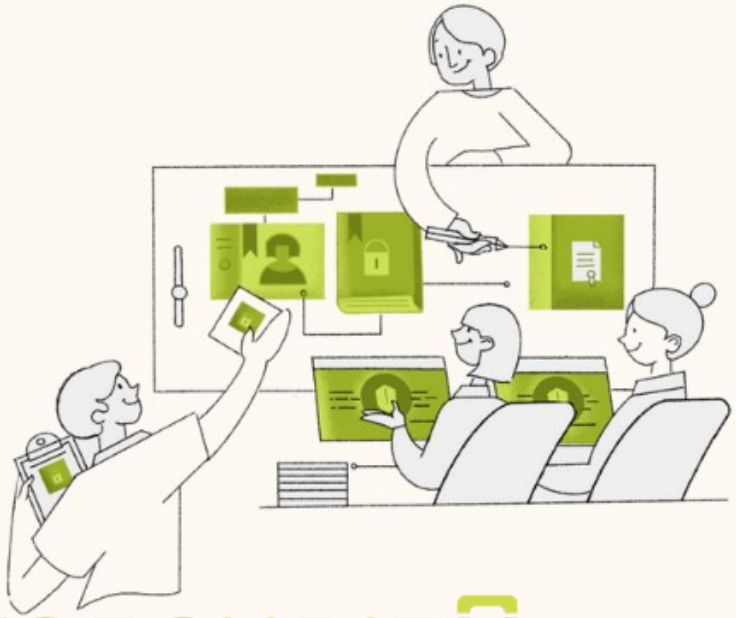
Barbinger Perspektiven 1

Daten, Viren, Spam

Zehn Tipps für ein sicheres Internet

22. Mai 2025, 19 Uhr, Bücherei Barbing, 1. OG, Referent: Matthias Kampmann







ITSECURITY

www.it-sicherheitscluster.de

Übersicht



01 Abdichten

02 Sichern

03 Verschlüsseln

04 Vernetzen

05 Bereinigen

Übersicht



06 Updaten

07 Brausen

08 Privatisieren

09 Lernen

10 Reagieren

TOP 1 – Abdichten

- Passwörter, min. 20 Stellen, Beispiel:
  u[J<L-$kä\qWjh3*2cHr
- Passwörter niemals recyceln!
- Passwortmanager benutzen oder besser gleich neuere Technologien wie Passkeys einsetzen.
- Mehrfaktorauthentisierung: Ubikey/Nitrokey etc., bedingt Windows Hello.
- *Für Unternehmer:innen: Wie hoch ist mein Schutzbedarf? Kenne ich die Risiken? Was kostet ein Ausfall?*

TOP 2 – Sichern

- Regelmäßige Backups fahren.
- Bei Cloud-Backups auf Ausstiegsregelungen und -möglichkeiten achten (Vendor Lock-in-Effekte vermeiden). Wenn man sich an einen Anbieter wechselt, steigt das Risiko von Datenverlusten, etwa wenn der Unternehmer Ihre Systeme nicht mehr unterstützt.
- Backups immer auf externe HD. Ideal ist das 3-2-1-Prinzip: drei Backups auf zwei verschiedenen Medien, eins davon nicht am Ort der anderen.
- Externe Festplatten *nicht* an der Maschine *dauerhaft* gemountet lassen, sondern nur für die Zeit, die das Backup geschrieben wird.
- Rückspielen des Backups regelmäßig üben!
- Festplatten verschlüsseln.

TOP 3 – Verschlüsseln

- S/MIME: Es gibt Anbieter kostenloser Zertifikate.
- Vielleicht lohnt es sich, über die eID und eIDAS nachzudenken (qualifizierte digitale Signatur).
- Motivieren Sie Freund:innen und Verwandte.
- Am Telefon: Nutzen Sie unabhängige Messenger, etwa Signal oder Threema, die transparent entwickelt werden.
- Zapfen Sie Ihre Ressourcen vor Ort an (z. B. in Regensburg die Binary Kitchen e. V.).
- Nutzen Sie freie Tools, etwa GnuPG. Stichwort Kryptoparty!

TOP 4 – Vernetzen

- WLAN: Ändern Sie den SSID. Ändern Sie die Default-Passwörter (s. Top 1).
- Verstecken Sie Ihr Netzwerk gegebenenfalls.
- Segmentieren Sie. Legen Sie ein Gäste-WLAN an.
- Verstehen Sie ihre Hardware. Was läuft auf Ihrem Router? Beenden Sie alle Dienste, die Sie nicht nutzen (NetBIOS/WINS).
- Schließen Sie alle nicht genutzten Ports.
- Firewalling: Vermeiden Sie Standardregeln und passen Sie alle auf Ihre Netzwerke und Arbeitsweisen an.
- Auch auf Ihren Laptops und/oder PC.

TOP 5 – Bereinigen

- Alles, was Sie nicht brauchen, kann weg: digital nachhaltig denken.
- Beherzigen Sie immer die DSGVO-Regeln zur Datensparsamkeit in alle Richtung nicht nur bei der Datenerhebung.
- Jede überflüssige Software macht Arbeit. Im Zweifel sollte sie gelöscht werden.
- Schließen Sie nicht mehr genutzte Accounts. Je weniger Sie betreiben, umso weniger Angriffsfläche gibt es für Identitätsdiebstahl. Und Sie haben weniger Arbeit.
- Nutzen Sie zumindest die Bordmittel zur Säuberung und Untersuchung. Regelmäßig!
- Caches leeren! Cookies löschen! Browserverläufe löschen!

TOP 6 – Updaten

- Updaten Sie regelmäßig.
- Upgraden Sie regelmäßig.
- Weniger ist mehr: Je weniger Software, umso weniger Arbeit haben Sie damit.
- Wenn Sie keinerlei spezielle Software benutzen müssen, denken Sie über alternative Betriebssysteme (Linux, FreeBSD etc.) nach, die in der Regel weniger anfällig sind und schnellere Patches/Updates bekommen als proprietäre OS (Achtung: persönliche Erfahrung/Meinung).

TOP 7 – Anwendungen

- Wechseln Sie zu sicheren Browsern (z. B. Brave, Vivaldi).
- Minimieren Sie die Anzahl der Plugins/Addons.
- Nutzen Sie sichere DNS (z. B. Quad9, *9.9.9.9*).
- Stellen Sie Ihren Browser auf stumm. Die meisten Programme sind enorm geschwätzig.
- Speichern Sie keine Passwörter (nutzen Sie Passwortmanager, etwa Bitwarden).
- Blockieren Sie Inhalte, die Sie nicht brauchen.
- Bestimmen Sie, wann was spielt: Click-to-play! Es ist Ihre Wahl, nicht die der Anbieter!

TOP 8 – Privatisieren

- Nutzen Sie Privacy-Tools und entsprechende Einstellungen. Verhindern Sie Tracking durch robuste Einstellungen in Browsern.
- Vermeiden Sie es, auf jeden Reiz zu reagieren. Lassen Sie Ihre Schutzbefohlenen geschützt (keine Kinderbilder offen in Social Media)!
- Vermeiden Sie Teilnahmen an Preisausschreiben.
- Erkennen Sie, wo die Klick-Trigger bei Ihnen sind. Sprechen Sie mit Ihren Familienmitgliedern: Auf was reagiere ich sofort? Ist das eine, meine Schwachstelle? **Erst denken, dann klicken ;-)**
- Verschlüsseln.
- Enkeltricks und andere Formen des Betrugs lauern überall (Fachjargon: Social Engineering)
- Obacht bei supergünstigen Angeboten!
- Online-Banking nur daheim, nie in öffentlich WLANs.

TOP 9 – Lernen

- Nutzen Sie die Angebote zum Erkennen von Schadsoftware (Phishing)
- Wie ist ein Link aufgebaut? Woran erkenne ich «böse» E-Mails?
- On-mouse-over before click! Was sagt der Link mir? Was ist die TLD, wie erkenne ich Betrugsversuche?
- Lernen Sie, wie man Phishing*-E-Mails erkennt. (**P**assword **H**arvesting+F**ishing**)
- *In Firmen: Machen Sie Informationssicherheit zum Thema in Ihrer Organisation: Pflegen Sie Offenheit und Transparenz! Aus Fehlern lernt man. Scham hilft keinem weiter.*
- Gewöhnen Sie sich sichere Verhaltensweise an! Bildschirmsperren (Windowstaste+l) mit Kennwörtern sichern.
- Accountsharing ist verboten und gefährlich.
- Lernen Sie, NICHT auf Reize zu reagieren.

TOP 10 – Erkennen, Reagieren

- Mein Rechner rackert sich ab, obwohl ich noch gar kein Programm geöffnet habe. Routine oder Vorfall?
- Wenn etwas passiert ist, was muss getan werden?
- Rechner vom Netzwerk nehmen? Ausschalten?
- Sind Daten abgeflossen? Wessen Daten, wenn?
- Weiß ich, wen ich in welchem Fall zu benachrichtigen habe? Soll ich Anzeige erstatten?
- Habe ich einen Notfallplan?

Und was hindert uns daran,

diese und weitere Ratschläge zu beherzigen?

- Mangelndes Bewusstsein: Viele Menschen unterschätzen die Bedeutung der Informationssicherheit, was zu einem Mangel an Bewusstsein und Vernachlässigung von notwendigen Schutzmaßnahmen führt.
- Ressourcenbeschränkungen: Begrenzte Zeit und Mittel können die Umsetzung robuster Sicherheitsmaßnahmen, etwa Firewalls oder gute, solide Backup-Technik, verhindern.
- Unkenntnis: Oftmals wird unbeabsichtigt die Sicherheit durch Aktionen wie das Anklicken von Phishing-E-Mails oder die Verwendung schwacher Passwörter gefährdet. Unkenntnis, Unerfahrenheit und Fahrlässigkeit führen zum Versagen. Das bleibt eine große Herausforderung.
- Technologische Komplexität: So wie sich die Technologie weiterentwickelt, so entwickeln sich auch die Sicherheitsbedrohungen. Mit der sich ständig verändernden Landschaft der Cybersicherheit Schritt zu halten, ist eine ständige Herausforderung.
- Compliance und Regulierung: Die Einhaltung von Datenschutzgesetzen und -vorschriften kann komplex und ressourcenintensiv sein und ist für Bürger:innen bisweilen eine unüberwindliche Hürde.

Was hindert uns noch?

- Ausgefeilte Bedrohungen: Cyberkriminelle werden immer raffinierter und erschweren es, sich gegen Bedrohungen wie Zero-Day-Exploits (=bislang unentdeckte Sicherheitslücken in Software) und gezielte Angriffe zu schützen.
- Wir kennen die Risiken nicht: Internetkauderwelsch von Tekkies versteht niemand. Dennoch muss man sich damit ein wenig auseinandersetzen, um zu verstehen, dass man lieber vorsichtig sein sollte.
- Balance zwischen Sicherheit und Benutzerfreundlichkeit: Das richtige Gleichgewicht zwischen robusten Sicherheitsmaßnahmen und Benutzerfreundlichkeit muss gefunden werden – angemessen und verhältnismäßig. Aber man sollte nicht auf jeden Werbegag hereinfallen: Was bringen einem computergesteuerte LED-Lampen, wenn sie im WLAN hängen, aber niemals Updates bekommen und für Botnetze missbraucht werden können?
- Böswillige oder fahrlässige Handlungen können ein erhebliches Sicherheitsrisiko darstellen.
- Veraltete Systeme: Älteren Technologien und Systemen kann es an eingebauten Sicherheitsmerkmalen fehlen, was sie anfällig für Angriffe macht.
- Es ist, ja, so ist es, einfach immer viel zu viel Information. Es ist zu viel Arbeit, alle Geräte immer im Blick zu haben. Man muss ja nicht jede Version dokumentieren. Aber je weniger Soft- und Hardware Sie nutzen, umso leichter behalten Sie den Überblick. Wenn aber jeder Personenwaage im Netz hängt, jeder Kühlschrank nach China funkt, braucht man sich nicht zu wundern, dass wir angreifbar werden.

Fazit

Um Hindernisse zu überwinden, muss man sie erkennen können. Vorausschauend sollte man sich, selbst wenn es langweilig ist, damit beschäftigen. Wir brauchen daher mehr Bildung und Investitionen in eine starke Sicherheitskultur, die alle Lebensbereiche umfasst, weil Computer überall sind. Seien und bleiben Sie skeptisch!

Diese Top Ten kann immer nur *ein* Ausgangspunkt sein.

Weiterführende Links

- Allgemeine Anlaufstelle ist das Bundesamt für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de/DE/Home/home_node.html
- Tipps vom BSI: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweiser_Checklisten_Flyer/Brosch_A6_Surfen_aber_sicher.pdf?__blob=publicationFile&v=11

  (von 2021, aber immer noch weitgehend hilfreich und in Deckung mit dem hier Gesagten).
- Bürger:innenhilfe (NRW): https://www.cybersicherheit.nrw/de/buergerinnen-und-buerger
- Initiative Deutschland sicher im Netz: https://www.sicher-im-netz.de/
- Tipps von der Polizei in Niedersachsen: https://www.polizei-praevention.de/themen-und-tipps/links/internetsicherheit
- Anlaufstelle in Bayern: https://www.polizei.bayern.de/kriminalitaet/internetkriminalitaet/002464/index.html
- Lagebericht Bayern zur Cybersicherheit 2024: https://www.stmi.bayern.de/news/detail/bericht-zur-cybersicherheit-in-bayern-2024/

ARTIFICIAL INTELLIGENCE REGENSBURG

Erasmus+

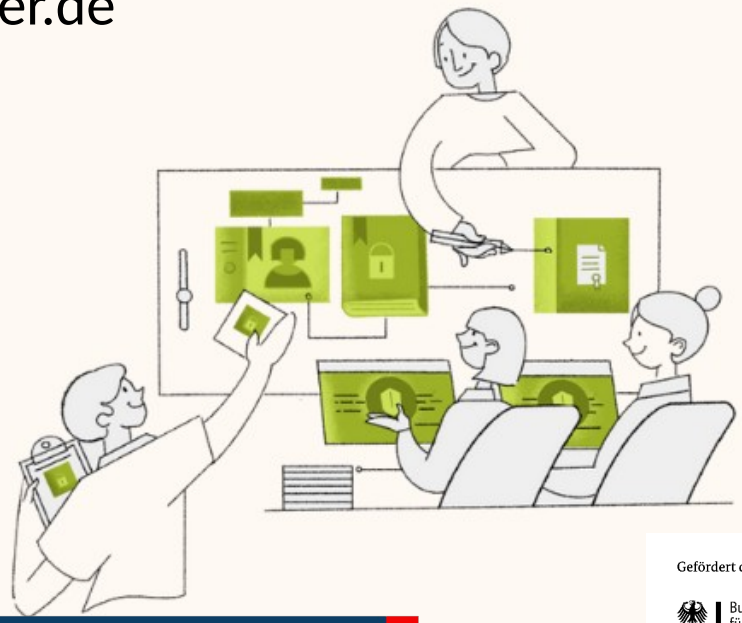
European DIGITAL SME Alliance

Bundesverband IT-Mittelstand e.V.

Vielen Dank für Ihre Aufmerksamkeit

IT-Sicherheitscluster e. V.
Dr. Matthias Kampmann
matthias.kampmann@it-sicherheitscluster.de
privat: matthias.kampmann@gruene-barbing.de
https://www.it-sicherheitscluster.de







Allianz für Cyber-Sicherheit

CYBERsicher

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Bundesministerium für Bildung und Forschung