Vertrauen ist gut

Zero Trust ist besser

Alles beginnt mit einer Information

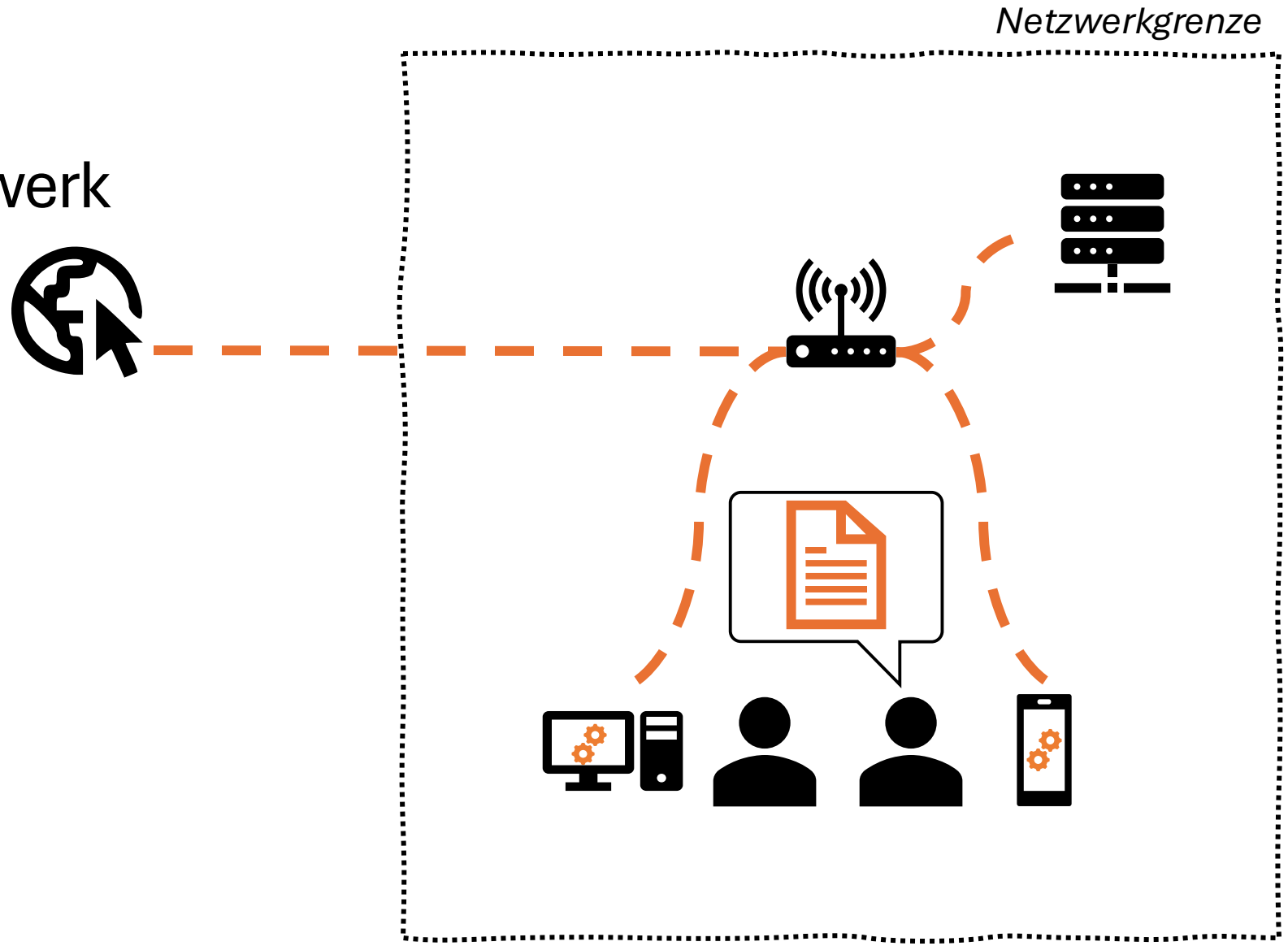
- Geschäftskritisch
- Persönlich

➔ vertraulich

➔ schützenswert

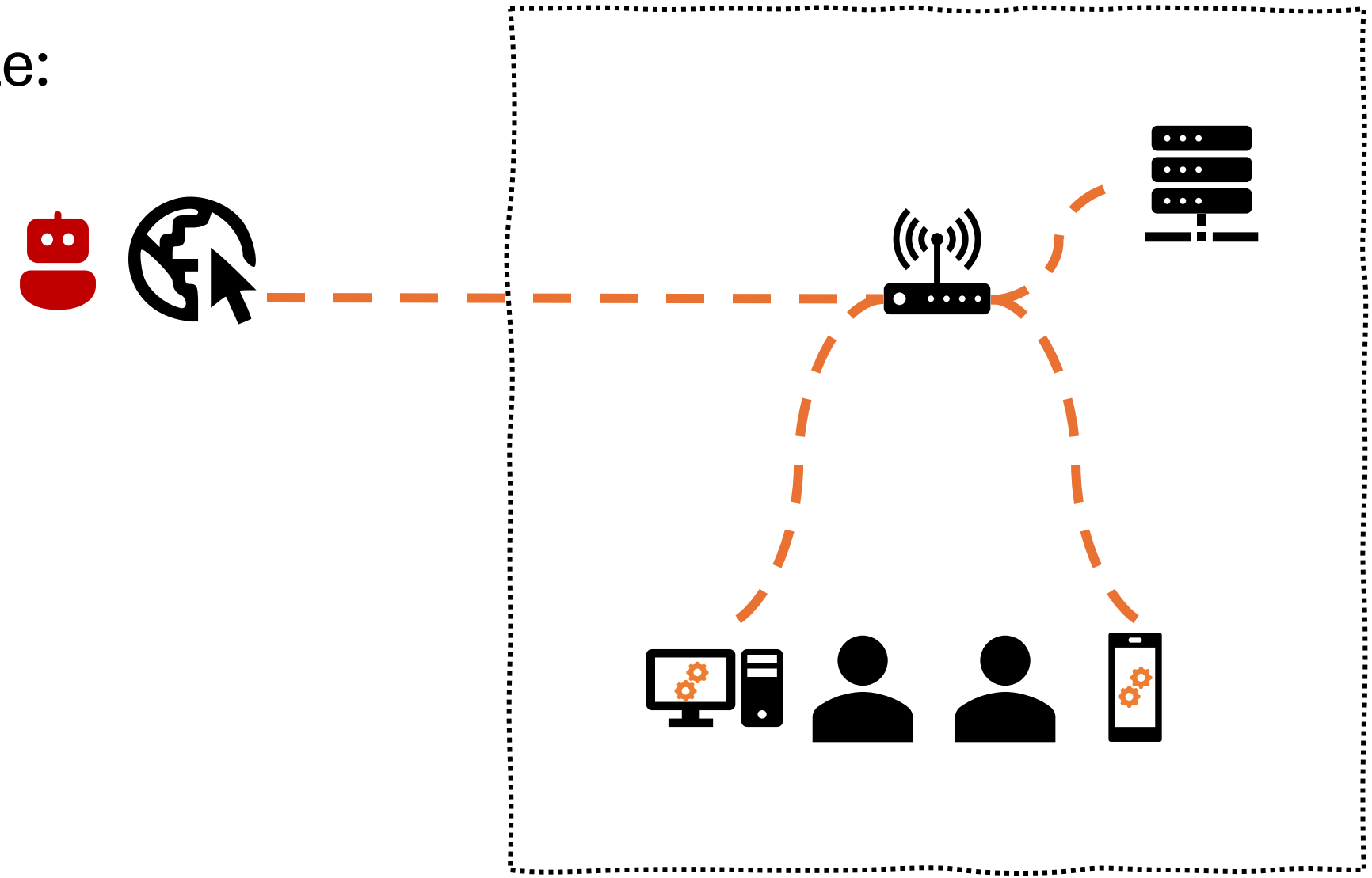
Teilnehmer im Informationsnetzwerk

- Personen
- Geräte
- Anwendungen



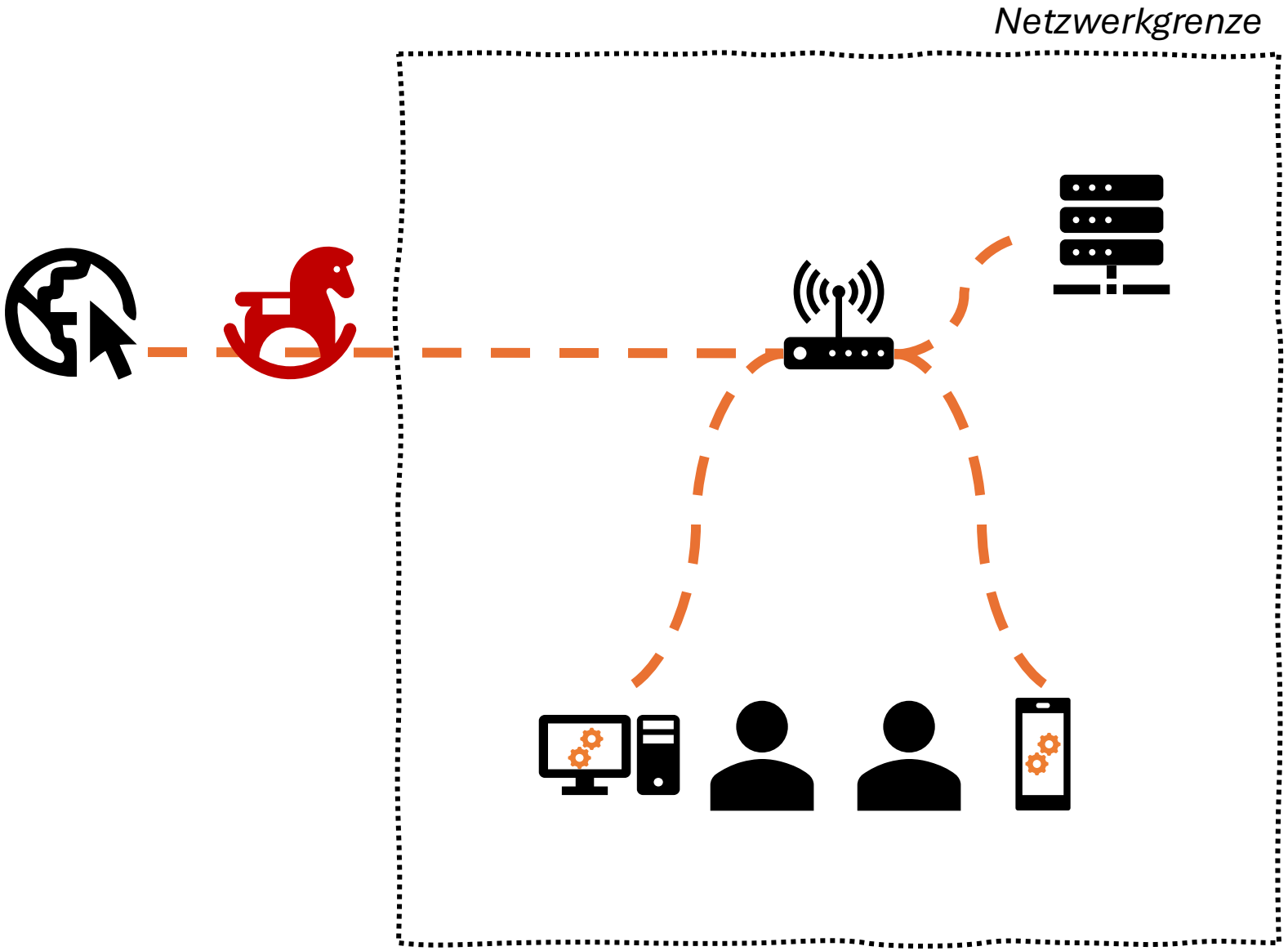
Schwachstelle: Vertrauen

- Bot-Angriffe



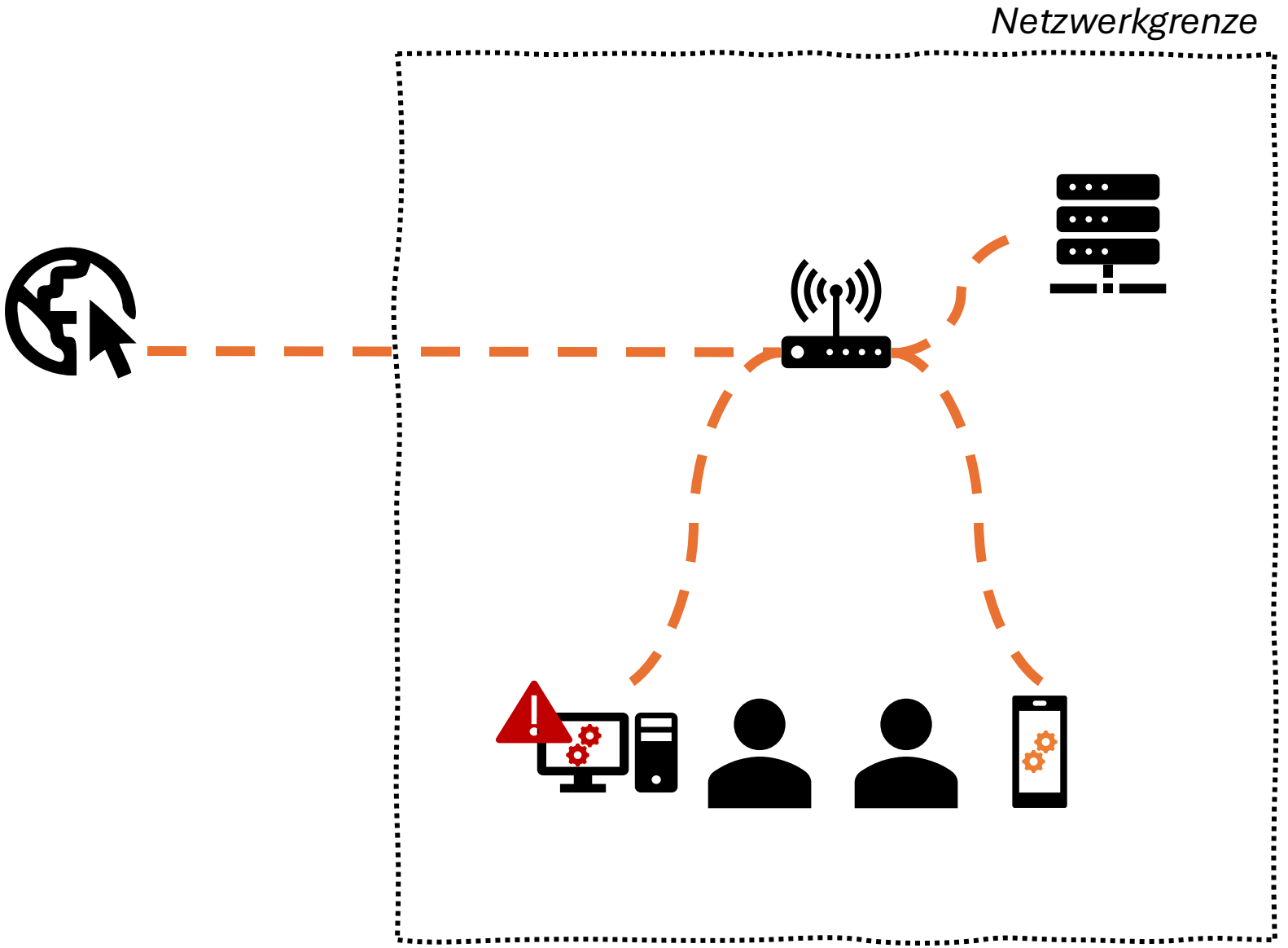
Schwachstelle: Vertrauen

- Bot-Angriffe
- Direkte Malware-Verteilung



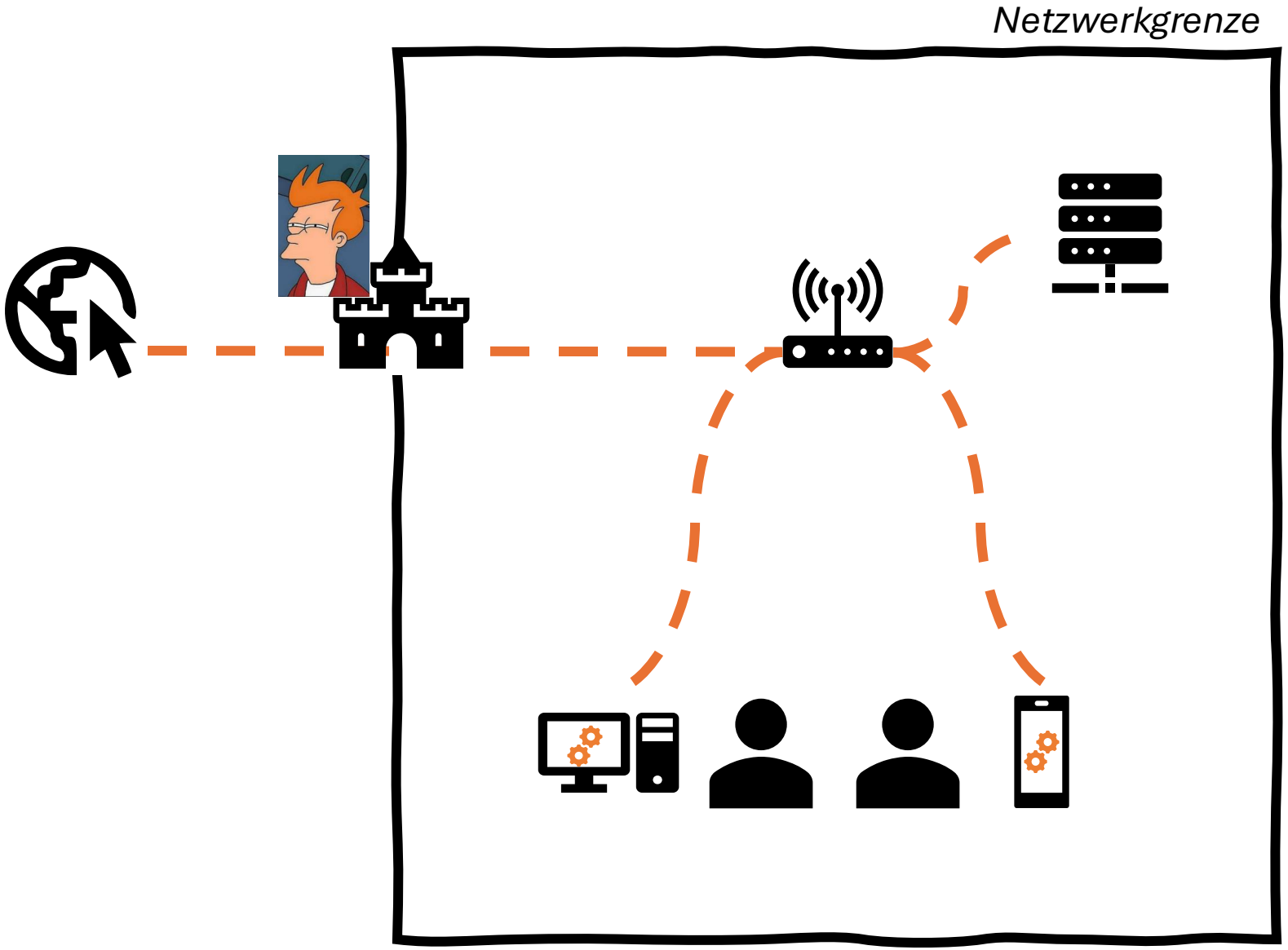
Schwachstelle: Vertrauen

- Bot-Angriffe
- Direkte Malware-Verteilung
- Ausnutzung bekannter Sicherheitslücken



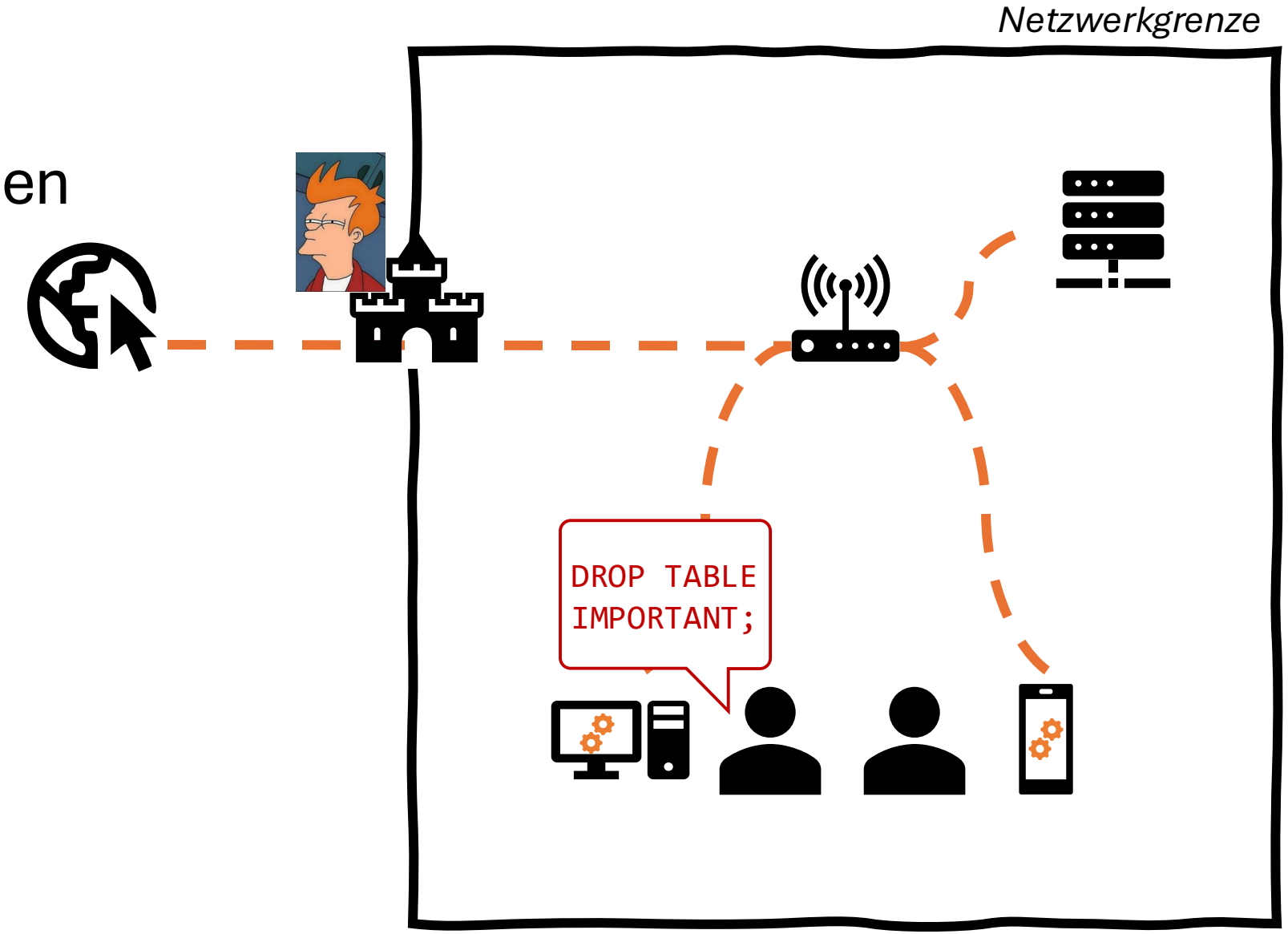
Die digitale Festungsmauer

- Abschirmung vom offenen Internet
- Zugangskontrolle
- Angriffserkennung
- Prüfung von Datenabflüssen



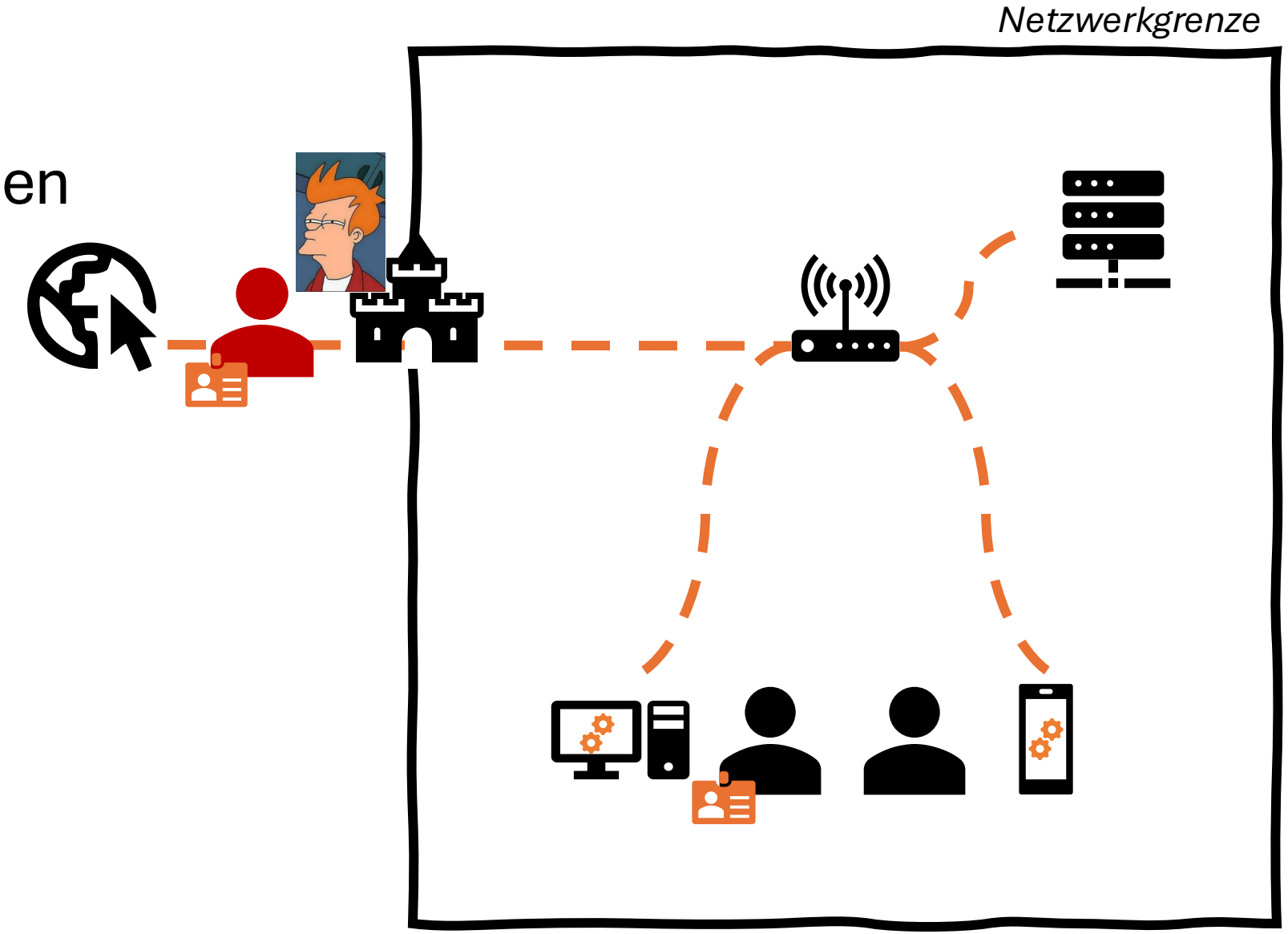
Schwachstelle: *implizites* Vertrauen

- Insider-Bedrohungen



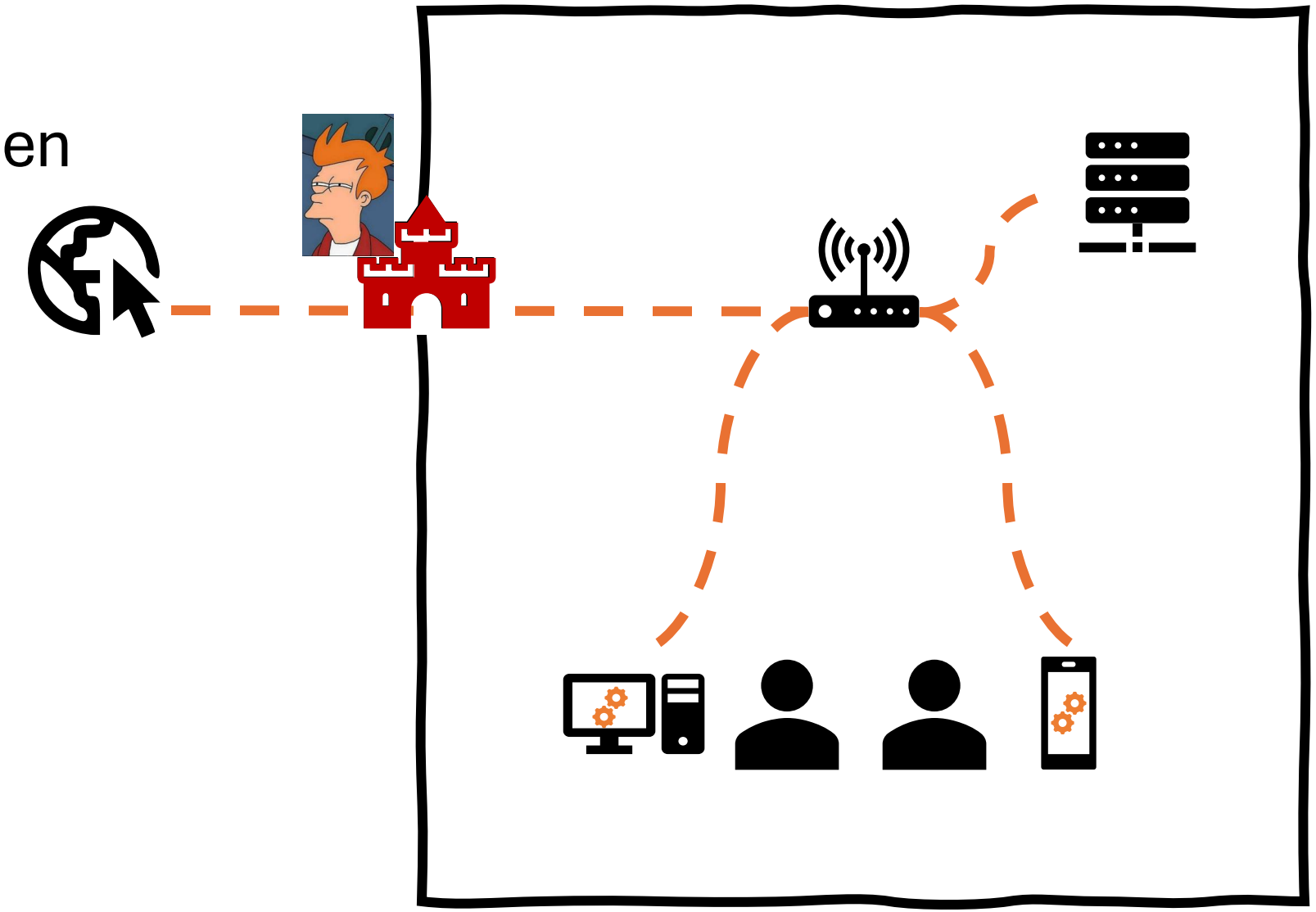
Schwachstelle: *implizites* Vertrauen

- Insider-Bedrohungen
- Gestohlene Zugangsdaten



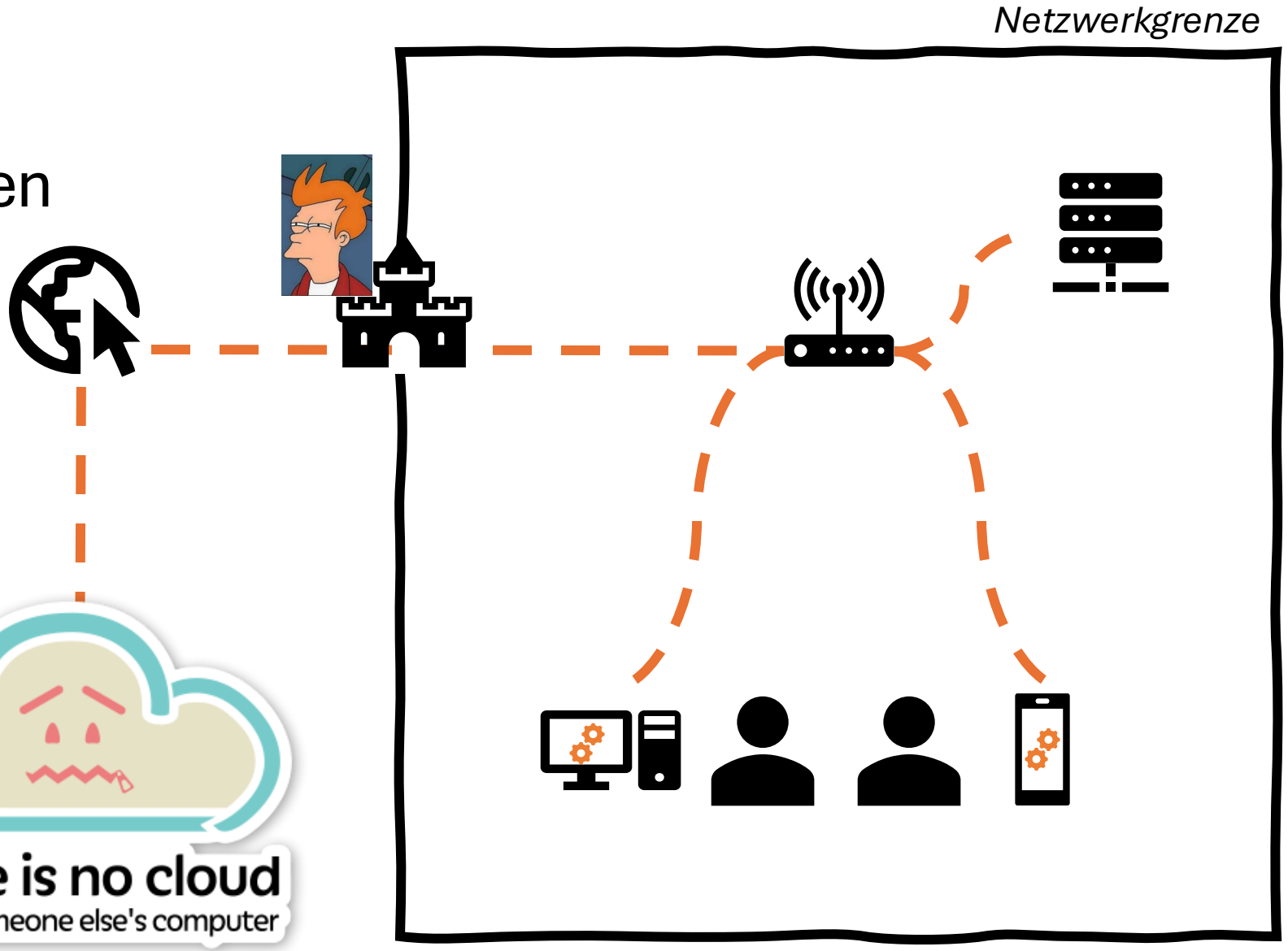
Schwachstelle: *implizites* Vertrauen

- Insider-Bedrohungen
- Gestohlene Zugangsdaten
- Fehlkonfiguration



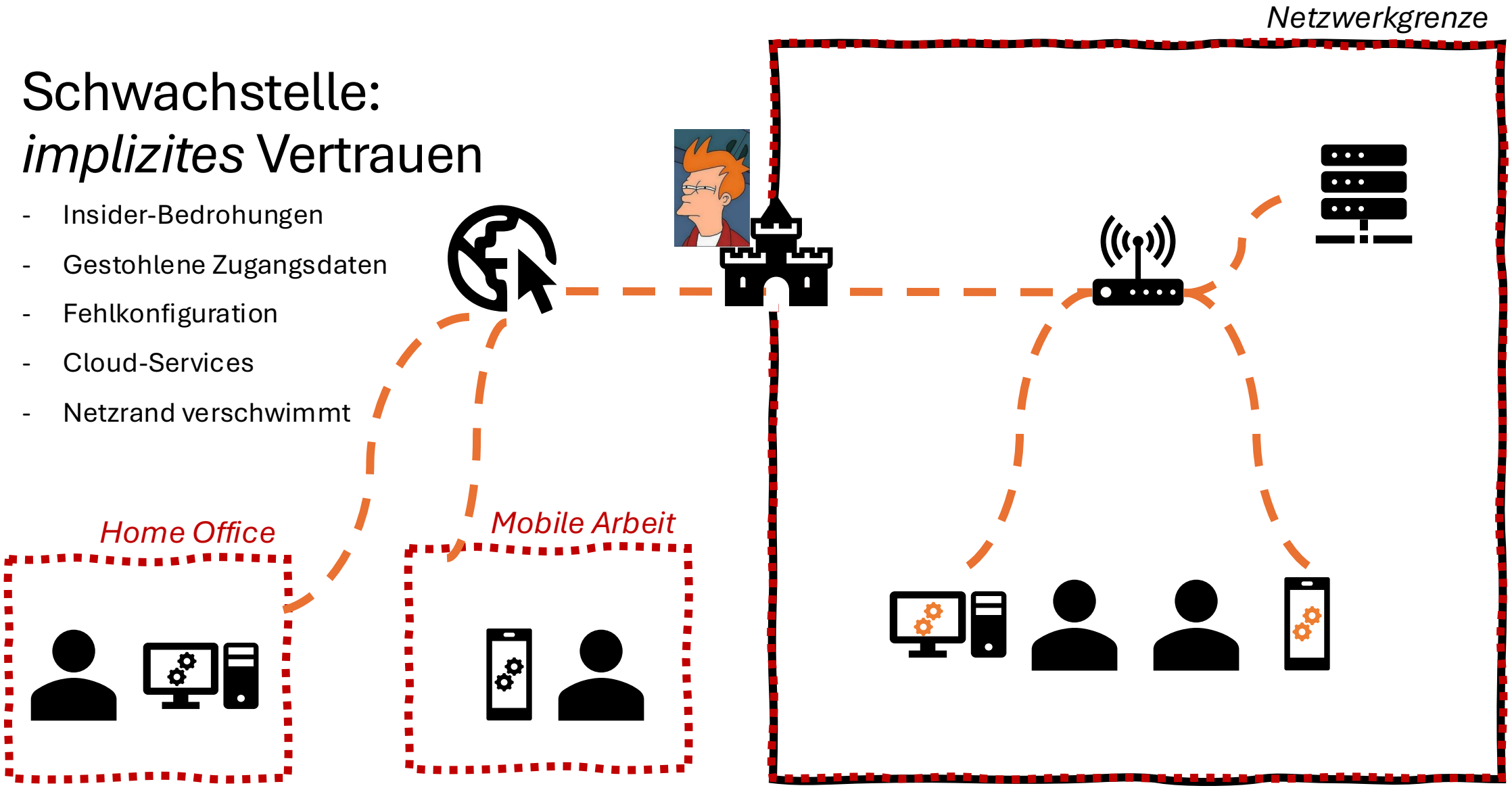
Schwachstelle: *implizites* Vertrauen

- Insider-Bedrohungen
- Gestohlene Zugangsdaten
- Fehlkonfiguration
- Cloud-Services



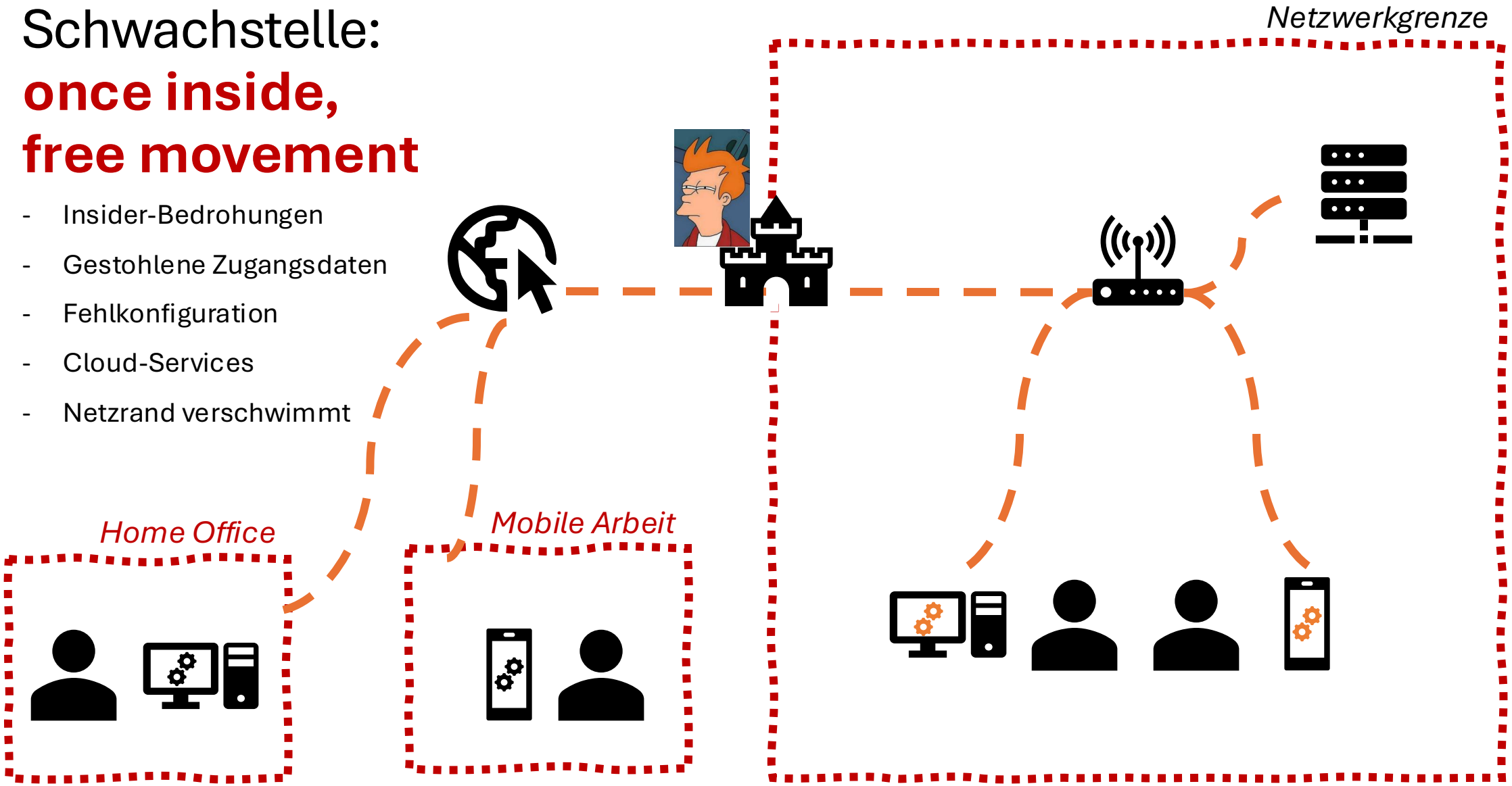
Schwachstelle: *implizites* Vertrauen

- Insider-Bedrohungen
- Gestohlene Zugangsdaten
- Fehlkonfiguration
- Cloud-Services
- Netzrand verschwimmt

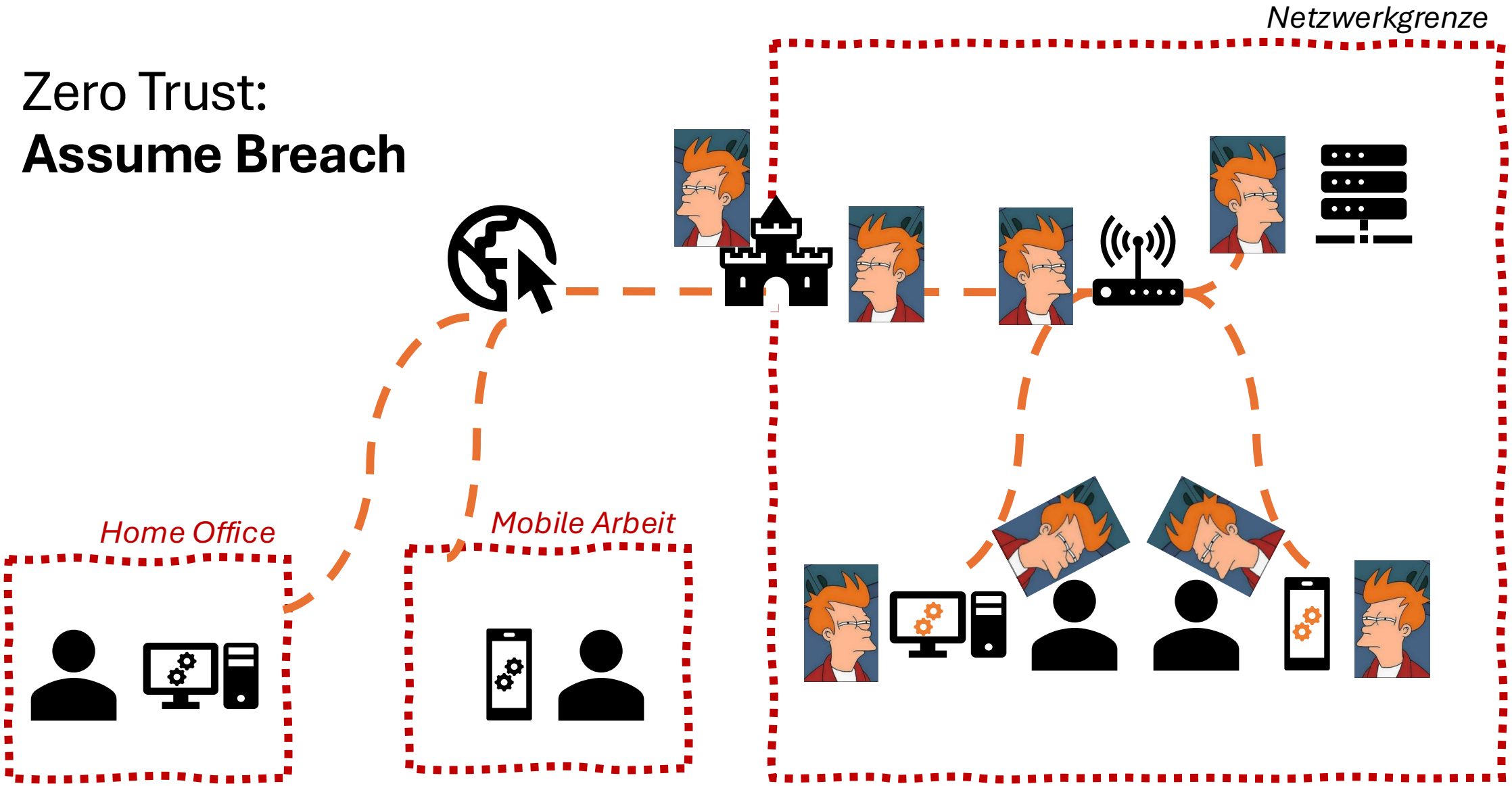


Schwachstelle:
once inside, free movement

- Insider-Bedrohungen
- Gestohlene Zugangsdaten
- Fehlkonfiguration
- Cloud-Services
- Netzrand verschwimmt

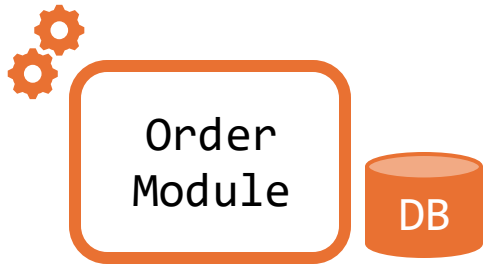


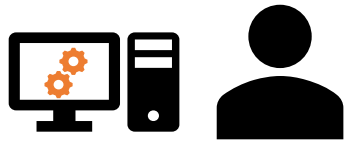
Zero Trust:
Assume Breach

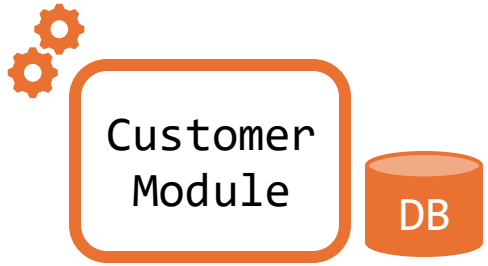


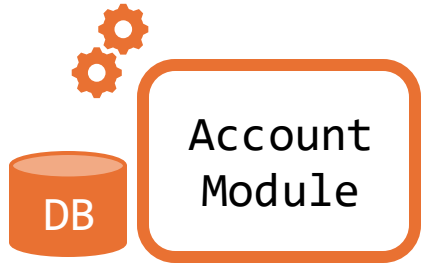
Zero Trust: **Anwendungen**

- *Modularisierung und Datentrennung*



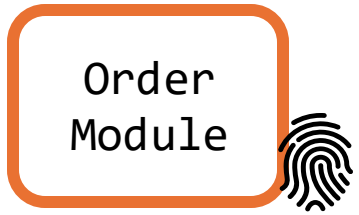


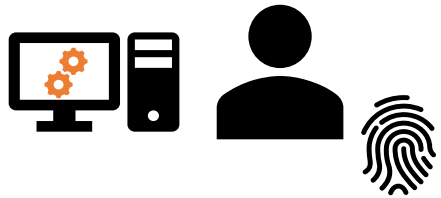


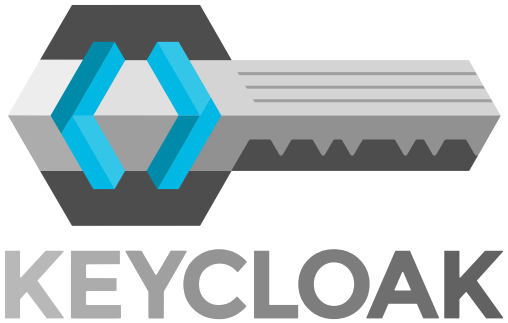


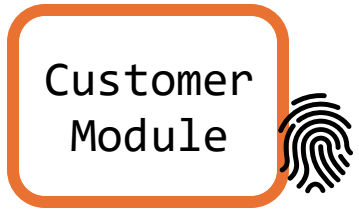
Zero Trust: **Anwendungen**

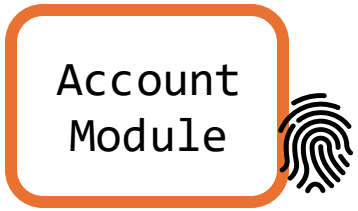
- *Modularisierung und Datentrennung*
- Identity Management
  - Identity Provider
  - Phishing-sichere Multi-Faktor-Authentifizierung (z.B. Passkeys)
  - Service-Identitäten (statt Shared Secrets)





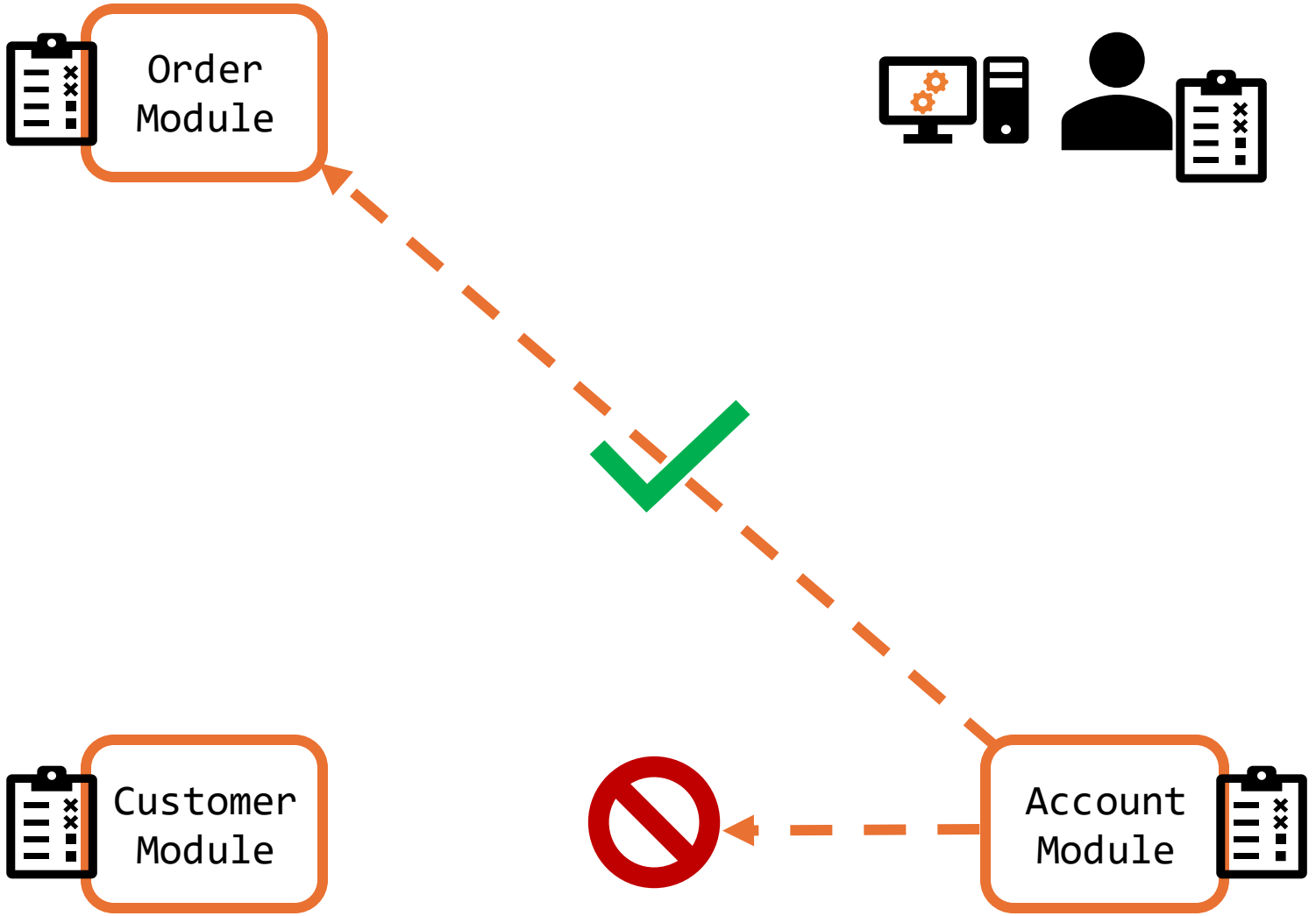






Zero Trust: **Anwendungen**

- *Modularisierung und Datentrennung*
- Identity Management
  - Identity Provider
  - Phishing-sichere Multi-Faktor-Authentifizierung (z.B. Passkeys)
  - Service-Identitäten (statt Shared Secrets)
- Access Management
  - Deny by default
  - Least Privilege
  - Audit-Logs

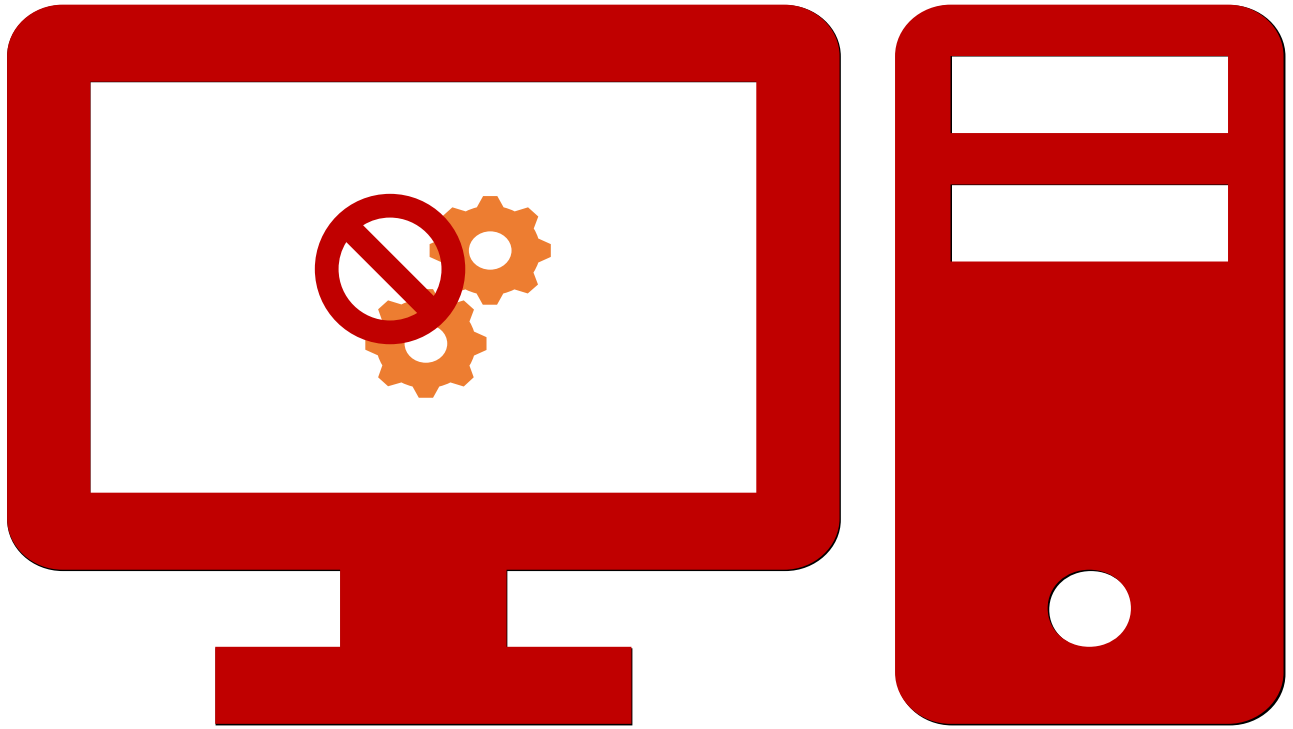


Zero Trust:
Geräte

- Device Identity & Conditional Access
  - Geräte-Registrierung
  - Zugriff abhängig vom Sicherheitszustand

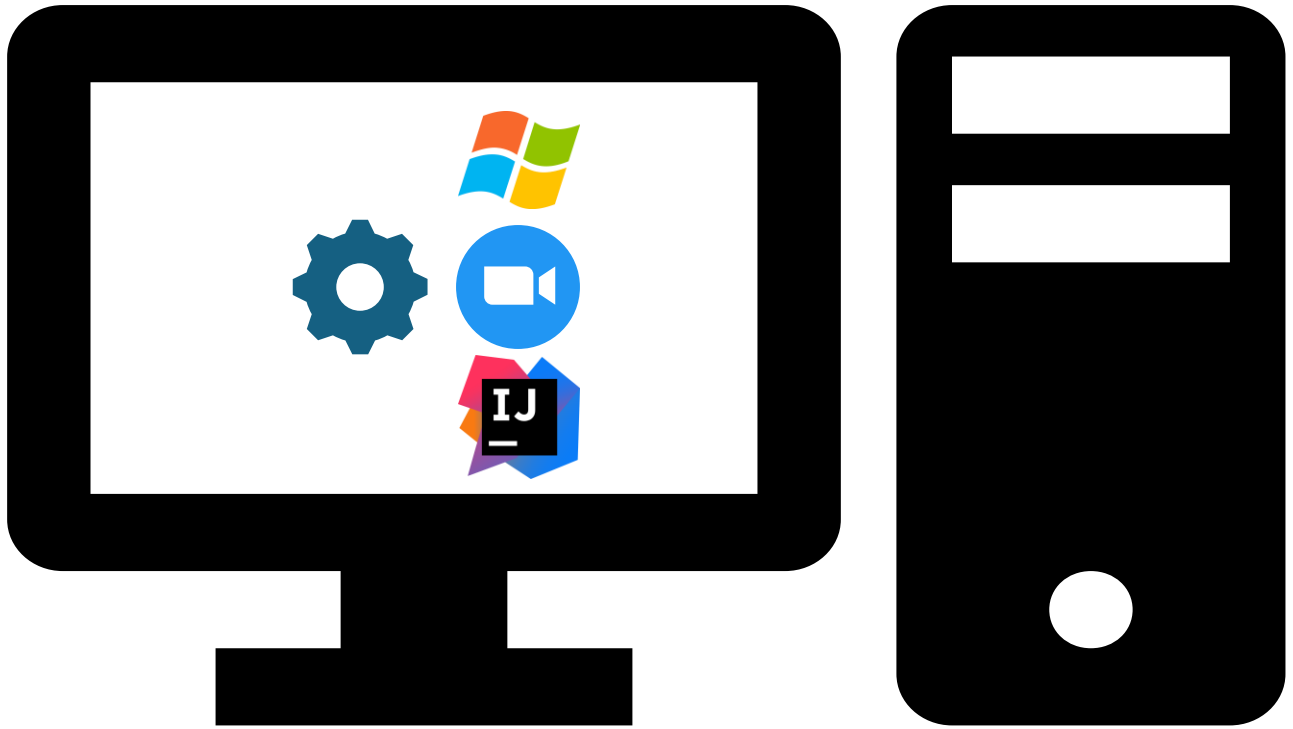
Zero Trust:
Geräte

- Device Identity & Conditional Access
  - Geräte-Registrierung
  - Zugriff abhängig vom Sicherheitszustand
  - Kein Zugriff für unbekannte bzw. unsichere Geräte
  - Device Isolation in Verdachtsfällen



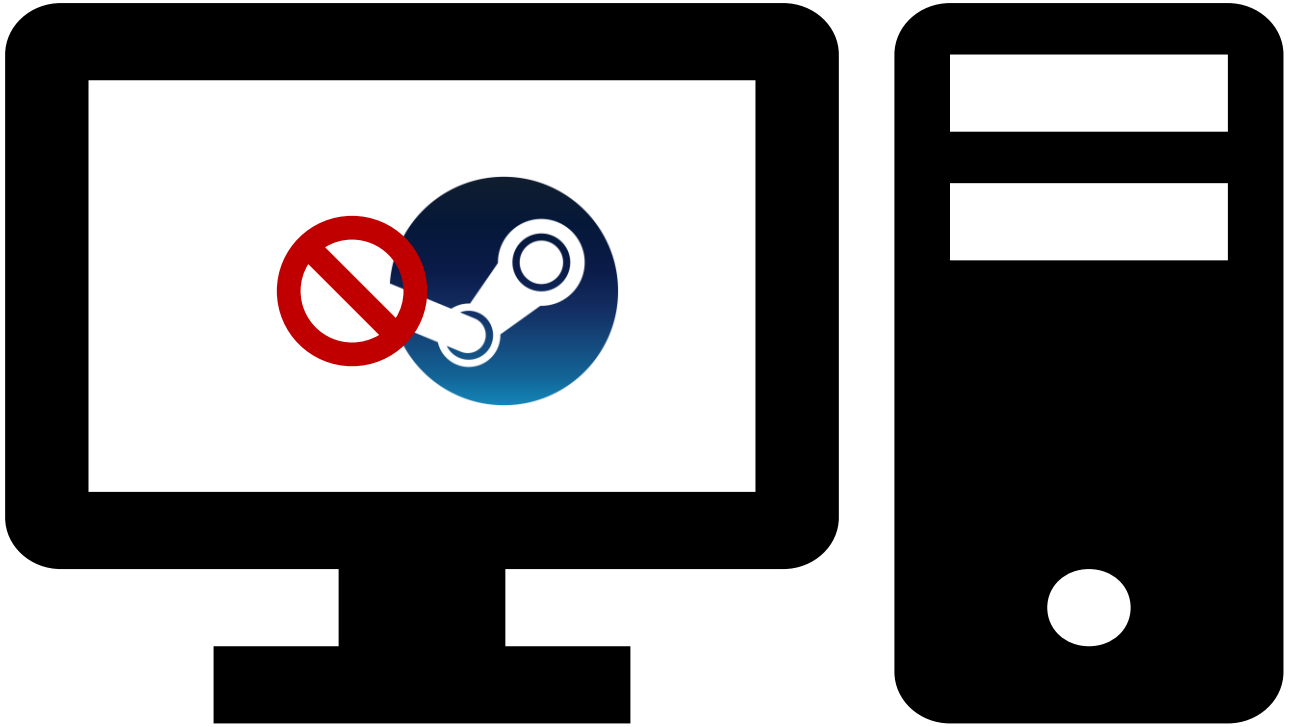
Zero Trust:
Geräte

- Device Identity & Conditional Access
  - Geräte-Registrierung
  - Zugriff abhängig vom Sicherheitszustand
  - Kein Zugriff für unbekannte bzw. unsichere Geräte
  - Device Isolation in Verdachtsfällen
- Unified Endpoint Management
  - Automatisierte Gerätekonfiguration



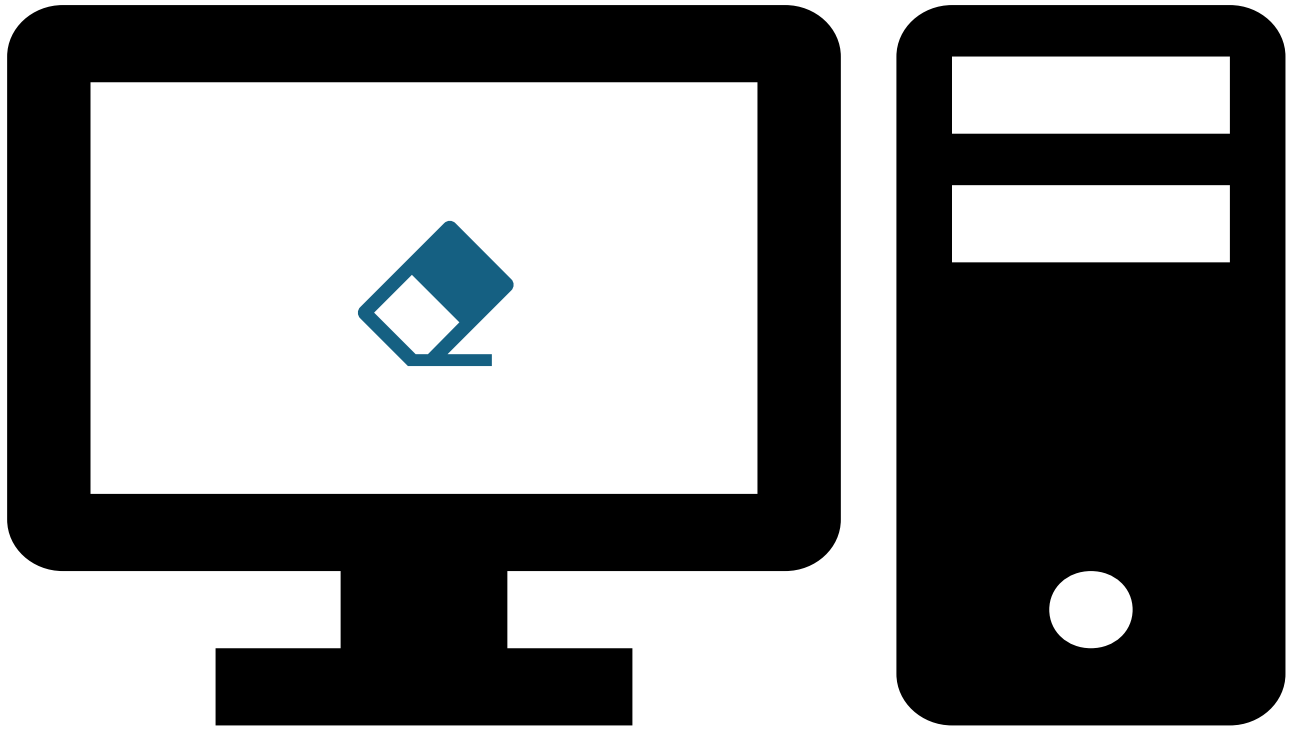
Zero Trust:
Geräte

- Device Identity & Conditional Access
  - Geräte-Registrierung
  - Zugriff abhängig vom Sicherheitszustand
  - Kein Zugriff für unbekannte bzw. unsichere Geräte
  - Device Isolation in Verdachtsfällen
- Unified Endpoint Management
  - Automatisierte Gerätekonfiguration
  - Erzwingen von Richtlinien



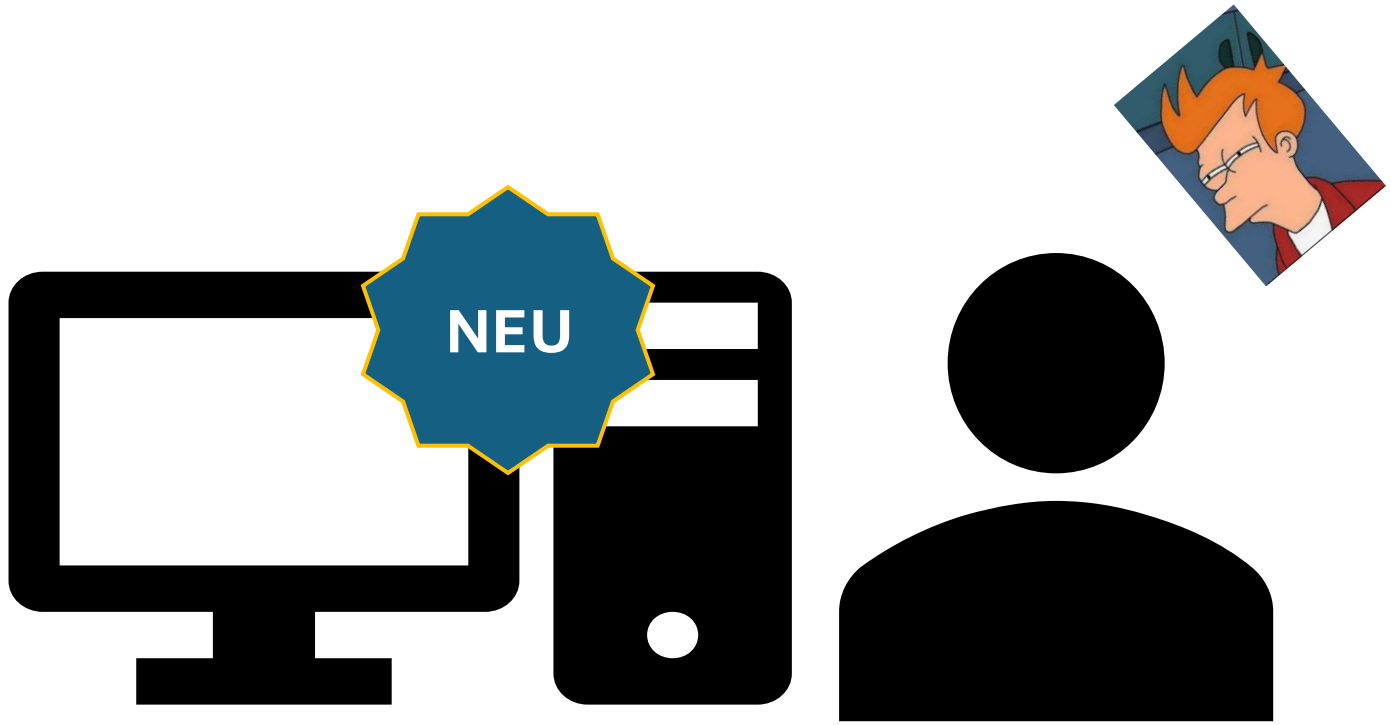
Zero Trust:
Geräte

- Device Identity & Conditional Access
  - Geräte-Registrierung
  - Zugriff abhängig vom Sicherheitszustand
  - Kein Zugriff für unbekannte bzw. unsichere Geräte
  - Device Isolation in Verdachtsfällen
- Unified Endpoint Management
  - Automatisierte Gerätekonfiguration
  - Erzwingen von Richtlinien
  - Remote Wipe bei Geräteverlust



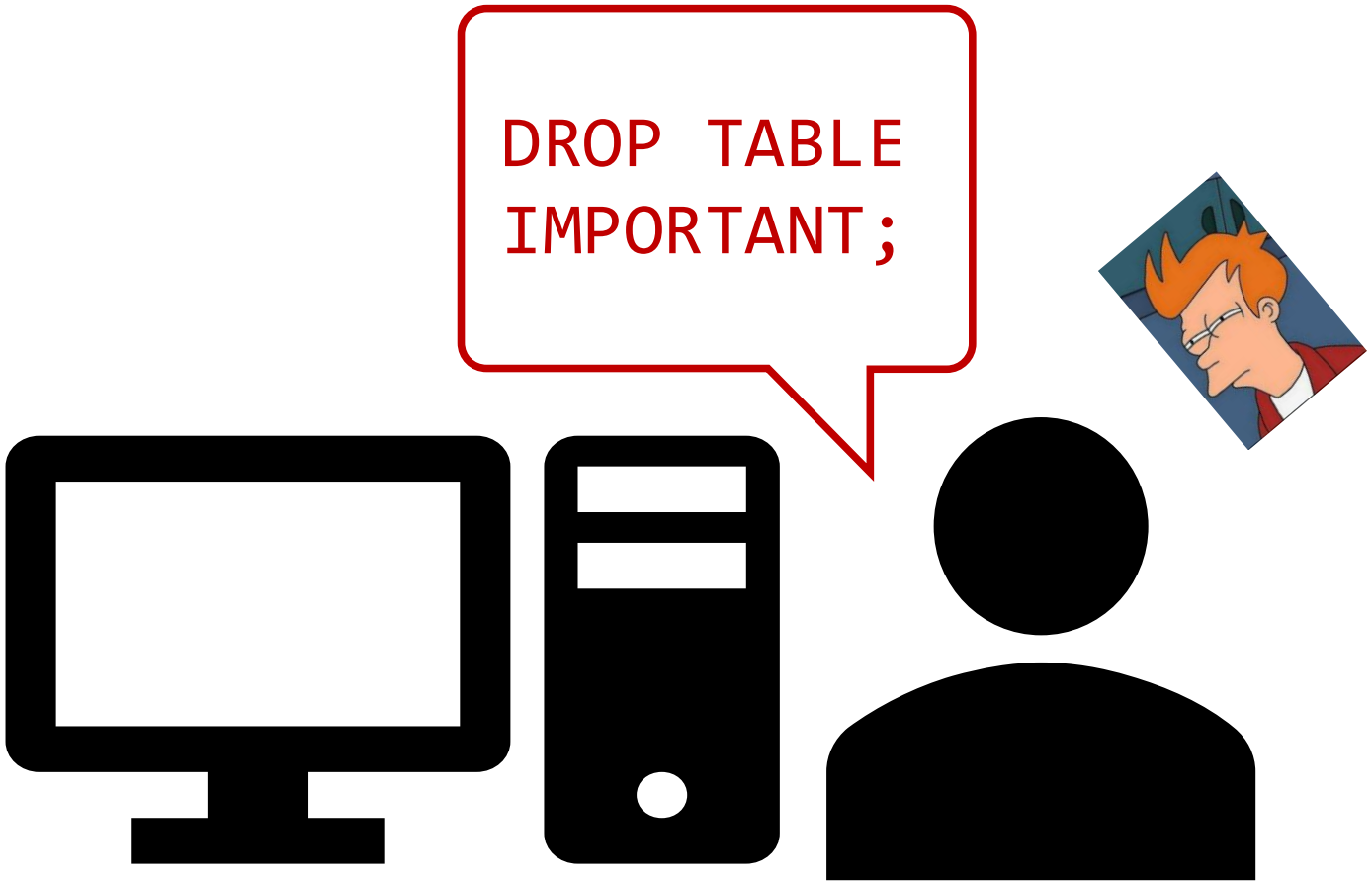
Zero Trust:
Nutzer

- User Behaviour Analytics
  - Adaptive Authentication; zusätzlicher MFA-Faktor bei Risikosignalen (z.B. neues Gerät)



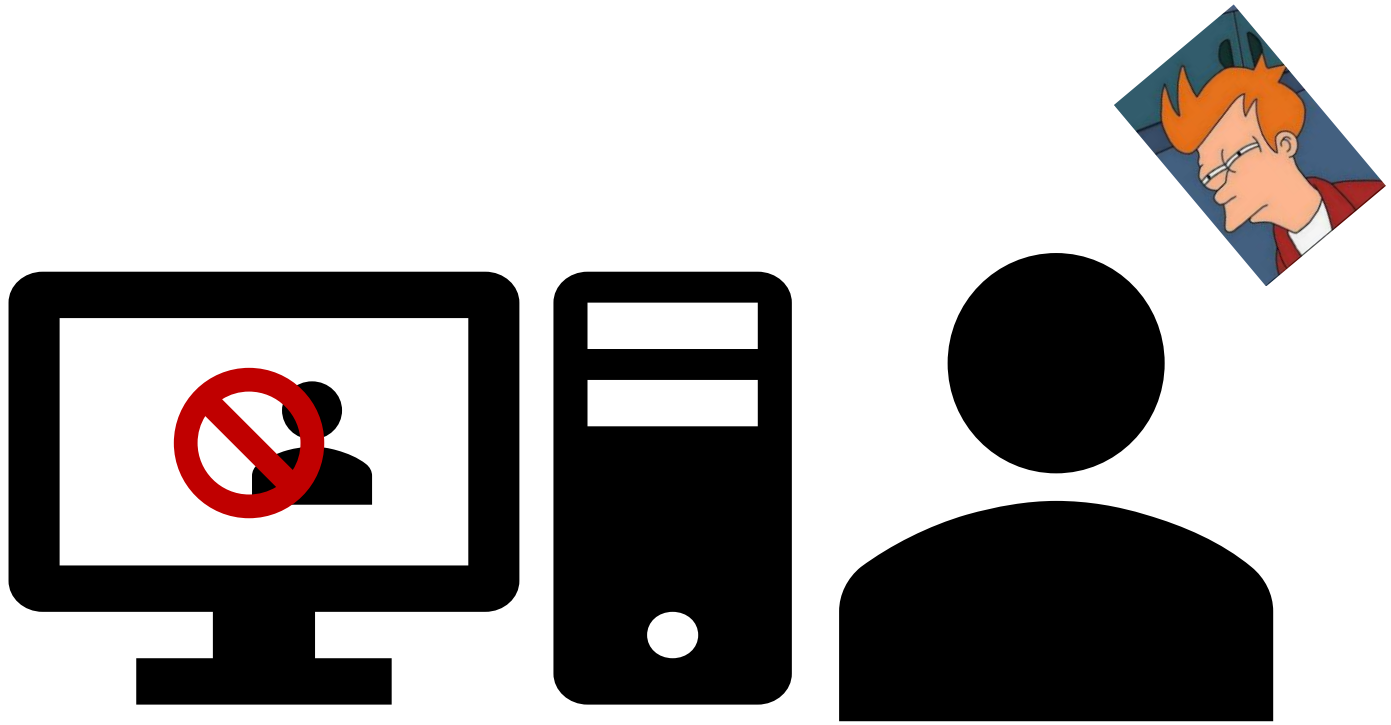
Zero Trust:
Nutzer

- User Behaviour Analytics
  - Adaptive Authentication; zusätzlicher MFA-Faktor bei Risikosignalen (z.B. neues Gerät)
  - Prüfung von Auffälligkeiten



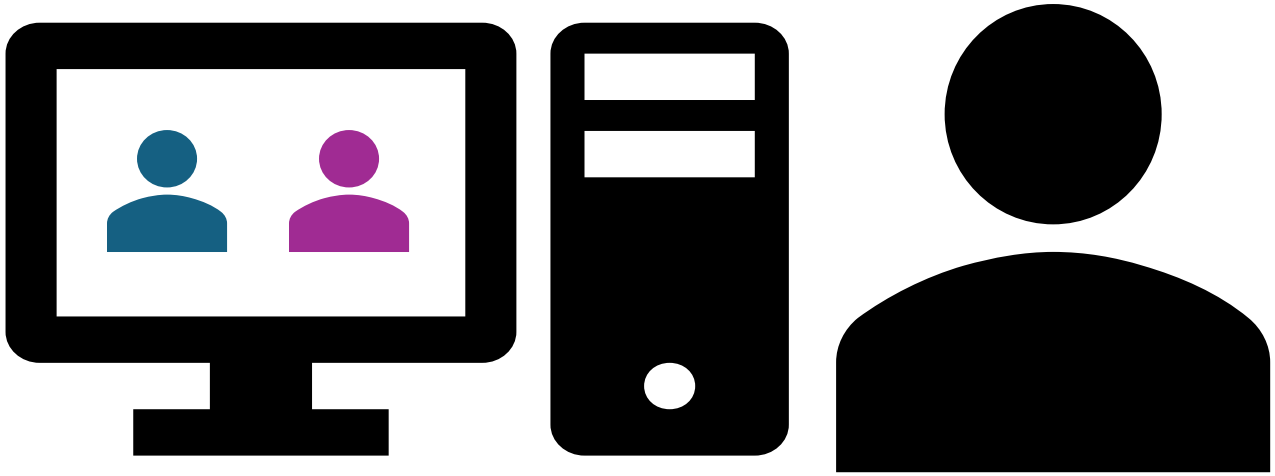
Zero Trust:
Nutzer

- User Behaviour Analytics
  - Adaptive Authentication; zusätzlicher MFA-Faktor bei Risikosignalen (z.B. neues Gerät)
  - Prüfung von Auffälligkeiten
  - Konto in Verdachtsfällen sperren



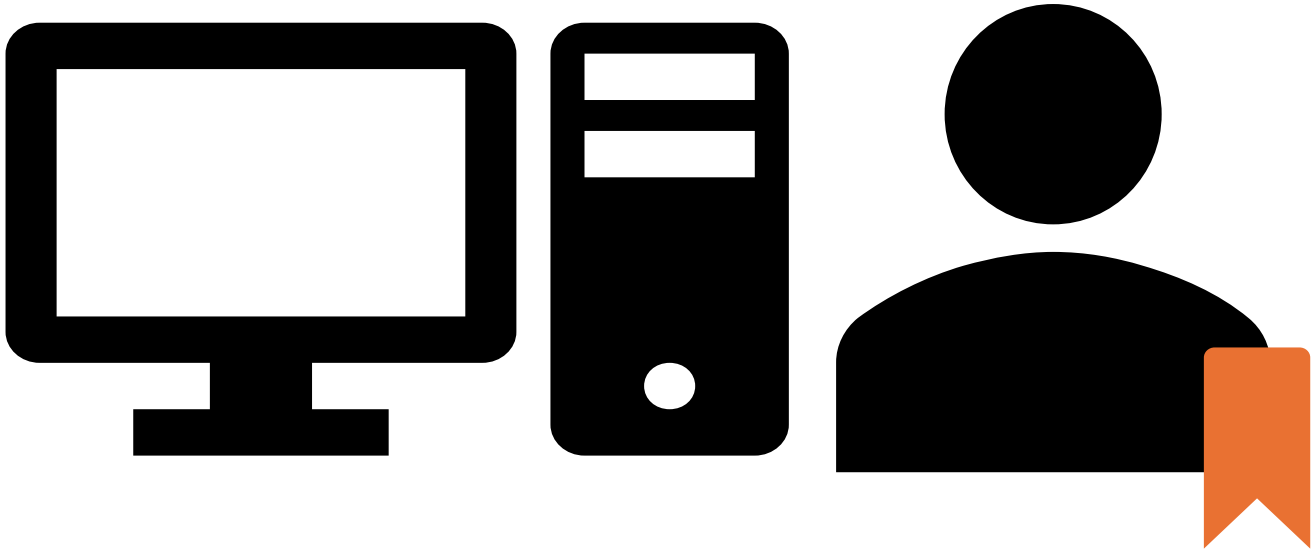
Zero Trust:
Nutzer

- User Behaviour Analytics
  - Adaptive Authentication; zusätzlicher MFA-Faktor bei Risikosignalen (z.B. neues Gerät)
  - Prüfung von Auffälligkeiten
  - Konto in Verdachtsfällen sperren
- Identity Segmentation
  - Konten (z.B. Arbeit & privat)



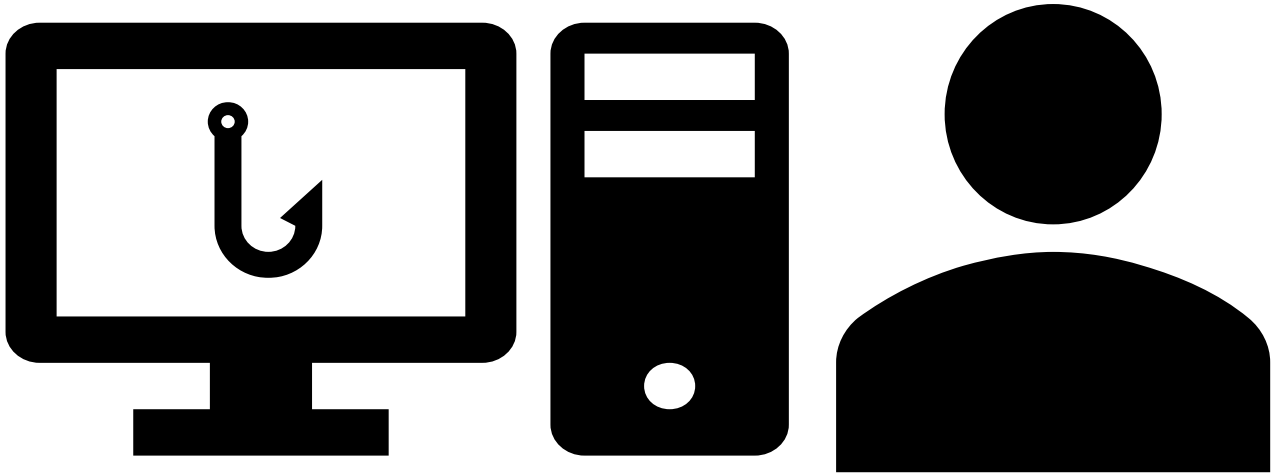
Zero Trust:
Nutzer

- User Behaviour Analytics
  - Adaptive Authentication; zusätzlicher MFA-Faktor bei Risikosignalen (z.B. neues Gerät)
  - Prüfung von Auffälligkeiten
  - Konto in Verdachtsfällen sperren
- Identity Segmentation
  - Konten (z.B. Arbeit & privat)
  - Rollen (z.B. Entwickler & Mitarbeiter)



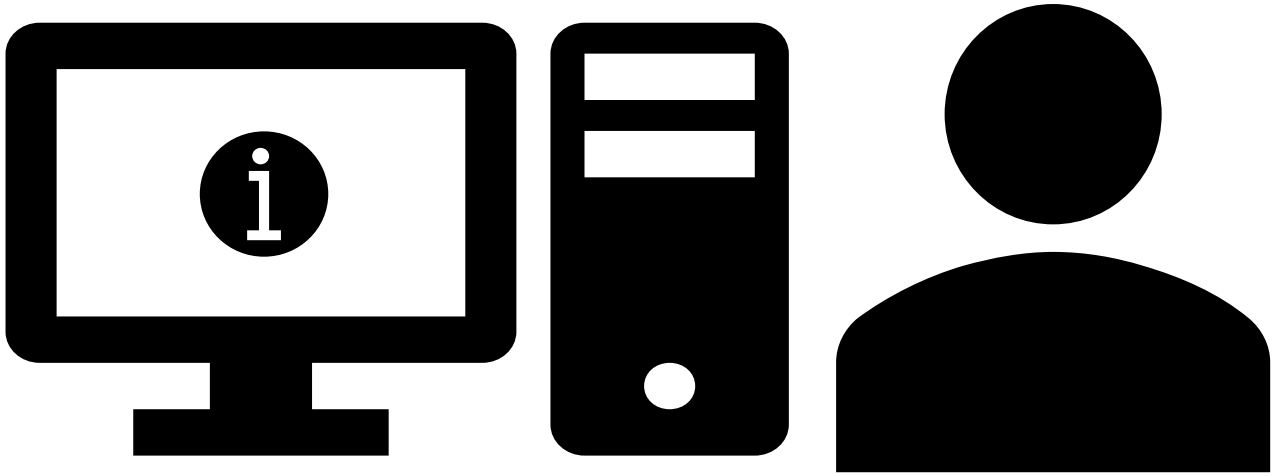
Zero Trust:
Nutzer

- User Behaviour Analytics
  - Adaptive Authentication; zusätzlicher MFA-Faktor bei Risikosignalen (z.B. neues Gerät)
  - Prüfung von Auffälligkeiten
  - Konto in Verdachtsfällen sperren
- Identity Segmentation
  - Konten (z.B. Arbeit & privat)
  - Rollen (z.B. Entwickler & Mitarbeiter)
- Security Awareness
  - Phishing-Simulationen



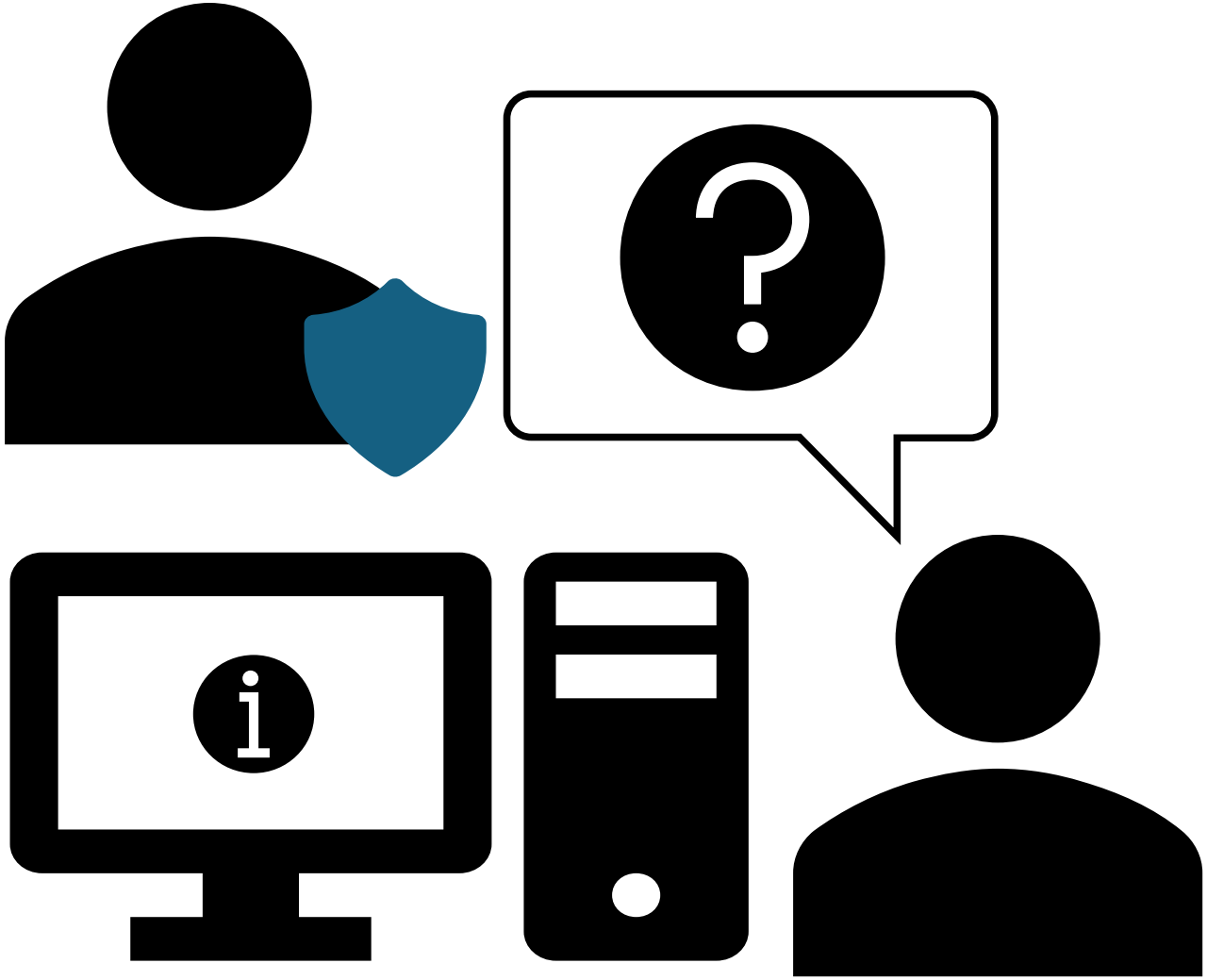
Zero Trust:
Nutzer

- User Behaviour Analytics
  - Adaptive Authentication; zusätzlicher MFA-Faktor bei Risikosignalen (z.B. neues Gerät)
  - Prüfung von Auffälligkeiten
  - Konto in Verdachtsfällen sperren
- Identity Segmentation
  - Konten (z.B. Arbeit & privat)
  - Rollen (z.B. Entwickler & Mitarbeiter)
- Security Awareness
  - Phishing-Simulationen
  - Schulungen



Zero Trust: **Nutzer**

- User Behaviour Analytics
  - Adaptive Authentication; zusätzlicher MFA-Faktor bei Risikosignalen (z.B. neues Gerät)
  - Prüfung von Auffälligkeiten
  - Konto in Verdachtsfällen sperren
- Identity Segmentation
  - Konten (z.B. Arbeit & privat)
  - Rollen (z.B. Entwickler & Mitarbeiter)
- Security Awareness
  - Phishing-Simulationen
  - Schulungen
  - Ansprechpartner

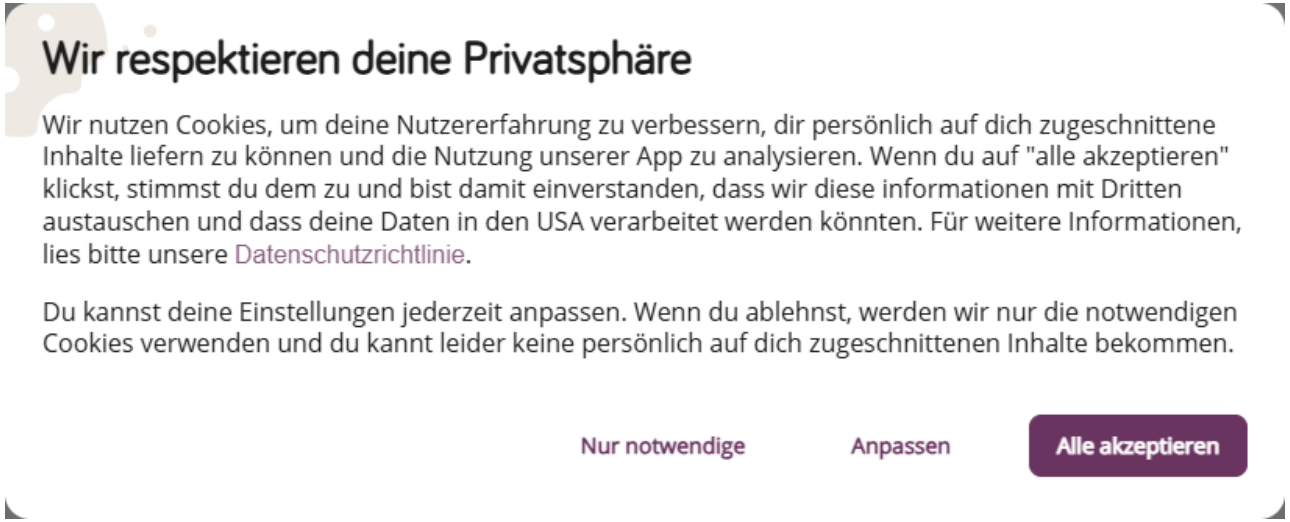


Zero Trust: **Alltag**

- **Verify explicitly**
- Least Privilege
- Strong Identity
- Zero Implicit Trust
- Segmentation

Zero Trust: **Alltag**

- Verify explicitly
- **Least Privilege**
- Strong Identity
- Zero Implicit Trust
- Segmentation



Zero Trust: **Alltag**

- Verify explicitly
- Least Privilege
- **Strong Identity**
- Zero Implicit Trust
- Segmentation

Zero Trust: **Alltag**

- Verify explicitly
- Least Privilege
- Strong Identity
- **Zero Implicit Trust**
- Segmentation

Zero Trust: **Alltag**

- Verify explicitly
- Least Privilege
- Strong Identity
- Zero Implicit Trust
- **Segmentation**

TolleEmail+amazon@mega.de

TolleEmail+netflix@mega.de

TolleEmail+newsletter@mega.de

Ende!