Tipps und Hinweise für mehr IT-Sicherheit

Ein einfacher IT-Sicherheitsleitfaden des Caritas-Netzwerk IT e.V.

Veranstaltung: Wohlfahrt Digital 7

Datum: 19.11.2025

Kommen Sie gerne auf uns zu! Kontaktdaten zum Caritas-Netzwerk IT e. V.:

Mirco Beyer
Referent für Kooperationsentwicklung
E-Mail: mirco.beyer@caritas-netzwerk-it.de
Tel.: +49-155 - 661 75294

Gerhard Müller
Geschäftsführer
E-Mail: gerhard.mueller@caritas-netzwerk-it.de
Tel.: +49-179 - 133 8060

Webseite: https://caritas-netzwerk-it.de

Inhalt:

5 Basisschritte zu mehr Sicherheit,

die Sie sofort umsetzen können!

Hier sind fünf einfache, aber extrem wirksame Maßnahmen, mit denen Sie Ihre persönliche digitale Sicherheit ab sofort deutlich erhöhen können.

1. Starke Passwörter und ein Passwort-Manager

Ein starkes Passwort ist die erste und wichtigste Verteidigungslinie. Da man sich Dutzende einzigartige Passwörter nicht merken kann, ist ein Passwort-Manager die Lösung.

Was zu tun ist:

- Verwenden Sie für jeden Online-Dienst ein **einzigartiges und langes Passwort** (mindestens 12 Zeichen, Mix aus Groß-, Kleinbuchstaben, Zahlen und Symbolen).
- Installieren Sie einen **Passwort-Manager**, der sichere Passwörter für Sie erstellt, speichert und automatisch ausfüllt. Sie müssen sich dann nur noch ein einziges, sehr starkes Master-Passwort merken.

Tipp & Weiterführende Infos:

Tool-Tipp: Bekannte und geprüfte Passwort-Manager sind z.B. **1Password** oder **KeePassXC**.

Weiterführende Informationen finden Sie hier: BSI-Tipps zu Passwörtern

2. Multi-Faktor-Authentifizierung (MFA) aktivieren

Selbst wenn jemand Ihr Passwort stiehlt, schützt die MFA Ihren Account, da eine zweite Bestätigung zumindest auf einem anderen Gerät (meist Ihr Smartphone) erforderlich ist.

Was zu tun ist:

- Aktivieren Sie MFA (auch 2FA genannt) für Ihre wichtigsten Konten wie E-Mail, Online-Banking, Social Media, Cloud-Speicher & Co.
- Nutzen Sie am besten eine **Authenticator-App** (z.B. Google Authenticator, Microsoft Authenticator) statt einer SMS, da Apps als sicherer gelten.

Tipp & Weiterführende Infos:

Tipp: Nehmen Sie sich 15 Minuten Zeit und gehen Sie die Einstellungen Ihrer drei wichtigsten Online-Dienste durch. Suchen Sie nach "Sicherheit" oder "Login" und aktivieren Sie MFA.

Weiterführende Informationen finden Sie hier: BSI-Tipps zur Zwei-Faktor-Authentisierung

3. Software und Apps aktuell halten (Updates installieren!)

Cyberkriminelle nutzen oft bekannte Sicherheitslücken in veralteter Software aus, um sich Zugang zu Systemen zu verschaffen. Updates schließen diese Lücken.

Was zu tun ist:

- Aktivieren Sie **automatische Updates** für Ihr Betriebssystem (Windows, macOS, Android, iOS), Ihren Webbrowser und andere wichtige Programme.
- Wenn Sie eine Benachrichtigung über ein verfügbares Update erhalten, installieren Sie es zeitnah.

Tipp & Quelle:

Tipp: Überprüfen Sie noch heute auf Ihrem Computer und Smartphone die Einstellungen für automatische Updates. Meist ist das nur ein einziger Klick, der Sie dauerhaft sicherer macht.

Weiterführende Informationen finden Sie hier: BSI zu Updates/Patches

4. Regelmäßige Backups erstellen

Ein Backup ist Ihre Versicherung gegen Datenverlust – sei es durch einen Festplattenschaden, Diebstahl oder einen Ransomware-Angriff, der Ihre Daten verschlüsselt.

Was zu tun ist:

- Sichern Sie Ihre wichtigen Daten (Dokumente, Fotos) regelmäßig auf einem externen Medium (z.B. externe Festplatte) oder in einem Cloud-Speicher.
- Stellen Sie sicher, dass mindestens eine Kopie Ihrer wichtigsten Daten an einem anderen Ort aufbewahrt wird.

Tipp & Quelle:

Tipp: Nutzen Sie bspw. die eingebauten Funktionen Ihres Betriebssystems wie **Time Machine (macOS)** oder **Dateiversionsverlauf (Windows)**. Diese können automatisch Backups erstellen.

Hinweis: Ein gutes Backup ist von Ihrem Computer getrennt, nachdem es erstellt wurde, damit Ransomware nicht auch die Sicherung verschlüsseln kann.

5. Vorsicht bei E-Mails und Links: Erst prüfen, dann klicken!

Phishing-Mails sind nach wie vor das Haupteinfallstor für Angriffe. Betrüger versuchen, Sie dazu zu bringen, auf bösartige Links zu klicken oder schädliche Anhänge zu öffnen.

Was zu tun ist:

- **Prüfen Sie den Absender:** Klicken Sie auf den Namen, um die tatsächliche E-Mail-Adresse zu sehen. Passt sie zum angeblichen Absender?
- **Fahren Sie mit der Maus über Links** (ohne zu klicken!), um die echte Zieladresse zu sehen.
- Seien Sie misstrauisch bei E-Mails, die **dringenden Handlungsbedarf** fordern, seltsame Anhänge enthalten oder Rechtschreibfehler aufweisen.

Tipp: Im Zweifel gilt: Löschen Sie die E-Mail und rufen Sie die Webseite des Anbieters (z.B. Ihrer Bank) manuell im Browser auf oder kontaktieren Sie den Absender auf einem bekannten Weg.

Das BSI bietet exzellente und anschauliche Informationen zum Erkennen von Phishing-Mails: BSI Phishing

Das 10-Schritte-Programm für mehr IT-Sicherheit in Ihrer Organisation

Um von der reinen Bewusstseinsbildung zur konkreten Umsetzung innerhalb von Organisationen der Freien Wohlfahrtspflege zu gelangen, folgt ein bewährtes 10-Schritte-Programm. Es basiert auf den Empfehlungen von Gerhard Müller (Caritas-Netzwerk IT e. V.) und bricht das komplexe Thema Cybersicherheit in handhabbare Aufgaben herunter. Nutzen Sie die folgenden Punkte als direkten Leitfaden, um die Sicherheit in Ihrer Organisation systematisch zu verbessern. Das 10-Schritte-Programm gibt es zusätzlich als YouTube-Video. Den Link dazu finden Sie in der Material- und Linksammlung.

Schritt 1 – IT-Sicherheit ist Chefsache

- **Das Prinzip:** Sicherheit ist eine Führungsaufgabe. Sie definieren die Strategie und stellen Ressourcen bereit.
- **Ihre Aufgabe als GF/Vorstand:** Geben Sie Budgets frei und definieren Sie klare Verantwortlichkeiten, zum Beispiel durch die Benennung eines Informationssicherheitsbeauftragten (ISB).
- **Ihre Aufgabe als IT-Leitung:** Übersetzen Sie Risiken für die Geschäftsführung verständlich.

Schritt 2 – Lagebild: Die eigenen Kronjuwelen kennen

- **Das Prinzip:** Sie müssen wissen, was Ihre schützenswertesten Daten und Prozesse sind, da Sie nicht alles gleich gut schützen können (z.B. Klientendaten, Abrechnung).
- **Handlungsoption:** Führen Sie eine einfache Risikoanalyse durch. Stellen Sie sich die Frage: „Wo tut ein längerer Ausfall am meisten weh?“

Schritt 3 – Datensicherung: Die Lebensversicherung

- **Das Prinzip:** Regelmäßige und getestete Backups sind nicht verhandelbar. Ein Backup, das nie getestet wurde, ist keine Sicherheit, sondern eine Hoffnung.
- **Handlungsoption:**
    - Befolgen Sie die **3-2-1-Regel:** Halten Sie **3** Kopien auf **2** verschiedenen Medien, wovon **1** Kopie extern (offline) ist.
    - Überprüfen Sie Ihr Backup-Konzept mit der Frage: „Wann haben Sie das letzte Mal erfolgreich eine komplette Wiederherstellung getestet?“

Schritt 4 – Notfallplan & Cyber-Feuerwehr: Vorbereitet sein für den Tag „X“

- **Das Prinzip:** Vorbereitung auf den Notfall verhindert das Schlimmste. Ohne Vertrag warten Sie im Krisenfall sonst bis zu sieben Wochen auf einen Spezialisten.
- **Handlungsoption:** Erstellen Sie einen Notfall- und Wiederherstellungsplan. Schließen Sie **jetzt** einen Vertrag mit einem spezialisierten DFIR-Dienstleister (Cyber-Feuerwehr) ab. Definieren Sie ein kleines Kern-Team, das sich wöchentlich 2 Stunden damit befasst.

Schritt 5 – Der Mensch als Schutzschild: Awareness schaffen

- **Das Prinzip:** Der Mensch ist der größte Hebel und die größte Schwachstelle zugleich. Da zukünftige KI-gestützte Phishing-Angriffe perfektioniert sein werden, wird das menschliche Gespür für „merkwürdige“ Anfragen entscheidend sein.
- **Handlungsoption:** Führen Sie regelmäßige, einfache Schulungen durch (z.B. Phishing erkennen, sichere Passwörter).

Schritt 6 – Basishygiene: Das digitale Fundament härten

- **Das Prinzip:** Es gibt eine digitale Grundhygiene, die aus den „Big Four“ der Prävention besteht und nicht verhandelbar ist.
- **Die „Big Four“ sind:**
    1. **Updates einspielen („Patch-Management“):** Sicherheitslücken schnell schließen.
    2. **Multi-Faktor-Authentifizierung (MFA):** Zugänge absichern.
    3. **Passwort-Manager:** Nur so kann man sich gute, pro Dienst unterschiedliche Passwörter merken.
    4. **Professionelle Schutzsysteme:** Ohne geht es gar nicht mehr.

Schritt 7 – Lieferanten im Blick: Perfekte Phishing-Quellen & Co.

- **Das Prinzip:** Angriffe erfolgen oft über Ihre Dienstleister. Die Kette ist nur so stark wie ihr schwächstes Glied.
- **Handlungsoption:** Fordern Sie von Ihren wichtigsten Partnern Nachweise zur IT-Sicherheit. Machen Sie Sicherheit zu einem Auswahlkriterium.

Schritt 8 – Standards als Leitplanken: NIS-2 & BSI-Grundschutz & Co. nutzen

- **Das Prinzip:** Diese Standards sind kein bürokratisches Monster, sondern ein exzellenter Baukasten für den systematischen Aufbau von Sicherheit.
- **Ihre Option:** Nutzen Sie diese Standards als Fahrplan. Sie müssen das Rad nicht neu erfinden.

Schritt 9 – Effizienz durch Technologie & Dienstleister

- **Das Prinzip:** Wenn Sie nicht genug qualifiziertes Personal haben, lassen Sie die Technik und Dienstleister für sich arbeiten.
- **Handlungsoptionen:**
    - **Managed Services:** Sicherheit als Dienstleistung einkaufen (z.B. Managed Firewall, SOC as a Service).
    - **KI in der Abwehr:** Moderne Schutzlösungen erkennen Angriffe automatisiert.
    - **Penetrationstests:** Lassen Sie Experten Ihr System von außen auf Schwachstellen überprüfen.

Schritt 10 – Sicherheit als Prozess verstehen: Am Ball bleiben

- **Das Prinzip:** Sicherheit ist kein einmaliges Projekt. Angreifer, Software und Bedrohungen entwickeln sich ständig weiter.
- **Handlungsoption:** Planen Sie einen festen Termin (z.B. quartalsweise) für ein „Sicherheits-Update“ in der Führungsebene. Bleiben Sie neugierig auf neue Technologien und Bedrohungen.

Material- & Linksammlung zum Thema

YouTube-Videos zu weiteren IT-Sicherheits-Vorträgen des Caritas-Netzwerk IT e. V.:

- Der 10-Schritteprogramm zur Cybersicherheit: https://youtu.be/FpYwNfJutrg?si=sUMAqOemkX3M1ode
- Cyberangriffe unwahrscheinlicher machen & den Ernstfall überleben https://youtu.be/zBDL-ni5KYM?si=6LNbIQGdqkqmrZee
- NIS-2: Neue Anforderungen an Cybersicherheit- auch für die Caritas relevant? https://youtu.be/PRfCgZstNws?si=fnBhVGz565i_oOeo

Bonus:

- Chancen und Notwendigkeit der Digitalisierung in der Wohlfahrtspflege https://youtu.be/uo_TgzlcgBo?si=UsR81_4DQl_xBeeX

Links:

- Die Lage der IT-Sicherheit in Deutschland 2025 – Bundesamt für Sicherheit in der Informationstechnik (BSI) https://medien.bsi.bund.de/lagebericht/de/index.html
- Management von Cyberrisiken – Allianz für Cybersicherheit https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/Management-Handbuch/management-handbuch_node.html
- Wirtschaftsschutzstudie – Bitkom https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz
- Leseempfehlung: Buch „Deutschland im Ernstfall“ von Ferdinand Gehringer und Johannes Steger: https://hoffmann-und-campe.de/products/83277-deutschland-im-ernstfall