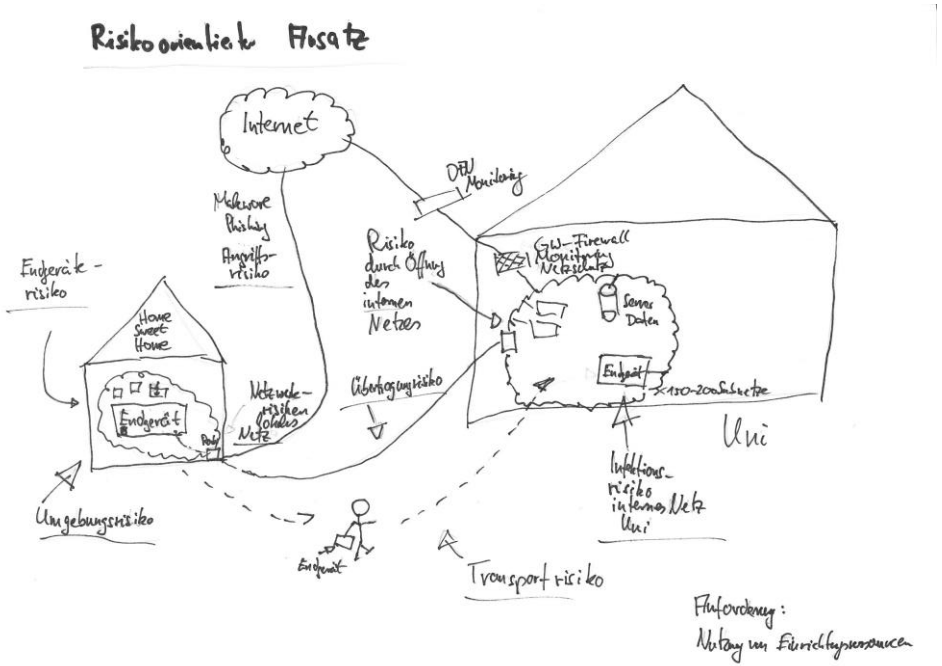
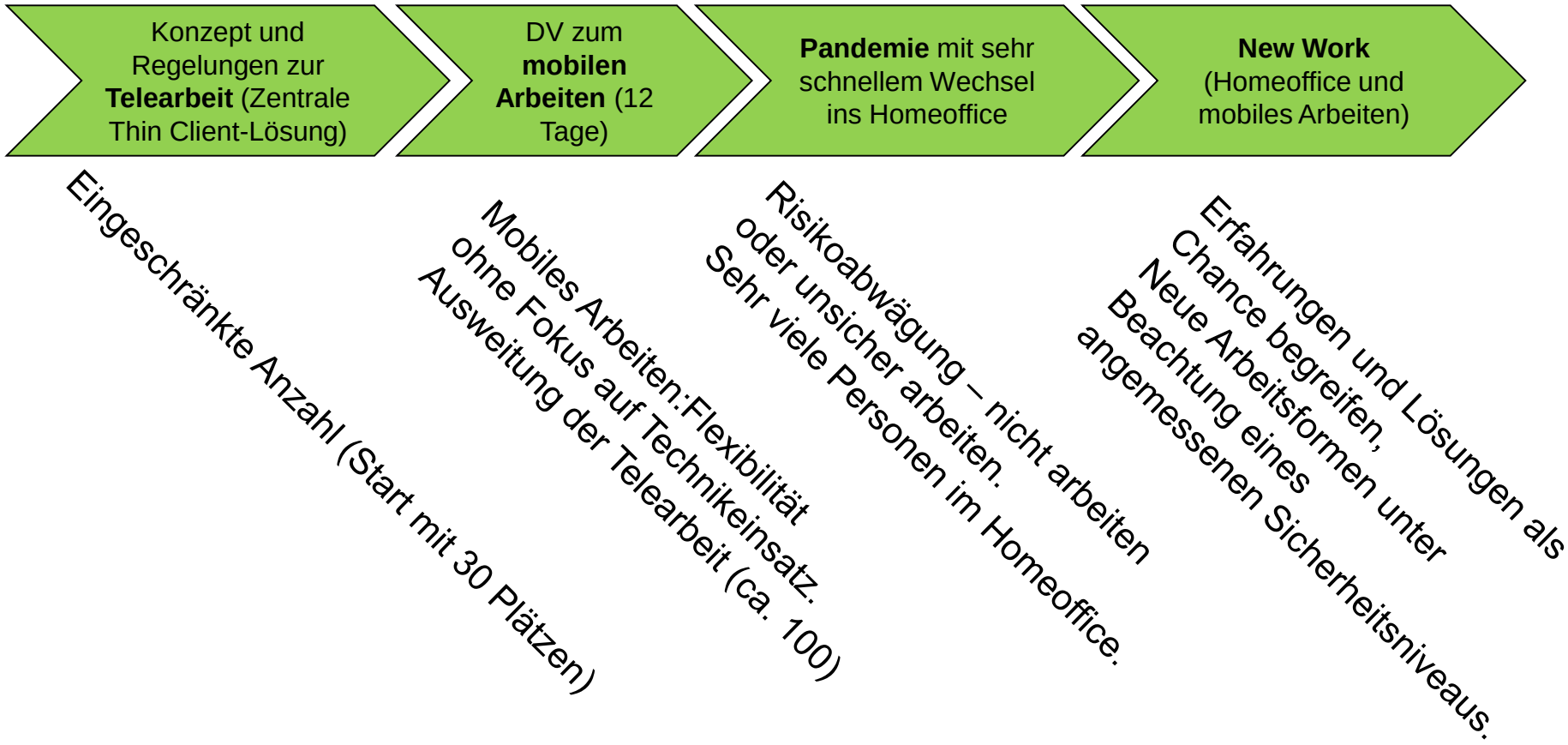
Leibniz Universität IT Services

Leibniz Universität Hannover

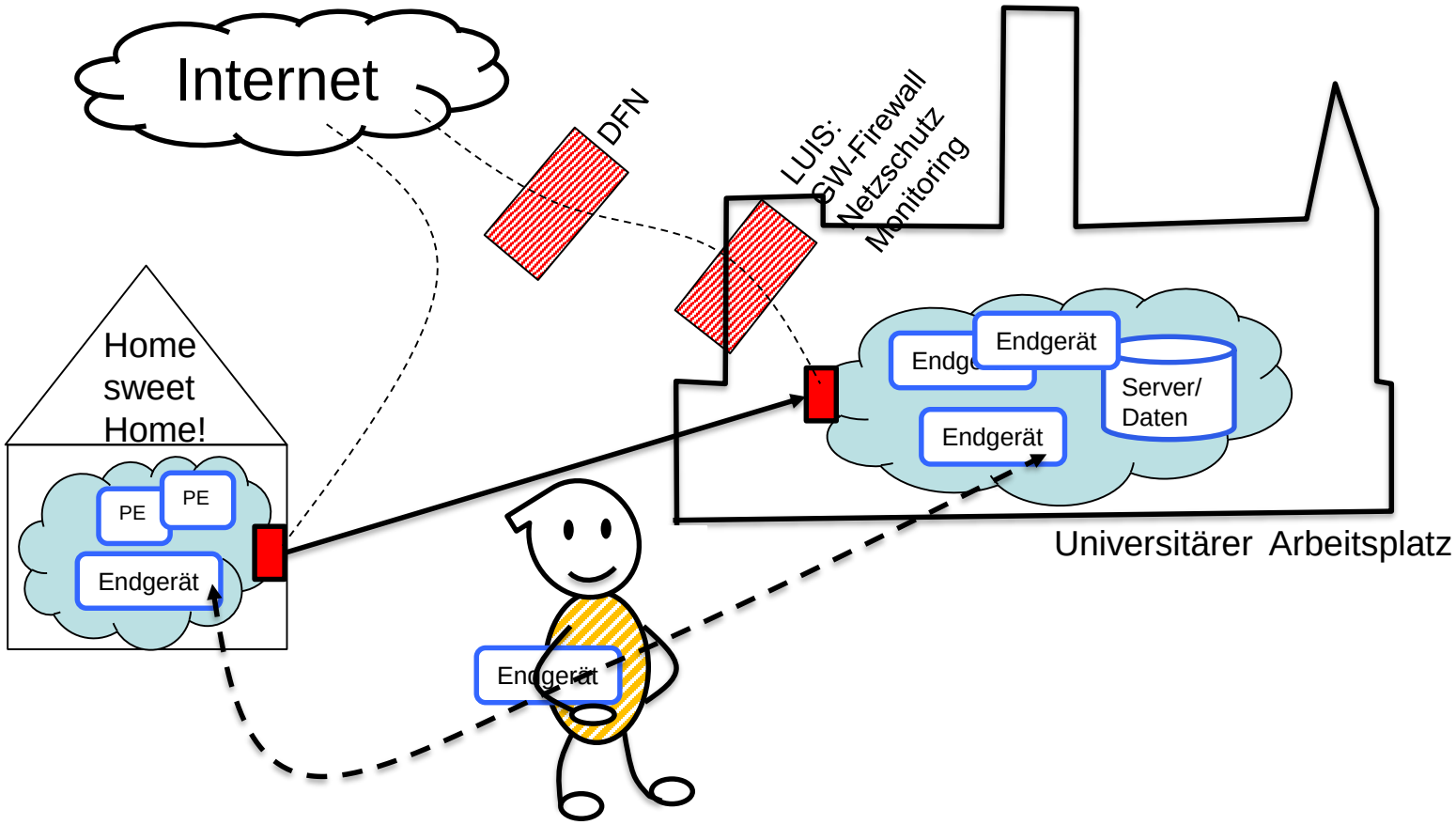
VORSTELLUNG
SICHERHEITS- UND TECHNIKKONZEPT FÜR HOMEOFFICE UND MOBILES ARBEITEN



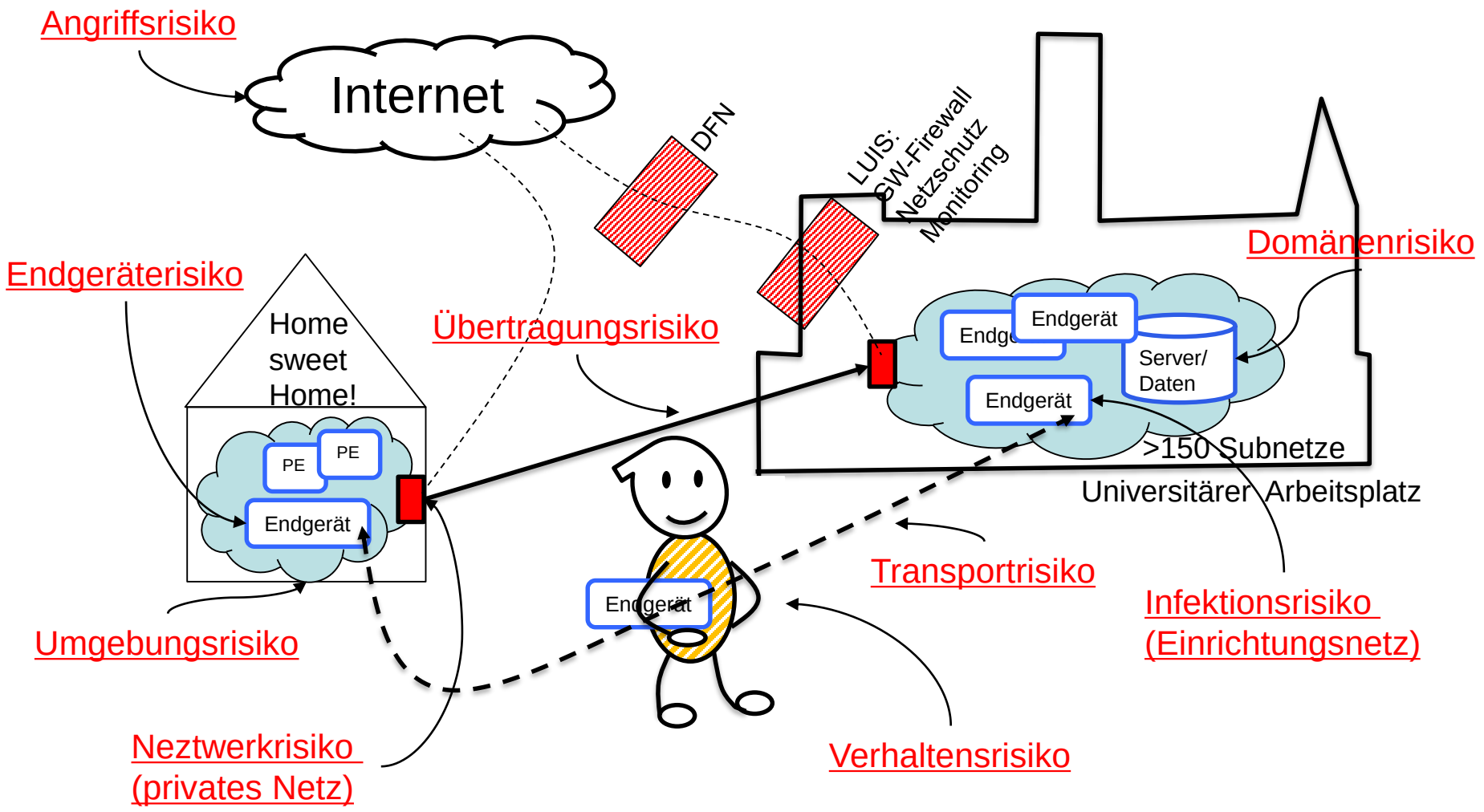
Dr. Thomas Rupp, Leibniz Universität IT Services (LUIS)


Konzept und Regelungen zur **Telearbeit** (Zentrale Thin Client-Lösung)
DV zum **mobilen Arbeiten** (12 Tage)
Pandemie mit sehr schnellem Wechsel ins Homeoffice
New Work (Homeoffice und mobiles Arbeiten)
Eingeschränkte Anzahl (Start mit 30 Plätzen)
Mobiles Arbeiten:Flexibilität ohne Fokus auf Technikeinsatz. Ausweitung der Telearbeit (ca. 100)
Risikoabwägung – nicht arbeiten oder unsicher arbeiten. Sehr viele Personen im Homeoffice.
Erfahrungen und Lösungen als Chance begreifen, Neue Arbeitsformen unter Beachtung eines angemessenen Sicherheitsniveaus.

Risikoorientierter Ansatz



Risikoorientierter Ansatz - Risiken

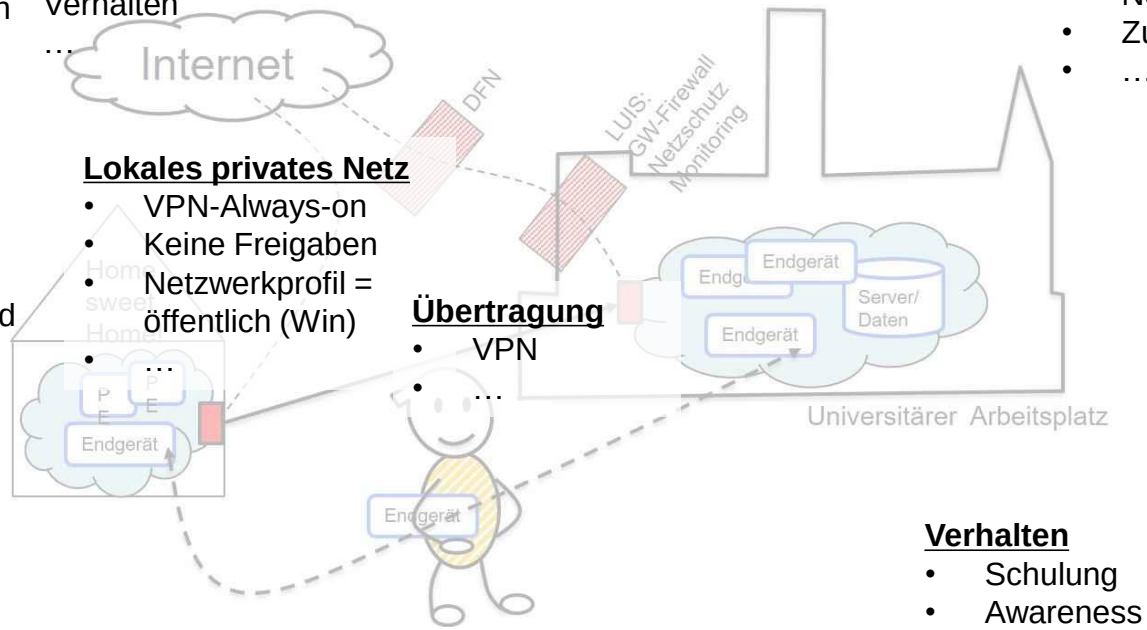


Risikoorientierter Ansatz - Maßnahmen

Angriffe
- Virenschutz
- Updates
- VPN-Always-on
- Kein split tunelling Verhalten
- …

Endgeräte
- Verschlüsselung
- Updates
- Zentrale Administration
- Virenschutz
- Remoteunterstützung
- VPN-Always-ON
- Multifaktor-Authentifikation
- Härtung
- MDM
- Endpoint Detection and Response (EDR)
- …

Domänenrisiko/ Internes LUH-Netz
- Koppelnetz
- Netzsegmentierung
- Zugangsverwaltung
- …



Lokales privates Netz
- VPN-Always-on
- Keine Freigaben
- Netzwerkprofil = öffentlich (Win)
- …

Übertragung
- VPN
- …

Umgebung
- Rechner sperren
- Gerät schützen
- Fenster zu
- Auf Kameras achten
- Auf Sprachassistenten achten (z.B. Siri, Alexa)
- Sichtschutz
- …

Transport
- Verschlüsselung
- Sichere Aufbewahrung
- …

Verhalten
- Schulung
- Awareness Maßnahmen
- Suportprozesse
- Meldeketten
- …

Vorgehen und Rahmenbedingungen

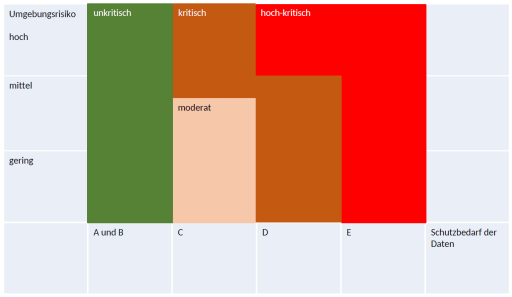
- Anlehnung an Vorgaben des Bundesamtes für Sicherheit in der Informationstechnologie (BSI)
- Berücksichtigung der Bausteine „Häuslicher Arbeitsplatz“ (INF.8) und „Mobiler Arbeitsplatz“ (INF.9) des Grundschutzkompendiums
- Den Risiken werden konkrete Maßnahmen an der LUH zugeordnet
- Das Konzept dient sowohl der Dokumentation der sicherheitstechnischen Bewertung der neuen Arbeitsformen auf zentraler Ebene (z.B. als Nachweis gegenüber Aufsichtsbehörden) als auch als Leitlinie zur strukturierten Auseinandersetzung mit dem komplexen Thema für Führungskräfte und Beschäftigte
- Das Konzept gibt Hilfestellungen für die Auswahl und Umsetzung eigener technischer Szenarien für Homeoffice und mobiles Arbeiten
- Das Sicherheits- und Technikkonzept ist Bestandteil der Dienstvereinbarung
- Das ThinClient-Szenario (bisher eingesetztes Szenario für Telearbeit) ist weiterhin als zentral bereitgestellte Lösung verfügbar

Auswahl angemessenes Technikszenario

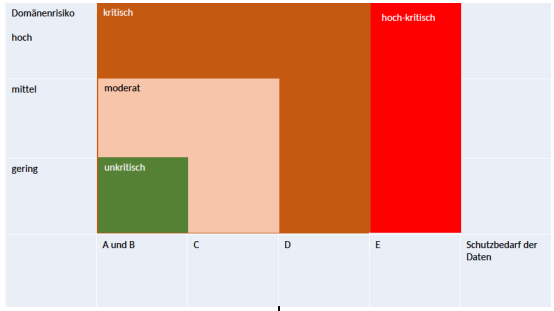
Schutzbedarf der Daten feststellen

(Beispiele in der Dienstanweisung)

Bewertung Umgebungsrisiko



Bewertung Domänenrisiko

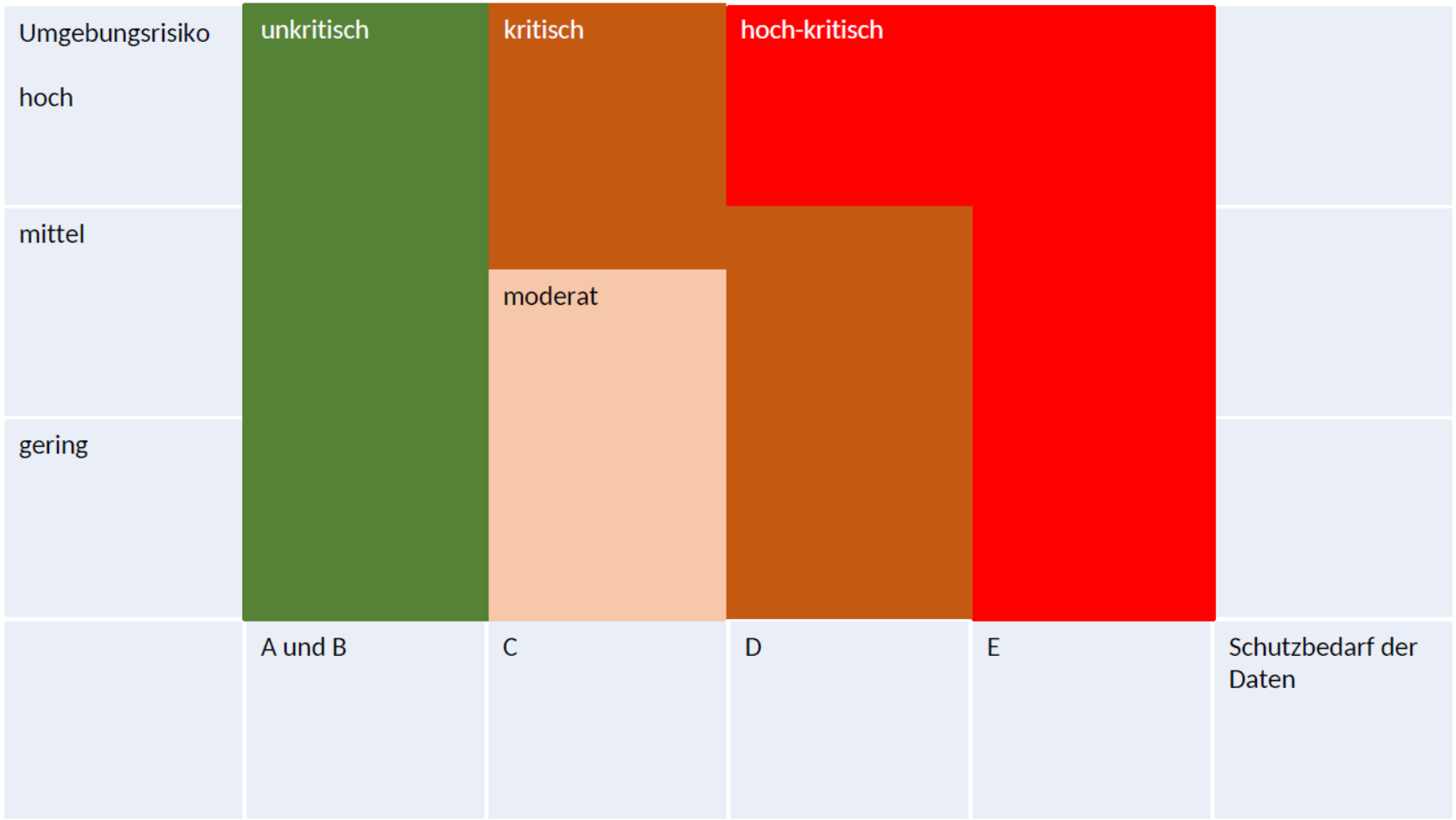


Kombination

Aggregierte Risikoklasse: unkritisch, moderat oder kritisch

Technikszenario + Schutzmaßnahmen

Umgebungsrisiko

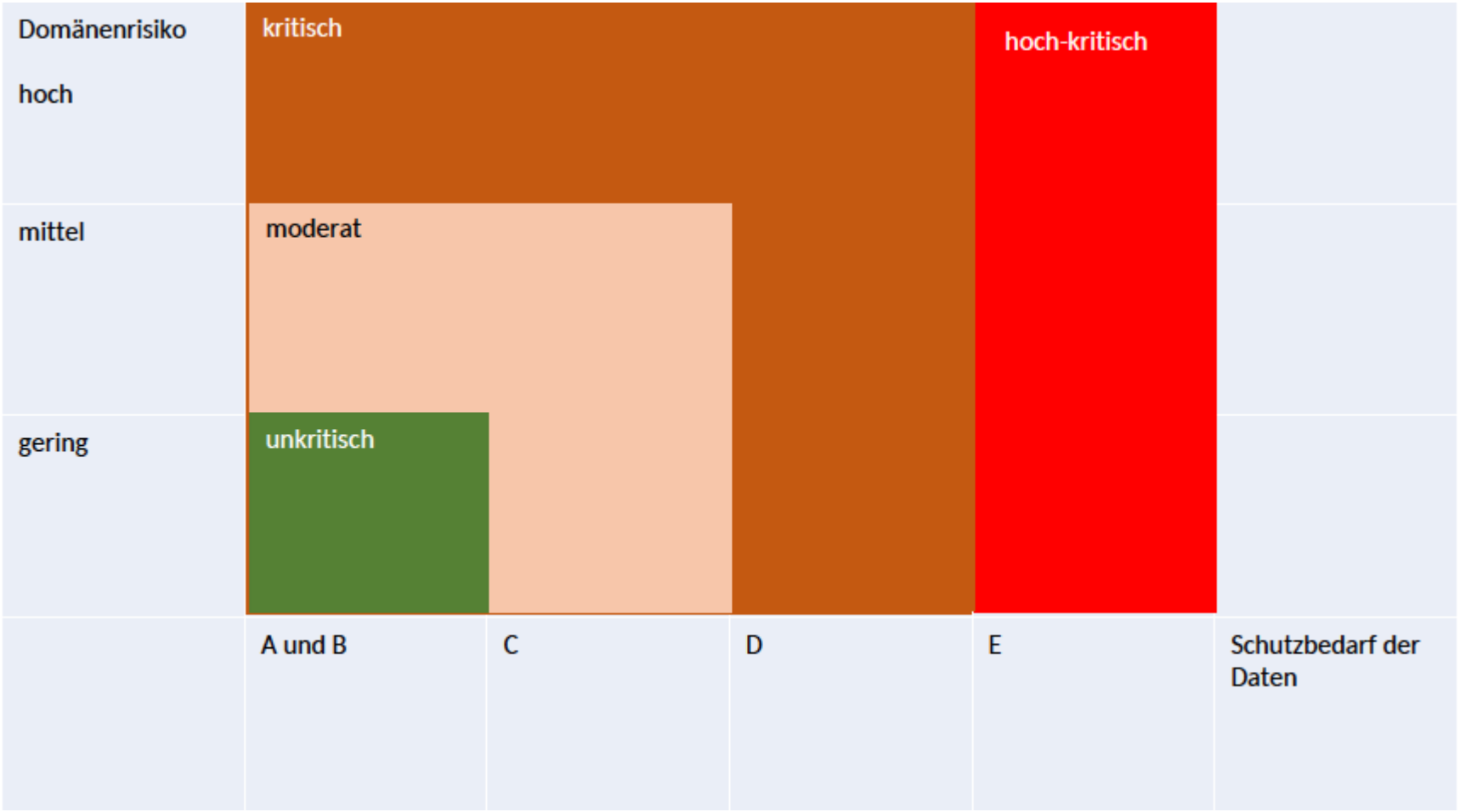


Beispiele

Umgebungsrisiko:

- Gering: Universitärer Arbeitsplatz, Homeoffice im separaten Arbeitszimmer
- Mittel: Homeoffice ohne separates Arbeitszimmer
- Hoch: Kaffee, Restaurant, im Park, Bahn

Sicherheitsdomänenrisiko



Beispiele

Domänenrisiko

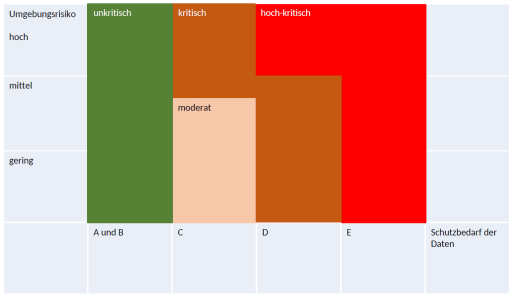
- Zugreifbare Daten in der Sicherheitsdomäne:
  - Gering: Schutzstufe A und B
  - Mittel: Schutzstufe C
  - Hoch: Schutzstufe D
- Weitere beispielhafte Rahmenbedingungen zur Einstufung der Sicherheitsdomäne:
  - Auch Schutzbedarf von in der Domäne verfügbaren Geräten, Prototypen, Patenten
  - Anzahl der Nutzenden, Endgeräte
  - Auswirkungen z.B. auch Schadenshöhe bei Kompromittierung der Sicherheitsdomäne (z.B. des gesamten Subnetzes)

Auswahl angemessenes Technikszenario

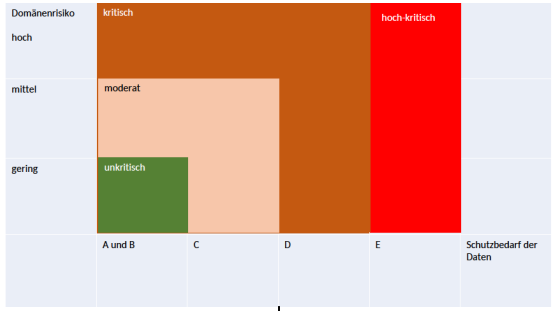
Schutzbedarf der Daten feststellen

(Beispiele in der Dienstanweisung)

Bewertung Umgebungsrisiko



Bewertung Domänenrisiko



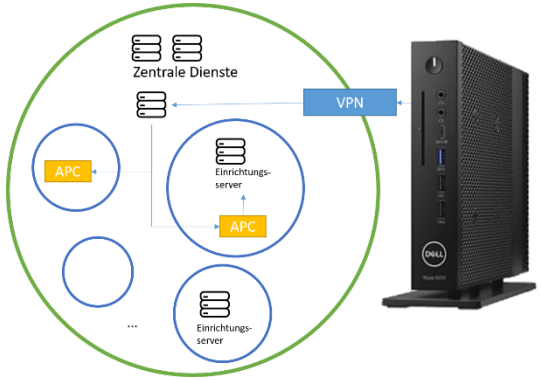
Kombination

Aggregierte Risikoklasse: unkritisch, moderat oder kritisch

Technikszenario + Schutzmaßnahmen

Thinclient

- Rudimentäres gehärtetes Betriebssystem
- Reduzierte Hardware-Plattform
- Arbeit erfolgt auf einer Umgebung in der LUH (physischen Büro-PC oder virtueller PC z. B. per Terminal-Server oder Virtual Desktop Infrastructure) → Umgebungsrisiko entspricht Büroarbeitsplatz
- Keine lokale Datenhaltung
- Aufschaltung nur über einen spezifischen VPN-Tunnel zum LUIS
- Die Verwaltung des Gerätes erfolgen durch das LUIS
- Notwendige Updates des Systems werden rechtzeitig vom LUIS initiiert
- Nachteile:
  - Nicht mobil und somit nur für Homeoffice geeignet
  - Eingeschaltetes Endgerät (oder virtueller PC auf Server) in Einrichtung erforderlich
- Vorteile:
  - Zwei vollwertige Arbeitsplätze
  - Kein Transport von Geräten zwischen Homeoffice und LUH
  - Vom LUIS verwaltet/administriert (inkl. Beschaffung und Geräteausgabe)
  - Baut selbständig einen VPN-Tunnel auf
  - Identische Arbeitsumgebung im Homeoffice und in der LUH
  - Direkter Zugriff ausschließlich auf einen einzelnen Arbeitsplatz
  - Besonders sicher, weil Betriebssystem besonders geschützt ist (gehärtet)
  - Keine lokale Datenhaltung



Road-Warrior ohne Zugriff auf interne Einrichtungsressourcen

- Mobiles Endgerät
- Ohne aufwändige infrastrukturelle Vorkehrungen
- Dienstliche Stand-Alone Endgeräte
- Beachtung der "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" der LUH (siehe auch http://go.lu-h.de/mobrichtlinie)
- Kein dediziertes zentrales VPN (LUH-VPN) und kein Einrichtungs-VPN
- Übertragung dienstlicher Daten muss immer verschlüsselt erfolgen (z.B. TLS-verschlüsselte Verbindungen, Einsatz digitaler Zertifikate)
- Verwendung von LUIS Cloud-Dienste und/oder LUIS-Projektablage sowie zulässige dezentrale Dienste für Collaboration/Dateiablage
- Eine lokale Datenhaltung und der Versand von bearbeiteten Dokumenten per E-Mail müssen für schutzbedürftige Informationen unbedingt unterbleiben

- Vorteil: Da keine Integration in lokale Netze geringes Sicherheitsdomänenrisiko

Einrichtungs-Laptops mit VPN-Zugang in die Einrichtung

- Durch die Einrichtung administrierte mobile Endgeräte
- Vorgaben der "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" beachten
- Zusätzliche Gefährdung durch Nutzung eines Instituts-/Einrichtungs-VPNs im Rahmen des Sicherheitsdomänenrisikos beachten
- Zusätzliche Gefährdung bei Split Tunneling beachten
- Erhöhung der Sicherheit durch zusätzliche Maßnahmen möglich (z.B. 2FA, MDM, Endpoint-Detection and -Response-System).

Bring Your Own Device (BYOD)

- Die Nutzung von privaten Geräten (BYOD), die den Vorgaben der "Richtlinie für den dienstlichen Einsatz mobiler und privater Geräte" entsprechen, ist zwar in gewissen Arbeitsbereichen zulässig, sollte jedoch aus der Sicherheitsperspektive weitestgehend vermieden werden.
- Gemäß § 4 Abs. 3 der oben genannten Richtlinie ist durch die Einrichtungsleitung über eine spezifische Risikobewertung festzulegen, welche Daten auf den Geräten gespeichert werden dürfen.
- Als Szenario für Homeoffice und mobiles Arbeiten mit schützenswerten dienstlichen Informationen ist BYOD grundsätzlich nicht geeignet.

Managed Device

- Mobiles Endgeräte (vorwiegend Notebooks)
- Installation, Wartung und Software-Pflege nicht durch die Nutzenden
- Viele Endgeräte mit etablierten und dokumentierten Prozessabläufen und zentraler Administration (z.B. mit automatischer Softwareverteilung, Updatemanagement, Remoteunterstützung)
- Idealerweise mit Zwei-Faktor-Authentifizierung
- Zentrales Geräte-VPN mit separiertem Koppelnetz
- VPN-Always-on und kein Split Tunneling (d.h. alles via VPN)
- Lokale Datenhaltung ist möglich: Verschlüsselung, Backupkonzept
- RDP/SSH-Sitzung auf Arbeitsplatz-Computer/Server für Zugriff auf Spezialanwendungen möglich

- *Das Managed Devices-Szenario kann derzeit nicht zentral durch das LUIS angeboten werden*

Fortrex

- Mobiles Endgerät als „beweglichen Festung“
- Erheblichen Eingriff in das Management des mobilen Endgerätes
- Besonders abgestimmte zentrale Management-Infrastruktur notwendig:
  - MDM - Mobile Device Management
  - ID / Policy Management
  - Zentrales Geräte-VPN
  - MFA - Multifaktor Authentifizierung
  - Device Posture Checks (Konformitätsprüfung)
  - EDR - Endpoint Detection & Response

- *Das Fortrex-Szenario kann derzeit nicht zentral durch das LUIS angeboten werden.*

Beispielhafte Maßnahmen Endgerätesicherheit

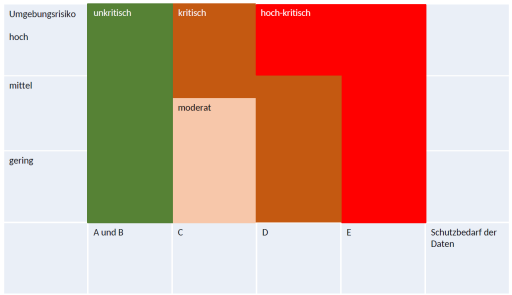
- **Immer erforderlich (**http://go.lu-h.de/mobrichtlinie**):**
  - Verschlüsselung
  - Authentifizierung am Gerät und Bildschirmsperre
  - Regelmäßige zeitnahe Einspielung von Updates (Betriebssystem, Applikationen)
  - Virenschutz mit automatischer Aktualisierung
  - Keine Administrationsrechte bei normaler Nutzung
  - Unterweisung/Schulung der Nutzenden
  - Backup lokaler Daten sicherstellen
  - Vertrauenswürdiges WLAN oder LUH Zentral-VPN
  - Keine unbekannten Datenträger/USB-Geräte anschließen
  - Geräte sicher verwahren
  - Keine Weitergabe an Dritte
  - Software aus vertrauensw. Quellen
- **Weitere Maßnahmen:**
  - Zentrale Administration
  - Bootvorgang absichern (z.B. Trusted Boot)
  - Softwareverteilung
  - Remoteunterstützung
  - VPN-Always-ON
  - Kein Split Tunneling
  - Sichtschutzfolie (insb. beim mobilen Arbeiten)
  - Erweiterter Diebstahlschutz (z.B. Kensington-Schloss)
- **Maßnahmen bei erhöhtem Schutzbedarf:**
  - 2Faktor-Authentifikation zur Anmeldung
  - Härtung des Betriebssystems
  - Deaktivierung von USB-Ports (Schnittstellenkontrolle)
  - Mobile Device Management (MDM)
  - Endpoint Detection and Response (EDR)

Auswahl angemessenes Technikszenario

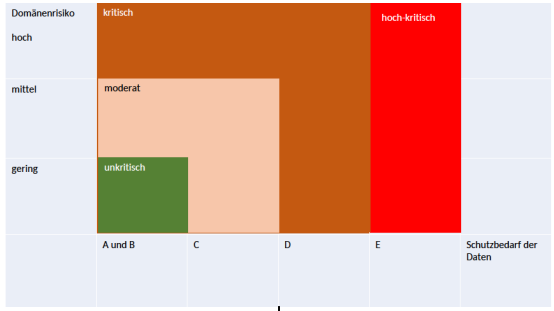
Schutzbedarf der Daten feststellen

(Beispiele in der Dienstanweisung)

Bewertung Umgebungsrisiko



Bewertung Domänenrisiko



Kombination

Aggregierte Risikoklasse: unkritisch, moderat oder kritisch

Technikszenario + Schutzmaßnahmen

Auswahl Technikszenario und Maßnahmen

aggregierte Risikoklasse	Szenario
unkritisch	Thinclient Fortrex Managed Device Road-Warrior Einrichtungs-Laptops mit VPN-Zugang in die Einrichtung alle Geräte, die der Mobilrichtlinie der LUH genügen
moderat	Thinclient Fortrex Managed Device Road-Warrior Einrichtungs-Laptops mit VPN-Zugang in die Einrichtung
kritisch	Thinclient Fortrex Managed Device
hoch-kritisch	Hier ist weder mobiles Arbeiten, noch Homeoffice zulässig

Wer ins kalte Wasser springt,
taucht ins Meer der
Möglichkeiten.

(Finnland)

WITH GREAT POWER THERE MUST ALSO
COME - GREAT RESPONSIBILITY!

Amazing Fantasy #15 (August 1962) – The first Spider-Man story.