Workshop IT-Sicherheit

Wie schütze ich meine Daten richtig?

Become a human firewall!

Agenda

1. Begriffsklärung
2. Verantwortliche Parteien
3. Maßnahmen zur Steigerung der IT-Sicherheit
4. Alice in IT Wonderland

Fragen über Fragen.

Wie wichtig ist für Sie der Schutz und die Sicherheit ihrer Daten?

Wie schützen Sie ihre Daten? Privat & geschäftlich.

Was verstehen Sie unter den Begriffen Datensicherheit und Datenschutz?

Warum diese Veranstaltung?

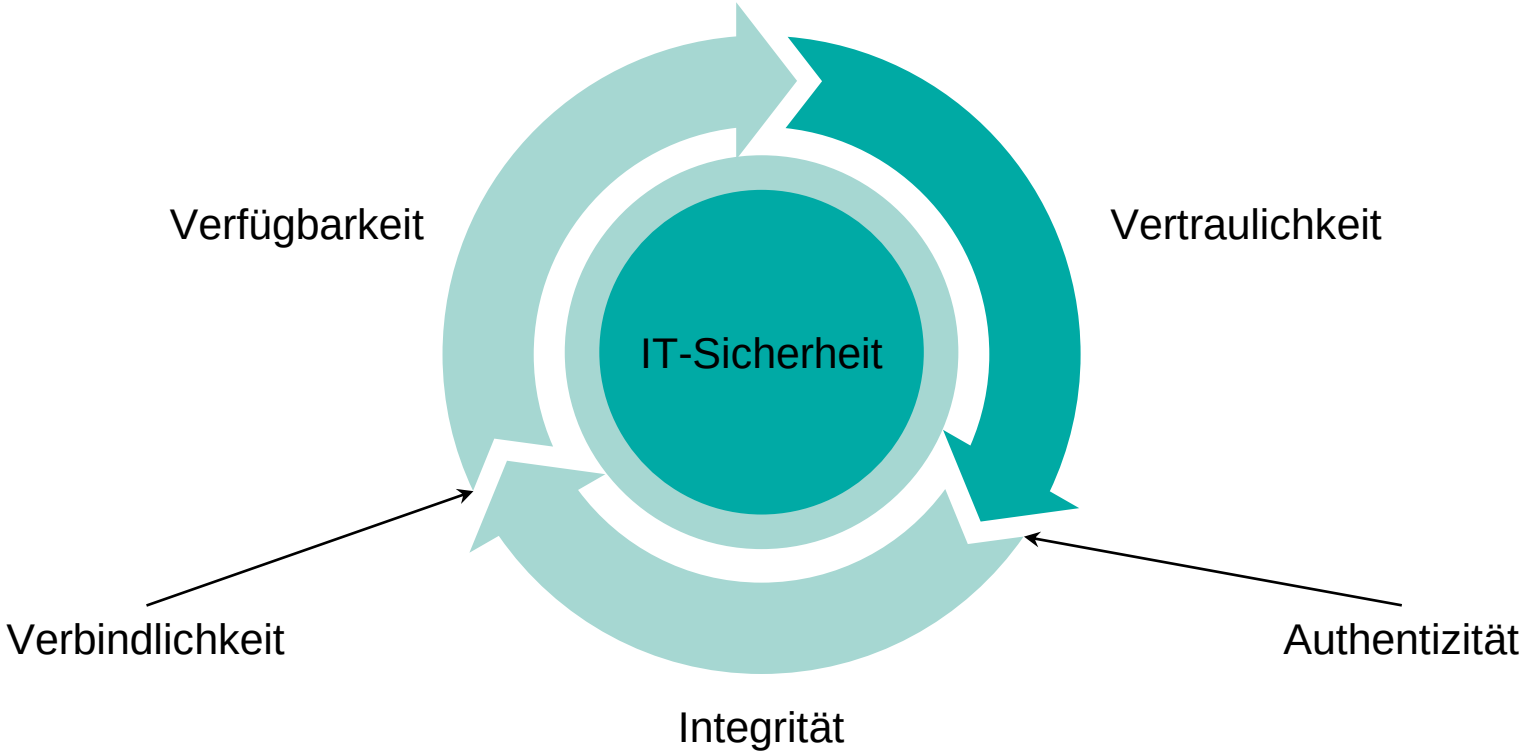
Was sind Ihre Erwartungen an den Workshop?

Begriffsklärung

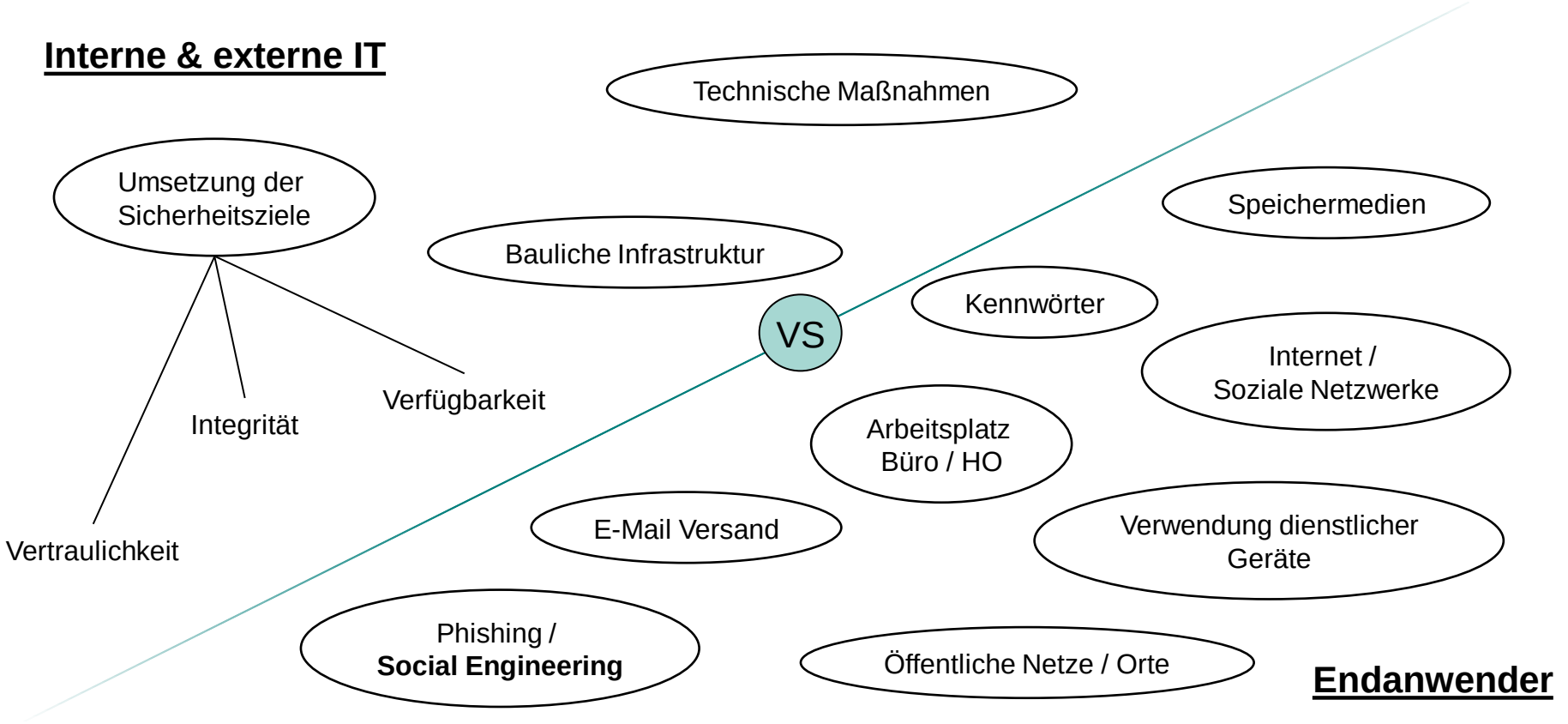
Datensicherheit	Datenschutz
■ Technische Maßnahmen ■ Schutz vor Verlust, Missbrauch, Zerstörung & Zugriff durch Unbefugte ■ Umsetzung von Sicherheitszielen → Vertraulichkeit, Integrität und Verfügbarkeit.	■ Schutz von *personenbezogenen* Daten ■ Schutz vor „Datenpannen“ & Missbrauch □ Grundsatz der Zweckbindung □ Grundsatz der Datensparsamkeit ■ Umsetzung gesetzlicher Vorschriften

Datensicherheit ≠ Datenschutz

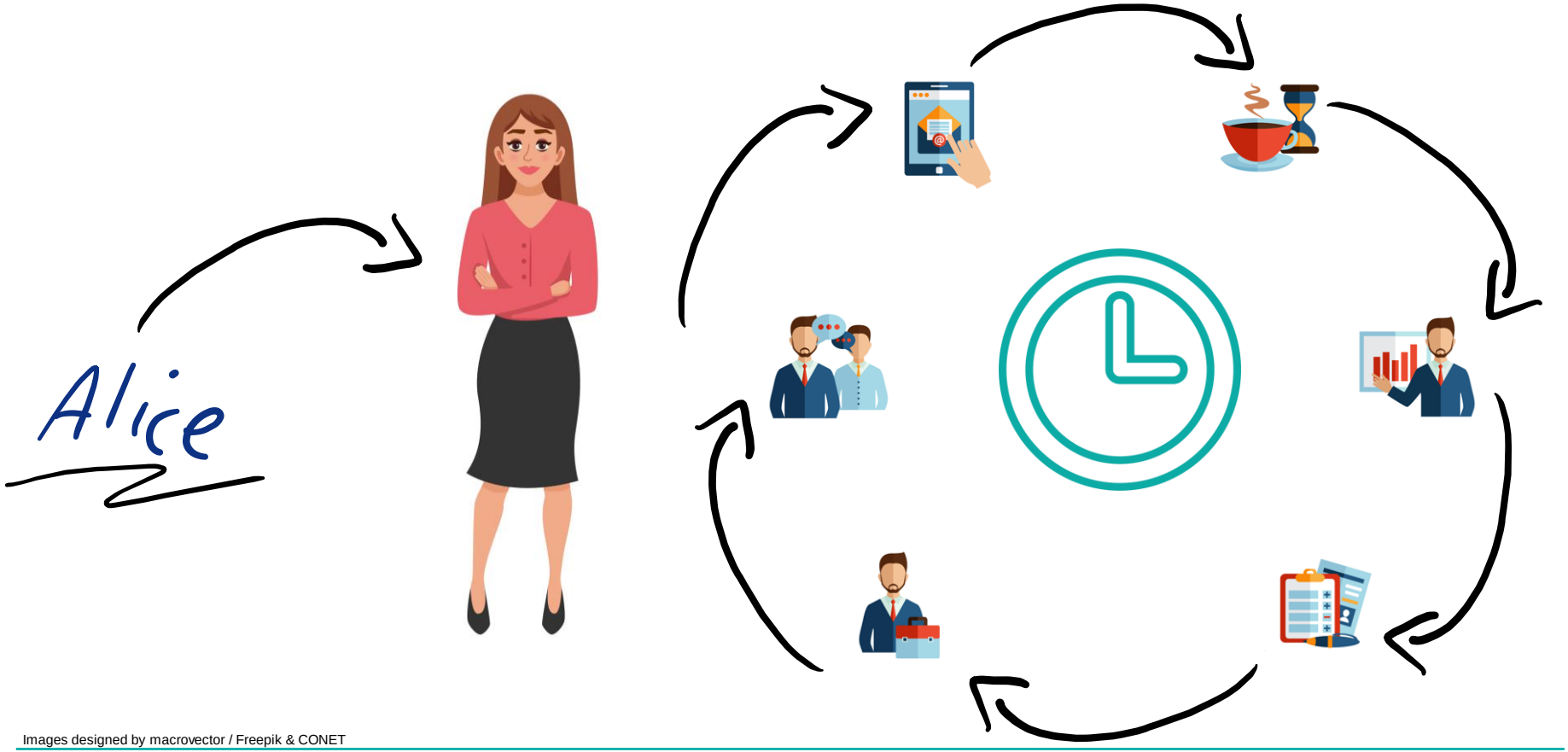
Begriffsklärung



Verantwortliche Parteien

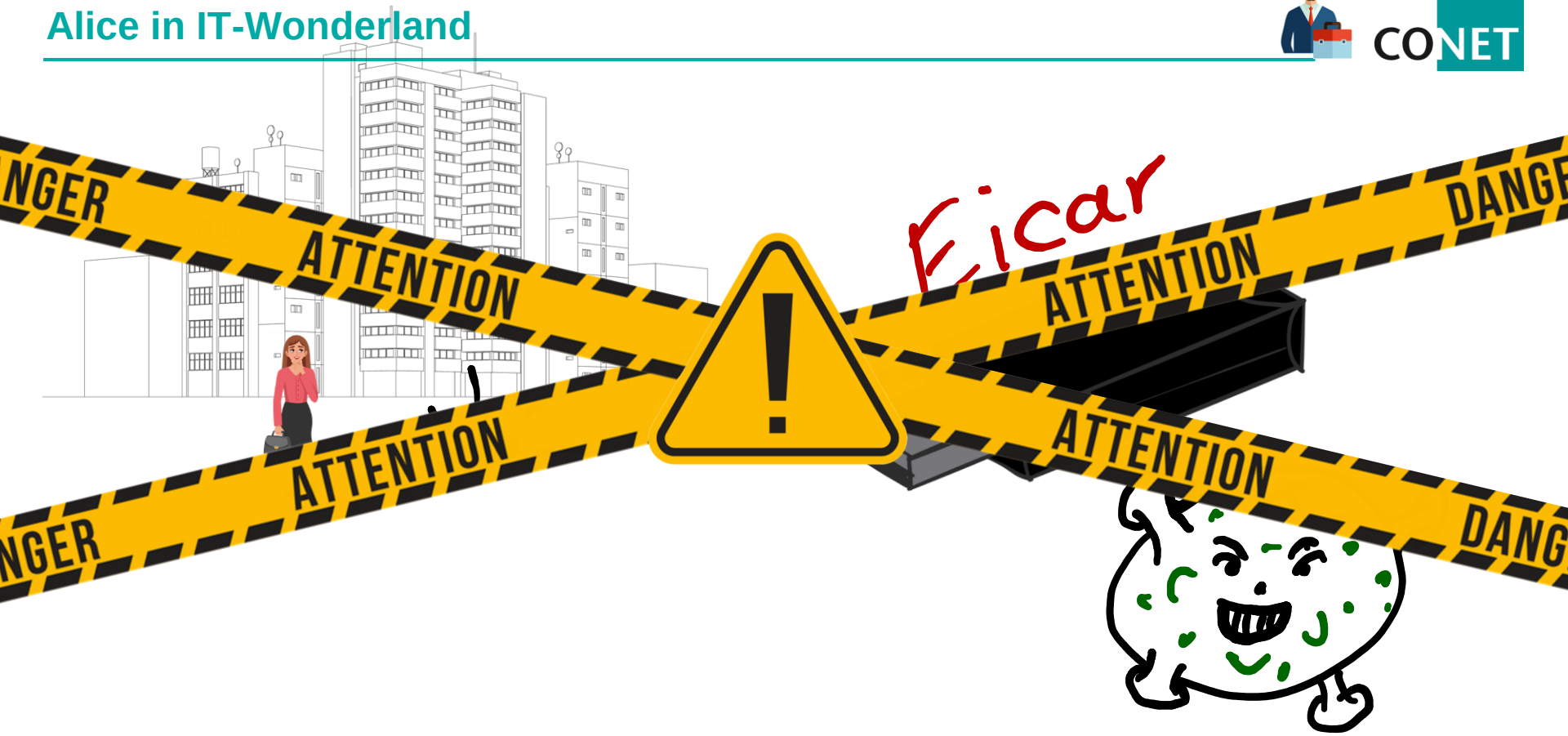


Alice in IT-Wonderland



Images designed by macrovector / Freepik & CONET

Alice in IT-Wonderland



Images designed by macrovector, macrovector_official, pch.vector & rocketpixel / Freepik

Maßnahmen zur Steigerung der IT-Sicherheit

Externe Speichermedien (USB-Sticks, SD-Karten, etc.)

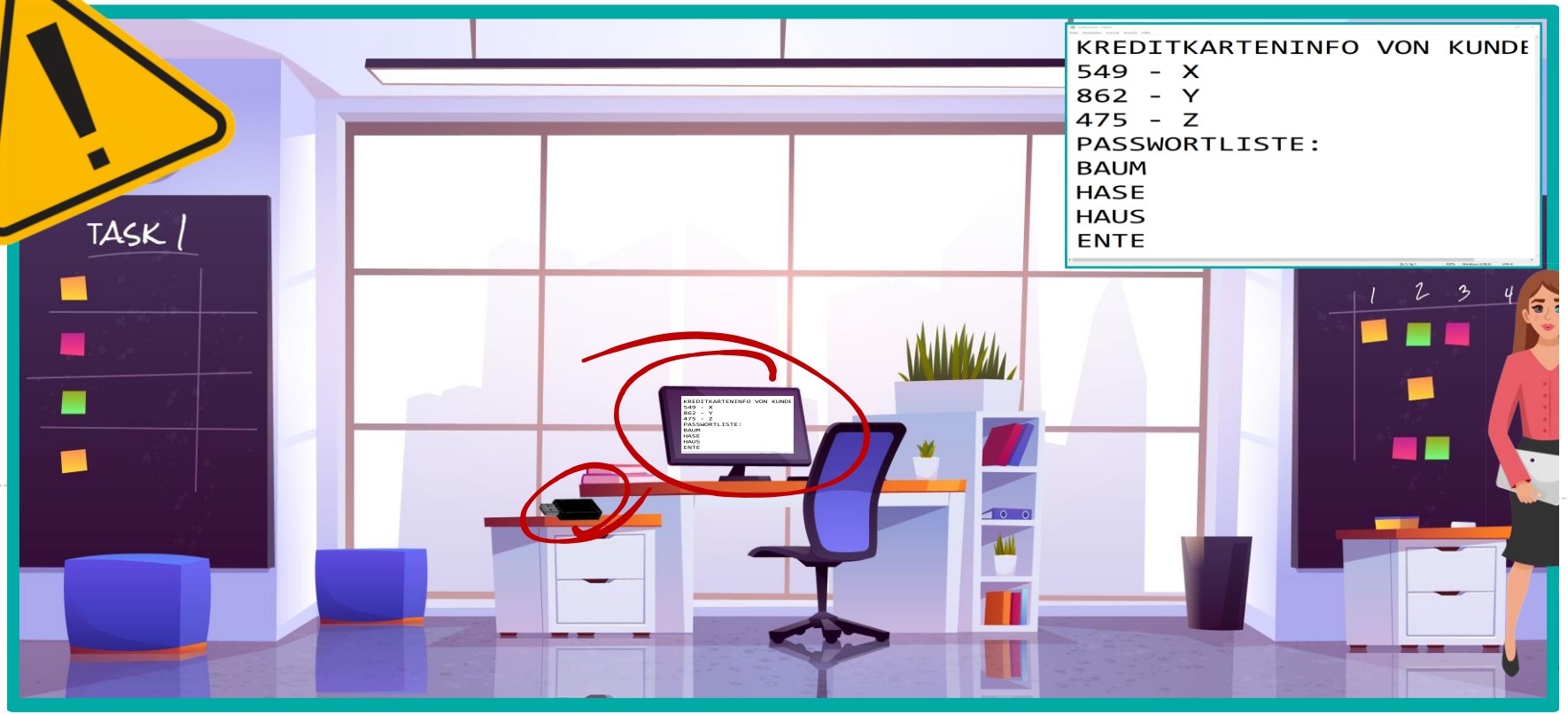
- Bei vertraulichen Daten nur verschlüsselte Speichermedien verwenden
- Keine fremden / gefundenen Speichermedien verwenden
- Speichermedien nur gemäß Firmenanweisung nutzen
  → nur Speichermedien des VÖB nutzen

Maßnahmen zur Steigerung der IT-Sicherheit

Drittanbieter-Software und ihre Verwendung

- Software nur aus vertrauenswürdigen Quellen herunterladen & installieren
- Sicherheit-Warnungen ernst nehmen

Alice in IT-Wonderland



Images designed by macrovector & pch.vector / Freepik & CONET

Maßnahmen zur Steigerung der IT-Sicherheit

Büro Arbeitsplatz

- Clean-Desk-Ansatz
- Sensible Unterlagen verschlossen halten
  → alle Dokumente unlesbar auf dem Tisch lagern
- Desktop bei Abwesenheit stets sperren
- Türen und Fenster beim Verlassen des Raums schließen

Maßnahmen zur Steigerung der IT-Sicherheit

Internet & Soziale Medien

- Passwörter nicht im Browser speichern
- Zertifikatswarnungen ernst nehmen
- Privates Surfen am Arbeitsplatz im geringen Rahmen erlaubt
  → Vorsicht vor unbekannten Links, Werbebannern
- Soziale Medien im privaten Umfeld


+ ? =
pause

Alice in IT-Wonderland

Images designed by macrovector & pch.vector / Freepik

Maßnahmen zur Steigerung der IT-Sicherheit

E-Mail Versand & Phishing

- Keine Weiterleitung an private E-Mail Adressen
  → Ungesicherter Datentransport & Ablage auf ungesicherten Geräten / Servern
- Phishing E-Mails technisch nur schwer erkennbar
  → Erkennungsmechanismen

Maßnahmen zur Steigerung der IT-Sicherheit

Öffentliche Orte & Netze

- Öffentliche Netze / WLANs mit Vorsicht nutzen
  - VPN Verbindung zeitnah starten
  - Besser LTE nutzen
- Wer hört und liest mit?
- Sichtschutzfolien verwenden
- Nicht an öffentlichen USB-Schnittstellen laden
  → Vorsicht vor Datenabfluss (USB-Filter)

Maßnahmen zur Steigerung der IT-Sicherheit

Smartphone Nutzung #1

- Private Nutzung kurzfristig zulässig
- Nutzung im Ausland gestattet
  → Bei IT anmelden
  → Datenroaming beachten
- Die Sache mit den „Apps“
  → Keine Spiele
- Keine Kopplung mit privaten Endgeräten
- Keine Synchronisation mit Cloud-Diensten
  → Dropbox, iCloud etc.

Maßnahmen zur Steigerung der IT-Sicherheit

Smartphone Nutzung #2

- PIN oder biometrische Absicherung
- Bei Ablage des Smartphones
  - Display immer nach unten legen
  - Display sperren
  - Niemals entsperrt ablegen
- Stets aktuellste Updates zeitnah installieren

Deep Dive - Mobile Application Management (MAM)

Deep Dive – Mobile Application Management (MAM)

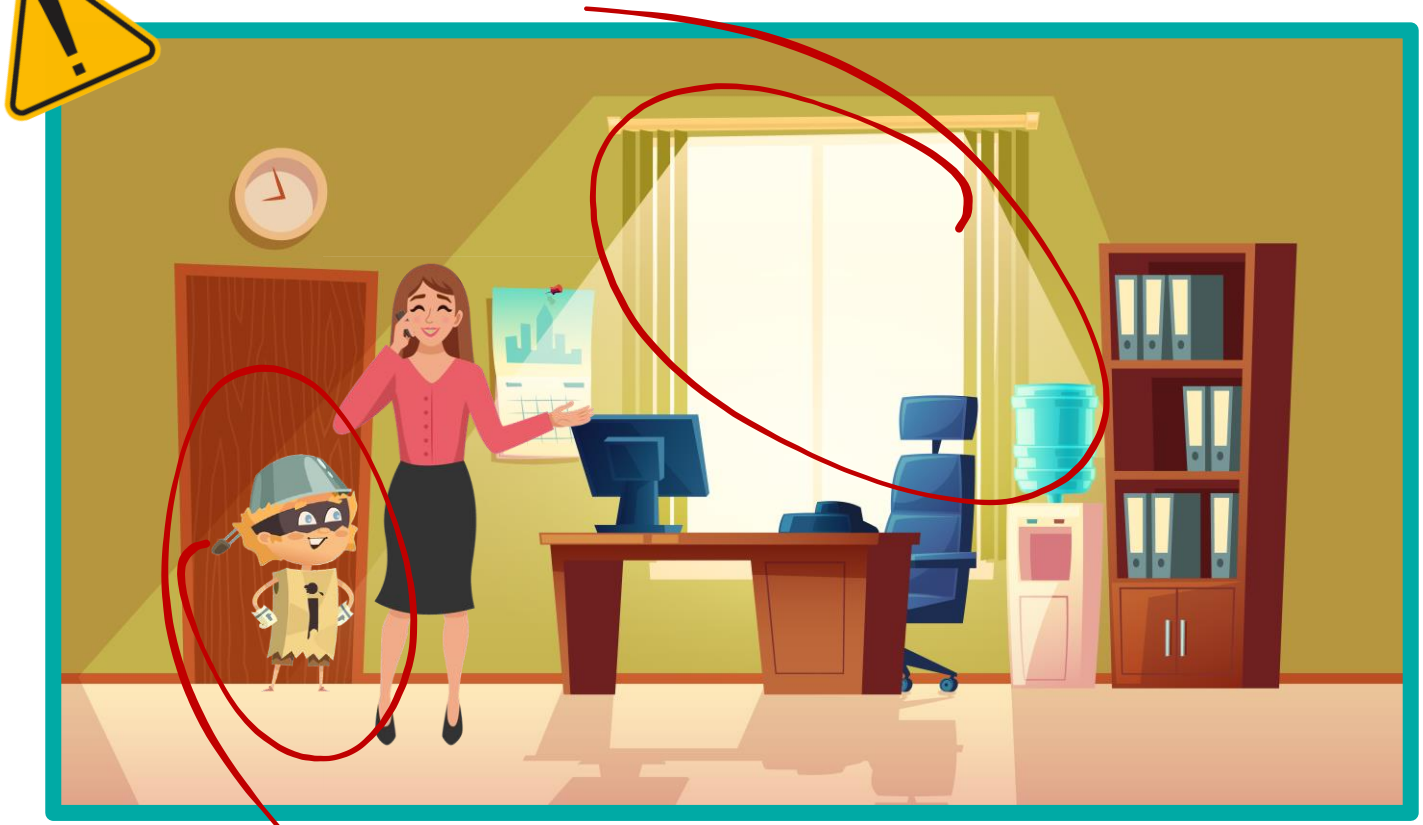
- Voraussetzung
  - Microsoft Outlook E-Mail-App
  - Microsoft Authenticator
  - (Bei Android aus technischen Gründen zusätzlich das Microsoft Unternehmensportal)
- Verschlüsselter Container um MS-Outlook
- Ausschließlich Verwaltung dieser App
- KEIN Zugriff außerhalb dieser App durch die VÖB-IT möglich, insbesondere KEINE Ortungsdienste
- Private Daten zu 100% separiert

Deep Dive – Managed Apple IDs

- Erstellung privater Apple-IDs für Firmengeräte entfällt künftig
- „Managed Apple ID“ wird in Zukunft vom Unternehmen gestellt
  - Erhöhung der Sicherheit
  - Verbesserung der Verwaltung der dienstlichen Endgeräte
  - Verknüpfung mit dem Microsoft-Account
    → Mitarbeiter loggt sich mit seinen Microsoft-Anmeldeinformationen bei Apple an
  - Vereinfachter Einrichtungs- und Rückgabeprozess für Endnutzer und IT

!
- Sollte die Firmen-Email-Adresse @voeb.de bereits für eine private Apple-ID genutzt werden, muss hier eine Umstellung erfolgen.
  → Wir werden Sie bei der Umstellung unterstützen und dazu auf Sie zukommen.

Alice in IT-Wonderland



Images designed by macrovector & pch.vector / Freepik

Maßnahmen zur Steigerung der IT-Sicherheit

Arbeiten im Homeoffice

- Wer hört und liest mit?
  - Telefonate nur an geschützten (geschlossenen) Orten
  - Behutsam mit vertraulichen Informationen umgehen

Maßnahmen zur Steigerung der IT-Sicherheit

Verwendung dienstlicher Endgeräte

- Nicht an Kinder weitergeben
- Keine Spiele-Apps installieren
- Bei Auslandsreisen das Gerät im ausgeschalteten Zustand transportieren
  → Daten sind somit verschlüsselt
- Bei Dienstreisen das Gerät immer bei sich führen, oder verschlossen halten

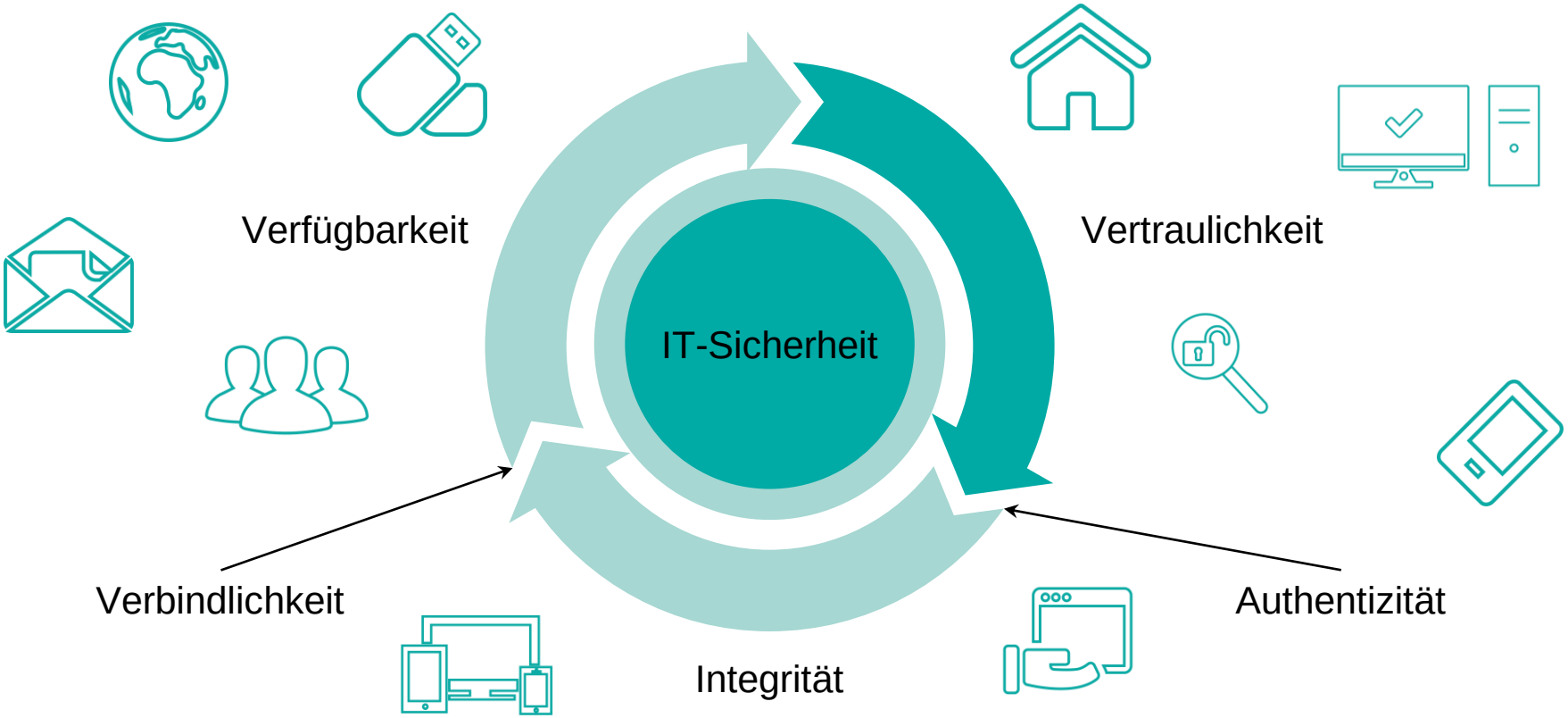
Maßnahmen zur Steigerung der IT-Sicherheit

Kennwörter

- Privat und dienstlich wichtig
- Hohe Komplexität
- Niemals auf Papier aufschreiben
- Ablage innerhalb gesicherter, geeigneter Kennwort-Safes
- **Zukünftig**: Moderne Anmeldeverfahren (Windows Hello for Business)

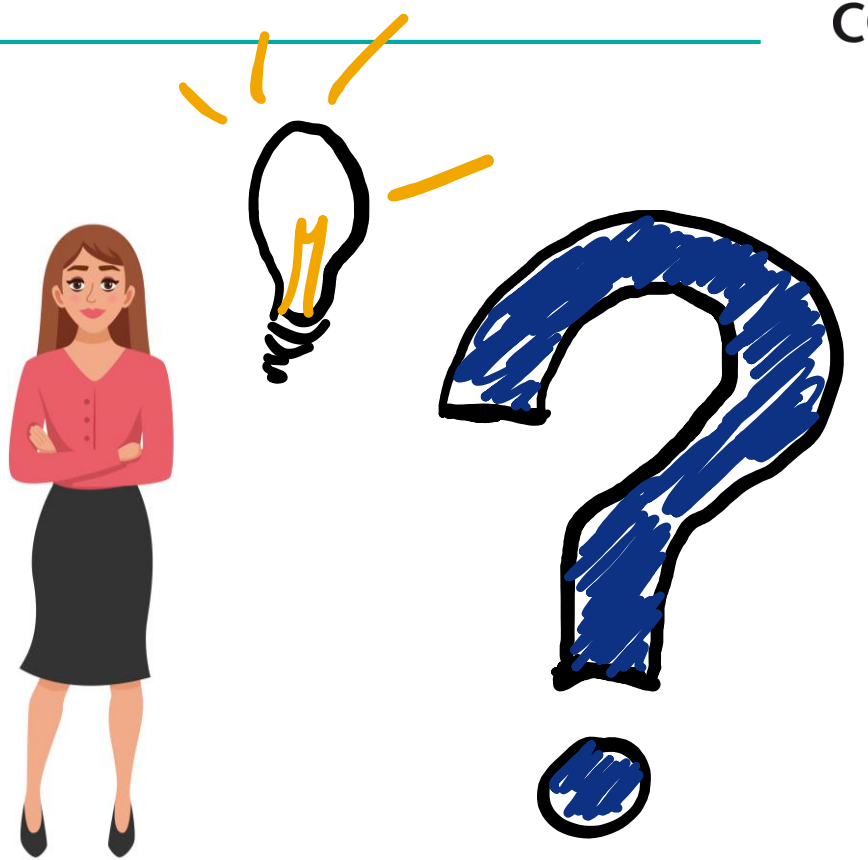
Kennwörter niemals weitergeben!

Maßnahmen zur Steigerung der IT-Sicherheit



Alice in IT-Wonderland

Was würde Alice machen?



Vielen Dank für Ihre Aufmerksamkeit!

Kevin, Jung ▪ Junior Consultant ▪ +49 2242 939-739 ▪ kjung@conet.de
CONET Solutions GmbH ▪ Theodor-Heuss-Allee 19 ▪ 53773 Hennef