ECONSTOR
Make Your Publications Visible.

A Service of
ZBW
Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Rudel, Steffi; Kolb, Lisa

Research Report

Federated Learning Enhancing IT-Security (FLEIS) - Projektbericht

Suggested Citation: Rudel, Steffi; Kolb, Lisa (2024) : Federated Learning Enhancing IT-Security (FLEIS) - Projektbericht, ZBW – Leibniz Information Centre for Economics, Kiel, Hamburg

This Version is available at:
https://hdl.handle.net/10419/290556

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

Federated Learning Enhancing IT-Security (FLEIS)

Projektbericht

Dr. Steffi Rudel & Lisa Kolb (geb. Verlande)

Universität der Bundeswehr München,
Institut für Schutz und Zuverlässigkeit (Prof. Dr. Ulrike Lechner)

Inhaltsverzeichnis

1 Einführung ... 5

1.1 IT-Sicherheit im Human Resource Management ... 5

1.2 Das Forschungsprojekt FLEIS ... 5

1.3 Vorgehensweise und wissenschaftliche Methoden ... 6

1.4 Abgrenzung der Forschung ... 7

2 Arbeitspaket 2.3: Geschäftsprozesse identifizieren ... 8

2.1 Forschungsgegenstand und Forschungsfragen ... 8

2.2 Methoden und Ergebnisse ... 10

2.2.1 Literaturrecherche ... 10
2.2.2 Qualitative Erhebung & Auswertung ... 15
2.2.3 Modellierung der Geschäftsprozesse & IT-Infrastrukturmodelle ... 18
2.2.4 Workshops zur Schwachstellenanalyse ... 21

2.3 Zwischenfazit ... 23

3 Arbeitspaket 3.1: Anforderungsanalyse Anwender ... 24

3.1 Forschungsgegenstand und Forschungsfragen ... 24

3.2 Methoden und Ergebnisse ... 25

3.2.1 System Design: Kreativ-Workshop & Auswertung ... 26
3.2.2 Ergebnis System Design: Anforderungskatalog ... 29
3.2.3 UX: Qualitative Erhebung & Auswertung ... 30
3.2.4 Ergebnis UX: Anforderungskatalog ... 34

3.3 Zwischenfazit ... 34

4 Arbeitspaket 8.2: Kompetenzaufbau Cybersicherheit in Personalabteilungen ... 35

4.1 Forschungsgegenstand und Forschungsfragen ... 35

4.2 Methoden und Ergebnisse ... 36

4.2.1 Kenntnisstand IT-Sicherheit: Quantitative Erhebung & Auswertung ... 36
4.2.2 Kenntnisstand IT-Sicherheit: Ausgewählte Ergebnisse ... 39
4.2.3 Entwicklung, Durchführung und Validierung eines Trainings ... 45

4.3 Zwischenfazit ... 49

5 Arbeitspaket 8.1: Anwendungsszenario & Geschäftsmodellinnovationen ... 50

5.1 Forschungsgegenstand und Forschungsfragen ... 50

5.2 Methoden und Ergebnisse ... 51

5.2.1 Marktrecherche: Geschäftsmodelle HRM Startups ... 52

5.2.2 Die Methode Business Model Canvas 53
5.2.3 Durchgeführter Workshop 1 55
5.2.4 Durchgeführter Workshop 2 56
5.2.5 Auswertung Workshops 58
5.2.6 Ergebnis: Entwickeltes Geschäftsmodell FLEIS4Bayern 59
5.2.7 Ergebnis: Alternatives Geschäftsmodell FLUniBwM 60

5.3 Zwischenfazit 64

6 Zusammenfassung & Ausblick 65

7 Danksagung 66

8 Literatur 67

9 Anhang 70

1 Einführung

1.1 IT-Sicherheit im Human Resource Management

Ohne das richtige Personal kann kaum ein Unternehmen erfolgreich agieren, daher spielt der "Produktionsfaktor Mensch", trotz aller Digitalisierung, eine zentrale Rolle. Zuständig im Unternehmen ist für diese Ressource das Personalwesen (Human Resource Management HRM), das neben der Verwaltung und Entwicklung des vorhandenen Personals auch für die Beschaffung neuen Personals (Recruiting) zuständig ist (Scholz & Scholz, 2019).

Im Recruiting werden Bewerberdaten gesammelt, verarbeitet und gespeichert, um fundierte Personalentscheidungen treffen zu können, wobei sich sowohl interne als auch externe Kandidaten auf eine ausgeschriebene Stelle bewerben können. Mit Blick auf externe Bewerbungen ergibt sich nun ein für die IT-Sicherheit des Unternehmens kritischer Bereich, denn als zentrale Abteilung benötigt das HRM offene Schnittstellen zu externen Personen, die dem Unternehmen in der Regel unbekannten sind, um Interaktionen zu ermöglichen. Die eingehenden Bewerbungsunterlagen müssen vom Recruiter und Hiring Manager gesichtet werden, jedoch könnten Cyberkriminelle diesen Kommunikationskanäle missbrauchen, indem sie beispielsweise über Social Engineering (Salahdine & Kaabouch, 2019) oder andere Methoden versuchen, Schadsoftware in das Unternehmensnetzwerk einzuschleusen (Verhoeven, 2020).

Für Unternehmen ist es daher wichtig, im HRM und insbesondere im Rekrutierungsprozess geeignete Schutzmaßnahmen zu ergreifen, um die Sicherheit der zu verarbeitenden personenbezogenen Daten (gemäß Datenschutzgrundverordnung, DSGVO) zu gewährleisten. Dazu gehören unter anderem technische Maßnahmen, die Implementierung von Zugriffsbeschränkungen, die Schulung der Mitarbeitenden im Umgang mit sensiblen Daten sowie die regelmäßige Überprüfung der Systeme auf Schwachstellen (Bundesamt für Sicherheit in der Informationstechnik – BSI, 2017), (Moody et al., 2018).

1.2 Das Forschungsprojekt FLEIS

Das Projekt Federated Learning Enhancing IT-Security (FLEIS) war ein vom Freistaat Bayern gefördertes Forschungsprojekt im Förderprogramm „Informations- und Kommunikationstechnik“. In dem Verbundprojekt arbeiteten die beiden Unternehmen itWatch (als Experten für IT-Sicherheit, https://www.itwatch.de), Trevisto (als Experten für Künstliche Intelligenz, https://www.trevisto.de) sowie die Forschungseinrichtung Universität der Bundeswehr München (UniBw M, als Experten für wissenschaftliche Methoden) zusammen.

Inhaltlich beschäftigte sich FLEIS mit der Erkennung und proaktiven Abwehr von Cyberangriffen im HRM mittels föderierten, also verteilten Lernens (Federated Learning FL)[1].

Die UniBw M war dabei zu Beginn mit der Ermittlung des Ist-Zustands im HRM und der Erhebung der Geschäftsprozesse und der zugrundeliegenden IT-Infrastruktur beauftragt. Anschließend wurden die Anforderungen der Anwender an ein FL-System zur Verbesserung der IT-Sicherheit im HRM erhoben. Im dritten Schritt wurde der Kenntnisstand der Mitarbeitenden im HRM bezüglich IT-Sicherheit ermittelt und ein passendes Training zur Verbesserung dieser Kompetenzen entwickelt. Im letzten Schritt wurde für das von den Projektpartnern entwickelte FL-System eine explizite Geschäftssicht entwickelt.

Die folgende Abbildung 1 zeigt die Anteile der UniBw M am Projekt FLEIS.

Beschreibung der Arbeitspakete	2021			2022												2023								
	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9
AP2.3: Geschäftsprozesse identifizieren																								
AP3.1: Anforderungsanalyse Anwender																								
AP8.1: Anwendungsszenario & Geschäftsmodellinnovationen																								
AP8.2: Kompetenzaufbau Cybersecurity in Personalabteilungen																								

Abbildung 1: Arbeitspakete der UniBw M im Projekt FLEIS

1.3 Vorgehensweise und wissenschaftliche Methoden

Um ein angemessenes Sicherheitsniveau im HRM zu erreichen, war zunächst ein umfassendes Verständnis der Abläufe im Rekrutierungsprozess sowie der involvierten IT-Infrastruktur nötig. Daher wurde im Projekt FLEIS zunächst untersucht, wie Bewerberdaten im Recruiting erhoben, verarbeitet und gespeichert werden (**AP 2.3: Geschäftsprozesse identifizieren**). In diesem Zusammenhang wurde auch die beteiligte IT-Infrastruktur identifiziert und grafisch dargestellt. Im Zuge des Arbeitspaketes wurde abschließend eine Schwachstellenanalyse durchgeführt und dokumentiert. Als wissenschaftliche Methoden kamen eine systematische Literaturrecherche sowie Experteninterviews (ausgewertet nach (Kuckartz & Rädiker, 2022)) zur Anwendung, die daraus resultierenden Geschäftsprozesse wurden mit Hilfe der Business Process Model and Notation (BPMN) dargestellt. Für die Schwachstellenanalyse wurden zwei Workshops durchgeführt, die dabei gewonnenen Ergebnisse wurden mit Hilfe der Attack Tree Methode (Schneier, 1999) erarbeitet und dokumentiert.

[1] Der Begriff Federated Learning (FL) wurde 2016 von Google eingeführt. Bei FL geht es vor allem darum, sensible Daten von Personen oder Unternehmen zu schützen, indem jeder einzelne Client ein lokales KI-Modell auf Grundlage seiner eigenen Daten trainiert und lediglich Metadaten an den zentralen Server versendet (McMahan et al., 2016).

Im nächsten Schritt wurden die Anforderungen der Nutzer an das zu entwickelnde FL-System erhoben (**AP 3.1: Anforderungsanalyse Anwender**). Hierfür wurden eine Online-Umfrage sowie Leitfadeninterviews durchgeführt und ausgewertet. Darüber hinaus wurde ein digitaler Kreativ-Workshop realisiert, dessen Auswertung nach der Grounded Theory Methode (Glaser & Strauss, 2017) erfolgte. Als Ergebnis wurden zwei Anforderungskataloge „Service Design“ und „User Experience“ erstellt.

Darauffolgende wurden der Kenntnisstand und der Kompetenzaufbau zu IT-Sicherheit im HRM (**AP 8.2: Kompetenzaufbau Cybersicherheit in Personalabteilungen**) untersucht. Hierfür wurde zunächst eine quantitative Umfrage (Döring & Bortz, 2016) in deutschen Unternehmen durchgeführt und ausgewertet. Aufbauend auf den Ergebnissen wurde anschließend ein Training in Form eines Serious Games (Yasin et al., 2019) konzeptioniert, durchgeführt und ausgewertet. Bei der Entwicklung des Trainings wurden wissenschaftliche Grundlagen zur Kompetenzentwicklung berücksichtigt. Das Training wurde insgesamt viermal durchgeführt, dokumentiert und evaluiert.

Mittels einer Desk Research Methode wurden Geschäftsmodell für die mögliche Bereitstellung einer FL-Lösung ermittelt (**AP 8.1: Anwendungsszenario & Geschäftsmodellinnovationen**). Zusätzliche Workshops, welche auf der Business Model Canvas (Osterwalder & Pigneur, 2011) aufsetzen vertieften die gewonnenen Erkenntnisse und dienten als Grundlagen für die beiden Geschäftsmodelle „FLEIS4Bayern“ und „FLUniBwM“.

1.4 Abgrenzung der Forschung

Ein in der Forschung zur IT-Sicherheit bekannter Angreifertyp ist der sogenannte **Innentäter**. Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) definiert den (potenziellen) Innentäter als „sämtliche Personen mit (privilegiertem) Zugriff auf bzw. Zutritt zu IT-Komponenten, IT-Diensten, Installationen, Dokumenten oder sonstigen ggf. kritischen Informationen und Geräten“ ((BSI, 2018), S. 1).

Dieser Innentäter kann also eine erhebliche Gefahr für die IT-Sicherheit im Unternehmen darstellen – von der vorliegenden Forschung wird dieser Angreifer-Typ jedoch explizit ausgenommen. Der Grund hierfür ist, dass im Projekt FLEIS (siehe Kapitel 1.2) zusammen mit zwei Unternehmen eine technische Lösung zum Schutz von HRM vor Cyberangriffen erforscht wird, wobei der Fokus in diesem Projekt auf *externen* Bewerbenden liegt.

2 Arbeitspaket 2.3: Geschäftsprozesse identifizieren

Im Folgenden werden die Inhalte des Arbeitspaketes „*2.3 Geschäftsprozesse identifizieren*“ beschrieben. Dieses Arbeitspaket 2.3 ist (wie in Abbildung 1 zu sehen) das erste Arbeitspaket der UniBw M im Projekt FLEIS.

Die folgende Abbildung 2 zeigt die geplanten Inhalte des Arbeitspaketes.

AP 2.3: Geschäftsprozesse identifizieren	**6 PM (UniBw M)**
Zuständig	**Lead UniBw M, Mitarbeit alle**
Vorgehen	• Erstellung eines Leitfadens für die Experteninterviews • Erhebung & Abbildung der Geschäftsprozesse in Personalabteilungen • Erfassung der Systemarchitekturen, Datenquellen und Schnittstellen • Analyse der Schwachstellen • Ableitung möglicher Angriffsvektoren
Methoden	• Desk Research • Experteninterviews • Workshops • Geschäftsprozessmodellierung
Ergebnisse	• Durchgeführte, transkribierte und ausgewertete Experteninterviews • Durchgeführte und ausgewertete Workshops • Durchgeführte und dokumentierte Schwachstellenanalyse • Abbildung der Geschäftsprozesse, Architekturen, Datenquellen und Schnittstellen in geeigneter Form (z.B. BPMN) • Abgeleitete Angriffsvektoren

Abbildung 2: Geplante Inhalte des Arbeitspaketes 2.3

2.1 Forschungsgegenstand und Forschungsfragen

In jedem Unternehmen spielt das Personal bzw. der „Produktionsfaktor Mensch“ eine entscheidende Rolle. Das Human Resource Management (HRM) ist dabei für die Verwaltung dieser Ressource zuständig und nimmt eine unabdingbare Steuerungsfunktion in allen Unternehmen ein. So ist das HRM für die Verwaltung, Entwicklung und Personalbeschaffung zuständig. Die **Personalbeschaffung, auch als Recruiting** bezeichnet, steht hierbei im Fokus der vorliegenden Forschung ((Scholz & Scholz, 2019), S. 48).

Soll eine Position im Unternehmen neu besetzt werden, so wird in aller Regel ein Recruiting-Prozess angestoßen. Die folgende Abbildung 3 gibt einen Überblick über diesen Prozess.

Abbildung 3: Ablauf des Recruiting-Prozesses (Quelle: https://metajobs.it/recruiting-prozess/, 09.05.22)

Grundsätzlich können auf eine veröffentlichte Stellenanzeige Bewerbungsunterlagen von internen und externen Bewerbenden[2] eingehen. Gerade im Hinblick auf **externe Bewerbungen** entsteht nun ein Thema, das für die IT-Sicherheit von Unternehmen relevant ist: Damit aus externen Bewerbenden irgendwann Mitarbeitende eines Unternehmens werden können, muss das Recruiting die eingegangenen Bewerbungsunterlagen sichten. Diese wurden früher postalisch an Unternehmen versendet – heute gehen die Unterlagen in aller Regel digital beim Unternehmen ein. Das macht das Recruiting und somit auch das HRM anfällig für Angriffe und zu einem Einfallstor für Schadsoftware, welche mittels digitaler Unterlagen eingeschleust werden könnten.

Im vorliegenden Arbeitspaket 2.3 werden zunächst die Ist-Geschäftsprozesse sowie die beteiligte IT-Infrastruktur im Recruiting analysiert und modelliert.

Das Arbeitspaket 2.3 orientiert sich an folgenden **Forschungsfragen**:

> *F2.3.1: Wie sind die Geschäftsprozesse in Unternehmen unterschiedlicher Größen und Branchen im Recruiting gestaltet?*
>
> *F2.3.2: Welche IT-Infrastruktur ist unternehmensintern an diesem Geschäftsprozess beteiligt?*
>
> *F2.3.3: Wo können sich in diesem Recruitingprozess Angriffspunkte für Cyberangriffe ergeben? Wie können diese Angriffe ausgestaltet sein?*

[2] Als interne Bewerbende werden in der vorliegenden Arbeit Bewerbende definiert, welche bereits im Unternehmen angestellt sind und somit lediglich die Position wechseln möchten. Als externe Bewerbende werden dagegen Bewerbende bezeichnet, welche sich von außerhalb des Unternehmens auf die ausgeschriebene Stelle bewerben.

2.2 Methoden und Ergebnisse

Um die **Forschungsfrage F2.3.1** zu beantworten, wurden die Geschäftsprozesse im Recruiting erhoben. Dazu wurde zunächst eine Literaturrecherche durchgeführt. Anschließend wurden Interviews mit Unternehmen verschiedener Branchen und Größen geführt, als Methode wurden Leitfadeninterviews gewählt. Zur Auswertung wurden die Interviews anschließend transkribiert, nach der Methode von Kuckartz codiert und mit Hilfe der Business Process Model and Notation (BPMN) dargestellt.

Aus den ausgewerteten Interviews sowie den Prozessmodellen wurden anschließend IT-Infrastrukturmodelle erstellt (**Forschungsfrage F2.3.2**). Diese IT-Infrastrukturmodelle bildeten zusammen mit den Prozessmodellen die Grundlage für zwei anschließende Workshop zur Schwachstellenanalyse (**Forschungsfrage F2.3.3**). Als Ergebnis dieser Workshops wurden mögliche Angriffsvektoren in Form von Attack Trees dokumentiert.

2.2.1 Literaturrecherche

Um den aktuellen Stand der Wissenschaft zu erheben, wurde im Oktober 2021 zunächst eine systematische Literaturrecherche durchgeführt.

Als Suchwörter wurden folgende Begriffe festgelegt:

Tabelle 1: Suchwörter Literaturrecherche AP 2.3

Alternative Suchwörter	Detail	Forschungsfrage
Personalabteilung **Human Resources Management**	Bezeichnung der Abteilung	F2.3.1
Bewerbung **Recruiting** **Dokumente** **Unterlagen**	Bewerbungsunterlagen, die zugeschickt werden sowie zugehöriger Prozess	F2.3.1
Prozess **Geschäftsprozess**	Geschäftsprozesse des Recruiting-Prozesses	F2.3.1
Schnittstellen **Weitergabe**	Schnittstellen und wie Unterlagen im Unternehmen während des Recruiting-Prozesses weitergegeben werden	F2.3.1, F2.3.2
IT-System	Am Recruiting-Prozess beteiligte IT-Systeme	F2.3.2

Angriffe **Schadsoftware** **Malware** **Cyberangriff** **Hacker** **IT-Sicherheit** **Cybersecurity**	Aspekte der IT-Sicherheit	F2.3.3

Als Plattform für die Recherche wurde der OPAC+ der Bibliothek der Universität der Bundeswehr München verwendet und die Zeitspanne für die Literatur auf 2010 bis 2021 eingeschränkt.

Die **erste Suche** wurde für die Forschungsfrage F2.3.1 ausgeführt. Dafür wurden die Begriffe

Personalabteilung, Human Resource, Bewerbung, Recruiting, Dokument*, Unterlage*, *prozess*

in unterschiedlichen Kombinationen und Verknüpfungen (AND, OR) genutzt. Die Auswertung der aufgefundenen Literatur ergab für die Forschungsfrage

> *F2.3.1: Wie sind die Geschäftsprozesse in Unternehmen unterschiedlicher Größen und Branchen im Recruiting gestaltet?*

folgende relevante Quellen:

(Reitgruber, 2017) teilt die Einführung / Nutzung von IT-Systemen in Personalabteilungen in zwei Teile ein: organisatorisch und technisch (S. 13). Dabei betont sie, dass IT-Prozesse unterstützen, nicht dominieren soll (S. 15).

(Ullah & Witt, 2018) stellte fest, dass gerade kleine und mittlere Unternehmen (KMU) nicht über genügend Ressourcen im HRM verfügen, um eine Spezialisierung vornehmen zu können. Vielmehr wäre es so, „dass in kleineren Unternehmen nur eine Person zuständig ist für die Personalbetreuung und Rekrutierung.“ (S. 27). Im weiteren Verlauf gehen sie, ähnlich wie (Fliegen, 2020) zwar auf den Recruiting-Prozess ein (S. 85ff.), der Dokumentenfluss sowie die IT-Komponenten werden jedoch nicht weiter vertieft. Die Digitalisierung wird zwar immer wieder aufgegriffen, dabei geht es jedoch eher um die Anwendung von digitalen Systemen zur Unterstützung der Mitarbeitenden (z.B. die Nutzung von Plattformen mit Jobbörsen im Internet oder Social Media für die Ausschreibungen). Die technische Sicht auf die IT-Prozesse und deren Sicherheit liegen nicht im Fokus dieser Studie. In Kapitel 3.6 erwähnen Ullah & Witt explizit Bewerbermanagementsysteme: „In Anbetracht der Datenschutzdiskussionen in Deutschland und der Regularien ist allerdings die Anschaffung eines

Bewerbermanagementsystems [im Kontrast zur E-Mail-Bewerbung, Anm. der Autorin] ratsam.“ (S. 132). In Kapitel 3.6 werden Job-Aggregatoren als Alternative oder als Ergänzung zu den Bewerbermanagementsystemen vorgestellt (S. 164-165), auch hier wird jedoch nicht im Detail auf die Informationstechnische Sicht eingegangen.

(Fliegen, 2020) geht zwar auf den gesamten Recruiting-Prozess (S. 11ff.) und damit auch auf die aufeinanderfolgenden Phasen ein, bleibt dabei jedoch bei der Betrachtung der „Anwendersicht“ von HRM (was ist wann und wie zu tun?). Der Geschäftsprozess im Unternehmen (welche Dokumente werden wann und wo im Unternehmen genutzt?), insbesondere in Kombination mit IT-Komponenten, werden nicht thematisiert.

Das Herausgeberwerk von (Petry & Jäger, 2021) erweist sich als sehr umfangreiches Werk, welches auf über 500 Seiten umfassend zum Thema Digital-HR informiert. Es wird an vielen Stellen auf die Veränderung im HRM und speziell im Recruiting durch die Digitalisierung eingegangen (z.B. E-Recruiting, Robot-Recruiting oder Mobile Recruiting, Recruiting Chatbots, KI-basiertes Recruiting, Data Driven Recruiting etc.), der Geschäftsprozess des Recruitings aus technischer und IT-Sicherheits-Perspektive wird jedoch nicht thematisiert.

Der Beitrag (Holm, 2012) fokussiert sich auf den Prozess des E-Recruitings, lieferte jedoch auch eine Erkenntnis zum Geschäftsprozess einer papierbasierten Bewerbung: „*In the case of recruitment, this process is normally performed for either internal customers – line managers and executives from various parts of the organisation - or external ones, e.g. clients, resulting in a shortlist of candidates which customers can choose from*.“ (S. 243). Zur technischen IT-Sicht auf den Recruiting-Prozess konnte keine Erkenntnis aus dieser Quelle gezogen werden.

(Jäger, 2012) erwähnt in seinem Beitrag die Vorteile von Bewerbermanagementsystemen als zentrales System. Bezüglich der Prozesse oder IT-Infrastruktur im Recruiting können aus dem Beitrag jedoch keine verwertbaren Informationen entnommen werden.

(Frintrup & Piechowski, 2011) gehen in ihrem Artikel auf Prozessverbesserungen im Recruiting mittels Integration der Prozesse ein, fokussieren sich jedoch auf die personaldiagnostische Perspektive (also die Auswahl geeigneter Bewerber nach Eingang der Bewerbungen). In dem Artikel ist zwar ein Workflow des Recruitings abgebildet, jedoch können aus diesem aufgrund der erwähnten Fokussierung auf die Personalauswahl keine Erkenntnisse für die Forschungsfrage gezogen werden.

Der Beitrag (Hartmann, 2015) geht darauf ein, dass Prozessen in der Personalabteilung häufig nicht die Bedeutung beigemessen wird, welche ihnen eigentlich strategisch zusteht und dadurch ein systematisches Geschäftsprozessmanagement fehlt. Bewerbermanagement-Systemen misst er hohe Bedeutung zu, da diese sowohl die „Servicequalität gegenüber dem Kandidaten“ erhöhen (S. 224) als auch Prozesskosten senken und Durchlaufzeiten reduzieren kann.

Außerdem propagiert der Beitrag „medienbruchlose, IT-unterstützte Beschaffungsprozesse“ (S. 224). Eine Prozessmodellierung oder Sicht auf die IT-Infrastruktur bietet der Beitrag nicht.

In (Muenstermann et al., 2010) wurden im Rahmen einer Fallstudie mehrere Recruiting-Prozesse in einem Unternehmen erhoben und diese im nächsten Schritt in einem einzigen, neuen Standard-Prozess neugestaltet. Die erhobenen (bisherigen) Recruiting-Prozesse werden in dem Beitrag nicht im Detail beschrieben, lediglich der neue, standardisierte Prozess wird vorgestellt; Dabei werden die Schritte *Sourcing – Incoming Applications – Pre-selection – Final selection and employment* verbal sowie grafisch dargestellt. Es wird ausgeführt, dass eine standardisierte Bewerber-Datenbank eingeführt wurde, die direkt aus einem Bewerber-Formular (übers Internet erreichbar) gespeist wird. Je nach Bewerbergruppe sind Bewerbungen nur noch über dieses Formular (über die unternehmenseigene Webseite) oder per E-Mail möglich. Nachdem die Bewerbungen erfasst wurden, werden diese durch HRM geprüft. Die Weitergabe interessanter Kandidaten an die Fachabteilung geschieht über eine standardisierte E-Mail, welche die HTML-Ansicht des Profils des Bewerbenden in einer internen Bewerber-Datenbank ermöglicht („*If a recruiter identifies an appropriate candidate for a given vacancy, the profile of this candidate is sent to the operating department by a standardized email using the company's internal email system. A standardized email contains a hyperlink to the profile of the particular applicant displayed on an HTML page.* “ S. 933). Durch die Verwendung dieses führenden, neuen IT-Systems werden laut dem Beitrag Medienbrüche beseitigt und viel Kommunikation mit dem Bewerbenden kann automatisiert ablaufen. Dadurch wird der Recruiting-Prozess verkürzt und Kosten werden eingespart. Für die Forschungsfrage F2.3.1 können hier einige Anhaltspunkte für den Recruiting-Prozess in Unternehmen herausgelesen werden.

Die **zweite Suche** wurde für die Forschungsfrage F2.3.2 ausgeführt. Dafür wurden die Begriffe

*Personalabteilung, Human Resource, IT-System**

in unterschiedlichen Kombinationen und Verknüpfungen (AND, OR) genutzt. Die Auswertung der aufgefundenen Literatur ergab für die Forschungsfrage

> *F2.3.2: Welche IT-Infrastruktur ist unternehmensintern an diesem Geschäftsprozess beteiligt?*

folgende relevanten Quellen:

(Wagner & Patzak, 2020) beschreiben einige interessante Aspekte zum Prozessmanagement sowie zu der Modellierungsmethode BPMN, die Verknüpfung zur IT-Struktur im HRM fehlt jedoch.

(Strohmeier, 2008) geht umfassend auf IT-Systeme in Personalabteilungen ein. Den Beschaffungsmanagementsystemen, zu denen er auch Bewerbermanagementsysteme zählt, widmet er ein komplettes Kapitel (Kap. 16, S. 201-214) und geht ausführlich auf beteiligte IT-Systeme sowie deren Schnittstellen-Kommunikation ein. Die folgende Abbildung 4 zeigt die „idealtypische Architektur“ der beteiligten IT-Systeme.

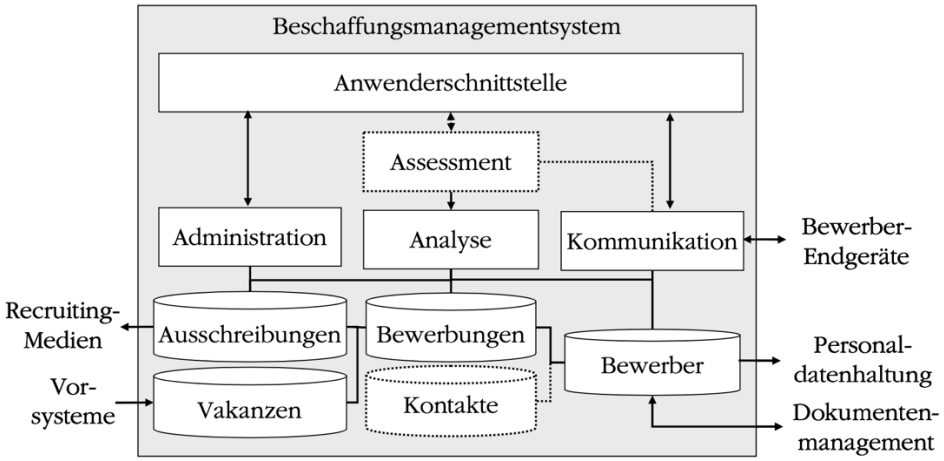


Abbildung 4: Idealtypische Architektur von Beschaffungsmanagementsystemen ((Strohmeier, 2008), S. 201)

Bezüglich der Datenhaltungskomponenten (Kap. 16.1.1) werden unter anderem die Bewerbungs-, die Bewerber- sowie die Kontaktdatei beschrieben (S. 203-204). Betreffend der Kommunikationskomponente (Kap. 16.1.3) wird unter anderem auf E-Mail und Online-Formular eingegangen (S. 206-207).
Darüber hinaus wird im Kapitel 6 das Dokumentenmanagementsystem beschrieben (S. 81-91), welches für die Ablage sowie den Zugriff auf Dokumente im HRM zuständig ist.
Die Informationen aus dem Buch wurden später für die Erarbeitung der IT-Infrastrukturen (siehe Kapitel 2.2.3) verwertet.

Die **dritte Suche** wurde für die Forschungsfrage F2.3.3 ausgeführt. Dafür wurden die Begriffe

Personalabteilung, Human Resource, Angriff, Schad, Malware, Cyberangriff, Hacker, IT-Sicherheit, IT-Security, Cybersecurity*

in unterschiedlichen Kombinationen und Verknüpfungen (AND, OR) genutzt. Die Auswertung der aufgefundenen Literatur ergab für die Forschungsfrage

> *F2.3.3: Wo können sich in diesem Recruitingprozess Angriffspunkte für Cyberangriffe ergeben? Wie können diese Angriffe ausgestaltet sein?*

folgende relevante Quellen:

(Satter, 2017) beschreibt den Diebstahl personenbezogener Daten als mögliche Folgen eines Cyberangriffs auf Unternehmen. Darüber hinaus nennt der populärwissenschaftliche Beitrag acht Maßnahmen, die ergriffen werden können.

Der ebenfalls populärwissenschaftlich einzuordnende Beitrag (Erickson, 2018) beschäftigt sich explizit mit Cyberangriffen auf die HRM-Abteilung und trägt ebenfalls Maßnahmen zusammen. In dem Beitrag wird explizit der Innentäter als Gefahr erwähnt.

Im Beitrag von (Clearswift, 2015) wird eine Studie vorgestellt, nach der die Finanzabteilung sowie HRM die gefährdetsten Abteilungen bezüglich Datenverlusts im Unternehmen sind. Auch dieser Beitrag ist in die Kategorie populärwissenschaftlich einzuordnen.

2.2.2 Qualitative Erhebung & Auswertung

Zunächst galt es herauszufinden, wie sich die Recruitingprozesse in deutschen Unternehmen darstellen. Dazu wurde die Methode der qualitativen Interviews in Form von Experteninterviews in der Ausprägung von Leitfaden-Interviews gewählt. Für den Leitfaden wurden 15 Fragen identifiziert, wobei nur die ersten zwölf Fragen (1-12) der Abbildung der Geschäftsprozesse dienen sollten. Darüber hinaus war die Absicht, bereits in diesem Arbeitspaket einen Eindruck von der IT-Sicherheit im jeweils befragten Unternehmen zu erhalten; daher wurden vier weitere Fragen (12-15) ergänzt.

Die folgende Tabelle 2 listet die Fragen der Experteninterviews auf:

Tabelle 2: Leitfaden der Interviews im AP 2.3

Frage	Inhalt	Geschäftsprozesse abbilden	Eindruck IT-Sicherheit
1	Welche Unterlagen erhalten Sie im Laufe des Bewerberprozesses wann von wem?	x	
2	Über welche Kanäle kommen diese Unterlagen zu Ihnen? (Klassische und neue wie Twitter, WhatsApp, …)	x	
3	Wie viele Bewerbungen erhalten Sie etwa im Monat/Jahr? Wie viele davon sind Initiativ-Bewerbungen, grob geschätzt?	x	
4	Kommen Unterlagen auch manchmal über andere Kanäle/an andere Personen an? Wenn ja, welche und wo?	x	
5	Wie sieht es mit Unterlagen aus, die nachgefordert werden müssen - wie ist da der Ablauf und welche Systeme sind dann beteiligt?	x	
6	Arbeiten Sie evtl. mit einem externen Dienstleister im Bewerberprozess zusammen (wie z.B. Arbeitsamt, Dienstleister wie Stepstone o.ä.)? Wie unterstützen diese externen Dienstleiter Ihren Prozess?	x	

7	Wie gehen Sie mit den erhaltenen Unterlagen um? Öffnen Sie alles oder geben Sie auch Unterlagen ungesehen weiter?	x	
8	An wen geben Sie wann welche Unterlagen weiter?	x	
9	Über welche Kanäle geben Sie diese Unterlagen weiter?	x	
10	Welche IT-Systeme und Programme sind an dem Prozess beteiligt?	x	
11	Welche Art von Unterlagen erhalten Sie bei Bewerbungen?	x	
12	Gab es schon einmal einen Vorfall zur IT-Sicherheit in Ihrer Abteilung? Was war da passiert? Wie ging es dann weiter?		x
13	Gibt es Vorgaben zur IT-Sicherheit zu den hereinkommenden Unterlagen? Wenn ja, welche?		x
14	Welche Hilfestellung/Unterstützung haben Sie zum Schutz vor Cyberangriffen? (Vertiefung: z.B. Programme, Personen, Vorgehensvorschriften, …)		x
15	Gibt es Schulungen in Ihrem Unternehmen zur IT-Sicherheit? Und speziell für HRM (Human Resource Management)?		x

Nach intensiver Suche nach Interviewpartnern konnten schließlich zwölf Unternehmen befragt werden. Die Interviews wurden aufgrund der Corona-Pandemie ausnahmslos online durchgeführt und dauerten im Durchschnitt ca. 30 Minuten. Sie wurden im Zeitraum von Dezember 2021 bis Februar 2022 erhoben.

Die folgende Tabelle 3 zeigt die Übersicht der interviewten Unternehmen.

Tabelle 3: Befragte Unternehmen im AP 2.3

ID	Art des Unternehmens / Branche	Anzahl Mitarbeitende im Unternehmen (ca.)	Bewerbungen pro Jahr (ca.)
1	Beratungsunternehmen	10	30
2	IT-Unternehmen	30	200
3	Technologieunternehmen	50.000	135.000
4	Forschung & Wissenschaft	Bereich ca. 12	100
5	Bildungseinrichtung	60	80
6	IT-Unternehmen	9.000	20.000
7	Pharma-Dienstleistungen	650	1.800
8	Lebensmittelherstellung	100	1.000
9	Versorgungsunternehmen	450	1.000
10	Versicherung	7.000	8.500
11	Chemiebranche	1.300	550
12	Forschung & Wissenschaft	Gesamt ca. 50	600

Im nächsten Schritt wurden die Interviews im Software-Werkzeug MaxQDA wörtlich transkribiert. Zur Auswertung der Interviews wurde die Methode der inhaltlich strukturierenden Inhaltsanalyse nach Kuckartz angewandt (Kuckartz, 2018).

Die folgende Abbildung 5 zeigt das generelle Vorgehen.

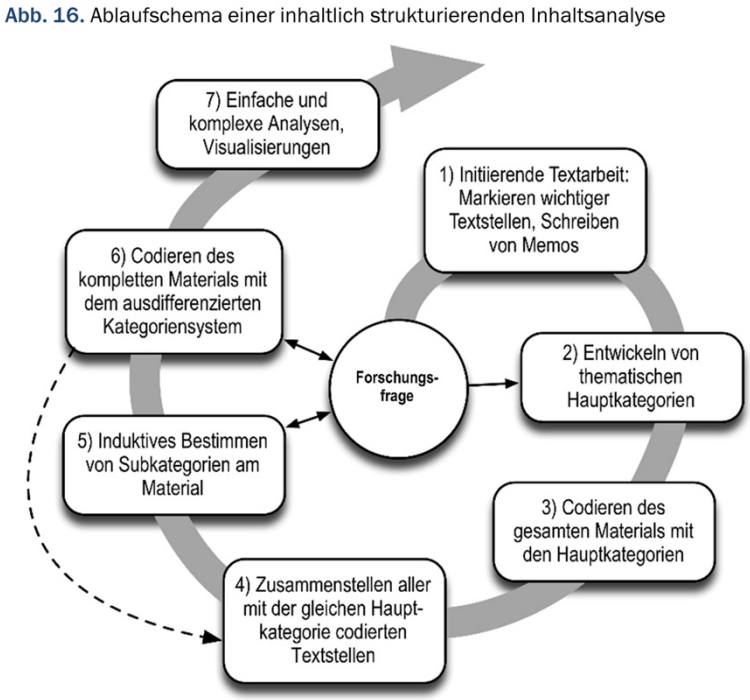


Abbildung 5: Generelles Ablaufschema einer inhaltlich strukturierenden Inhaltsanalyse nach (Kuckartz, 2018), S. 100

Für die Codierung und zur Festlegung des Kategoriensystem (Haupt- und Subkategorien) wurde im Team gearbeitet. Mehrere Teammitglieder codierten zunächst unabhängig voneinander mehrere Interviews und erstellten ein zugehöriges Kategoriensystem. Anschließend wurden diese Codierungen und Kategoriensysteme verglichen und ein einheitliches Kategoriensystem mit zugehörigen Codes festgelegt (Tabelle 4).

Tabelle 4: Kategoriensystem und zugehörige Codes der qualitativen Interviews im AP 2.3

Code		Erläuterung
Hauptkategorie	Subkategorie	
IT-Sicherheit		
	Reaktive Maßnahmen	Was wird oder wurde nach einem Vorfall gemacht?
	Vorfälle	Ist schon mal etwas passiert?
	Präventiv-maßnahmen	Vorgaben, Schulungen, Belehrungen etc.

Verhalten / Umgang mit Dokumenten		Was wird mit den Unterlagen gemacht, wie werden sie weitergegeben etc.
Personen / Abteilungen		Welche Personen und Abteilungen sind an den Prozessen beteiligt?
IT-Service		Alle IT-Services: externe (LinkedIn, Stepstone, E-Mail), interne (Bewerbermanagementtool) und die Übertragungswege per Mail oder Tool (wie Teams etc.)
Dokumententyp		PDF, Bilddatei, Word-Dokument, Link, Webseite etc.

2.2.3 Modellierung der Geschäftsprozesse & IT-Infrastrukturmodelle

Aus den so ausgewerteten Interviews wurde im nächsten Schritt die Prozesssicht der Geschäftsprozesse im Recruiting mit Hilfe der Business Process Model and Notation (BPMN) dargestellt (Freund & Rücker, 2019), (Fleischmann et al., 2018). Es wurde hierfür die Version BPMN 2.0 genutzt (BPM Offensive Berlin, o. J.), wobei lediglich der Pool[3] „Unternehmen“ ausformuliert wurde. Diese Vereinfachung wurde angewandt, da die Vorgänge im Pool „Unternehmen“ im Fokus der vorliegenden Forschung stehen und die Aufmerksamkeit daher auf die Prozesse dieses Akteurs gelenkt werden sollten. Zeitlichen Aspekte im Sinne von Wartezeiten etc. wurden im Modell nicht modelliert.

Die Modelle wurden in der kostenfreien Online-Version „Business Process Modeling“ des Anbieters Cawemo (https://cawemo.com/) erstellt. Die Versionen der Modelle wurden im internen FLEIS-Team fortlaufend vorgestellt und diskutiert, so dass sie iterativ weiterentwickelt werden konnten, bis nach mehreren Versionen schließlich die endgültigen Prozessmodelle feststanden.

In den folgenden Grafiken sind die Geschäftsprozesse für die Hauptkanäle E-Mail (Abbildung 6) und ATS (Abbildung 7) dargestellt.

[3] In BPMN-Modellen werden die Akteure eines Prozesses in sog. Pools dargestellt, wobei die Pools wiederum mit Swimlanes unterteilt werden können. So stellen im Recruiting-Prozess beispielsweise die Bewerbenden und das Unternehmen jeweils eigene Pools dar, während das Unternehmen mittels Swimlanes, z.B. in HRM und Fachabteilungen, unterteilt werden kann.

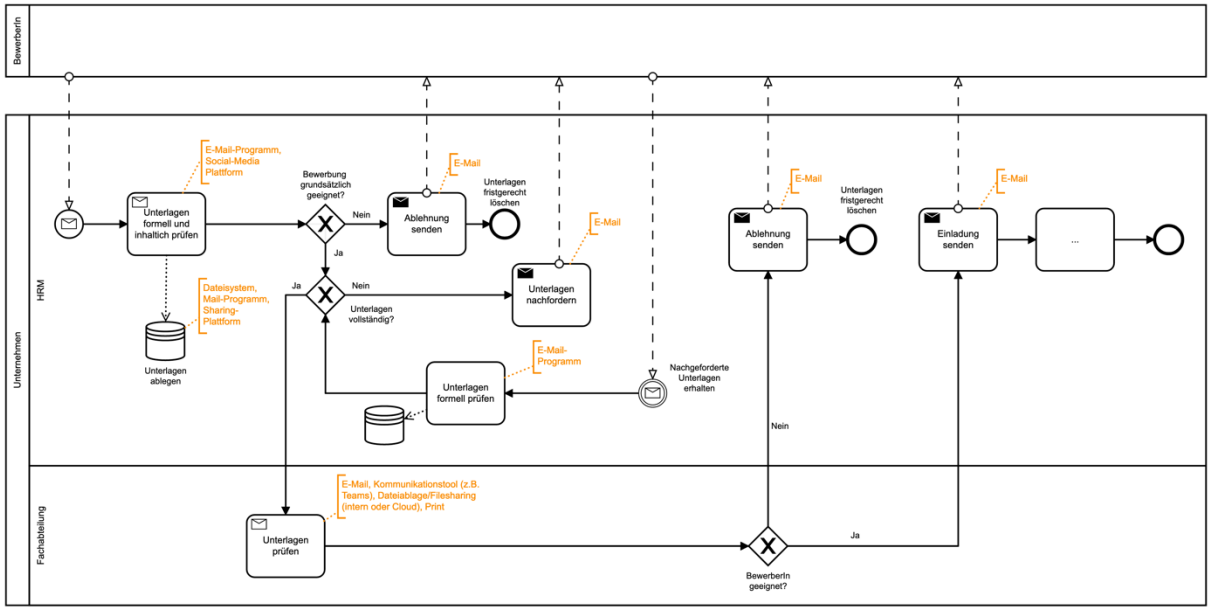


Abbildung 6: BPMN-Prozessmodell des Szenarios E-Mail

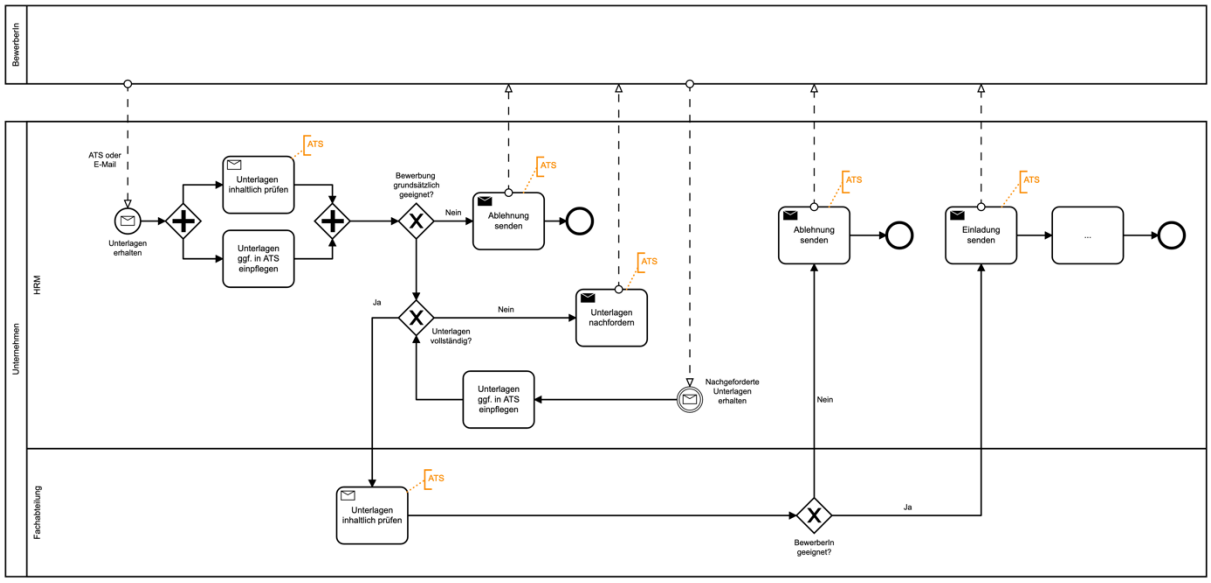


Abbildung 7: BPMN-Prozessmodell des Szenarios Bewerbermanagement-Tool (Applicant Tracking System, ATS)

Aus den ausgewerteten Interviews sowie den Prozessmodellen wurden im nächsten Schritt IT-Infrastrukturmodelle erstellt. Diese sollten als Diskussionsgrundlage für die Workshops zur Schwachstellenanalyse dienen. Die Infrastrukturmodelle wurden in MS Powerpoint erstellt und ebenfalls iterativ durch fortlaufende Diskussion im Team über mehrere Versionen schrittweise verbessert.

Die folgenden Grafiken zeigen die final entstandenen IT-Infrastrukturmodelle für die beiden Szenarien E-Mail (Abbildung 8) und ATS (Abbildung 9).

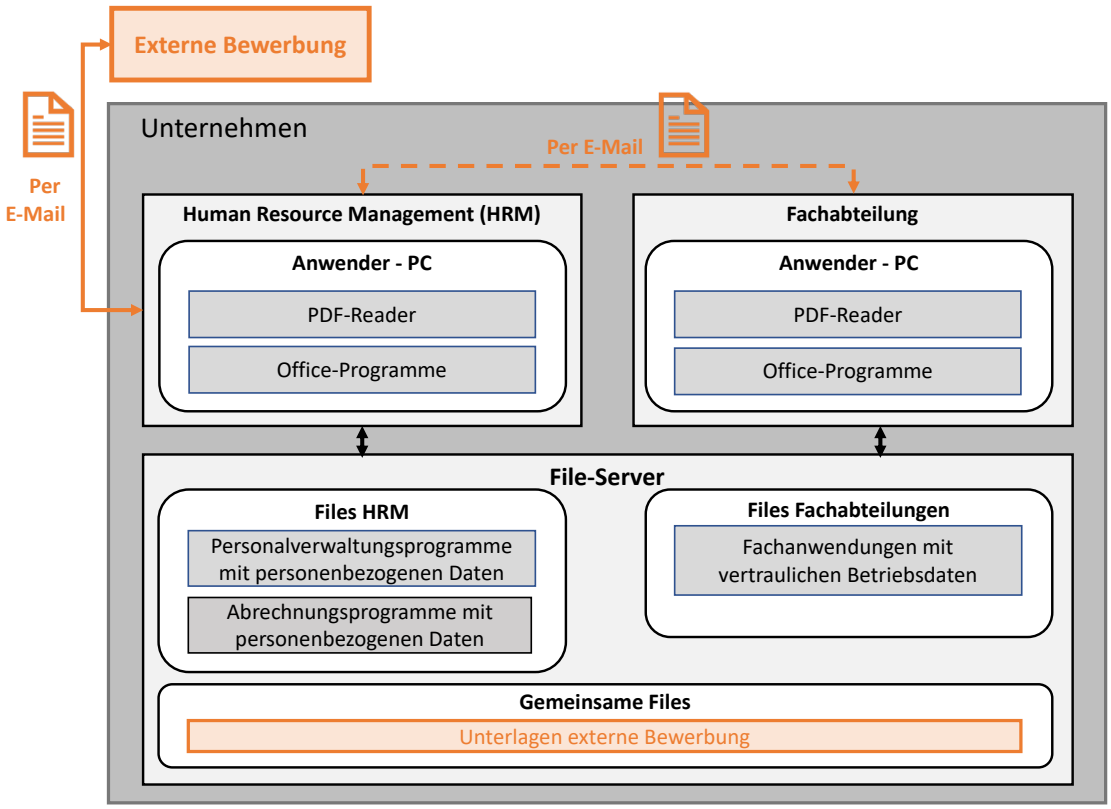


Abbildung 8: IT-Infrastrukturmodell des Szenarios E-Mail

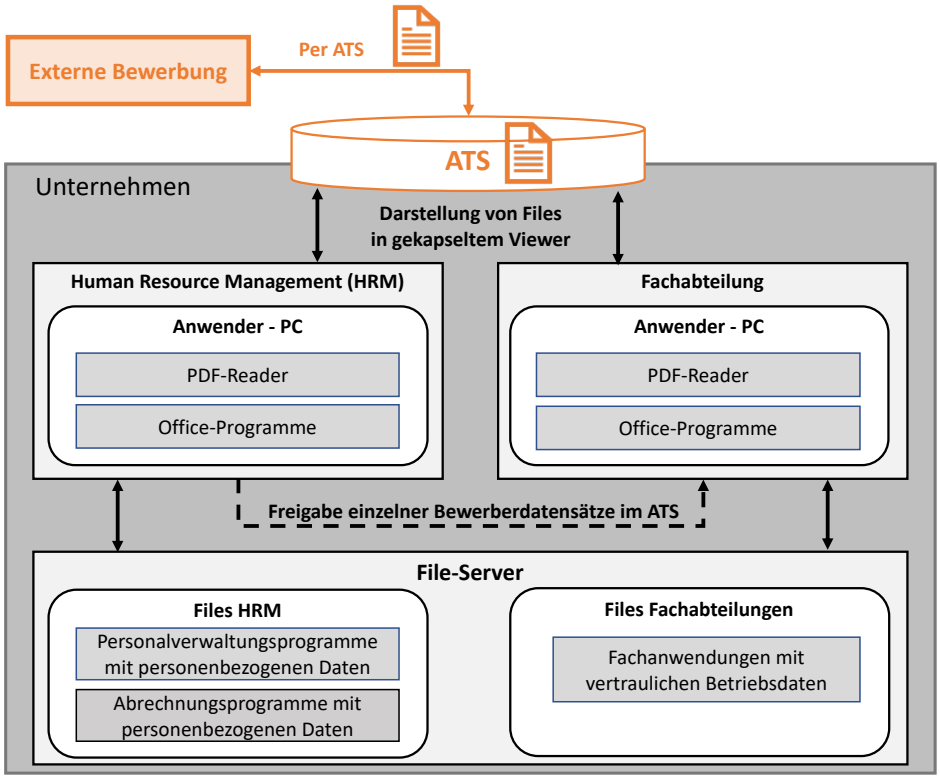


Abbildung 9: IT-Infrastrukturmodell des Szenarios ATS

2.2.4 Workshops zur Schwachstellenanalyse

Die identifizierten Geschäftsprozesse und IT-Infrastrukturen wurden anschließend einer Schwachstellenanalyse unterzogen. Dafür wurde methodisch auf einen institutsinternen Workshop der UniBw M, sowie auf einen Workshop mit den Projektpartnern von FLEIS zurückgegriffen. Beide Workshops waren im zeitlichen Ablauf gleich, organisatorisch unterschied sich das Vorgehen nur leicht. Als Methode zur Schwachstellenanalyse wurden Attack Trees (Schneier, 1999) gewählt.

Beide Workshops enthielten eine kurze Einführung, über die Thematik und die Methode der Attack Trees. Die darauffolgende Arbeitsphase zur Erarbeitung der Attack Trees erfolgte in zwei Runden, welche das Szenario E-Mail und das Szenario ATS enthielten. Zum Abschluss der Workshops erfolgte jeweils eine kurze Zusammenfassung.

Bei der Erarbeitung der Attack Trees wurden explizit Pfade modelliert, welche das Zusenden digitale Unterlagen beinhaltete. Andere Möglichkeiten, welche sich z.B. physikalischer Werkzeuge bedienen (manipulierter USB-Stick), wurden ausgeschlossen, da sie nicht im Fokus des Projektes FLEIS liegen.

Zunächst wurde am 01.06.2022 der interne Workshop (Teilnehmer n=6) mit einer Dauer von drei Stunden durchgeführt. Die Attack Trees wurden jeweils in Einzelarbeit von den Teilnehmenden erstellt und sind im Anhang enthalten.

Im zweiten Schritt wurde am 29.06.2022 ein inhaltsgleicher Workshop mit den Projektpartnern in FLEIS (im Rahmen eines Projekttreffens) mit zehn Teilnehmenden durchgeführt. In diesem Workshop wurden, aufgrund der höheren Teilnehmerzahl, die Arbeitsphasen in Gruppen durchgeführt: Es wurden drei Gruppen zu drei bis vier Personen gebildet, die im Team jeweils einen (oder mehrere) gemeinsame Attack Trees erarbeiteten. Eine dieser Personen stammte aus dem Team der UniBw M und fungierte als Betreuer des jeweiligen Teams. Die entstandenen Attack Trees sind im Anhang enthalten.

Aus der Untersuchung und Abbildung der Abläufe und Strukturen im Rekrutingprozess sowie die Auswertung der Attack Trees konnten folgende Erkenntnisse für die IT-Sicherheit im Recruiting gewonnen werden:

Sensibilisierung
Als Hauptangriffsziele haben sich in den Attack Trees unter anderem Social Engineering, das Einschleusen von Malware über Phishing-E-Mails und Ransomware als Drive-by-Angriff herauskristallisiert. Daher zielt die erste Empfehlung auf die Sensibilisierung der Mitarbeitenden im HRM, Abteilungsleitenden und Hiring Manager ab. Es wird empfohlen, Mitarbeitende, die häufig digitale Unterlagen von externen, unbekannten Quellen erhalten, durch regelmäßige Schulungen verstärkt für die Gefahren von Angriffen über den Bewerbungsprozess zu sensibilisieren. Hintergrund diese Empfehlung ist, dass der vermehrte Kontakt mit Externen dazu führen kann, dass die betreffenden Mitarbeitenden externe Quellen weniger als Gefahr wahrnehmen; dies gilt insbesondere, wenn sie selbst keine schlechten Erfahrungen gemacht haben (Overtrust-Effekt gemäß (Verhoeven, 2020)).

Überwachung von Kommunikationswegen
Wie aus den Prozess- und Infrastrukturmodellen abzulesen ist, werden insbesondere innerhalb von KMU Unterlagen von Bewerbenden per E-Mail oder über einen gemeinsamen Fileserver weitergeleitet. Daher wird empfohlen, zusätzliche technische Mittel einzusetzen, um interne Kommunikationswege zu überwachen und so die Angriffserkennung zu unterstützen. Dies könnte z.B. über die Integration einer demilitarisierten Zone (DMZ) erfolgen. Diese Erweiterung der technisch/organisatorischen Maßnahmen zur Stärkung der IT-Sicherheit erscheint insbesondere empfehlenswert, da die Angriffsraten und -arten exponentiell steigen und so herkömmliche Antivirenprogramme und Spamfilter aufgrund der zunehmenden Vielfalt nicht alles abdecken können (European Union Agency for Cybersecurity ENISA, 2022). Denkbar wäre hier auch der Einsatz spezialisierter, auf künstlicher Intelligenz basierender IT- Sicherheitsdienste zur Überwachung der Kommunikationswege (Sarker et al., 2021).

Gekapselte Umgebung
Vor allem anhand der Infrastrukturmodelle lassen sich die Schwachstellen einer nicht abgeschirmten Umgebung schnell erkennen. So könnte für das Szenario E-Mail insbesondere die Weiterleitung der Unterlagen an die Fachabteilung sowie die gemeinsam genutzten Files eine Gefahr darstellen, durch die sich eine unentdeckte Malware schnell im Unternehmen verbreiten könnte. Im Szenario ATS scheint diese Gefahr nicht gegeben, da die Bewerbungsunterlagen in einem gekapselten System vorgehalten werden. Eine Empfehlung ist daher, auch in KMU über die Integration einer gekapselten Umgebung (Fileserver oder ATS) nachzudenken, da diese die Verbreitung von Malware im gesamten Unternehmen minimieren kann. Wichtig ist jedoch, das Herunterladen von Dokumenten aus dem gekapselten System technisch zu unterbinden, da ansonsten gerade die Einschleusung von Malware über Drive-By-Angriffe ins Unternehmen weiterhin möglich ist.

2.3 Zwischenfazit

Zunächst lässt sich sagen, dass in der wissenschaftlichen Literatur bisher nur wenig zum Thema Geschäftsprozesse und beteiligte IT-Infrastruktur im Recruiting zu finden ist. Auch das Thema IT-Sicherheit im HRM wird wenig betrachtet.

Aus den geführten Interviews konnten die Geschäftsprozesse sowie die beteiligte IT-Infrastruktur bezüglich des Recruiting-Prozesses für Unternehmen aller Größen und Branchen abstrahiert werden, wobei sich die Unterteilung in die Szenarios E-Mail und ATS bewährt haben. Diese Modelle stehen der Wissenschaft zur weiteren Forschung zur Verfügung.

Aus der abschließenden Schwachstellenanalyse konnte diverse Angriffe in Attack Trees dargestellt und Implikationen für die IT-Sicherheit im HRM abgeleitet werden. Diese Modelle und Implikationen stehen der Wissenschaft zur weiteren Forschung zur Verfügung.

3 Arbeitspaket 3.1: Anforderungsanalyse Anwender

Im Folgenden werden die Inhalte des Arbeitspaketes *3.1 Anforderungsanalyse* beschrieben. Dieses Arbeitspaket 3.1 ist (wie in Abbildung 1 zu sehen) das zweite Arbeitspaket der UniBw M im Projekt.

Die folgende Abbildung 10 zeigt die geplanten Inhalte des Arbeitspaketes.

AP 3.1: Anforderungsanalyse Anwender	**6 PM (UniBw M)**
Zuständig	**Lead UniBw M, Mitarbeit alle**
Vorgehen	• Verfeinerung des Leitfadens für die Interviews auf Basis 2.3 • Erhebung, Abbildung & Priorisierung der Anforderungen in Personalabteilungen
Methoden	• Desk Research • Experteninterviews • Workshops
Ergebnisse	• Durchgeführte, transkribierte und ausgewertete Experteninterviews • Durchgeführte und ausgewertete Workshops • Abgeleiteter Anforderungskatalog mit priorisierten Anforderungen

Abbildung 10: Geplante Inhalte des Arbeitspaketes 3.1

3.1 Forschungsgegenstand und Forschungsfragen

Nachdem im Arbeitspaket 2.3 zunächst die Prozesse und IT-Infrastrukturen im Recruiting-Prozess erarbeitet und dargestellt wurden, unterstützt das Arbeitspaket 3.1 den nächsten Schritt in der Designforschung in Richtung FL-Dienstleistung. Dazu sollen die Anforderungen an das System erfasst werden, wie es in der Dienstleistungswissenschaft üblich ist (Alter, 2001). (Horkoff, 2019) zeigt, dass nicht-funktionale Anforderungen im Machine Learning (ML) neu betrachtet werden müssen, und (Habibullah & Horkoff, 2021) verbinden die Anforderungen sogar mit industriellen Herausforderungen. (Vogelsang & Borg, 2019) erheben Anforderungen aus der Perspektive von Data Scientists und stellen fest, dass sich verändernde Entwicklungsprozesse mit veränderten Anforderungen einhergehen.

Das vorliegenden Arbeitspaket 3.1 fokussiert sich daher insbesondere auf die Anforderungen, die ein FL-System zur Verbesserung der IT-Sicherheit im HRM aus Anwendersicht erfüllen muss und untersucht folgende **Forschungsfragen**:

> *F3.1.1: Welche Anforderungen der Stakeholdergruppe muss ein FL-System zur Erhöhung der IT-Sicherheit im HRM aus Sicht des **Service Designs** erfüllen?*

*F3.1.2: Welche Anforderungen der Stakeholdergruppe muss ein FL-System zur Erhöhung der IT-Sicherheit im HRM aus der Perspektive **der Nutzer** erfüllen?*

Um die **Forschungsfrage F3.1.1** zu beantworten, wurde zunächst eine Online-Umfrage durchgeführt und ausgewertet. Auf Basis der Erkenntnisse wurde anschließend ein digitaler Kreativ-Workshop durchgeführt, die Auswertung erfolgte nach der Grounded Theory. Als Ergebnis wurde der Anforderungskatalog „System Design“ erstellt.

Um die **Forschungsfrage F3.1.2** zu beantworten, wurden Daten in Unternehmen unterschiedlicher Größen und Sicherheitsstandards erhoben, als Methode wurden Leitfadeninterviews gewählt. Die Auswertung der Interviews erfolgte, wie bereits in Arbeitspaket 2.3, nach der Methode von Kuckartz. Als Ergebnis wurde der Anforderungskatalog „User Experience“ erstellt.

3.2 Methoden und Ergebnisse

Um die Anforderungsanalyse der Anwender durchzuführen, wurden zwei Ebenen betrachtet: die übergeordnete Ebene des System Designs und die konkrete Ebene der User Experience (UX).

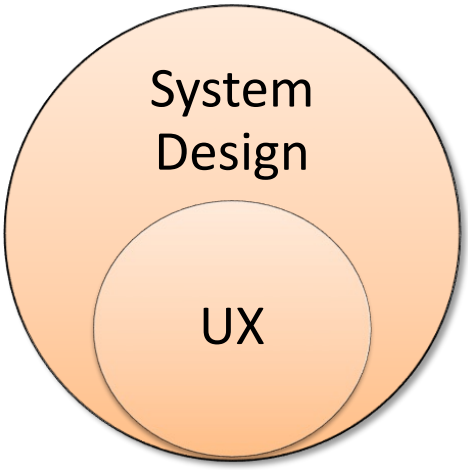


Abbildung 11: Zwei Ebenen der Anforderungsanalyse

Diese beiden Sichtweisen wurden mittels unterschiedlicher wissenschaftlicher Methoden untersucht und ausgewertet, (siehe Kapitel 3.2.1und 3.2.3).

Tabelle 5: Erhebungsmethoden Anwendungsanalyse

Sichtweise/Ebene	Teilnehmergruppe	Methode Erhebung	Methode Auswertung
System Design	HRM, IT-Sicherheit, Datenschutz, IT-Fachpersonal	Quantitativ (Online-Umfrage);	Mixed Methodes

		Kreativ-Workshop (Miro-Board)	
User Experience (UX)	HRM	Qualitativ (Experteninterviews)	Codierung nach Kuckartz

3.2.1 System Design: Kreativ-Workshop & Auswertung

In einem ersten Schritt wurde ein Fragebogen mit 38 geschlossenen Fragen und 16 Filterfragen erstellt, der sich an den Fachkenntnissen der Teilnehmer orientierte. Die abgefragten Themenbereiche umfassten sowohl personelle als auch technische und organisatorische Aspekte, die sich aufgrund einer Literaturanalyse als wesentlich für die Gestaltung eines FL-Systems herausgestellt hatten. Die Befragung wurde von Juli bis August 2022 online durchgeführt. Das Ergebnis waren n=110 vollständige Datensätze und n=31 unvollständige Datensätze, welche in die nachfolgende Auswertung einbezogen wurden.

Die Ergebnisse, die einen ersten Überblick über die Anforderungen im Umfeld der Systemgestaltung lieferten, dienten anschließend als Grundlage für den Workshop, der als Vertiefung und Erweiterung der neu identifizierten Anforderungsmerkmale zu sehen ist.

Der Kreativ-Workshop wurde im September 2022 als dreistündiger digitaler Workshop mit sechs Stakeholdern (Personalverantwortliche, IT-Sicherheitsexperten, technische Mitarbeiter und Datenschutzbeauftragte) durchgeführt. Während des Workshops wurden die Anforderungen der Teilnehmer mit Hilfe eines Dashboards und Post-it-Notizen erfasst und diskutiert (MIRO-Board, Abbildung 12).

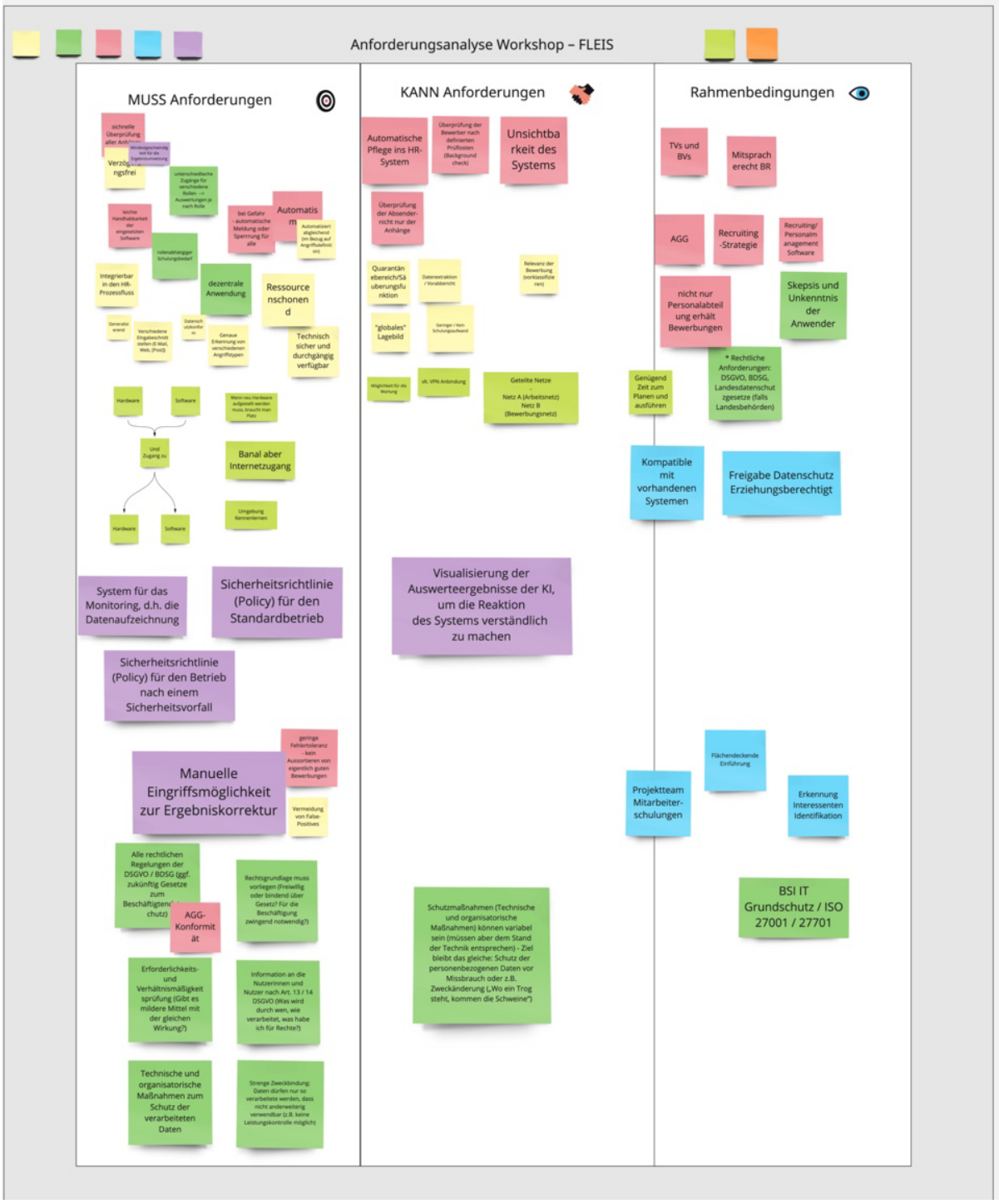


Abbildung 12: Ausschnitt aus dem Kreativ-Workshop (Miro-Board)

In Verbindung mit dem System Design wurden innerhalb des Workshops folgende Anforderungen besonders hervorgehoben: Unsichtbarkeit des Systems für die Abteilung HRM, effiziente Einbindung in die Aufgabengebiete und somit Erzielung der Zweckbindung, Visualisierung des Systems für die technischen Bereiche, unter Beachtung der User Experience. Für die

Teilnehmer waren darüber hinaus die Aspekte Geschwindigkeit, verzögerungsfreie Abläufe und Verfügbarkeit, geringe Fehlertoleranz, ressourcenschonende Verwendung der eingesetzten Güter, sowie die allgemeine Zeitersparnis von hoher Relevanz.

Die anschließende Datenanalyse erfolgte nach der Grounded Theory Methodik (Glaser & Strauss, 2017). Die 40 Post-it-Notizen wurden dazu als offene Codes adaptiert, und im nächsten Schritt mit den vorherigen neun Anforderungen aus der Umfrage zu axialen Codes verknüpft. Die Axialen Codes wurde untereinander verknüpft, sodass am Ende eine Übersicht der Zusammenhänge und Relevanzen zwischen den Anforderungen entstand (Selektive Codes, Abbildung 13).

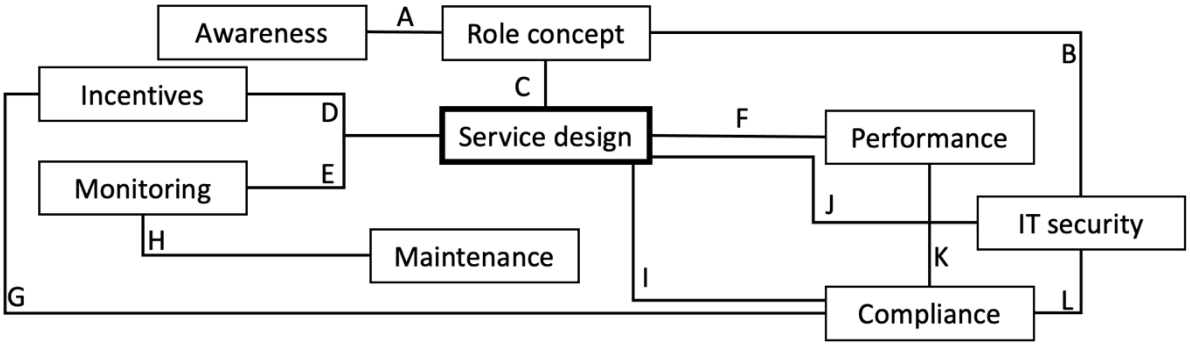


Abbildung 13: Selektive Codes

(A) Die Sensibilisierung in Kombination mit dem Rollenkonzept wurde vor allem von den nicht-technischen Mitarbeitern gefordert, die sich die Integration eines FL-Systems nur schwer vorstellen konnten. Daraus leiteten die Teilnehmer die Anforderungen an die Schulung, die Beseitigung von Skepsis und Unwissenheit, die Erhöhung des Verständnisses und die Einbindung der Explainable AI-Methode ab.

(B, C) Die Teilnehmer diskutierten das Rollenkonzept in Kombination mit dem Design und der Verteilung der Zugriffsrechte durch die IT-Sicherheit.

(D) Der Zusammenhang zwischen den offenen Codes und dem Element der Anreizsysteme ist nicht auf den ersten Blick erkennbar. Der Wunsch, einen zusätzlichen Mehrwert zu generieren und die Frage der Teilnehmer nach einem Grund für die Einführung zeigt jedoch, dass Anreizsysteme im Rahmen des Service Designs die Einbindung der Unternehmen erhöhen könnten.

(E, H) Die Elemente Überwachung und Wartung stehen in einem gekoppelten Verhältnis. Die Wartung reagiert auf die im Monitoring identifizierten Schwachstellen, wobei die Begriffe in den offenen Codes einzeln benannt und erst in der zweiten Runde des Workshops von den Teilnehmern zusammengeführt wurden.

(F) Für die Teilnehmer waren die Aspekte Schnelligkeit, verzögerungsfreie Abläufe, Verfügbarkeit, geringe Fehlertoleranz, ressourcenschonender Einsatz der eingesetzten Güter und allgemeine Zeitersparnis häufig angesprochene Themen im Workshop, die mit den Gestaltungselementen Service Design und Performance in Einklang gebracht werden sollen.

(J) Aber auch die Integration von Schutzmaßnahmen, Sicherheitsrichtlinien, manuelle Eingriffsmöglichkeiten in die Sicherheit, die allgemeine Verfügbarkeit und der Schutz durch die Vergabe von Zugriffsrechten an die Nutzer wurden als relevant genannt und decken das Gestaltungselement der IT-Sicherheit ab.

(G, I, K, L) Die Einhaltung bestehender Vorschriften war nicht nur für den Datenschutzbeauftragten, sondern auch für die Personalverantwortlichen und den IT-Sicherheitsbeauftragten von besonderer Bedeutung, da sie die Möglichkeiten der Systemeinführung und -gestaltung beeinflusst.

Die Ergebnisse der Umfrage und des Kreativ-Workshops wurden in einer Kohortenanalyse erneut ausgewertet und im Anforderungskatalog „System Design“ festgehalten.

3.2.2 Ergebnis System Design: Anforderungskatalog

Folgender Anforderungskatalog System Design wurde aus dem Kreativ-Workshop erstellt (Tabelle 6):

Tabelle 6: Anforderungskatalog System Design

Anforderung	Beschreibung der Anforderung	Priorität	Bemerkung	Ausprägung Maßnahme
Awareness	Skepsis und Unwissenheit beseitigen. Die Teilnehmer mit Informationen versorgen, sodass eine Mitbestimmung/-gestaltung ihrerseits möglich ist.	hoch	Erfüllung durch AP 8 (Leitung UniBw)	Mensch
Richtlinien	Aufstellen von Richtlinien für die Teilnehmenden aber auch den Service Provider. Abstimmung in Zusammenarbeit mit den Teilnehmer. Relevant sind Ausgestaltung der Mitarbeit und Kommunikation, Auflagen für den Eintritt ins System, Bereitstellungen und zu gewährende Zugriffsrechte etc.	mittel	Sollte nach Fertigstellung des Prototypen angepasst werden. In Zusammenarbeit (Interview/Workshop) mit möglichen Teilnehmern.	Organisatorisch
Datensicherheit	Gewährleistung der Datenhoheit und Absicherung der Kommunikationsstränge gegen Sabotage und Spionage	hoch	Technische Herausforderung	Technisch
Gesetzliche Auflagen	Einhaltung von IT-Sicherheitsnormen (BSI/ISO27001), Vordnungen zum Datenschutz (DSGVO) und spezifisch fürs HRM die AGG, BVs und TVs	hoch	Sind bei der Erstellung des Prototypen zu beachten	Organisatorisch
Anreizsysteme	Darstellung der Anreize (Mehrwert des Systems darstellen) und Generierung von "Belohungssystemen" für die Mitarbeit. Dadurch Mehrwert erhöhen aber auch die Fairness steigern.	niedrig	Technische Implementierung möglich. Prüfung innerhalb der Erstellung des Prototypen	Technisch/ Organisatorisch
Rollenkonzepte	Klare Darlegung der benötigten Rollen im Unternehmen. Beschreibung der Tatigkeiten und des benötigten Fachwissens. Festlegen von Schulungskonzepten für die Rollen und klare Eingrenzung der Zugriffsrechte. Nicht nur das HRM sollte mit dem System verknüpft sein, sondern auch das Personal aus den Fachabteilungen, welches für die Prüfung von Bewerbungen zuständig ist.	hoch	System sollte in der IT-Fachabteilung aufgehangen sein in Bezug auf Implementierung und Wartung. Es sollte zu keinem großen Stellen Auf-/Abbau kommen. Outsourcing ist ebenfalls unerwünscht. Verteilung auf bestehende Rollen. Höhere Belastung wird allgemein durch die technische Abteilung mitgetragen.	Mensch/ Organisatorisch
Design	Handhabung, Bedienbarkeit sollten einfach, einprägsam und intuitiv sein. Die Nutzer wünschen möglichst in ihren Hauptprozessen nicht gestört zu werden (Unsichtbarkeit des Systems). Eine vollständige Automatisierung ist ebenfalls wünschenswert unter gleichzeitig hoher Zuverlässigkeit der Ergebnisse. Mit Blick auf die Systemkommunikation können sich die Nutzer vorstellen per Mail oder ein zusätzliches System, sowie einen Chatbot mit dem System zu kommunizieren.	mittel	Aufgrund von Sicherheitskonzepten, der KI-Ethik und staatlichen Richtlinien, scheint eine vollständige Automatisierung nicht umsetzbar.	Technisch
Wartung und Installation	Einfach und intuitiv, keine langen Prozesse, keinen hohen zusätzlichen Kosten für Beschaffung von Material oder Fachpersonal.	niedrig	Verbindung zu Rollenkonzepte	Technisch/ Organisatorisch
Interoperabilität	System sollte Schnittstellen zu anderen IT-Sicherheitssoftwares ermöglichen, sowie dem File- und Mailserver und der im HRM verwenden Software (SAP; ATS)	mittel	Prüfung innerhalb der Entwicklung des Prototypen	Technisch
Performance	geringer Zeitaufwand (Wartezeit/Verzögerungsfreie Kommunikation) für die Berechnungen. Geringer Ressourcenverbrauch (Nachhaltigkeit).	hoch	Ausschöpfen der Möglichkeiten während der Erstellung des Prototypen	Technisch
Monitoring	Die Überwachung der Systeme durch KPIs/Messgrößen und die Überwachung der verwendeten Trainingsdaten durch Fachpersonal sollte gegeben sein. Transparenz des Systems für die Kontrollinstanz. Quarantänebereich für aussortierte Bewerbungen.	hoch	An dieser Stelle scheint die Verwendung von manuellen Steuerungssystemen durch die Nutzer akzeptiert.	Technisch/ Organisatorisch
Sicheres Lernen	Lernumgebung sollte aktuelle Sicherheitsstandards erfüllen. Datensicherheit (Datensouveränität) steht hier im Fokus.	hoch	Verbindung zu Datensicherheit	Technisch
Datenbasis	Schaffen einer gemeinsamen Datenbasis bei allen Teilnehmern oder Generierung einer Möglichkeit für das Lernen mit heterogenen Datensätzen.	mittel	Prüfung innerhalb der Entwicklung des Prototypen	Technisch
Daten	Es sollte eine Überprüfung vor allem von Links, PDFs und Office Dateien möglich sein, aber auch die direkte Integration von Daten aus dem ATS ist wünschenswert. Eine Überprüfung der Mails, wird aufgrund der bereits vorhandenen Systeme eher nicht gewünscht.	mittel	Prüfung innerhalb der Entwicklung des Prototypen	Technisch
zusätzliche Erwartungen an ein System zum Schutz der IT-Sicherheit im HRM	Beseitigung der Schadquelle, Information über den Angriff, Verringerung der erfolgreichen Angriffe	mittel	Prüfung innerhalb der Entwicklung des Prototypen	Technisch

3.2.3 UX: Qualitative Erhebung & Auswertung

Um die Wünsche der Anwender an eine Software zur Erhöhung der IT-Sicherheit im Personalwesen zu untersuchen, wurde eine Masterarbeit vergeben. Diese Masterarbeit wurde von

April 2022 bis August 2022 von Fr. Lena Techam (Studiengang Management & Medien der Universität der Bundeswehr München) durchgeführt (Techam, 2022).

Die Masterandin führte mit zehn Unternehmen explorative Experteninterviews ((Lamnek & Krell, 2016), S. 687-691) in der Ausprägung von Leitfadeninterviews durch und transkripierte sie anschließend wörtlich im Software-Werkzeug MaxQDA. Die Kodierung und Auswertung folgte der inhaltlich strukturierenden Inhaltsanalyse nach Kuckartz (Kuckartz & Rädiker, 2022) aus.

Die folgende Tabelle 7 zeigt die Übersicht der interviewten Unternehmen.

Tabelle 7: Befragte Unternehmen der qualitativen Erhebung im Arbeitspaket 3.1

ID	Art des Unternehmens / Branche	Anzahl Mitarbeitende im Unternehmen (ca.)	Bewerbungen pro Jahr (ca.)
ID_02	Energie	10.000	12.000
ID_03	Energie	2.500	2.000-2.500
ID_04	Energie	450	3.000-4.200
ID_05	Energie	150	480-600
ID_06	Halbleiter	51.000	250.000
ID_07	Lebensmittel	3.000	1.200
ID_08	Nahrungs- & Genussmittel	1.000	1.200
ID_09	Rüstung	6	60-80
ID_10	Mobilität	30	240-360
ID_11	Energie	50	600

Da für die Erhebung der Nutzerforderungen im Forschungsprojekt FLEIS jedoch nur die Fragen der Kategorie „Nutzeranforderungen und -Anregungen“ aus dem Leitfaden relevant waren, wurden diese transkribierten Teile der Interviews ID_02 – ID_11 (Interview ID_01 wurde als Pre-Test verwendet und floss nicht in die Auswertung ein) in eine neue Datei exportiert und im Oktober 2022 von Steffi Rudel neu codiert.

Die folgende Tabelle 8 zeigt die verwendeten Fragen des Leitfadens sowie die daraus deduktiv (a priori) gebildeten Kategorien der qualitativen Inhaltsanalyse.

Tabelle 8: Leitfaden der Interviews „Nutzeranforderungen“ sowie gebildete Kategorien

Frage	Inhalt	Codierung
1	Wissen Sie, welche Sicherheitssoftware ihr Unternehmen derzeit benutzt?	Verbesserungsvorschlag
2	Wie zufrieden sind Sie damit auf einer Skala von 1-6?	Verbesserungsvorschlag

3	Welche Vor- und Nachteile sehen Sie in der Benutzung Ihres firmeninternen Programms?	Verbesserungsvorschlag
4	Wie viel Kontrolle (Entscheidungsspielraum) möchten Sie im regulären (täglichen) Umgang mit/über einer IT-Sicherheitssoftware haben?	Handlungsspielraum Anwender
5	Was wäre Ihnen bei der Nutzung einer Sicherheitssoftware am wichtigsten? ein ästhetisch ansprechendes Design ein Erlebnis bei der Nutzung der Anwendung zu haben so wenig wie möglich bei meiner Arbeit gestört zu werden	Handlungsspielraum Anwender
6	Wie involviert möchten Sie mit IT-Sicherheits-Software sein? Welcher Aussage stimmen Sie am ehesten zu: Ich möchte, dass ich selbst entscheiden kann, was sicher ist und was nicht. Ich möchte eine Unterstützung durch eine Software haben. Ich möchte, dass mir die Software so viel wie möglich abnimmt und ich mich nicht darum kümmern muss.	Handlungsspielraum Anwender
7	Falls Sie Unterstützung möchten, wie würden Sie sich das vorstellen? Anschlussfrage: Wie sehr darf eine Software Ihrer Meinung nach eingreifen?	Handlungsspielraum Anwender
8	Möchten Sie aktiv mit einer Sicherheitssoftware kommunizieren? (kommunizieren bspw. mit Chat-Bot, Mitteilungen bekommen oder kein aktives Zutun)	Handlungsspielraum Anwender
9	Bitte bewerten Sie die folgenden Maßnahmen: 24h Notrufhotline Persönlicher, permanenter Ansprechpartner im Unternehmen bei Problemen Ausführliche Selbstanleitung/ Guidelines mit Schritt-für-Schritt-Anleitung Frage-Antwort-Systeme *(ähnlich FAQs)* Erinnerungsdienste Benutzerfreundliche Warnplatzierungen für Phishing-Mails oder Malware Automatisierter Link-Check Forum, um über Updates und User Experience zu erfahren und selbst beizutragen Kontaktformular Automatisierte Chat-Bot-Funktionen (programmierte Chat-Konversation) Schulungen mit Gamification-Ansatz („spielerisches Lernen“ mit Gewinnanreizen oder Scores)	Funktionen (mit Subkategorien)
10	Welche davon wären Ihrer Ansicht nach essenziell oder besonders wichtig?	Funktionen (mit Subkategorien)
11	Sie sagten vorhin, Sie würden sich (nicht/teils/....) sicher im Umgang mit der IT-Sicherheit fühlen. Wie könnte dies verbessert werden? Was würde Ihnen speziell dabei helfen?	Verbesserungsvorschlag

Die folgende Tabelle 9 listet die Codes der Haupt- und Subkategorien mit den jeweiligen Erläuterungen nochmals zusammenfassend auf.

Tabelle 9: Kategoriensystem und zugehörige Codes (AP 3.1)

Code		Erläuterung
Hauptkategorie	**Subkategorie**	
Verbesserungs-vorschlag		Welches Verbesserungspotential wird an bereits vorhandenen Systemen gesehen? Was wurde sonst noch genannt?
Handlungsspiel-raum Anwender		Wie stark möchte der Anwender in die IT-Sicherheitssoftware eingreifen können/müssen?
Funktionen		Wie werden die folgenden Funktionen beurteilt
	24h-Hotline	Eine Hotline, die man 24 Stunden am Tag bei Problemen anrufen kann
	Persönlicher AP	Einen persönlichen, permanenten Ansprechpartner im Unternehmen bei Problemen haben
	Selbstanleitung	Anleitungen zur Selbsthilfe
	Frage-Antwort-System	System, in dem die häufigsten Fragen beantwortet sind (ähnlich FAQ's auf Webseiten)
	Erinnerungs-dienste	Automatisierte Erinnerung z.B. für Passwort-Änderung oder Updates
	Warnplatzierung	Wo/wie sollten Warnungen bei potentiellen Phishing-Mails platziert werden?
	Link-Check	Sollten Links in Mails automatisiert gecheckt und entsprechend markiert werden?
	Forum	Nutzung zur Verbesserung der IT-Sicherheitssoftware
	Kontaktformu-lar	Bei Problemen oder Fragen per Kontaktformular an die IT schreiben können
	Chat-Bot	Bei Fragen / Problemen über einen Chatbot kommunizieren können
	Schulung Gami-fikation	Wie könnten Schulungen interessant ausgestaltet werden?
Gewichtung Funktionen		Welche der Funktionen wird mit welcher Wichtigkeit bewertet?

Anschließend wurden diese Codes ausgewertet. Die Überführung in die Priorisierung der Anforderungen aus den zehn Interviews wurde wie folgt vorgenommen (Tabelle 10):

Tabelle 10: Priorisierung Anforderungen UX aus qualitativer Erhebung

Priorisierung	Anzahl Nennungen
hoch	7 und mehr Nennungen
mittel	4 – 6 Nennungen

niedrig	0 – 3 Nennungen

Darüber hinaus wurden die Anforderungen in die Kategorien technische, organisatorische und menschliche Maßnahme eingeteilt.

3.2.4 Ergebnis UX: Anforderungskatalog

Folgender Anforderungskatalog User Experience (UX) wurde aus den qualitativen Interviews erstellt:

Tabelle 11: Anforderungskatalog User Experience (UX)

Anforderung	Beschreibung der Anforderung	Priorität	Nennungen	Code	Ausprägung Maßnahme
Interaktion mit Sicherheitssoftware	Anwender in HRM wollen möglichst wenig mit Sicherheitssoftware interagieren müssen, sie soll möglichst viel Arbeit abnehmen. ODER Anwender in HRM wollen mittelviel mit Sicherheitssoftware interagieren oder selbst entscheiden können, wieviel sie interagieren.	hoch	7	Handlungsspielraum Anwender	Technisch
Möglichst kein Einfluss auf operative Arbeit	Anwender im HRM wollen durch Sicherheitssoftware möglichst wenig bei der Arbeit gestört werden.	hoch	10	Handlungsspielraum Anwender	Technisch
Sichtbarkeit der Überprüfung	Anwender im HRM möchten erkennen können, was geprüft / sicher ist und was nicht.	mittel	5	Verbesserungsvorschlag	Technisch
Funktion: (Notfall-) Ansprechpartner	Anwender im HRM wünschen sich eine 24h-Notrufhotline oder einen persönlichen Ansprechpartner	hoch	9	Funktionen: 24h-Hotline oder pers. AP	Organisatorisch
Funktion: Selbstanleitung	Anwender im HRM wünschen sich eine Anleitung zur Selbsthilfe	niedrig	3	Funktion: Selbstanleitung	Organisatorisch
Funktion: Frage-Antwort-System	Anwender im HRM wünschen sich ein System in dem die häufigsten Fragen beantwortet sind (ähnlich FAQ's auf Webseiten)	niedrig	2	Funktion: Frage-Antwort-System	Organisatorisch
Funktion: Erinnerungsdienste	Anwender im HRM möchten automatisch z.B. an Passwortänderungen oder Systemupdates erinnert werden	mittel	5	Funktionen: Erinnerungsdienste	Technisch
Funktion: Platzierung Warnhinweise	Anwender im HRM wünschen sich eine passende Platzierung für Warnhinweise vor potentiellen Phishing-Mails	hoch	8	Funktionen: Warnplatzierung	Technisch
Funktion: Link-Check	Anwender im HRM wünschen sich, dass Links in Mails automatisiert gecheckt und entsprechend markiert werden	mittel	5	Funktionen: Link-Check	Technisch
Funktion: Forum	Anwender im HRM wünschen sich ein Forum zur Verbesserung der IT-Sicherheitssoftware	niedrig	0	Funktion: Forum	Organisatorisch
Funktion: Kontaktforumlar	Anwender im HRM möchten bei Problemen oder Fragen per Kontaktformular an die IT schreiben können	niedrig	2	Funktion: Kontaktformular	Organisatorisch
Funktion: Chat-Bot	Anwender im HRM möchten bei Fragen oder Problemen über einen Chatbot kommunizieren können	niedrig	1	Funktion: Chat-Bot	Technisch
Funktion: Schulungen Gamifikation	Anwender im HRM wünschen sich interessant und motivierend ausgestaltete Schulungskonzepte	mittel	4	Funktionen: Schulung Gamifikation	Mensch

3.3 Zwischenfazit

Dieses Arbeitspaket 2.3 lieferte als Ergebnisse zwei Anforderungskataloge System Design und User Experience, welche die Forschungsfragen 2.3.1 und 2.3.2 beantworten konnten.

Mit diesen Ergebnissen wird ein Beitrag zum Wissen über Anforderungen und Service Design für ein FL-System im HRM. Dieses Wissen steht der wissenschaftlichen Gemeinschaft nun für die weitere Forschung zur Verfügung.

4 Arbeitspaket 8.2: Kompetenzaufbau Cybersicherheit in Personalabteilungen

Im Folgenden werden die Inhalte des Arbeitspaketes *8.2 Kompetenzaufbau Cybersicherheit in Personalabteilungen* beschrieben. Dieses Arbeitspaket 8.2 ist (wie in Abbildung 1 zu sehen) das dritte Arbeitspaket der UniBw M im Projekt.

Die folgende Abbildung 14 zeigt die geplanten Inhalte des Arbeitspaketes.

AP 8.2: Kompetenzaufbau Cybersecurity in Personalabteilungen	**6 PM (UniBw M)**
Zuständig	**Lead UniBw M, Mitarbeit alle**

Vorgehen	• Kenntnisstand in Personalabteilungen zu Cybersecurity erheben:
	  ○ Online-Umfrage konzipieren, testen, bewerben, durchführen, auswerten, dokumentieren
	  ○ Vertiefen durch Experteninterviews
	• Konzeptentwicklung für Kompetenzaufbau Cybersecurity in Personalabteilungen
	• Validierung des Konzeptes

Methoden	• Desk Research • Experteninterviews • Online-Umfrage • Workshops

Ergebnisse	• Erhobener Kenntnisstand in Personalabteilungen zu Cybersecurity aus
	  ○ Durchgeführten und ausgewerteten Online-Umfrage („Monitor“)
	  ○ Durchgeführten, transkribierten und ausgewerteten Experteninterviews
	• Validiertes Konzept zum Kompetenzaufbau Cybersecurity in Personalabteilungen

Abbildung 14: Geplante Inhalte des Arbeitspaketes 8.2

4.1 Forschungsgegenstand und Forschungsfragen

Um Personalabteilungen einen *ganzheitlichen* Kompetenzaufbau bezüglich Cybersecurity zu ermöglichen, genügt es nicht, sich allein auf technische Maßnahmen zu verlassen. Vielmehr müssen die drei Faktoren *Mensch – Technik – Organisation* gleichermaßen im Blick behalten werden. Die Mensch-Technik-Organisations-Analyse (Strohm, O. & Ulich, E., 1997) untermauert dies mit der Annahme, dass eine optimale Anpassung und Abstimmung der drei Faktoren die Arbeitsqualität und die Effizienz im Unternehmen steigern kann.

Im Rahmen dieses Arbeitspaketes wird der Fokus zur IT-Sicherheit auf den Faktor Mensch gelegt. Dafür wird in einem ersten Schritt der Kenntnisstand zur IT-Sicherheit im HRM erhoben. Im zweiten Schritt wurde ein Training zur gezielten Aus- und Weiterbildung entwickelt, um die Kompetenz zur Erkennung und zur Abwehr von Angriffen im HRM zu fördern und so die IT-Sicherheit des gesamten Unternehmens zu erhöhen. Dieses Training soll als Ergänzung der technologischen Lösung von den Projektpartner dienen.

Das Arbeitspaket 8.2 greift folgende, aufeinander aufbauende **Forschungsfragen** auf:

> *F8.2.1: Was ist der Kenntnisstand von Mitarbeitenden und Führungskräften im HRM in Bezug auf IT-Sicherheit?*
>
> *F8.2.2: Welches Trainingskonzept führt zum zielgruppenorientierten und wirksamen Kompetenzaufbau bezüglich IT-Sicherheit im HRM?*

4.2 Methoden und Ergebnisse

Um die **Forschungsfrage F8.2.1** zu beantworten, wurde eine Umfrage in deutschen Unternehmen konzipiert, durchgeführt und ausgewertet. Der Fragebogen dazu wurde basierend auf vorhergehenden Arbeiten entworfen und als quantitative Umfrage durchgeführt. Die Ergebnisse aus der Umfrage wurden anschließend ausgewertet und mit der Software Tableau grafisch aufbereitet.

Aufbauend auf den ausgewerteten Ergebnissen wurde ein Training konzeptioniert, durchgeführt und ausgewertet (**Forschungsfrage F8.2.2**). Das Training wurde nach einem iterativen Ansatz in Erweiterung des Wasserfallmodells entwickelt. Bei der Entwicklung des Trainings wurden wissenschaftliche Grundlagen zur Kompetenzentwicklung berücksichtigt. Im weiteren Verlauf wurde das Training drei weitere Male durchgeführt, dokumentiert und evaluiert.

4.2.1 Kenntnisstand IT-Sicherheit: Quantitative Erhebung & Auswertung

Um den Kenntnisstand zur IT-Sicherheit in deutschen Personalabteilungen zu erheben, wurde eine Masterarbeit vergeben. Diese Masterarbeit wurde in der Zeit von April bis August 2023 vom Masteranden Leon Schwarz (Masterstudium Management & Medien) durchgeführt (Schwarz, 2022). Der Fragebogen der Umfrage wurde basierend auf den Arbeiten von Adele Da Veiga (ISCA, (Da Veiga, 2018)) sowie Kathie Parsons (HAIS-Q, (Parsons et al., 2017)) erstellt, wobei ISCA zur Messung der IT-Sicherheitskultur und HAIS-Q zur Messung des IT-Sicherheitsbewusstseins herangezogen wurden.

Nach der Entwicklung des Fragebogens wurde zunächst mit n=12 Personen ein Pretest durchgeführt und der Fragebogen daraufhin nochmals leicht angepasst. Der vollständige Fragebogen umfasste 109 Items und ist im Anhang enthalten.

Die Befragung fand im Zeitraum 1. Juni – 31. Juli 2022 statt. Verteilt wurde die Umfrage über die Online-Plattform www.soscisurvey.de, sowie über drei Verbände für KMU in Deutschland und LinkedIn. In dieser Zeit wurde der Fragebogen 109-mal ausgefüllt, wovon

nach Bereinigung durch den Masteranden n=98 gültige Rückläufer übrigblieben (=Rohdatensatz).

Dieser Rohdatensatz wurde vom Masteranden Ende August 2022 an FLEIS übergeben und anschließend im November 2022 von Steffi Rudel des Projektes FLEIS neu ausgewertet. Dazu wurde der Rohdatensatz zunächst aussortiert, um den wissenschaftlichen Anforderungen des Projektes FLEIS zu genügen. Folgende Datensätze wurden entfernt:

- Alle Datensätze, welche bei der Frage FI01 nicht die Antwort 1 oder 2 hatten (ID 54, 56, 65, 129, 130, 166, 170, 178, 187, 193, 197, 208, 226, 258), da die Antworten 5 und 6 nicht eineindeutig sicherstellen, dass diese Person in der Personalabteilung tätig ist.
- Alle Datensätze, welche die Kontrollfrage falsch beantwortet hatten (ID 89, 175, 202, 249, 282).

Übrig blieben **n=79 verwertbare Datensätze**. Aus diesen wurden folgende Fragen entfernt, da sie nicht relevant oder nicht eindeutig gestellt waren: SC01, SD01, SD17, SD10, SE01, SE05, HG01-HG13, H201-H203, SR01_03, SR01_05, NI02_01-10, NI02_12-13, VI01_02-06, VM01, VP01_01-11, WI01, PM01, EN01_03, EN01_09, IN01, SM01, MG01, UI01_01, UI01_03, IR01, FR01-10, SB01-06, SB07-08

Folgende Fragen verblieben und wurden zur Auswertung herangezogen (Tabelle 12):

Tabelle 12: Für FLEIS identifizierte, relevante Fragen

Code		Frage	Anmerkung
SE03		Bitte geben Sie an, zu wie viel Prozent Sie sich sicher sind, den Unterschied zwischen IT-Sicherheit und Datenschutz erläutern zu können.	Zahlenskala zwischen 0% und 100%
FI01		Bitte kreuzen Sie an, welche Position Sie im Unternehmen haben.	1 = Mitarbeitende Person im HRM; 2 = Führungskraft im HRM
H204		Wie möchten Sie Informationen zur IT-Sicherheit erhalten?	Mehrfachnennung möglich.
	H204_01	Internet	0=nein; 1=ja
	H204_02	Poster	0=nein; 1=ja
	H204_03	E-Mail	0=nein; 1=ja
	H204_04	Diskussionsgruppen	0=nein; 1=ja
	H204_05	Präsentationen	0=nein; 1=ja
	H204_06	Praktisches Training	0=nein; 1=ja
	H204_07	Über Messengerdienste	0=nein; 1=ja
	H204_08	Training über das Internet	0=nein; 1=ja
	H204_09	Video-Training	0=nein; 1=ja
	H204_10	Handbücher	0=nein; 1=ja

SR01		Bitte beurteilen Sie folgende Aussagen zu den IT-Sicherheitsrichtlinien in Ihrem Unternehmen.	Skala 1 (=stimme gar nicht zu) bis 5 (=stimme voll zu); 0=kann ich nicht beurteilen
	SR01_01	Der Inhalt der IT-Sicherheitsrichtlinien ist leicht verständlich.	
	SR01_02	Ich glaube, dass die IT-Sicherheitsrichtlinien umsetzbar sind.	
	SR01_04	Der Inhalt der IT-Sicherheitsrichtlinie wurde mir wirksam vermittelt.	
NI02		Bitte beurteilen Sie folgende Aussagen zur Notwendigkeit von IT-Sicherheit.	Skala 1 (=stimme gar nicht zu) bis 5 (=stimme voll zu); 0=kann ich nicht beurteilen
	NI02_11	Ich bin bereit, meine Arbeitspraktiken zu ändern, um die Sicherheit von Informationsgütern (z.B. Computersysteme und Informationen in Papier- oder elektronischer Form) zu gewährleisten.	
VI01		Bitte beurteilen Sie folgende Aussagen zur Verantwortlichkeit für IT-Sicherheit.	Skala 1 (=stimme gar nicht zu) bis 5 (=stimme voll zu); 0=kann ich nicht beurteilen
	VI01_01	Die IT-Sicherheit muss durch ein formelles System geregelt werden (Z.B. Aufgaben und Zuständigkeiten der Mitarbeiter im Bereich der IT-Sicherheit, Sensibilisierungskampagnen).	
	VI01_07	Ich bin der Meinung, dass zusätzliche Schulungen für den Einsatz von IT-Sicherheitsinstrumenten erforderlich sind, um Informationen zu schützen.	
VP01		Bitte beurteilen Sie folgende Aussagen zum Thema Verpflichtung zur IT-Sicherheit.	Skala 1 (=stimme gar nicht zu) bis 5 (=stimme voll zu); 0=kann ich nicht beurteilen
	VP01_12	Mein Unternehmen hat klare Richtlinien zum Schutz sensibler/vertraulicher Daten von Mitarbeitenden.	
EN01		Bitte beurteilen Sie folgende Aussagen zum Umgang mit Weblinks in E-Mails.	Skala 1 (=stimme gar nicht zu) bis 5 (=stimme voll zu); 0=kann ich nicht beurteilen
	EN01_10	Wenn eine E-Mail von einem unbekannten Absender interessant aussieht, klicke ich auf einen Link in der E-Mail.	
UI01		Bitte beurteilen Sie folgende Aussagen zum Umgang mit sicherheitsempfindlichen Datenträgern.	Skala 1 (=stimme gar nicht zu) bis 5 (=stimme voll zu); 0=kann ich nicht beurteilen
	UI01	Ich würde einen USB-Stick, den ich an einem öffentlichen Ort gefunden habe, an meinen Arbeitscomputer anschließen.	

Anschließend wurden bei einigen verbleibenden Fragen die Ziffern überführt, um eine bessere Logik und Auswertbarkeit zu gewährleisten:

Tabelle 13: Überführung der Werte der quantitativen Umfrage zur besseren Logik und Auswertbarkeit

Frage	Wert_alt	Wert_neu	Entspricht
SE03	1	0	0%
	2	10	10%
	3	20	20%
	4	30	30%
	5	40	40%
	6	50	50%
	7	60	60%
	8	70	70%
	9	80	80%
	10	90	90%
	11	100	100%
FI01	1	MitarbeiterIn	Mitarbeitende Person in der Personalabteilung
	2	Führungskraft	Führungskraft in der Personalabteilung
H204_01-10	1	0	nicht gewählt
	2	1	gewählt
SR01, VI01, VP01, EN01, UI01	-1	0	Kann ich nicht beurteilen

Zuletzt wurden die Spalten des Datensatzes in die chronologische Reihenfolge der Fragen gebracht, in das Datenanalyse-Tool Tableau eingelesen und ausgewertet. Einige ausgewählte Ergebnisse werden im Folgenden vorgestellt, alle Grafiken sind im Anhang enthalten.

4.2.2 Kenntnisstand IT-Sicherheit: Ausgewählte Ergebnisse

Die erste vorgestellte Frage (FL01) zielte darauf ab, herauszufinden, in welcher Position die Teilnehmer im HRM tätig sind. Es lässt sich erkennen, dass sich knapp 30% als Führungskraft einordneten, wohingegen knapp 70% als MitarbeiterInnen tätig sind (Abbildung 15).

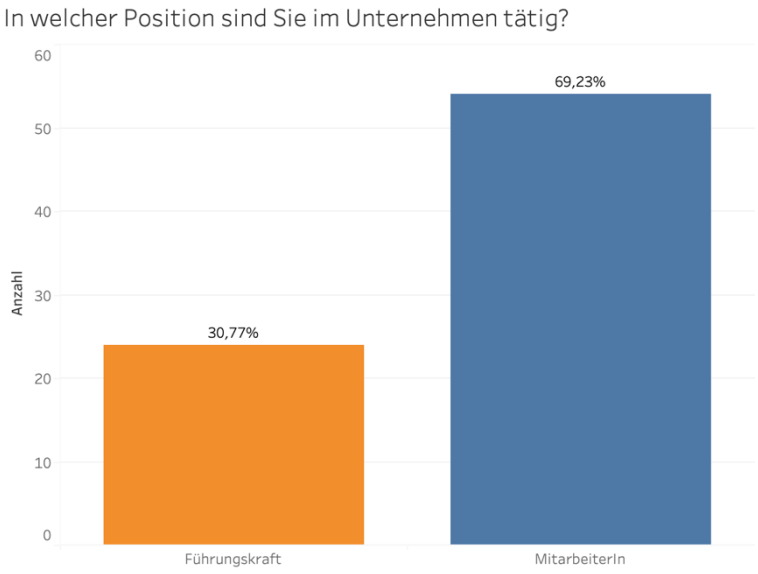


Abbildung 15: Verteilung Führungskräfte – Mitarbeitende

Einen guten Einblick in den Kenntnisstand der Befragten gibt die Frage SE03. Hier wurde um eine eigene Einschätzung gebeten, zu wieviel % sich die Befragten sicher sind, den Unterschied zwischen Datenschutz und IT-Sicherheit zu kennen (Abbildung 16). Gerade bei den Mitarbeitenden ist eine deutliche Ausprägung (22 Antworten) bei den 0% zu sehen – hier gibt es also noch einiges an Potential zum Kompetenzaufbau IT-Sicherheit.

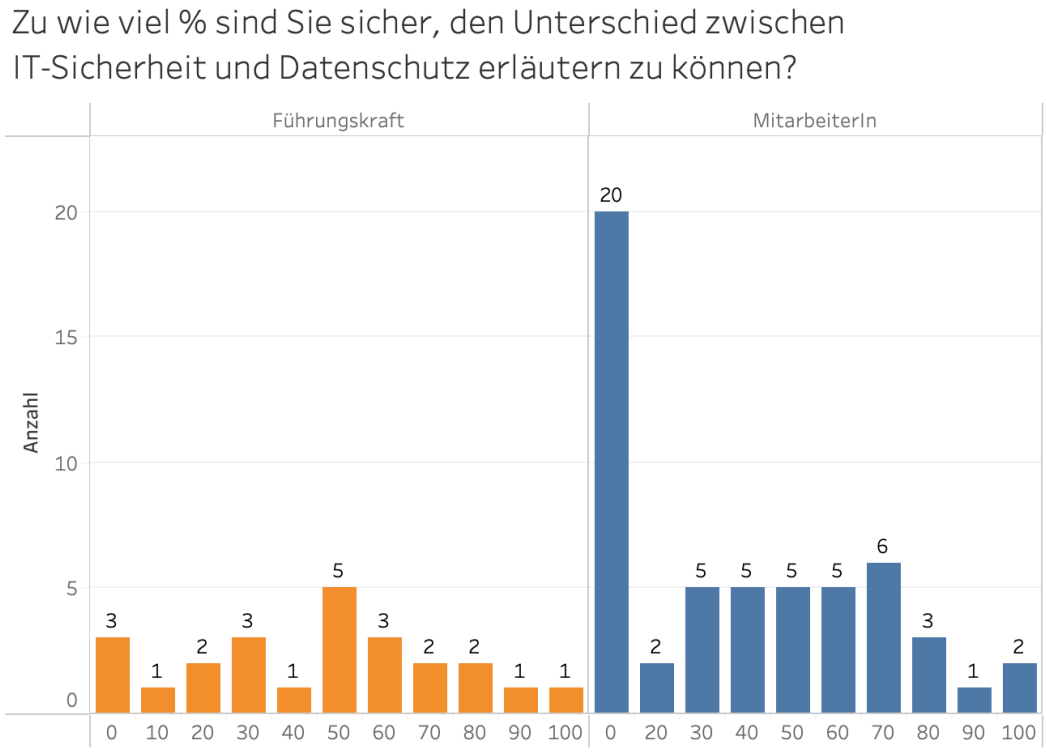


Abbildung 16: Sicherheit in der Unterscheidung IT-Sicherheit - Datenschutz

Die folgenden Fragen sollten anhand einer Likert-Skala von 0-5 beantwortet werden (Abbildung 17).

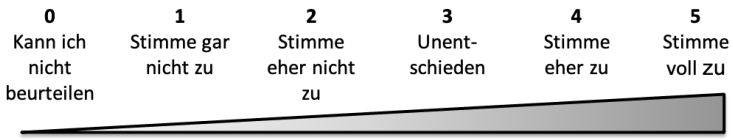


Abbildung 17: Likert-Skala

Einig sind sich die meisten Befragten, dass die Verantwortlichkeit für IT-Sicherheit klar geregelt sein sollte (VL01_01). So stimmten mehr als 60% der Führungskräfte und annähernd 50% der Mitarbeitenden der Aussage, dass die IT-Sicherheit durch ein formelles System geregelt sein muss, voll und ganz zu (Abbildung 18).

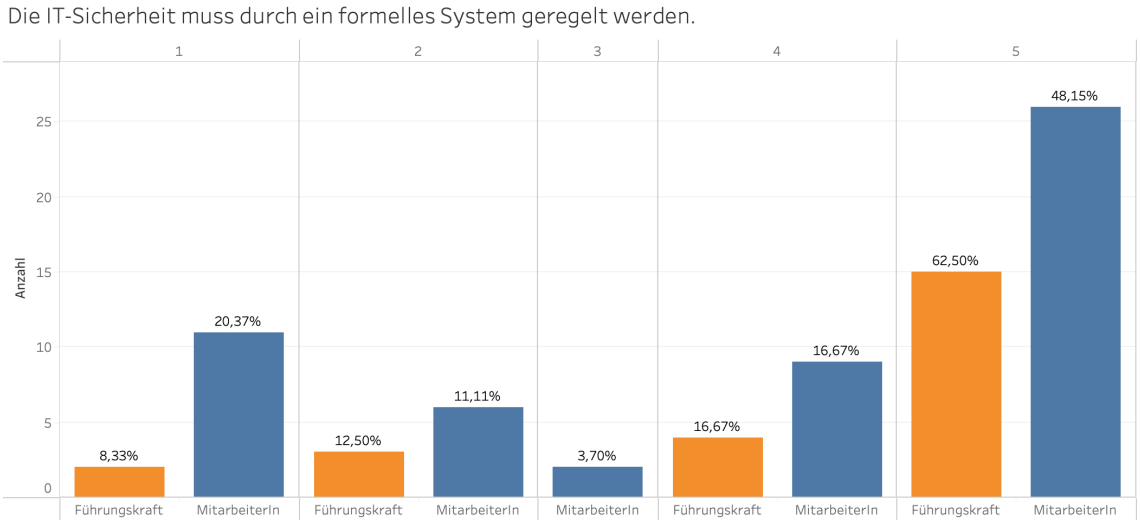


Abbildung 18: Regelung der IT-Sicherheit durch ein formelles System

Interessante Ergebnisse lieferten die Fragen zu den IT-Sicherheitsrichtlinien, also zu den formellen Vorgaben zur IT-Sicherheit, die im Unternehmen existieren (SR01_01). Es wurde hinterfragt, ob die IT-Sicherheitsrichtlinie des Unternehmens verständlich wären (Abbildung 19). Es lässt sich ablesen, dass sowohl bei den Führungskräften als auch bei den Mitarbeitern mehr als 37% dies nicht beurteilen können – entweder weil Sie die IT-Sicherheitsrichtlinie nicht kennen oder keine existiert.

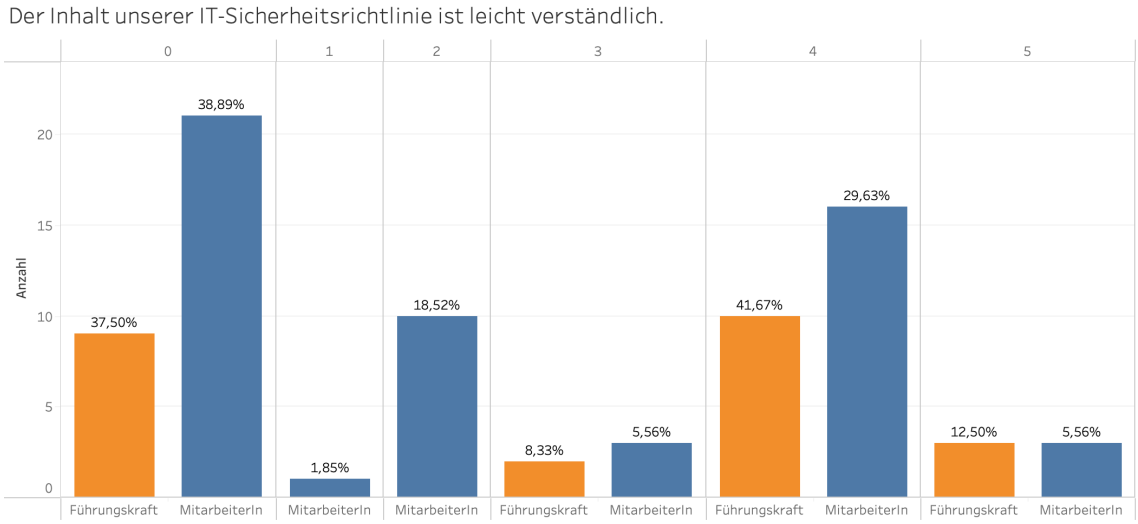


Abbildung 19: Frage nach der Verständlichkeit der IT-Sicherheitsrichtlinie im Unternehmen

Etwas besser sieht es bei der Frage zum Schutz sensibler/vertraulicher Daten von Mitarbeitenden aus (VP01_12). Die Antworten zeigen, dass mehr als 56% der Mitarbeitenden und mehr als 75% der Führungskräfte eher oder voll und ganz der Meinung sind, dass das eigene Unternehmen diese Daten ihrer Mitarbeitenden anhand klarer Richtlinien schützt (Abbildung 20).

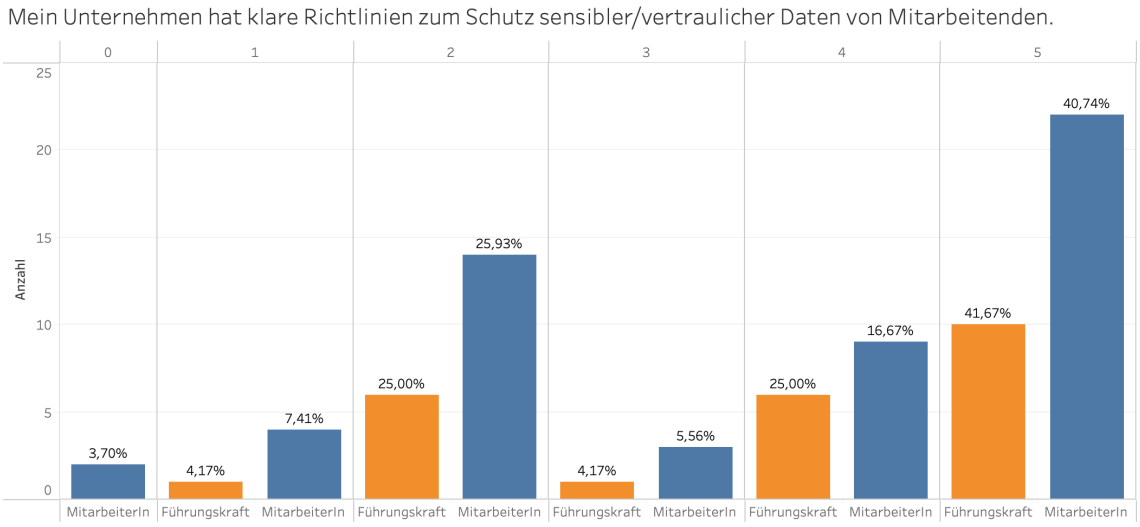


Abbildung 20: Frage nach klaren Richtlinien zum Schutz sensibler/vertraulicher Daten von Mitarbeitenden

Im nächsten Punkt wurde ein grundlegender Aspekt der IT-Sicherheit hinterfragt (UI01) – denn einen USB-Stick mit Malware „absichtlich zu verlieren“ ist eine gängige Methode von Angreifern (Tischer et al., 2016). Wird der betreffende Stick an einen PC angeschlossen, um festzustellen, was auf dem Stick gespeichert ist (um ihn mutmaßlich dem rechtmäßigen Besitzer zurückgeben zu können), installiert sich unbemerkt im Hintergrund eine Schadsoftware

auf dem System. In Abbildung 21 ist zu erkennen, dass immerhin fast 30% der Führungskräfte und fast 35% der MitarbeiterInnen den Stick eher oder bestimmt anschließen würden – dies birgt ein großes Gefahrenpotential für die IT-Sicherheit, ganz besonders im HRM.

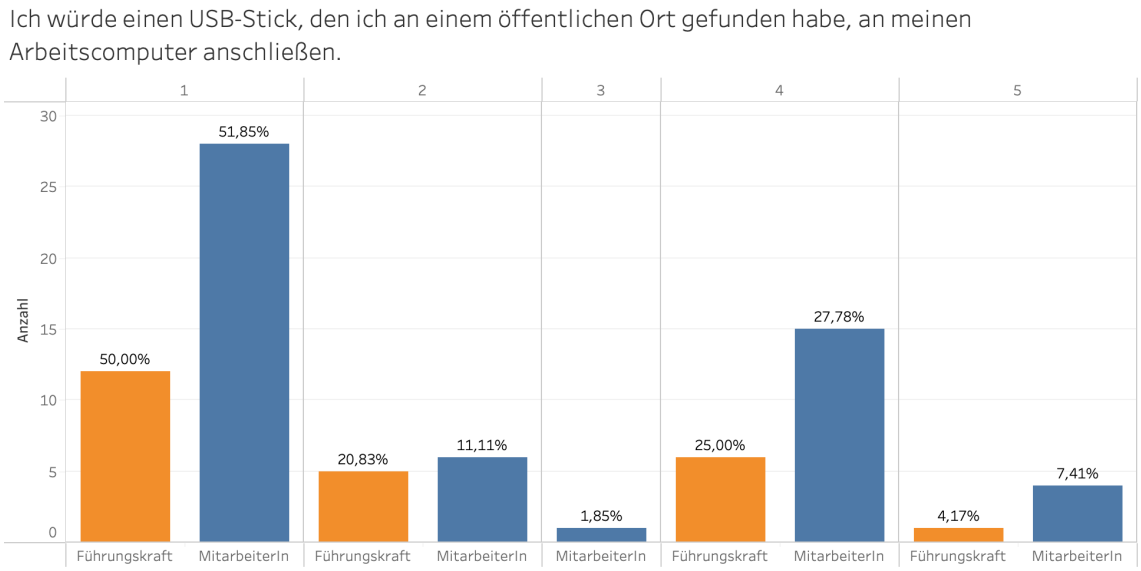


Abbildung 21: Unbekannten USB-Stick an PC anschließen

Nicht viel besser sieht es mit dem Klick-Verhalten auf Links in E-Mails unbekannter Absender aus (EN01_10) – ein Umstand, mit dem das Recruiting (als Teilbereich des HRM) beinahe täglich konfrontiert ist. Hier geben über 48% der Mitarbeitenden und mehr als 40% der Führungskräfte an, solche Links eher oder bestimmt anzuklicken, wenn der Absender „interessant aussieht“ (Abbildung 22). Auch dieses Verhalten kann gerade für HRM sehr gefährlich sein, da über einen angeklickten Link unbemerkt Schadsoftware auf dem Zielsystem platziert werden kann (Download im Hintergrund).

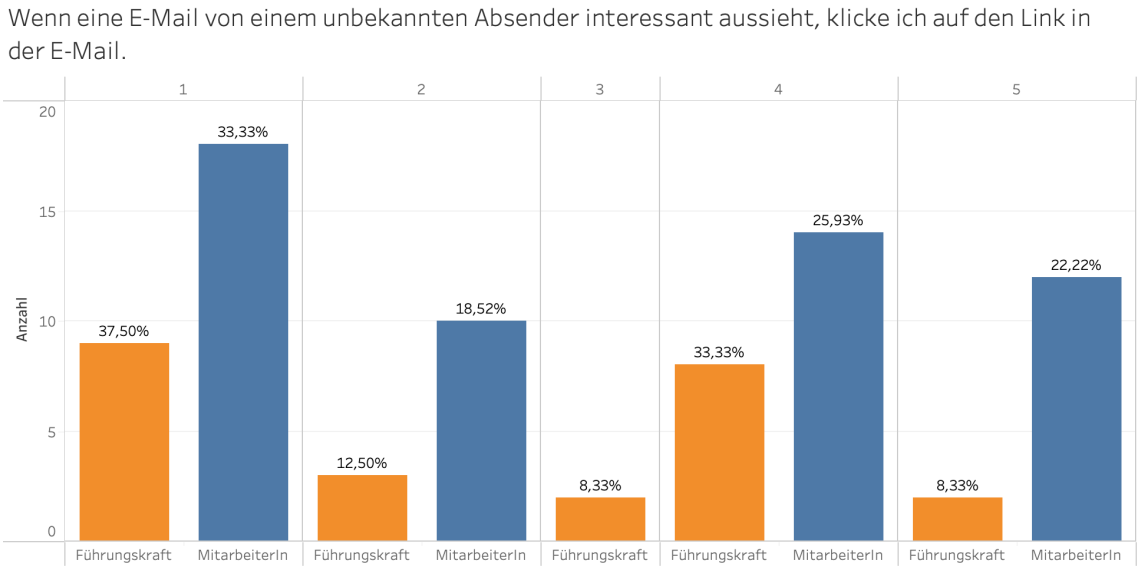


Abbildung 22: Klickverhalten auf Links in E-Mails unbekannter Absender

Zuletzt wurde noch hinterfragt (VI01_07), ob die Befragten zusätzliche Schulungen zum Einsatz von IT-Sicherheitsinstrumenten für erforderlich halten (Abbildung 23); dem stimmten über 57% der Mitarbeiter und mehr als 87% der Führungskräfte eher oder voll und ganz zu.

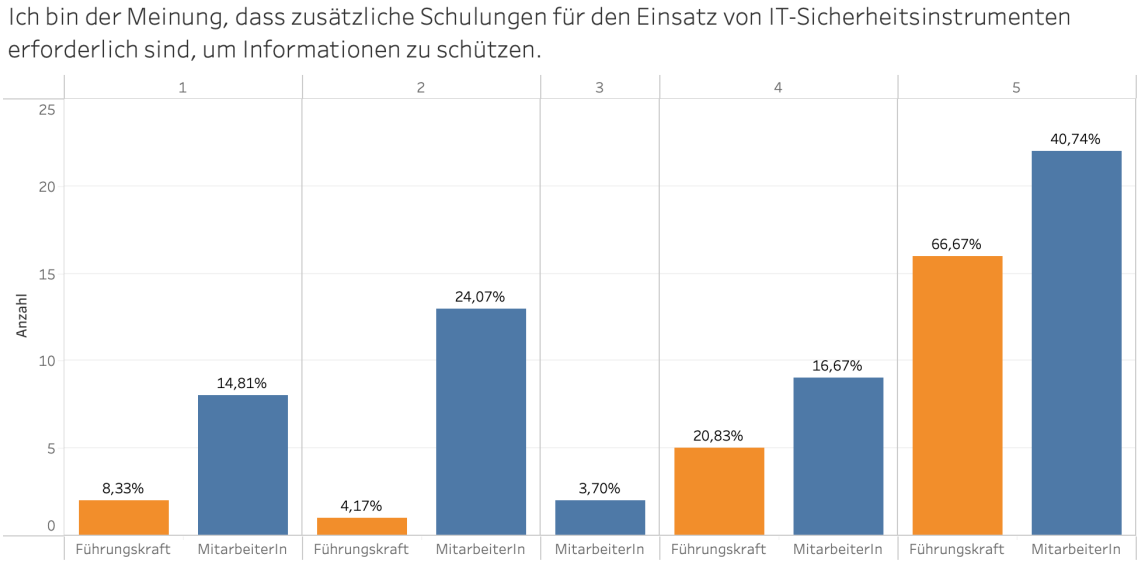


Abbildung 23: Erfordernis zusätzlicher Schulungen

Zur Frage nach der Methode (H204, Mehrfach-Nennung möglich) erhielt das praktische Training mit Abstand die meisten Stimmen (Abbildung 24). Dies belegt, dass das im Projekt angedachte Training für den Kompetenzaufbau eine geeignete Methode zum Aufbau der Kompetenz zu IT-Sicherheit in HRM darstellt.

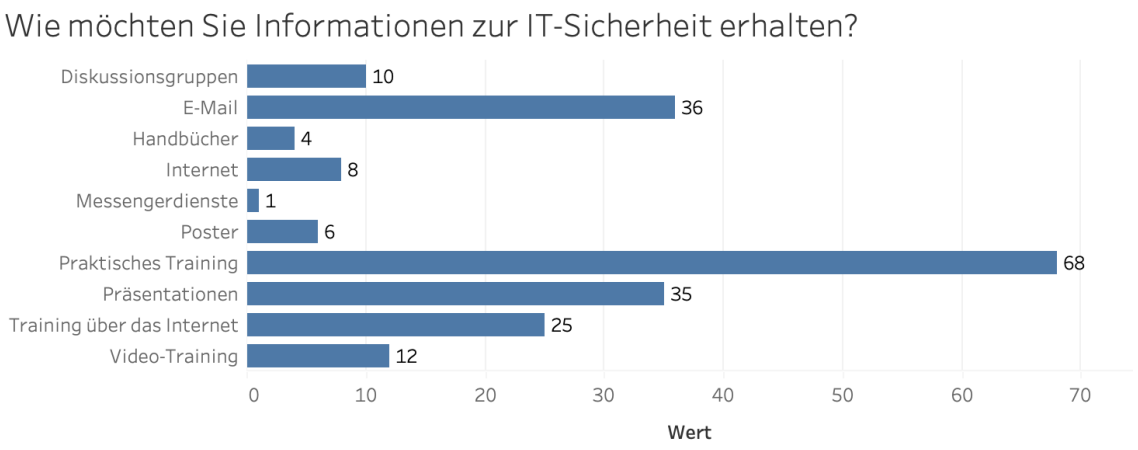


Abbildung 24: Wie sollen die Informationen vermittelt werden? (Mehrfachnennung möglich)

4.2.3 Entwicklung, Durchführung und Validierung eines Trainings

Um ein passendes Training für Mitarbeitende im HRM zu entwickeln und zu evaluieren, wurde eine Masterarbeit vergeben. Diese Masterarbeit wurde in der Zeit von Dezember 2022 bis Juni 2023 von der Masterandin Nora Steinle (Masterstudium Personalentwicklung, Weiterbildungsinstitut casc der UniBw M) durchgeführt (Steinle, 2023) und von ebendieser von Oktober 2023 bis Februar 2024 weitergeführt (Steinle, 2024).

Zunächst wurde eine theoretische Fundierung zu Trainingsmaßnahmen, Kompetenzentwicklung sowie zentralen Anforderungen an zukünftiges Lernen durchgeführt. Zur Festlegung der zu entwickelnden Trainingsmaßnahme wurden die Ergebnisse von Schwarz herangezogen (Abbildung 24), welche „Praktische Trainings“ klar favorisiert.

Anhand der Schritte Bedarfsanalyse, Zielfestlegung, Prozessfestlegung, Implementierung, Evaluation und Transfererfolg wurde eine Checkliste erarbeitet:

Tabelle 14: Wichtigste Aspekte des Trainingsprozesses ((Steinle, 2023), S. 40)

Der Trainingsprozess				
Bedarfsanalyse	Zielfestlegung	Prozessfestlegung	Implementierung	Evaluation und Transfererfolg
▪ Durchführung in Abhängigkeit des Trainingsziels	▪ Übergeordnete Trainingsziele, wie z. B. Entwicklungsmöglichkeiten, schaffen	▪ Festlegung der Bewertungskriterien	▪ Fragen zur Implementierung eines Trainings (siehe Tabelle 2) • An welchem Termin soll das Training stattfinden? • Wie oft soll das Training stattfinden? • An welchem Ort soll das Training durchgeführt werden? • Durch wen soll das Training durchgeführt werden? • Wer soll am Training teilnehmen? • Wie ist die allgemeine Haltung (insbesondere der Unternehmensleitung) gegenüber Trainings? • Nehmen die Teilnehmenden freiwillig teil? • Welche Erwartungen werden an die Teilnehmenden gestellt? • Welche Kompetenzen sollen vermittelt werden? • Welche Maßnahmen zum Lerntransfer sind vorgesehen?	▪ Ergebnisbezogene Evaluation
▪ Hilft, Inhalte, Methoden sowie Niveau an Teilnehmende anzupassen sowie Vorstellung der Organisation zu erfassen		▪ Erfolgsfaktoren für eine Transfersicherung		▪ Prozessbezogene Evaluation
▪ Garant für Kompetenzentwicklung	▪ Spezifische Trainingsziele, wie z. B. Konkretisierung der Verhaltens-, sowie Trainingsziele (Evaluationskriterien)	▪ Festlegung der Trainingsmethode		
▪ Analyseebenen • Organisationsanalyse • Aufgabenanalyse • Personenanalyse				

Die Konzeption des Trainings basierte auf dem konstruktivistischen Lernansatz, der den aktiven Lernenden, welcher das Wissen selbst konstruiert, in den Mittelpunkt stellt (Kauffeld, 2016). Berücksichtigt wurden zudem die von Kauffeld (2016) aufgeführten Faktoren für eine *wirksame* und *nachhaltige* Vermittlung des Lerninhaltes. Enthält der Lernprozess einen Praxisbezug und wird in Gruppenarbeit durchgeführt, erhöht dies das Interesse und die Relevanz und trägt zur Multiperspektivität bei. Die Möglichkeit mit „allen Sinnen“ zu lernen, d.h. komplexe Probleme aus verschiedenen Blickwinkeln zu diskutieren, trägt zur Vielfältigkeit der Anwendung des Gelernten bei (Kauffeld, 2016). Um all diese Faktoren zu vereinen und den sonst eher abstrakten sowie technischen Konzepten und Modellen in der IT-Sicherheit zu trotzen, wurde auf der Basis des spielbasierten Ansatzes von Serious Games ein Kartenspiel entwickelt (Yasin et al., 2019), welches der Trainingsform *near-the-job* zuzuordnen ist.

Das Training mit dem Namen *HRM Defender – The Cybersecurity Card Game* geht in Anlehnung an bereits existierende Kartenspiele, wie z. B. Riskio (Hart et al., 2022), individuell auf mögliche Bedrohungen im HRM ein. Das Spiel wird mit zwei bis acht Teilnehmenden und einer Spielleitung durchgeführt und dauert etwa vier Stunden. Der Ablauf gliedert sich in fünf Phasen:

1. Begrüßung & Einleitung
2. Einführung in das Themengebiet IT-Sicherheit mit praxisnaher Erläuterung der relevanten Fachbegriffe

3. Eigentliche Spielphase (rundenbasiert)
4. Gemeinsame Reflexion & Abschluss
5. Befragung der Teilnehmenden

Als praxisnahes Szenario wurde der Alltag in einer Personalabteilung gewählt, welches durch das haptische Spielbrett unterstützt wird. An Materialien werden

- ein Kartensatz mit 16 Angriffskarten (rot),
- sieben Informationskarten (blau, ausschließlich für die Spielleitung bestimmt) sowie
- 14 Verteidigungskarten (grün) und ein Spielbrett *pro Teilnehmer* benötigt.

Das Spielbrett bildet ein Stockwerk einer HRM-Abteilung ab, welches zur Orientierung für mögliche Angriffsszenarien dienen soll (Abbildung 25).

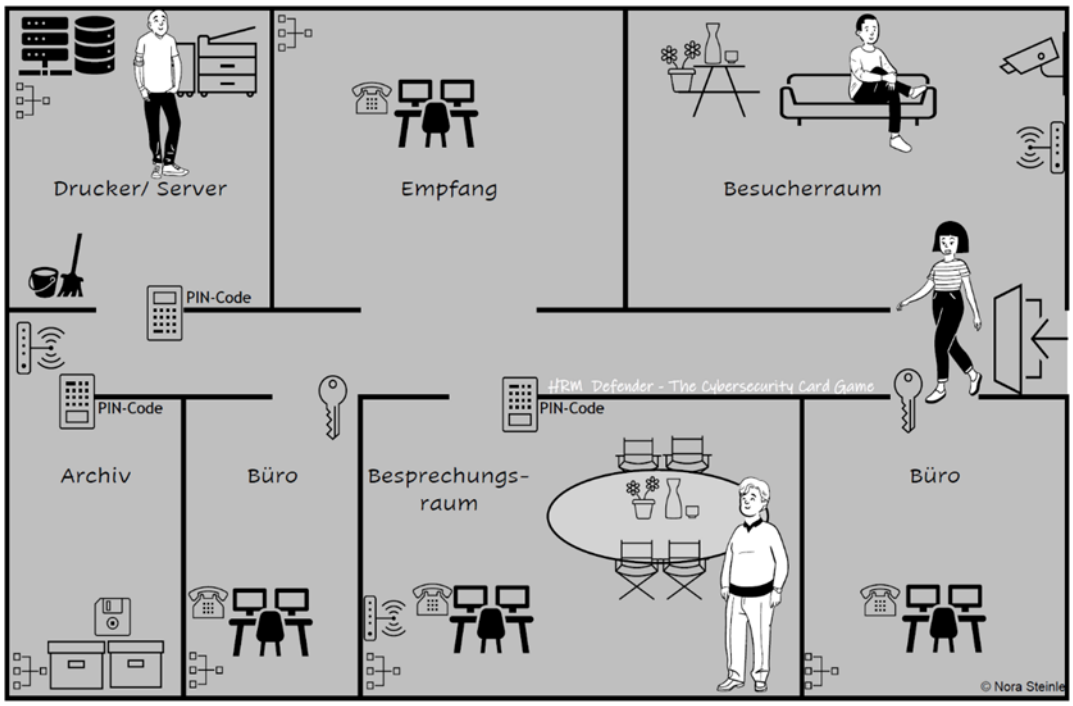


Abbildung 25: Prototyp des Spielfeldes HRM Defender - The Cybersecurity Card Game ((Steinle, 2023), S. 49)

Die folgende Abbildung 26 zeigt jeweils eine Beispielkarte der verschiedenen Kategorien.

Abbildung 26: Beispiele einer Verteidigungs-, Angriffs- sowie Informationskarte (v.l.n.r, (Steinle, 2023), S. 50)

Zum Spielstart werden die Angriffskarten in der vorgesehen Reihenfolge (1-16, Schwierigkeitsgrad der Angriffe aufsteigend) verdeckt auf einen Stapel platziert. Jede spielende Person erhält einen Satz an Verteidigungskarten, welche offen ausgebreitet oder auf der Hand gehalten werden können. Eine freiwillige, angreifende Person zieht die oberste Karte aus dem Angriffsstapel (rot) und liest diese vor. Die übrigen Spielenden wählen jeweils eine Verteidigungskarte aus ihrem Deck (grün) aus, mit welcher der Angriff abgewehrt werden soll. Anschließend stellen die Spieler ihre gewählte Verteidigungskarte vor und begründen ihre Auswahl, wobei die Spielleitung durch aktive Nachfrage die Diskussion unter den Teilnehmern fördert. Anschließend werden die Verteidigungskarten zurück in das eigene Kartendeck gelegt und der nächste Teilnehmende nimmt die Rolle der angreifenden Person ein. Die Informationskarten (blau) können von der Spielleitung bedarfsweise im Spielverlauf eingesetzt werden, um das Wissen der Spielenden zu vertiefen.

Um die Wirksamkeit des Trainings zu messen, wurde nach dem Training jeweils eine zweistufige Befragung auf der Basis von Grohmanns und Kauffelds *Questionnaire for Professional Training Evaluation* (Grohmann & Kauffeld, 2013) durchgeführt.

Das Kartenspiel wurde während der Projektlaufzeit insgesamt viermal von Fr. Steinle durchgeführt, dokumentiert und evaluiert:

Tabelle 15: Durchgeführte Trainings HRM-Defender während der Projektlaufzeit FLEIS

Termin	Teilnehmer	Ort
April 2023 (Pilot)	Sechs Spieler, eine Spielleiterin, ein Beobachter	Bundesbehörde, Mannheim
Oktober 2023	Fünf Spieler, eine Spielleiterin	Universität der Bundeswehr München
November 2023	Sechs Spieler, eine Spielleiterin	Universität der Bundeswehr München
Dezember 2023	Sechs Spieler, eine Spielleiterin	Bundesbehörde, Stuttgart

4.3 Zwischenfazit

Die durchgeführte Umfrage zur IT-Sicherheit im HRM stellt eine wertvolle Ergänzung für die Wissenschaft dar, mit der weitergehende Forschung betrieben werden kann. Die Auswertung der Daten zeigt, dass in vielen Bereichen des HRM bezüglich IT-Sicherheit Verbesserungspotential vorhanden ist.

Das folgende Zwischenfazit zum entwickelten Training *HRM Defenders – The Cybersecurity Card Game* ist ((Steinle, 2024), S. 33-34, teilweise wörtlich, teilweise sinngemäß, teilweise gekürzt) entnommen:

Die Auswertung der Befragungen zu den durchgeführten Trainings zeigt, dass die Trainingskonzeption von den Spielenden durchweg positiv bewertet wird. Hierbei ist irrelevant, ob die Abstimmenden aus dem Personalbereich oder anderen Bereichen, wie z. B. der IT, stammen. Es wurde deutlich, dass die Spielenden das Training selbst mit zeitlichem Abstand als sehr positiv in Erinnerung behalten und dass für die überwiegende Anzahl sehr viel neues Wissen vermittelt werden konnte. Zudem gaben die Spielenden in ihrer Bewertung an, dass die erworbenen Kenntnisse einen Nutzen für ihre tägliche Arbeit haben und dieses auch umgesetzt werden können. Weiterhin, dass die Teilnahme am Training durchaus auch Einfluss auf die jeweiligen Arbeitsabläufe haben kann.
Werden diese Aussagen der Teilnehmenden nach dem Training betrachtet, so wird die praxisnahe und spielerische Wissensvermittlung und die Form des Kartenspiels als durchweg positiv bewertet. Besonders die entstehende Gruppendynamik führt zu einer Erhöhung der Multiperspektivität. Dies konnte unabhängig der Gruppenzusammenstellung erreicht werden.
Bei den Durchführungen wurde deutlich, dass das Spiel die Faktoren Technik, Organisation und Mensch vereint. Vielen Spielenden wurde die Relevanz dieser drei Faktoren, insbesondere die Bedeutung der Zusammenarbeit von IT- und Personalabteilung, durch das Training erst richtig bewusst.
Die weiteren Durchführungen und Evaluationen haben gezeigt, dass das Trainingskonzept des *HRM Defender – The Cybersecurity Card Game* sein Ziel, den sonst eher abstrakten sowie technischen Cybersecurity-Konzepte trotzen konnte und es ein Format bietet, welches von unterschiedlichen Teilnehmenden gerne besucht, den Grad der Sensibilisierung der Mitarbeitenden spielerisch erhöht, sowie den Faktor Mensch in der Rolle des Sicherheitssensors gegen Cyberangriffe bestärkt.

5 Arbeitspaket 8.1: Anwendungsszenario & Geschäftsmodellinnovationen

Im Folgenden werden die Inhalte des Arbeitspaketes *8.1 Anwendungsszenario & Geschäftsmodellinnovationen* beschrieben. Dieses Arbeitspaket 8.1 ist (wie in Abbildung 1 zu sehen) das vierte Arbeitspaket der UniBw M im Projekt.

Die folgende Abbildung 27 zeigt die geplanten Inhalte des Arbeitspaketes.

AP 8.1: Anwendungsszenario & Geschäftsmodellinnovationen	**6 PM (UniBw M)**
Zuständig	**Lead UniBw M, Mitarbeit alle**
Vorgehen	• Anwendungsszenario identifizieren & beschreiben • Potential & Einsatzmöglichkeiten des entwickelten Systems prüfen • Geschäftsmodellinnovationen entwickeln & Potentiale untersuchen
Methoden	• Desk Research • Markt-Recherche von neuen Trends in der Startup-Szene • Workshops • Business Model Canvas
Ergebnisse	• Durchgeführte und ausgewertete Workshops • Identifiziertes und beschriebenes Anwendungsszenario • Einschätzung des Potentials und der Einsatzmöglichkeiten des entwickelten Systems • Mehrere entwickelte und dokumentierte Geschäftsmodelle

Abbildung 27: Geplante Inhalte des Arbeitspaketes 8.1

5.1 Forschungsgegenstand und Forschungsfragen

Wenn ein Unternehmen am Markt bestehen möchte, muss es wirtschaftlich handeln. Dies kann in einem Geschäftsmodell abgebildet werden: „Geschäftsmodelle sind Abbildungen von wirtschaftlich wertschaffenden Transaktionen (= Austauschbeziehungen).“ ((Hoffmeister, 2022), S. 46).

Für das Projekt FLEIS sind Geschäftsmodelle insbesondere in der Ausprägung eines *digitalen* Geschäftsmodelles relevant: „Digitale Geschäftsmodelle sind es dann, wenn die Austauschbeziehungen mittels digitaler Technologie realisiert und erfasst werden.“ ((Hoffmeister, 2022), S. 47)

Betrachtet man die Ziele digitaler Geschäftsmodelle genauer, so kann eine Einteilung in

- monetäre und nicht-monetäre Ziele
- direkte und indirekte ökonomische Ziele

vorgenommen werden (vgl. (Hoffmeister, 2022), S. 122). Die folgende Abbildung setzt diese Ziele in Relation:

Abbildung 28: Vorschlag zur Einordnung der Ziele eines digitalen Geschäftsmodells ((Hoffmeister, 2022), S. 123)

Für FLEIS sind insbesondere die direkten Ziele im monetären und nicht-monetären Bereich relevant: Zum einen soll das entwickelte technische Modell kommerzialisiert werden, zum anderen müssen jedoch zur Initialisierung und Verbesserung der FL-Modelle auch möglichst viele, qualitativ hochwertige Daten gesammelt werden (diese Aspekte werden insbesondere in den Kapiteln 5.2.6 und 5.2.7 berücksichtigt).

Dieses Arbeitspaket 8.1 untersucht folgende **Forschungsfragen**:

> *F8.1.1: Welche (digitalen) Geschäftsmodelle wenden Startups im HRM-Bereich an, um wirtschaftlich zu handeln?*
>
> *F8.1.2: Welches (digitale) Geschäftsmodell ist geeignet, um die in FLEIS entstandene technische Lösung zu vermarkten?*

5.2 Methoden und Ergebnisse

Um die **Forschungsfrage F8.1.1** zu beantworten, wurde eine Marktrecherche im Bereich HRM-Startups durchgeführt, als Methode wurde Desk Research gewählt. Als Ergebnis konnten ein Startup sowie ein weiteres Unternehmen identifiziert werden, deren Geschäftsmodell für FLEIS relevant ist. Diese wurden bei der Bearbeitung der Forschungsfrage F8.1.2 berücksichtigt.

Um die **Forschungsfrage F8.1.2** zu beantworten, wurden mehrere Workshops durchgeführt und ausgewertet, als Methode wurde die Business Model Canvas (Osterwalder & Pigneur, 2011) gewählt. Als Ergebnis wurden die beiden Geschäftsmodelle „FLEIS4Bayern“ und „FLUniBwM“ ausgearbeitet.

5.2.1 Marktrecherche: Geschäftsmodelle HRM Startups

Zur Beantwortung der *Forschungsfrage F8.1.1.* wurde von Oktober bis November 2023 eine Markt-Recherche im Bereich HRM-Startups durchgeführt. Informationsquelle war dabei die Zeitschrift „Personalmagazin“ (Fachmagazin für das Personalwesen), welches seit seiner Ausgabe 01/2020 monatlich ein Startup im Heft vorstellt.

Es wurden 48 Startups aus dem HRM-Bereich ausgewertet. Dabei wurde jeweils analysiert:

- Welche Lösung bietet das Startup an?
- Unter welcher Internetadresse sind weitere Informationen des Startups verfügbar?
- In welche Kategorie fällt das Startup?
- Welches Geschäftsmodell nutzt das Startup, um wirtschaftlich zu handeln?

Es stellte sich bei der Analyse heraus, dass keines der betrachteten Startups eine Software im Bereich IT-Sicherheit anbietet (die vollständige Tabelle der analysierten Startups ist im Anhang enthalten). Daher wurden insbesondere solche Startups betrachtet, welche eine Art „Add-On“ mit entsprechendem Mehrwert auf ein bestehendes System im HRM bieten; dies ist lediglich bei einem der analysierten Startups, „Ravio“, der Fall (Tabelle 16):

Tabelle 16: Analysiertes Startup Ravio

Name	Referenz	Kategorie	Kurzbeschreibung	Link	Zahlender Kunde?	Einnahmestrang
Ravio	PM 4/23	HR-Management	Bieten Echtzeit-Gehaltsübersichten zur Entwicklung von Gehaltsmodellen, indem sie sich direkt an HR-Systeme ankoppeln.	https://ravio.com/	Unternehmen	n.A.

Ein weiteres relevantes Geschäftsmodell ergab sich aus dem Interview mit einem Unternehmen zum Thema FL (*in Klammern wurde bereits die entsprechende Kategorie der Business Modell Canvas angegeben, siehe Kapitel 5.2.2*):

Das Unternehmen selbst ist Teil eines FL-Netzwerks und agiert in diesem als lokaler Kunde (*Data Owner, Teil der Zielgruppe*). Dabei versteht sich das Unternehmen als aktiver Teil des FL-Netzwerks (*Schlüsselpartner*), der Einfluss auf einzelne FL-Prozessschritte nimmt, seine Anforderungen einbringt und Entscheidungen des Service Providers (FL-Provider) beeinflussen kann. Die Aufbereitung der Daten (*Schlüsselressource*) ist für das Unternehmen von höchster Relevanz und nimmt mit einem Zeitraum von über zwei Jahren auch den größten Zeitansatz für die Vorbereitung und Aufnahme in das FL-System in Anspruch

(*Schlüsselaktivität*). Der Service Provider stellt dem Kunden für die Phase der Integration und auch darüber hinaus einen externen Berater und IT-Experten zur Seite, so dass das Unternehmen dauerhaft einen Ansprechpartner für individuelle Probleme hat, an den es sich persönlich wenden kann (*Kanäle, Kundenbeziehung*).

Als Grund für die Teilnahme an dem FL-Netzwerk gab das Unternehmen an, dass es sich von dem Projekt sowohl eine Steigerung der wirtschaftlichen Effizienz als auch eine Bereicherung im eigene Forschungs- und Entwicklungsbereich verspricht (*Kundennutzen*). Finanziell muss das Unternehmen derzeit keine Gebühren oder sonstige Aufwandsentschädigungen an den Service Provider zahlen, da dieser angibt, ebenfalls durch die Weiterentwicklung in der eigenen Forschung und die Nutzung des globalen FL-Modells von diesem Projekt zu profitieren (*Einnahmequellen*). Darüber hinaus gab der Interviewpartner an, dass sich die Ansprechpartner des Providers durchaus bewusst sind, dass das Projekt auch beim Kunden mit Kosten im personellen, technischen und organisatorischen Bereich verbunden ist und diese Kosten erst durch die Nutzung eines funktionsfähigen und wertschöpfenden FL-Systems kompensiert werden müssen (*Kostenstruktur*). Es wird vermutet, dass sich der Anbieter durch die kostenlose Bereitstellung einen größeren Kundenstamm erhofft, da ein FL-System nur durch die Zusammenarbeit vieler verschiedener Nutzer funktionieren kann. Eine weitere Herausforderung in diesem Fall besteht darin, dass es sich um ein horizontales Netzwerk handelt, so dass sich die angeschlossenen Unternehmen als Konkurrenten in einer Branche sehen, was die Zusammenarbeit, die stark auf Vertrauen und Partnerschaft basiert, zusätzlich erschweren kann.

Diese beiden Geschäftsmodelle wurden im Kapitel 5.2.7 für die Ausarbeitung des Geschäftsmodells für FLEIS berücksichtigt.

5.2.2 Die Methode Business Model Canvas

In der *Forschungsfrage F8.1.2* sollten zunächst mehrere Geschäftsmodell erarbeitet werden. Soll ein Geschäftsmodell erarbeitet werden, kann man verschiedene Methoden anwenden. Eine solche Methode ist die Business Model Canvas ((Osterwalder & Pigneur, 2011), im Folgenden mit BMC abgekürzt).

Die BMC wurde von Alexander Osterwalder im Jahr 2004 in seiner Dissertation an der Universität Lausanne in der Schweiz vorgestellt (Osterwalder, 2004). Anschließend wurde die BMC im Buch „Business Model Generation“ (Osterwalder & Pigneur, 2011) mit Prof. Yves Pigneur veröffentlicht.

Osterwälder wollten ein Geschäftsmodellkonzept schaffen, dass „so einfach wie möglich“ und dabei „so konkret wie nötig“ ist. Jeder sollte diese Methodik einfach verstehen, um damit die Grundlage für eine Diskussion über das Inhaltliche zu ermöglichen. Dies scheint mit der BMC gelungen: Die BMC wurde in den vergangenen 20 Jahren stetig weiterentwickelt und genutzt.

In der Original-Version setzt die BMC auf eine generische Canvas, die in der folgenden Abbildung 29 zu sehen ist:

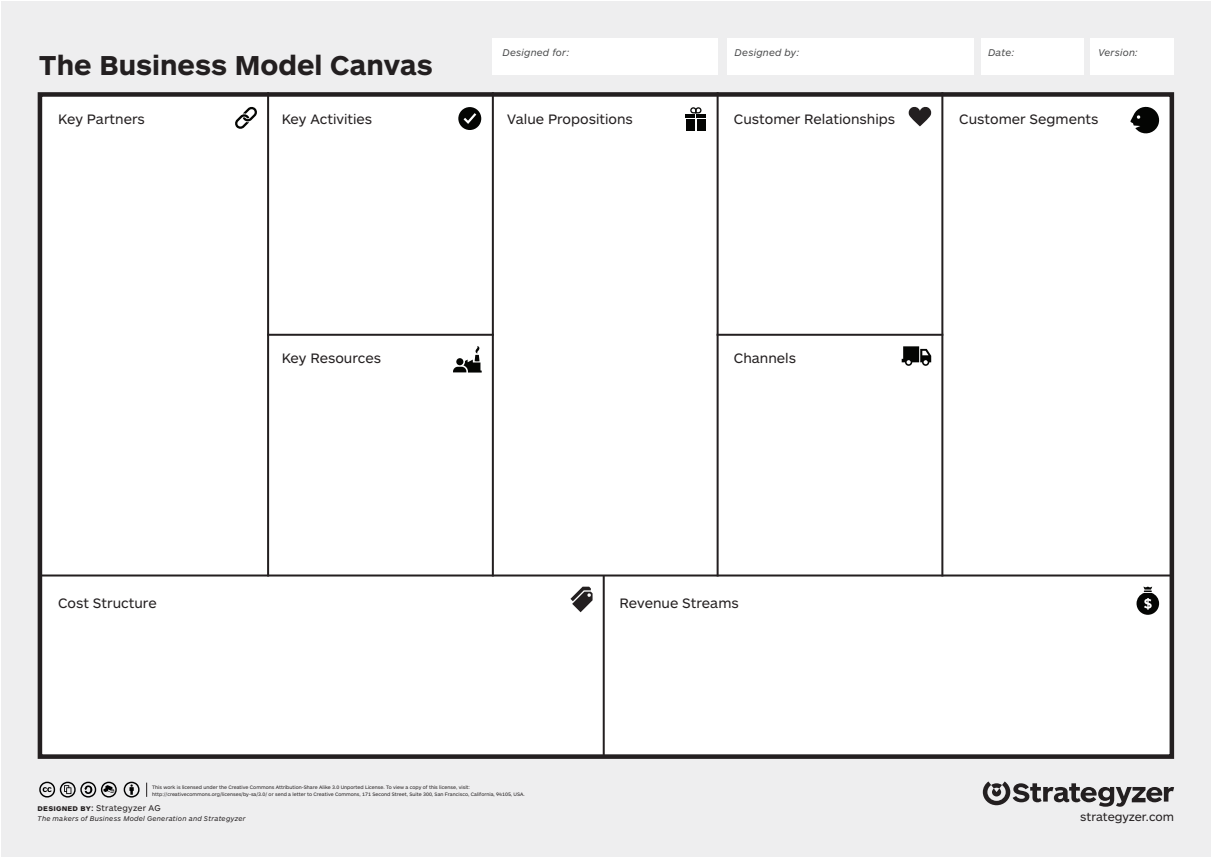


Abbildung 29: Die Business Model Canvas (Quelle: https://www.strategyzer.com/ vom 27.03.2018)

Neben dieser ersten, generischen Version der BMC wurden in den letzten Jahren viele spezielle BMC entwickelt, so z.B. auch eine für die Entwicklung von Geschäftsmodellen im KI-Umfeld (Abbildung 30):

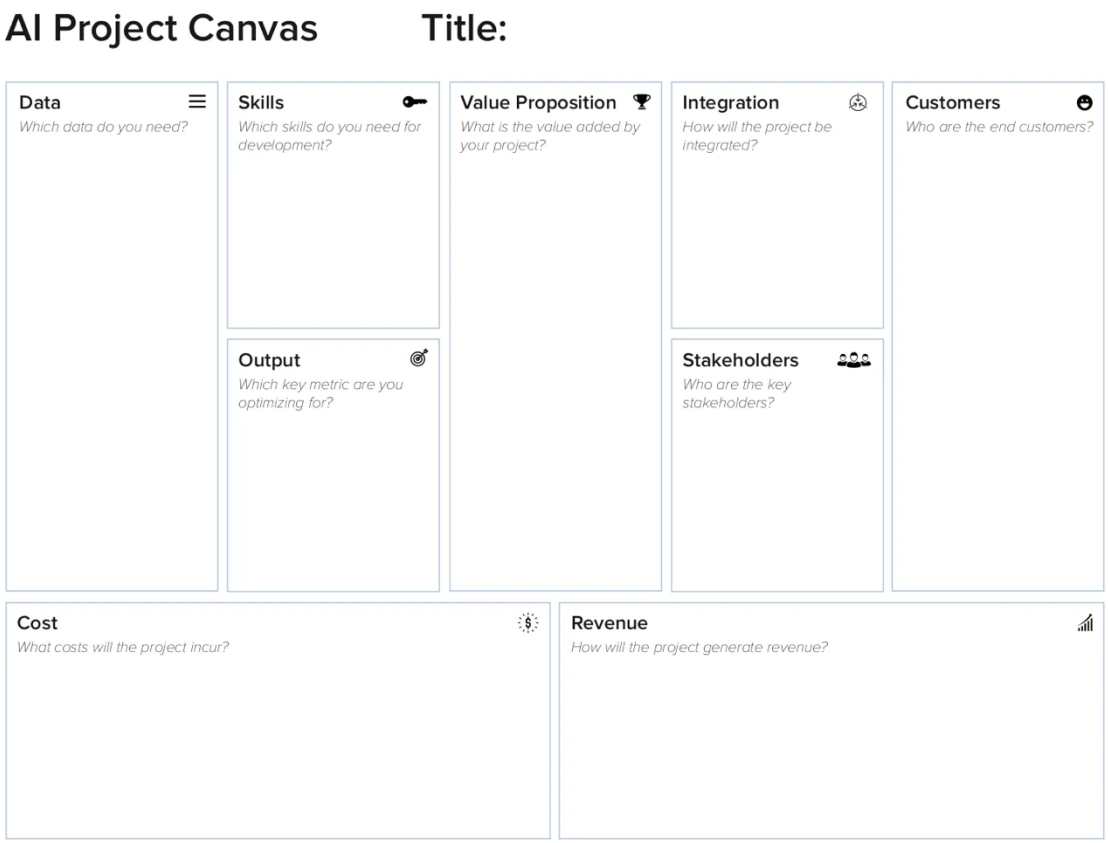


Abbildung 30: Eine Business Model Canvas speziell für KI-Projekte (Quelle: https://towardsdatascience.com/introducing-the-ai-project-canvas-e88e29eb7024 vom 21.03.2023)

Im Projekt FLEIS wurde sich bewusst gegen diese KI-Version und stattdessen für die generische Version der BMC entschieden, da die Methodik für die Workshops möglichst einfach und für die Teilnehmenden schnell zu verstehen sein sollte.

5.2.3 Durchgeführter Workshop 1

Am 05.06.2023 wurde im Rahmen der Vorlesung Modelle & Methoden der Wirtschaftsinformatik an der Universität der Bundeswehr München der erste Workshop zu Geschäftsmodell-Innovationen mit Hilfe der BMC durchgeführt. Diese Teilnehmergruppe wurde bewusst gewählt, da sie typische Anwender der in FLEIS entwickelten FL-Lösung darstellen können.

Die einzelnen Kategorien wurden von der Dozentin jeweils zunächst theoretisch erläutert. Anschließend erarbeiteten die Teilnehmenden in kleinen Gruppen mögliche Inhalte der jeweiligen Kategorie, welche dann im Plenum vorgestellt und diskutiert wurden. Die Ergebnisse

wurden parallel zu dieser Diskussion digital im Online-Tool Miro zu Dokumentationszwecken erfasst.

Die folgende Abbildung zeigt die entstandene Business Model Canvas (alle entstandenen BMC sind im Anhang dieses Berichtes enthalten).

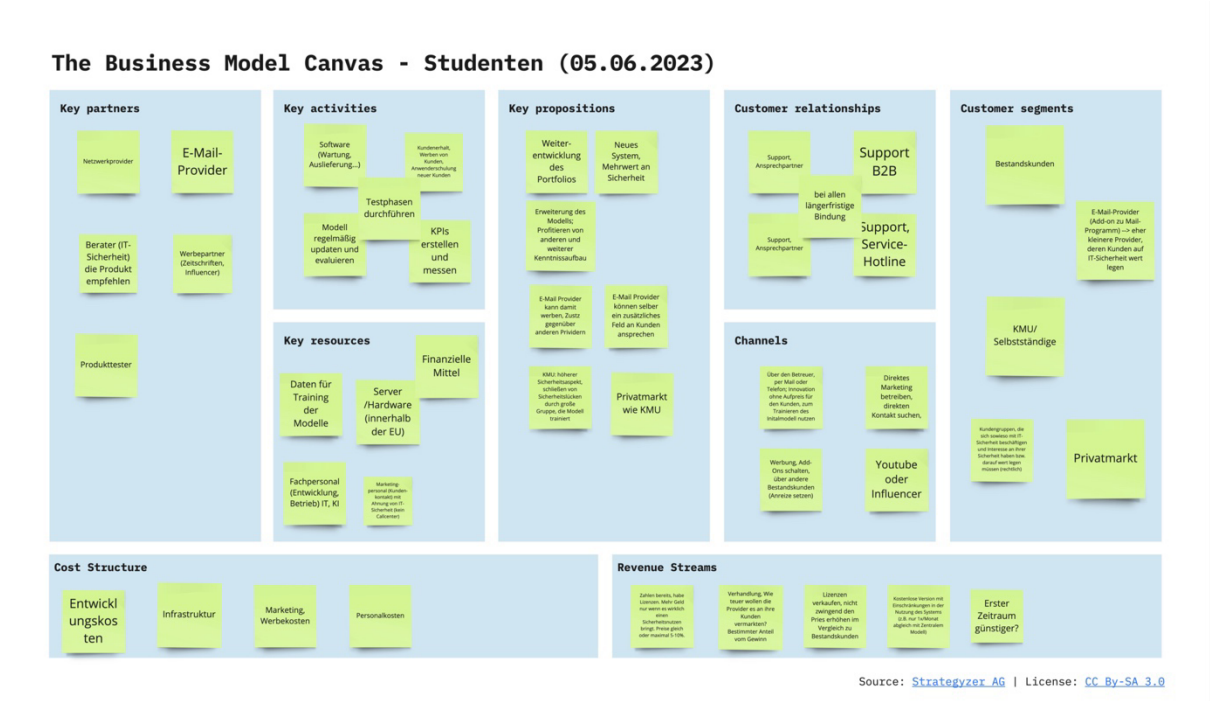


Abbildung 31: Erarbeitete Business Model Canvas vom 05.06.2023

5.2.4 Durchgeführter Workshop 2

Am 04.07.23 wurde im Rahmen des Projekttreffens FLEIS der zweite Workshop zu Geschäftsmodell-Innovationen mit Hilfe der BMC durchgeführt. Der Workshop dauerte ca. 120 Minuten und wurde in zwei Gruppen zu je vier Personen durchgeführt, wobei die MitarbeiterInnen der UniBw M als Moderatoren fungierten.

Bei diesem Workshop erfolgte die Einführung in die Methode BMC mittels eines kurzen Videos, da den meisten Teilnehmenden die Methode bereits bekannt war.

Im Anschluss an die Arbeitsphase wurden die Ergebnisse im Plenum vorgestellt und diskutiert. Die Ergebnisse wurden im Nachgang digital im Online-Tool Miro zu Dokumentationszwecken erfasst.

Die folgende Abbildung 32 und Abbildung 33 zeigen die entstandenen BMC (alle entstandenen BMC sind im Anhang dieses Berichtes enthalten).

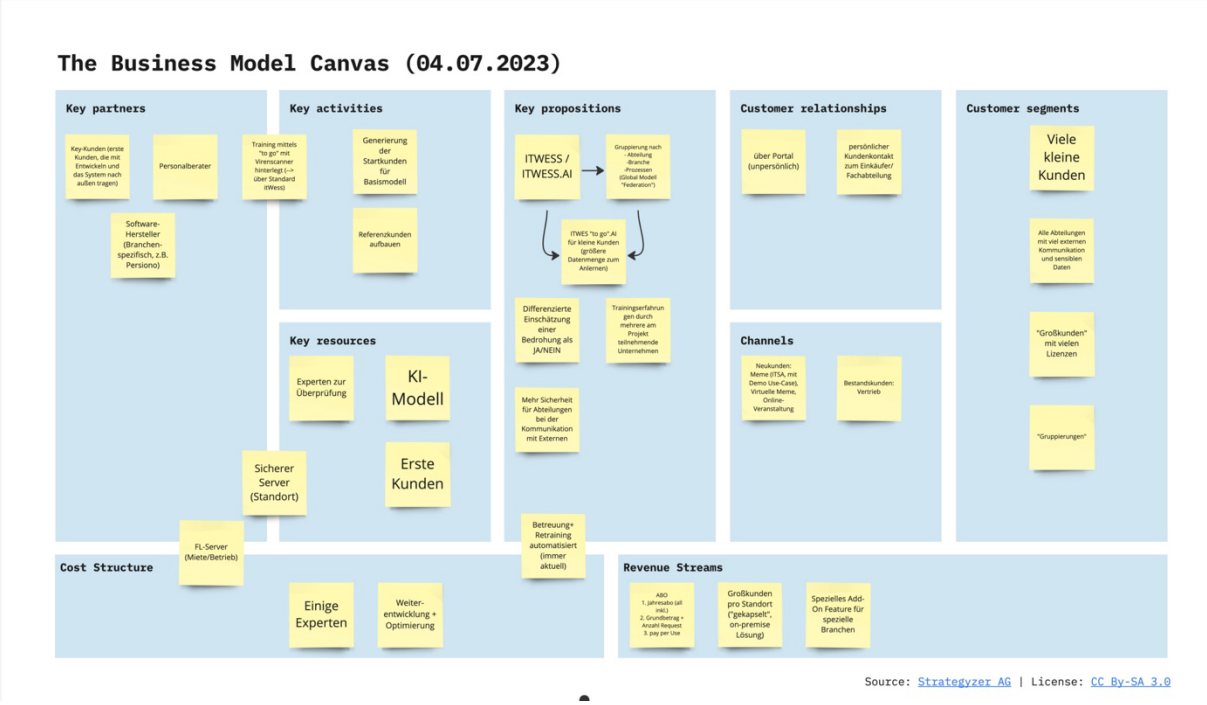


Abbildung 32: Entstandene BMC (Gruppe 1)

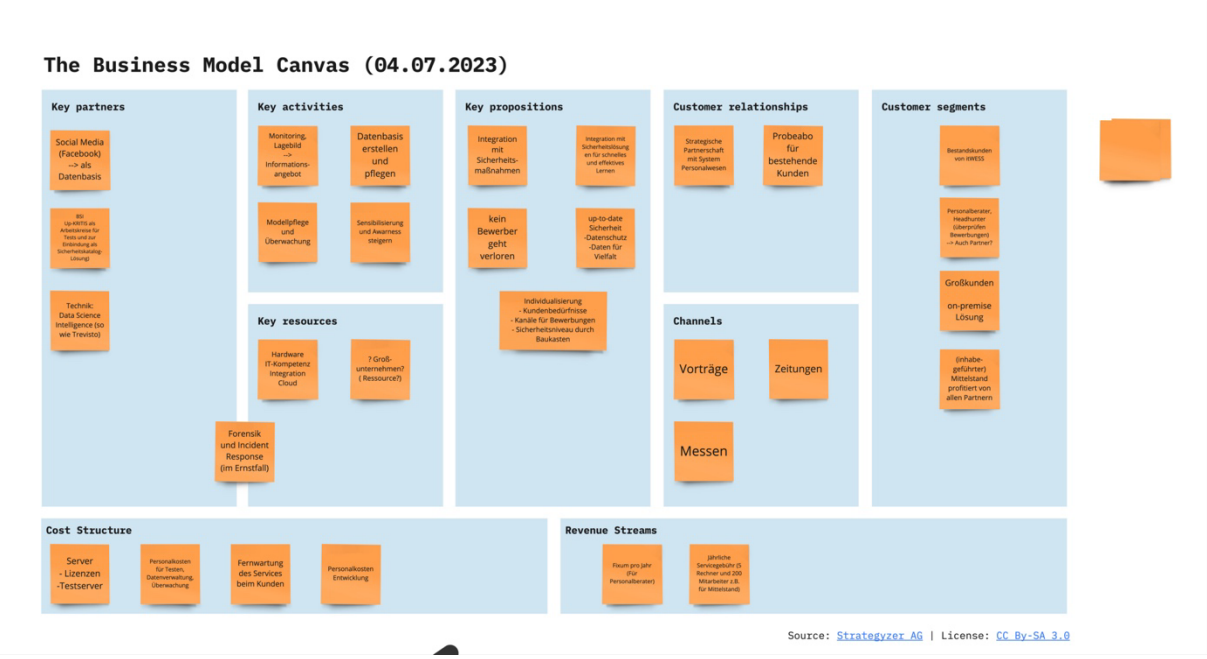


Abbildung 33: Entstandene BMC (Gruppe 2)

5.2.5 Auswertung Workshops

Die drei erarbeiteten Canvas‘ wurden zunächst in eine gemeinsame BMC überführt, um im nächsten Schritt eine Strukturierung zu erarbeitet. Die folgende Abbildung 34 zeigt die konsolidierte BMC.

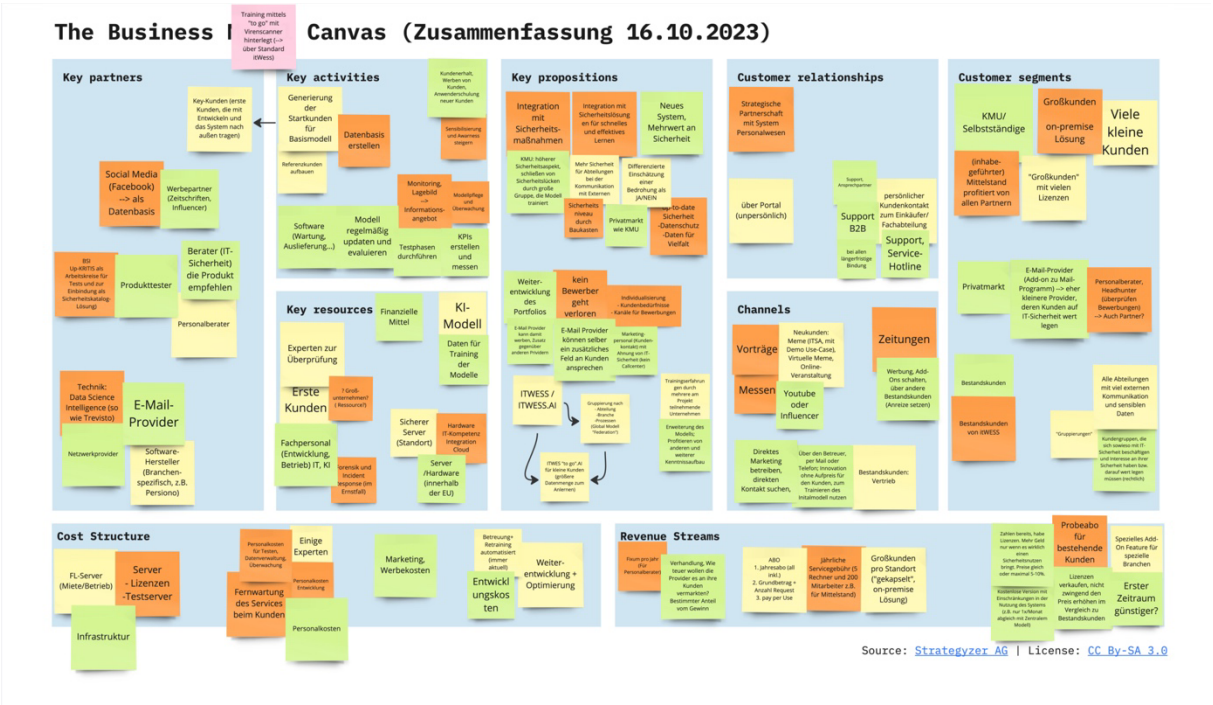


Abbildung 34: Zusammengeführte BMC

Für die Strukturierung wurde eine an die qualitative Inhaltsanalyse angelehnte Methode nach dem Vorbild der Codierung nach Kuckartz (siehe auch Kapitel 2.2.2) angewandt. Die Antworten in den verschiedenen Segmenten der BMC wurden gruppiert und mit einem Code versehen, um eine übersichtliche Strukturierung zu erhalten.

Die folgende Abbildung 35 zeigt das Ergebnis der Auswertung.

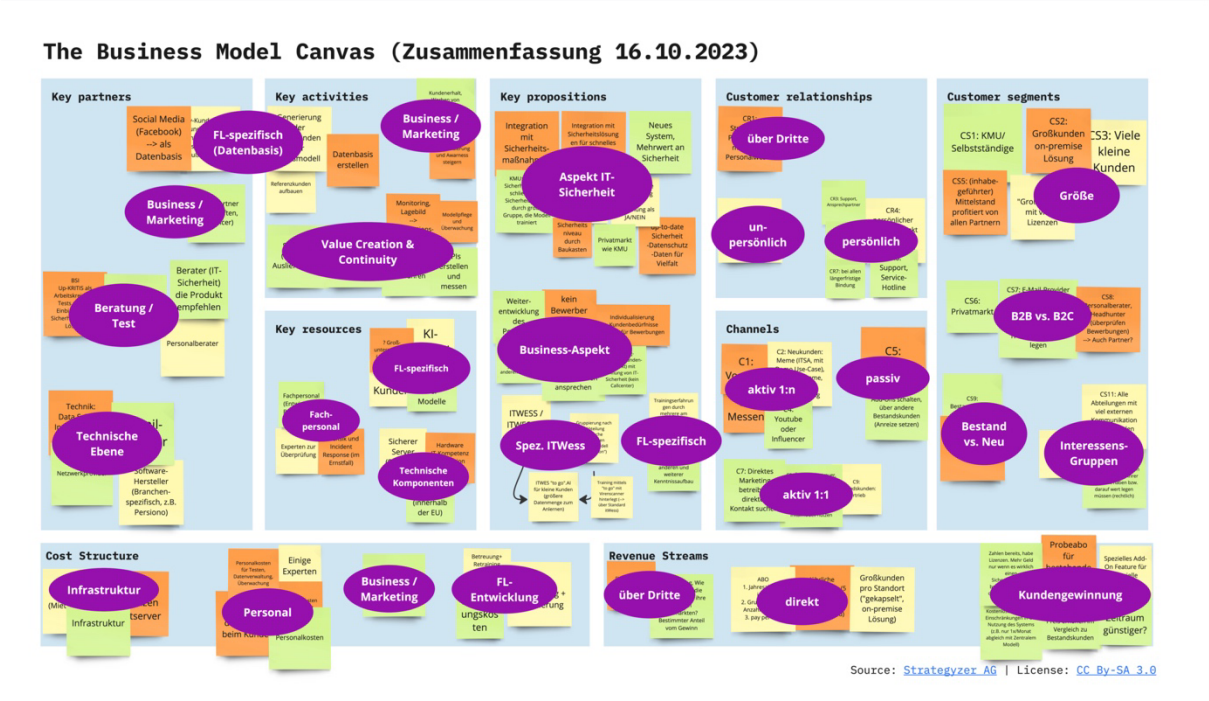


Abbildung 35: Zusammengeführte, strukturierte BMC

5.2.6 Ergebnis: Entwickeltes Geschäftsmodell FLEIS4Bayern

Am 06.11.2023 wurde den Projektpartnern die zusammengeführte, strukturierte BMC (Abbildung 35) im Rahmen eines virtuellen Projekttreffens vorgestellt. Anschließend wurden die Vorstellungen & Wünsche der Projektpartner bezüglich des zu entwickelnden Geschäftsmodells abgefragt. Aus diesen Daten wurde von der UniBw M das Geschäftsmodell „FLEIS4Bayern“ mit zugehöriger BMC entworfen.

Das Geschäftsmodell FLEIS4Bayern fällt in die Kategorie Business to Governance (B2G). Es verfolgt auf den ersten Blick ein *direktes monetäres* sowie ein *direktes ökonomisches* Ziel – für die Nutzung des FL-Modells sollen die Kunden bezahlen (Pay-per-X, vgl. (Hoffmeister, 2022), S. 78). Jedoch ist beim genaueren Betrachten auch ein *indirektes ökonomisches* Ziel enthalten – denn nur durch die Beteiligung vieler Instanzen (Kunden) am FL-Modell kann das Modell fortlaufend verbessert werden. Es muss also auch einen Anreiz für die Kunden geben, das lokal trainierte FL-Modell zu teilen und in das globale Modell einzuspeisen.

Da das Geschäftsmodell FLEIS4Bayern und die zugehörige BMC sehr spezifisch auf die teilnehmenden Unternehmen itWatch und Trevisto und das Projekt zugeschnitten sind, wird es an dieser Stelle nicht veröffentlicht.

5.2.7 Ergebnis: Alternatives Geschäftsmodell FLUniBwM

Aus den Erkenntnissen des Kapitels 5.2.1 erstellte das Team der UniBw M folgendes Geschäftsmodell, welches für die wirtschaftliche Nutzung eines serviceorientierten FL-Modells genutzt werden kann.

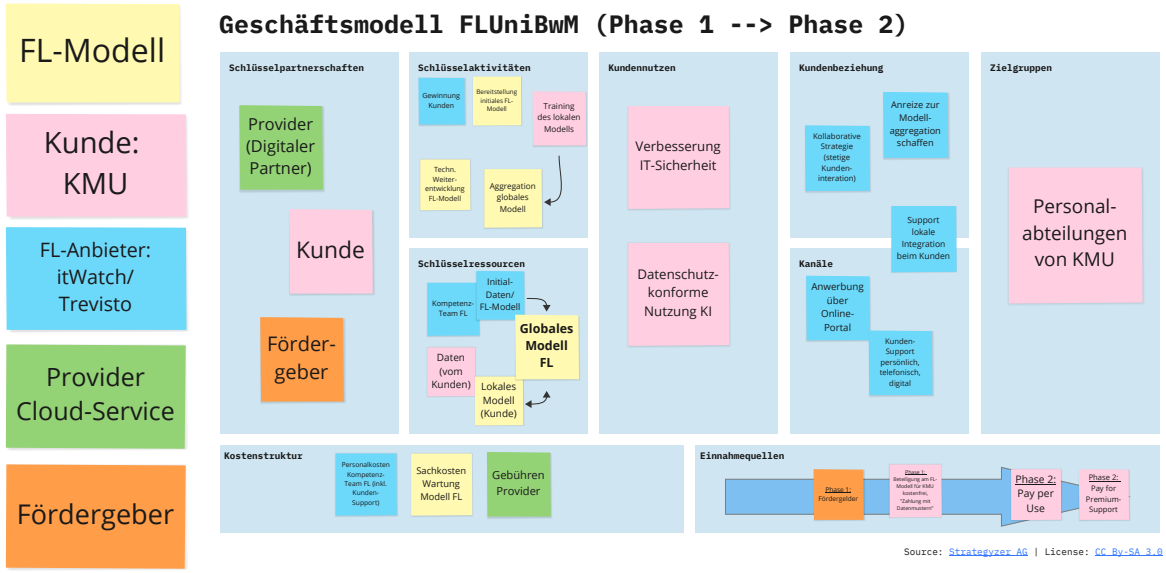


Abbildung 36: BMC für das Geschäftsmodell FLUniBwM

Das Geschäftsmodell FLUniBwM stellt den kollaborativen Gedanken von FL in den Mittelpunkt. Es unterscheidet sich damit von einer reinen Dienstleistung; vielmehr basiert das Geschäftsmodell auf einem kooperativer Wertschöpfungsprozess, an dem sowohl FL-Anbieter als auch Kunden gleichermaßen beteiligt sind. Insbesondere beleuchtet dieser Ansatz einige grundlegende Fragen genauer:

- Wie kann das FL-Modell in der Anfangsphase an Datenqualität gewinnen?
- In welcher Form müssen die Daten der lokalen Modelle vorliegen?
- Welchen Anreiz haben die Kunden, ihr lokales Modell in regelmäßigen Abständen mit dem globalen Modell zu aggregieren?
- Wie kann eine langfristige Bindung der Kunden erreicht werden?
- Wie kann eine gemeinsame Arbeitsumfeld für Provider und Kunde geschaffen werden?

Durch die Integration vieler Teilnehmer soll eine qualitativ hochwertige Datenbasis für das FL-System geschaffen und beibehalten werden. Dazu wird das Prinzip **Cross-Silo** umgesetzt, bei dem viele unterschiedliche Kunden mit großen Datenbeständen (="Silos") einer Branche miteinander im FL-Modell kooperieren. Dieses Prinzip steht im Gegensatz zum Cross-

Device-Ansatz, welcher auf viele kleine Kunden mit kleinen Datenbeständen setzt (wie z.B. Einzelpersonen).

Die Datenmuster, welche die Kunden mittels der lokalen Modelle zur Verfügung stellen, werden als **homogene Daten** aggregiert. Zwar würde die Strategie der heterogenen Daten einen Qualitätsgewinn für das FL-Modell bedeuten (Camajori Tedeschini et al., 2022), jedoch ist dieser Ansatz bisher nur wenig erforscht und daher für die praktische Umsetzung bisher nicht geeignet.

Das Geschäftsmodell ist zeitlich in zwei Phasen unterteilt. In der 1. Phase, die beispielsweise ein Jahr dauern kann, ist die Nutzung des FL-Systems für die Kunden kostenfrei. So wird die Datenqualität des FL-Modells zunächst gesteigert und zusammen mit den Kunden ein Mehrwert für die IT-Sicherheit bei den Teilnehmern geschaffen.

In der 2. Phase kann dann eine Monetarisierung des Geschäftsmodells erfolgen. So kann zum einen eine Unterscheidung in aktive und passive Teilnehmer des FL-Modells getroffen werden – aktive Nutzer zahlen weiterhin mit ihren Daten, welche sie in ihr lokale Modelle einpflegen, welches in regelmäßigen Abständen mit dem globalen Modell aggregiert wird, passive Nutzer entrichten eine Gebühr für die Nutzung des FL-Systems (sie pflegen keine eigenen Daten ein).

Für dieses Geschäftsmodell wurden unterschiedliche Rollen identifiziert, welche farblich in der BMC gekennzeichnet sind (Tabelle 17):

Tabelle 17: Rollen im Geschäftsmodell FLUniBwM

Rolle	Detail	Farbe	Erläuterung
FL-Modell	Globales FL-Modell	Gelb	Das dem Kunden bereitgestellte End-Produkt.
Kunde	KMU	Rosa	Kleine und mittlere Unternehmen deutschlandweit.
FL-Anbieter	Konsortium aus itWatch und Trevisto	Blau	Diese stellen das initiale FL-Modell und die initialen Daten zur Verfügung. Sie werben Kunden an und unterstützen die Kunden (Support) bei der Nutzung des FL-Modells. Darüberhinaus übernehmen sie die laufende Pflege (technisch sowie inhaltlich) des FL-Modells.
Provider Cloud-Service	Hosting für das FL-Modell	Grün	Dieser stellt die Cloud-Umgebung für das FL-Modell zur Verfügung.

Förderge-ber		Orange	Dieser finanziert in Phase 1 das FL-Kompetenzteam.

Im Folgenden wird auf die einzelnen Aspekte des Geschäftsmodells FLUniBwM (Abbildung 36) im Detail eingegangen.

Zielgruppen & Kundennutzen

Als Zielgruppe werden ausgewählte *KMU in Deutschland* gesehen. Im speziellen sollen dabei, aufgrund des Fokus‘ des Forschungsprojektes FLEIS, die Personalabteilungen dieser KMU angesprochen werden, da dort mit personenbezogenen Daten gearbeitet wird.

Als direkten Nutzen können diese Zielgruppen durch die Beteiligung am FL-Modell *KI datenschutzkonform nutzen* und damit die *IT-Sicherheit in den Personalabteilungen direkt erhöhen*.

Da viele KMU an dem FL-Modell beteiligt sind, kann das KI-Modell mit einer größeren Datenbasis trainieren werden, wovon jedes teilnehmende KMU wieder einen direkten Nutzen zieht.

Kundenbeziehung & Kanäle

Die Beziehung zu den Kunden sollte in einer *kollaborativen Strategie* mittels stetiger Kundeninteraktion aufrecht gehalten werden. Der Austausch von Modellaggregationen führt dazu, dass sich der Service wegbewegt von einer Dienstleistung, die vom FL-Anbieter bereitgestellt wird, hinzu einer kooperativen Wertschöpfung. An dieser Dienstleistung sind der FL-Anbieter und die Kunden gleichermaßen beteiligt. Ohne eine geregelte und intensive Kundenbeziehung ist das Geschäftsmodell, welches auf „Co-Creation“ beruht, auf längere Sicht nicht tragbar.

Gleichzeitig spielen in der Kundenbeziehung und -bindung auch *Anreize* eine große Rolle. Denn nur durch die Schaffung und der Vermittlung eines entsprechenden Anreizes wird der Kunde dazu animiert, mit den Datenmustern aus dem trainierten, lokalen Modell das globale Modell zu erweitern. Die Art des Anreizes ist ein wichtiger Faktor, welcher in der Kommunikation mit dem Kunden immer wieder geklärt werden sollte, um eine längerfristige Bindung zu gewährleisten.

Insbesondere für neu hinzugenommene Kunden sollte die lokale Integration des FL-Modells in bestehende Systeme beim Kunden mittels *Support*s unterstützt werden. Dies würde gerade bei kleinen Unternehmen die Hemmschwelle für die Teilnahme am FL-System deutlich senken.

Über den Kanal eines *Online-Portals* sollen sowohl neue Kunden angeworben als auch der Support der bestehenden Kunden organisiert werden. Wahlweise kann der Support für die Kunden auch *persönlich oder telefonisch* erfolgen.

Schlüsselressourcen, -partnerschaften und -aktivitäten

Ein Schwerpunkt des Geschäftsmodells wird in der Ressource *Daten* gesehen, sowohl auf der Seite des FL-Anbieters als auch auf der Kundenseite. Daten stellen die Kernressource eines FL-Modells dar und müssen dementsprechend gepflegt, geprüft und in das Modell eingespeist werden – ohne Daten ist ein FL-System nutzlos. Da die Kunden durch das Training der eigenen, lokalen Modelle und die Aggregation dieser lokalen Modelle in das globale Modell für eine stetige Erweiterung und Verbesserung des FL-Modells sorgen, werden die *Kunden* in diesem Geschäftsmodell nicht nur als Zielgruppe, sondern auch als Schlüsselpartner gesehen („Value Co-Creator"). Weitere Schlüsselpartner sind der *Provider*, welcher die FL-Lösung in einer sicheren Cloud für alle Teilnehmer zur Verfügung stellt, sowie der *Fördergeber*, welcher in der Phase 1 (für Kunden kostenfreie Phase) das FL-Kompetenzteam finanziert.

Als Schlüsselressourcen werden das *Kompetenzteam FL*, das *initiale FL-Modell* (inkl. der initialen Daten), die *Daten der Kunden* sowie das *FL-Modell* (lokal sowie global) gesehen.

Neben den Aktivitäten, die durch den FL-Anbieter übernommen werden (wie *Gewinnung der Kunden*, *Bereitstellung des initialen FL-Modells* sowie *technische Weiterentwicklung* des FL-Modells), wird auch das *lokale Training der Kunden* als Schlüsselaktivität betrachtet. Generieren die Kunden keine lokalen Modelle, die im globalen Modell aggregiert werden können, so ist das Geschäftsmodell gescheitert.

Einnahmequellen

In der Phase 1 (für die Kunden kostenfreie Phase) sollen *Fördergelder* genutzt werden, um das Kompetenzteam FL zu finanzieren. In dieser Phase „bezahlen" die beteiligten Kunden mit ihren Daten, welche mittels des Value Co-Creation-Ansatzes das FL-Modell stetig verbessern. Dieses Prinzip kann für aktive Nutzer (also solche, die ihre Daten in das Globale Modell einpflegen), in der Phase 2 weiter beibehalten werden.

Um das Geschäftsmodell in der Phase 2 zu monetarisieren, kann es um passive Teilnehmer erweitert werden. Diese nutzen das FL-Modell lediglich, ohne eigene Datenmuster einzusteuern, und zahlen nach dem Schema *„Pay per Use"*.

Darüber hinaus kann der *Kundensupport* für (aktive und passive) Kunden angeboten bzw. umgestellt werden – eine Basisversion des Supports (beispielsweise Reaktionszeit innerhalb von 48 Stunden) bleibt weiterhin kostenfrei, ein Premium-Support (schnellere Reaktionszeit bin hin zum Vor-Ort-Support) kann gegen Gebühr dazugebucht werden.

Kostenstruktur

Die Kostenstrukturen setzt sich aus den *Personalkosten* für das FL-Team, die *Sachkosten* für die Wartung des FL-Systems sowie aus den *Gebühren für den Provider* zusammen.

5.3 Zwischenfazit

Im Arbeitspaket 8.1 wurden für die technisch FL-Lösung in FLEIS ein mögliches Geschäftsmodell entwickelt und vorgestellt. Dieses steht als Blaupause der Wissenschaft für weitere Forschung zur Verfügung.

6 Zusammenfassung & Ausblick

Im Rahmen des Projektes FLEIS konnten alle Arbeitspakete abgeschlossen und die darin enthaltenden Forschungsfragen beantwortet werden. Hierfür wurde ein umfangreiches Methodenspektrum genutzt, welches auch den Projektpartnern nähergebracht wurde.

In den ersten Arbeitspaketen (**AP 2.3 und AP 3.1**) wurde primär Vorarbeit für das Design und die Erstellung des technischen FL-Modells der Projektpartner geleistet. Dafür wurde der Ist-Zustand im HRM erhoben und in BPMN- sowie Infrastrukturmodellen dargestellt. Anschließende wurden mögliche Cyberangriffe erarbeitet und in Attack-Trees skizziert. Abschließend wurden die Anforderungen seitens der Nutzer (Data Owner) an eine mögliche Integration eines FL-Systems erhoben und in Anforderungskatalogen festgehalten.

In dem nachfolgenden **AP 8.1** wurden auf Grundlage des technischen FL-Designs von Trevisto und itWatch das Geschäftsmodell FLEIS4Bayern ausgearbeitet, welches den Partnern zur Verfügung gestellt werden konnte. Zusätzlich wurde ein zweites Geschäftsmodell FLUniBwM skizziert, welches die Ergebnisse aus den vorherigen Recherchen und Workshops aufgreift und ein kollaboratives Geschäftsmodell für einen FL-Service darstellt.

Das **AP 8.2** kann als zusätzliches Ergebnis betrachtet werden, welches durch die Entwicklung des *HRM-Defenders* in Form eines Serious Games die Möglichkeit bietet, die technische FL-Lösung durch eine personelle Maßnahme zu unterstützen.

Insgesamt bietet das Themenfeld IT-Sicherheit im HRM viel Potenzial für weitere Forschungsarbeiten. Basierend auf den Ergebnissen aus AP 2.3 könnten Prozessoptimierungen durch Modelle der Visionsentwicklung und Soll-Strukturen erfolgen. Die entwickelten Attack-Trees könnten durch technische Untersuchungen im Hinblick auf Cyberangriffe verfeinert und erweitert werden. Die Anforderungskataloge aus AP 3.1 und die Geschäftsmodelle aus AP 8.1 könnten in einer Taxonomie vereint werden, um die Kommunikation zwischen Anbietern und Nutzern zu verbessern und Design-Anforderungen für einen FL-Service einheitlich darzustellen. Dies würde insbesondere Startups den Einstieg in die Entwicklung eines FL-Service erleichtern. Das in AP 8.2 dargestellte Serious Game könnte in weiteren Spielphasen weiterentwickelt und um neue Spielvarianten ergänzt werden.

7 Danksagung

Wir danken dem Bayerischen Staatsministerium für Wirtschaft, Landesentwicklung und Energie für die Möglichkeit der Forschung im Rahmen des FuE-Programms IuK des Freistaates Bayern (Förderkennzeichen DIK-2104-0082/DIK0242/03).

Den Projektpartnern Trevisto und itWatch danken wir für die gute Zusammenarbeit.

Abschließend danken wir allen beteiligten Studierenden, die durch ihre Arbeiten das Projekt unterstützt haben, sowie Prof. Dr. Ulrike Lechner, die diese Forschung am Institut für Schutz und Zuverlässigkeit (Inf8) ermöglichte.

8 Literatur

Alter, S. (2001). Which Life Cycle—Work System, Information System, or Software? *Communications of the Association for Information Systems*, *7*(1).

BPM Offensive Berlin (Hrsg.). (o. J.). *BPMN 2.0—Business Process Model and Notation*. Abgerufen 28. März 2022, von http://www.bpmb.de/index.php/BPMNPoster

BSI (Hrsg.). (2018). *Industrial Control System Security: Innentäter v2.0*. Bundesamt für Sicherheit in der Informationstechnik. https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_061.html

Bundesamt für Sicherheit in der Informationstechnik – BSI (Hrsg.). (2017). *Leitfaden zur Basis-Absicherung nach IT-Grundschutz: In drei Schritten zur Informationssicherheit*. https://www.bsi.bund.de/dok/10051454

Camajori Tedeschini, B., Savazzi, S., Stoklasa, R., Barbieri, L., Stathopoulos, I., Nicoli, M., & Serio, L. (2022). Decentralized Federated Learning for Healthcare Networks: A Case Study on Tumor Segmentation. *IEEE Access*, *10*, 8693–8708.

Clearswift. (2015, August 3). New Research Reveals Finance and Human Resource Departments Believed to Pose Biggest Security Risk to Organizations. *Business Wire*.

Da Veiga, A. (2018). An Approach to Information Security Culture Change Combining ADKAR and the ISCA Questionnaire to aid Transition to the Desired Culture. *Information and Computer Security*, *26*(5), 584–612.

Döring, N., & Bortz, J. (2016). *Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften* (5. Auflage). Springer Berlin Heidelberg.

Erickson, E. (2018). Data Security for HR. *Credit Union Management*, *41*(11), 30–32.

European Union Agency for Cybersecurity ENISA (Hrsg.). (2022). *ENISA Threat Landscape 2022*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Fleischmann, A., Oppl, S., Schmidt, W., & Stary, C. (2018). *Ganzheitliche Digitalisierung von Prozessen*. Springer Vieweg.

Fliegen, I. (2020). *Crashkurs Recruiting: Personalbeschaffung und -auswahl.* Haufe.

Freund, J., & Rücker, B. (2019). *Praxishandbuch BPMN* (6. Auflage). Hanser.

Frintrup, A., & Piechowski, S. (2011). Effiziente Prozesse der Mitarbeiterrekrutierung. *Industrie Management*, *27*(4), 19–22.

Glaser, B. G., & Strauss, A. L. (2017). *The discovery of grounded theory: Strategies for qualitative research*. Routledge.

Grohmann, A., & Kauffeld, S. (2013). Evaluating Training Programs: Development and Correlates of the Questionnaire for Professional Training Evaluation. *International Journal of Training and Development*, *17*(2), 135–155.

Habibullah, M. K., & Horkoff, J. (2021). Non-functional requirements for machine learning: Understanding current use and challenges in industry. *2021 IEEE 29th International*

Requirements Engineering Conference (RE), 13–23.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2022). Riskio: A Serious Game for Cyber Security Awareness and Education. *Computer & Security*, *95*(101827).

Hartmann, R. (2015). Rekrutierung im Mittelstand: Trends und Herausforderungen im Personalmanagement oder von Trüffelschweinen und Wollmilchsäuen. In *Hartmann, Michaela (Hrsg.): Rekrutierung in einer zukunftsorientierten Arbeitswelt: HR-Aufgaben optimal vernetzen* (S. 215–234). Springer Gabler.

Hoffmeister, C. (2022). *Digital Business Modelling: Digitale Geschäftsmodelle verstehen, designen, bewerten* (3. Auflage). Hanser.

Holm, A. B. (2012). E-Recruiting: Auf dem Weg zu einem ubiquitären Rekrutierungsprozess und integriertem Bewerber-Beziehungsmanagement. *Zeitschrift für Personalforschung*, *26*(3), 241–260.

Horkoff, J. (2019). Non-Functional Requirements for Machine Learning: Challenges and New Directions. *IEEE 27th International Requirements Engineering Conference (RE)*, 386–391.

Jäger, W. (2012). Die Königsdisziplin im Umschwung. *Personalmagazin*, *3/2012*, 30–31.

Kauffeld, S. (2016). *Nachhaltige Personalentwicklung und Weiterbildung: Betriebliche Seminare und Trainings Entwickeln, Erfolge Messen, Transfer Sichern* (2. Auflage). Springer.

Kuckartz, U. (2018). *Qualitative Inhaltsanalyse: Methoden, Praxis, Computerunterstützung* (4. Auflage). Beltz Juventa.

Kuckartz, U., & Rädiker, S. (2022). *Qualitative Inhaltsanalyse: Methoden, Praxis, Computerunterstützung* (5. Auflage). Beltz Juventa.

Lamnek, S., & Krell, C. (2016). *Qualitative Sozialforschung* (6. Auflage). Beltz Verlag.

McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Aguera y Arcas, B. (2016). Communication-Efficient Learning of Deep Networks from Decentralized Data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, *54*, 1273–1282.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, *42*(1), 285–311.

Muenstermann, B., von Stetten, A., Laumer, S., & Eckhardt, A. (2010). The performance impact of business process standardization: HR case study insights. *Management Research Review*, *33*(9), 924–939.

Osterwalder, A. (2004). *The Business Model Ontology: A Proposition in a Design Science Approach* [Disseration]. Université de Lausanne.

Osterwalder, A., & Pigneur, Y. (2011). *Business Model Generation: Ein Handbuch für Visionäre, Spielveränderer und Herausforderer*. Campus Verlag.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, *66*(5), 40–51.

Petry, T., & Jäger, W. (Hrsg.). (2021). *Digital HR : smarte und agile Systeme, Prozesse und Strukturen im Personalmanagement* (2. Auflage). Haufe.

Reitgruber, J. (2017). *IT-Systeme im Personalmanagement* [Masterarbeit]. https://pub.fh-campuswien.ac.at/urn:nbn:at:at-fhcw:1-573

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4).

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science*, *2*(3), article number 173.

Satter, M. Y. (2017). 8 Steps to Protect Employee Benefits Data from Hackers. *BenefitsPRO*, *09*, o.S.

Schneier, B. (1999). Attack trees. *Dr. Dobb's journal*, *24*(12), 21–29.

Scholz, C., & Scholz, T. M. (2019). *Grundzüge des Personalmanagements* (3. Auflage). Vahlen.

Schwarz, L. (2022). *IT-Sicherheit im Human Resources Management in deutschen Unternehmen – eine quantitative Studie* [Masterarbeit].

Steinle, N. (2023). *Kompetenzaufbau Cybersecurity in Personalabteilungen: Konzeptionierung, Durchführung und Validierung eines Trainings* [Masterarbeit].

Steinle, N. (2024). *Weiterentwicklung des Trainings HRM Defender – The Cybersecurity Card Game zum Kompetenzaufbau von Cybersecurity in Personalabteilungen* [Ausarbeitung].

Strohm, O. & Ulich, E. (1997). *Unternehmen arbeitspsychologisch bewerten. Ein Mehr-Ebenen-Ansatz unter besonderer Berücksichtigung von Mensch, Technik, Organisation.* vdf Hochschulverlag.

Strohmeier, S. (2008). *Informationssysteme im Personalmanagement: Architektur, Funktionalität, Anwendung*. Vieweg + Teubner.

Techam, L. (2022). *IT-Sicherheit im Recruiting: Anforderungsanalyse aus der Anwenderperspektive anhand einer qualitativen Studie* [Masterarbeit].

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., & Bailey, M. (2016). Users Really Do Plug in USB Drives They Find. *2016 IEEE Symposium on Security and Privacy (SP)*, 306–319.

Ullah, R., & Witt, M. (2018). *Praxishandbuch Recruiting: Grundlagenwissen—Prozess-Know-how – Social Recruiting* (2. Auflage). Schäffer-Pöschl.

Verhoeven, T. (Hrsg.). (2020). *Digitalisierung im Recruiting: Wie sich Recruiting durch künstliche Intelligenz, Algorithmen und Bots verändert*. Springer Fachmedien.

Vogelsang, A., & Borg, M. (2019). Requirements engineering for machine learning: Perspectives from data scientists. *2019 IEEE 27th International Requirements Engineering Conference Workshops (REW)*, 245–251.

Wagner, K. W., & Patzak, G. (2020). *Performance Excellence—Der Praxisleitfaden zum effektiven Prozessmanagement*. Hanser.

Yasin, A., Liu, L., Li, T., Fatima, R., & Jianmin, W. (2019). Improving software security awareness using a serious game. *IET Software*, *13*(2), 159–169.

9 Anhang

A. Modelle E-Mail und ATS (AP 2.1)

B. Attack Trees interner Workshop (AP 2.1)

C. Attack Trees externer Workshop (AP 2.1)

D. Fragebogen Umfrage IT-Sicherheit HRM (AP 8.2)

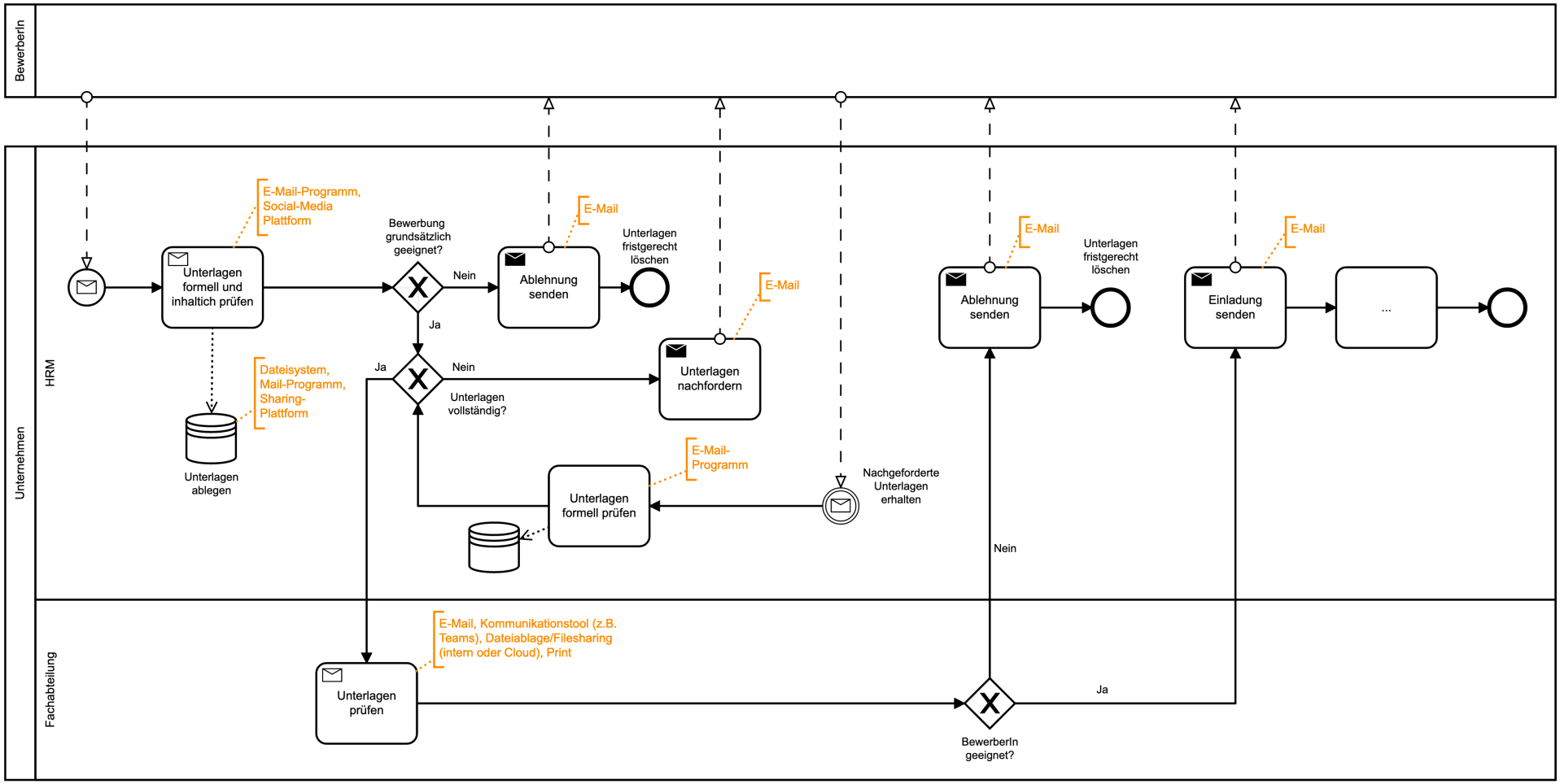
E. Grafiken Umfrage IT-Sicherheit HRM (AP 8.2)

F. Liste der analysierten HRM-Startups (AP 8.1)

G. BMC’s zu Geschäftsmodellen (AP 8.1)

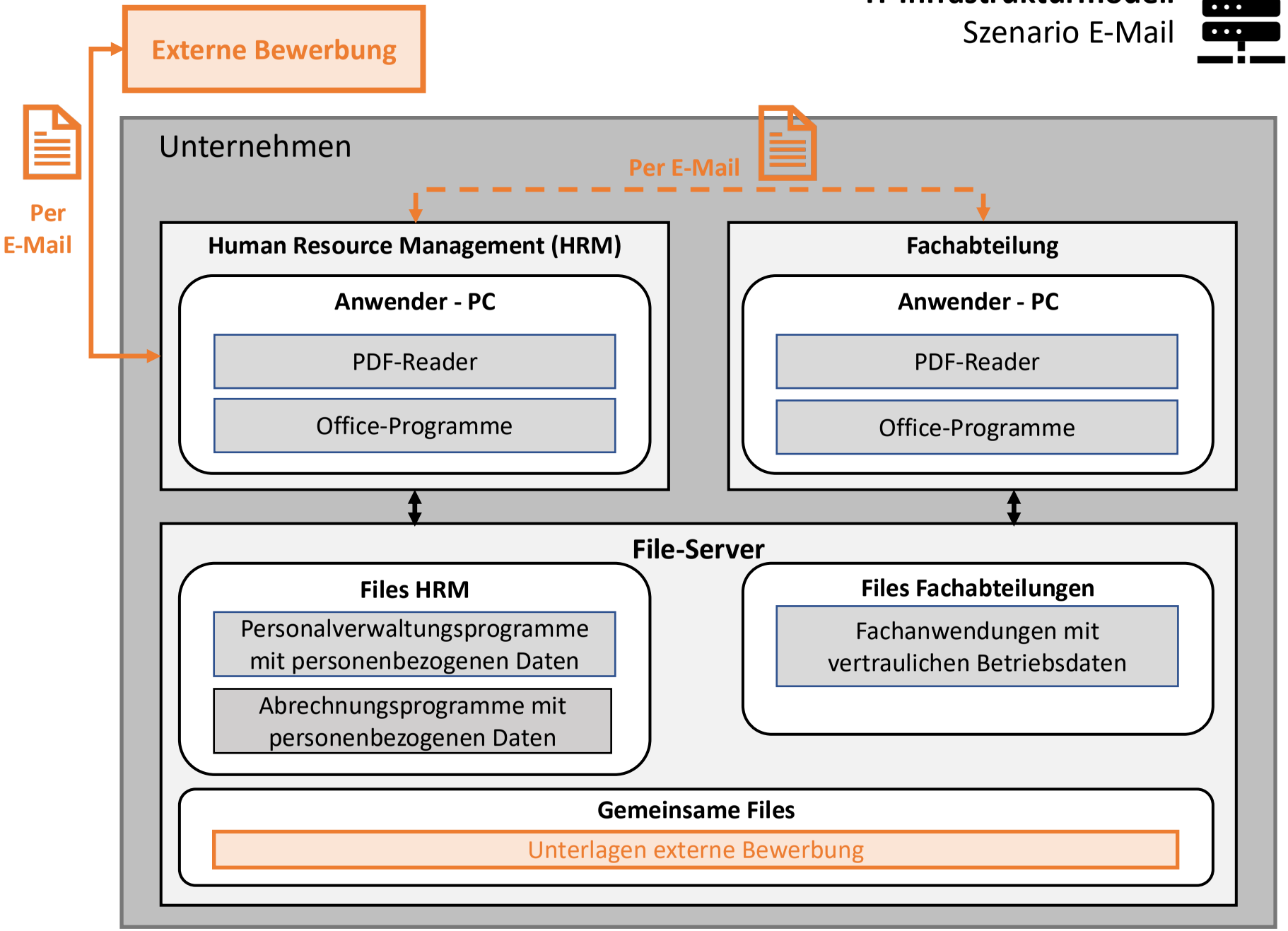
A

Prozessmodell
Szenario E-Mail

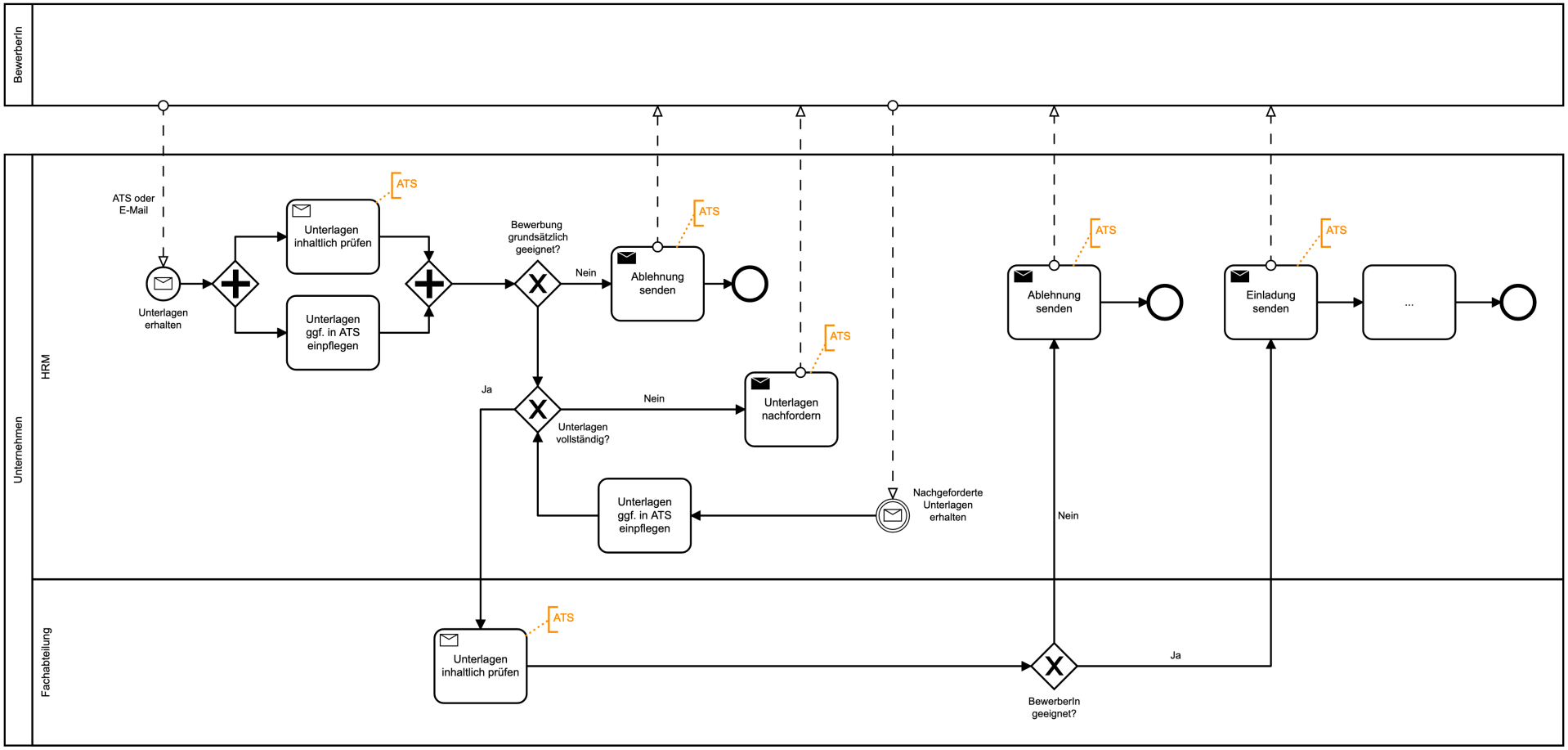


Version 1.0

IT-Infrastrukturmodell
Szenario E-Mail

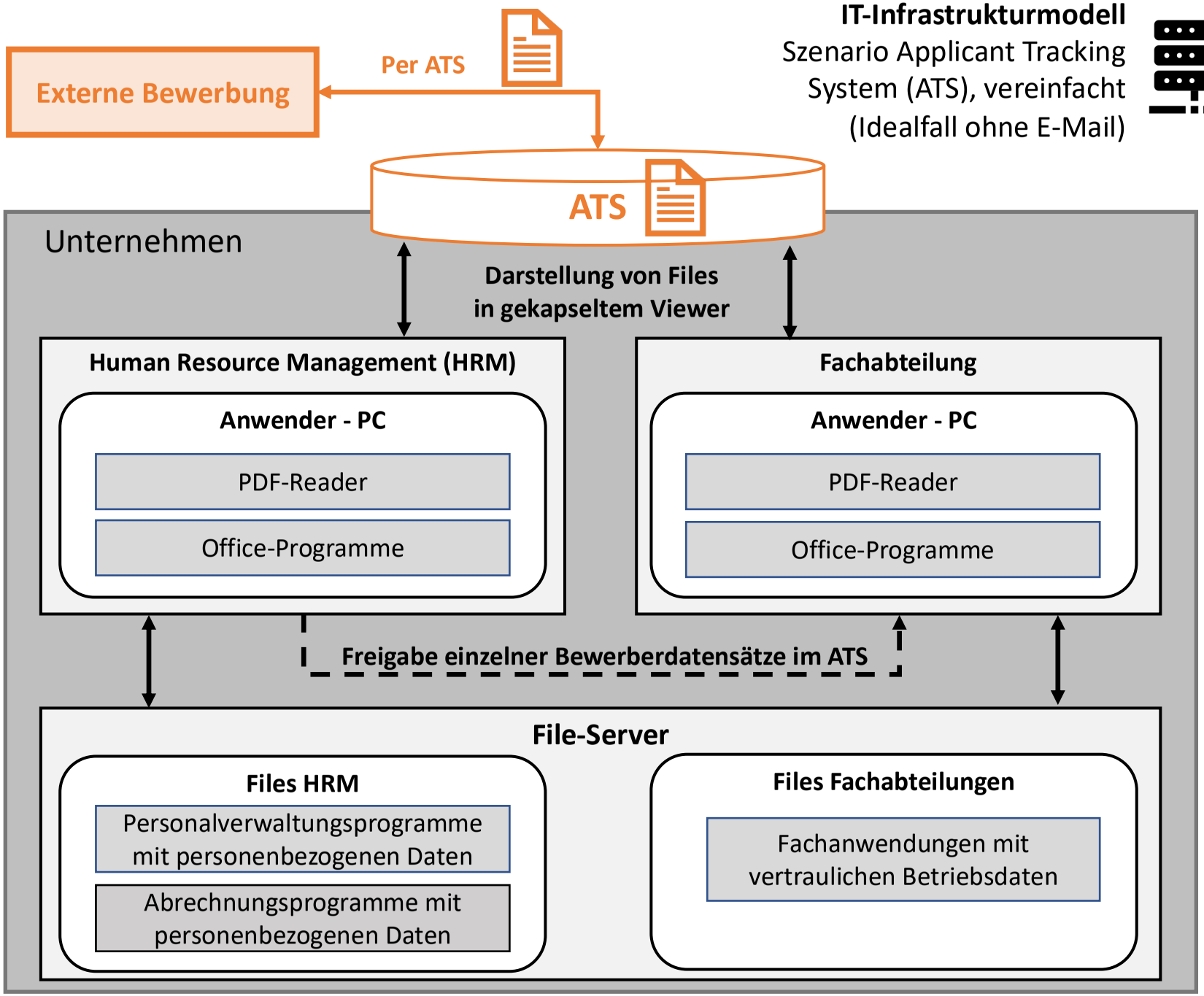


Prozessmodell
Szenario Applicant Tracking System (ATS)



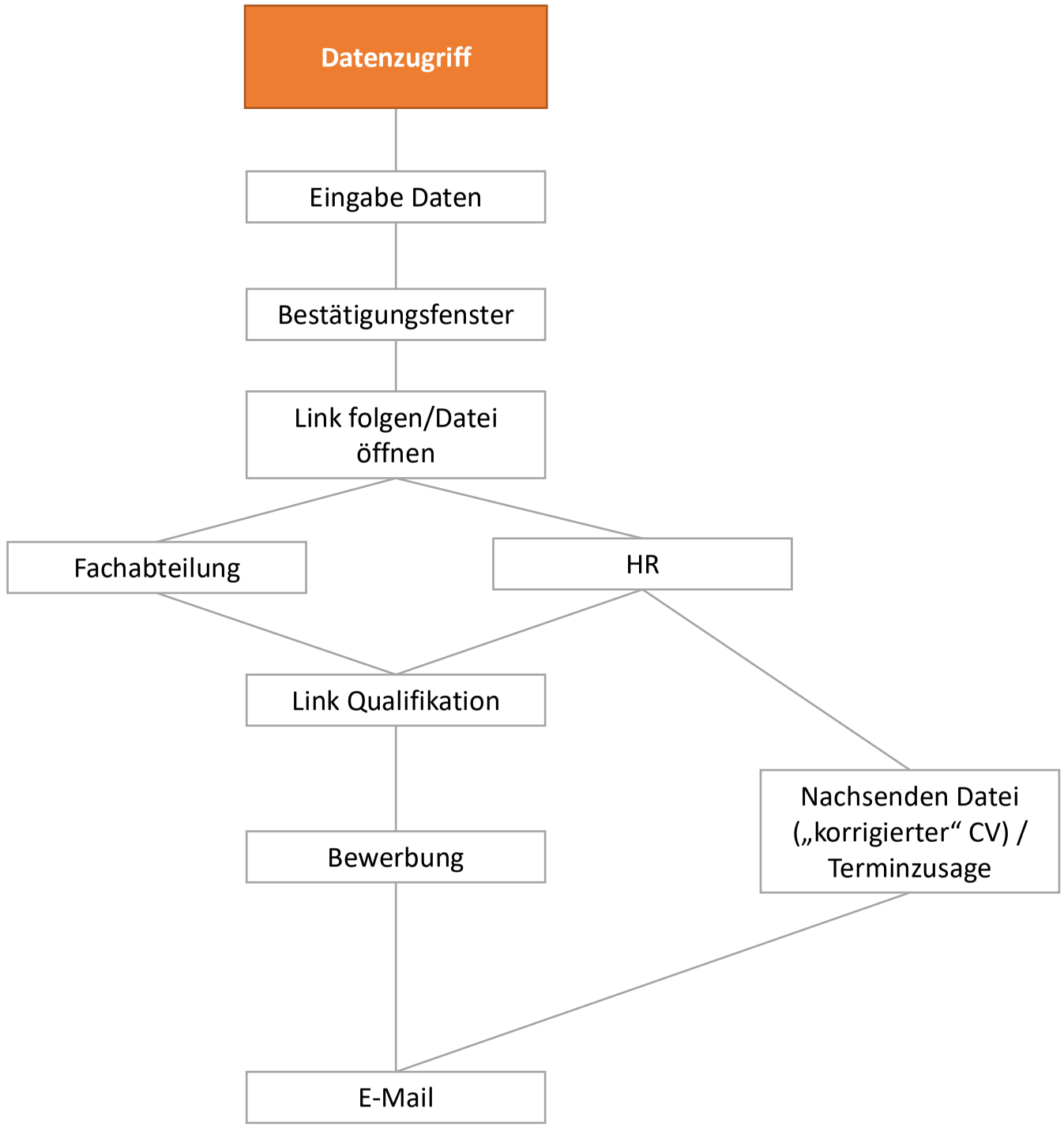
Version 1.0

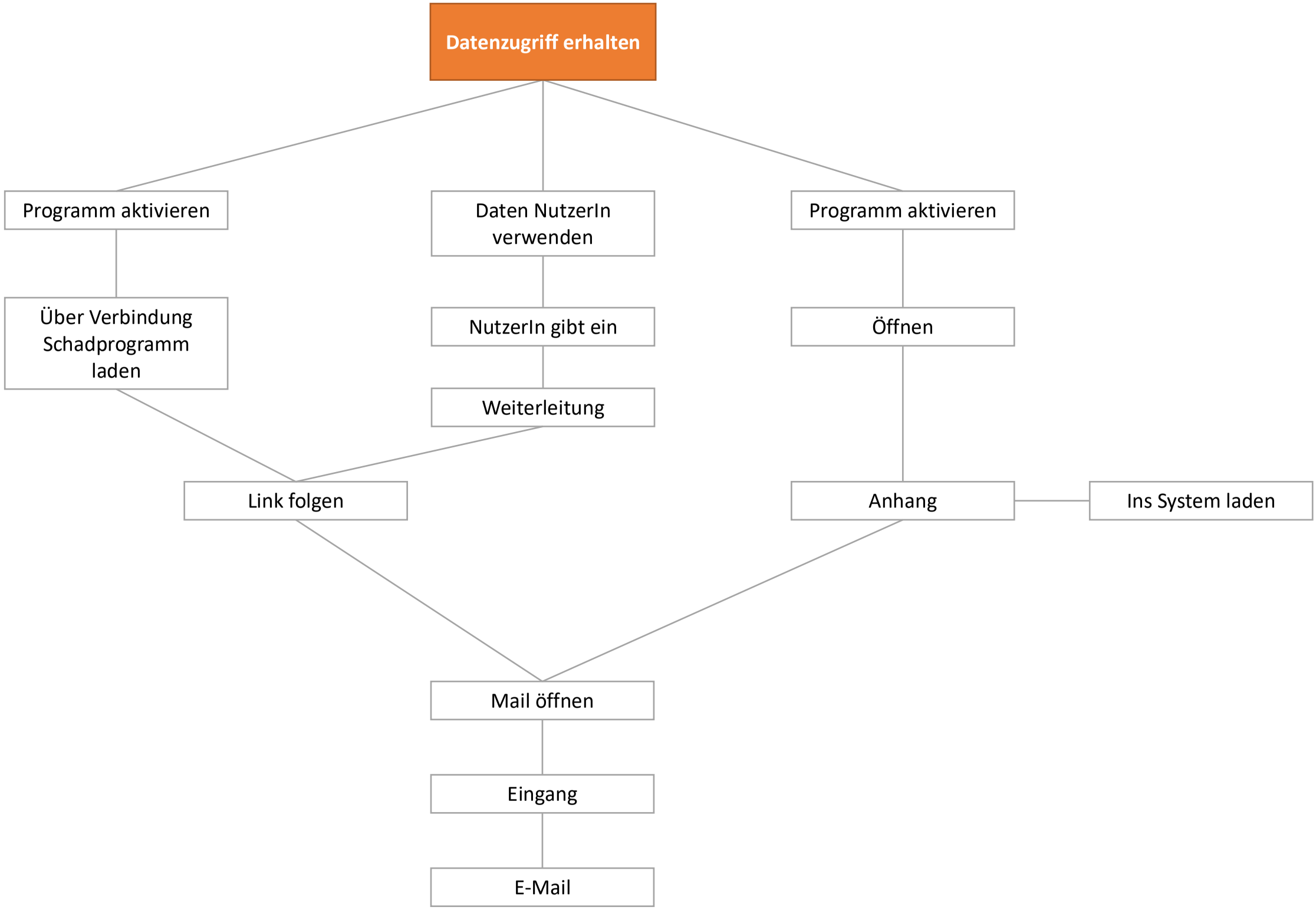
IT-Infrastrukturmodell
Szenario Applicant Tracking System (ATS), vereinfacht (Idealfall ohne E-Mail)



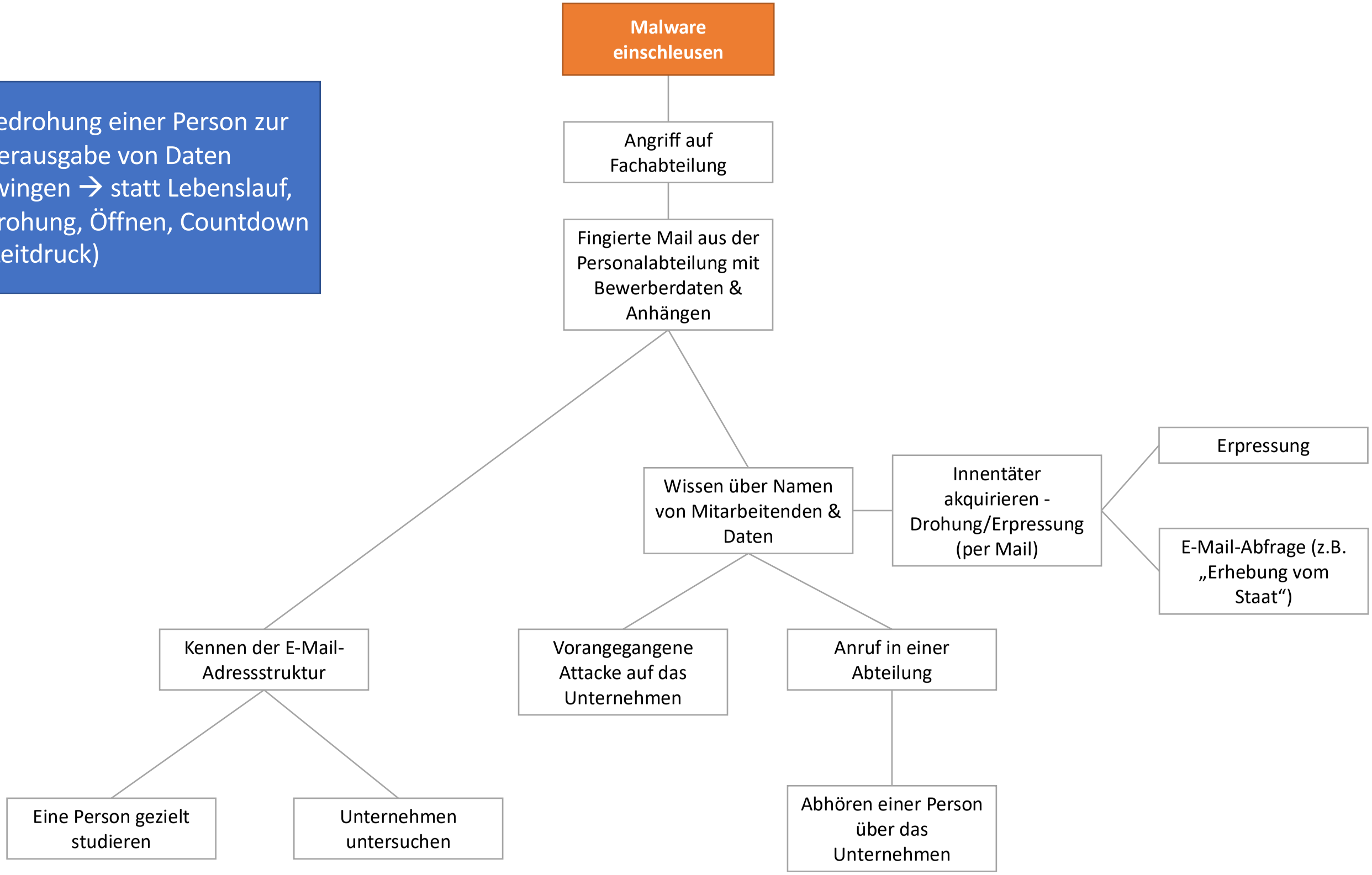
B

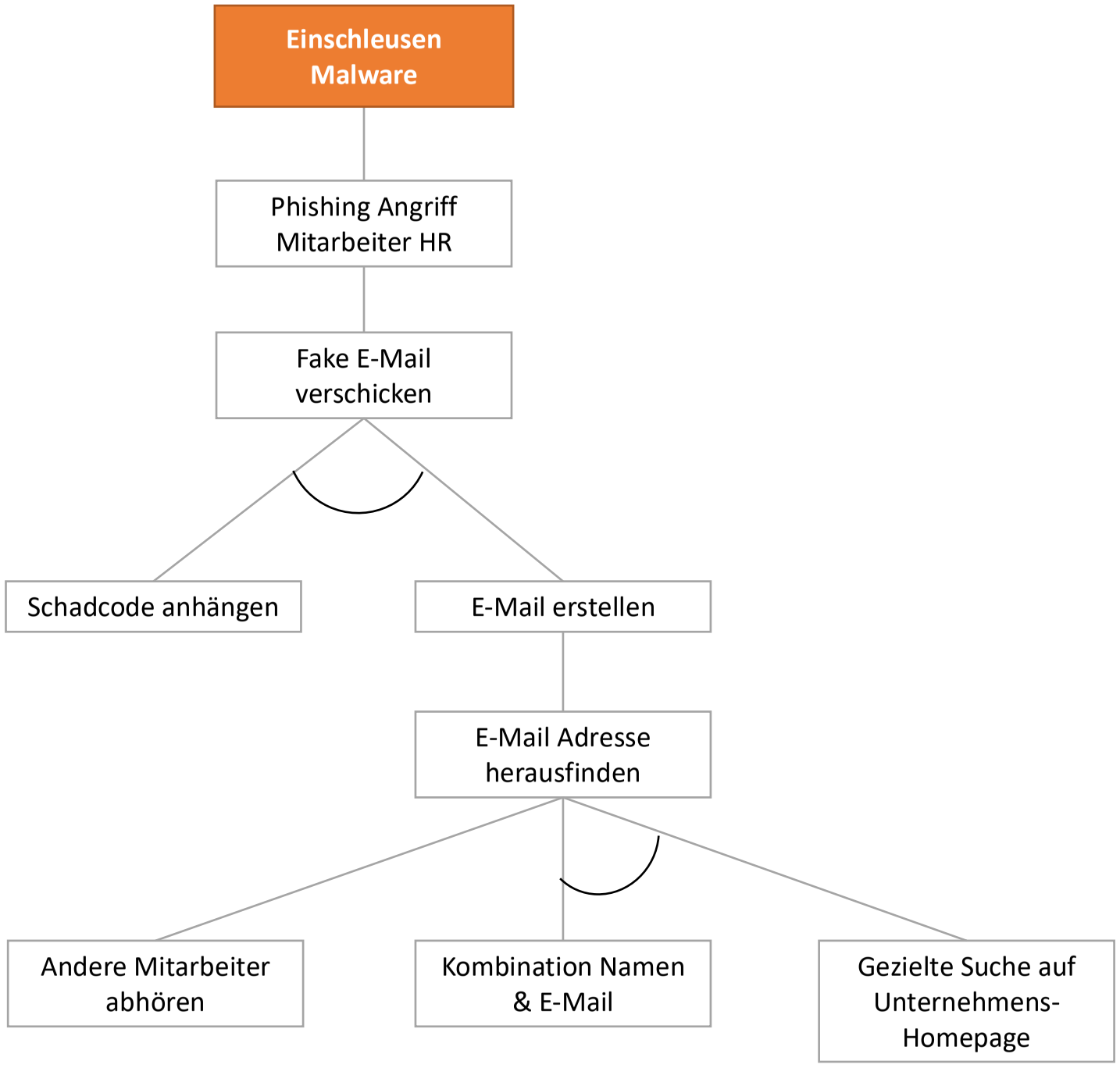
E-Mail

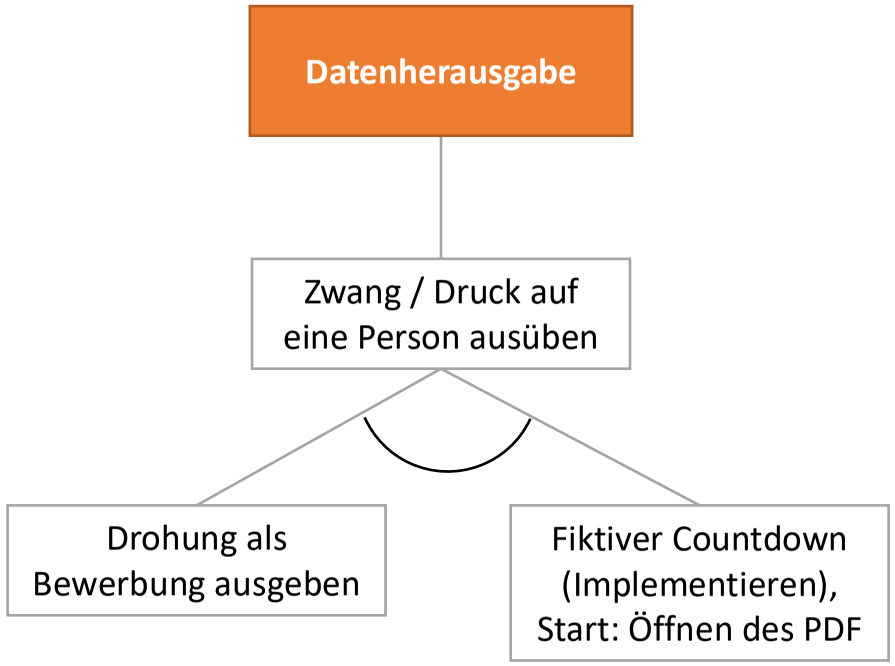

Datenzugriff
Eingabe Daten
Bestätigungsfenster
Link folgen/Datei öffnen
Fachabteilung
HR
Link Qualifikation
Bewerbung
Nachsenden Datei („korrigierter“ CV) / Terminzusage
E-Mail

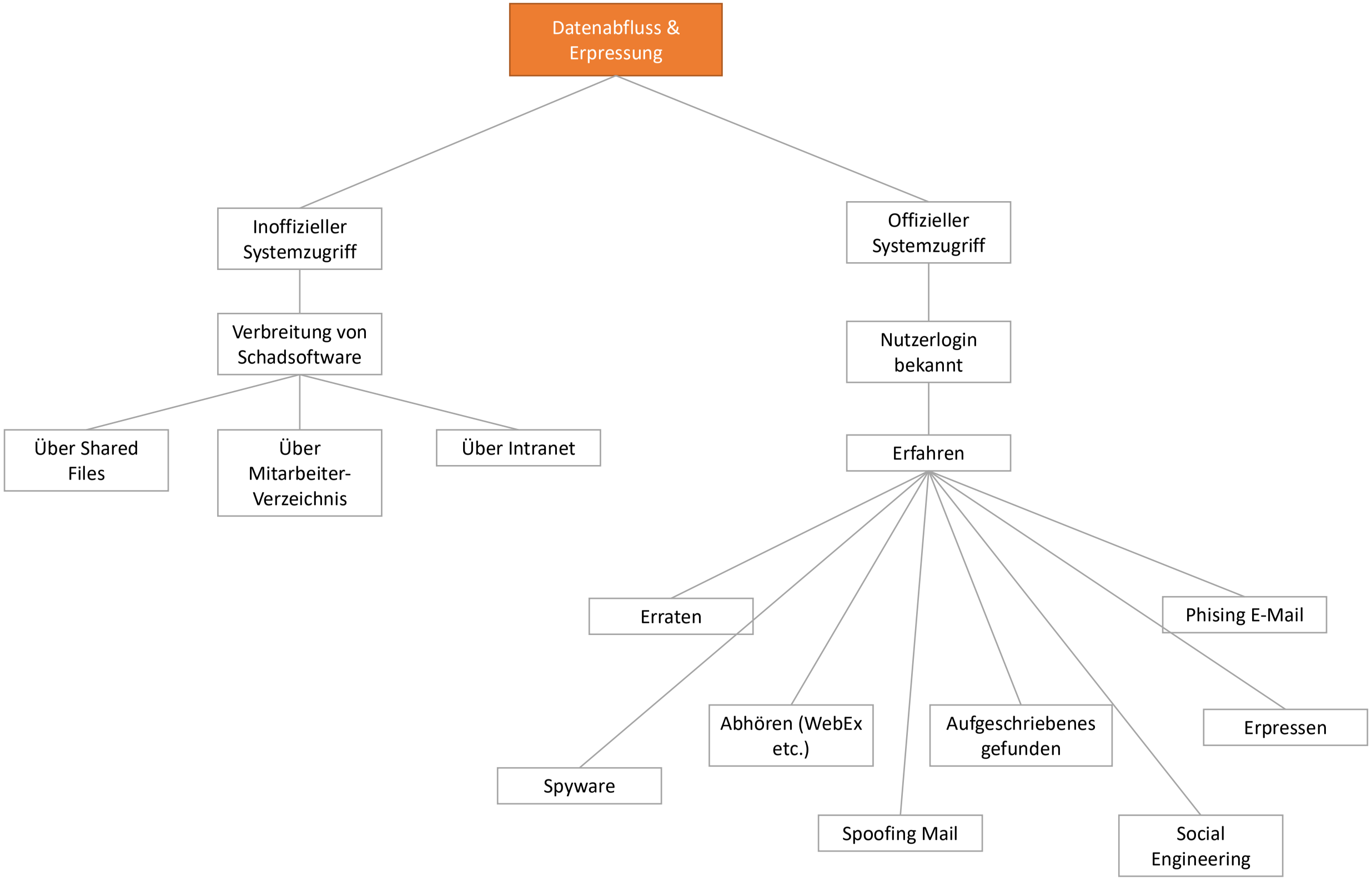

Datenzugriff erhalten
Programm aktivieren
Daten NutzerIn verwenden
Programm aktivieren
Über Verbindung Schadprogramm laden
NutzerIn gibt ein
Öffnen
Weiterleitung
Link folgen
Anhang
Ins System laden
Mail öffnen
Eingang
E-Mail

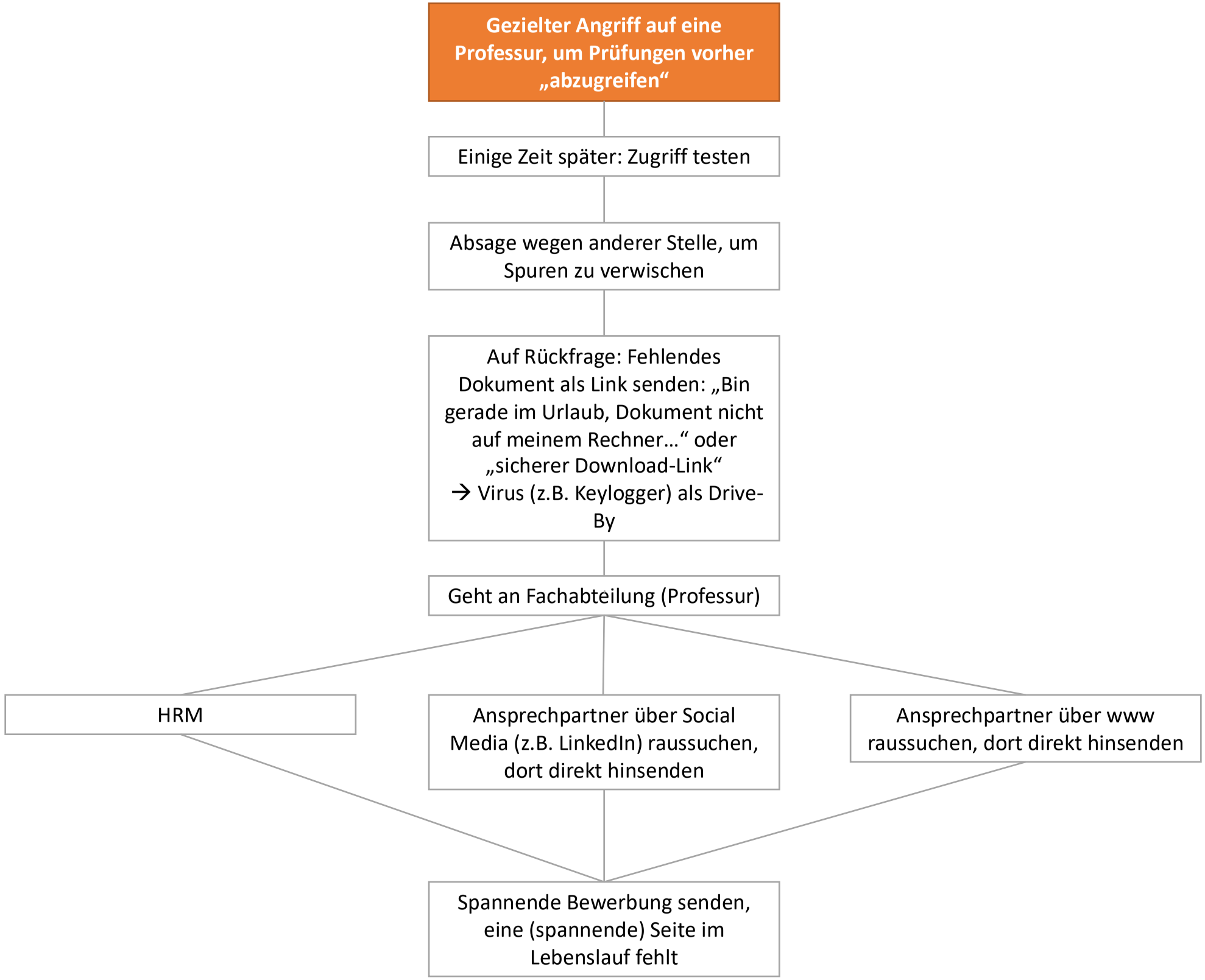
Bedrohung einer Person zur Herausgabe von Daten zwingen → statt Lebenslauf, Drohung, Öffnen, Countdown (Zeitdruck)

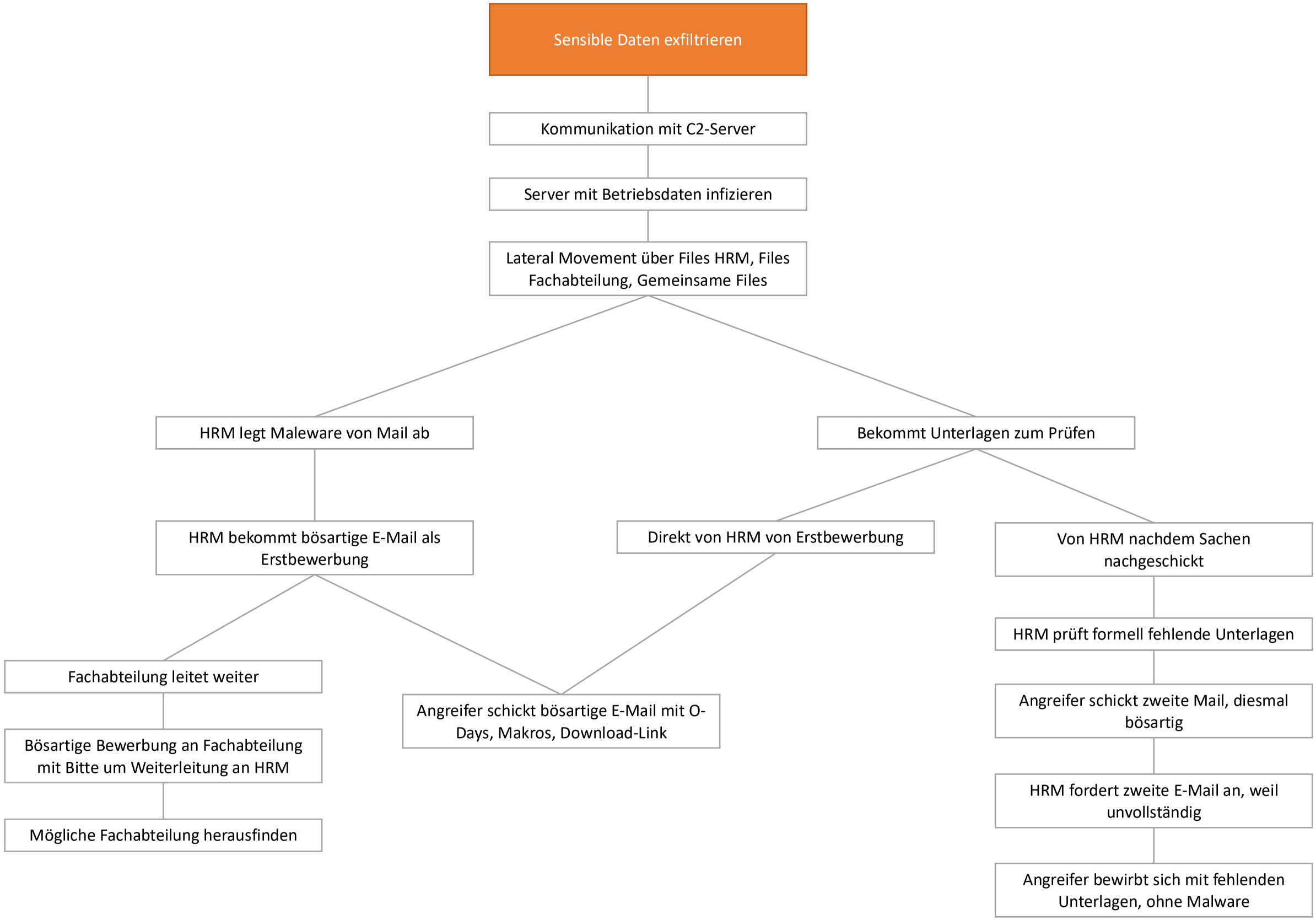



Einschleusen Malware
Phishing Angriff Mitarbeiter HR
Fake E-Mail verschicken
Schadcode anhängen
E-Mail erstellen
E-Mail Adresse herausfinden
Andere Mitarbeiter abhören
Kombination Namen & E-Mail
Gezielte Suche auf Unternehmens-Homepage


Datenherausgabe
Zwang / Druck auf eine Person ausüben
Drohung als Bewerbung ausgeben
Fiktiver Countdown (Implementieren), Start: Öffnen des PDF


Datenabfluss & Erpressung
Inoffizieller Systemzugriff
Offizieller Systemzugriff
Verbreitung von Schadsoftware
Nutzerlogin bekannt
Über Shared Files
Über Mitarbeiter-Verzeichnis
Über Intranet
Erfahren
Erraten
Phising E-Mail
Abhören (WebEx etc.)
Aufgeschriebenes gefunden
Erpressen
Spyware
Spoofing Mail
Social Engineering


Gezielter Angriff auf eine Professur, um Prüfungen vorher „abzugreifen“
Einige Zeit später: Zugriff testen
Absage wegen anderer Stelle, um Spuren zu verwischen
Auf Rückfrage: Fehlendes Dokument als Link senden: „Bin gerade im Urlaub, Dokument nicht auf meinem Rechner…“ oder „sicherer Download-Link“
→ Virus (z.B. Keylogger) als Drive-By
Geht an Fachabteilung (Professur)
HRM
Ansprechpartner über Social Media (z.B. LinkedIn) raussuchen, dort direkt hinsenden
Ansprechpartner über www raussuchen, dort direkt hinsenden
Spannende Bewerbung senden, eine (spannende) Seite im Lebenslauf fehlt


Sensible Daten exfiltrieren
Kommunikation mit C2-Server
Server mit Betriebsdaten infizieren
Lateral Movement über Files HRM, Files Fachabteilung, Gemeinsame Files
HRM legt Maleware von Mail ab
Bekommt Unterlagen zum Prüfen
HRM bekommt bösartige E-Mail als Erstbewerbung
Direkt von HRM von Erstbewerbung
Von HRM nachdem Sachen nachgeschickt
HRM prüft formell fehlende Unterlagen
Angreifer schickt zweite Mail, diesmal bösartig
HRM fordert zweite E-Mail an, weil unvollständig
Angreifer bewirbt sich mit fehlenden Unterlagen, ohne Malware
Fachabteilung leitet weiter
Bösartige Bewerbung an Fachabteilung mit Bitte um Weiterleitung an HRM
Mögliche Fachabteilung herausfinden
Angreifer schickt bösartige E-Mail mit O-Days, Makros, Download-Link

Angreifer: Auftrag durch staatl. Industrieunternehmen eines anderen Staates

OSINT: Open Source Intelligence
= Sammeln & Verknüpfen von Informationen aus frei zugänglichen Quellen
HRM: Human Resource Management

Vertrauliche Betriebsdaten erbeuten

Skript lädt in Hintergrund über Tage hinweg Dateien aus Netzlaufwerken und Spaces auf einen Server hoch (neu – alt)

Makro platziert Skript auf dem PC eines Mitarbeiters in der Fachabteilung

Fachabteilung öffnet Excel-Datei mit Makro

Fachabteilung liest Bewerbung mit Hinweis auf Forschungsdaten

HRM akzeptiert Bewerbung und leitet sie an die Fachabteilung weiter

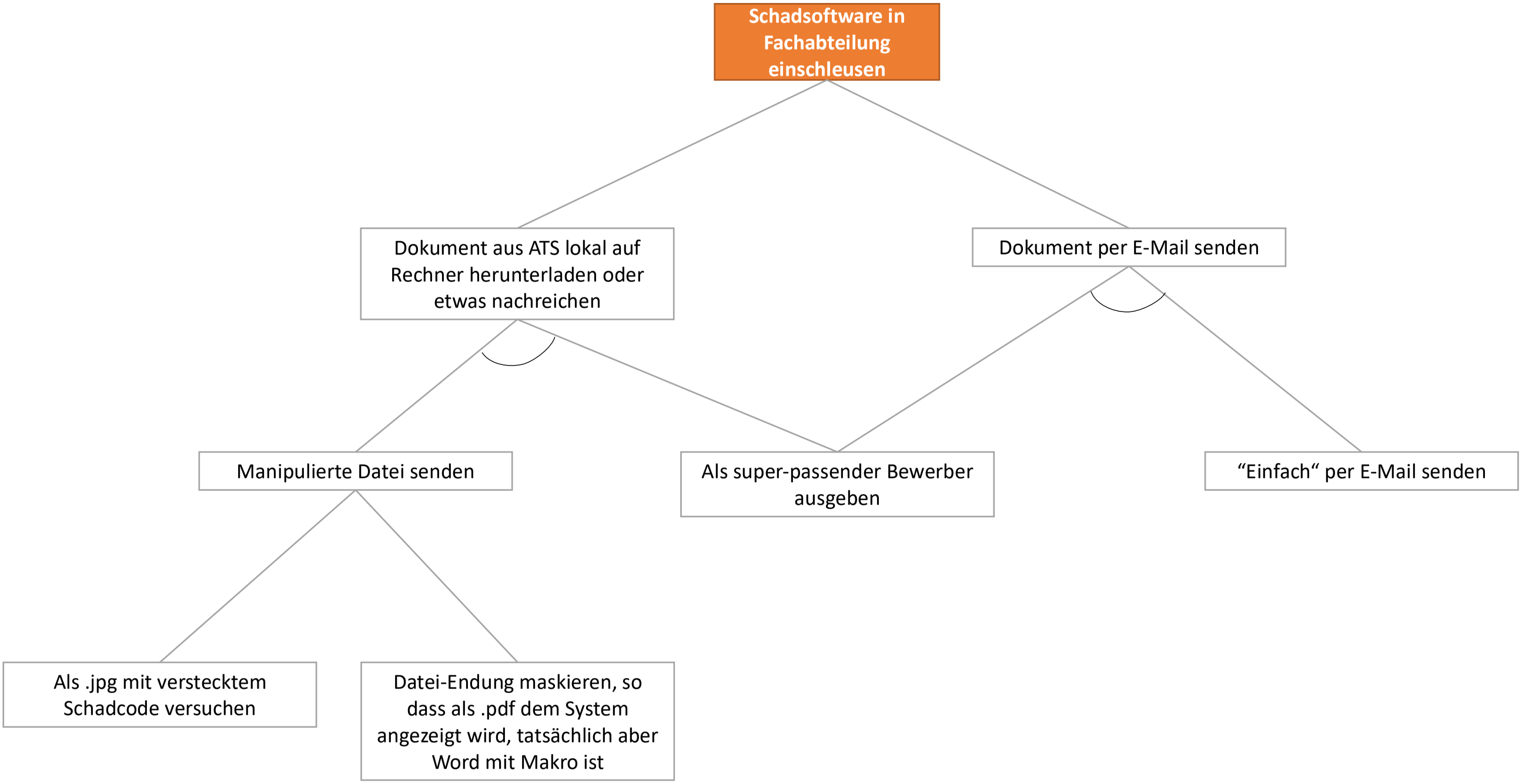
Verfassen einer Bewerbung mit guten Qualifikationen (gefälscht), an die auch als Beleg ein vermeintlicher Forschungs-Datensatz aus der Dissertation in Form eines XLSM-Dokuments angehängt ist

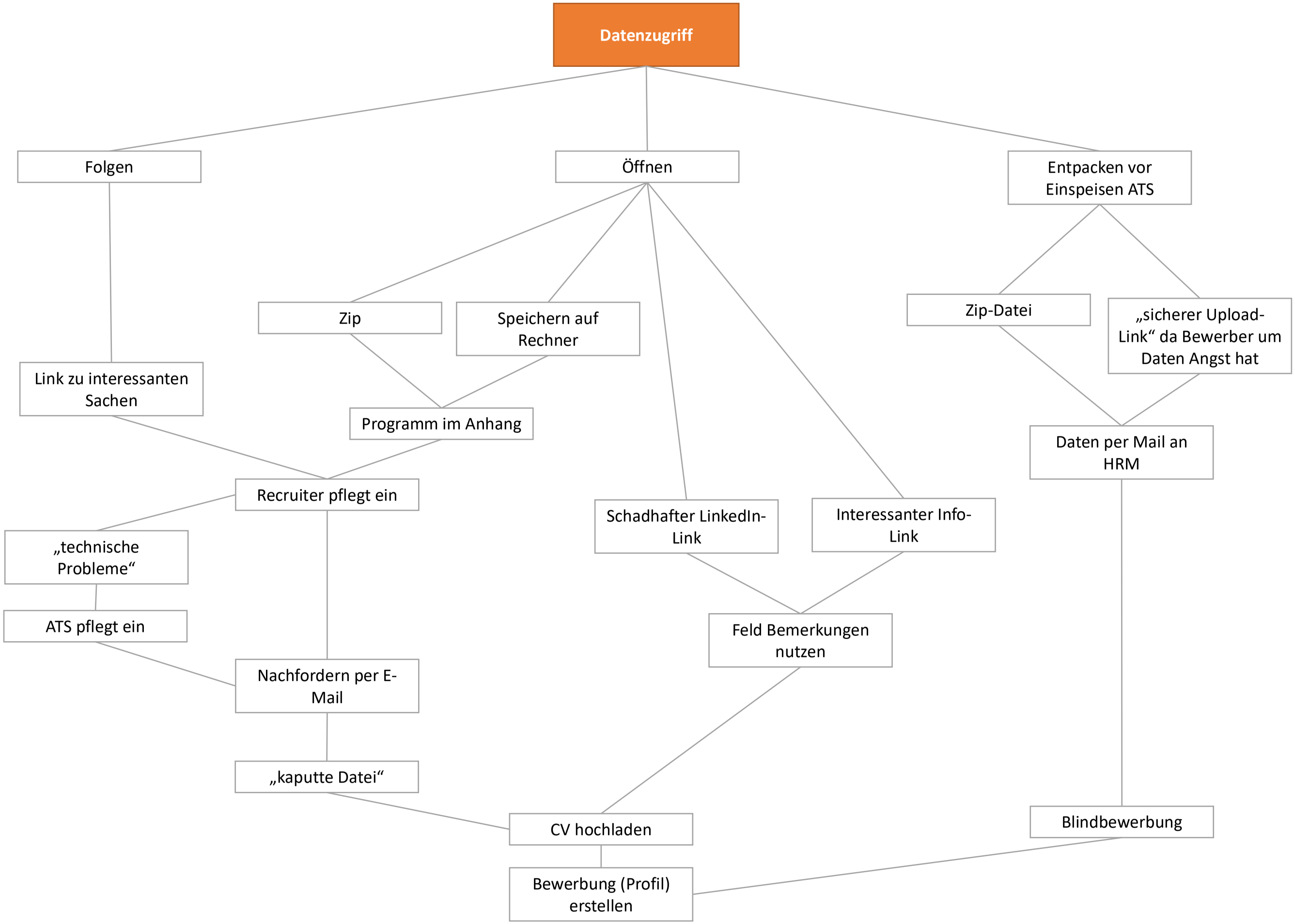
Fälschen von Zeugnissen und Zertifikation unter Inpersonifikation der Person

OSINT: Recherchieren einer echten Person, die für die Stelle in Frage käme

OSINT: Requirements für Bewerbung in der Organisation

ATS


Schadsoftware in Fachabteilung einschleusen
Dokument aus ATS lokal auf Rechner herunterladen oder etwas nachreichen
Dokument per E-Mail senden
Manipulierte Datei senden
Als super-passender Bewerber ausgeben
“Einfach“ per E-Mail senden
Als .jpg mit verstecktem Schadcode versuchen
Datei-Endung maskieren, so dass als .pdf dem System angezeigt wird, tatsächlich aber Word mit Makro ist


Datenzugriff
Folgen
Öffnen
Entpacken vor Einspeisen ATS
Zip
Speichern auf Rechner
Zip-Datei
„sicherer Upload-Link“ da Bewerber um Daten Angst hat
Link zu interessanten Sachen
Programm im Anhang
Daten per Mail an HRM
Recruiter pflegt ein
Schadhafter LinkedIn-Link
Interessanter Info-Link
„technische Probleme“
ATS pflegt ein
Feld Bemerkungen nutzen
Nachfordern per E-Mail
„kaputte Datei“
CV hochladen
Blindbewerbung
Bewerbung (Profil) erstellen

Raub der Zugangsdaten zum ATS
Raub der Zugangsdaten
Eingabe Daten
Öffnen der Webseite durch HR
Erläuterung der Nutzung von VPN → Installationstool o. Webseiten-Link
Ankündigungs-Mail über absofortige Nutzung des VPN
Erstellung VPN-Webpage

Abgreifen Passwort / Zugriffsdaten für ATS

Bewerbung geht ins ATS (mit Schadsoftware)

Schadsoftware, die auf der Seite platziert wird mit gezogen

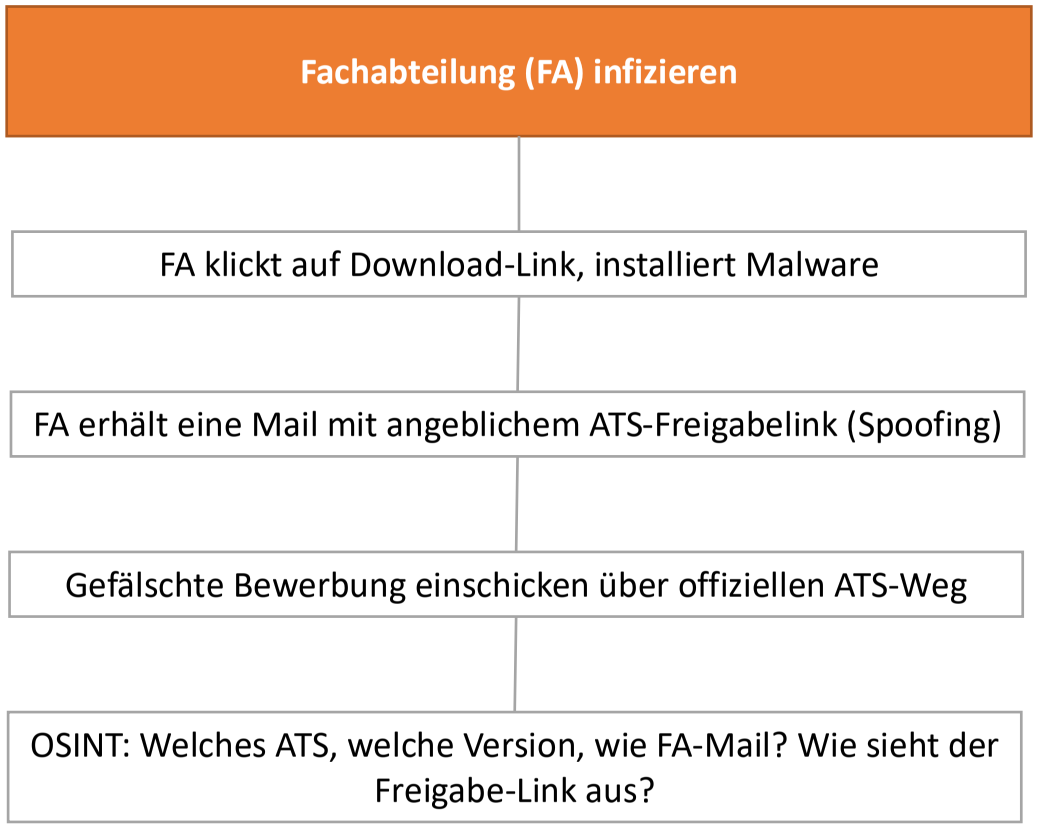
Abruf der Unterlagen durch HR

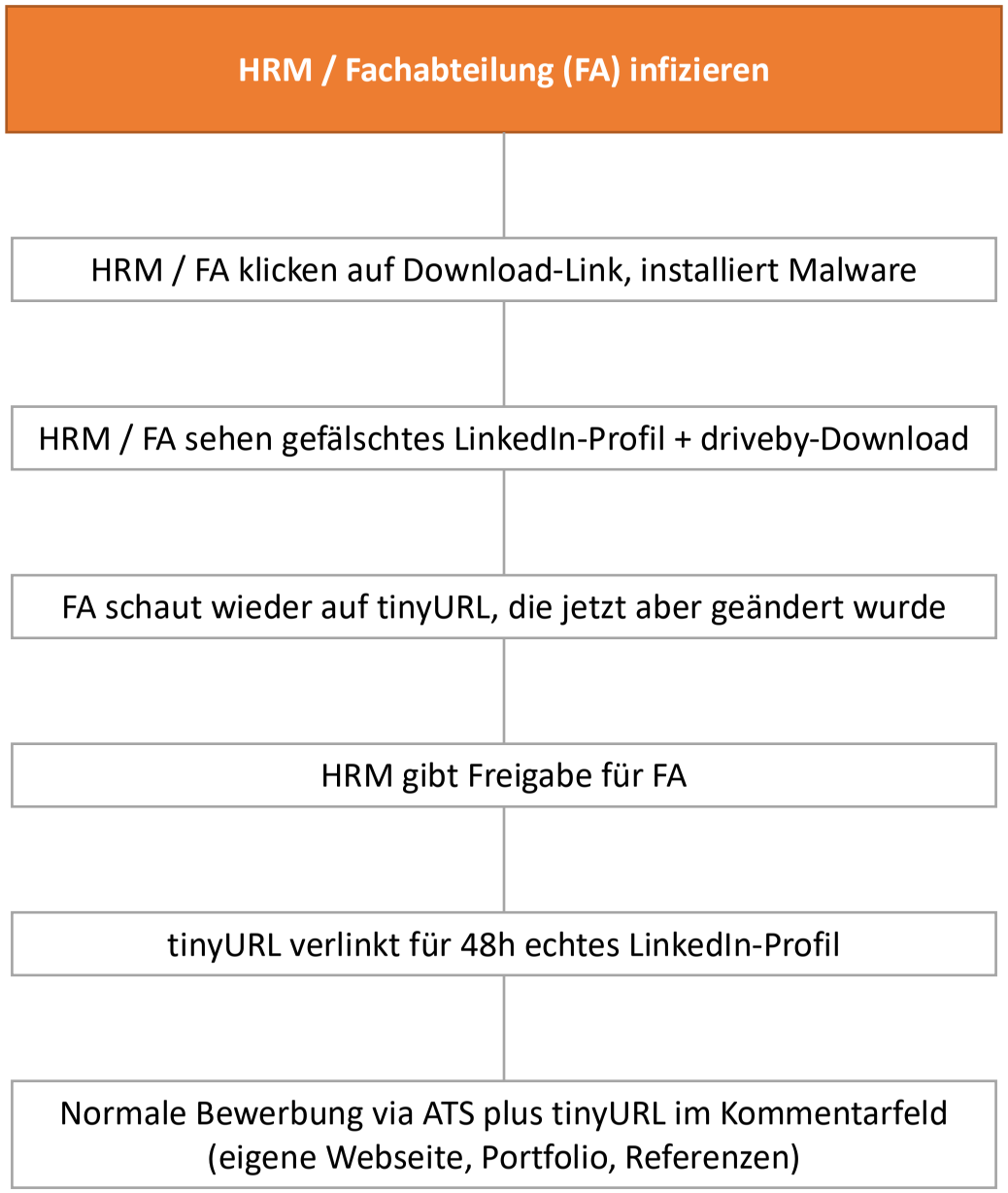
Anrufen und den Sachverhalt am Telefon ebenfalls schildern → Betroffenheit erzeugen

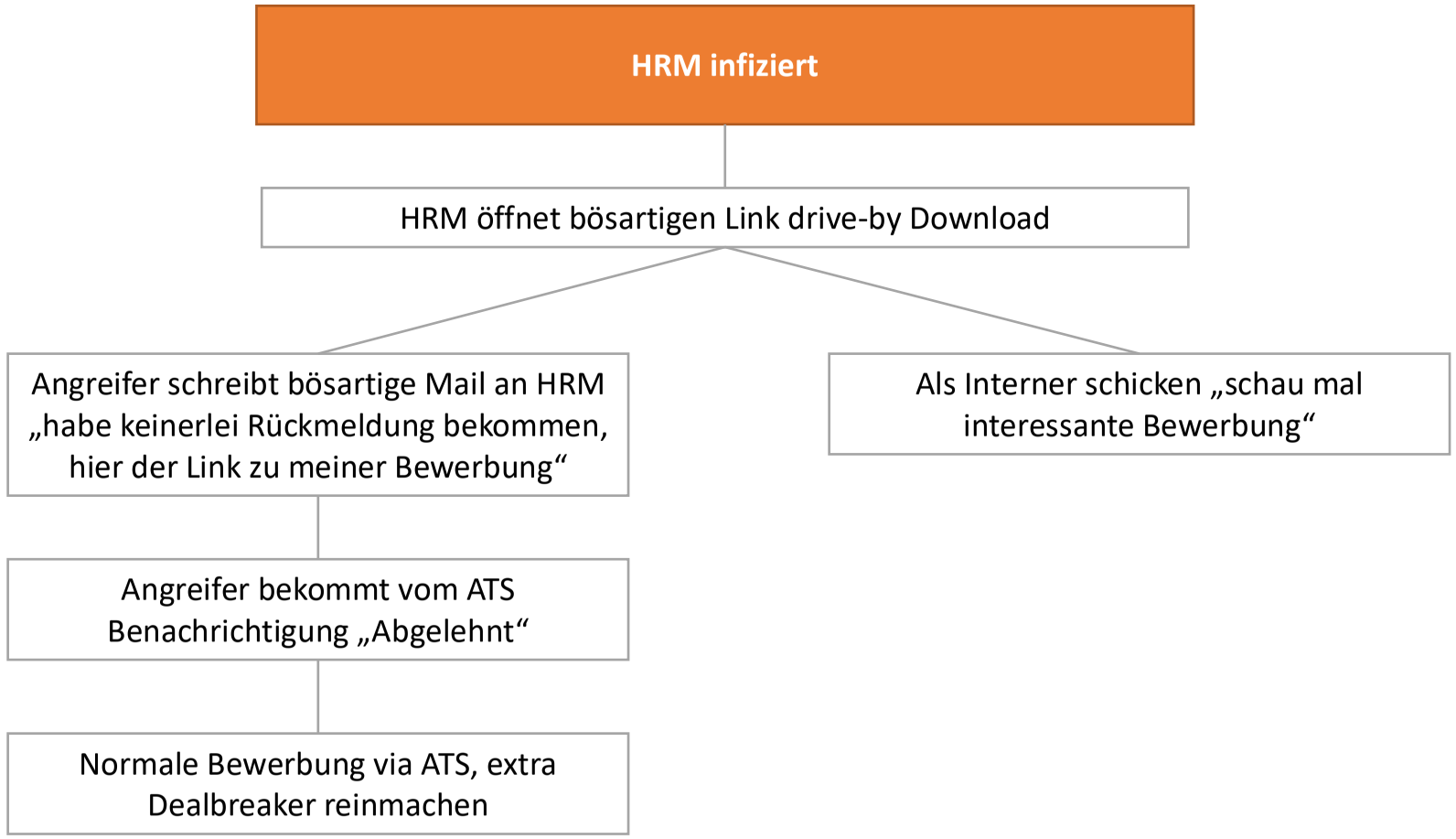
Bewerberunterlagen abrufbar über eine Link, Vertraulichkeit / Höherer Sicherheitsstandard

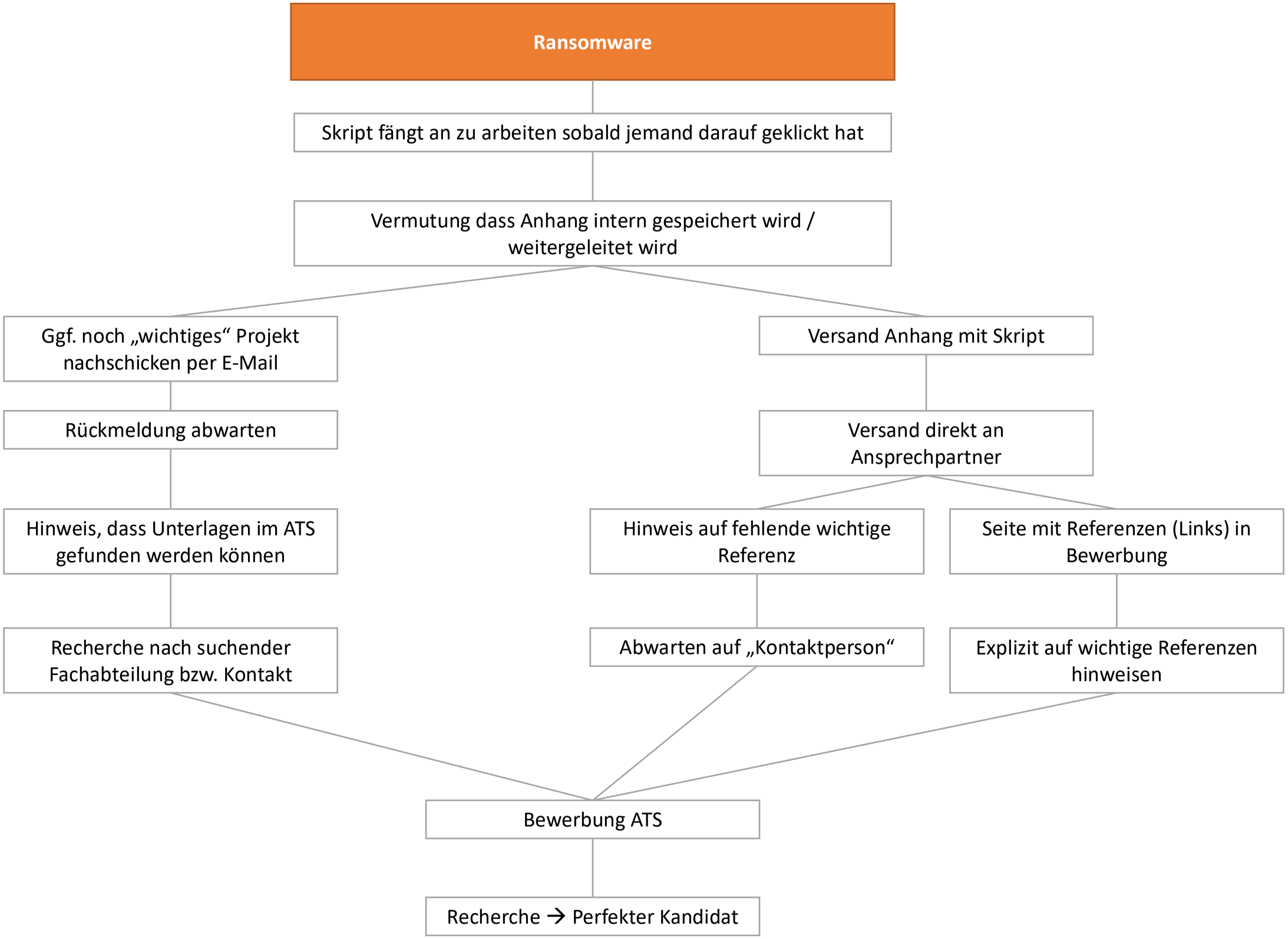
Nachreichen oder direkt „mitsenden“ der Bewerberunterlagen

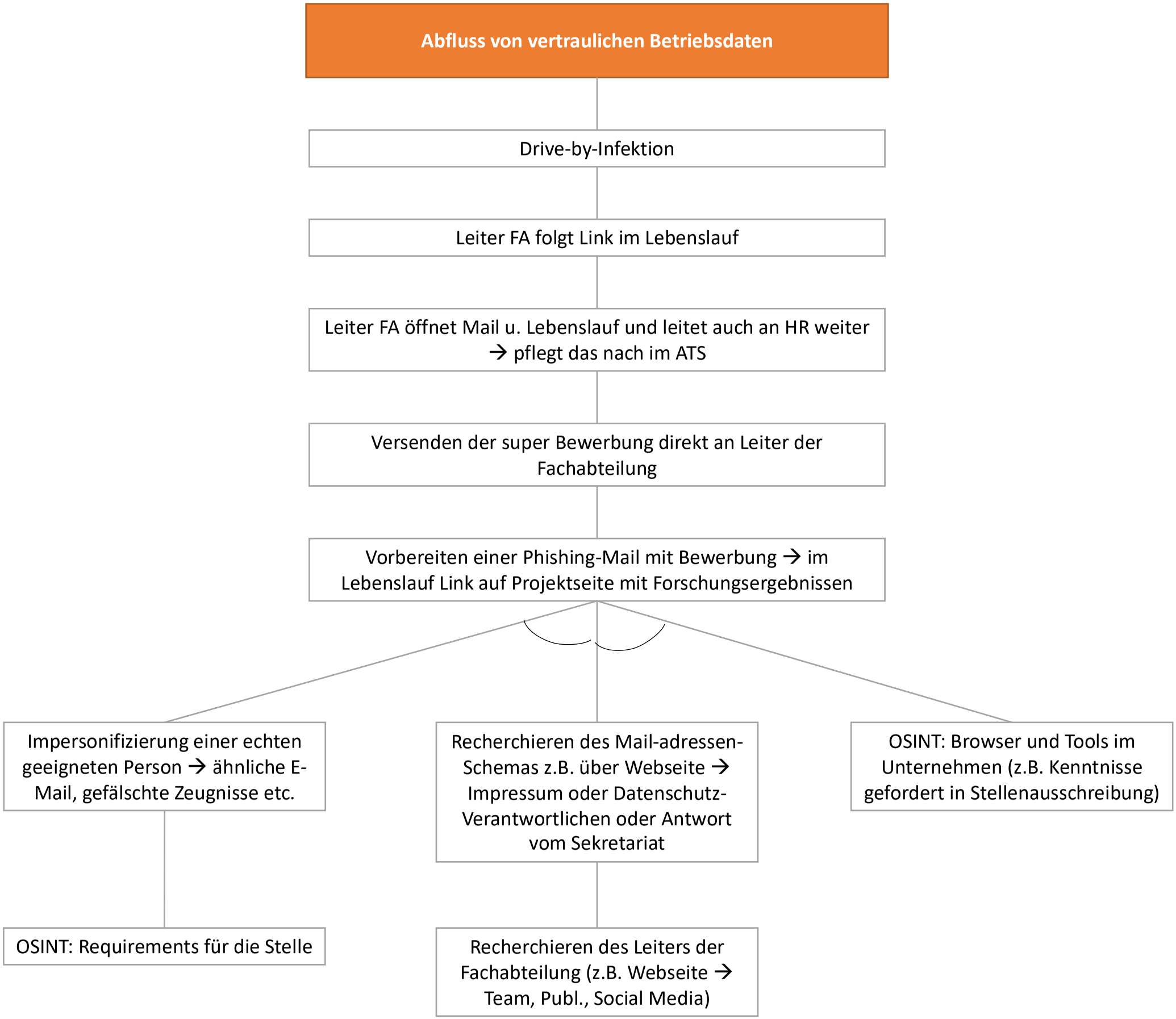
Kontaktaufnahme „Info—Mail, dass Bewerbung nicht eingepflegt werden kann → Tool funktioniert nicht


Fachabteilung (FA) infizieren
FA klickt auf Download-Link, installiert Malware
FA erhält eine Mail mit angeblichem ATS-Freigabelink (Spoofing)
Gefälschte Bewerbung einschicken über offiziellen ATS-Weg
OSINT: Welches ATS, welche Version, wie FA-Mail? Wie sieht der Freigabe-Link aus?


HRM / Fachabteilung (FA) infizieren
HRM / FA klicken auf Download-Link, installiert Malware
HRM / FA sehen gefälschtes LinkedIn-Profil + driveby-Download
FA schaut wieder auf tinyURL, die jetzt aber geändert wurde
HRM gibt Freigabe für FA
tinyURL verlinkt für 48h echtes LinkedIn-Profil
Normale Bewerbung via ATS plus tinyURL im Kommentarfeld
(eigene Webseite, Portfolio, Referenzen)


HRM infiziert
HRM öffnet bösartigen Link drive-by Download
Angreifer schreibt bösartige Mail an HRM „habe keinerlei Rückmeldung bekommen, hier der Link zu meiner Bewerbung“
Als Interner schicken „schau mal interessante Bewerbung“
Angreifer bekommt vom ATS Benachrichtigung „Abgelehnt“
Normale Bewerbung via ATS, extra Dealbreaker reinmachen

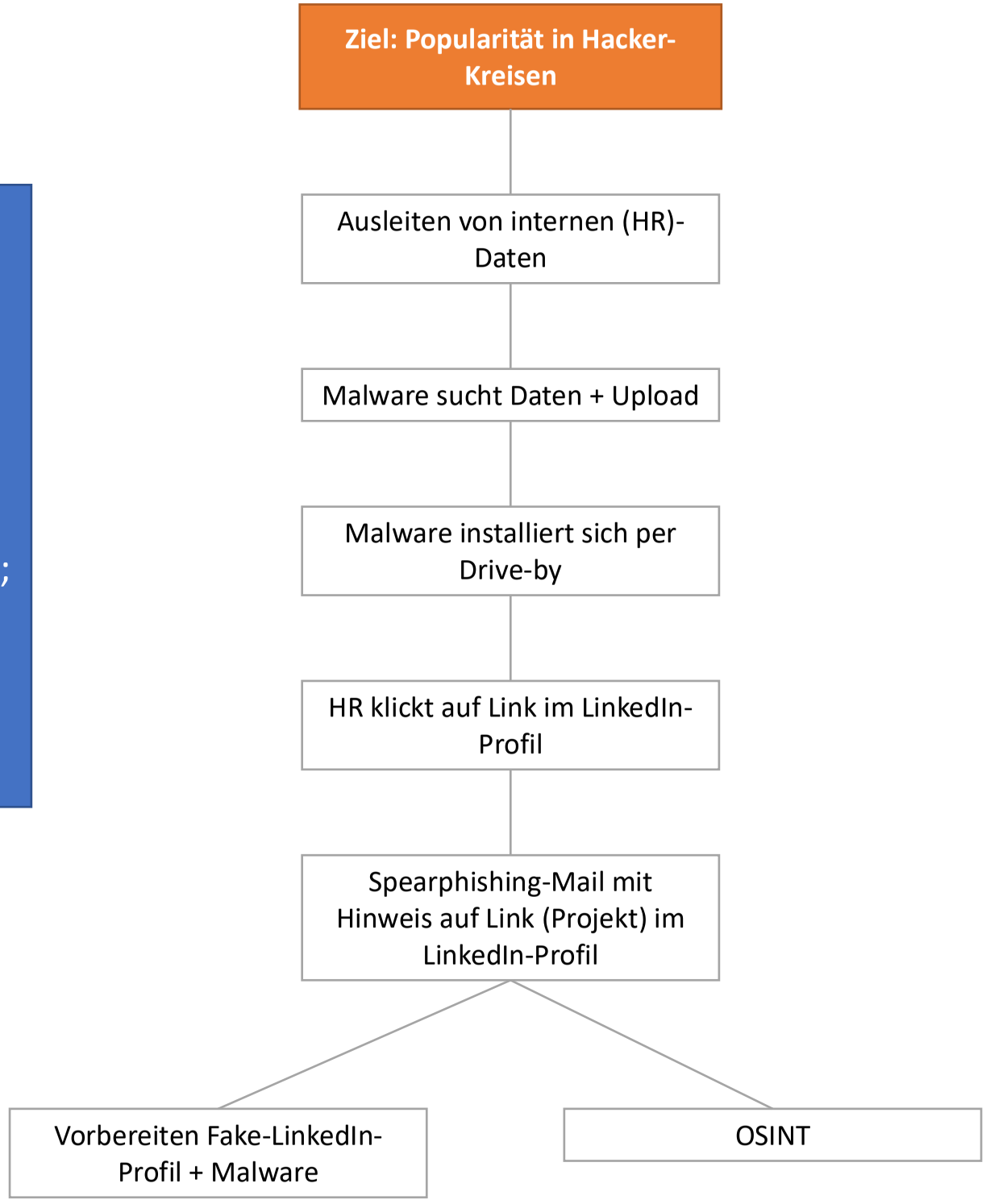

Ransomware
Skript fängt an zu arbeiten sobald jemand darauf geklickt hat
Vermutung dass Anhang intern gespeichert wird / weitergeleitet wird
Ggf. noch „wichtiges“ Projekt nachschicken per E-Mail
Rückmeldung abwarten
Hinweis, dass Unterlagen im ATS gefunden werden können
Recherche nach suchender Fachabteilung bzw. Kontakt
Versand Anhang mit Skript
Versand direkt an Ansprechpartner
Hinweis auf fehlende wichtige Referenz
Abwarten auf „Kontaktperson“
Seite mit Referenzen (Links) in Bewerbung
Explizit auf wichtige Referenzen hinweisen
Bewerbung ATS
Recherche → Perfekter Kandidat


Abfluss von vertraulichen Betriebsdaten
Drive-by-Infektion
Leiter FA folgt Link im Lebenslauf
Leiter FA öffnet Mail u. Lebenslauf und leitet auch an HR weiter → pflegt das nach im ATS
Versenden der super Bewerbung direkt an Leiter der Fachabteilung
Vorbereiten einer Phishing-Mail mit Bewerbung → im Lebenslauf Link auf Projektseite mit Forschungsergebnissen
Impersonifizierung einer echten geeigneten Person → ähnliche E-Mail, gefälschte Zeugnisse etc.
Recherchieren des Mail-adressen-Schemas z.B. über Webseite → Impressum oder Datenschutz-Verantwortlichen oder Antwort vom Sekretariat
OSINT: Browser und Tools im Unternehmen (z.B. Kenntnisse gefordert in Stellenausschreibung)
OSINT: Requirements für die Stelle
Recherchieren des Leiters der Fachabteilung (z.B. Webseite → Team, Publ., Social Media)

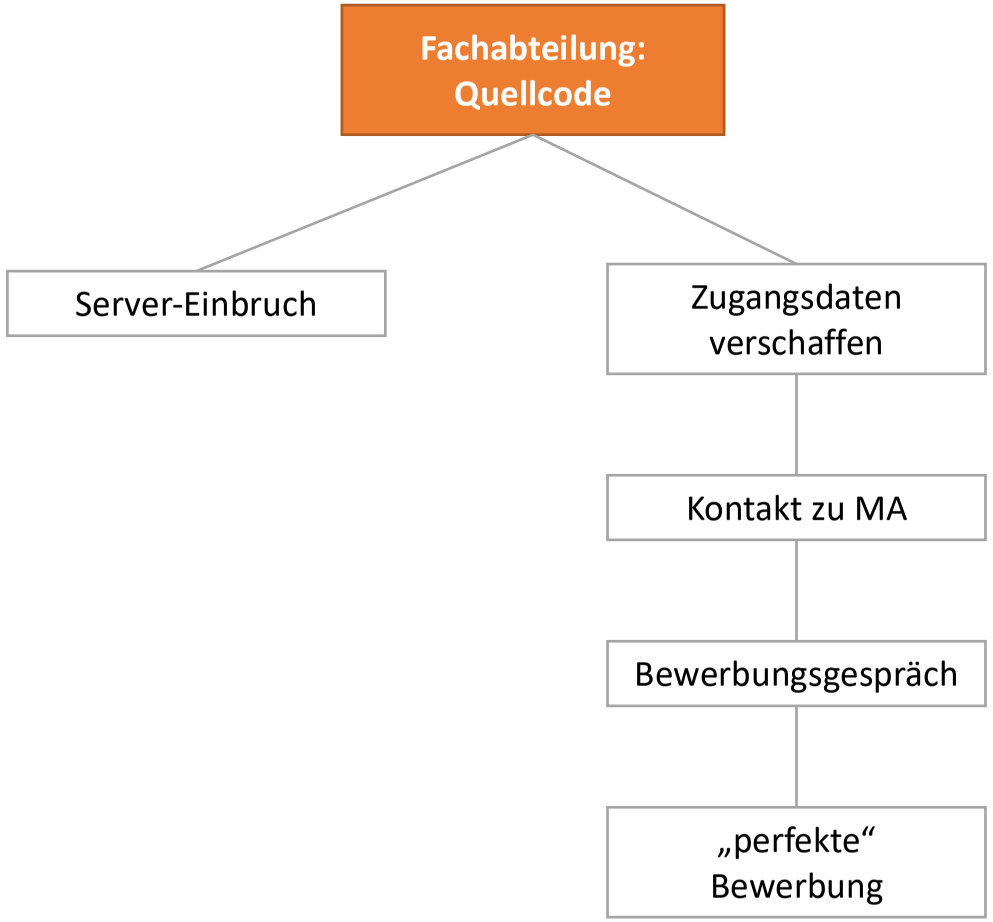
C

E-Mail

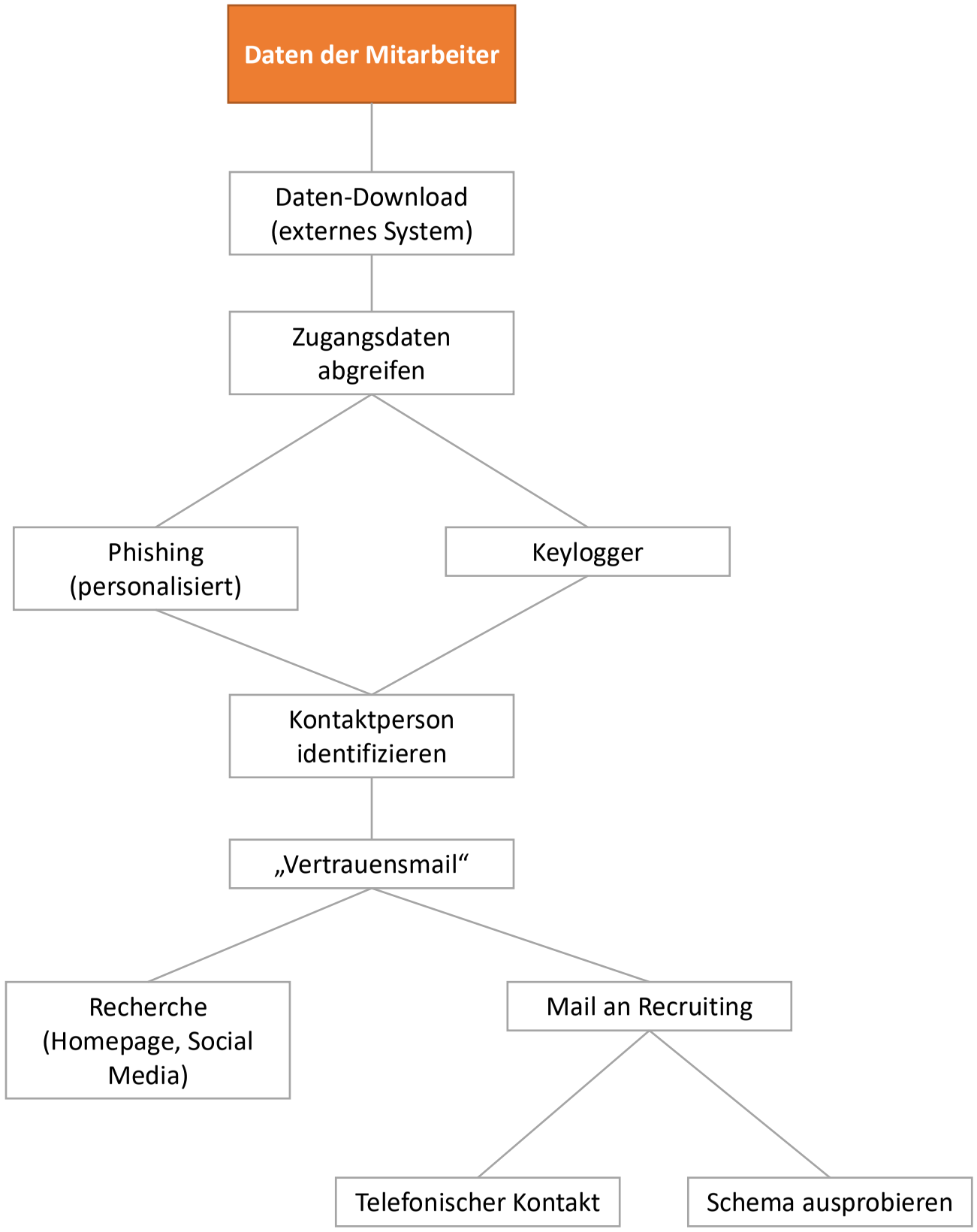
Student, 21-22 Jahre, wohnt im Wohnheim, will mal zeigen wo eine große Organisation ihre Lücken hat, er löst ohne „Gage“ auf und sucht die Fach-Öffentlichkeit, Bekanntheit im Netz; Ziel: Popularität in Macher-Kreisen; Beweis: Datenklau, Veränderung der Webseite; Beispiele: Liste von Bewerbern, Stammdaten

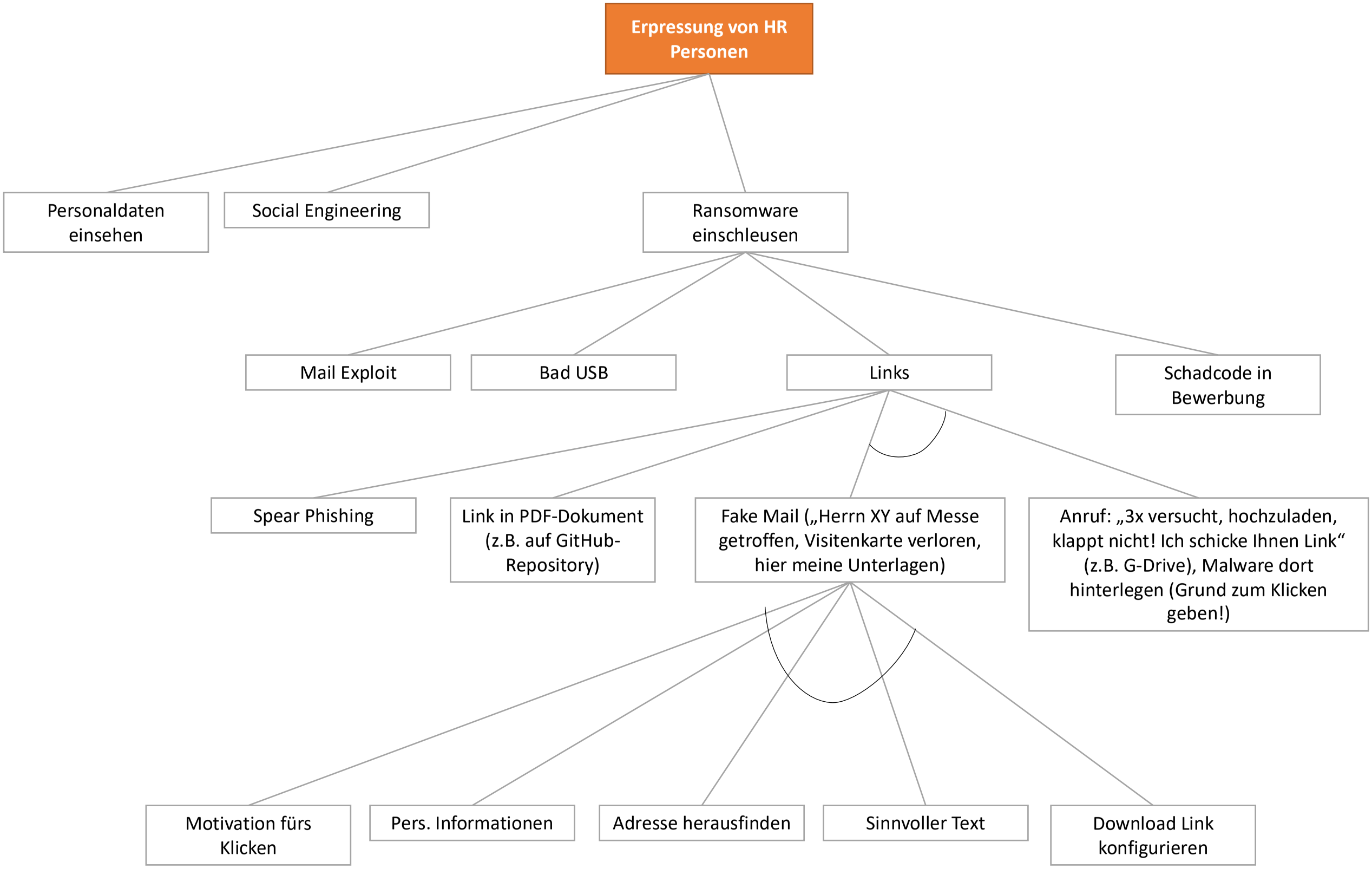


Akteur: Konkurrenz oder „Zwischenhändler“, der den Quellcode dann weiterverkaufen will



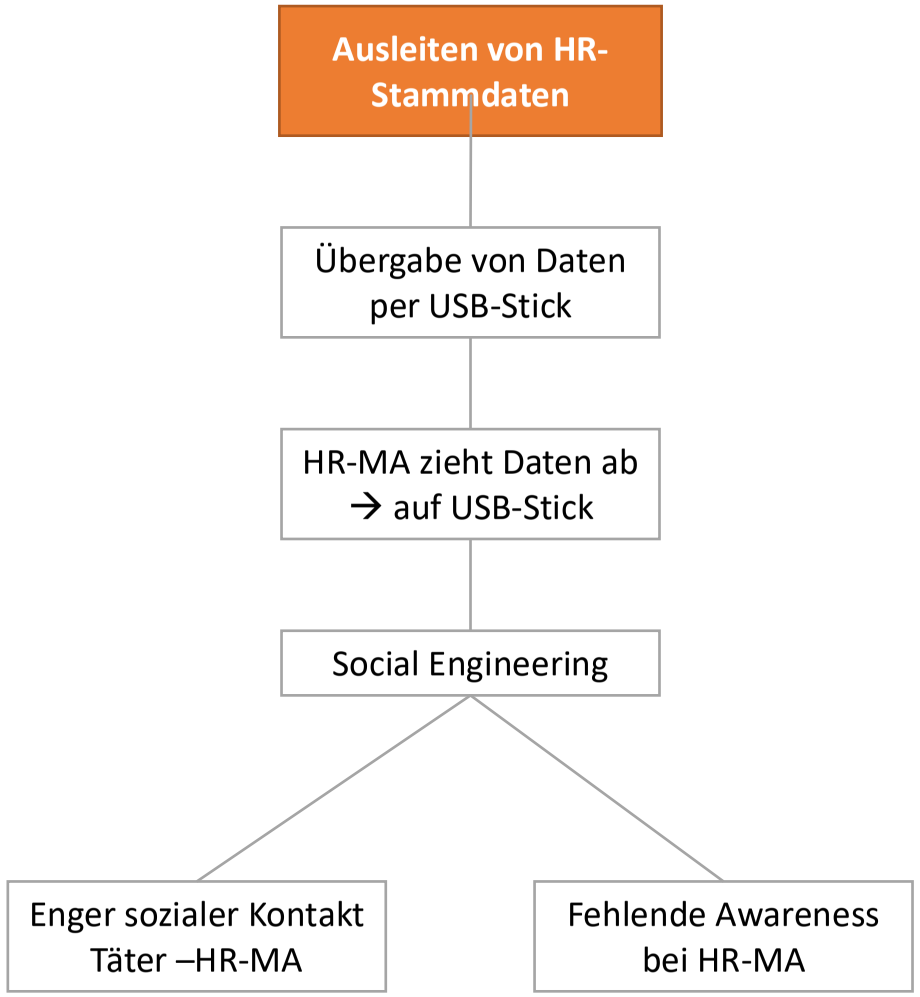
Akteur: Headhunter (Mitarbeiter abwerben) oder „Zwischenhändler“, der die Mitarbeiterdaten dann weiterverkaufen will

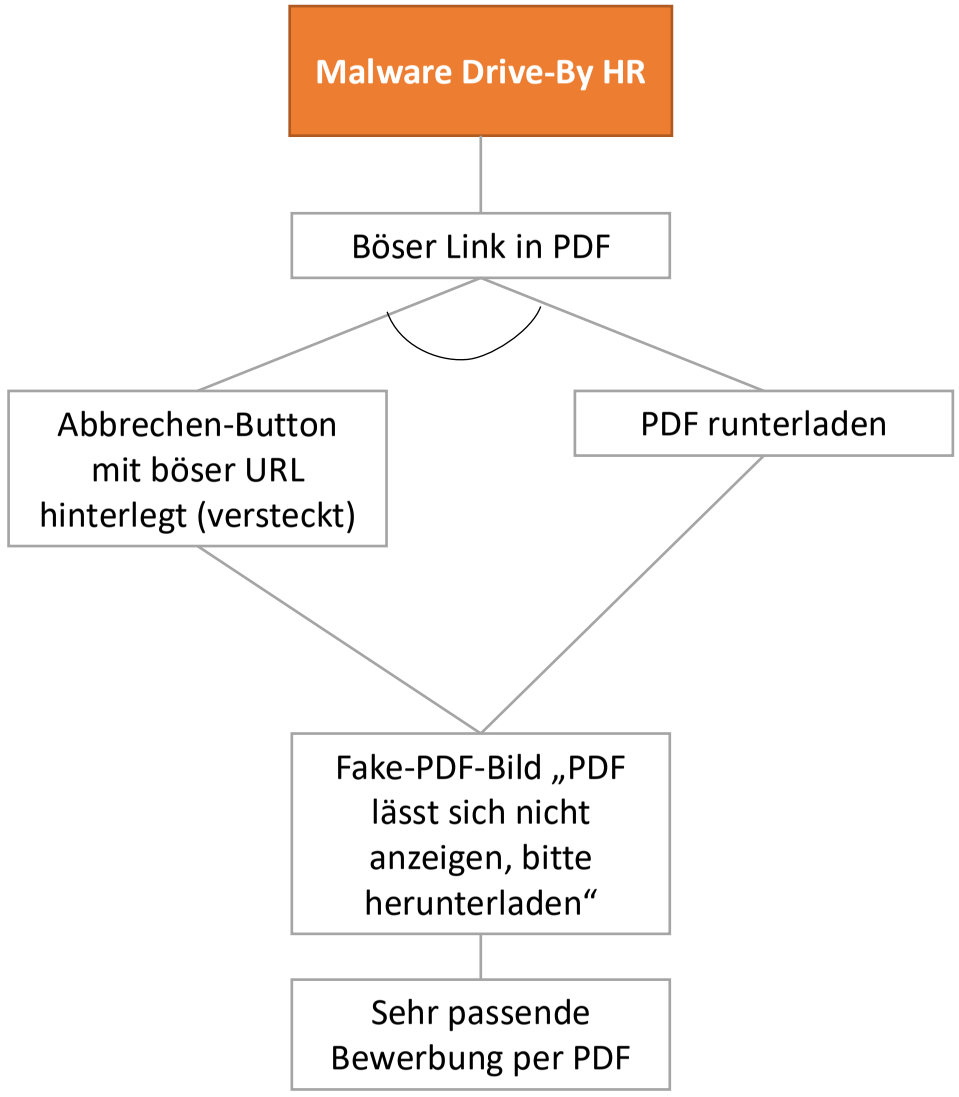


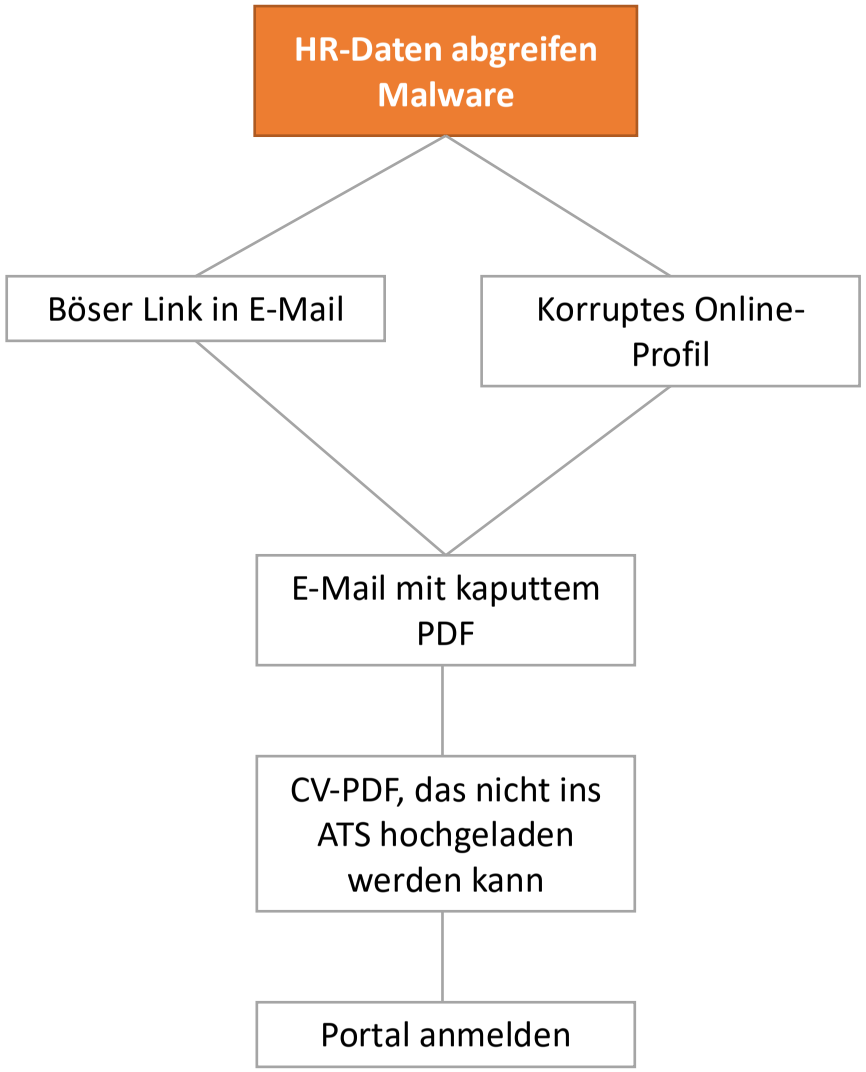

Erpressung von HR Personen
Personaldaten einsehen
Social Engineering
Ransomware einschleusen
Mail Exploit
Bad USB
Links
Schadcode in Bewerbung
Spear Phishing
Link in PDF-Dokument (z.B. auf GitHub-Repository)
Fake Mail („Herrn XY auf Messe getroffen, Visitenkarte verloren, hier meine Unterlagen)
Anruf: „3x versucht, hochzuladen, klappt nicht! Ich schicke Ihnen Link“ (z.B. G-Drive), Malware dort hinterlegen (Grund zum Klicken geben!)
Motivation fürs Klicken
Pers. Informationen
Adresse herausfinden
Sinnvoller Text
Download Link konfigurieren

ATS

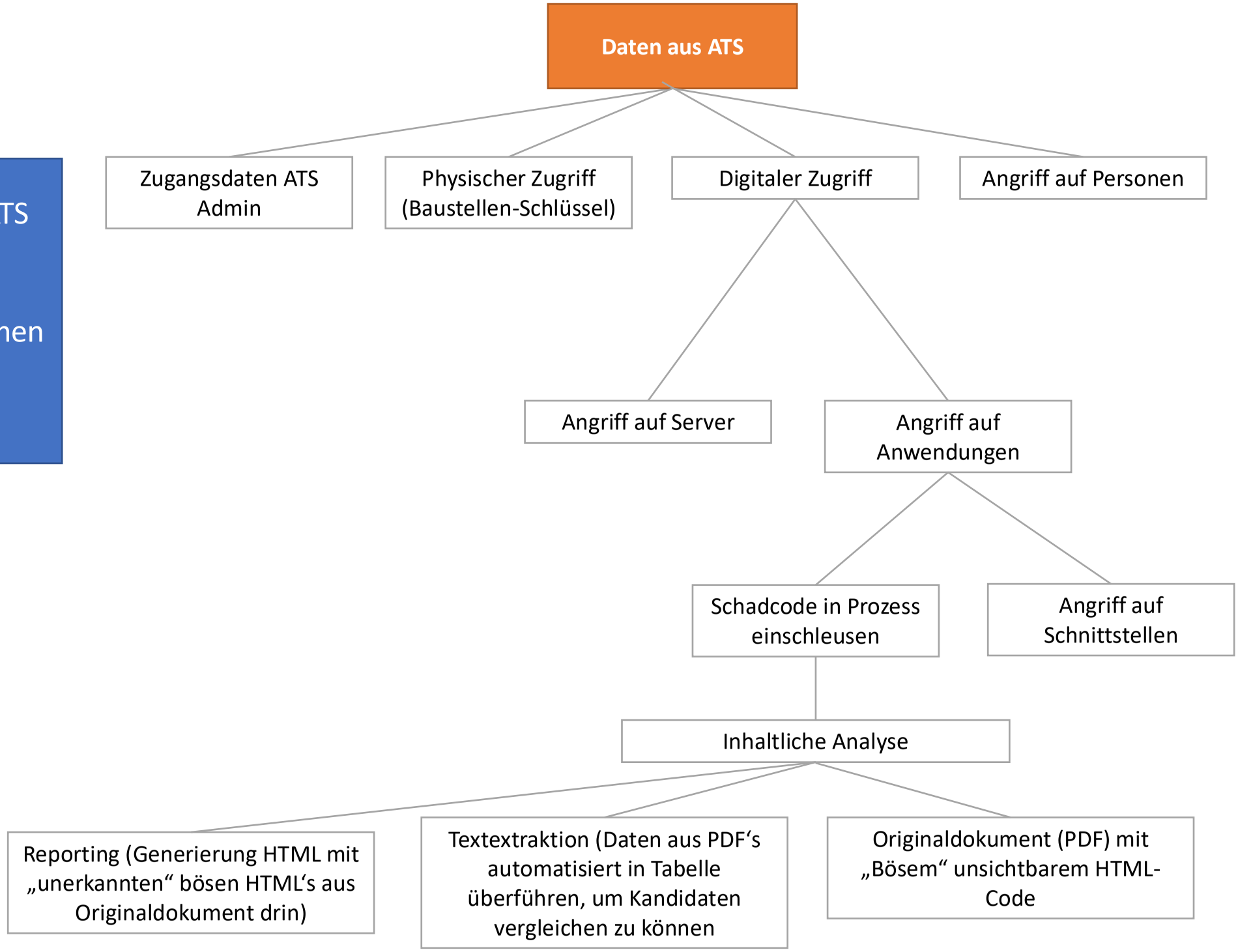
Kontext: Fehlende Awareness, persönlicher Kontakt, sozialer Kontakt; Ziel: verbotene Exporte von Daten, Übergabe der Daten (Datenträger, Medium, USB-Stick); Annahmen: Ausleiten von Daten ist möglich, Umgehung der AA u. Datenschutz, Speichern auf c:, Datenübertragung „physisch“




Malware Drive-By HR
Böser Link in PDF
Abbrechen-Button mit böser URL hinterlegt (versteckt)
PDF runterladen
Fake-PDF-Bild „PDF lässt sich nicht anzeigen, bitte herunterladen“
Sehr passende Bewerbung per PDF


HR-Daten abgreifen Malware
Böser Link in E-Mail
Korruptes Online-Profil
E-Mail mit kaputtem PDF
CV-PDF, das nicht ins ATS hochgeladen werden kann
Portal anmelden

Alles aus ATS abgreifen, aller Unternehmen die das nutzen



D

Universität der Bundeswehr München

Forschungsstudie zur IT-Sicherheit in Personalabteilungen deutscher Unternehmen

Sehr geehrte Teilnehmende,

in unserer digitalen Welt, ist IT-Sicherheit ein immer wichtiger werdendes Thema. Um deutsche Unternehmen wettbewerbsfähiger zu machen, untersuche ich den aktuellen Zustand der IT-Sicherheit in Personalabteilungen. Bitte nehmen Sie sich 20 Minuten Zeit, um meine Forschung und Ihr Unternehmen zu unterstützen.

Die Richtlinien guter ethischer Forschung sehen vor, dass sich die Teilnehmenden an empirischen Studien explizit und nachvollziehbar mit der Teilnahme einverstanden erklären.

Freiwilligkeit. Ihre Teilnahme an dieser Untersuchung ist freiwillig. Sie beruht auf Ihrer Einwilligung, die Sie erteilen, indem Sie untenstehendes Einwilligungskästchen anklicken (Art. 6, Abs. 1, lit. a EU-DSGVO). Es entstehen Ihnen keine Nachteile, sofern Sie die Teilnahme verweigern, oder die Befragung abbrechen.

Anonymität. Ihre Daten sind selbstverständlich vertraulich, werden nur in anonymisierter Form ausgewertet und nicht an Dritte weitergegeben. Demografische Angaben wie Alter oder Geschlecht lassen keinen eindeutigen Schluss auf Ihre Person zu.

Datenschutz: SoSci Survey ist eine deutsche Standardsoftware für akademische Forschung „made in Germany“, d.h. Server und Betreiber sitzen in Deutschland. Weitere Informationen finden sie unter www.socisurvey.de/de/pivacy .

Fragen. Falls Sie noch Fragen zu dieser Studie haben sollten, finden Sie im Anschluss ein Impressum mit Kontaktdaten der Studienleitenden.

Ich bin 18 Jahre, oder älter und erkläre hiermit meine Einwilligung in die Erhebung, Verarbeitung und Auswertung der nachfolgend gemachten Angaben. Die vorstehenden Hinweise habe ich zur Kenntnis genommen, insbesondere meine Rechte als teilnehmende Person an dieser Befragung.

- ○ Ja
- ○ Nein (nicht an der Studie teilnehmen)

Seite 02

SD

1. Welches Geschlecht haben Sie?

- weiblich
- männlich
- divers

2. Bitte geben Sie Ihr Alter an

[Bitte auswählen]

3. Welches ist der höchste Bildungsabschluss, den Sie haben?

- Hauptschulabschluss/Volksschulabschluss
- Realschulabschluss (Mittlere Reife)
- Abschluss polytechnische Oberschule 10. Klasse (vor 1965: 8. Klasse)
- Fachhochschulreife (Abschluss einer Fachoberschule)
- Abitur, allgemeine oder fachgebundene Hochschulreife (Gymnasium bzw. EOS)
- Bachelorabschluss
- Masterabschluss (oder vergleichbares)
- Promoviert
- Abgeschlossene kaufmännische Lehre
- Abgeschlossene gewerbliche oder landwirtschaftliche Lehre
- Meister-, Techniker- oder gleichwertiger Fachschulabschluss
- Andere

Seite 03

Um ein gemeinsames Verständnis zur Begrifflichkeit „IT-Sicherheit“ zu schaffen, beantworten Sie bitte folgende Fragen.

Seite 04

4. Es gibt einen Unterschied zwischen IT-Sicherheit und Datenschutz.

- Ja
- Nein

Seite 05

5. Bitte geben Sie an, zu wie viel Prozent Sie sich sicher sind, den Unterschied zwischen IT-Sicherheit und Datenschutz erläutern zu können.

0 10 20 30 40 50 60 70 80 90 100

Ich bin mir sicher, den Unterschied zwischen IT-Sicherheit und Datenschutz erläutern zu können.

Seite 06

Der Unterschied zwischen IT-Sicherheit und Datenschutz

IT-Sicherheit

Ziel der IT-Sicherheit ist es, informationstechnische Systeme von Organisationen, beispielsweise Unternehmen, und deren Werte vor Bedrohungen zu schützen. Es geht darum, alle elektronisch gespeicherten Daten des Unternehmens vor Zugriff durch Dritte zu schützen und damit schließlich auch wirtschaftlichen Schaden zu verhindern.

Datenschutz

Datenschutz beschreibt den Schutz vor der missbräuchlichen Verarbeitung personenbezogener Daten sowie den Schutz des Rechts auf informationelle Selbstbestimmung.

Seite 07

6. Bitte geben Sie an, inwieweit Ihre Einschätzung zum Unterschied zwischen IT-Sicherheit und Datenschutz korrekt war.

0 10 20 30 40 50 60 70 80 90 100

Mein Kenntnisstand zum Unterschied zwischen IT-Sicherheit und Datenschutz war zu ...% korrekt.

Seite 08

7. Bitte kreuzen Sie an, welche Position Sie im Unternehmen haben.

Falls Sie für IT-Sicherheit, oder Datenschutz in Nebentätigkeit verantwortlich sind, kreuzen sie bitte die jeweilige Option an.

- ◯ Mitarbeitende Person in der Personalabteilung
- ◯ Führungskraft in der Personalabteilung
- ◯ Mitarbeitende Person in einer anderen Abteilung
- ◯ Führungskraft in einer anderen Abteilung
- ◯ IT-Sicherheitsbeauftragte Person (oder vergleichbares)
- ◯ Datenschutzbeauftragte Person (oder vergleichbares)
- ◯ Keine Angabe

Seite 09

Vollständige Anonymität

Die Teilnahme an dieser Befragung lässt keinerlei Rückschlüsse auf Ihre Person zu. Alle Daten werden streng vertraulich behandelt.

Seite 10

8. Ich weiß, was IT-Sicherheit ist.

- Ja
- Nein

9. Das Unternehmen hat IT-Sicherheitsrichtlinien.

- Ja
- Nein
- Ich weiß nicht

10. Ich habe die IT-Sicherheitsrichtlinien gelesen.

- Ja
- Nein
- Keine Angabe

11. Ich weiß, wo ich eine Ausfertigung der IT-Sicherheitsrichtlinien bekommen kann.

- Ja
- Nein
- Keine Angabe

12. Ich weiß, wer die für meine Abteilung zuständige IT-Sicherheitsbeauftragte Person ist.

- Ja
- Nein
- Es gibt keine
- Keine Angabe

Seite 11

13. Ich weiß, wer die für meine Abteilung zuständige beauftragte Person für Datenschutz ist.

- Ja
- Nein
- Es gibt keine
- Ich bin mir nicht sicher

14. Ich kenne meine Verantwortlichkeiten in Bezug auf IT-Sicherheit.

- Ja
- Nein
- Ich bin mir nicht sicher

15. Ich weiß, was ein IT-Sicherheitsvorfall ist.

- Ja
- Nein

16. Ich weiß von mindestens einer Verletzung der IT-Sicherheit in meinem Geschäftsbereich innerhalb der letzten 12 Monate.

- Ja
- Nein

17. Ich wurde innerhalb der letzten sechs Monate über die Anforderungen an die IT-Sicherheit informiert. Z. B. Vorschriften für das Herunterladen von E-Mail-Anhängen oder dem Surfen im Internet.

- Ja
- Nein

18. Ich bin der Meinung, dass Passwörter geteilt werden sollten, um den Zugang zu Informationen leichter zu gestalten.

- Ja
- Nein

19. Ich weiß von anderen Mitarbeitenden, die ihre Passwörter untereinander teilen.

- Ja
- Nein

20. Ich verstehe, dass einige Dokumente sicherheitsempfindlicher sind als andere.

- ◯ Ja
- ◯ Nein

Seite 12

21. Welche der folgenden Informationsträger, könnten vertrauliche Informationen enthalten?
Bitte kreuzen Sie alle Zutreffenden an.

- ☐ Ausgedruckte Dokumente
- ☐ Elektronische Dokumente
- ☐ Faxe
- ☐ Geschäftliche Telefonate
- ☐ E-Mails
- ☐ Sprachnachrichten
- ☐ Dokumente, die sich auf einem Smartphone oder Tablet befinden
- ☐ Unterhaltungen über Messengerdienste

22. Wem dürfen Sie Ihrer Meinung nach Ihr Passwort mitteilen?
Bitte kreuzen Sie alle zutreffenden an.
* Ein Helpdesk, ist eine Einrichtung, an die Sie sich bei IT-Problemen wenden können.

- ☐ Dem Helpdesk*
- ☐ Der mir vorgesetzten Person
- ☐ Niemand
- ☐ Einer Verwaltungskraft
- ☐ Einem anderen Mitarbeitenden

23. Wem sollten Vorfälle im Bereich der IT-Sicherheit gemeldet werden?
Bitte kreuzen Sie alle Zutreffenden an.
* Ein Helpdesk, ist eine Einrichtung, an die Sie sich bei IT-Problemen wenden können.

- ☐ Dem Helpdesk*
- ☐ Der mir direkt vorgesetzten Person
- ☐ Der für meinen Bereich zugeteilten, für IT-Sicherheit verantwortlichen, Person
- ☐ Der IT-Abteilung
- ☐ Ich weiß es nicht
- ☐ Der Vorfall sollte publik gemacht werden

24. Wie möchten Sie Informationen zur IT-Sicherheit erhalten?

Kreuzen Sie alle an, die für Sie infrage kommen.

- ☐ Internet
- ☐ Poster
- ☐ E-Mail
- ☐ Diskussionsgruppen
- ☐ Präsentationen
- ☐ Praktisches Training
- ☐ Über Messengerdienste
- ☐ Training über das Internet
- ☐ Video-Training
- ☐ Handbücher

Seite 13

25. Bitte beurteilen Sie folgende Aussagen zu den IT-Sicherheitsrichtlinien in Ihrem Unternehmen.

	stimme gar nicht zu	stimme eher nicht zu	unent-schieden	stimme eher zu	stimme voll zu	kann ich nicht beurteilen
Der Inhalt der IT-Sicherheitsrichtlinien ist leicht verständlich.	○	○	○	○	○	○
Ich glaube, dass die IT-Sicherheitsrichtlinien umsetzbar sind.	○	○	○	○	○	○
Ich glaube, dass mein Unternehmen mir die relevanten Anforderungen an die IT-Sicherheit mitteilt.	○	○	○	○	○	○
Der Inhalt der IT-Sicherheitsrichtlinien wurde mir wirksam vermittelt.	○	○	○	○	○	○
Ich werde rechtzeitig darüber informiert, wie sich Änderungen in der IT-Sicherheit auf mich auswirken werden.	○	○	○	○	○	○

26. Bitte beurteilen Sie folgende Aussagen zur Notwendigkeit von IT-Sicherheit.

	stimme gar nicht zu	stimme eher nicht zu	unent-schieden	stimme eher zu	stimme voll zu	kann ich nicht beurteilen
Die IT-Sicherheitsrichtlinien meines Unternehmens gelten für mich bei der Ausführung meiner täglichen Aufgaben.	○	○	○	○	○	○
Ich widme der IT-Sicherheit gerne Zeit.	○	○	○	○	○	○
Es ist mir wichtig, die Bedrohungen (z. B. Diebstahl von Geräten und Änderung oder Missbrauch von Informationen) für die Informationsbestände in meiner Abteilung zu kennen.	○	○	○	○	○	○
Ich bin der Meinung, dass ich für den Schutz der Informationswerte meines Arbeitgebenden (z. B. Informationen und Computerressourcen) verantwortlich bin.	○	○	○	○	○	○
Es ist wichtig, Menschen für die IT-Sicherheit zu sensibilisieren.	○	○	○	○	○	○
IT-Sicherheit ist in meiner Abteilung notwendig.	○	○	○	○	○	○
Ich akzeptiere, dass einige Unannehmlichkeiten (z. B. regelmäßiges Ändern meines Passworts, Wegschließen wichtiger Dokumente oder Anlegen von Sicherungskopien) notwendig sind, um wichtige Informationen zu schützen.	○	○	○	○	○	○
Informationsbestände in elektronischem Format (z. B. auf meiner Festplatte, auf CDs oder einem USB-Stick gespeicherte Informationen) müssen geschützt werden.	○	○	○	○	○	○
Informationsbestände in Papierform (z. B. Verträge und gedruckte Berichte) müssen geschützt werden.	○	○	○	○	○	○
Ich bin mit den Aspekten der IT-Sicherheit vertraut, die mit meiner Tätigkeit zusammenhängen (z. B. Wahl eines Passworts oder Umgang mit vertraulichen Informationen).	○	○	○	○	○	○
Ich bin bereit, meine Arbeitspraktiken zu ändern, um die Sicherheit von Informationsgütern (z. B. Computersysteme und Informationen in Papier- oder elektronischer Form) zu gewährleisten.	○	○	○	○	○	○
Ich bin mir der negativen Folgen eines Verstoßes gegen die IT-Sicherheitsrichtlinien meines Arbeitgebendem bewusst.	○	○	○	○	○	○

Ich halte es für notwendig, dass meine arbeitgebende Person die Einhaltung der IT-Sicherheitspolitik überwacht.	○	○	○	○	○	○

27. Bitte beurteilen Sie folgende Aussagen zur Verantwortlichkeit für IT-Sicherheit.

	stimme gar nicht zu	stimme eher nicht zu	unent-schieden	stimme eher zu	stimme voll zu	kann ich nicht beurteilen
Die IT-Sicherheit muss durch ein formelles System geregelt werden (z. B. Aufgaben und Zuständigkeiten der Mitarbeiter im Bereich der IT-Sicherheit, Sensibilisierungskampagnen).	○	○	○	○	○	○
Ich bin der Meinung, dass die Vorgaben zur IT-Sicherheit in meine täglichen Aufgaben einfließen sollten.	○	○	○	○	○	○
Ich halte es für notwendig, Geld in die IT-Sicherheit zu investieren.	○	○	○	○	○	○
IT-Sicherheit sollte Teil meines Leistungsentwicklungsprogramms sein.	○	○	○	○	○	○
Um zu zeigen, dass Sie noch aufmerksam sind, wählen Sie bitte „stimme gar nicht zu“ aus.	○	○	○	○	○	○
Verstöße gegen die IT-Sicherheit, wie z.B. die Weitergabe von Passwörtern, vertraulichen Informationen oder der Besuch verbotener Internetseiten, sollten geahndet werden und Konsequenzen nach sich ziehen.	○	○	○	○	○	○
Ich bin der Meinung, dass zusätzliche Schulungen für den Einsatz von IT-Sicherheitsinstrumenten erforderlich sind, um Informationen zu schützen.	○	○	○	○	○	○

Seite 14

28. Bitte beurteilen Sie folgende Aussagen über das Verhalten ihrer vorgesetzten Personen, beim Umgang mit IT-Sicherheit.

Diese Umfrage ist vollständig anonym und lässt keine Rückschlüsse auf Sie zu.

	stimme gar nicht zu	stimme eher nicht zu	unent-schieden	stimme eher zu	stimme voll zu	kann ich nicht beurteilen
Führungskräfte und leitende Angestellte zeigen Engagement für die IT-Sicherheit.	○	○	○	○	○	○
Ich bin der Meinung, dass meine Abteilung ihre Informationswerte (z. B. Computerausrüstung und Dokumente) angemessen schützt.	○	○	○	○	○	○
Unsere Abteilung nimmt Veränderungen in unseren Arbeitsmethoden positiv auf, um die Sicherheit von Informationswerten zu gewährleisten.	○	○	○	○	○	○
Die Angehörigen meiner Kollegschaft zeigen Engagement für IT-Sicherheit.	○	○	○	○	○	○

29. Bitte beurteilen Sie folgende Aussagen zum Thema Verpflichtung zur IT-Sicherheit.

	stimme gar nicht zu	stimme eher nicht zu	unent-schieden	stimme eher zu	stimme voll zu	kann ich nicht beurteilen
Mitarbeitende aus der IT zeigen Engagement für die IT-Sicherheit.	○	○	○	○	○	○
Ich glaube, dass in dem Unternehmen, in dem ich arbeite, Maßnahmen zur IT-Sicherheit ergriffen werden.	○	○	○	○	○	○
Ich glaube, meine Abteilung widmet der IT-Sicherheit genügend Zeit.	○	○	○	○	○	○
IT-Sicherheit wird von anderen Mitarbeitenden als wichtig empfunden.	○	○	○	○	○	○
Ich glaube, dass meine Abteilung genügend Mitarbeitende für die IT-Sicherheit einsetzt.	○	○	○	○	○	○
Ich bin der Meinung, dass die Informationen, mit denen ich arbeite, angemessen geschützt sind (z. B. Zugangskontrolle zu Gebäuden und Arbeitsplätzen, Wegschließen von vertraulichen Informationen, Bewusstsein dafür, welche Informationen ich anderen Personen gebe und Anmeldedaten).	○	○	○	○	○	○
Ich glaube, dass meine Abteilung genug Geld für die IT-Sicherheit investiert.	○	○	○	○	○	○
In meiner Abteilung ist klar festgelegt, was von mir in Bezug auf die IT-Sicherheit erwartet wird.	○	○	○	○	○	○
Ich glaube, alle Mitarbeitenden in meinem Unternehmen halten sich an die IT-Sicherheitsrichtlinien.	○	○	○	○	○	○
Meine Abteilung ermutigt zur Einhaltung der IT-Sicherheitsrichtlinien.	○	○	○	○	○	○
Ich glaube, dass die Initiativen zur Sensibilisierung für die IT-Sicherheit wirksam sind.	○	○	○	○	○	○
Mein Unternehmen hat klare Richtlinien zum Schutz sensibler/vertraulicher Daten von Mitarbeitenden.	○	○	○	○	○	○

30. Bitte Beurteilen Sie folgende Aussagen und wie Sie den Umgang mit Informationen wahrnehmen.

	stimme gar nicht zu	stimme eher nicht zu	unent-schieden	stimme eher zu	stimme voll zu	kann ich nicht beurteilen
Die Angehörigen meiner Kollegschaft sind vorsichtig, wenn sie an öffentlichen Orten über vertrauliche Informationen sprechen.	○	○	○	○	○	○
In meinem Unternehmen gibt es klare Richtlinien zum Schutz sensibler/vertraulicher Mitarbeiterdaten.	○	○	○	○	○	○
Ich halte es für wichtig, die Erfassung und Weitergabe sensibler, persönlicher Daten zu begrenzen.	○	○	○	○	○	○
Die Angehörigen meiner Kollegschaft sorgen dafür, dass Daten von Bewerbenden geschützt (z.B. verschlüsselt) werden, wenn sie außer Haus gebracht werden (z.B. Homeoffice).	○	○	○	○	○	○

Seite 15

31. Bitte beurteilen Sie folgende Aussagen zum Umgang mit Passwörtern.

	stimme gar nicht zu	stimme eher nicht zu	unent-schieden	stimme eher zu	stimme voll zu	kann ich nicht beurteilen
Ich verwende ein anderes Passwort für meine Konten bei sozialen Medien und bei der Arbeit.	○	○	○	○	○	○
Ich teile meine Arbeitspasswörter mit anderen Mitarbeitenden.	○	○	○	○	○	○
Ich verwende eine Kombination aus Buchstaben, Zahlen und Sonderzeichen in meinen Arbeitspasswörtern.	○	○	○	○	○	○

32. Bitte beurteilen Sie folgende Aussagen zum Umgang mit Weblinks in E-Mails.

	stimme gar nicht zu	stimme eher nicht zu	unent-schieden	stimme eher zu	stimme voll zu	kann ich nicht beurteilen
Ich klicke hin und wieder auf Links in E-Mails, nur wenn diese von jemandem kommen, den ich kenne.	○	○	○	○	○	○
Ich öffne keine E-Mail-Anhänge, wenn mir der Absender unbekannt ist.	○	○	○	○	○	○
Wenn eine E-Mail von einem unbekannten Absender interessant aussieht, klicke ich auf einen Link in der E-Mail.	○	○	○	○	○	○

33. Bitte beurteilen Sie folgende Aussagen zur Internetznutzung am Arbeitsplatz.

	stimme gar nicht zu	stimme eher nicht zu	unent-schieden	stimme eher zu	stimme voll zu	kann ich nicht beurteilen
Wenn ich bei der Arbeit ins Internet gehe, besuche ich jede Website, die ich besuchen möchte.	○	○	○	○	○	○
Ich lade alle Dateien auf meinen Arbeitscomputer herunter, die mir helfen, meine Arbeit zu erledigen.	○	○	○	○	○	○
Ich prüfe die Sicherheit von Websites, bevor ich Informationen eingebe.	○	○	○	○	○	○

34. Bitte beurteilen Sie folgende Aussagen zur privaten Nutzung von sozialen Medien am Arbeitsplatz.

	stimme gar nicht zu	stimme eher nicht zu	unent-schieden	stimme eher zu	stimme voll zu	kann ich nicht beurteilen
Ich überprüfe meine Datenschutzeinstellungen in den sozialen Medien regelmäßig.	○	○	○	○	○	○
Ich poste nichts in den sozialen Medien, bevor ich nicht die negativen Folgen bedacht habe.	○	○	○	○	○	○
Ich poste in den sozialen Medien alles, was ich will, über meine Arbeit.	○	○	○	○	○	○

Seite 16

35. Bitte beurteilen Sie folgende Aussagen zum Umgang mit dienstlichen, mobilen Endgeräten in der Öffentlichkeit.

	stimme gar nicht zu	stimme eher nicht zu	unent-schieden	stimme eher zu	stimme voll zu	kann ich nicht beurteilen
Wenn ich an einem öffentlichen Ort arbeite, lasse ich meinen Laptop manchmal unbeaufsichtigt.	○	○	○	○	○	○
Ich sende sensible Arbeitsdateien über ein öffentliches Wi-Fi-Netzwerk.	○	○	○	○	○	○
Ich achte darauf, dass Fremde meinen Laptop-Bildschirm nicht sehen können, wenn ich an einem sensiblen Dokument arbeite.	○	○	○	○	○	○

36. Bitte beurteilen Sie folgende Aussagen zum Umgang mit sicherheitsempfindlichen Datenträgern.

	stimme gar nicht zu	stimme eher nicht zu	unent-schieden	stimme eher zu	stimme voll zu	kann ich nicht beurteilen
Wenn sensible Ausdrucke entsorgt werden müssen, sorge ich dafür, dass sie geschreddert oder ordnungsgemäß vernichtet werden.	○	○	○	○	○	○
Ich würde einen USB-Stick, den ich an einem öffentlichen Ort gefunden habe, an meinen Arbeitscomputer anschließen.	○	○	○	○	○	○
Ich lasse Ausdrucke mit vertraulichen Informationen auf meinem Schreibtisch liegen, wenn ich nicht da bin.	○	○	○	○	○	○

37. Bitte beurteilen Sie folgende Aussagen zu Ihrem Verhalten bei IT-Sicherheitsvorfällen.

	stimme gar nicht zu	stimme eher nicht zu	unent-schieden	stimme eher zu	stimme voll zu	kann ich nicht beurteilen
Wenn ich sehen würde, dass sich jemand an meinem Arbeitsplatz verdächtig verhält, würde ich etwas dagegen unternehmen.	○	○	○	○	○	○
Wenn ich feststellen würde, dass eine mitarbeitende Person, die Sicherheitsvorschriften missachtet, würde ich nichts unternehmen.	○	○	○	○	○	○
Wenn ich einen Sicherheitsvorfall bemerken würde, würde ich ihn melden.	○	○	○	○	○	○

Seite 17

FK

38. Wie viele Mitarbeitende sind in Ihrem Unternehmen tätig?

[Bitte auswählen]

39. Wie viel Umsatz erwirtschaftet Ihr Unternehmen pro Jahr?

[Bitte auswählen]

40. In welcher Branche ist Ihr Unternehmen tätig?

[Bitte auswählen]

41. Wie oft bietet Ihr Unternehmen Schulung zum Thema IT-Sicherheit an?

[Bitte auswählen]

42. Ist die Teilnahme an diesen Schulungen freiwillig?

- Ja
- Nein
- Keine Angabe
- Ich weiß es nicht

43. Wie viel Budget wird pro Jahr für IT-Sicherheit ausgegeben?

In % vom Umsatz [Bitte auswählen]

44. War Ihr Unternehmen schon einmal von einer erfolgreichen Cyberattacke betroffen?

- Ja
- Nein
- Keine Angabe
- Ich weiß es nicht

45. Wurden in Ihrem Unternehmen schon einmal Daten durch eine Cyberattacke gestohlen?

- Ja
- Nein
- Keine Angabe
- Ich weiß es nicht

46. Entstand in Ihrem Unternehmen schon einmal ein finanzieller Verlust durch eine Cyberattacke?

- Ja
- Nein
- Keine Angabe
- Ich weiß es nicht

47. Falls es in Ihrem Unternehmen schon einmal ein finanzieller Verlust durch eine Cyberattacke entstand, wie hoch war dieser?

In % vom Umsatz pro Jahr

- 0-1%
- 1-2%
- 2-3%
- 3-4%
- 4-5%
- Mehr als 5%
- Keine Angabe
- Ich weiß es nicht

Seite 18

IT

48. Wird in Ihrem Unternehmen die Verwendung einer IT-Sicherheitssoftware vorgegeben?

- Ja
- Nein
- Keine Angabe
- Ich weiß es nicht

49. Wird in Ihrem Unternehmen IT-Sicherheitshardware verwendet (z.B. Hardware Firewall)?

- Ja
- Nein
- Keine Angabe
- Ich weiß es nicht

50. Wird sicherheitsrelevante Hardware (z.B. Server, Computer, Tablets) physisch gesichert?

Kreuzen Sie Zutreffendes an.

- [ ] Räumliche Trennung
- [ ] Zugang nur mit Karte
- [ ] Zugang nur mit PIN
- [ ] Zugang nur über biometrische Erkennung (z.B. Fingerabdruck)
- [ ] Videoüberwachung der Hardware
- [ ] Andere
- [ ] Keine der genannten Optionen
- [ ] Keine Angabe
- [ ] Ich weiß es nicht

51. Verwendet Ihr Unternehmen im Bereich Personalverwaltung Cloud Technologie?

- ( ) Ja
- ( ) Nein
- ( ) Keine Angabe
- ( ) Ich weiß es nicht

52. Verwendet Ihr Unternehmen im Bereich Personalverwaltung eine künstliche Intelligenz?

- ( ) Ja
- ( ) Nein
- ( ) Keine Angabe
- ( ) Ich weiß es nicht

53. Verwendet Ihr Unternehmen ein Security Operations Center*?

*Ein zentraler Knotenpunkt für Steuerung und Überwachung der IT-Sicherheit

- ( ) Ja
- ( ) Nein
- ( ) Weiß ich nicht
- ( ) Keine Angabe
- ( ) Ich weiß es nicht

54. Welche Arten von Cyberattacken oder Angriffe auf Informationsträger erfährt Ihr Unternehmen?

Zutreffende bitte ankreuzen

- ☐ Physischer Schaden
- ☐ Innentäter/ -in
- ☐ Identitätsdiebstahl
- ☐ Cyber-Spionage
- ☐ Exploit Kits
- ☐ Denial of Service
- ☐ Botnets
- ☐ Spam
- ☐ Phishing (durch Mail, oder Messengerdienste)
- ☐ Ransomsoftware
- ☐ Übertragung durch private IT im/aus dem Homeoffice
- ☐ Nutzung von Fremd-IT (angemietet, Testgeräte, Schatten-IT)
- ☐ Andere
- ☐ Keine Angabe
- ☐ Ich weiß es nicht

55. Wie viele Cyberattacken registrieren Sie in Ihrem Unternehmen pro Woche?

- ○ 0-10
- ○ 10-50
- ○ 50-100
- ○ 100-200
- ○ 200-300
- ○ Mehr als 300
- ○ Ich weiß es nicht
- ○ Keine Angabe

Letzte Seite

Vielen Dank für Ihre Teilnahme!

Wir möchten uns ganz herzlich für Ihre Mithilfe bedanken.

Bei Fragen zum Forschungsprojekt FLEIS, oder um die Ergebnisse dieser Studie zu erhalten, wenden Sie sich bitte an Frau Dr. Rudel.

Projektleiterin Federated Learning Enhancing IT Security (FLEIS)

Fakultät für Informatik Institut für Schutz und Zuverlässigkeit

Universität der Bundeswehr München

Werner-Heisenberg-Weg 39

85577 Neubiberg

Steffi.Rudel@unibw.de

Bei Fragen, oder Anmerkungen zu dieser Erhebung wenden Sie sich bitte an Leutnant Schwarz.

Universität der Bundeswehr München

Werner-Heisenberg-Weg 39

85577 Neubiberg

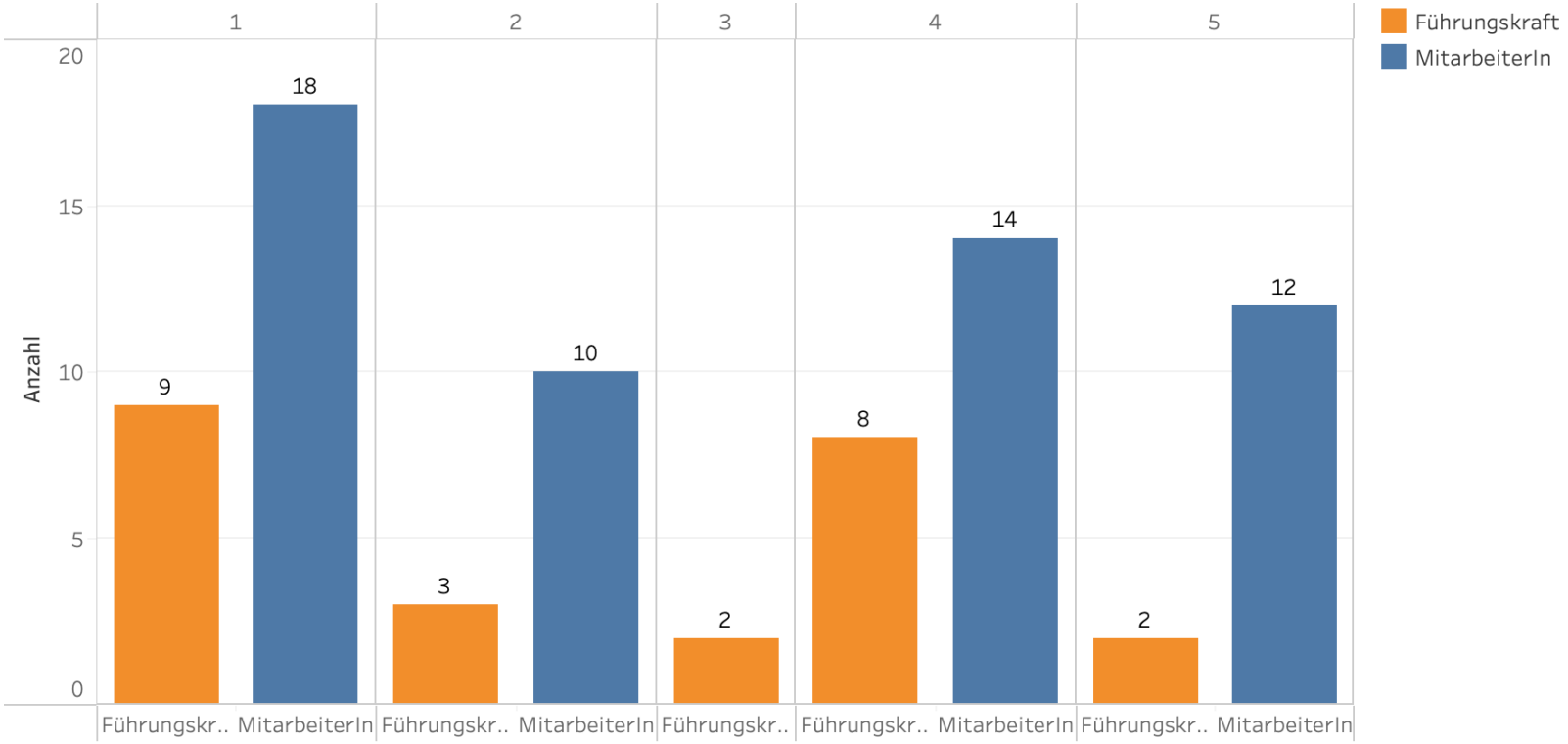
Leon.Schwarz@unibw.de

Ihre Antworten wurden gespeichert, Sie können das Browser-Fenster nun schließen.

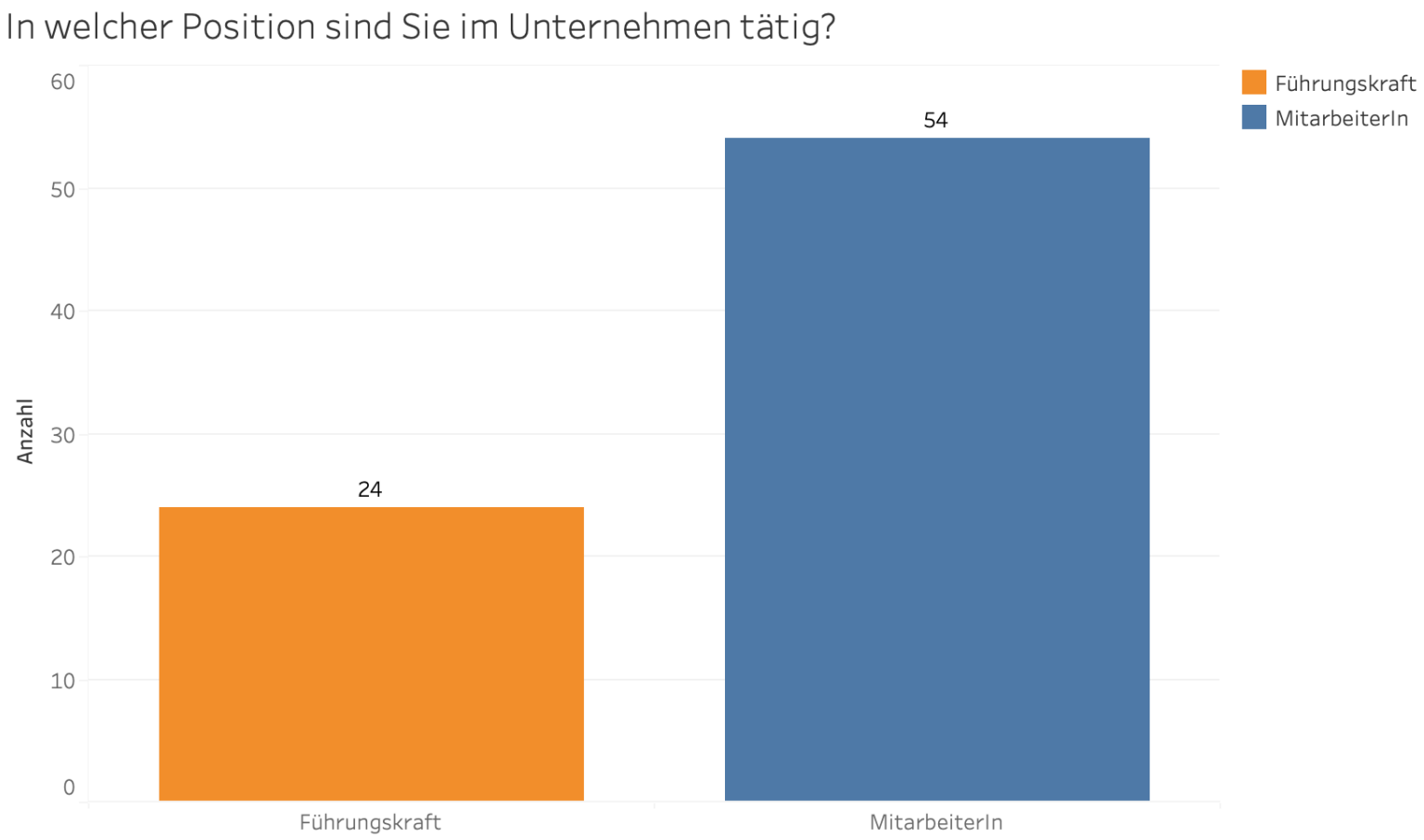
E

EN01_10

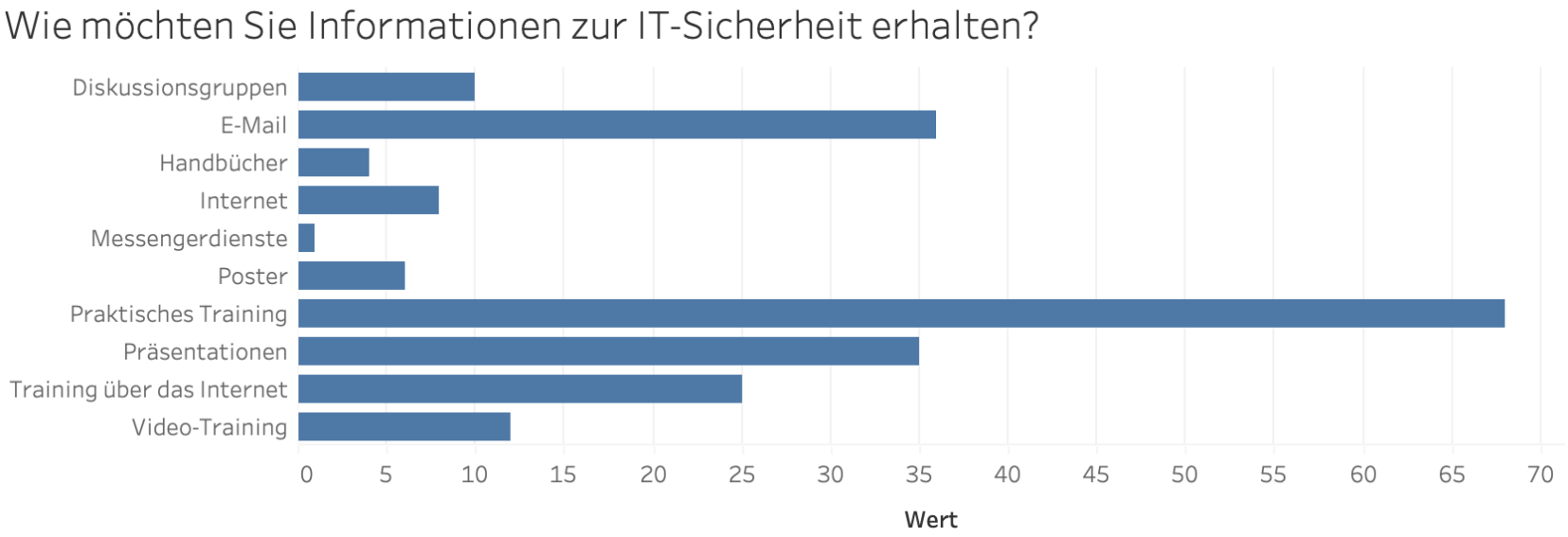
Wenn eine E-Mail von einem unbekannten Absender interessant aussieht, klicke ich auf den Link in der E-Mail.



FI01

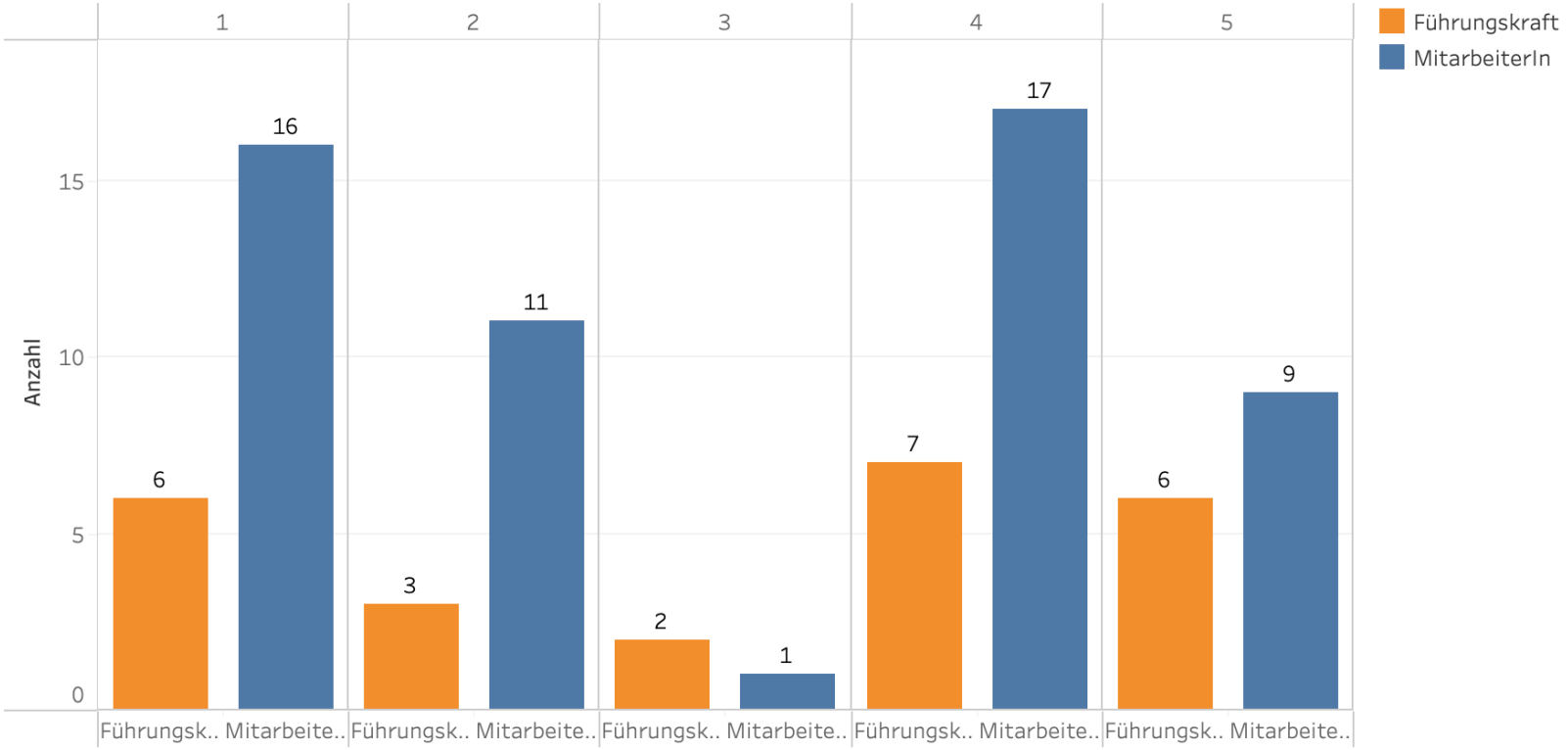

In welcher Position sind Sie im Unternehmen tätig?
Führungskraft
MitarbeiterIn
Anzahl
60
50
40
30
20
10
0
24
54
Führungskraft
MitarbeiterIn

H204


Wie möchten Sie Informationen zur IT-Sicherheit erhalten?
Diskussionsgruppen
E-Mail
Handbücher
Internet
Messengerdienste
Poster
Praktisches Training
Präsentationen
Training über das Internet
Video-Training
0
5
10
15
20
25
30
35
40
45
50
55
60
65
70
Wert

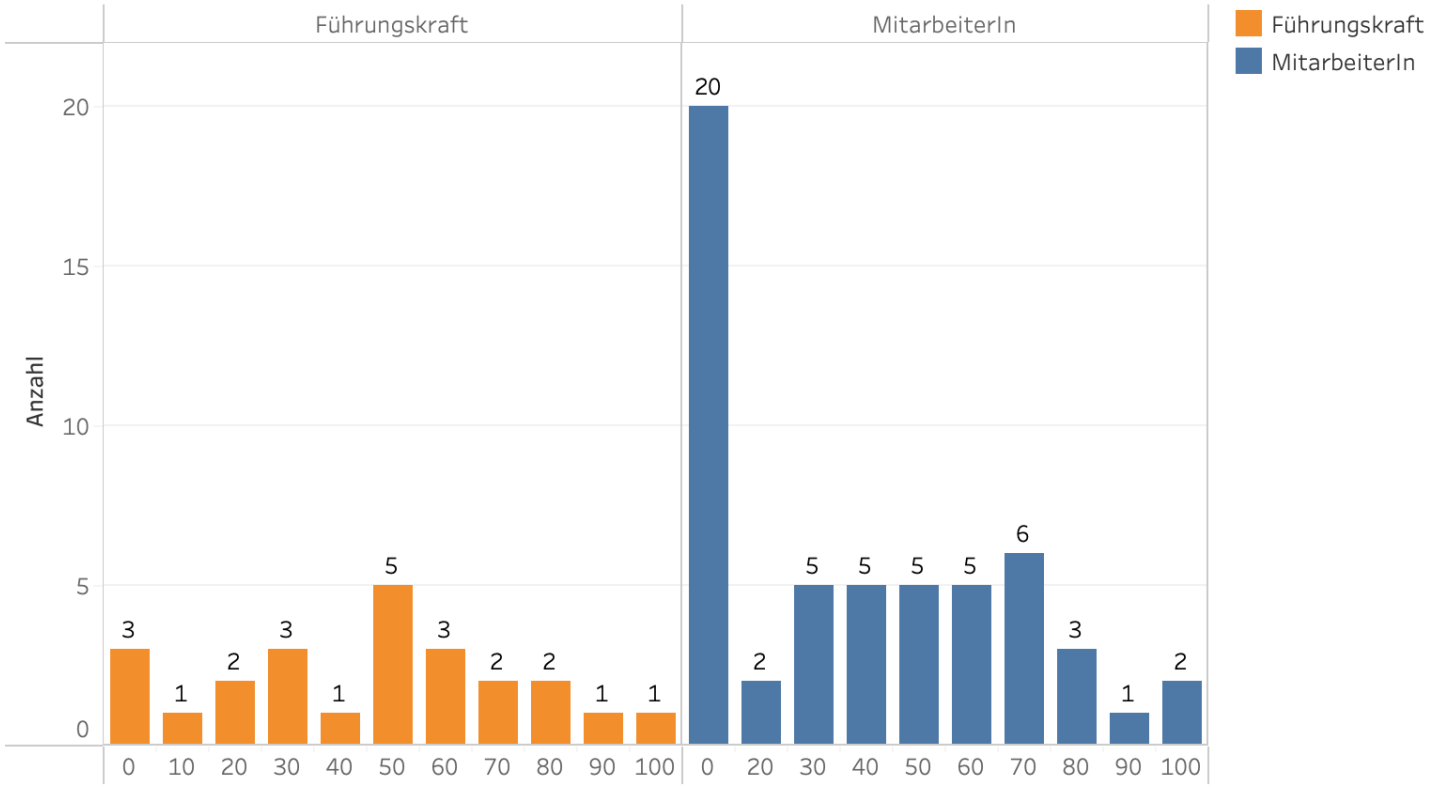
NI02_11

Ich bin bereit, meine Arbeitspraktiken zu ändern, um die Sicherheit von Informationsgütern zu gewährleisten.



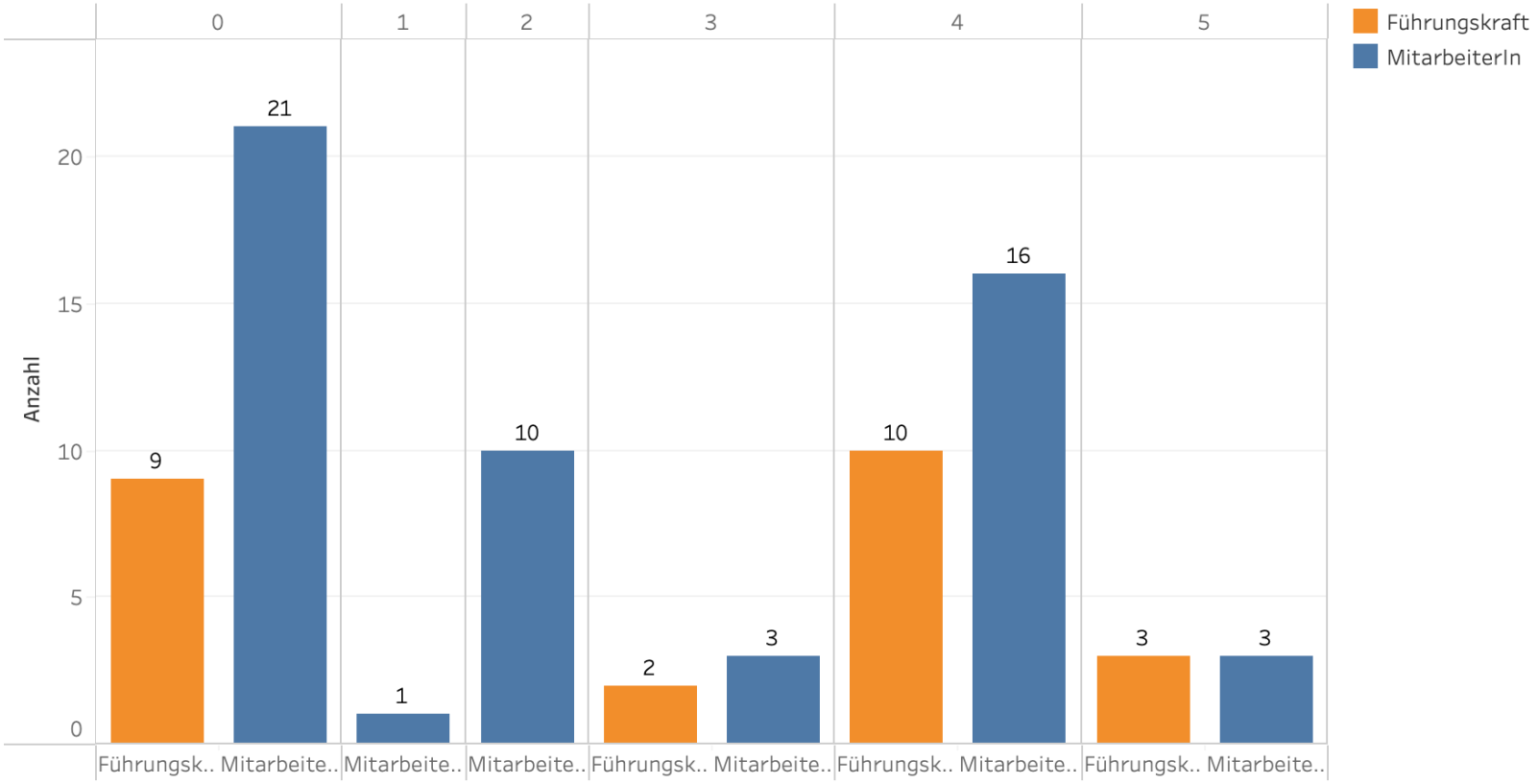
SE03

Zu wie viel % sind Sie sicher, den Unterschied zwischen IT-Sicherheit und Datenschutz erläutern zu können?



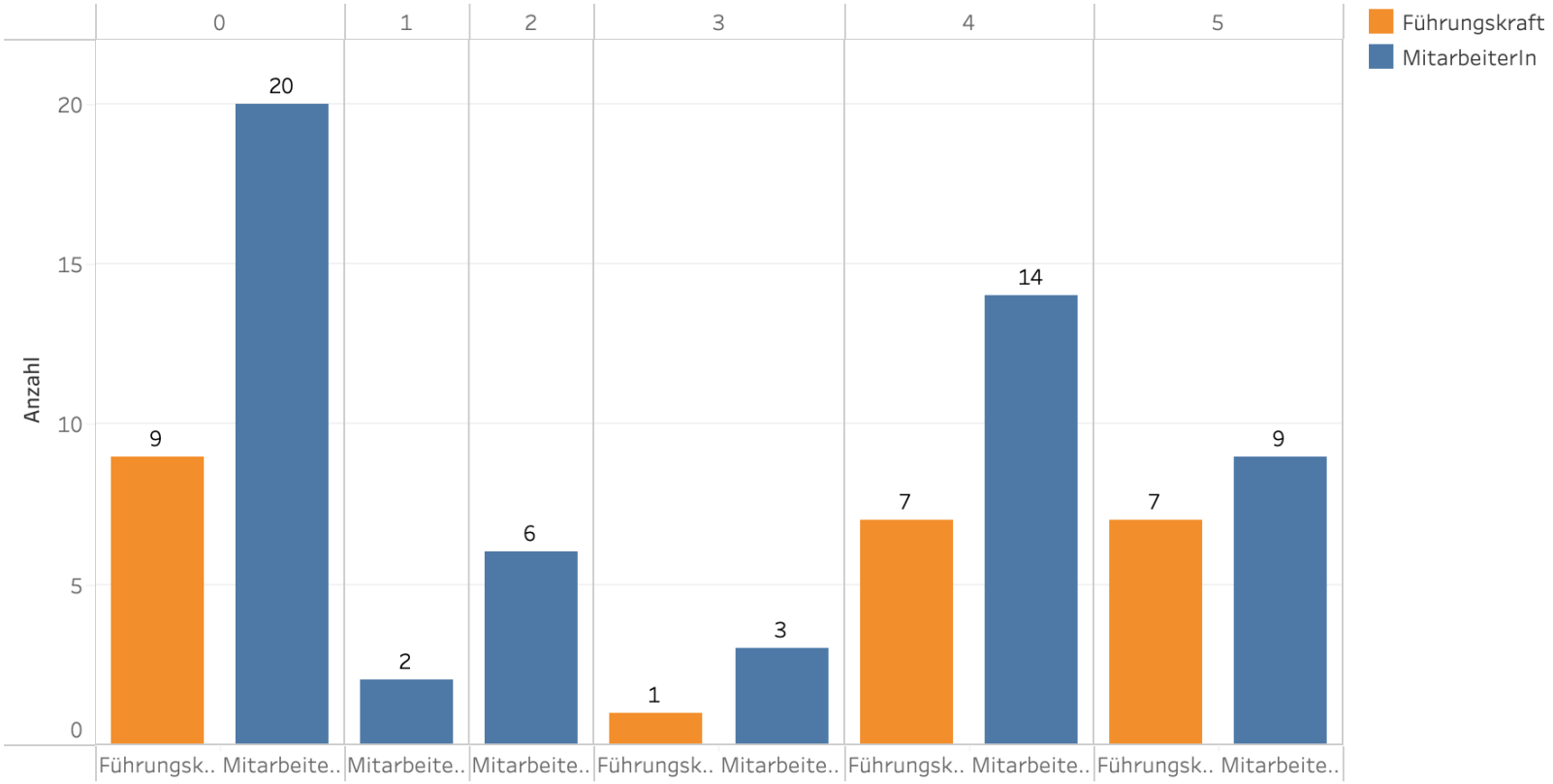
SR01_01

Der Inhalt unserer IT-Sicherheitsrichtlinie ist leicht verständlich.



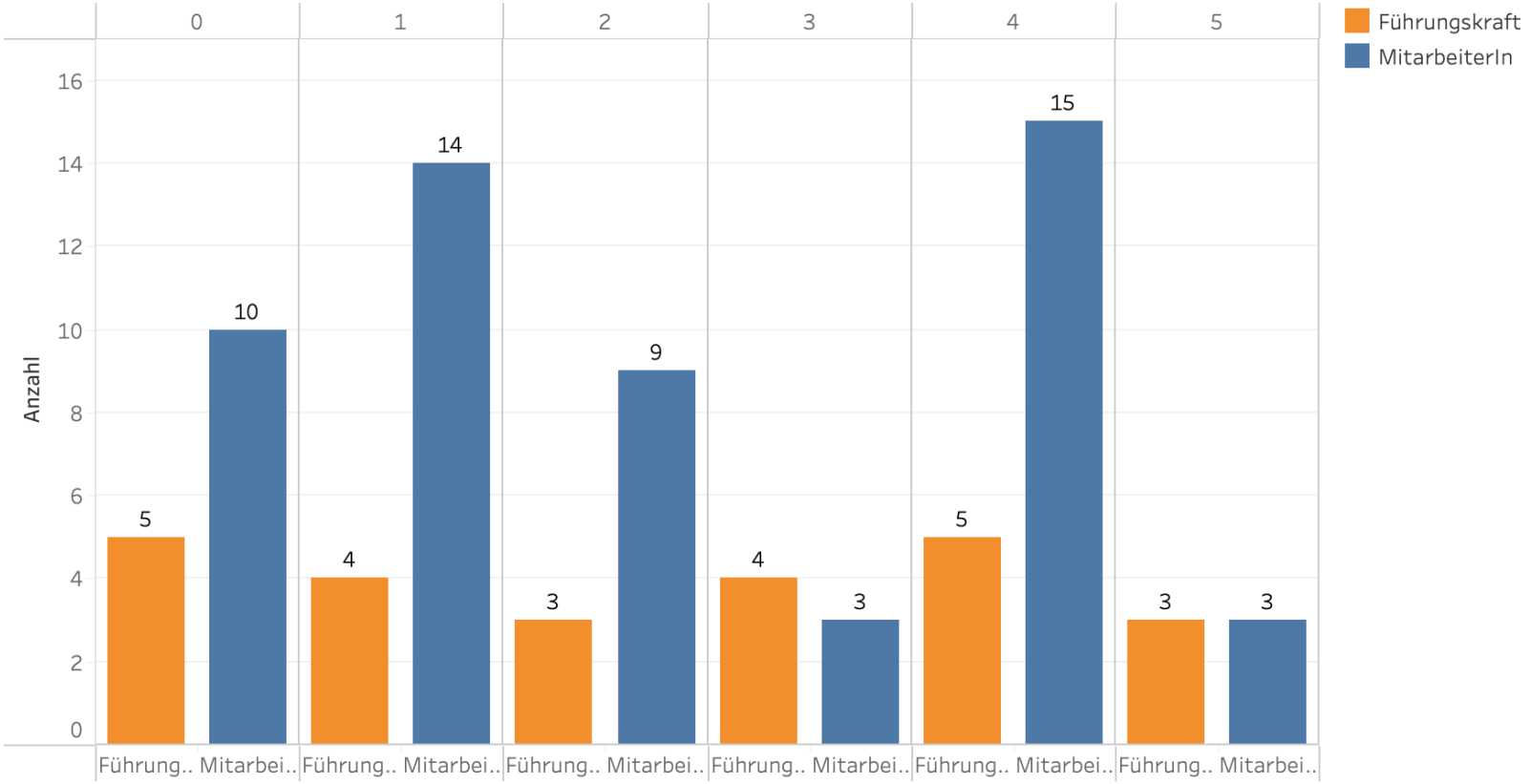
SR01_02

Ich glaube dass unsere IT-Sicherheitsrichtlinie umsetzbar sind.



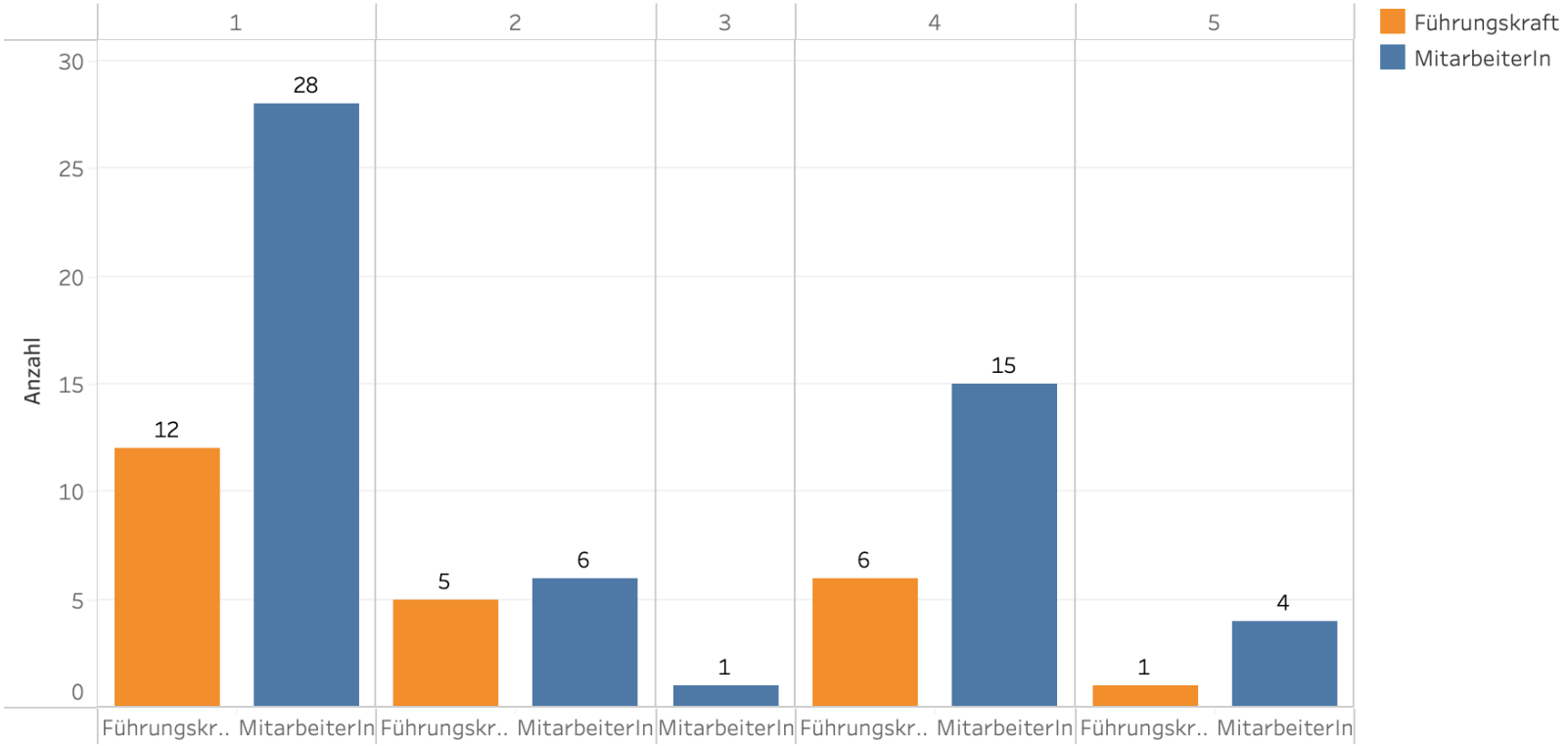
SR01_04

Der Inhalt unserer IT-Sicherheitsrichtlinie wurde mir wirksam vermittelt.



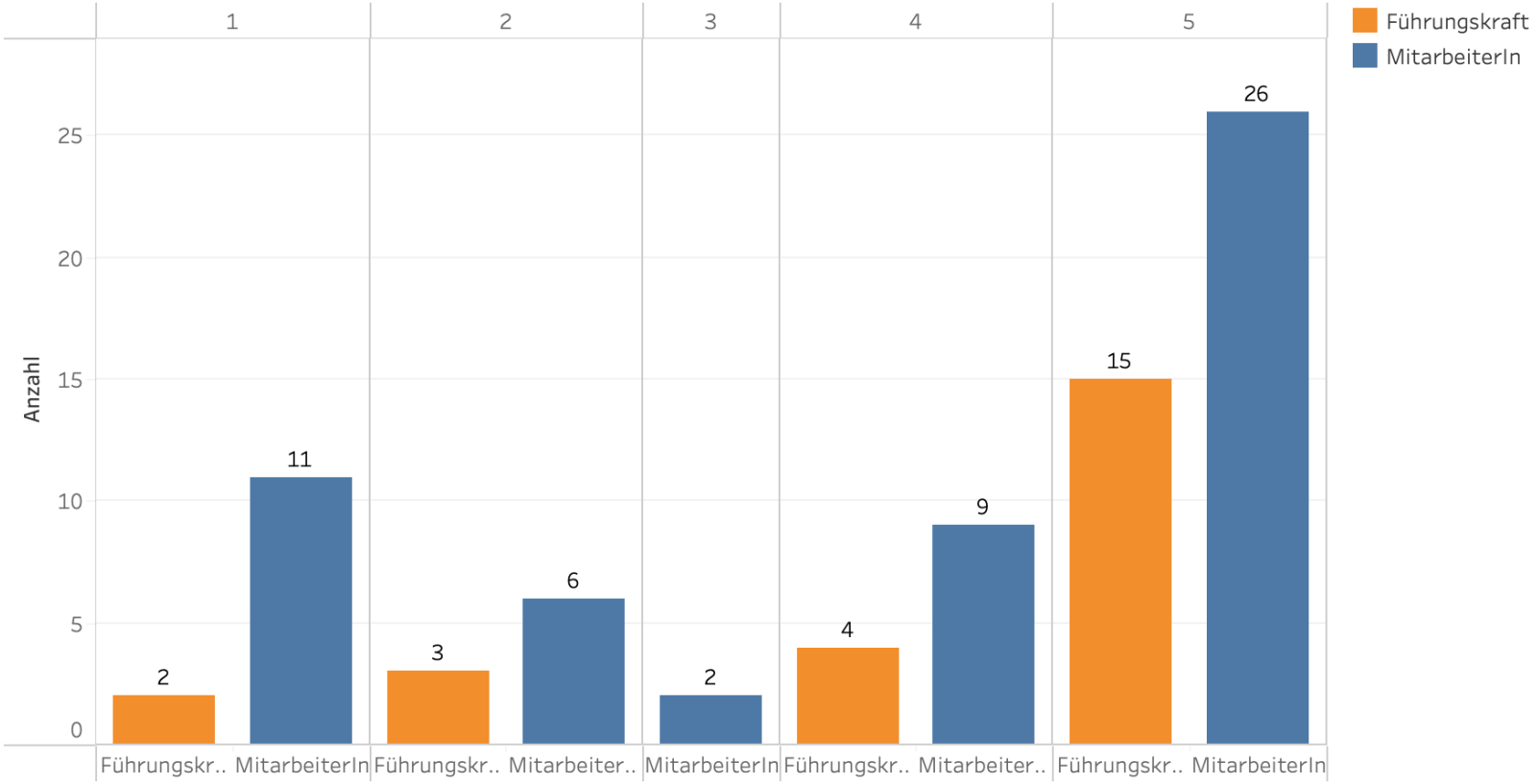
UI01

Ich würde einen USB-Stick, den ich an einem öffentlichen Ort gefunden habe, an meinen Arbeitscomputer anschließen.



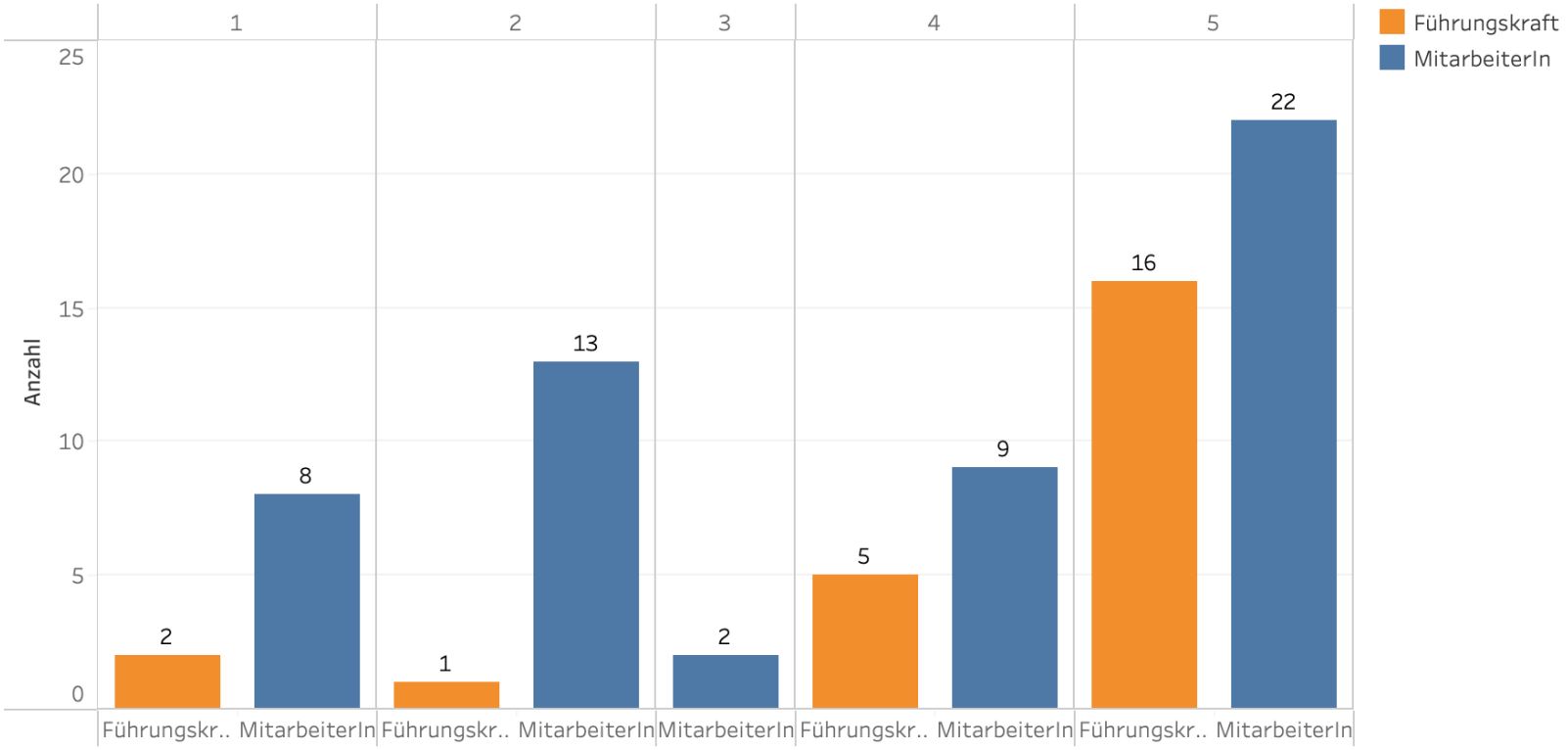
VI01_01

Die IT-Sicherheit muss durch ein formelles System geregelt werden.



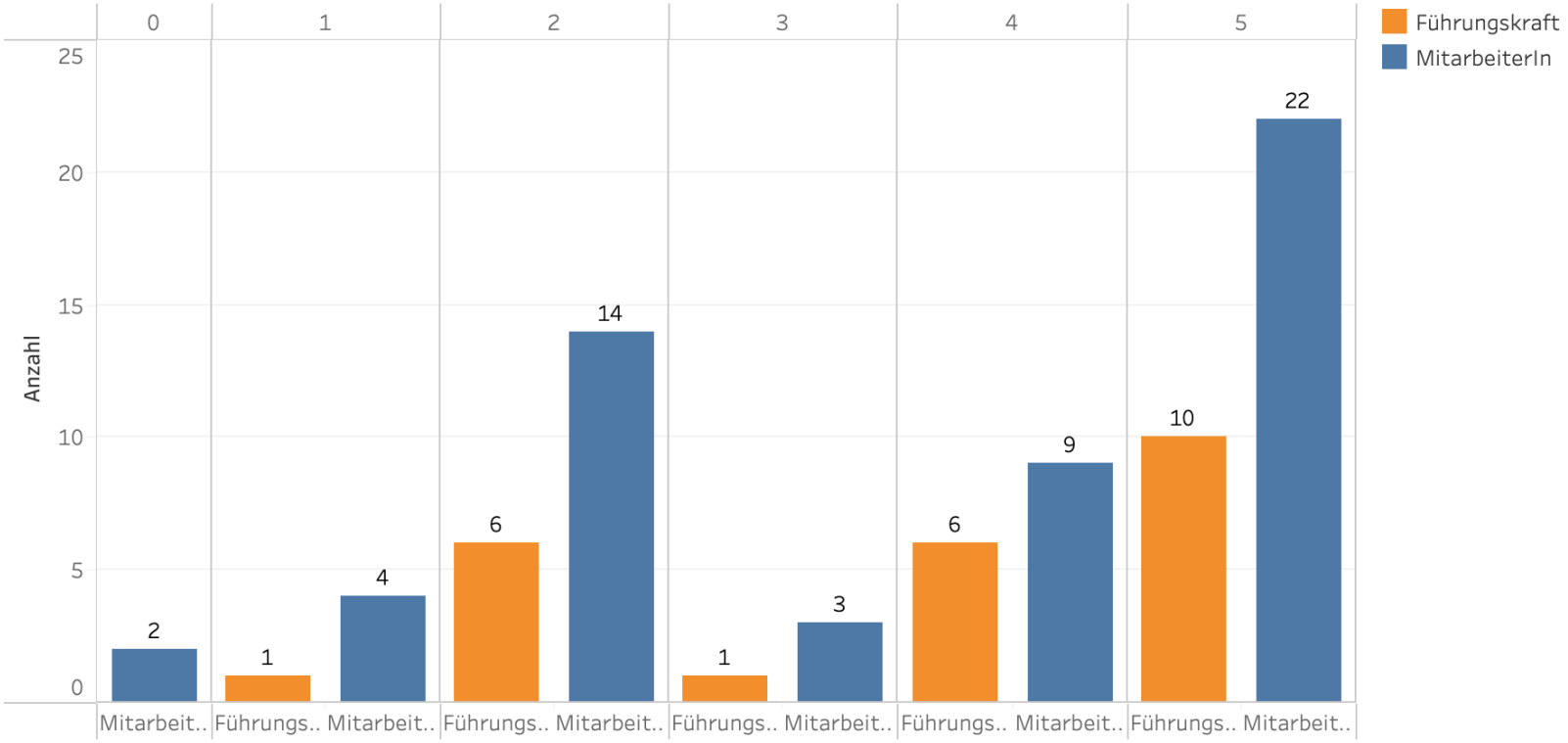
VI01_07

Ich bin der Meinung, dass zusätzliche Schulungen für den Einsatz von IT-Sicherheitsinstrumenten erforderlich sind, um Informationen zu schützen.



VP01_12

Mein Unternehmen hat klare Richtlinien zum Schutz sensibler/vertraulicher Daten von Mitarbeitenden.



F

Recherche HRM-Startups

Name	Referenz	Kategorie	Kurzbeschreibung	Link	Zahlender Kunde?	Einnahmestrang
Lotaro	PM 11/23	Coaching, Learning und Development	Trainingsplattform für hochwertige interaktive People-Skill-Trainings (virtuelles Training in Kleingruppen)	https://www.lotaro.de/	Unternehmen	n.A.
Cvift	PM 10/23	Recruiting und Zeitarbeit	Cvift ist eine auf passive IT- und Tech-Talente spezialisierte Candidate Conversion Plattform.	https://www.cvift.com/	Suchendes Unternehmen (Registrierung für Kandidaten kostenfrei)	n.A.
Znapp	PM 9/23	Recruiting und Zeitarbeit	Znapp ist wie Tinder für Jobs und verfolgt das Konzept des Reverse Recruiting (Plattform, Unternehmen bewerben sich bei Talenten)	https://znapp.de/informationen_fuer_arbeitgeber/preise	Suchendes Unternehmen (Registrierung für Kandidaten kostenfrei)	Kontaktanfrage an interessanten KandidatIn kostenfrei, wenn ok gibt: 9,95 EUR
Hintbox	PM 8/23	HR-Management	Ein digitales Hinweisgebersystem zum einfachen, sicheren und vor allem vertraulichen Empfangen von Meldungen (Unternehmen > 50 MA sind dazu verpflichtet, so ein Meldesystem einzubauen, um Misstände im Unternehmen aufzudecken oder zu verhindern); zusätzlich: Complience-Suite	https://www.hintbox.de/	Unternehmen	Monatliche Gebühr, abhängig vom Paket und Anzahl Mitarbeitende im Unternehmen
Baito	PM 7/23	Recruiting und Zeitarbeit	Plattform mit Job-Angeboten im Impact-Segment („singstiftende Arbeit“, z.B. Umweltschutz, Gesellschaft)	https://www.getbaito.com/de	Suchendes Unternehmen	Pro Anzeige 119,- bis 499, EUR
Robyyn Good	PM 6/23	Recruiting und Zeitarbeit	Recruiting-Plattform, die Arbeitgebern einen Zugang zu Arbeitnehmerinnen und Arbeitnehmern in Festanstellung (die sich vorher regestriert haben) bietet, die nicht aktiv einen neuen Job suchen.	https://www.robyyngood.com/	Suchendes Unternehmen	Von 0,- EUR - 999,- EUR / BenutzerIn / Jahr
Cerfif-ID	PM 5/23	HR-Management	Fachkräftelücke in Deutschland schließen, indem der Migrationsprozess von Expertinnen und Experten digitalisiert wird (z.B. Zeugnisse aus Indien digital mittels Blockchain bestätigen). Betreiben: https://talentsure.io/ und https://credsure.io/	https://certif-id.com/	—	—
CredSure	Cerfif-ID	HR-Management	Plattform, die PDF-Zertifikate auf Blockchain-Basis zur Verfügung stellt	https://credsure.io/	Unternehmen und Endkunden	Ab 920,- EUR / Jahr
TalentSure	Cerfif-ID	Recruiting und Zeitarbeit	Plattform, die Talente für Gesundheitsbranche aus dem Ausland nach D. vermittelt	https://talentsure.io/	Unternehmen	„Individuelles Angebot“
Ravio	PM 4/23	HR-Management	Bieten Echtzeit-Gehaltsübersichten zur Entwicklung von Gehaltsmodellen, indem sie sich direkt an HR-Systeme ankoppeln.	https://ravio.com/	Unternehmen	n.A.
Hidden Smiles	PM 3/23	Feedback	SaaS-Lösung, die Feedback-Kultur im Unternehmen etabliert. MA sollen sich wertgeschätzt fühlen.	https://hidden-smiles.com/	Unternehmen	n.A.

Name	Referenz	Kategorie	Kurzbeschreibung	Link	Zahlender Kunde?	Einnahmestrang
Empion	PM 2/23	Recruiting und Zeitarbeit	Automatisiertes Headhunting-System mittels der „Empion-Methode“ (KI-gestützt, steht Promotion dahinter)	https://empion.io/	Suchendes Unternehmen (Registrierung für Kandidaten kostenfrei)	n.A.
Pair To Share	PM 1/23	Recruiting und Zeitarbeit	Recruiting- und Matching-Plattform für Stellen im Jobsharing-Modell.	https://www.pairtoshare.com/de	n.A.	n.A.
Heynannyly	PM 12/22	HR-Management	On-Demand-Plattform für Kinderbetreuung (vermittelt im Auftrag von Unternehmen schnell verfügbare & qualifizierte Nannys)	https://www.heynanny.com/	Unternehmen für Ihre MA (Registrierung für Nannys kostenfrei)	Plattform mit Service-Vorteilen für MA des Unternehmens einkaufen; optional: Nanny-Stunden als Guthaben für MA kaufen (Steuerfrei)
Fount	PM 11/22	Feedback	SaaS-Lösung, die Unternehmen helfen soll zu verstehen, wo die MA schlechte Erfahrung bei der Arbeit machen. Basiert auf TI People (https://www.ti-people.com/)	https://getfount.com/	n.A.	Preise nicht angegeben
Crewting	PM 10/22	Feedback	SaaS-Lösung, die Mitarbeiterzufriedenheit misst und steuert, Web-basiert, speziell für hybrides Arbeiten.	https://www.crewting.de/	Unternehmen	Gestaffelt nach Unternehmensgröße, 30-Tage-Test kostenlos. Preise nicht angegeben
HRtbeat	PM 9/22	Recruiting und Zeitarbeit	Agentur für digitales Recruiting und Employer Branding; Teil der Vogel Communications Group	https://hrtbeat.com/	Unternehmen	Preise nicht angegeben
Giveajoy	PM 8/22	Andere Start-ups	Kleine Aufmerksamkeiten & Weihnachtskörbe für MA, Steuerfrei	https://giveajoy.de/	Unternehmen	Gebühr pro Geschenkebox
Club of Code	PM 7/22	Recruiting und Zeitarbeit	Recruiting-Plattform, spezialisiert auf Softwareentwickler	https://clubofcode.io/	Suchendes Unternehmen (Registrierung für Kandidaten kostenfrei)	Preise nicht angegeben
Twise	PM 6/22	?	Will mehr Frauen in die Führung bringen	https://www.twise.eu/	Für Bewerbende kostenfrei. Unternehmen zahlen für verschiedene Dienstleistungen	Preise nicht angegeben
Viind	PM 5/22	HR-Management	Anfangs Recruiting via Whatsapp und co., jetzt DSGVO-Konforme Kommunikation mit Unternehmen oder Behörden über WhatsApp etc., Nutzung von Chatbots; online oder on-premise möglich.	https://www.viind.com/	Unternehmen	Preise nicht angegeben
Planco	PM 4/22	HR-Management	Soll Schichtarbeitende vernetzen, um die Organisation des Alltags einfacher zu machen.	Auch nach intensiver Suche nicht auffindbar	—	—
HR for Startup	PM 3/22	Andere Start-ups	Videoplattform für KMU, um sich in HR einzuarbeiten	https://hrforstartup.de/	n.A.	n.A.

Name	Referenz	Kategorie	Kurzbeschreibung	Link	Zahlender Kunde?	Einnahmestrang
Talentbay	PM 2/22	Recruiting und Zeitarbeit	Recruiting- und Matching-Plattform im Tinder-Stil zwischen Studierenden und Unternehmen; inzwischen in Belgien ansässig	https://talentbay.be/	n.A.	n.A.
HR Tech Consulting	PM 1/22	People Analytics	Dienstleistungen für HR im Unternehmen.	https://hr-tech.de/	Unternehmen	n.A. (wahrscheinlich individuell)
Recunited	PM 12/21	Recruiting und Zeitarbeit	Wertebasierte Jobplattform: Einordnung anhand eines Tests, ob cultural Fit passt.	https://recunited.com/	n.A.	Keine Preise angegeben
Onesome	PM 11/21	Coaching, Learning und Development	Digitaler Coach für Persönlichkeitsentwicklung per App	https://onesome.de/	Unternehmen	Keine Preise angegeben
My Lui	PM 10/21	HR-Management	MyLUI ist der persönliche Sprachassistent für das digitale Aufgaben- und Terminmanagement Ihrer MitarbeiterInnen.	https://iwos.io/	n.A.	Keine Preise angegeben
Independendesk	PM 9/21	—	Arbeitsplätze an alternativen Orten zur Verfügung stellen	insolvent	—	—
Voice of Jobs	PM 8/21	Recruiting und Zeitarbeit	Spezielle Job-Börse	https://www.voiceofjobs.de/	Suchendes Unternehmen	Je nach gewünschtem Service: https://www.voiceofjobs.de/preisliste
Monday Rocks	PM 7/21	Coaching, Learning und Development	Software für Teamführung	https://www.monday.rocks/	Nutzendes Unternehmen	„Die Kosten setzen sich zusammen aus einer einmaligen Gebühr für das Onboarding, einer Empowerment Gebühr für die Begleitung der Teams im ersten Jahr (alternativ werden Ihre eigenen hausinternen „Teamentwickler“ oder Coaches geschult) und einer monatlichen SaaS-Lizenz je User (Mitarbeiter*in).“ https://www.monday.rocks/loesung/
Copetri	PM 6/21	Andere Start-ups	Plattform für People, Transformation und Innovation. Workshops, Podcasts, Messen etc.	https://www.copetri.com/	Mehrere	Plattform
Storybox	PM 5/21	HR-Management	Erstelle mit deinem Team einfach und schnell qualitativ hochwertige Videos für den gesamten HR-Prozess (B2B-SaaS)	https://storybox.cloud/	Nutzendes Unternehmen	Keine Preise angegeben
Entwicklerheld	PM 4/21	Andere Start-ups	Coding-Plattform, um zu üben, Coins zu verdienen und Arbeitsproben zu liefern.	https://entwicklerheld.de/	Für Bewerbende kostenfrei, können sogar am schreiben des Codes verdienen. Unternehmen zahlen für verschiedene Services.	Preise nicht angegeben
Auto.mates	PM 3/21	HR-Management	Automatisierung von Routine-Aufgaben für MA SaaS	https://auto-mates.de/	Nutzendes Unternehmen	Diverse Leistungen für verschiedene Preise: https://auto-mates.de/unser-angebot/

Name	Referenz	Kategorie	Kurzbeschreibung	Link	Zahlender Kunde?	Einnahmestrang
Culcha	PM 2/21	Coaching, Learning und Development	App, die bei Verhaltensänderung unterstützen soll (Digitale Transformation)	https://www.culcha.com/	Nutzendes Unternehmen	Ab 19,- EUR / nutzendem User (https://landing.culcha.com/de/pricing/scale-ups) bis ca. 1200,- / Nutzer (https://www.culcha.com/produkt/preise)
Parrotpolls	PM 1/21	Feedback	Aufgegangen in Crunchmetric. Stimmungsbarometer für High-Performance-Teams.	Crunchmetric.com	Nutzendes Unternehmen	Zwischen 15,- und 25,- EUR / Team / Monat: https://www.crunchmetric.com/
Mehrsalz	PM 12/20	HR-Management	HR-Beratungen für Projekte, z.B. SAP	https://www.mehrsalz.de/	Unternehmen	Individuell
Applaudio	PM 11/20	Feedback	App, um gegenseitige Anerkennung & Wertschätzung unter MA (peer-to-peer) zu dokumentieren; kann vom Unternehmen monetär hinterlegt werden.	https://applaudio.de/	Nutzendes Unternehmen	Abhängig von Nutzer-Anzahl: https://applaudio.de/
People Tree	PM 10/20	HR-Management	HR-Beratung für Veränderungsprojekte, Planung und Durchführung von Umfragen oder Pulse Checks, Unterstützung beim Etablieren einer Fehlerkultur oder auch bei der Einführung einer App für die Beschäftigten.	Auch nach intensiver Suche nicht auffindbar	—	—
Jobmatch Pro	PM 9/20	Recruiting und Zeitarbeit	„Online-Partnerbörse für Jobs“, Online-Plattform zum Matching im Recruiting, im Stil von Parship	https://jobmatch.pro/	Suchendes Unternehmen	Monatsgebühr abhängig von gewählter Leistung; oder: kostenfrei, bei Einstellung 22% des ersten Jahresgehaltes: https://jobmatch.pro/preise
superheldin.io	PM 8/20	Recruiting und Zeitarbeit	Recruting-Portal speziell für Mütter	https://www.superheldin.io/	Ausschreibendes Unternehmen	Fixgebühr pro Monat ab 4000,- EUR (mind. 3 Monate Laufzeit): https://unternehmen.superheldin.io/home#preise
Maxmatch	PM 7/20	Recruiting und Zeitarbeit	Personalberater speziell für die Bereiche Finance, Tax, Audit, Legal und Real Estate	https://maxmatch.de/	Suchendes Unternehmen	Gebühr pro vermittelter Fachkraft, richtet sich nach Jahreseinkommen der Fachkraft
Spendesk	PM 6/20	HR-Management	Lösung zum Finanzmanagement, z.B. Reisekosten und andere Ausgaben der MA	https://www.spendesk.com/de/	Unternehmen	Gebühr abhängig von Unternehmensgröße und gewünschten Services (keine Preise angegeben): https://www.spendesk.com/de/pricing/
Limpala	PM 5/20	Coaching, Learning und Development	Führungskräfteentwicklung online	https://limpala.de/	Unternehmen	Pro Führungskraft, keine Preise angegeben
Studie HR-Startups	PM 4/20	—	—	—	—	—
Lubu	PM 3/20	Andere Start-ups	Vernetzt MA mittels einer App im virtuellen Café	https://lubu-app.com/de/home/	Unternehmen	Preismodell richtet sich nach Unternehmensgröße und gewünschten Services (Preise nicht angegeben): https://lubu-app.com/de/home/#pricing
Lytt / Evermood	2/20	Coaching, Learning und Development	Anonyme Meldungen im Unternehmen abgeben (Lytt). Jetzt ergänzt um Coaching zur mentalen Gesundheit und Gesundheitsförderung in der App (Evermood)	https://www.evermood.com/	Unternehmen	Preismodell richtet sich danach, was in der App alles mit drin sein soll (Preise nicht angegeben): https://www.evermood.com/plans

Name	Referenz	Kategorie	Kurzbeschreibung	Link	Zahlender Kunde?	Einnahmestrang
Deskcloud	1/20	HR-Management	Mobile und flexible Arbeitsplatzlösungen mit App buchbar	https://joindeskcloud.com/	Unternehmen; Startups & Freiberufler; Anbieter Co-Working-Spaces können sich kostenfrei registrieren	Startups ab 19,99 pro Monat, Gemietete Arbeitsplätze kommen dazu. Unternehmen ab 199,-EUR pro MA: https://joindeskcloud.com/loesungen-fuer-coworking/

G

The Business Model Canvas - Studenten (05.06.2023)

Key partners

- Netzwerkprovider
- E-Mail-Provider
- Berater (IT-Sicherheit) die Produkt empfehlen
- Werbepartner (Zeitschriften, Influencer)
- Produkttester

Key activities

- Software (Wartung, Auslieferung...)
- Kundenerhalt, Werben von Kunden, Anwenderschulung neuer Kunden
- Testphasen durchführen
- Modell regelmäßig updaten und evaluieren
- KPIs erstellen und messen

Key resources

- Finanzielle Mittel
- Daten für Training der Modelle
- Server /Hardware (innerhalb der EU)
- Fachpersonal (Entwicklung, Betrieb) IT, KI
- Marketing-personal (Kunden-kontakt) mit Ahnung von IT-Sicherheit (kein Callcenter)

Key propositions

- Weiter-entwicklung des Portfolios
- Neues System, Mehrwert an Sicherheit
- Erweiterung des Modells; Profitieren von anderen und weiterer Kenntnissaufbau
- E-Mail Provider kann damit werben, Zustz gegenüber anderen Prividern
- E-Mail Provider können selber ein zusätzliches Feld an Kunden ansprechen
- KMU: höherer Sicherheitsaspekt, schließen von Sicherheitslücken durch große Gruppe, die Modell trainiert
- Privatmarkt wie KMU

Customer relationships

- Support, Ansprechpartner
- Support B2B
- bei allen längerfristige Bindung
- Support, Ansprechpartner
- Support, Service-Hotline

Channels

- Über den Betreuer, per Mail oder Telefon; Innovation ohne Aufpreis für den Kunden, zum Trainieren des Initalmodell nutzen
- Direktes Marketing betreiben, direkten Kontakt suchen,
- Werbung, Add-Ons schalten, über andere Bestandskunden (Anreize setzen)
- Youtube oder Influencer

Customer segments

- Bestandskunden
- E-Mail-Provider (Add-on zu Mail-Programm) --> eher kleinere Provider, deren Kunden auf IT-Sicherheit wert legen
- KMU/ Selbstständige
- Kundengruppen, die sich sowieso mit IT-Sicherheit beschäftigen und Interesse an ihrer Sicherheit haben bzw. darauf wert legen müssen (rechtlich)
- Privatmarkt

Cost Structure

- Entwicklungskosten
- Infrastruktur
- Marketing, Werbekosten
- Personalkosten

Revenue Streams

- Zahlen bereits, habe Lizenzen. Mehr Geld nur wenn es wirklich einen Sicherheitsnutzen bringt. Preise gleich oder maximal 5-10%.
- Verhandlung, Wie teuer wollen die Provider es an ihre Kunden vermarkten? Bestimmter Anteil vom Gewinn
- Lizenzen verkaufen, nicht zwingend den Pries erhöhen im Vergleich zu Bestandskunden
- Kostenlose Version mit Einschränkungen in der Nutzung des Systems (z.B. nur 1x/Monat abgleich mit Zentralem Modell)
- Erster Zeitraum günstiger?

Source: Strategyzer AG | License: CC By-SA 3.0

The Business Model Canvas (04.07.2023)

Key partners

- Key-Kunden (erste Kunden, die mit Entwickeln und das System nach außen tragen)
- Personalberater
- Training mittels "to go" mit Virenscanner hinterlegt (--> über Standard itWess)
- Software-Hersteller (Branchen-spezifisch, z.B. Persiono)

Key activities

- Generierung der Startkunden für Basismodell
- Referenzkunden aufbauen

Key propositions

- ITWESS / ITWESS.AI → Gruppierung nach - Abteilung -Branche -Prozessen (Global Modell "Federation")
- ITWES "to go".AI für kleine Kunden (größere Datenmenge zum Anlernen)
- Differenzierte Einschätzung einer Bedrohung als JA/NEIN
- Trainingserfahrungen durch mehrere am Projekt teilnehmende Unternehmen
- Mehr Sicherheit für Abteilungen bei der Kommunikation mit Externen
- Betreuung+ Retraining automatisiert (immer aktuell)

Customer relationships

- über Portal (unpersönlich)
- persönlicher Kundenkontakt zum Einkäufer/ Fachabteilung

Customer segments

- Viele kleine Kunden
- Alle Abteilungen mit viel externen Kommunikation und sensiblen Daten
- "Großkunden" mit vielen Lizenzen
- "Gruppierungen"

Key resources

- Experten zur Überprüfung
- KI-Modell
- Sicherer Server (Standort)
- Erste Kunden
- FL-Server (Miete/Betrieb)

Channels

- Neukunden: Meme (ITSA, mit Demo Use-Case), Virtuelle Meme, Online-Veranstaltung
- Bestandskunden: Vertrieb

Cost Structure

- Einige Experten
- Weiter-entwicklung + Optimierung

Revenue Streams

- ABO 1. Jahresabo (all inkl.) 2. Grundbetrag + Anzahl Request 3. pay per Use
- Großkunden pro Standort ("gekapselt", on-premise Lösung)
- Spezielles Add-On Feature für spezielle Branchen

Source: Strategyzer AG | License: CC By-SA 3.0

The Business Model Canvas (04.07.2023)

Key partners

- Social Media (Facebook) --> als Datenbasis
- BSI Up-KRITIS als Arbeitskreise für Tests und zur Einbindung als Sicherheitskatalog-Lösung)
- Technik: Data Science Intelligence (so wie Trevisto)
- Forensik und Incident Response (im Ernstfall)

Key activities

- Monitoring, Lagebild --> Informations-angebot
- Datenbasis erstellen und pflegen
- Modellpflege und Überwachung
- Sensibilisierung und Awarness steigern

Key resources

- Hardware IT-Kompetenz Integration Cloud
- ? Groß-unternehmen? (Ressource?)

Key propositions

- Integration mit Sicherheits-maßnahmen
- Integration mit Sicherheitslösungen für schnelles und effektives Lernen
- kein Bewerber geht verloren
- up-to-date Sicherheit -Datenschutz -Daten für Vielfalt
- Individualisierung - Kundenbedürfnisse - Kanäle für Bewerbungen - Sicherheitsniveau durch Baukasten

Customer relationships

- Strategische Partnerschaft mit System Personalwesen
- Probeabo für bestehende Kunden

Channels

- Vorträge
- Zeitungen
- Messen

Customer segments

- Bestandskunden von itWESS
- Personalberater, Headhunter (überprüfen Bewerbungen) --> Auch Partner?
- Großkunden on-premise Lösung
- (inhabe-geführter) Mittelstand profitiert von allen Partnern

Cost Structure

- Server - Lizenzen -Testserver
- Personalkosten für Testen, Datenverwaltung, Überwachung
- Fernwartung des Services beim Kunden
- Personalkosten Entwicklung

Revenue Streams

- Fixum pro Jahr (Für Personalberater)
- Jährliche Servicegebühr (5 Rechner und 200 Mitarbeiter z.B. für Mittelstand)

Source: Strategyzer AG | License: CC By-SA 3.0

The Business M Canvas (Zusammenfassung 16.10.2023)

Training mittels "to go" mit Virenscanner hinterlegt (--> über Standard itWess)

Key partners

Key-Kunden (erste Kunden, die mit Entwickeln und das System nach außen tragen)

Social Media (Facebook) --> als Datenbasis

Werbepartner (Zeitschriften, Influencer)

BSI Up-KRITIS als Arbeitskreise für Tests und zur Einbindung als Sicherheitskatalog-Lösung)

Produkttester

Berater (IT-Sicherheit) die Produkt empfehlen

Personalberater

Technik: Data Science Intelligence (so wie Trevisto)

E-Mail-Provider

Netzwerkprovider

Software-Hersteller (Branchen-spezifisch, z.B. Persiono)

Key activities

Kundenerhalt, Werben von Kunden, Anwenderschulung neuer Kunden

Generierung der Startkunden für Basismodell

Datenbasis erstellen

Sensibilisierung und Awarness steigern

Referenzkunden aufbauen

Monitoring, Lagebild --> Informations-angebot

Modellpflege und Überwachung

Software (Wartung, Auslieferung...)

Modell regelmäßig updaten und evaluieren

Testphasen durchführen

KPIs erstellen und messen

Key resources

Finanzielle Mittel

KI-Modell

Daten für Training der Modelle

Experten zur Überprüfung

Erste Kunden

? Groß-unternehmen? (Ressource?)

Fachpersonal (Entwicklung, Betrieb) IT, KI

Forensik und Incident Response (im Ernstfall)

Sicherer Server (Standort)

Hardware IT-Kompetenz Integration Cloud

Server /Hardware (innerhalb der EU)

Key propositions

Integration mit Sicherheits-maßnahmen

Integration mit Sicherheitslösungen für schnelles und effektives Lernen

Neues System, Mehrwert an Sicherheit

KMU: höherer Sicherheitsaspekt, schließen von Sicherheitslücken durch große Gruppe, die Modell trainiert

Mehr Sicherheit für Abteilungen bei der Kommunikation mit Externen

Differenzierte Einschätzung einer Bedrohung als JA/NEIN

Sicherheits niveau durch Baukasten

Privatmarkt wie KMU

up-to-date Sicherheit -Datenschutz -Daten für Vielfalt

Weiter-entwicklung des Portfolios

kein Bewerber geht verloren

Individualisierung - Kundenbedürfnisse - Kanäle für Bewerbungen

E-Mail Provider kann damit werben, Zusatz gegenüber anderen Privdern

E-Mail Provider können selber ein zusätzliches Feld an Kunden ansprechen

Marketing-personal (Kunden-kontakt) mit Ahnung von IT-Sicherheit (kein Calcenter)

ITWESS / ITWESS.AI

Gruppierung nach - Abteilung -Branche -Prozessen (Global Modell "Federation")

Trainingserfahrungen durch mehrere am Projekt teilnehmende Unternehmen

ITWES "to go".AI für kleine Kunden (größere Datenmenge zum Anlernen)

Erweiterung des Modells; Profitieren von anderen und weiterer Kenntnissaufbau

Customer relationships

Strategische Partnerschaft mit System Personalwesen

über Portal (unpersönlich)

Support, Ansprechpartner

Support B2B

persönlicher Kundenkontakt zum Einkäufer/ Fachabteilung

bei allen längerfristige Bindung

Support, Service-Hotline

Channels

Vorträge

Neukunden: Meme (ITSA, mit Demo Use-Case), Virtuelle Meme, Online-Veranstaltung

Zeitungen

Messen

Youtube oder Influencer

Werbung, Add-Ons schalten, über andere Bestandskunden (Anreize setzen)

Direktes Marketing betreiben, direkten Kontakt suchen,

Über den Betreuer, per Mail oder Telefon; Innovation ohne Aufreis für den Kunden, zum Trainieren des Initalmodell nutzen

Bestandskunden: Vertrieb

Customer segments

KMU/ Selbstständige

Großkunden

on-premise Lösung

Viele kleine Kunden

(inhabe-geführter) Mittelstand profitiert von allen Partnern

"Großkunden" mit vielen Lizenzen

Privatmarkt

E-Mail-Provider (Add-on zu Mail-Programm) --> eher kleinere Provider, deren Kunden auf IT-Sicherheit wert legen

Personalberater, Headhunter (überprüfen Bewerbungen) --> Auch Partner?

Bestandskunden

Bestandskunden von itWESS

"Gruppierungen"

Alle Abteilungen mit viel externen Kommunikation und sensiblen Daten

Kundengruppen, die sich sowieso mit IT-Sicherheit beschäftigen und Interesse an ihrer Sicherheit haben bzw. darauf wert legen müssen (rechtlich)

Cost Structure

FL-Server (Miete/Betrieb)

Server - Lizenzen -Testserver

Infrastruktur

Personalkosten für Testen, Datenverwaltung, Überwachung

Einige Experten

Personalkosten Entwicklung

Fernwartung des Services beim Kunden

Personalkosten

Marketing, Werbekosten

Betreuung+ Retraining automatisiert (immer aktuell)

Entwicklungskosten

Weiter-entwicklung + Optimierung

Revenue Streams

Fixum pro Jahr (Für Personalberater)

Verhandlung, Wie teuer wollen die Provider es an ihre Kunden vermarkten? Bestimmter Anteil vom Gewinn

ABO 1. Jahresabo (all inkl.) 2. Grundbetrag + Anzahl Request 3. pay per Use

Jährliche Servicegebühr (5 Rechner und 200 Mitarbeiter z.B. für Mittelstand)

Großkunden pro Standort ("gekapselt", on-premise Lösung)

Zahlen bereits, habe Lizenzen. Mehr Geld nur wenn es wirklich einen Sicherheitsnutzen bringt. Preise gleich oder maximal 5-10%.

Probeabo für bestehende Kunden

Spezielles Add-On Feature für spezielle Branchen

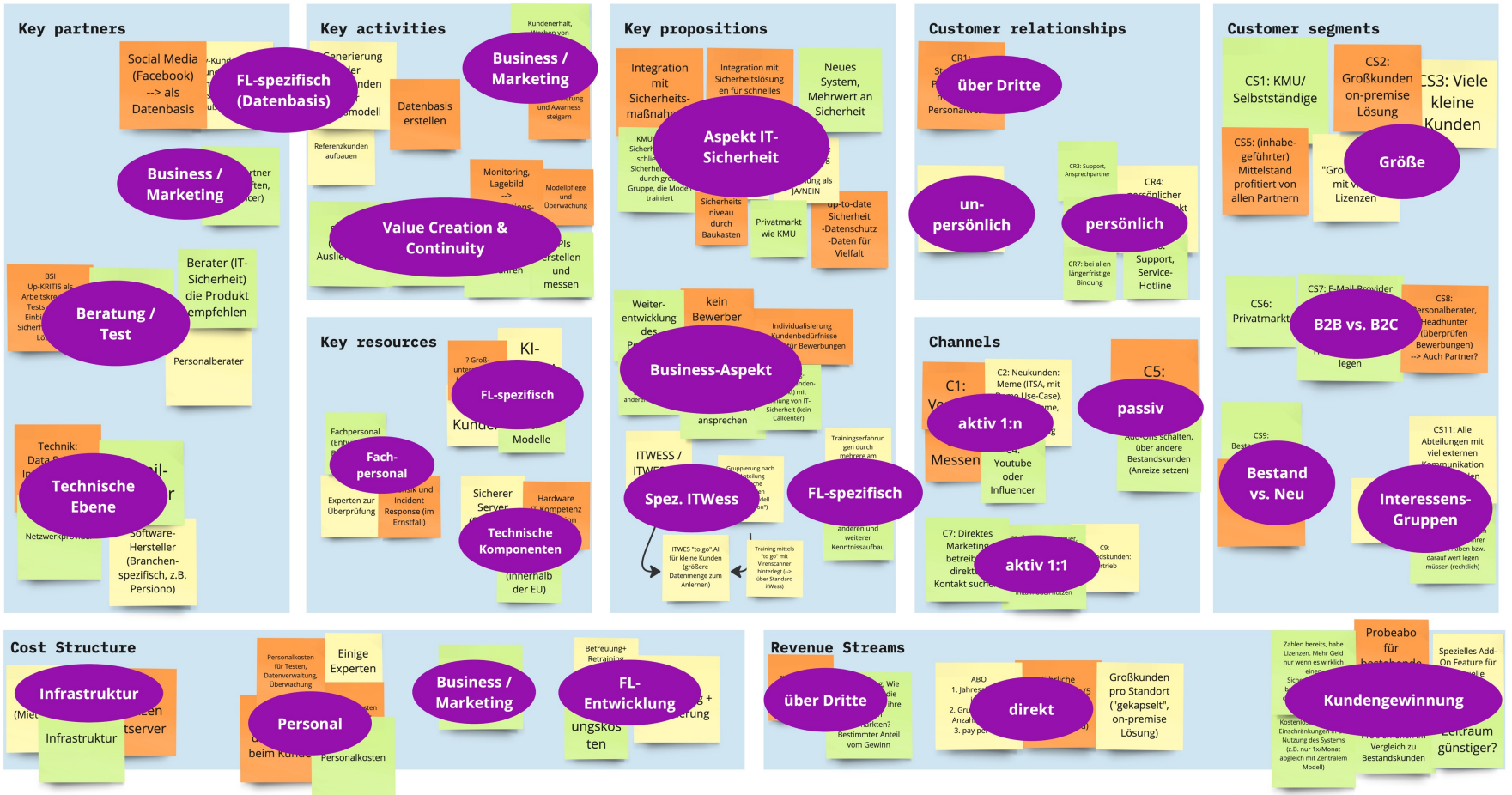
Kostenlose Version mit Einschränkungen in der Nutzung des Systems (z.B. nur 1x/Monat abgleich mit Zentralem Modell)

Lizenzen verkaufen, nicht zwingend den Preis erhöhen im Vergleich zu Bestandskunden

Erster Zeitraum günstiger?

Source: Strategyzer AG | License: CC By-SA 3.0

The Business Model Canvas (Zusammenfassung 16.10.2023)



Source: Strategyzer AG | License: CC By-SA 3.0

FL-Modell

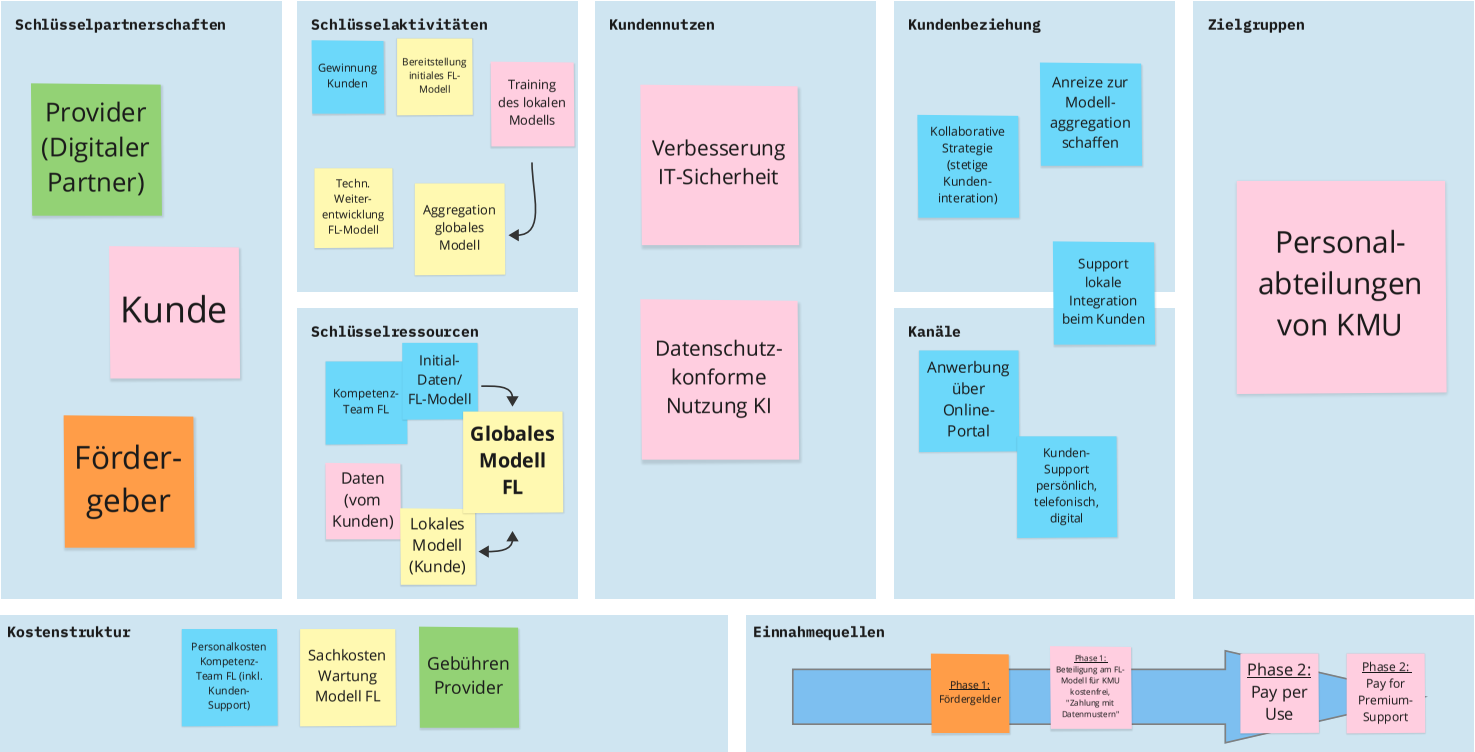
Kunde: KMU

FL-Anbieter: itWatch/ Trevisto

Provider Cloud-Service

Fördergeber

Geschäftsmodell FLUniBwM (Phase 1 --> Phase 2)



Source: Strategyzer AG | License: CC By-SA 3.0