SPD On: Wachsam sein. Tipps für mehr IT-Sicherheit im politischen Ehrenamt.

Warum Informationssicherheit für Parteiarbeit wichtig ist

Bundesamt
für Sicherheit in der
Informationstechnik

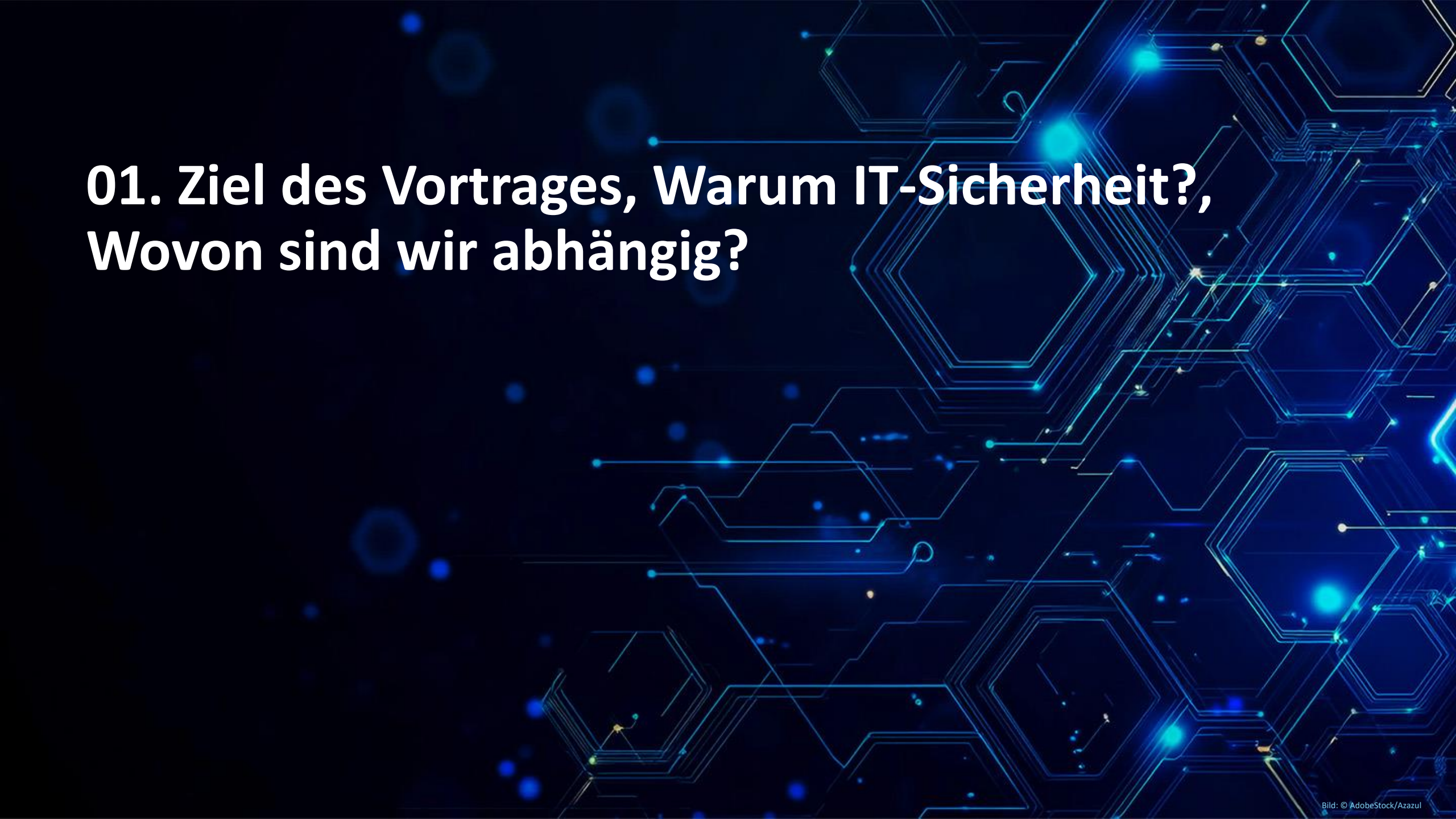
Konstantin Beck, Referatsleiter
Steven Müller, Referent
Max Schumann, Sachbearbeiter

Referat I 13 - Umsetzungsberatung in digitalisierten Verwaltungsleistungen, Justiz und Politik

Agenda

- Ziele des Vortrages
- Abhängigkeit von IT
- Gefahren
- IT im Ehrenamt
- Szenarien aus dem Alltag
- Sofortmaßnahmen
- Zeit für Fragen

01. Ziel des Vortrages, Warum IT-Sicherheit?, Wovon sind wir abhängig?



Aktuelle Situation – gefühlte Lage in Deutschland

Alert!

IT-Management-Plattform SolarWinds über mehrere Wege angreifbar

Die SolarWinds-Entwickler haben mehrere Sicherheitslücken in ihrer Software geschlossen. Angreifer können etwa für Abstürze sorgen.

IT-Sicherheitsvorfall: Varta stoppt Produktion

Der Batteriehersteller Varta AG hat nach einem Cybervorfall die IT-Systeme sowie seine Produktion heruntergefahren.

174

Chinesische Cyberkriminelle hatten jahrelang Zugriff auf Chiphersteller NXP

Die in China verortete Cybergang Chimera soll zwischen 2017 und 2020 Zugang zu NXP-Netzwerken gehabt und vor allem Chipdesigns in die Finger bekommen haben

Cyberkriminalität

Immer mehr Lösegeldattacken

Vor allem Mittelständler sind häufig unzureichend gegen Angriffe mit Erpressungssoftware geschützt. Cyberversicherungen werden teuer.

Susanne Schier Frankfurt, Baden-Baden

Der Markt für US-Staatsanleihen ist der größte und wichtigste der Welt. Und doch gelang es Hackern am vergangenen Donnerstag, dieses riesige Geschäft durcheinanderzubringen. Der US-Ableger der chinesischen Großbank ICBC meldete eine sogenannte Ransomware-Attacke: werden die Preise tendenziell weiter steigen, da auch die Schäden aktuell wieder zunehmen", prognostizierte Hasse.

Die Juristin ist bereits seit mehr als 20 Jahren bei Munich Re tätig und seit 2019 unter anderem für das Cybergeschäft in Europa und Lateinamerika verantwortlich. Im deutschen Markt ist ein gutes Dutzend größerer Erstversicherer im Cy-

Russische Angreifer klauen Quellcode von Microsoft

Seit Monaten greifen staatlich geförderte Cyberkriminelle die Systeme von Microsoft an. Das dauert auch jetzt noch an, dabei konnten Daten entwendet werden.

373

US-Regierungsbehörden: IT seit Jahren durch chinesische Angreifer unterwandert

Sicherheitsbehörden in den USA schlagen Alarm – Volt Typhoon ist bereits vor Jahren in kritische US-Infrastrukturen eingedrungen. Ursprung der Attacken: China.

Cybercrime: KI-generierte Malware in freier Wildbahn gesichtet

Sicherheitsexperten von HP weisen auf einen beunruhigenden Trend hin: Kriminelle nutzen verstärkt generative KI zur Entwicklung von Malware.

Londoner Kliniken: Cyberkriminelle veröffentlichen Daten

Infolge eines Cyberangriff auf einen Pathologiedienstleister sind Londoner Kliniken im Notbetrieb. Jetzt haben die Cyberkriminellen Daten veröffentlicht.

Datenleck: AT&T setzt die Passwörter von Millionen von Kunden zurück

Nachdem Kontodaten von etwa 73 Millionen aktuellen und ehemaligen AT&T-Kontoinhabern im Dark Web aufgetaucht sind, wird das Unternehmen aktiv.

Kritische Infrastruktur

Mehr Cyberangriffe auf deutsche Seehäfen

Stand: 05.09.2024 08:56 Uhr

Deutsche Seehäfen waren zuletzt immer häufiger von Cyberangriffen betroffen. Besonders seit Beginn des russischen Angriffskrieges hat die Zahl der Cyberattacken zugenommen.

Cyber-Angreifer erbeuten E-Mails aus Microsofts Cybersicherheitsabteilung

Die kriminelle Gruppe Midnight Blizzard hat sich Zugang zu E-Mails von Microsoft-Mitarbeitern verschafft. Sie wollte wohl wissen, was Microsoft über sie weiß.

Zehntausende Kunden betroffen

Cyberattacke auf Immobilientochter der DZ-Bank

Stand: 22.06.2024 16:36 Uhr

Mehr Börsenbetrug durch Social Media und KI?

Stand: 18.01.2024 15:35 Uhr

Dubiose Finanztipps oder manipulierte Bilder, die Kurse einbrechen lassen: Soziale Medien und KI eröffnen neue Möglichkeiten, Märkte zu beeinflussen. Macht es das für Börsenbetrüger einfacher?

Malware: Cyberkriminelle verteilen Malware über Videos auf Youtube

Teils auf verifizierten Youtube-Kanälen werden Spiele-Cracks versprochen. In Wirklichkeit jedoch wird Malware geliefert.

Updates unmöglich: Niederlande müssen Ampeln wegen Sicherheitslücke austauschen

Per Funk können Angreifer die Ampeln aus der Ferne umschalten und somit den Straßenverkehr stören. Der Austausch wird Jahre in Anspruch nehmen.

CYBERANGRIFF

Iranische Hacker greifen laut FBI in US-Wahlkampf ein

Ziele des Vortrages

- **Bewusstsein schaffen**
  - Warum IT-Sicherheit nicht nur „Technik-Problem“, sondern Gemeinschaftsaufgabe ist
  - Weckruf: Digitale Angriffe können schon kleine Gruppen existenziell bedrohen
- **Risiken kennen**
  - Überblick über aktuelle Gefahren: von Schadsoftware bis Desinformation
  - Konkrete Beispiele: Was passiert, wenn ein Ortsverband plötzlich keine E-Mails mehr versenden kann?
- **Schutzmaßnahmen vermitteln**
  - Ansatz „Pragmatismus vor Perfektion“: Welche ersten Schritte sind machbar?
  - Vorstellung bewährter Tools und Vorgehensweisen
- **Handlungskompetenz stärken**
  - Jeder weiß am Ende, wie er im Alltag besser auf sich und die Gruppe Acht gibt
  - Erste-Hilfe-Checkliste für den Fall, dass doch mal etwas schiefgeht
- **Denkanstoß:**

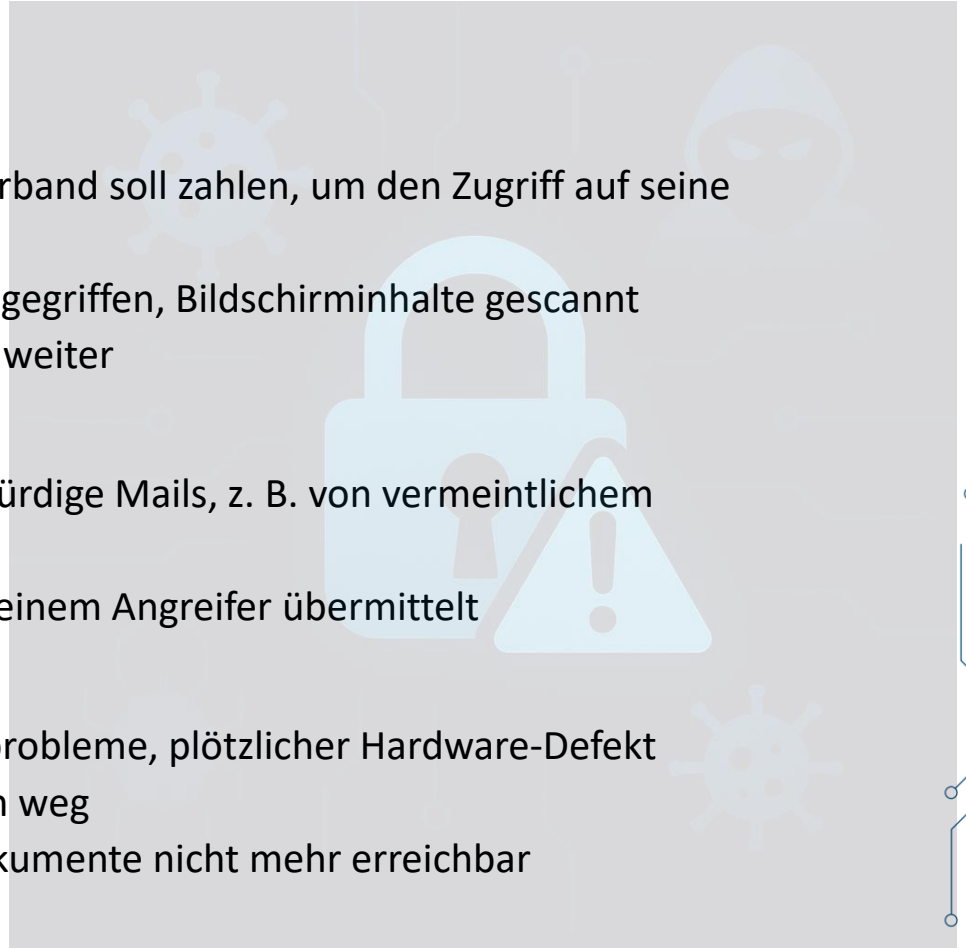
  „Welche konkrete Sofortmaßnahme kann ich noch heute umsetzen, damit wir sicherer arbeiten?“

Von welchen IT-Diensten sind wir abhängig?

1. **E-Mail & Messenger**
   - Austausch von Protokollen, Beschlüssen, Mitgliedsanfragen
   - Organisatorische Absprachen: Wer bringt was zum nächsten Treffen mit?
2. **Terminplanung & Kalender**
   - Gemeinsamer Kalender (z. B. Google Calendar, Outlook): Einladungen, Erinnerungen, virtuelle Räume
   - Konsequenz bei Kompromittierung: Doppelbelegungen, verpasste Fristen, Verwirrung bei Terminen
3. **Dateifreigabe & Cloud-Dienste**
   - Gemeinsame Ablage von Programmentwürfen, Finanzunterlagen, Satzungen
   - Zugriffskontrolle: Wer darf welche Dateien sehen/bearbeiten?
   - Gefahr: Unbefugter Dritter liest interne Dokumente oder manipuliert Beschlüsse
4. **Soziale Netzwerke & Webauftritt**
   - Facebook, Twitter, Instagram, eigene Website: Kontakt zu Wählern, Mitgliedergewinnung, Öffentlichkeitsarbeit
   - Risiko: Fake-Profile, Social-Engineering-Angriffe gegen Administratoren, gefälschte Posts
5. **Videokonferenzen & Online-Tools**
   - Zoom, Webex und Co. für Sitzungen, Diskussionsrunden, Fortbildungen
   - Sicherheitsverletzung: Externe schaltet sich ungebeten dazu („Zoom bombing“), Mitschnitte im Netz

KI-generiert mithilfe von chat.openai.com - Public Domain Mark

Gefahren in der digitalen Welt



1. **Schadsoftware (Malware)**
   - **Ransomware:** Verschlüsselt Dateien, fordert Lösegeld. Beispiel: Ein Ortsverband soll zahlen, um den Zugriff auf seine Webseite und Social Media Konten wiederzubekommen
   - **Trojaner:** Unbemerkte Hintertüren, Im Hintergrund werden Passwörter abgegriffen, Bildschirminhalte gescannt
   - **Spyware:** Lauscht bei Online-Konferenzen mit und leitet Gesprächsinhalte weiter
2. **Spionage & Datenabfluss**
   - **Phishing & Spear Phishing:** Zugangsdaten werden gestohlen, Sehr glaubwürdige Mails, z. B. von vermeintlichem Landesvorstand
   - **Keylogger:** Spionagegerät, welches alle Tastatureingaben mitschreibt und einem Angreifer übermittelt
3. **Technische Ausfälle & Datenverlust**
   - **Veraltete Hardware/Software:** Keine Sicherheitsupdates, Kompatibilitätsprobleme, plötzlicher Hardware-Defekt
   - **Kein Backup:** Festplatte defekt → alle Sitzungsprotokolle und Kontaktlisten weg
   - **Cloud-Provider-Ausfall:** Wenn der genutzte Cloud-Dienst ausfällt, sind Dokumente nicht mehr erreichbar
4. **Manipulationen & Desinformation**
   - **Fake News & Deepfakes:** Manipulierte Videos oder Posts, die eine Partei-Position falsch darstellen
   - **Social Engineering:** Angreifer „ergaunert“ per Telefon oder Chat Zugangsdaten, indem er sich als Mitglied ausgibt
   - **Echte vs. gefälschte Ankündigungen:** Gefälschte Wahlaufrufe, Sitzungs-Einladungen, die auf falsche Links verweisen

Warum IT-Sicherheit im Ehrenamt?

KI-generiert mithilfe von chat.openai.com - Public Domain Mark

1. **Digitalisierung als Basis unserer Arbeit**
   - E-Mail, Gruppen-Chat, Videokonferenz: Unser Meetingraum ist virtuell geworden
   - Terminplanung und Protokolle in der Cloud: Mobilität und Flexibilität, aber auch neue Angriffsflächen
2. **Angriffe können jede Ebene treffen**
   - Einzelner Nutzer: E-Mail-Account gehackt → Identitätsdiebstahl, Datenverlust (z. B. Kontaktlisten, vertrauliche Infos)
   - Lokales MdB: Oftmals enger Kontakt zu lokalen Parteistrukturen → Social Engineering Vorfälle strahlen auf MdB
   - Ortsverband: Backup fehlt, Leitung fällt aus → Sitzungen abgesagt, wichtige Fristen verpasst
   - Partei insgesamt: Datenleck → politischer Imageschaden, Verlust von Vertrauen bei Mitgliedern
3. **Abhängigkeit ist hoch**
   - Ohne funktionierende IT: Keine Kommunikation, keine Öffentlichkeitsarbeit, keine Terminabstimmung
   - Beispiel 1: Wahlkampf – plötzlich keine Mailingliste erreichbar
   - Beispiel 2: Pressemitteilung mit falschen Kontaktdaten, da jemand ins E-Mail-Konto eingedrungen ist
4. **Praktische Folge:**

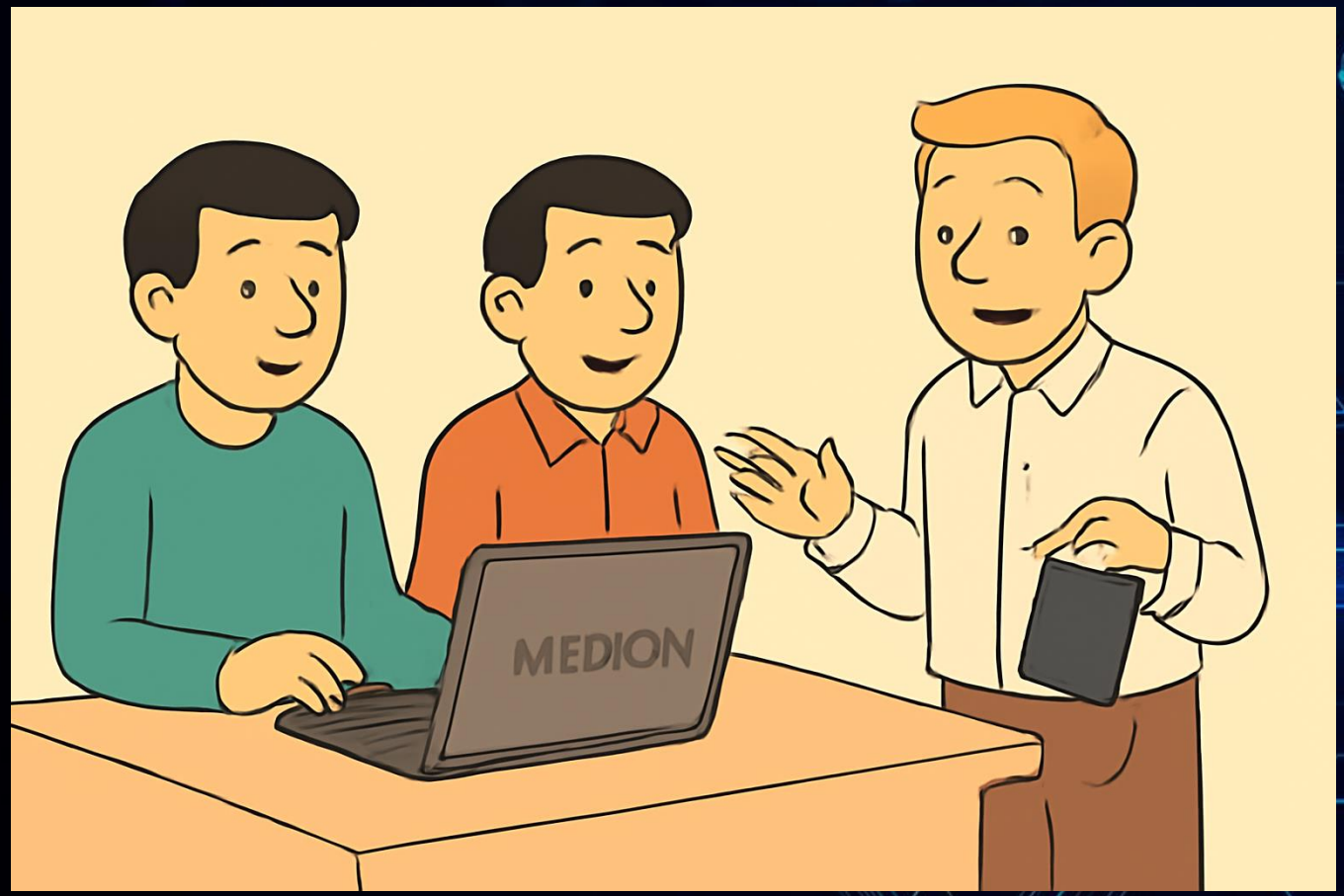
   Wer IT-Sicherheit vernachlässigt, riskiert den reibungslosen Ablauf von Prozessen und gefährdet die Glaubwürdigkeit.

Wer ist betroffen?

1. **Einzelne Mitglieder**
   - **Beispiel:** Konto gehackt → private Fotos veröffentlicht, E-Mails an Arbeitgeber geleakt → arbeitsrechtliche Probleme
   - **Datendiebstahl:** Namen und Adressen werden gestohlen und für Spam-Kampagnen missbraucht
2. **Orts-, Stadt- und Kreisverbände**
   - **Manipulierte Protokolle:** Achtung, wenn Protokolle zentral in der Cloud liegen, kann jemand unbemerkt Änderungen vornehmen
   - **Terminchaos:** Abhängigkeit von einem Kalender. Bei Kompromittierung: Doppelbuchungen, Mitglieder erfahren nicht rechtzeitig von Treffen
   - **Kommunikationsstörungen:** Wenn E-Mail-Server angreifbar ist, fallen Newsletter und Abstimmungsrunden aus
3. **Partei als Gesamtorganisation**
   - **Rufschädigung:** „Leaks“ aus interner Kommunikation landen in der Presse
   - **Vertrauensverlust:** Mitglieder und auch Wähler trauen der Organisation nicht mehr
   - **Rechtliche Folgen:** Verstoß gegen Datenschutz-Grundverordnung (DSGVO), Bußgelder, Abmahnungen
4. **Kernaussage:**

IT-Sicherheit betrifft nicht nur die Technik, sondern unsere ganze Arbeit und unseren Zusammenhalt.

02. Szenarien aus dem Alltag



KI-generiert mithilfe von chat.openai.com - Public Domain Mark

Szenario 1 – Veraltete Technik

Situation

- Nutzung älterer Computer und Kommunikationstechnik

Risiko

- Alte Betriebssysteme sind das gefährlichste Einfallstor für Ransomware
- Plötzlicher Ausfall einzelner Computerteile. Wenn die Festplatte kaputt ist, sind alle Dokumente weg

Prävention / Lösung

Kurzfristige Maßnahmen:

- Regelmäßig Datensicherungen erstellen (wichtige Dokumente auf USB-Stick oder in Cloud kopieren)

Mittelfristige Maßnahme:

- Aktuelle Computer und Kommunikationstechnik verwenden:
- Wartung und Datensicherung automatisieren
- IT-Verantwortlichen im Ortsverband ernennen, der einmal im Quartal Hardware & Software prüft

Lernpunkte & Diskussion

- Geräte haben nur eine begrenzte Lebensdauer – IT-Kompetenz bedeutet, das rechtzeitig zu erkennen
- Backup ist kein Extra, sondern Grundvoraussetzung (3-2-1-Regel: 3 Kopien, 2 Datenträger, 1 externer Standort)

KI-generiert mithilfe von chat.openai.com - Public Domain Mark

02. Szenarien aus dem Alltag

KI-generiert mithilfe von chat.openai.com - Public Domain Mark

Szenario 2 – E-Mail-Kommunikation

Situation

- Leichtfertiges Vertrauen in E-Mail Kommunikation

Risiko / Gefahren

- Gefälschte E-Mail (Inhalt, Absender)
- Angriffe mit E-Mail (Phishing & Spear Phishing):
  - *Gefälschte täuschend echt wirkende Mails*
  - *Ziel: Anmeldenamen, Passwörter, vertrauliche Infos ergattern*
- Angriffe mit E-Mail (Malware-Verbreitung):
  - *E-Mail-Anhang (Word/PDF) mit bösartigem Makro*
  - *Links zu Webseiten, die zu manipulierten Inhalten oder der Aktivierung direkter Angriffe führen*

KI-generiert mithilfe von chat.openai.com - Public Domain Mark

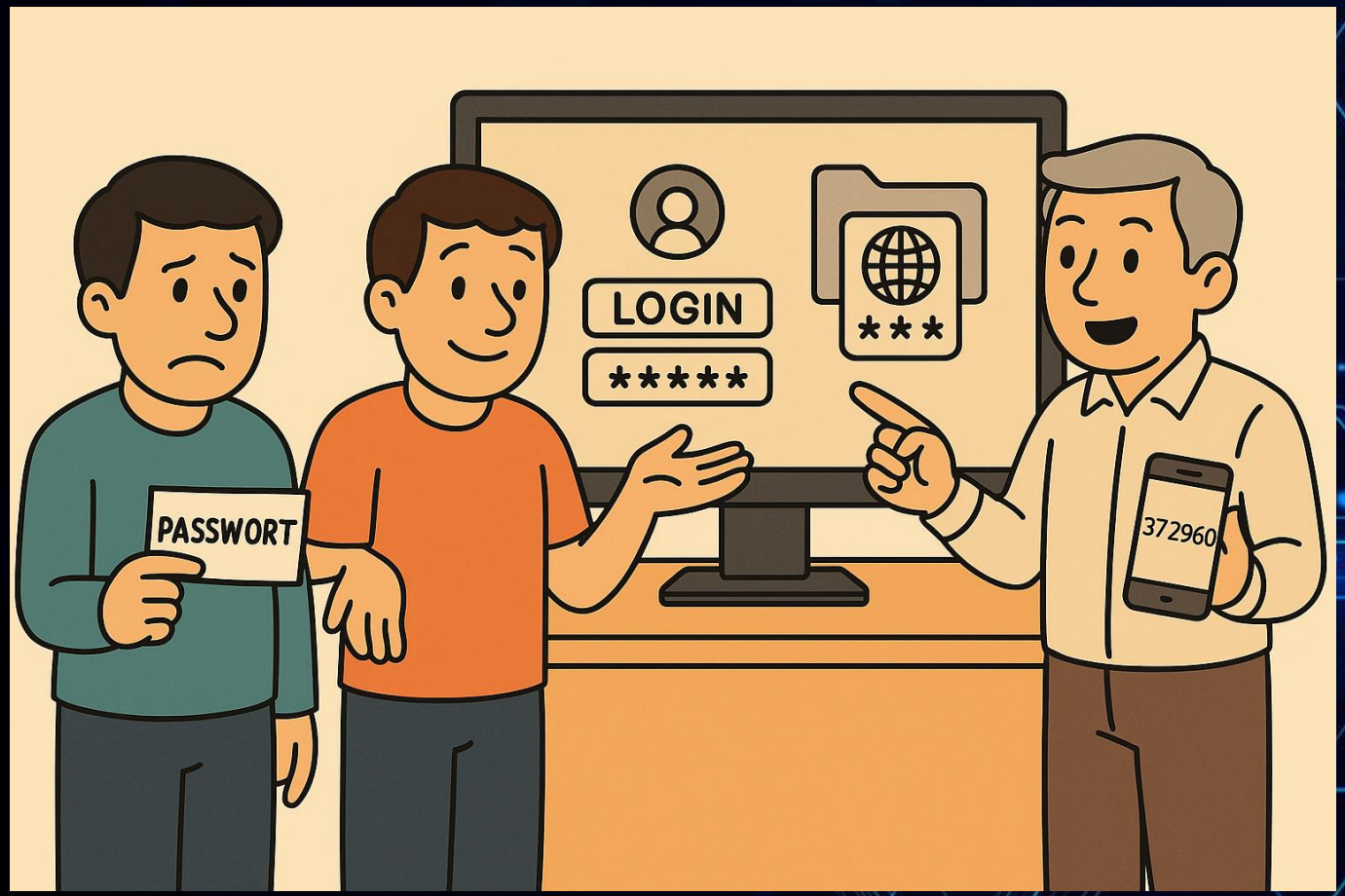
Prävention / Lösung

- Absender immer überprüfen
  - *Verdächtige Mails IMMER telefonisch oder persönlich verifizieren*
  - *klare Absenderprüfung: Domain sieht fast gleich aus* (z. B. kreisvorstand-party.de vs. kreisvrstand-party.de)
- Spamfilter & sichere E-Mail-Provider
- E-Mail-Verschlüsselung

Lernpunkte & Diskussion

- Vorsicht ist besser als Nachsicht – E-Mails erst verifizieren, bevor man Anhänge öffnet

02. Szenarien aus dem Alltag



KI-generiert mithilfe von chat.openai.com - Public Domain Mark

Szenario 3 – Webdienste & Passwörter

Situation

- Nutzung von Webanwendungen ist mit sogenannten Zugangsdaten abgesichert

Risiko / Gefahren

- Schwache Zugangsdaten ermöglichen
  - *Missbräuchliche Nutzung von Webdiensten (Auspionieren, Manipulieren)*
  - *Feindliche Accountübernahme*
- Riskante Passwörter
  - *Mehrfachverwendung, zu leichte Passwörter („Partei2022“), Zettel an Monitor, Teilen von Zugangsdaten*

Prävention / Lösung

- Passwortstärke erhöhen
  - *Mindestens 12 Zeichen, Mischung aus Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen*
  - *Passwortrichtlinien vereinbaren*
- Passwortmanager-Einführung
  - *Jede Webanwendung verwendet einzigartiges kompliziertes Passwort*
  - *Nur Master-Passwort merken, Rest wird automatisch generiert und gepflegt*
- 2-Faktor-Authentifizierung (2FA) oder Passkey

Lernpunkte & Diskussion

- Passwörter sind sehr sensibel. Webanwendungen sollten nur mit starken Zugangsdaten genutzt werden.

KI-generiert mithilfe von chat.openai.com - Public Domain Mark

Das Wichtigste - Hardware & Gerätepflege

- **Regelmäßige Updates:**
  - Aktuelle Betriebssysteme nutzen
  - Automatische Updates für Betriebssystem & Antivirus aktivieren (Windows 10/11, macOS, Linux, Android, iOS)
  - Firmware-Updates für WLAN-Router, NAS-Systeme
- **Backup-Strategie (3-2-1-Regel):**
  - Mindestens 3 Kopien: 1 Original + 2 Backups
  - 2 verschiedene Datenträger: externe HDD/SSD + Cloud-Dienst
  - 1 Backup an externem Ort (z. B. bei Mitglied zu Hause lagern)
- **Festplattenverschlüsselung:**
  - Windows: BitLocker aktivieren
  - Linux: LUKS-Verschlüsselung
  - macOS: FileVault
- **Geräte-Lifecycle-Management:**
  - Dokumentation: Kaufdatum, Modell, Zustand
  - Austauschplan: Gerät nach 5–7 Jahren austauschen

KI-generiert mithilfe von chat.openai.com - Public Domain Mark

Das Wichtigste - Software & Accounts

- **Passwortmanager + 2FA**
  - Kommerzielle oder OpenSource Lösungen
  - Sicherheitsschulungen, kurze Demo in der Gruppe
- **E-Mail & Verschlüsselung**
  - PGP oder S/MIME-Zertifikate
  - Interne Regel: Vertrauliche Infos nur verschlüsselt verschicken
- **Cloud-Dienste**
  - Vertrauenswürdige Anbieter (Europäische oder Deutsche Anbieter bevorzugen, DSGVO-konform)
  - Zugriffsrechte: Nur notwendige Personen mit Bearbeitungsrecht
- **Updates und Patches**
  - E-Mail-Infrastruktur immer auf aktuellem Stand halten
  - Regelmäßige Überprüfung mit IT-Verantwortlichen

KI-generiert mithilfe von chat.openai.com - Public Domain Mark

Das Wichtigste - Verhalten & Awareness

- **Phishing erkennen & melden**
  - Sensibilisieren für Phishing-Mails
  - Interner Prozess: Verdächtige Mails an Technikbeauftragte weiterleiten
- **Social Engineering reduzieren**
  - Keine sensiblen Infos am Telefon oder Chat herausgeben
  - Identitätsprüfung: Rückruf unter bekannten Telefonnummern
- **Kommunikationsregeln**
  - Kein ungeprüftes Teilen von Links in Social-Media-Kanälen
  - Nur lizenzierte Tools für Videokonferenzen (keine unbekannten Web-Tools)
- **Konsequente Rechtevergabe**
  - Nur autorisierte Personen haben Admin-Rechte in Cloud & E-Mail-System
  - Rollen- und Aufgabenverteilung: Wer darf was? Wer ändert welche Passwörter?
- **Eigene Reflektion, Inhalte hinterfragen**

KI-generiert mithilfe von chat.openai.com - Public Domain Mark

Fragen und Antwortrunde

Vielen Dank für Ihre Aufmerksamkeit!

Referat I13 - Umsetzungsberatung in digitalisierten Verwaltungsleistungen, Justiz und Politik

sicherheitsberatung-politik@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn

www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us: