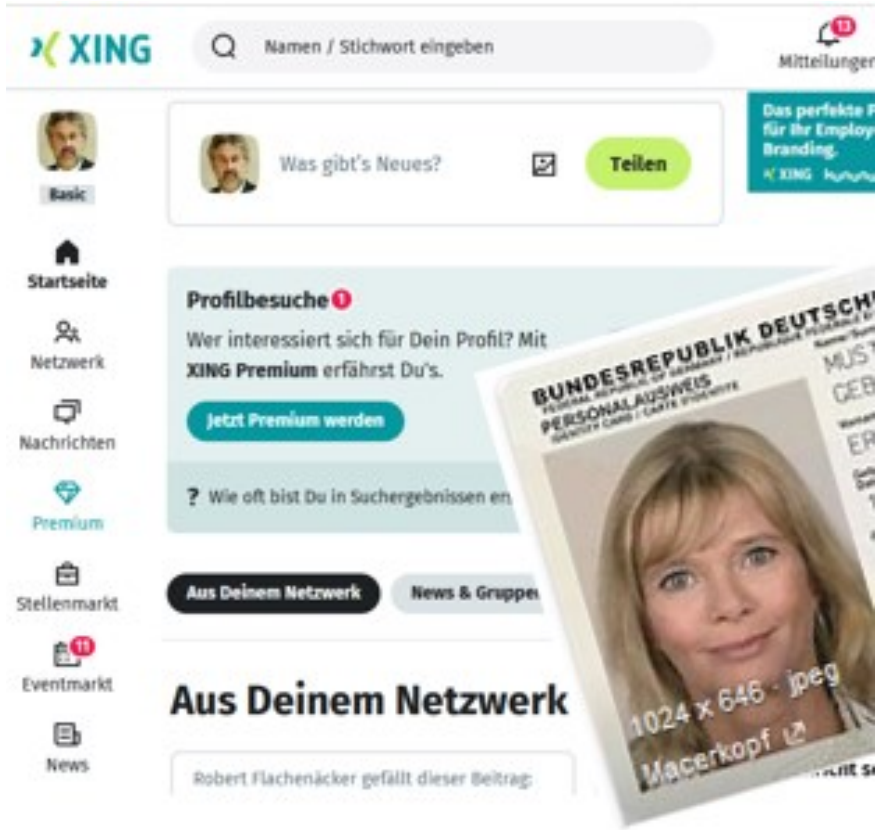
Identitätsdiebstahl

Schützen Sie, was Ihnen gehört

- **Identitätsdiebstahl** (oder Identitätsbetrug) liegt vor, wenn jemand persönliche Informationen stiehlt und diese Daten zur Vorspiegelung einer falschen Identität zum eigenen Vorteil (z.B. Warenkreditbetrug) nutzt.

- Zu diesen Daten können u.a.
  - Ihr Name,
  - Ihre Führerschein- und Personalausweisnummer sowie
  - Kontodaten und Kreditkartennummern gehören.

- **Gehen Sie restriktiv mit persönlichen Daten um**
- **Geben Sie Fremden keine privaten Daten (Fakeprofile)**
  - Kreditauskunfteien benachrichtigen
  - Anzeige erstatten
  - Finanzinstitute kontaktieren



Zugänge und Daten schützen

Paretoprinzip

Verfügbarkeit

Vertraulichkeit

Integrität

Kontakt für weitere Informationen

JÜRGEN SCHÜLER
Physiker & Mathematiker

Magdeburger Str. 80
55218 Ingelheim am Rhein

juergen.schueler@t-online.de
Telefon +49 06132 88133

Newsletter des Kompetenzzentrum Smart Services
https://smart-service-bw.de/newsletter/

Kontakt für weitere Informationen

CHRISTOPHE SAID
Projektleitung „Kompetenzzentrum Smart Services“ Universität Siegen

Lehrstuhl für Dienstleistungsentwicklung
in KMU und Handwerk
Kohlbettstr. 15
57072 Siegen

said@wiwi.uni-siegen.de
Telefon +49 271 740 3613

www.wiwi.uni-siegen.de/service-development
www.smart-service-bw.de

Newsletter des Kompetenzzentrum Smart Services
https://smart-service-bw.de/newsletter/

Kontakt für weitere Informationen

HENRIK LERCHE
Projektleitung „Kompetenzzentrum Smart Services“ itb - Institut für Betriebsführung im DHI e. V.

itb - Institut für Betriebsführung im DHI e. V.
Unterweingartenfeld 6
76135 Karlsruhe

lerche@itb.de
Telefon +49 721 93 103 - 39

www.itb.de
www.smart-service-bw.de

Newsletter des Kompetenzzentrum Smart Services
https://smart-service-bw.de/newsletter/