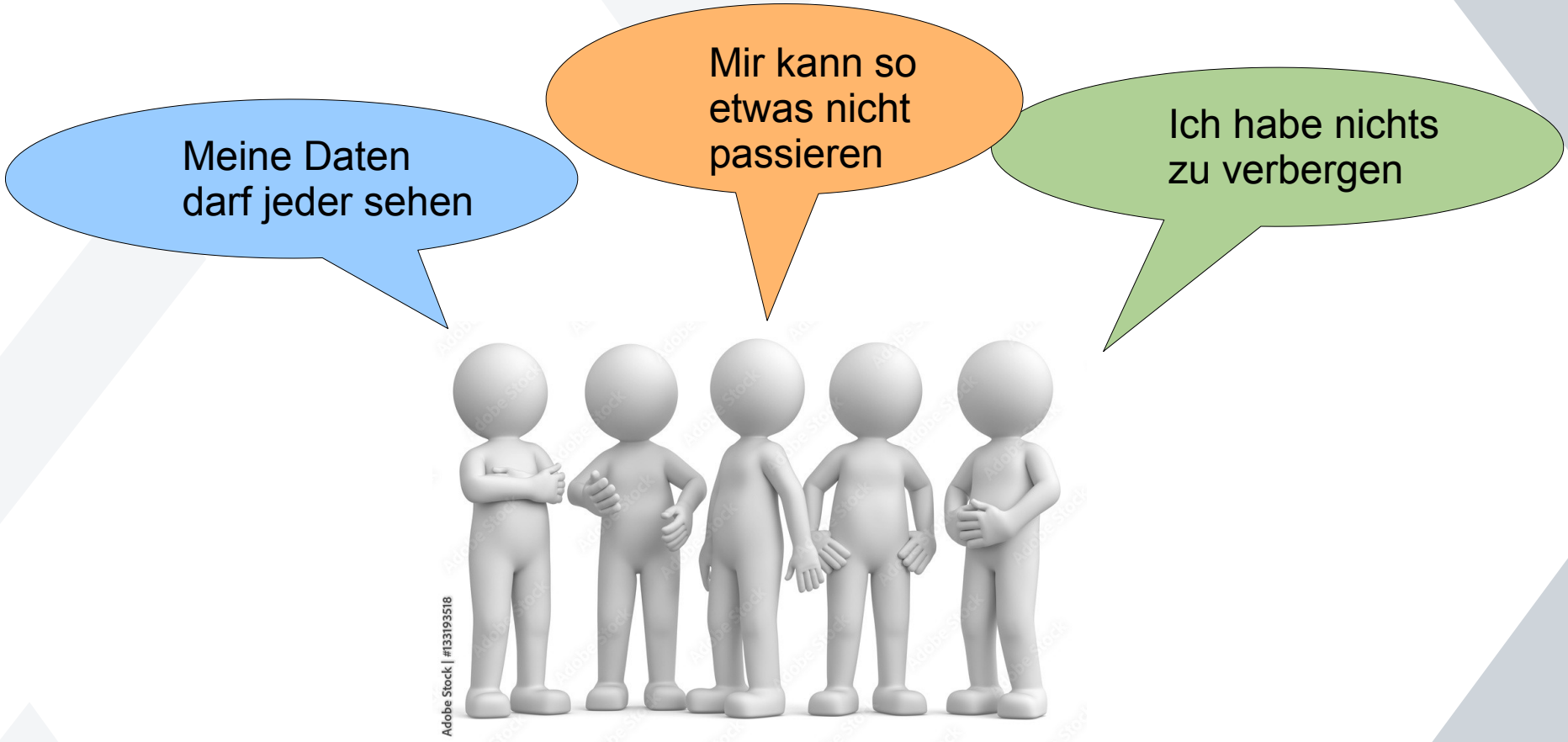
Sicher durch den digitalen Alltag: Tipps für PC, Smartphone & Co.

Martin Stegmeyer, Mai 2026

Quelle: Clipartmax.com

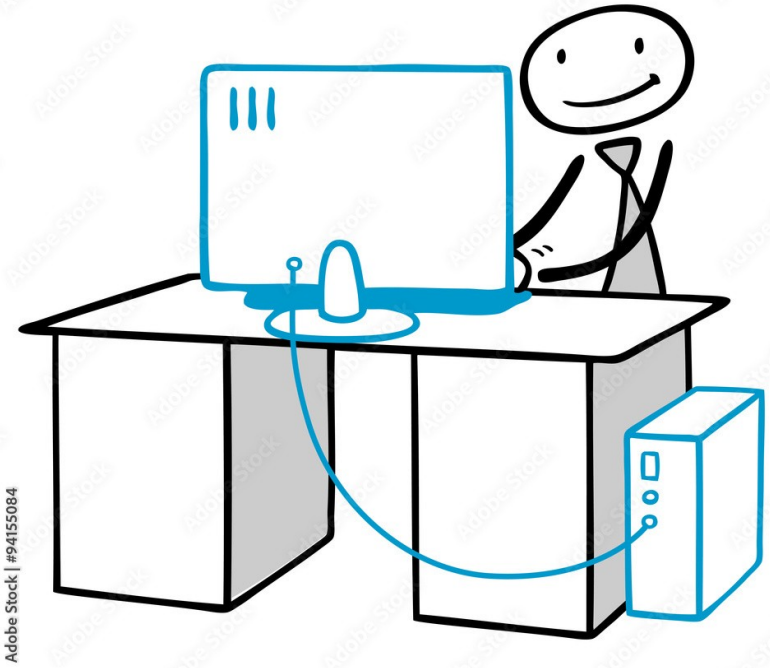
Quelle: fokus.swiss

Warum sollte ich mich für Computer-Sicherheit interessieren?



Wirklich??

Sicherheit vs. Bequemlichkeit



Gefahr durch (Nach)lässigkeit

Quelle: de.vecteezy.com

Quelle: de.dreamstime.com

Reale Gefahren durch Cyber-Angriffe

- Finanzieller Verlust (bis zur Insolvenz)
  - Kontokarten-Betrug
  - Konto-Plünderung
  - Erpressung
  - Verschlechterung Schufa-Status
  - ungewollte Verträge
- Identitätsdiebstahl
  - Cyber-Stalking
  - Rufschädigung
  - Verbreitung von Unwahrheiten
  - Deepfakes, Mobbing

Beispiele für Cyber-Angriffe

Teilen:

Hacker-Angriff auf IT-Dienstleister hat Folgen für Stadtverwaltung Euskirchen

Eine Cyberattacke auf den IT-Dienstleister Südwestfalen.IT sorgt auch im Rathaus der Stadt Euskirchen und in der Kreisverwaltung für Probleme. Das bestätigen die Behörden-Sprecher.

Veröffentlicht: Montag, 30.10.2023 11:49

Die Euskirchener Stadtverwaltung könne weder E-Mails versenden noch empfangen, sagt Stadtsprecherin Winter. "Auch das Serviceportal ist nicht erreichbar. Darüber hinaus können verschiedene publikumsintensive Dienststellen wie das Bürgerbüro und das Standesamt nur eingeschränkt arbeiten."

Auch die Kreisverwaltung Euskirchen ist nach ersten Informationen betroffen. Hier arbeiten die Ausländerbehörde und der Fachbereich Einbürgerung mit dem gehackten IT-Dienstleister zusammen. Dort sei es derzeit etwa nicht möglich, Termine zu vereinbaren.

Wer hinter dem Hackerangriff steckt, ist bisher unklar.

Radio Euskirchen

Cyberattacke mit bösen Folgen: Kriminelle haben einen Serviettenhersteller aus Euskirchen in den Ruin getrieben. 240 Beschäftigte der Traditionsfirma sind betroffen.

Seit fast 100 Jahren produziert die Papierfabrik im rheinischen Euskirchen-Stotzheim Servietten. Nun muss der traditionsreiche Hersteller Fasana Insolvenz anmelden. Der Grund: Eine Cyberattacke hat das Werk im Mai zeitweise komplett lahmgelegt und Produktionsausfälle in Millionenhöhe verursacht. Am 1. Juni stellte Fasana Antrag auf Insolvenz, 240 Beschäftigte sind betroffen.

DW IM FOKUS Ukraine-Krieg Iran-Krieg Donald Trump Neueste Videos

REISE | DEUTSCHLAND

Nach Cyberattacke: Kein Normalbetrieb am Flughafen BER

24.09.2025

Die Festnahme eines Tatverdächtigen in Großbritannien dürfte Reisende am Berliner Flughafen nur am Rande interessieren. Sie müssen sich weiterhin auf lange Wartezeiten, Verspätungen und Ausfälle einstellen.

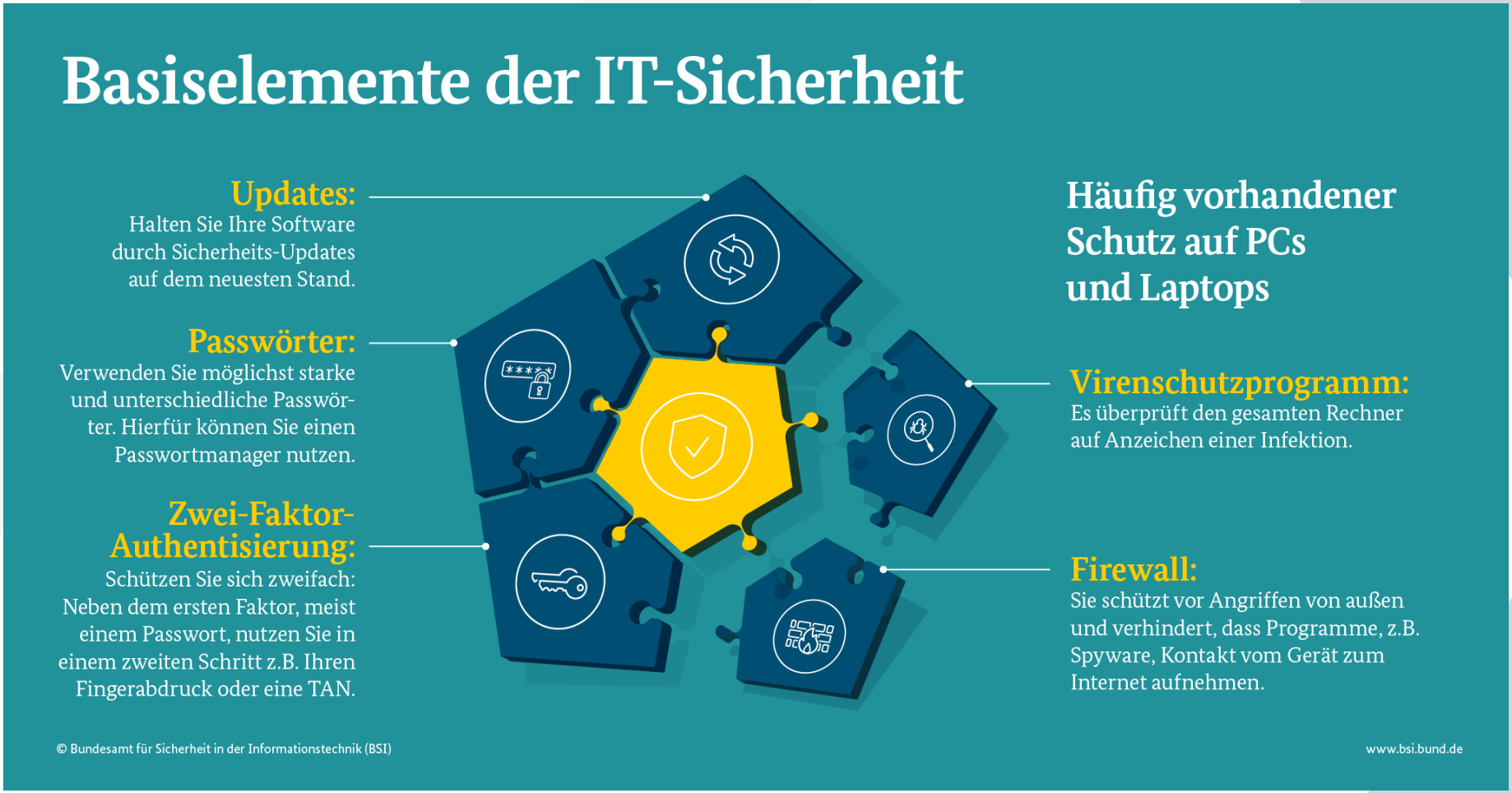
Betrüger versuchen auch über Anrufe persönliche Daten zu ergaunern.

KStA 11.05.2026

300 Euro Schaden durch einen Moment der Unachtsamkeit, erlebte Kölnerin Antje M.. Was hinter Phishing steckt - und wie man den Betrug rechtzeitig erkennt.

Die Kölnerin Antje M. ist im Urlaub in Kopenhagen, als sie auf eine gefälschte Park-App hereinfällt. Sie gibt ihre Kreditkartendaten und TAN ein – dann erscheint auf dem

Wie kann ich mich schützen?

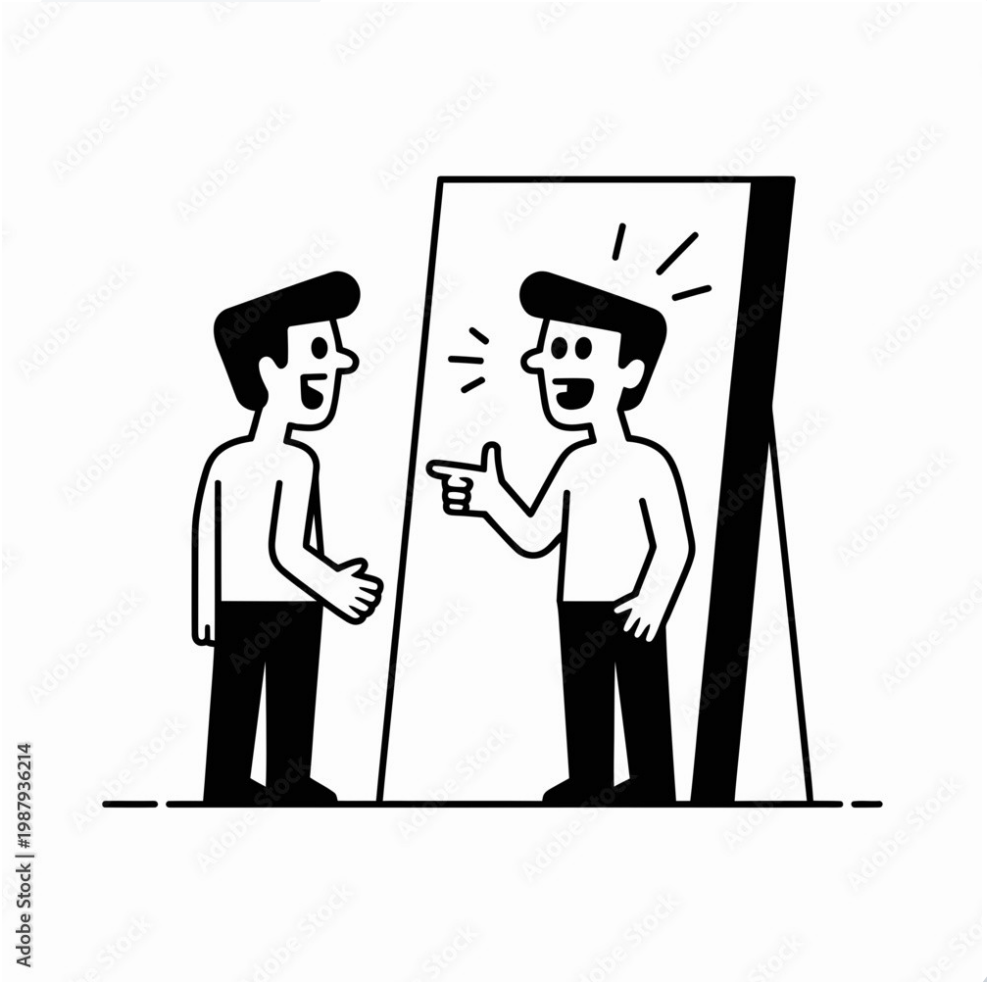


Quelle: Bundesamt für Sicherheit in der Informationstechnik

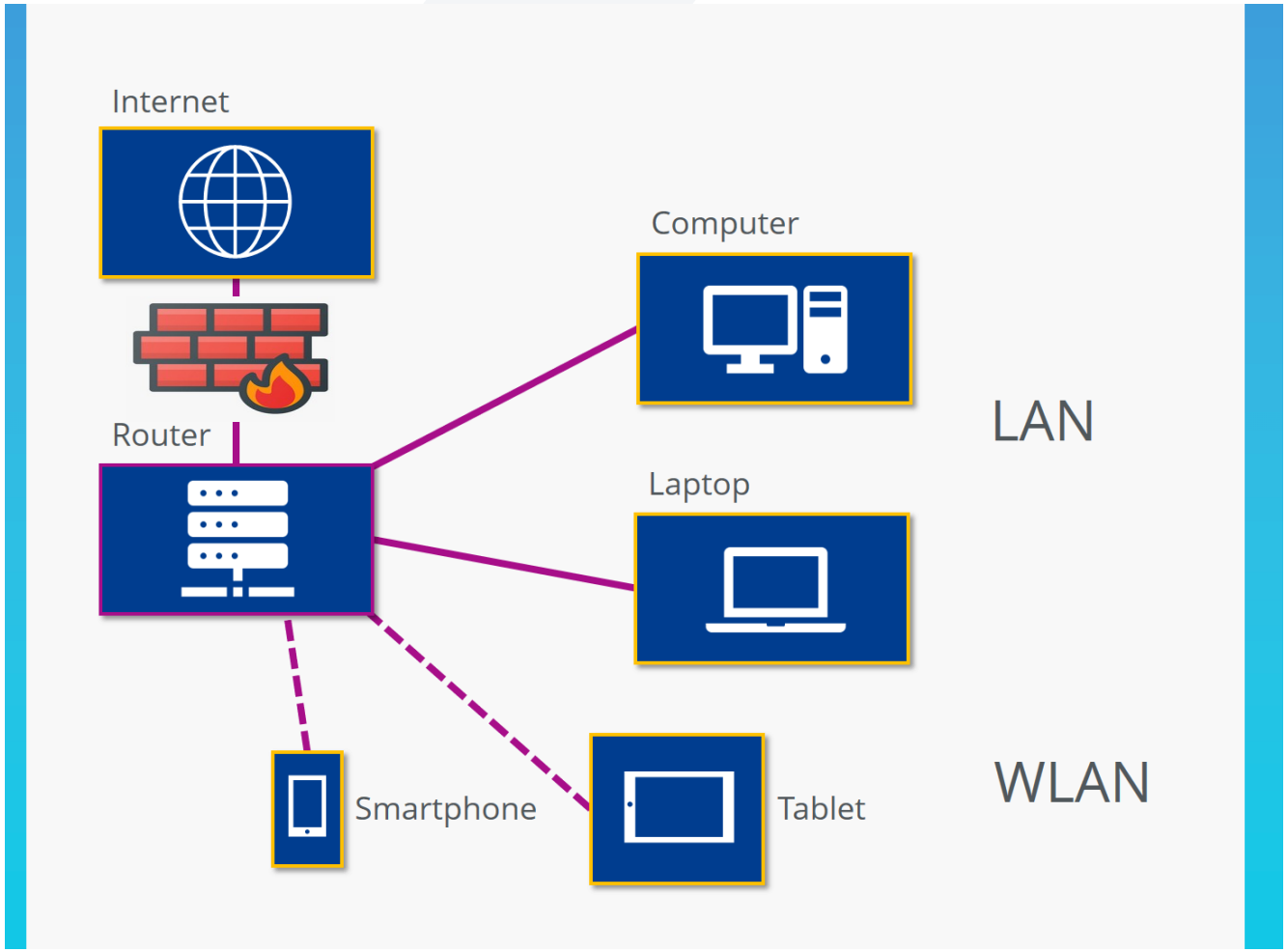
Und noch ein Basiselement der IT-Sicherheit…

Technische Lösung alleine helfen nicht.

Der Mensch ist ein wesentlicher Faktor!



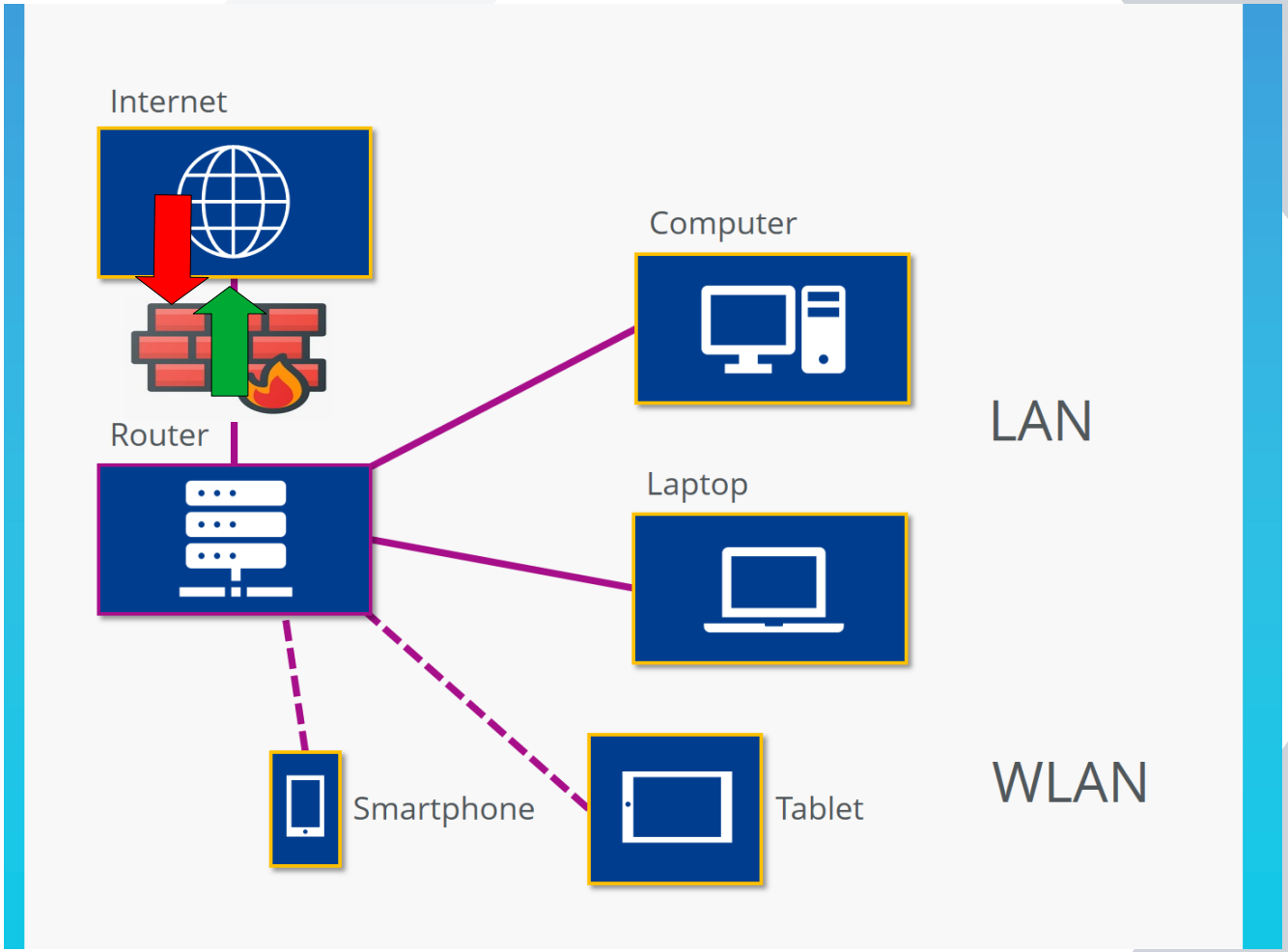
Wie funktioniert ein Netzwerk zu Hause?



Quelle: Ionos

Welche Zugriffe sind möglich?

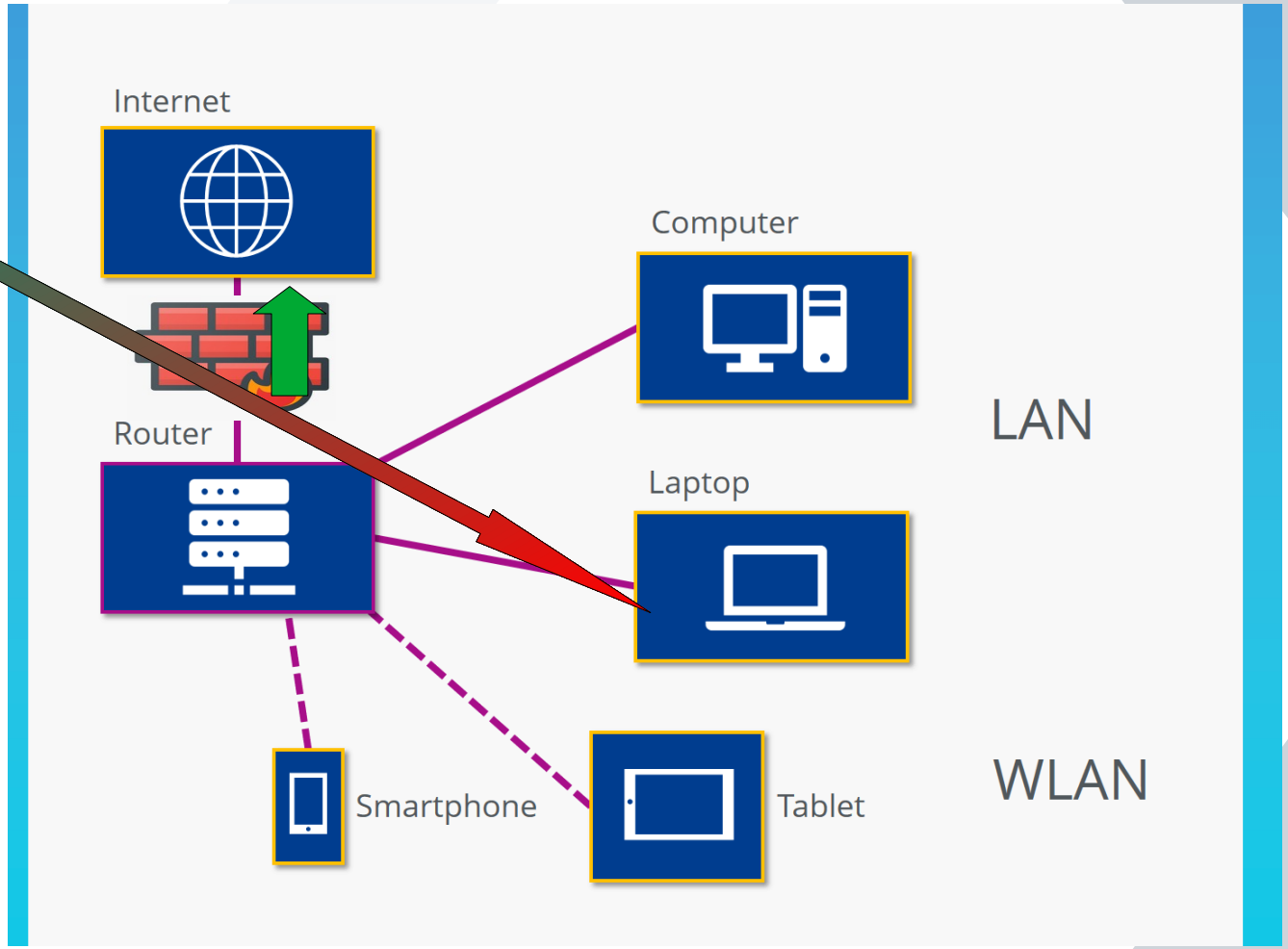
Der Zugriff ist grundsätzlich nur von innen nach außen möglich



Quelle: Ionos

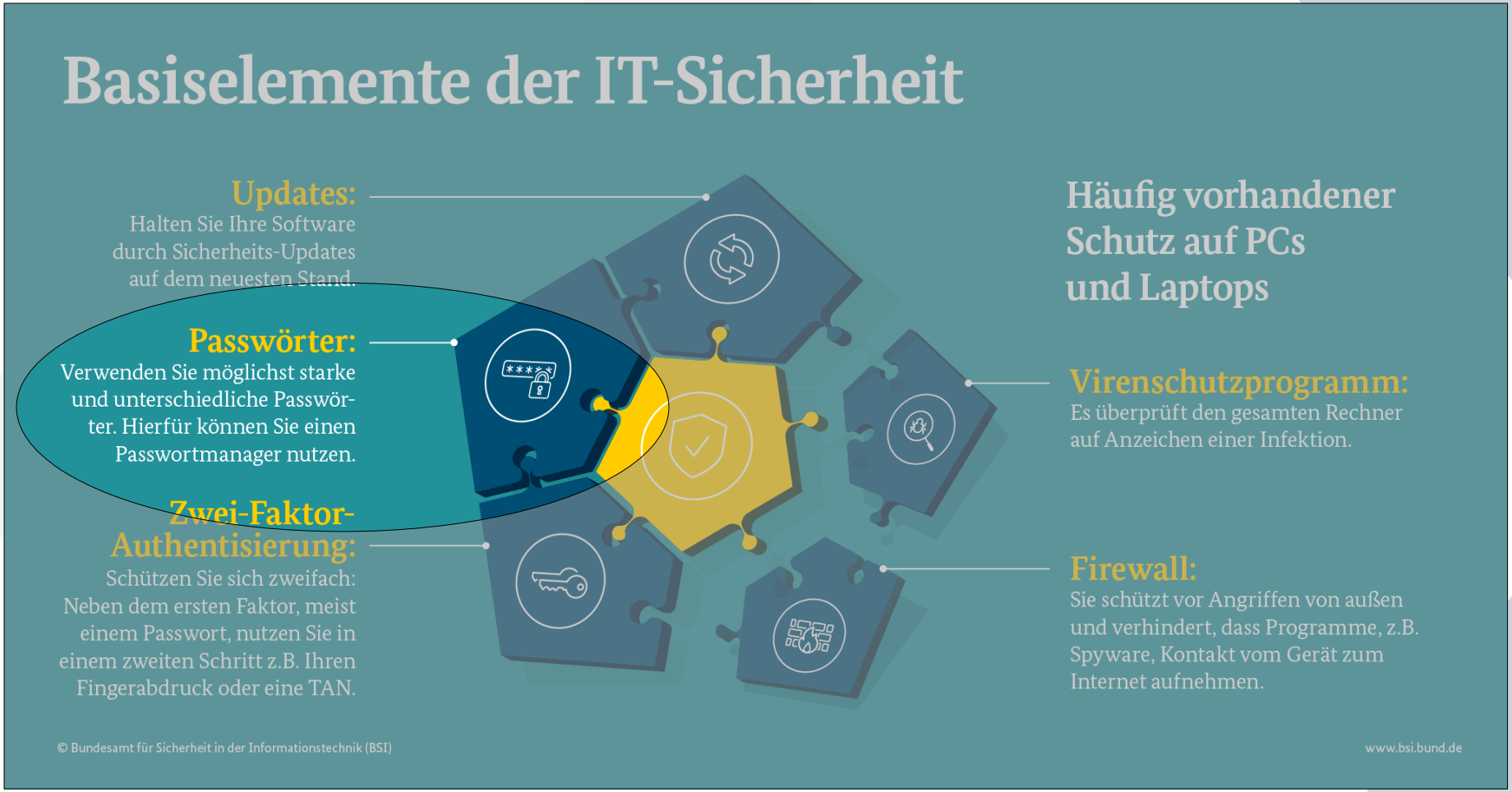
Angreifer können Zugriff erlangen…

Ein Schadprogramm kann den Zugriff für einen Angreifer öffnen!



Quelle: Ionos

Passwörter



Quelle: Bundesamt für Sicherheit in der Informationstechnik

Passwort-Prüfung

- Passwörter werden bei Änderung oder Prüfung verschlüsselt
- Beispiel verschlüsseltes Passwort:
  yj9T$M9VkqReC4oifUrqqHFprT1$BHxadkhdfKzCb8PzZS/P1wV7pyNz
- Die verschlüsselten Daten werden verglichen. Sind diese identisch, wird der Zugriff erlaubt.
- Aus den verschlüsselten Daten lässt sich nicht das tatsächliche Passwort ermitteln!
- Bei Angriffen wird probiert, welches Passwort funktioniert

Sicherheit von Passwörtern

- Angreifer nutzen Programme mit Datenbanken auf Hochleistungs-Computern, um Passwörter zu knacken
- Simple Passwörter bieten keinen Schutz – sie werden innerhalb von Sekunden geknackt.
- Wörter, die im Lexikon vorkommen, sollte man nicht als Passwort verwenden
- Beispiele, wie lange das Knacken dauert:

Passwort	**Dauer**
12345678	0,4 Sekunden
Martin	3 Sekunden
qwertz	3 Minuten
8154711	17 Minuten
Schatzi	29 Minuten
twVSYcdY<6S4	3 Tausend Jahre
2022-mein_H@ustier	2 Millionen Jahre

Die Werte wurden mit dem Passwort-Manager von Avira ermittelt.

Wie kommen Angreifer an Daten?

- Datenbestände von Internet-Händlern werden gestohlen und Kundendaten ausgelesen:
  - E-Mail Adressen bzw. Benutzernamen
  - Kontoverbindungen
  - Kreditkarten-Nummern
  - Adressdaten
  - ...

Aktuelles Beispiel (März 2026) von heise security:

brillen.de: Kundendaten nach erneutem Angriff im Darknet aufgetaucht

Bei brillen.de gab es erneut einen IT-Angriff. Dabei erbeuteten die Täter 1,5 Millionen Kundendatensätze. Die stehen nun im Darknet.

09:24 Uhr 2 | heise Security

Wie geht es dann weiter?

- Im Darknet* werden gestohlene Daten zum Kauf angeboten
- Beispiel: 10 Kreditkarten-Nummern mit Namen und PIN
- …mit Funktions-Garantie und online-Support
- Mit den Zugangsdaten können Betrüger Geldbeträge abbuchen, Waren oder Dienstleistungen bezahlen etc.
- …oder mit gestohlenen Identitäten falsche Informationen verbreiten

*) Wikipedia: Darknet

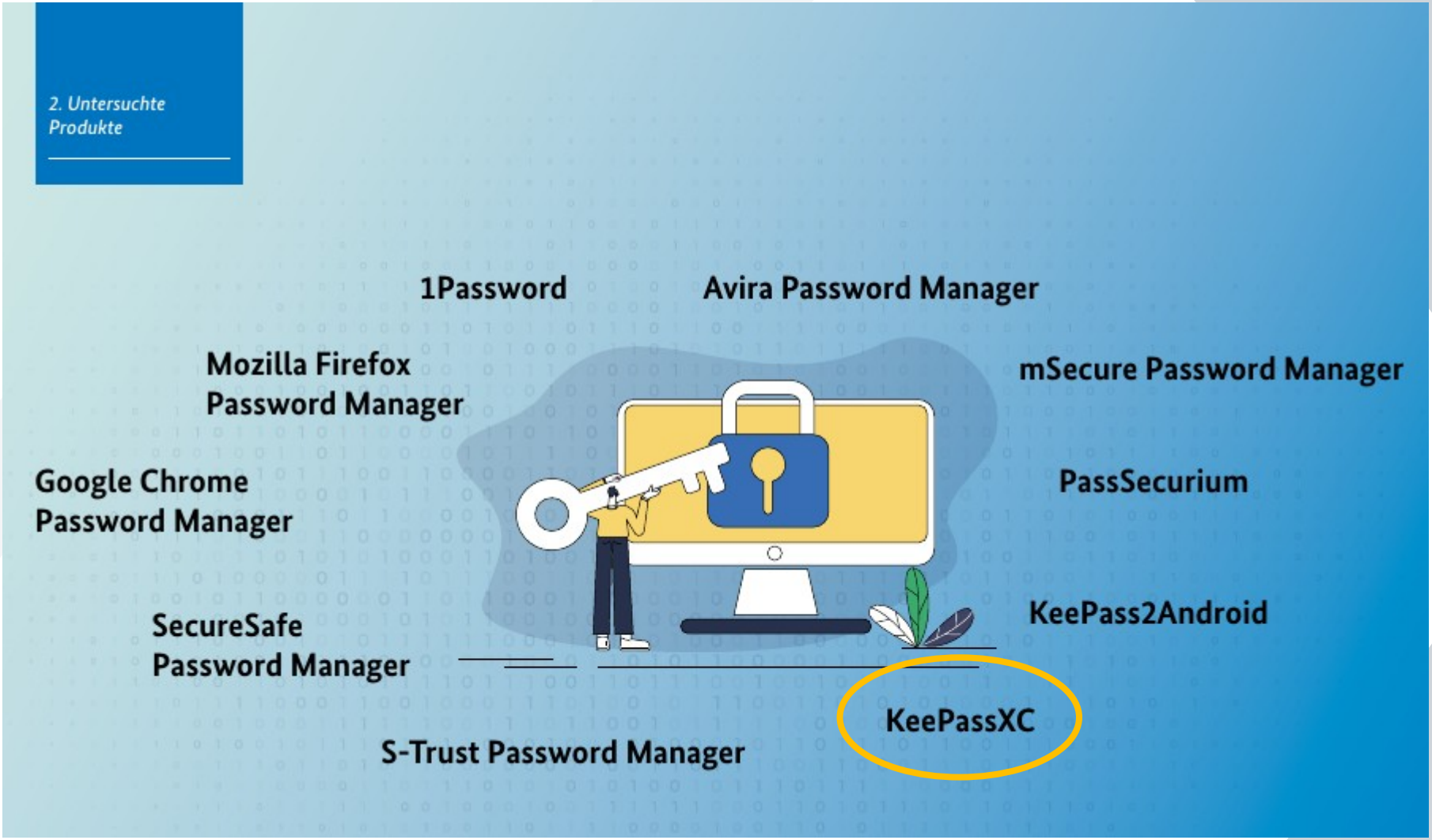
Mehrfach verwendete Passwörter

- Passwörter sollten bei Online-Diensten **nicht mehrfach verwendet** werden.
- Also nicht bei otto.de, amazon.de, ebay.com etc. „Das1st#geheim$“ verwenden.
- **Aber wie soll ich mir die ganzen Passwörter merken?**
- Hier werden verschiedene Methoden verglichen:
  https://www.bsi.bund.de/dok/1148996
- Eine Möglichkeit: Passwörter **zusammensetzen**.
  - Teil 1 kann man sich merken: „DPwk1mgm“ (dieses Passwort kann ich mir gut merken)
  - Teil 2 aufschreiben:

otto.de	sd82$a
amazon.de	rT&!08
ebay.com	qpa1047

  - zusammengesetzt: DPwk1mgmsd82$a

Passwort-Manager: Test vom BSI und der Verbraucherzentrale

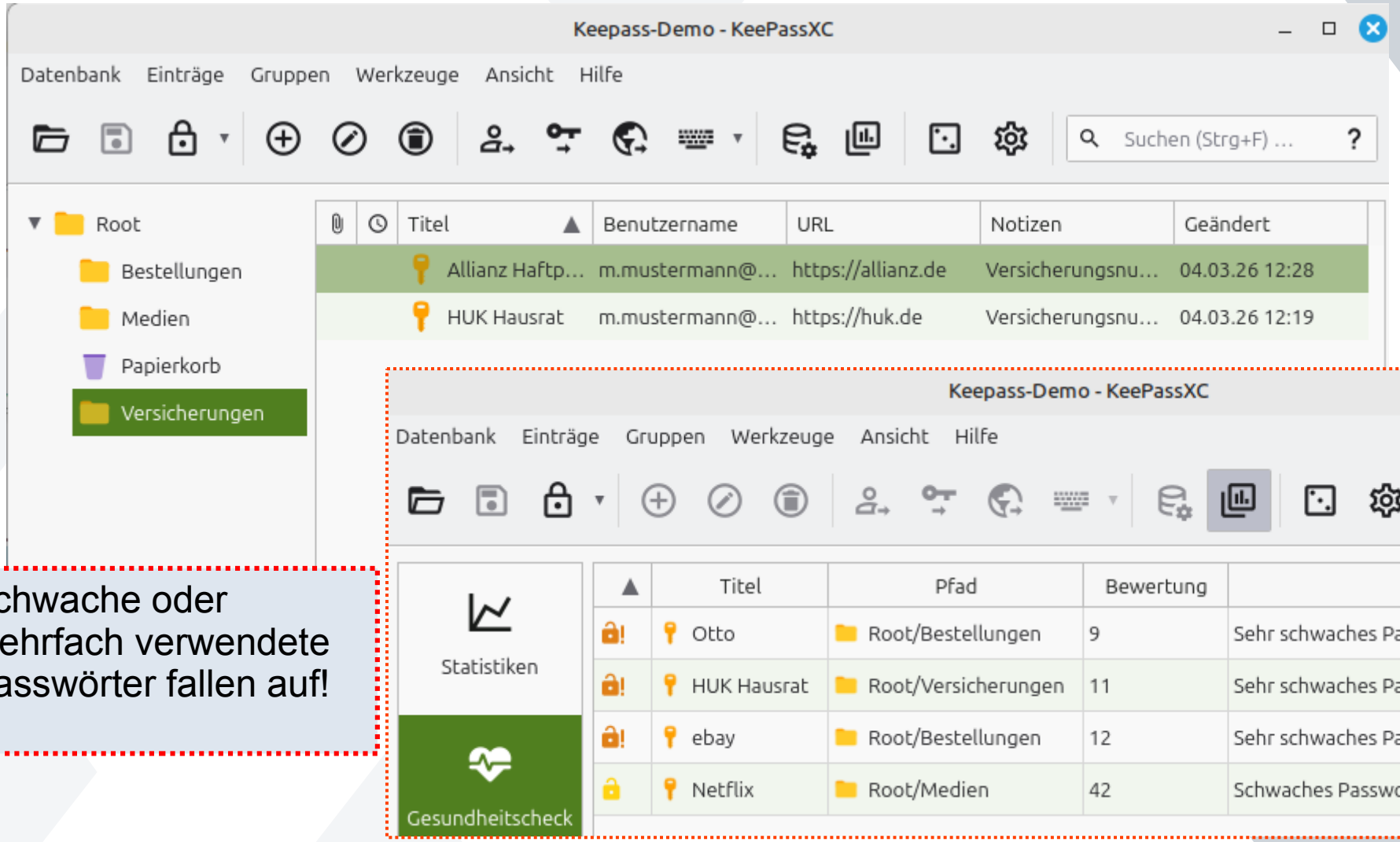


Quelle: Bundesamt für Sicherheit in der Informationstechnik

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/passwortmanager_sicherheit_datenschutz.html

Beispiel KeePassXC

- Die Datenbank wird in einer Datei mit der Erweiterung .kdbx gespeichert.
- Der Inhalt ist verschlüsselt und kann nur nach Eingabe des Master-Passworts eingesehen werden.

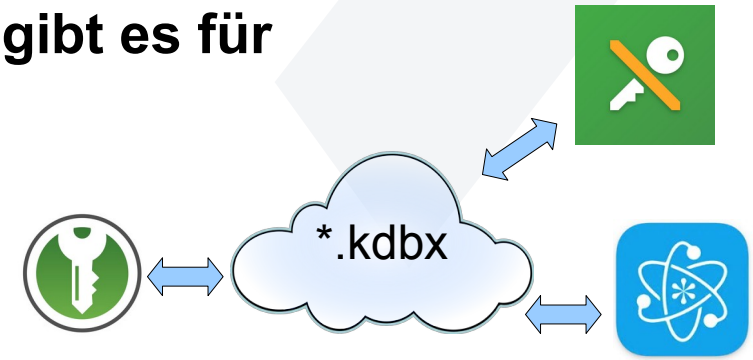


Schwache oder mehrfach verwendete Passwörter fallen auf!

KeePassXC und andere

KeePassXC gibt es für

- Windows
- Mac OS
- Linux



unter https://keepassxc.org/

Die Daten werden lokal gespeichert, können aber über einen Cloud-Speicher synchronisiert werden.

Für Android:
KeePassDX

Für IOS (iPhone):

KeePassium

oder

Strongbox

Diese Apps können mit den Daten von KeePassXC verwendet werden.

Weitere Password-Manager:
- Bitwarden
- Keeper
- **Proton Pass** (open source, kostenlose Variante verfügbar)

Neues Benutzerkonto anlegen

- Neuen Eintrag in Password-Manager anlegen
- Password erzeugen lassen
- Eintrag speichern
- Neues Benutzerkonto anlegen:
  - Benutzername und Password: aus PW-Manager einfügen

Anwendung Password-Manager

- Wenn der Password-Manager in einen Browser integriert ist, werden automatisch Benutzername und Password ausgefüllt, wenn die passende Website aufgerufen wird.
- Ansonsten:
  - Kopiere Benutzernamen / Passwort in Zwischenablage
  - Füge Benutzernamen / Passwort in entsprechendes Feld ein (STRG + V)

Weitere Funktionen von Password-Managern

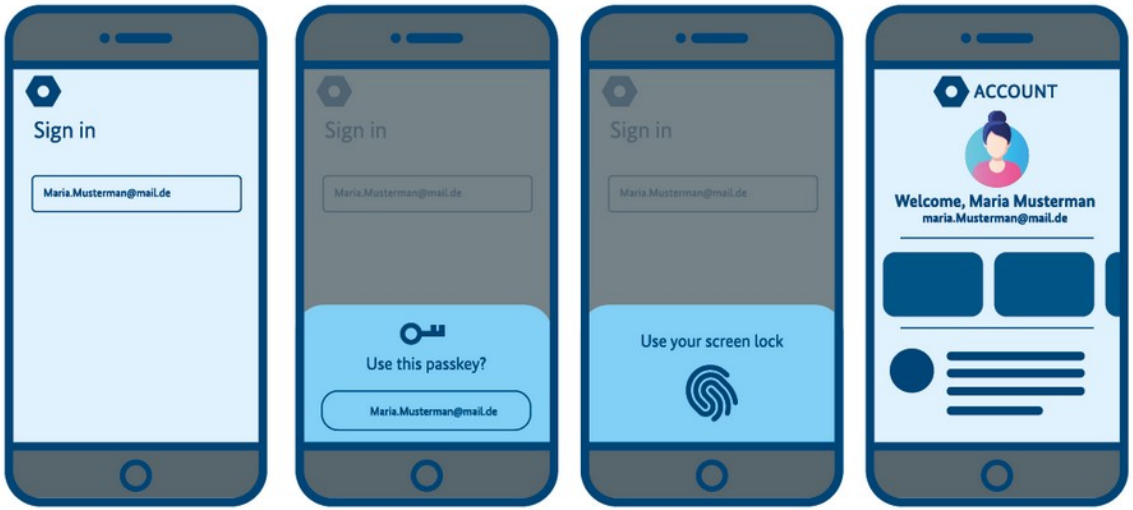
- Speichern von Web-Adressen (URL)
  das kann den Aufruf von gefälschten Adressen verhindern!
- Speichern von Notizen (z. B. Versicherungsnummer, Ansprechpartner)
- Speichern von Zusatzinformationen wie PIN, PUK, Gültigkeitsdatum von Kreditkarten
- Notfallzugriff, teilweise ohne Weitergabe des Master-Passworts
- Prüfung, ob Zugangsdaten kompromittiert wurden
  https://haveibeenpwned.com/

Ergänzung und Alternative zu Passwörtern

- Mehrfaktor-Authentisierung, z. B. mit Smartphone-App oder per SMS
- Passkey
- Wikipedia: FIDO2

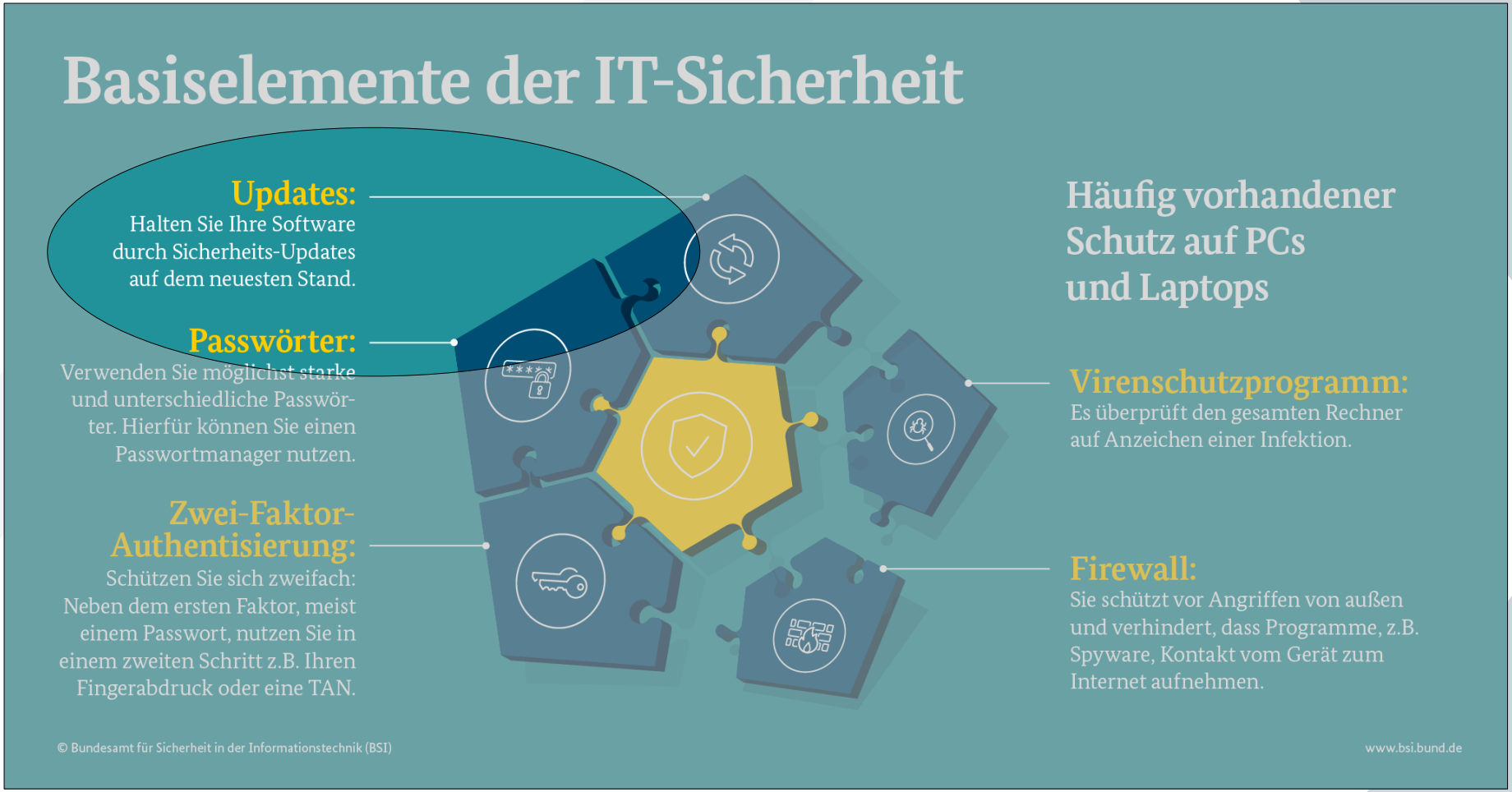
Wie funktioniert Passkey?

Wenn ein Diensteanbieter den Login mittels Passkey ermöglicht, müssen Sie zunächst einmal die Anmeldung per Passkey im entsprechenden Account einrichten. Das geht über die Sicherheitseinstellungen auf der Webseite oder in der App des Anbieters. Ist die Funktion eingerichtet, hinterlegt Ihr Gerät einen sogenannten geheimen Schlüssel im internen Speicher. Gleichzeitig wird ein passender öffentlicher Schlüssel erstellt, der bei Ihrem Onlinedienst, z. B. einem Onlineshop oder einem Streamingdienst, gespeichert wird. Diese Schlüssel sind die Grundlage für ein komplexes, kryptografisches Verfahren, das ab der Registrierung bei jeder Anmeldung von Ihnen unbemerkt abläuft.



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Updates



Quelle: Bundesamt für Sicherheit in der Informationstechnik

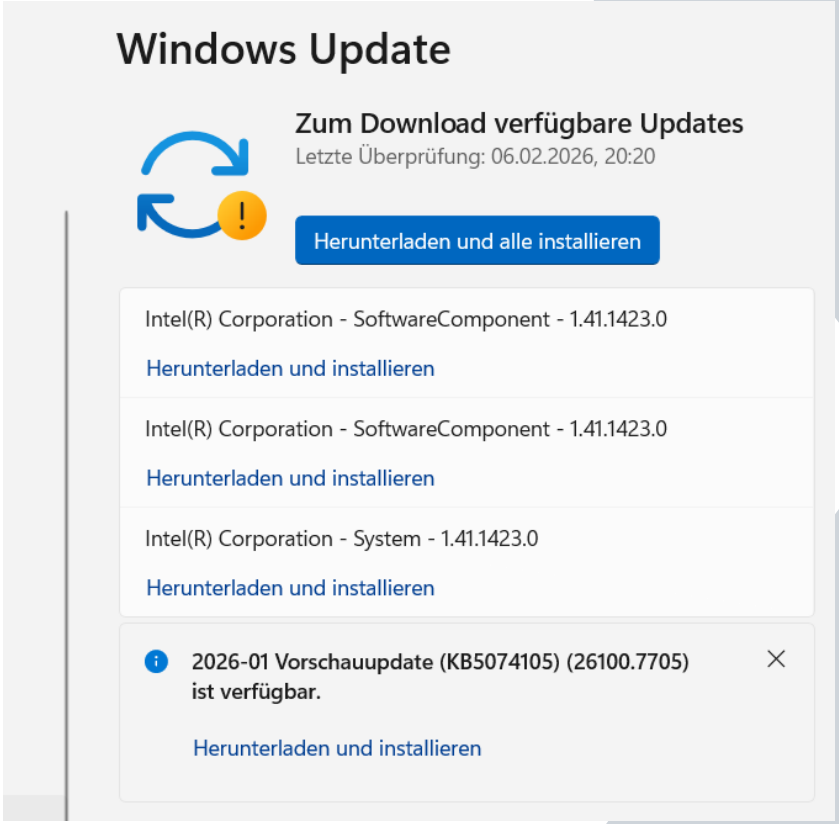
Warum Updates?

- Jede Software enthält Fehler, die Computer, Router etc. angreifbar machen. Werden Schwachstellen vom Hersteller erkannt, werden sie im Idealfall durch ein Update beseitigt.
- Das Betriebssystem Windows ist am meisten verbreitet, und deshalb für Angreifer am interessantesten.
- Für einen sicheren Internet-Zugriff werden Zertifikate* benötigt, die mit Updates verteilt werden. Ohne Updates funktionieren manche Zugriffe nicht mehr oder sind unsicher.

*) PKI – Wikipedia: Public-Key-Infrastruktur

Updates

- Installieren Sie Updates auf Ihren Geräten!
- Infos zu verfügbaren Updates finden Sie u. a. bei Wikipedia unter den Stichworten
  - Windows_11
  - macOS
  - Android_(Betriebssystem)
  - IOS_(Betriebssystem)

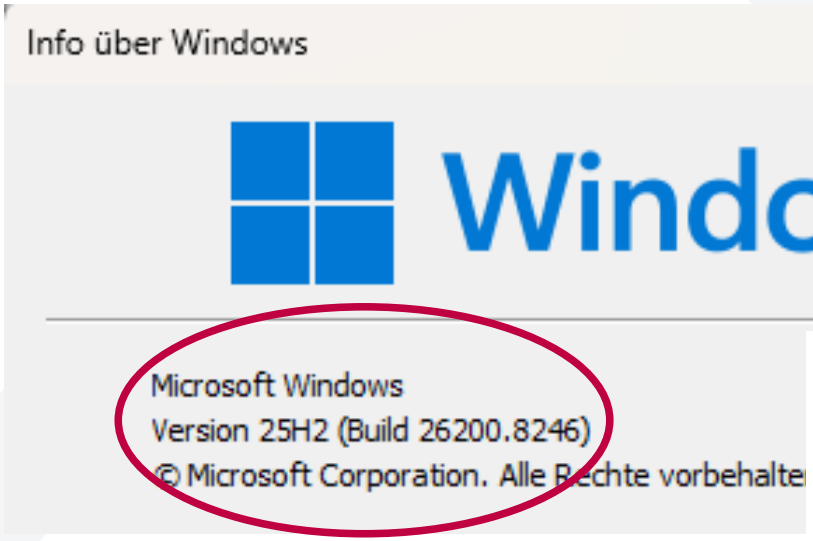


Das gilt auch für Router, z. B. Fritz!box:

https://fritz.com/pages/update-news?product_group=FRITZ%21Box

Windows Versionen

Anzeige der installierten Version mit dem Befehl „winver“
hier: **25H2**



Info von Wikipedia

24H2	26100	2024 Update (Hudson Valley) [63]	15. Juni (für Copilot+-PCs), 1. Okt. 2024 für alle	13. Okt. 2026
25H2	26200	2025 Update (Hudson Valley 2)	30. Sep. 2025	**12. Okt. 2027**[66]
26H1	28000	2025 Update (Hudson Valley 2)	10. Feb. 2026	**14. März 2028**[68]

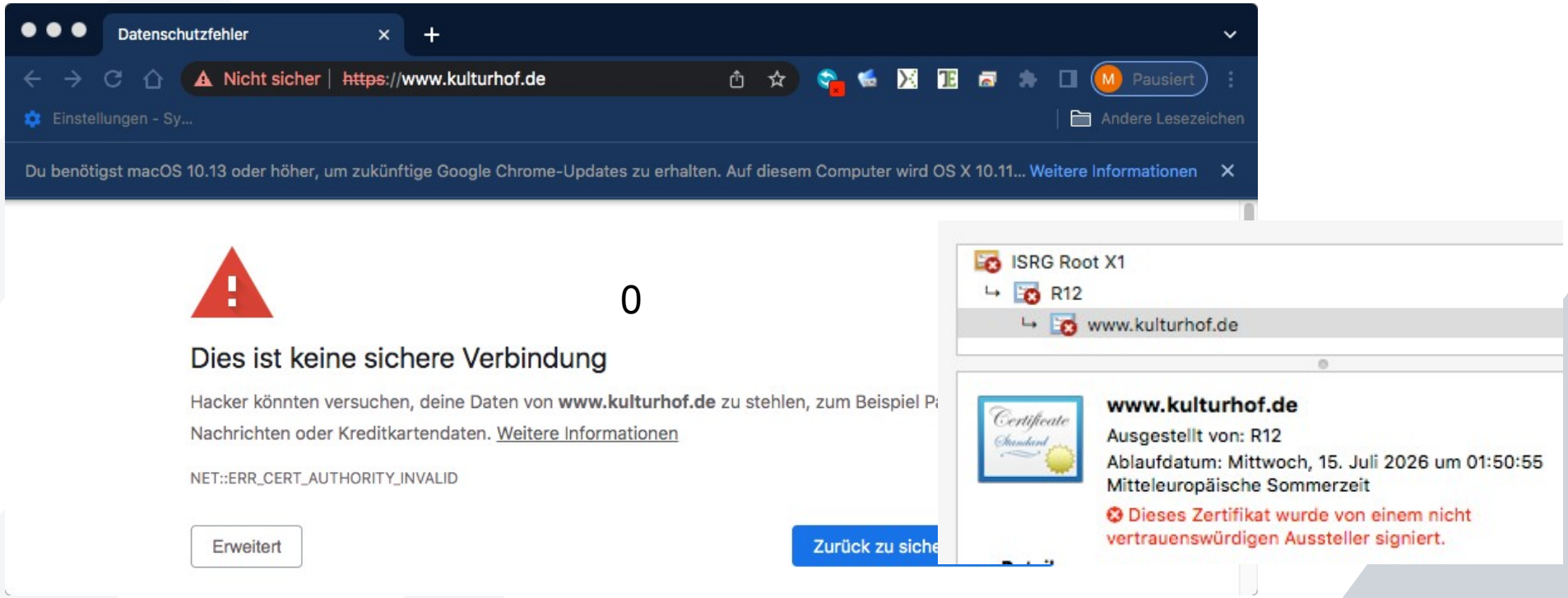
Legende: Ältere Version; nicht mehr unterstützt | Ältere Version; noc

Updates und Upgrades

- Upgrades sind neue Versionen, z. B. der Wechsel von Windows 10 zu Windows 11 oder Ubuntu 24.04 zu Ubuntu 26.04
- Updates sind Zwischenschritte, z.B. von Windows 11 24H2 zu 25H2 oder auch die Aktualisierung von einzelnen Paketen (täglich bis monatlich)
- Wird eine Version nicht mehr unterstützt, gibt es keine Updates mehr. Schwachstellen werden nicht beseitigt und die Funktion ist irgendwann eingeschränkt. Mit einem Browser von 2017 kann man nicht (sicher) auf Internetseiten zugreifen.

Beispiel: iMac von 2007

- Mac OS X El Capitan (10.11), letztes Update 2018
- Google Chrome 103.0.5060 von 2022
- Keine aktuellen Zertifikate; Server-Zertifikat kann nicht geprüft werden

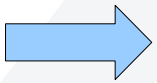


Android Versionen

- Einstellungen > Telefoninfo > Softwareinformationen
  - z. B. Android-Version 13 (seit 2023)
  - Aktuell ist Android 16 (seit 2025)
- Wie lange Updates angeboten werden (teilweise 5 bis 7 Jahre nach Erscheinen des Modells) ist vom Gerätehersteller abhängig
- Informationen gibt es bei den Herstellern oder über eine Internet-Recherche

Apple IOS Versionen

- Einstellungen > Allgemein > Info
  - Aktuell ist IOS 26 (iPhone 17)
  - Das iPhone 11 (von 2019) unterstützt noch IOS 26
- Apple bietet mindestens 5 Jahre* Updates für iPhones an; einzelne Modelle wurden bis zu 10 Jahre mit Updates versorgt

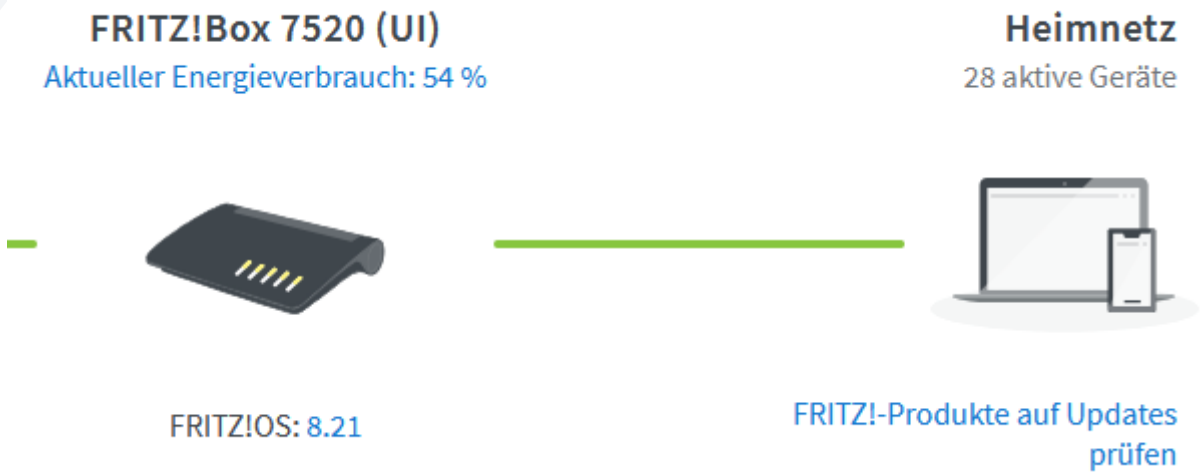


https://support.apple.com/de-de/guide/iphone/iphe3fa5df43/ios

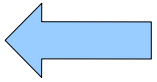
*) Die Zeit beginnt bei Markteinführung des Modells, nicht bei Kauf Ihres Exemplars!

Router (Beispiel Fritz!Box)

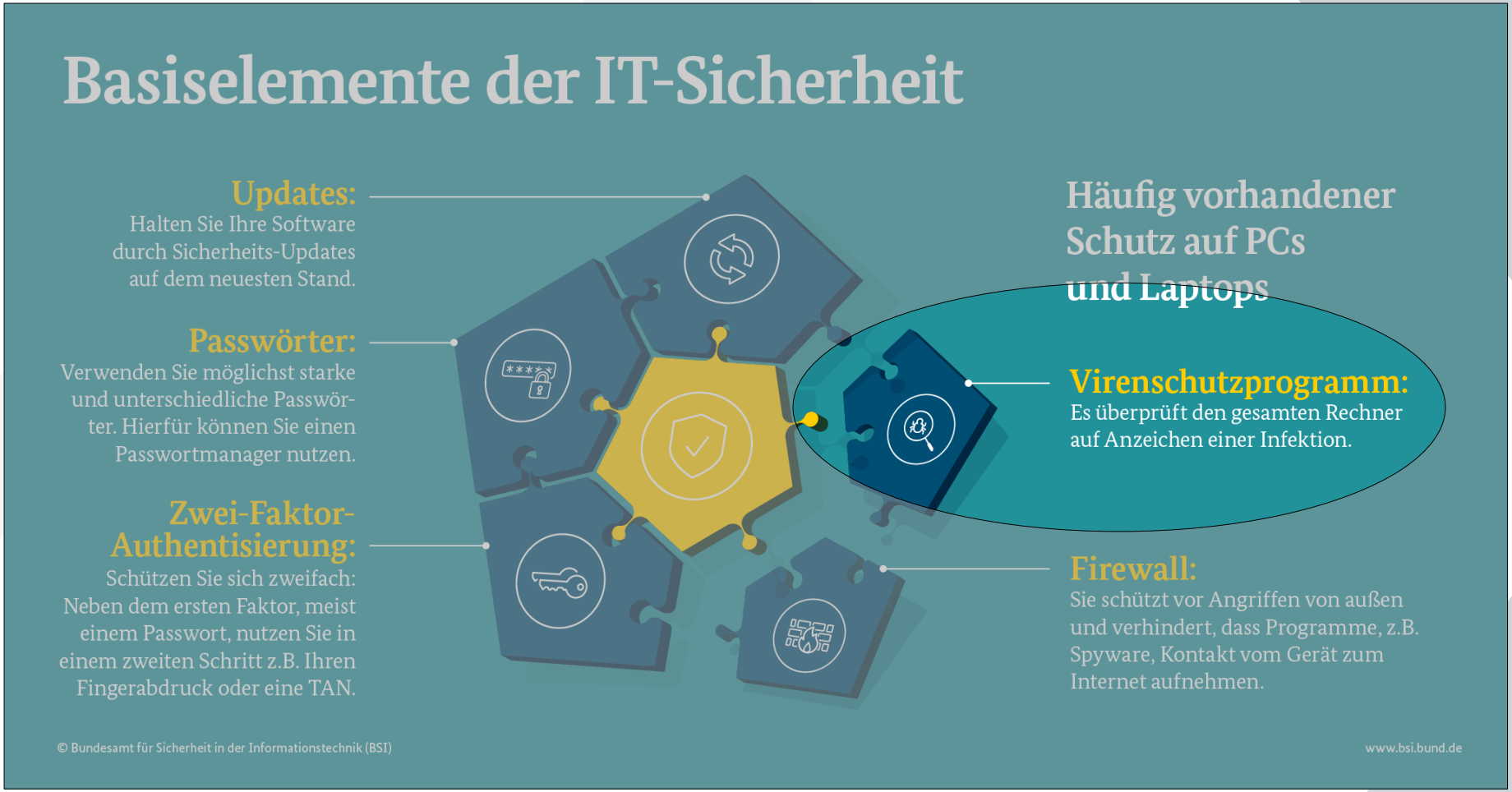
- Info zu Versionen und Updates:
  https://fritz.com/pages/update-news?product_group=FRITZ!Box
- Infos und Update über die Adresse https://fritz.box im Heimnetz
- Wenn es (ca. länger als 1 Jahr) keine Updates mehr gibt, sollte man über die Anschaffung eines neuen Routers nachdenken



und wenn es keine Updates gibt?

- Die Hersteller bieten nur für begrenzte Zeit Updates für ihre Geräte an. Beim Kauf sollte man darauf achten, wie lange noch Updates angeboten werden.
- Windows 11 kann nicht auf älteren PC’s installiert werden, und für Windows 10 gibt es maximal bis Oktober 2026 Updates.
- **Linux** läuft auf den meisten (auch älteren) Computern (PC, Mac), ist kostenlos und lässt sich leicht installieren.
  https://www.linuxguides.de/linux-fuer-einsteiger/ 
- Für Android-Geräte gibt es teilweise alternative Betriebssysteme (Custom ROM). Leider nicht ganz so leicht zu installieren.

Virenschutz



Quelle: Bundesamt für Sicherheit in der Informationstechnik

Virenschutz

- Virenschutz wird nur für Windows benötigt,
  nicht * für Linux oder Mac OS
- Der von Microsoft Windows mitgelieferte Defender reicht für den Hausgebrauch völlig aus
- Mit (neuen) Windows-PCs ausgelieferte Antivirus-Programme von Drittanbietern wie Avira oder avast können entfernt werden; dann wird automatisch der Defender aktiviert
- Wenn Sie sich für ein alternatives Antivirus-Programm entscheiden, dann nicht, weil es vom PC-Hersteller als Lockangebot mit begrenzter Laufzeit mitgeliefert wurde, sondern weil Sie sich entsprechend informiert haben, bestimmte Funktionen benötigen und sich bewusst für dieses Produkt entschieden haben
- Spätestens wenn die Testzeit abgelaufen ist, sollte man ein Abo abschließen oder die AV-Software entfernen! Ohne Updates wird das Programm wirkungslos!

*) Ausnahme: Linux oder Mac als Dateiserver im Netzwerk

Weniger ist mehr!

- Löschen Sie **nicht benötigte Apps** bzw. Programme
  - Oft werden Programme vorinstalliert, die nach einer Testphase kostenpflichtig sind. Wählen Sie selbst aus, was Sie nutzen möchten. Meist reichen kostenlose Programme vollständig aus (z. B. LibreOffice statt Microsoft Office)
- Löschen Sie nicht mehr benötigte Dateien und E-Mails
- Kündigen Sie nicht benötigte **Newsletter**
  Das ist oft nicht ganz einfach. Lesen Sie genau die Hinweise!
- Blockieren Sie Werbung (z. B. mit uBlock Origin in Firefox)
- Meiden Sie unnötige Cloud-Dienste (Datenschutz!)
- Geben Sie nicht mehr Daten preis als unbedingt erforderlich
- Löschen Sie regelmäßig Browser-Daten (Verlauf, Cache etc.) und nicht benötigte Erweiterungen

Sicherheit von E-Mails

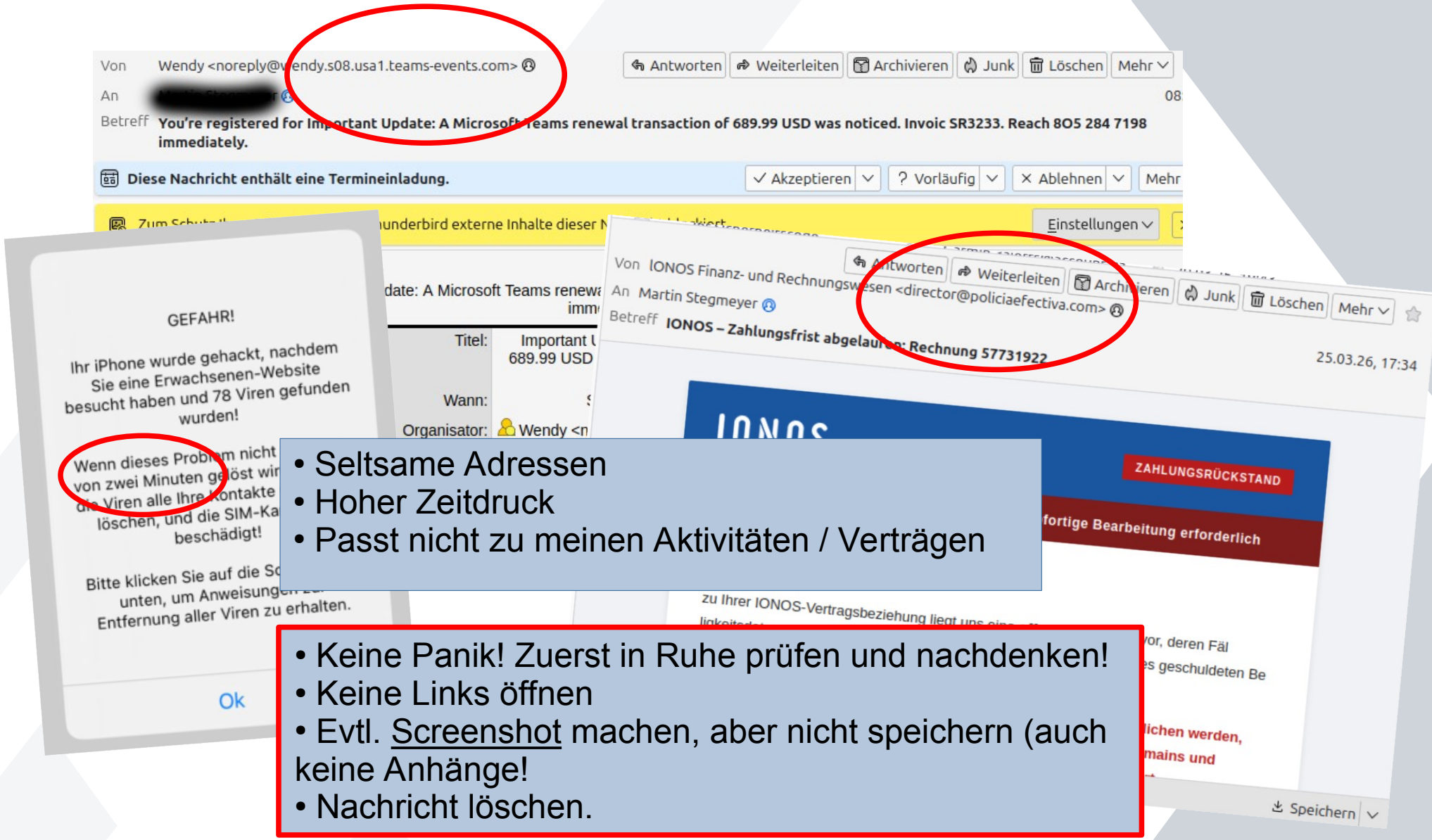
Wie können E-Mails gefährlich werden?
E-Mails werden gerne von Angreifern genutzt.
Sie können einen Anhang oder einen Link enthalten.
Öffnet man diese, wird möglicherweise ein Programm gestartet, was einen Angriff ermöglicht.

Phishing *
Sie werden auf eine Seite gelockt
Um Ihr Passwort einzugeben.
Der Angreifer kann es dann im Klartext auslesen und verwenden!

Quelle: © Can Yesil / fotolia.com und BSI

*) von „fishing“, engl. für „angeln“ und „phreaking“ für „hacken“

Erkennen von Pfishing-Nachrichten



- Seltsame Adressen
- Hoher Zeitdruck
- Passt nicht zu meinen Aktivitäten / Verträgen

- Keine Panik! Zuerst in Ruhe prüfen und nachdenken!
- Keine Links öffnen
- Evtl. Screenshot machen, aber nicht speichern (auch keine Anhänge!
- Nachricht löschen.

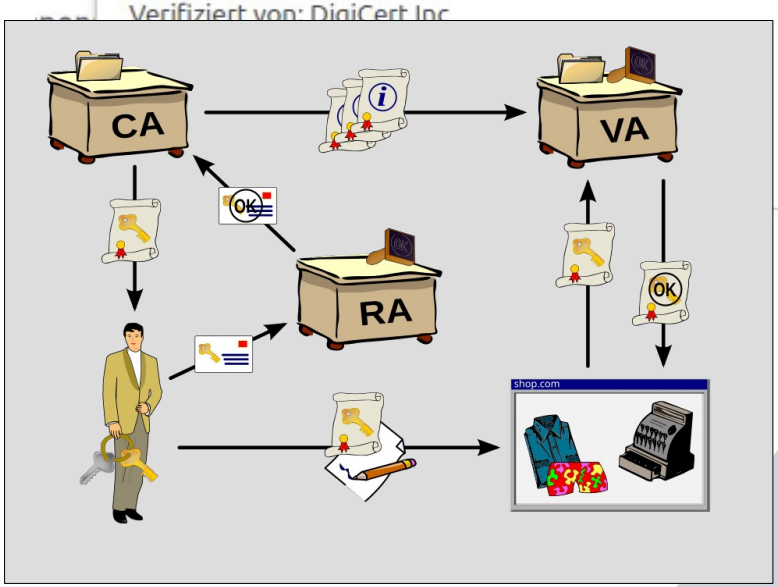
Quishing

- Ein QR-Code wird mit einem anderen Code überklebt
- Statt aus die Seite eines seriösen Anbieters gelangen Sie auf eine gefälschte Seite von Kriminellen
- Vorsicht bei der Eingabe von persönlichen Daten!
  - Android-App
    QR & Barcode Scanner
    zeigt Adresse vor dem Öffnen!

Infos der Polizeigewerkschaft

Verschlüsselung

- Daten werden bei der Übertragung zum Internet heute meistens verschlüsselt.
- Achten Sie im Browser auf das Symbol in der Adresszeile!
- E-Mails werden zwischen Sender und Empfänger **nicht** lückenlos verschlüsselt!
- Nachrichten bei Signal und Whatsapp werden bei Gruppenchats **nicht** verschlüsselt.
- Festplatten sollten bei mobilen Computern verschlüsselt werden *



*) Geräteverschlüsselung / Bitlocker bei Windows, FileVault bei Mac, LUKS bei Linux

Quelle: Wikipedia

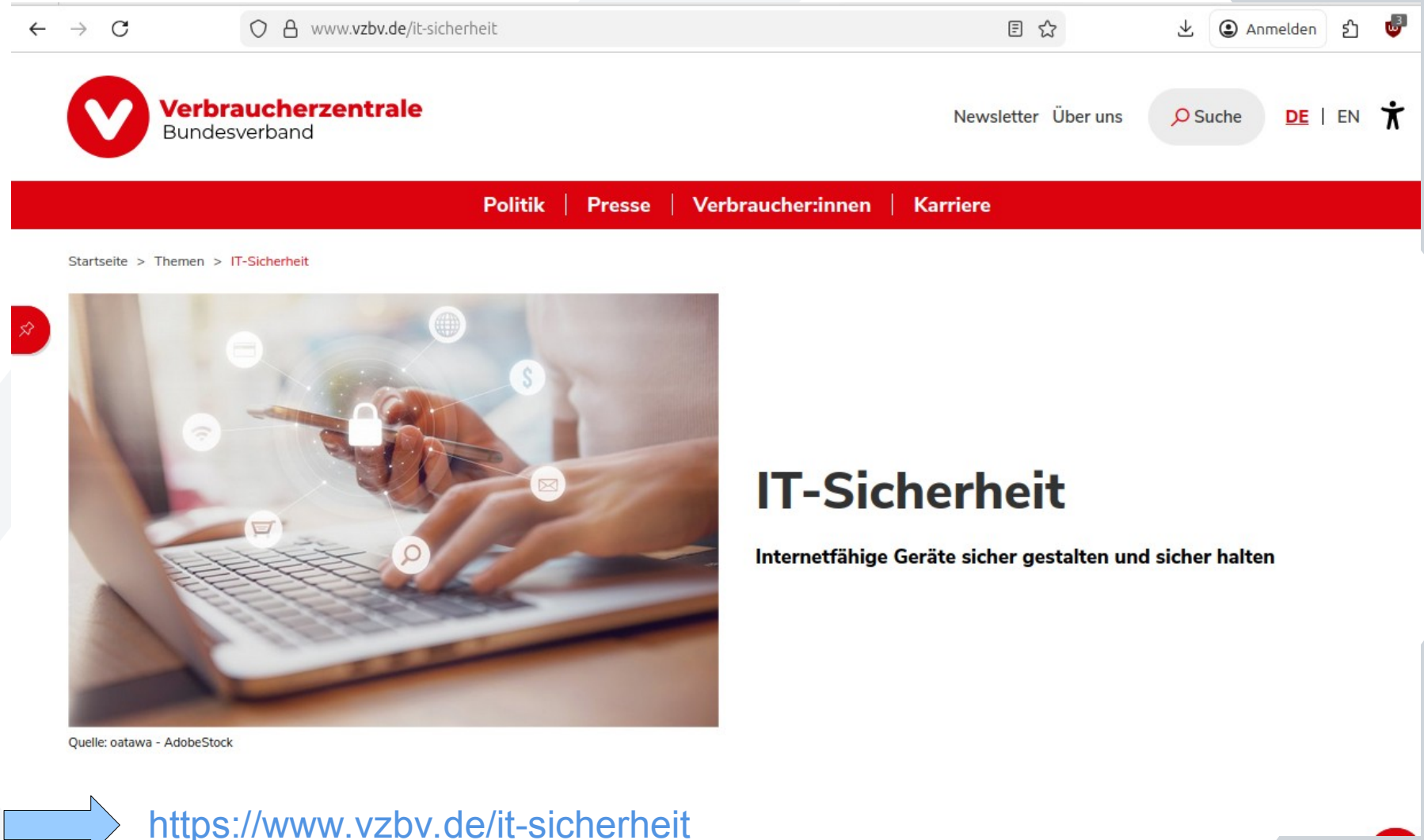
Datensicherung / Backup

- Daten sollten regelmäßig gesichert werden!
- Datenträger oder ganze Computer können beschädigt werden oder verloren gehen
- **Windows: -** Wiederherstellungslaufwerk erstellen
  - Ashampoo Backup
- **Mac OS:** Time Machine
- **Linux:** Time Shift
- **Alle:** Duplicati (nur Daten, nicht das System)

Wo kann ich mich informieren?

- Verbraucherzentrale
- VHS-Kurse
- Bundesamt für Sicherheit in der Informationstechnik
- Sicherheits-Tipps von Banken oder in der Tagespresse
- Computer-Zeitschriften (auch online), z. B. https://heise.de
- Kommen Sie zum Digitalen Donnerstag
- https://www.quarks.de/technik/digitalisierung/

Verbraucherzentrale



https://www.vzbv.de/it-sicherheit

BSI für Büger

Unsere Top-Themen

Aktuelle Themen und Vorfälle

Tipps für den digitalen Alltag

Kooperationen und Forschung

Basistipps – digitale Fenster und Türen absichern

Sichere Passwörter sind das A und O

Online Banking, Online Shopping & mobil bezahlen

Wurde mein E-Mail-Konto gehackt? Hilfe für Betroffene

Sicherheit bei E-Mail, Social Media und Co.

Gaming – Spielregeln für digitale Sicherheit

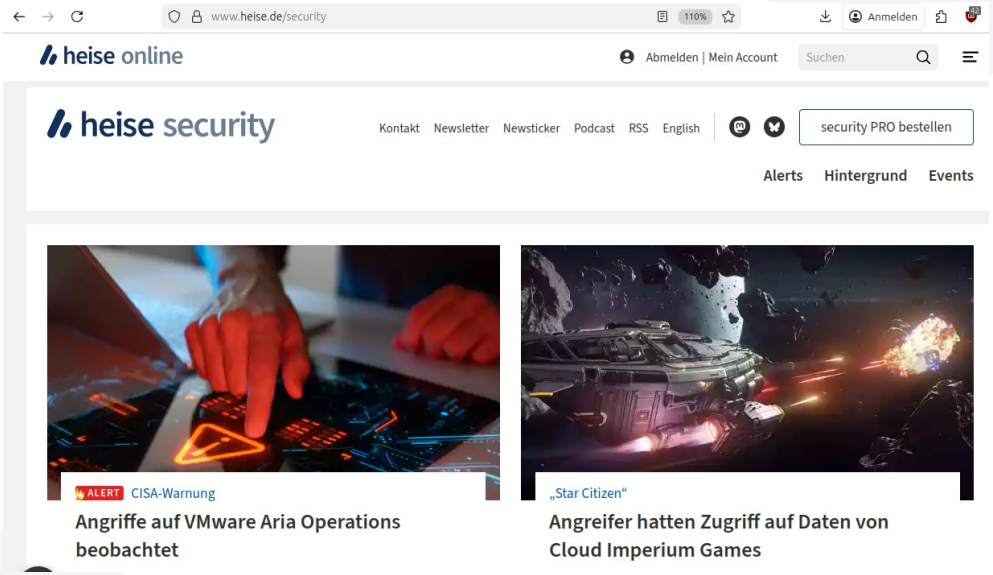
Malbuch, Checklisten & Broschüren

Videos & Podcast in der Mediathek

Quelle: Bundesamt für Sicherheit in der Informationstechnik

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html

Heise Security, c’t



https://www.heise.de/security

Download: http://ct.de/ygzw