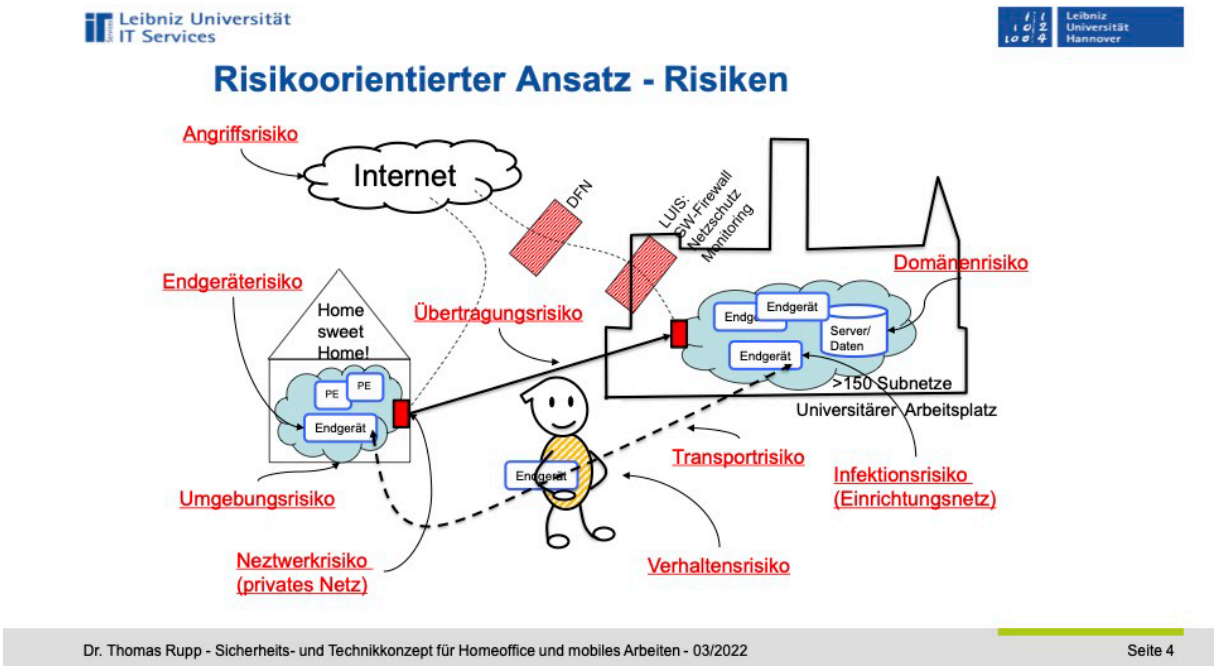
Gesprächsleitfaden zur Beantragung „Mobiles Arbeiten“
mit dem Ziel der Ermittlung des anzuwendenden Technikszenarios

Beantragende Person: _____

Vorgesetzte Person: _____

(Beratende Person:) _____

Datum: _____



Es soll ein geeignetes Technikszenario für die mobil durchzuführenden Arbeiten ermittelt werden.
→ Wichtig ist dafür zu ermitteln, was wo erledigt werden soll.

Die folgenden Seiten enthalten einen Leitfaden, der anhand von Fragen die komplexe Beurteilung der Risiken ermöglicht.

Als Ergebnis der Bearbeitung soll eine Einstufung des relativen Risikos („Risikoklasse“) in die Kategorien „unkritisch“, „moderat“, „kritisch“ oder „hoch kritisch“ erfolgen.

Daraus resultiert eine Auswahl von möglichen Technikszenarien.

1) Feststellung der Schutzstufe *(gem. Sicherheits- und Technikkonzept für Homeoffice und mobiles Arbeiten des LUIS)*.
Leitfrage: Welche Tätigkeiten sollen mobil oder im Homeoffice durchgeführt werden? In welchem Umfang?

Schutzstufe A:

- keine „nicht öffentlich zugänglichen“ personenbezogenen Daten werden verarbeitet
- keine schützenswerten Forschungsdaten

Beispiele: Literaturrecherche, Bearbeitung oder Erstellung von Webinhalten, Entwicklung von Lehr- und Lernkonzepten, Schreiben von Artikeln etc.

Soll durchgeführt werden: ☐ ja ☐ nein

Notizen dazu: _____

_____

_____

Schutzstufe B:

- Kontaktinformationen Dritter, interne Kommunikationsdaten, dienstliche Daten von Mitarbeitenden
- keine schützenwerten Forschungsdaten

Beispiele: Terminabstimmungen, Einholen von Angeboten, Bestellvorgänge, Organigramme etc.

Soll durchgeführt werden: ☐ ja ☐ nein

Wäre es möglich, Tätigkeiten dieser Schutzstufe im Rahmen mobiler Arbeit zu unterlassen?
☐ ja ☐ nein

Notizen dazu: _____

_____

_____

Schutzstufe C:

- Personenbezogene Daten, deren unsachgemäße Handhabung Betroffene in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen beeinträchtigen könnte
- Verwaltung und Kontrolle von Drittmittelprojekten, unveröffentlichte Forschungsergebnisse

Beispiele: Beratung von Studieninteressierten, Korrektur von Studien- und Prüfungsleistungen, Verwaltung von Stud.IP-Veranstaltungen, Personalkostenverwaltung, lesender SAP-Zugang, Reisekostenabrechnungen etc.

Soll durchgeführt werden: ☐ ja ☐ nein

Wäre es möglich, Tätigkeiten dieser Schutzstufe im Rahmen mobiler Arbeit zu unterlassen?
☐ ja ☐ nein

Notizen dazu: _____

_____

_____

Schutzstufe D:

- Personenbezogene Daten, deren unsachgemäße Handhabung Betroffene in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen **erheblich** beeinträchtigen könnte
- Forschungsdaten, die vertraglich der Geheimhaltung unterliegen

Beispiele: Personalangelegenheiten, Gesundheitsdaten, Berufungs- und Bewerbungsverfahren, Leistungsinformationen über Studierende etc.

Soll durchgeführt werden: ☐ ja ☐ nein
Wäre es möglich, Tätigkeiten dieser Schutzstufe im Rahmen mobiler Arbeit zu unterlassen?
☐ ja ☐ nein

Notizen dazu: _____

_____

_____

Es gibt auch eine Schutzstufe E, die z. B. Strafprozessakten betrifft, also für die LUH kaum relevant ist (erst recht nicht im Kontext mobilen Arbeitens).

Ermittelte Schutzstufe der Tätigkeiten für die beantragte, mobile Arbeit:

☐ A ☐ B ☐ C ☐ D

2) Ermittlung zum Umgebungsrisiko und daraus resultierende Risikoklasse

Grundsätzlich wird das Umgebungsrisiko bei Arbeiten mit mobilen Endgeräten als „mittel“ eingestuft. Wird das Gerät ohne weitere Schutzmaßnahmen im öffentlichen Raum (Park, Café, Bahn, im Rahmen von Tagungen) genutzt, steigt das Umgebungsrisiko auf „hoch“!

Potentielle Gefährdungen sind: Diebstahl der Hardware, Einsicht des Bildschirms durch Dritte, ggf. auch durch Kameras, Mithören von Gesprächen, unsichere WLAN-Netze…

- Für Tätigkeiten der Schutzstufen A und B ist die Risikoklasse „unkritisch“.
- Für Tätigkeiten der Schutzstufe C ist die Risikoklasse bei mittlerem Umgebungsrisiko „moderat“, bei hohem Umgebungsrisiko „kritisch“.
- Für Tätigkeiten der Schutzstufe D ist die Risikoklasse bei mittlerem Umgebungsrisiko „kritisch“, bei hohem Umgebungsrisiko „hoch kritisch“.

3) Ermittlung des Domänenrisikos

Soll auf bestimmte Ressourcen im Netz der LUH zugegriffen werden, die über die Erreichbarkeit des „Standard-VPN“ nicht gewährt sind? Z.B. institutseigenen Server, Fernwartung von Messsystemen, etc.

☐ ja[1] ☐ nein[1]

Bei „ja“: Ist administrativ sichergestellt, dass nur auf notwendige Daten und Systeme zugegriffen werden kann?

☐ ja ☐ nein

worauf soll _____

zugegriffen _____

werden? _____

[1] Bei „nein“ hat das Domänenrisiko keinen Einfluss auf die Risikoklasse, bei „ja“, muss eine spezifische Bewertung des Risikos unter Berücksichtigung der Daten innerhalb der Domäne durchgeführt werden.

Ermittelte Risikoklasse für die beantragte, mobile Arbeit:

☐ unkritisch ☐ moderat ☐ kritisch ☐ hoch kritisch

4) Mögliche Technikszenarien für die Beantragung in Abhängigkeit von der ermittelten Risikoklasse

Hoch kritisch:
Diese Arbeiten dürfen nicht in der mobilen Arbeit durchgeführt werden!

Kritisch:
„Thinclient“, „Managed Device“ und „Fortrex“ Szenarien sind zulässig – Alle drei Szenarien sind im Sicherheits- und Technikkonzept für Homeoffice und mobiles Arbeiten des LUIS unter Punkt 9.1 explizit beschrieben.

- Ein Thinclient ist ein „Mini-Desktop-PC“ der sich direkt und sicher zum angeschalteten Rechner im Büro tunnelt. Arbeiten ist ausschließlich getunnelt möglich.
- Ein Managed Device ist (meist) ein Laptop, das mittels Geräte-VPN auf einen Rechner in der Uni zugreift und die eigentliche Arbeit dort durchgeführt wird.
- Fortrex bezeichnet ein Laptop, das mittels eines Mobile Device Managements betreut wird und so auf dem aktuellsten sicheren Stand gehalten wird.

Managed Devices und Fortrex-Laptops erfordern einen enormen administrativen Aufwand, der nicht vom LUIS angeboten wird, also in den Instituten bedacht und ggf. vorgehalten werden muss.

Moderat:
zusätzlich sind die Technikszenarien „Road-Warrior“ und „Einrichtungs-Laptop mit VPN-Zugang zur Einrichtung“ möglich.

- Als Road Warrior wird das klassische Szenario bezeichnet, in dem verschlüsselte mobile Endgeräte zur Arbeit unterwegs benutzt werden, ohne auf Netzwerkressourcen der LUH zurückzugreifen. Eine mögliche Maßnahme, um die Arbeit mit lokalen Dateien zu ermöglichen, ist die temporäre Speicherung der Arbeitsdateien im Cloud-Seafile.
- Das andere Szenario beinhaltet zusätzlich einen Zugriff auf lokale Netzwerke, erfordert aber eine lokale Administration von institutseigenen Endgeräten.
  Wenn auf diesen Zugriff verzichtet werden kann, ist das Road Warrior Szenario vorzuziehen.

Unkritisch:
Alle Geräteszenarien gem. der „Richtlinie für den Einsatz mobiler und privater Geräte“ sind zulässig.

Ausgewähltes Technikszenario:

☐ Thinclient ☐ Managed Device ☐ Fortrex

☐ Road Warrior ☐ Einrichtungs-Laptop mit VPN-Zugang zur Einrichtung

☐ _____

Ich bin über die Risiken der mobilen Arbeit aufgeklärt worden und werde nur Tätigkeiten der ermittelten Schutzstufe im Rahmen der besprochenen Umgebung durchführen.
Mein Laptop ist passwortgeschützt und die Festplatte meines Endgeräts und meine weiteren mobilen Datenträger sind verschlüsselt.

_____

Beantragende Person