# Herzlich willkommen zum Schulungsleitfaden für **PAUL** - Ihrer praxisnahen Awareness- und IT-Sicherheitsschulung für Lernende im öffentlichen Dienst!

Dieser Leitfaden soll Ihnen als Schulungsleiter helfen, eine effektive und zielgerichtete Präsenzschulung zu gestalten. Ziel ist es, die Teilnehmenden für die Bedeutung von IT-Sicherheit zu sensibilisieren und ihnen das notwendige Wissen sowie die Fähigkeiten zu vermitteln, um Risiken in der digitalen Arbeitswelt aktiv zu minimieren.

In einer immer stärker digitalisierten Welt nehmen Sicherheitsbedrohungen kontinuierlich zu. Der [BSI-Lagebericht](https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html) zeigt, dass sich insbesondere für den öffentlichen Dienst die Gefahrenlage stetig verschärft. Der Umgang mit sensiblen und schützenswerten personenbezogenen Daten macht Behörden zu einem bevorzugten Ziel für Cyberangriffe. Hier spielt der Faktor Mensch eine Schlüsselrolle – sowohl als potenzielles Angriffsziel als auch als zentrale Säule im Schutz gegen derartige Bedrohungen.

Ihre Aufgabe als Schulungsleiter geht über das Vermitteln technischer Inhalte hinaus. Sie tragen dazu bei, das Bewusstsein der Teilnehmenden für sicherheitskritische Verhaltensweisen zu stärken und eine verantwortungsbewusste IT-Kultur in Ihrer Behörde zu etablieren. PAUL begleitet Sie Schritt für Schritt – von der Planung und Vorbereitung über die Durchführung bis hin zur Nachbereitung und Evaluierung der Schulung.

### **Das erwartet Sie in diesem Leitfaden:**

* **6 Module à ~20 Minuten:**
  1. Einführung in die IT-Sicherheit
  2. Sichere Passwörter und Authentifizierung
  3. Umgang mit Wechseldatenträgern
  4. Social Engineering und Manipulation
  5. Datensicherheit
  6. Reaktion auf Sicherheitsvorfälle
* **Praktische Übungen und interaktive Elemente**
* **Materialien zur Schulung**

### **Individuelle Anpassung und kreative Freiheit**

PAUL wurde im Rahmen eines Studierendenprojekts im Wintersemester 2024/25 an der Hochschule Rhein-Waal von Til Anheier, Fabian Bas, Lisa Franzke und Marcel Weber bei Prof. Dr. Ulrich Greveler mit der Stadt Kamp-Lintfort entwickelt. Die Materialien dieses Leitfadens stehen unter der [CC BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/) (Attribution – NonCommercial – ShareAlike). Das bedeutet, dass Sie die Inhalte nicht für kommerzielle Zwecke verwenden dürfen, da wir überzeugt sind, dass Awareness im Bereich IT-Sicherheit eine gemeinsame öffentliche Aufgabe ist. Die Lizenz erlaubt Ihnen maximale Flexibilität, die Materialien unverändert zu verwenden, an die spezifischen Anforderungen Ihrer Behörde anzupassen oder nach Bedarf zu erweitern, solange diese bei einer Veröffentlichung unter gleicher Lizenz veröffentlicht werden. Falls Sie auf Probleme stoßen oder Rückfragen haben, wenden Sie sich bitte an die hinterlegten Kontaktdaten des Teams. Durch diese aktive Zusammenarbeit tragen Sie dazu bei, dass Ihre Schulung nicht nur Wissen vermittelt, sondern auch langfristig die IT-Sicherheitsstandards in Ihrer Behörde stärkt.

Um eine Übersättigung durch immer gleiche Schulungsinhalte zu vermeiden, empfehlen wir, die Materialien mit der Zeit gezielt für Ihre Behörde weiterzuentwickeln. Zusätzliches Material wird in den jeweiligen Modulen verlinkt. Bitte prüfen Sie sorgfältig die Lizenzbedingungen externer Inhalte, da für diese keine Haftung übernommen werden kann.

Ihr Engagement als Schulungsleiter ist ein entscheidender Beitrag zur IT-Sicherheit und zum Schutz sensibler Daten in Ihrer Behörde. Dafür gebührt Ihnen unser Dank.

**Viel Erfolg bei der Durchführung Ihrer Schulung!**

## Modul 1: Einführung in die IT-Sicherheit

### Ziel des Moduls:

Das Modul „Einführung in die IT-Sicherheit“ hat das Ziel, den Teilnehmenden ein grundlegendes Verständnis für die Bedeutung von IT-Sicherheit zu vermitteln und zentrale Begriffe sowie Konzepte kompakt zu erläutern. Es soll verdeutlicht werden, wie stark IT-Sicherheit mit der täglichen Arbeit verknüpft ist, und gleichzeitig das Bewusstsein für die Notwendigkeit präventiver Maßnahmen geschärft werden. Dieses Modul bildet die Grundlage für alle nachfolgenden Inhalte, indem es sowohl die Risiken unzureichender Sicherheitsmaßnahmen als auch die Vorteile einer durchdachten und strategischen Herangehensweise an IT-Sicherheit aufzeigt.

### Hintergrundwissen:

**Cyber-Angriff auf den Landkreis Anhalt-Bitterfeld**

Der Cyberangriff auf den Landkreis Anhalt-Bitterfeld im Juli 2021 stellte eine erhebliche Bedrohung für die IT-Infrastruktur der Verwaltung dar und führte zu weitreichenden Störungen öffentlicher Dienste. Die Angreifer setzten eine Ransomware ein, die mehr als 400 Server verschlüsselte und den Betrieb wesentlicher Verwaltungsprozesse lahmlegte. Als Reaktion auf den Angriff rief der Landkreis am 9. Juli 2021 den Katastrophenfall aus, um die Notfallmaßnahmen zu koordinieren und die Unterstützung von externen Sicherheitsbehörden wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu sichern. Die Zusammenarbeit mit dem BSI und weiteren externen Partnern war jedoch als herausfordernd zu bewerten, da der Wiederherstellungsprozess langwierig und technisch anspruchsvoll war. Die Angreifer forderten ein Lösegeld von 500.000 US-Dollar, welches jedoch vom Landkreis abgelehnt wurde. Stattdessen entschloss sich der Landkreis, keine Zahlungen zu leisten und die Schadsoftware selbst zu bekämpfen. Trotz dieser Entscheidung führte der Angriff zu finanziellen Schäden von etwa 2,5 Millionen Euro, die durch direkte Kosten für die Wiederherstellung der Infrastruktur und indirekte Kosten durch den Ausfall von Verwaltungsdiensten und den Notbetrieb entstanden. Zu den betroffenen Bereichen zählten unter anderem Bürgerbüro-Dienste, die Bearbeitung von Anträgen sowie die Verwaltung von Sozialleistungen. Die Analyse betonte Griebsch, 2022, dass der Vorfall die Schwächen der IT-Sicherheit innerhalb öffentlicher Verwaltungen aufdeckte und eine grundlegende Neubewertung der Sicherheitsstrategien erforderlich machte. Der Landkreis hatte zwar auf eine schnelle Wiederherstellung durch externe Sicherheitsdienste gehofft, jedoch zeigte sich, dass fehlende präventive Sicherheitsvorkehrungen und eine unzureichende Resilienz gegen Cyberbedrohungen eine zügige Reaktion erschwerten. Die langfristigen Auswirkungen des Angriffs auf die Verwaltung und die Bevölkerung waren spürbar, da die Behörde mehrere Wochen benötigte, um die Systeme vollständig wiederherzustellen und den Betrieb in vollem Umfang wieder aufzunehmen. Die Entscheidung, das Lösegeld nicht zu zahlen, und die aktive Zusammenarbeit mit dem BSI zur Bekämpfung der Ransomware unterstrichen den starken Willen des Landkreises, sich nicht erpressen zu lassen. Trotz der langwierigen und ressourcenintensiven Wiederherstellung stellte der Vorfall sicher, dass der Landkreis aus den Fehlern des Angriffs lernte und künftig verstärkte Sicherheitsvorkehrungen treffen wird, um derartige Bedrohungen abzuwehren und die öffentliche Verwaltung resilienter gegenüber Cyberangriffen zu machen.

*Quellen: Griebsch, 2022, Heise Online, 2021b, Heise Online, 2021a, Heise Online, 2023b*

**Cyber-Angriff auf Südwestfalen-IT**

Ende Oktober 2023 erlebte die Südwestfalen-IT (SIT), ein wichtiger IT-Dienstleister für zahlreiche Kommunen, einen massiven Ransomware-Angriff, der zu einem der größten Vorfälle dieser Art in Deutschland wurde. Die Hackergruppe Akira, die auf gezielte Ransomware-Angriffe spezialisiert ist, nutzte eine Schwachstelle in der VPN-Software, um sich unbefugten Zugang zu den IT-Systemen der SIT zu verschaffen. Dies ermöglichte es den Angreifern, administrative Rechte zu erlangen, ihre Ransomware im gesamten Netzwerk zu verbreiten und große Teile der IT-Infrastruktur lahmzulegen.

Ein wesentlicher Faktor, der den Angriff ermöglichte, waren schwache Passwörter. Es wird angenommen, dass die Angreifer einen Brute-Force-Angriff auf unzureichend gesicherte Passwörter durchgeführt haben, was ihnen den Zugang zu mehreren Systemen und Benutzerkonten ermöglichte. Diese Schwachstelle, kombiniert mit unzureichenden Sicherheitsvorkehrungen und einem Mangel an regelmäßigen Updates, begünstigte den erfolgreichen Angriff. Der Angriff führte zu massiven Ausfällen: 1.463 Server waren betroffen, 871 Server mussten neu aufgesetzt werden, und etwa 160 Fachverfahren standen monatelang nicht zur Verfügung. Zu den betroffenen Bereichen gehörten Einwohnermeldewesen, Standesamt, Sozialwesen und Kraftfahrzeugwesen, was dazu führte, dass Bürger und Kommunen über Wochen auf zentrale Verwaltungsdienste verzichten mussten. Die betroffenen 72 Verbandsmitglieder der SIT, darunter Städte und Gemeinden, konnten ihre Dienstleistungen nur eingeschränkt oder gar nicht anbieten, was in einigen Fällen zu langen Wartezeiten und Bearbeitungsrückständen führte. Positiv zu bewerten ist, dass ein Monitoring des Darkwebs durch den IT-Sicherheitsdienstleister r-tec bisher keine Hinweise auf einen Datenabfluss ergeben hat. Erst im ersten Quartal 2024 konnten viele der betroffenen Systeme wieder in den Normalbetrieb überführt werden, doch erst seit dem 01.10.2024 läuft der Normalbetrieb. Die Auswirkungen des Angriffs sind weiterhin spürbar, da es zu großen finanziellen Schäden sowie Vertrauensverlust kam. So beendete bspw. die Stadt Witten die Zusammenarbeit mit der SIT.

*Quellen: Südwestfalen-IT, 2023b, Südwestfalen-IT, 2023a, Heise Online, 2023a, Heise Online, 2023c*

**IKT-Sicherheitsarchitektur der Stadt Berlin**

Die IKT-Sicherheitsarchitektur der Stadt Berlin stellt ein System zur zentralen und effizienten Gewährleistung der IT-Sicherheit in öffentlichen Einrichtungen dar. Sie definiert einheitliche Standards und Verfahren, etwa zur Passwortsicherheit und Verschlüsselung, um Schwachstellen zu minimieren und eine konsistente Sicherheitsstrategie zu fördern. Die Koordination zwischen verschiedenen Akteuren und das Informationssicherheitsmanagement stellen sicher, dass alle Maßnahmen miteinander abgestimmt sind. Die Verantwortung dafür liegt bei der Chief Digital Officer (CDO).

Praktische Maßnahmen beinhalten regelmäßige Sicherheitsüberprüfungen wie Penetrationstests und Audits sowie Schulungen zur Sensibilisierung der Mitarbeitenden zu Themen wie Phishing und Social Engineering. Die Netzwerksegmentierung schützt sensible Daten, während starke Zugangskontrollen wie Zwei-Faktor-Authentifizierung den Zugriff auf Systeme absichern. Durch regelmäßige Sicherheitsübungen und Schulungseinheiten wird die Reaktion auf Angriffe geübt, auch für nicht-technische Mitarbeitende. Zudem werden Daten verschlüsselt und durch regelmäßige Updates und Patches bleiben die Systeme stets sicher. Diese Architektur sorgt dafür, dass Berlin gut auf Cyberbedrohungen vorbereitet ist und im Falle eines Vorfalls schnell und effektiv reagieren kann.

*Quelle: Stadt Berlin, 2024.*

### Hinweise zur praktischen Übung:

1. **Ablauf der Übung**

* Abschreckung der Teilnehmenden durch Erläuterung bereits entstandener Cyber-Angriffe und dessen Folgen.

1. **Lerneffekt**

* Die Teilnehmenden erhalten ein Grundverständnis zur IT-Sicherheit.
* Die Teilnehmenden verstehen die Wichtigkeit, sich mit dem Thema IT-Sicherheit zu befassen.

### Verfügbares Material:

1. Foliensatz
2. **aktuelle** Beispiele für kommunale IT-Notfälle sind regelmäßig auf [Kommunaler Notbetrieb](https://kommunaler-notbetrieb.de/) zu finden und können ggf. in Schulung eingebaut werden

## 

## Modul 2: Sichere Passwörter und Authentifizierung

### Ziel des Moduls:

Den Teilnehmenden sollen die Grundlagen der sicheren Passworterstellung praktisch vermittelt werden. Außerdem werden die Verwendung von Passwort-Managern und Multi-Faktor-Authentisierung (MFA) kurz vorgestellt.

### Hintergrundwissen:

Unsichere Passwörter sind einer der häufigsten Angriffsvektoren auf IT-Systeme: 30% der Nutzer:innen haben bereits Datendiebstählen wegen unsicheren Passwörtern erlebt, trotzdem verwenden 46% das gleiche Passwort mehrfach und 63% ändern ihr Passwort nur, wenn sie dazu aufgefordert werden (Sebastian, 2025). Es besteht der Mythos, dass häufige Passwortänderungen zu mehr Sicherheit führen. Häufig führt dies stattdessen zu zu schwachen Varianten (z. B. "Passwort1", "Passwort2"). Das SBI empfiehlt daher, Passwörter nur bei Verdacht auf Kompromittierung zu ändern.  
Zur Erstellung eines sicheren Passworts gibt es zwei gebräuchliche Ansätze: Ein kürzeres und komplexes Passwort zu erstellen oder ein langes und weniger komplexes Passwort zu erstellen (BSI, o.D.). Die zwei in der Übung vorgestellten Methoden zur Erstellung eines sicheren Passworts (Satzmethode und Wortkombination), erfüllen die Voraussetzungen für diese Ansätze:

Bei der Satzmethode wird ein leicht merkbarer Satz ausgewählt und von jedem Wort wird der erste Buchstabe genommen, Zahlen oder Sonderzeichen werden beibehalten/hinzugefügt.

**Beispile 1**: Der Satz “Ich gehe jeden Morgen um Punkt 6 ins Büro!” kann zum Passwort “**IgjMu.6:00iB!**” umgewandelt werden.

**Beispiel 2**: "Mein Hund Max jagt 3x täglich um den Park!" → **MHmj3x#tüdP!**

Bei Wortkombinationen werden zufällige, unzusammenhängende Wörter (mindestens vier) und Zahlen ausgesucht. Dazu können Sonderzeichen eingefügt werden.

**Beispiel 1**: "Wolke", "Hebel", "Tiger", "17", "Stern" werden zum Passwort WolkeHebelTiger17\*Stern

**Beispiel 2:**  **Regen\*Tasse2023!Feder**

*Quellen: Bundesamt für Informationssicherheit (o.D.), Sebastian (2025)*

### Hinweise zur praktischen Übung:

1. **Ablauf der Übung**

* Die den Teilnehmenden bekannten Passwortrichtlinien aus ihren Behörden werden kurz besprochen, z.B. wie oft müssen Passwörter geändert werden, wie müssen Passwörter aussehen? (ca. 5 Min)
* Kenntnisse zur sicheren Passworterstellung werden durch die Erstellung sicherer Passwörter mit Satzmethode und Wortkombination und ein Quiz vertieft. Die Teilnehmenden erstellen jeweils selbst ein sicheres Passwort und teilen es mit dem Rest der Gruppe (ca. 10 Min)
* Passwortmanager und Multifaktorauthentifizierung werden als weitere Tools zur Erhöhung der Passwortsicherheit vorgestellt (ca. 5 Min). Die Verwendung eines Passwortmanagers wird kurz gezeigt, hierfür sollte, wenn vorhanden, das tatsächlich in Ihrer Behörde verwendete Programm benutzt werden (z. B. KeePass, LastPass) → Generierung, Speicherung, Autofill..
* Optional: MFA wird kurz vorgestellt, und es wird diskutiert inwieweit es in der Behörde genutzt wird.

1. **Schwerpunkt der Übung**

* erlernen von Techniken zur eigene Erstellung sicherer Passwörter

### Verfügbares Material:

1. für Schulung:
   1. Foliensatz
   2. Vorlage Passwort Quiz
2. weiterführende Materialhinweise für Schulende:
3. [Sichere Passwörter erstellen](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html), BSI
4. [Behörden Sicherheits IT- Training Passwörter](https://www.bits-training.de/training/03-lektion-passwoerter/), Kommunal Agentur NRW GmbH
5. Landesbetrieb Verkehr, [Behörden IT-Sicherheitstraining Passwörter](https://www.bits-training.de/training/03-lektion-passwoerter/)

## 

## Modul 3: Umgang mit Wechseldatenträgern

### Ziel des Moduls:

Das Modul „Umgang mit Wechseldatenträgern“ zielt darauf ab, den Teilnehmenden ein grundlegendes Verständnis bei der Nutzung fremder Wechseldatenträgern zu vermitteln und ein Bewusstsein möglicher Risiken und damit verbundenen Konsequenzen zu schaffen.

### Hintergrundwissen:

**Warum ist Sensibilisierung beim Umgang mit Wechseldatenträgern wichtig?**

* Mitarbeitern ist nicht bewusst, dass Wechseldatenträger möglicherweise Schadprogramme enthalten, die sämtliche vertrauenswürdige Daten kompromittieren könnten. Je nach Vorfall kann ein hoher wirtschaftlicher Schaden entstehen. Die frühzeitige Sensibilisierung und Auseinandersetzung mit dem Thema ist dabei entscheidend, damit Mitarbeiter:innen wissen, wie mit Wechseldatenträgern umgegangen wird.

### Hinweise zur praktischen Übung:

Die praktische Übung basiert auf einem modifizierten **USB-Stick (Rubber Ducky) mit einem simulierten Script**

1. **Ablauf der Übung**

* Der/die Schulungsleiter:in legt verschiedene USB-Sticks, worunter sich der Rubber Ducky befindet, auf einem Tisch in unmittelbarer Nähe aus und stellt einen Rechner oder einen Laptop zum Ausprobieren zur Verfügung.
* Die Teilnehmenden nehmen sich in beliebiger Reihenfolge einen USB-Stick.
* Jeder Teilnehmer kommt nacheinander nach vorne und schließt den Wechseldatenträger an den zur Verfügung gestellten Rechner oder Laptop an.
* Der Teilnehmende beschreibt, was in dem Moment auf dem Arbeitsrechner passiert.

1. **Schwerpunkt der Übung**

* Welche Schritte unternehmen die Teilnehmenden?
* Wie reagieren die Teilnehmenden auf die daraus entstandenen Konsequenzen?

1. **Auswertung**Lessons Learned

* Was habe ich gelernt?
* Was kann ich beim nächsten Mal besser machen/worauf muss ich achten?

=> Ergebnisse werden im Plenum aller Teilnehmenden zusammengefasst

1. **Lerneffekt**

* Die Übung endet mit der Diskussion über die Erkenntnisse und der zusammengetragenen Punkte von „Lessons Learned”

## 

## 

## Modul 4: Social Engineering und Manipulation

### Ziel des Moduls:

Teilnehmende erkennen typische Methoden des Social Engineerings, verstehen die psychologischen Mechanismen dahinter und können angemessen auf Manipulationsversuche reagieren.

### Hintergrundwissen:

**Social Engineering** bezeichnet die gezielte Manipulation von Personen, um vertrauliche Informationen (z. B. Passwörter, Finanzdaten) zu erlangen oder unberechtigte Handlungen auszulösen. Angreifer:innen nutzen psychologische Tricks wie:

* **Vertrauensbildung** (z. B. Vorgabe einer autoritären Rolle, z.B. „Ich bin der neue IT-Leiter – senden Sie mir die Zugangsdaten.“),
* **Druck / Dringlichkeit**  („Antworten Sie innerhalb von 24 Stunden, sonst Löschung Ihres Kontos!“)
* **Angst** („Ihr Konto wurde gehackt!“).

**Beispiele:**

* **Phishing:** Gefälschte E-Mails, SMS oder Websites, die zur Preisgabe von Daten auffordern (z. B. „Ihr Konto wurde gesperrt – bitte melden Sie sich hier an“).
* **CEO-Fraud:** Betrüger:innen geben sich als Vorgesetzte aus und fordern dringende Überweisungen oder sensible Dokumente an.
* **Pretexting:** Erfinden einer plausiblen Geschichte (z. B. „IT-Support-Mitarbeiter“), um Zugang zu Systemen zu erhalten.

### Hinweise zur praktischen Übung:

**Vorbereitung:** Teilnehmende erhalten im Vorfeld simulierte Phishing-Mails (z. B. „Gehaltsabrechnung angehängt“).

Im Modul dann gemeinsame Identifikation von Warnsignalen (z. B. falsche Absenderadresse, Rechtschreibfehler) und Diskussion welche psychologischen Tricks genutzt wurden.

### Verfügbares Material:

1. für Schulung
   1. Simulierte Phishing-Mails (vorab versendet).
2. für Schulenden:
   1. [Awareness-Poster](https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/partner/20190116_Awareness_Poster_SoSafe.pdf?__blob=publicationFile&v=2)
   2. [NoPhish](https://secuso.aifb.kit.edu/betruegerische_nachrichten_erkennen.php) (urheberrechtlich geschützt) von Karlsruher Institut für Technologie (KIT)

### Tipps für die Durchführung:

* **Praxisnahe Beispiele:** Nutzen Sie reale Vorfälle aus dem öffentlichen Dienst (z. B. Ransomware-Angriffe durch Phishing).
* **Sicherheitskultur stärken:** Betonen Sie, dass Rückfragen kein Misstrauen, sondern Professionalität zeigen.
* **Notfallplan:** Teilnehmende erhalten eine Schritt-für-Schritt-Anleitung für Verdachtsfälle („An wen melde ich mich?“).

## 

## Modul 5: Datensicherheit

### Ziel des Moduls:

Das Modul „Datensicherheit“ vermittelt den Teilnehmenden grundlegende Kenntnisse, um Daten in all ihren Lebensphasen (Erstellung, Speicherung, Verarbeitung und Entsorgung) effektiv zu schützen. Hierbei werden drei zentrale Themen fokussiert:

1. Verschlüsselung von Daten
2. Backups
3. Sicheres Arbeiten im Homeoffice

Ziel ist es, ein ganzheitliches Verständnis für die Bedeutung des Datenschutzes und der Datensicherheit in unterschiedlichen Arbeitsumgebungen zu schaffen. Die Teilnehmenden sollen durch praxisnahe Beispiele und Übungen lernen, wie sie Daten vor unbefugtem Zugriff bewahren, Datenverluste verhindern und vertrauliche Informationen auch außerhalb der Behörde (z. B. im Homeoffice) sicher bearbeiten können. Teilnehmende verstehen am Ende des Moduls die Grundprinzipien der Datensicherheit, lernen praktische Methoden zum Schutz sensibler Daten und reflektieren über Risiken im Umgang mit digitalen Informationen.

### Hintergrundwissen:

**Warum Datensicherheit so wichtig ist**

**Schutz sensibler Daten:** Öffentliche Behörden verarbeiten personenbezogene und teils hochsensible Daten. Ein Verlust oder eine Offenlegung dieser Informationen kann erhebliche Konsequenzen für die Betroffenen nach sich ziehen und rechtliche wie auch finanzielle Schäden für die Behörde bedeuten.

**Verpflichtung gegenüber Bürger:innen:** Der Schutz von Daten ist gesetzlich verankert (z. B. DSGVO). Behörden tragen eine besondere Verantwortung, da öffentliches Vertrauen auf gesicherte Dienste angewiesen ist.

**Risiken bei der Datenverarbeitung**: Von unverschlüsselten E-Mails über ungeschützte USB-Sticks bis hin zu Phishing-Angriffen im Homeoffice – die Bedrohungslage ist vielfältig und erfordert entsprechende Schutzmaßnahmen.

### Hinweise zur praktischen Übung:

**Ablauf der Übung**

* Verschlüsselung von Dateien und Festplatten (5 min):

Mit den Teilnehmenden wird diskutiert warum Verschlüsselung sinnvoll ist (Vertraulichkeit, Integrität der Daten, Datenschutz und Compliance, Schutz vor Cyberangriffen, etc.) und welche Daten besonders schützenswert sind (Persönliche Daten, etc.). Es wird kurz BitLocker und die Verschlüsselung individueller Dateien/Ordner vorgestellt

* Backups (5 min):

Es werden kurz automatische und manuelle Backups unter Windows vorgestellt. Außerdem können für die Schulungsteilnehmende in ihrer Behörde relevante Themen, wie z.B. das Backup von Browser-Lesezeichen, thematisiert werden.

* Sicherheit im Homeoffice (10 min):

Basierend auf einer modifizierten Version der [Checkliste zur Sicherheit im Home-Office](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Remote/Home-Office/Checkliste-Home-Office/checkhomeoffice_node.html) des BSI werden mit den Teilnehmenden 8 Fragen zur Umsetzung von Sicherheit im Homeoffice in ihrer Behörde besprochen

### Verfügbares Material:

1. für Schulung:
   1. Foliensatz
2. weiterführende Materialhinweise für Schulende:

[Home-Office? – Aber sicher!](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Remote/Home-Office/home-office_node.html), BSI

[Checkliste zur Sicherheit im Home-Office](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Remote/Home-Office/Checkliste-Home-Office/checkhomeoffice_node.html), BSI

## 

## Modul 6: Reaktion auf Sicherheitsvorfälle

### Ziel des Moduls:

Das Modul „Reaktion auf IT-Sicherheitsvorfälle“ zielt darauf ab, die Teilnehmenden auf den Ernstfall vorzubereiten. Sie sollen lernen, auf Sicherheitsvorfälle angemessen zu reagieren und durch koordinierte Maßnahmen Schäden zu minimieren. Dabei werden sowohl technische als auch organisatorische Aspekte betrachtet, um ein ganzheitliches Verständnis für die Herausforderungen eines Sicherheitsvorfalls zu vermitteln.

### Hintergrundwissen:

**Warum ist die Reaktion entscheidend?**

* Eine schnelle und effektive Reaktion kann den Schaden erheblich begrenzen und Wiederherstellungszeiten verkürzen. Laut BSI-Berichten bleibt jedoch oft wertvolle Zeit ungenutzt, weil Mitarbeitende unsicher sind, wie sie handeln sollen.

**Typische Sicherheitsvorfälle**

* Beispiele wie Ransomware-Angriffe, Phishing-Angriffe oder unerlaubte Zugriffe verdeutlichen, wie wichtig klare Handlungsanweisungen sind.

**Grundlagen der Reaktion**:

* **Meldung**: Schnelle Kommunikation mit der IT-Abteilung oder zuständigen Stelle.
* **Isolierung**: Eindämmung des Vorfalls, z. B. durch Trennen vom Netzwerk.
* **Dokumentation**: Erfassen aller relevanten Informationen zum Vorfall.
* **Zusammenarbeit**: enge Abstimmung mit internen oder externen Experten.

### Hinweise zur praktischen Übung:

Die praktische Übung basiert auf einem simulierten **Ransomware-Szenario auf einen Arbeitsplatzrechner**: Ziel der Übung ist es, dass die Teilnehmenden selbstständig überlegen, wie sie angemessen auf die Situation reagieren und gegebenenfalls Unterstützung einholen. Für Schulungsgruppen ohne oder nur wenig Vorerfahrung wird ein strukturierter, anleitender Ansatz durch gezielte Fragen empfohlen. Fortgeschrittene Schulungsgruppen können eine offenere Variante der Übung wählen, bei der sie komplett selbstständig Lösungen entwickeln.

**Übungsszenario: "E-Mail-Anhang enthält potenziell schädliche Datei"**

Sie sitzen an Ihrem Arbeitsplatz, als plötzlich eine dringende E-Mail eintrifft. Nach dem Öffnen des E-Mail-Anhangs erscheint der Bildschirm, der auf der Folie zu sehen ist.

**Aufgabe:** Analysieren Sie die Situation und entwickeln Sie innerhalb von 10 Minuten konkrete Schritte, um angemessen zu reagieren.

### **Ablauf der Übung:**

#### **1. Einführung:**

Stellen Sie das Szenario vor. In einem realen Arbeitsumfeld könnten die Teilnehmenden mit so einer Situation konfrontiert werden, bei der sie genau entscheiden müssen, wie sie reagieren. Die Aufgabe für die Teilnehmenden ist es, zu entscheiden, welche Schritte sie unternehmen würden, um mit dieser Situation umzugehen und sie zu lösen.

**2a. Geführte Übung (für Schulungsgruppen ohne Vorerfahrung):**

Beginnen Sie mit den folgenden Fragen, um die Diskussion und die Lösungsfindung anzuleiten:

* **Frage 1:** Was sehen Sie auf dem Bildschirm? Beschreiben Sie die Situation (Art des Anhanges, Datei und Nachricht).
* **Frage 2:** Was könnte das Risiko dieser Datei sein? (Mögliche schadhafte Software, Viren, Ransomware)
* **Frage 3:** Was sollten Sie tun, bevor Sie die Datei öffnen oder weiter damit arbeiten? (Sicherheitsmaßnahmen wie Antivirenprüfung, Bestätigung der Quelle)
* **Frage 4:** Wie können Sie sicherstellen, dass der E-Mail-Anhang keine Bedrohung darstellt? (Antiviren-Software, IT-Abteilung konsultieren, Dateiansicht anstelle von -Öffnung)
* **Frage 5:** Welche Kommunikation ist notwendig? Sollten Sie den Absender kontaktieren? Wie setzen Sie Ihre IT-Abteilung in Kenntnis?
* **Frage 6:** Sollte der Vorfall dokumentiert oder weiter eskaliert werden? Welche Protokolle sind für eine solche Situation zu befolgen?

#### **Interaktive Phase: Simulation einer IT-Abteilung zur Kommunikation:**

Für ein praxisnahes Übungserlebnis haben die Teilnehmenden die Möglichkeit, mit einer simulierten IT-Abteilung zu kommunizieren. Schlagen Sie vor, dass jeder Teilnehmende die Situation beschreibt und Unterstützung anfragt, falls Unsicherheit besteht.

Ermutigen Sie die Teilnehmenden, folgendermaßen vorzugehen:

* **Melden Sie das Problem der IT-Abteilung und fragen Sie nach der besten Vorgehensweise.**
* **Fragen Sie nach den von der IT-Abteilung empfohlenen Prüfungen oder Prüfmechanismen.**
* **Dokumentieren Sie die Schritte zur Eskalation, falls die IT-Abteilung nicht zur Lösung des Problems beiträgt.**

Während der Übung können Sie weitere Fragen oder hypothetische Szenarien einstreuen (z. B. „Was passiert, wenn die Datei geöffnet wurde und es wird ein Virus gefunden? Was tun Sie?“).

**2b. Offene Übung (für fortgeschrittene Schulungsgruppen):**

Die Teilnehmenden lösen das Übungsszenario eigenständig, z.B. in kleineren Gruppen, und beschreiben anschließend ihre Schritte zur Problemlösung. Sehr fortgeschrittene Teilnehmende können hierbei angehalten werden, eine detaillierte Lösung zu erarbeiten, die Folgendes umfasst:

* Plan zur Überprüfung der Datei, sei es durch Antiviren-Software, virtuellen Sandkasten oder andere Prüfverfahren, die in ihrer Behörde vorhanden sind
* konkrete Handlungsschritte, die das Eindämmen der Gefahr betreffen, wie das Abtrennen des Geräts vom Netzwerk oder das Benachrichtigen von relevanten Teams oder Managern

Fragen zur Selbstreflexion für Fortgeschrittene:

* Welche Schwachstellen oder Risiken könnten in einer Behörde für derartige Vorfälle bestehen? (Verweis auf die Sicherheitsvorfälle aus Modul 1)
* Welche präventiven Maßnahmen könnten vorab getroffen werden, um diese Situationen zu minimieren? (Verweis auf die Sicherheitsvorfälle und Posititvbeispiel aus Modul 1)

#### **3. Diskussion & Abschluss:**

Nach der ersten Analyse und Reaktion der Teilnehmenden wird mit der gesamten Gruppe die Lösungsansätze besprochen und eingeordnet:

* Was haben alle Teilnehmende als erste Schritte vorgeschlagen?
* Ablauf anhand der IT-Notfallkarte durchsprechen: Welche Informationen sind wichtig und kann ich als Nicht-IT-Kolleg:in liefern? Ggf. IT-Notfallkarte ausdrucken und den Teilnehmenden mitgeben für ihren Arbeitsplatz
* **Best Practices**: Positives Verhalten wird hervorgehoben, z. B. sofortiges Melden, systematische Dokumentation.
* **Worst Practices**: Fehler und potenzielle Folgen, z. B. unsachgemäße Kommunikation oder unnötige Verzögerungen.
* optimales Vorgehen wird zusammengefasst.
* Welche Sicherheitstools oder Ressourcen haben Sie genutzt?
* Was wären die möglichen Folgen, wenn nicht sofort reagiert wird?
* Gibt es präventive Maßnahmen zur Minderung des Risikos?

### Wichtige Lernpunkte:

* **Sicherheit zuerst!** Die Vermeidung eines Öffnens potenziell schadhafter Dateien oder das Verifizieren der Quelle des Anhangs ist essenziell.
* **Proaktive Kommunikation.** Klare Kommunikation mit der IT-Abteilung hilft, Risiken zu erkennen und geeignete Maßnahmen zu ergreifen.
* **Dokumentation und Eskalation.** In jeder Sicherheitsangelegenheit muss ein ordentliches Eskalationsverfahren zur Fehlerbehebung und Vermeidung von Wiederholung festgelegt werden.
* **Lerneffekt:**
  1. in der Übung wird über die Lösungsansätze, Probleme und Erkenntnisse offen diskutiert und offene Fragen geklärt.
  2. Ziel ist es, den Teilnehmenden Sicherheit im Umgang mit realen Vorfällen zu vermitteln und eine klare Handlungsstruktur einzuprägen.

### Verfügbares Material:

1. für Schulung:
   1. Foliensatz
   2. IT-Notfallkarte \*Allianz für Cybersicherheit
      1. unter freier Lizenz veröffentlicht
      2. kann ausgedruckt, verteilt und ausgefüllt werden im Rahmen der Schulung
   3. Lan-Kabel (sollte in jeder Behörde vorhanden sein, um so eins zu zeigen)
2. weiterführende Materialhinweise für Schulende:
   1. [Cyberresilience-Framework. In IT-Krisen schneller agieren (kurz: RESI)](https://www.dialog-cybersicherheit.de/media/), Krisenkommunikation, Dialog für Cybersicherheit im BSI
   2. [Kommunale IT-Krisen: Handlungsfähigkeit sichern - Ein Wegweiser zur Bewältigung und Prävention](https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/KRITIS/wegweiser-kommunale-it-krisen_download.pdf?__blob=publicationFile&v=9), BKK und BSI
   3. allgemeine Informationen von BSI und der Allianz für Cybersicherheit zum [Faktor Mensch](https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/faktor-mensch_node.html) in der IT-Sicherheit

## Evaluation

Die Evaluation der Schulung stellt einen entscheidenden Schritt dar, um deren Effektivität und Nutzen zu bewerten. Mithilfe der Rückmeldungen der Teilnehmenden können wertvolle Erkenntnisse darüber gewonnen werden, wie gut die Inhalte verstanden wurden und in der Praxis angewendet werden können. Dies bildet die Grundlage, Inhalte und Methoden gezielt an die spezifischen Bedürfnisse Ihrer Behörde anzupassen und einen nachhaltigen Lerneffekt zu erzielen.

Die Evaluation sollte unmittelbar nach Abschluss der Schulung erfolgen, damit Eindrücke frisch sind und idealerweise in einem Dialog Rückmeldungen und Verbesserungsvorschläge diskutiert werden können. Sie gliedert sich in zwei Abschnitte: Im ersten Teil wird die subjektive Wahrnehmung der Teilnehmenden abgefragt, beispielsweise welche Module besonders gut gefallen haben oder welche Themen in Zukunft gewünscht werden. Im zweiten Teil wird der tatsächliche Lerneffekt durch eine Wissensabfrage überprüft.

Die Evaluation sollte nicht länger als 15 Minuten dauern. Beim ersten Teil empfiehlt es sich, den Schwerpunkt auf einen offenen Austausch zu legen, um mögliche Unklarheiten aus den Rückmeldungen zu klären oder detaillierte Vorschläge im Dialog zu erfassen. Idealerweise erfolgt die Befragung anonym und digital, um ohne zusätzliche Auswertungszeit einen direkten Überblick über das Feedback zu erhalten. Eine Vorlage zur Evaluation Ihrer Schulung finden Sie in den bereitgestellten Materialien.

# Quellenverzeichnis:

Bundesamt für Informationssicherheit (o.D.), Sichere Passwörter erstellen, [Abgerufen am 14. Januar 2025]. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen\_node.html

Griebsch, S. (2022). Cyberangriff auf den Landkreis Anhalt-Bitterfeld – Herausforderungen bei der Reaktion auf die Bedrohungen [Abgerufen am 26. November 2024]. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/C3Conference/2022/Griebsch\_LandkreisAnhaltBitterfeld.pdf?\_\_blob=publicationFile&v=3

Heise Online. (2021a). BSI: Kooperation mit Anhalt-Bitterfeld nach Cyberattacke war herausfordernd [Abgerufen am 26. November 2024]. https://www.heise.de/news/BSI- Kooperation- mit- Anhalt- Bitterfeld-nach-Cyberattacke-war-herausfordernd-9229888.html

Heise Online. (2021b). Cyberangriff auf Anhalt-Bitterfeld: Landkreis zeigt sich weiterhin unerpressbar [Abgerufen am 26. November 2024]. https : / / www. heise . de / news / Cyberangriff - auf - Anhalt - Bitterfeld -Landkreis-zeigt-sich-weiterhin-unerpressbar-6160917.html

Heise Online. (2023a). Cyberangriff auf Südwestfalen-IT: Mehr Kommunen betroffen – Notbetrieb hält an [Abgerufen am 26. November 2024]. https://www.heise.de/news/Cyberangriff-auf-Suedwestfalen-IT-

Mehr-Kommunen-betroffen-Notbetrieb-haelt-an-9532453.html

Heise Online. (2023b). Ransomware kostete Anhalt-Bitterfeld rund 2,5 Millionen Euro [Abgerufen am 26. November 2024]. https://www.heise.de/news/Ransomware - kostete - Anhalt- Bitterfeld - rund - 2 - 5 -Millionen-Euro-9650816.html

Heise Online. (2023c). Südwestfalen-IT: Angreifer errieten Passwort und kamen über bekannte Cisco-Lücke [Abgerufen am 26. November 2024]. <https://www.heise.de/news/Suedwestfalen-IT-Angreifer-errieten-Passwort-und-kamen-ueber-bekannte-Cisco-Luecke-9610102.html>

Sebastian, Nathan (2025). Top Password Strengths and Vulnerabilities: Threats, Preventive Measures, and Recoveries [Abgerufen am 15. Januar 2025]. <https://www.goodfirms.co/resources/top-password-strengths-and-vulnerabilities>

Stadt Berlin. (2024). IKT-Sicherheitsarchitektur. Abgerufen am 02.12.2024, von<https://www.berlin.de/moderne-verwaltung/prozesse-und-technik/ikt-sicherheit/ikt-sicherheitsarchitektur/artikel.947487.php>

Südwestfalen-IT. (2023a). Cyber-Angriff auf Südwestfalen-IT – Aktueller Stand. https://notfallseite.sit.nrw/aktuelle-meldungen?tx\_news\_pi1%5Baction%5D=detail&tx\_news\_pi1%5Bcontroller%5D=News&tx\_news\_pi1%5Bnews%5D=774&cHash=c9a93ee75846ddc335c34a3cbf61ae76

Südwestfalen-IT. (2023b). SIT Incident Response – Version 1.1. https://notfallseite.sit.nrw/fileadmin/user\_upload/SIT\_Incident\_Response\_v1.1.pdf