A user-centred approach to facilitate locating company security policies
Nutzerzentrierter Ansatz zur Vereinfachung des Auffindens von Security Policies

Lukas Aldag
Fabian Lucas Ballreich
Benjamin Maximilian Berens
Melanie Volkamer
lukas.aldag@kit.edu
fabian.ballreich@kit.edu
benjamin.berens@kit.edu
melanie.volkamer@kit.edu
Karlsruhe Institut für Technologie
Karlsruhe, Germany

ABSTRACT

English: An important factor for the effectiveness of security awareness measures in companies is awareness and consistency of security policies. As part of a case study, a document was created using a user-centred approach that gives an overview of all relevant individual documents (so-called overview document). In addition, a process for publication was developed and evaluated iteratively. The case study took place at a medium-sized energy company in Germany. General lessons learned are derived from the case study. For example, distributing important documents via e-mail carries the risk that this is perceived as less important or is not perceived at all.

Deutsch: Ein wichtiger Faktor für die Effektivität von Security Awareness-Maßnahmen in Unternehmen sind die Bekanntheit und Konsistenz von Security Policies. Im Rahmen einer Case Study wurde mit einem nutzerzentrierten Ansatz ein Dokument, das den Nutzenden eine Übersicht über alle relevanten Einzeldokumente (sog. Übersichtsdokument) gibt und ein Prozess zur Bekanntmachung iterativ entwickelt und evaluiert. Die Case Study fand bei einem mittelgroßen Energieversorgungsunternehmen in Deutschland statt. Aus der Case Study werden allgemeine Lessons Learned abgeleitet. Beispielsweise birgt eine Verteilung von wichtigen Dokumenten über E-Mail die Gefahr, dass diese gar nicht oder als weniger wichtig wahrgenommen wird.

KEYWORDS

Security Policies; Informationssicherheit; Security Awareness; Case Study

MuC '23, September 03–06, 2023, Rapperswil, Switzerland

ACM ISBN 979-8-4007-0771-1/23/09.
https://doi.org/10.1145/3603555.3603573

ACM Reference Format:
Lukas Aldag, Fabian Lucas Ballreich, Benjamin Maximilian Berens, and Melanie Volkamer. 2023. A user-centred approach to facilitate locating company security policies. In *Mensch und Computer 2023 (MuC '23), September 03–06, 2023, Rapperswil, Switzerland*. ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3603555.3603573

1 EINLEITUNG

Ein wesentliches Problem großer Organisationen ist die hohe Anzahl existierender Richtlinien und Vorgaben (zusammenfassend als Security Policies bezeichnet) insbesondere im Bereich der IT- und Informationssicherheit. Dies kann einerseits zu einem hohen Aktualisierungsaufwand, andererseits zu einer starken Unübersichtlichkeit für die Anwender und Anwenderinnen führen. Bevor ein Unternehmen jedoch weitergehende Maßnahmen zur Steigerung der Security Awareness durchführt, sollte grundsätzlich die Aktualität, Konsistenz und Bekanntheit von Richtlinien und Vorgaben sichergestellt sein [14]. Diese genannten Faktoren tragen zu einer besseren "Usability" [8] bei und können die Einfachheit der Benutzung und Effektivität eines Systems verbessern. Usability wird im Security Bereich auch Usable Security genannt und sollte besonders beachtet werden. Beispielsweise wurde in einer Studie von Beautement et al.[4] gezeigt, dass Menschen dazu tendieren, Sicherheitsrichtlinien zu missachten, wenn der Kosten-Nutzen-Faktor gering ist. Wenn notwendige Informationen zu schwer zu finden, nicht aktuell oder unverständlich sind, neigen Menschen eher dazu, diese Informationen nicht zu verwenden. Das Ziel dieser Arbeit war es, im Rahmen einer nutzerzentrierten Fallstudie ein Dokument (sog. Übersichtsdokument) zu erstellen, das den Nutzenden eine Übersicht über alle relevanten Richtlinien innerhalb der Organisation, welche bis dato nur in Form von Einzeldokumenten vorlagen. Weiterhin wurde ein geeigneter Speicherort und ein Prozess zur Bekanntmachung dieses Übersichtsdokument iterativ entwickelt und evaluiert (siehe 1). Ebenfalls Teilziel dieser Arbeit war es daher auch festzustellen, welcher der verschiedenen Kommunikationskanäle für die Verteilung von Informationen mit Bezug zur Informationssicherheit bevorzugt geeignet sind. Diese Fallstudie wurde in

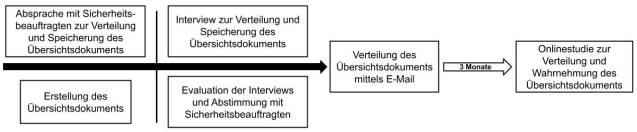

Figure 1: Planungsübersicht und Ablauf der Studien.

Zusammenarbeit mit der Stadtwerke Ettlingen (SWE) durchgeführt. Zu Beginn wurden mit dem Informationssicherheitsbeauftragten des Unternehmens der Aufbau sowie mögliche Optionen zur Speicherung und Verteilung des Dokuments diskutiert. Im Anschluss wurden Interviews mit Mitarbeiter:innen des Unternehmens aus unterschiedlichen Abteilungen geführt, wobei nach nach Feedback zu den verschiedenen Optionen sowie eigenen Vorschlägen gefragt wurde. Auf Basis der Ergebnisse fiel die Wahl in Abstimmung mit dem Informationssicherheitsbeauftragten auf eine Verteilung des Dokuments per E-Mail an alle registrierten E-Mail Adressen innerhalb des Unternehmens (sog. AllUser) und eine Speicherung an einer dedizierten Stelle im Intranet. Die E-Mail wurde vom Informationssicherheitsbeauftragten selbstständig über seine eigene Adresse verschickt, wobei das Übersichtsdokument als Anhang beigefügt war. Die Evaluation des Dokuments sowie der Verteilungsart wurde nach drei Monaten mittels eines Onlinefragebogen durchgeführt,welcher an alle Beschäftigten versendet wurde. Der Fokus lag hierbei auf der Bewertung der Verteilung, der Erfassung möglicher Gründe, weshalb das Übersichtsdokument von manchen Nutzer:innen nicht wahrgenommen wurde sowie weitere mögliche Verbesserungsoptionen.

Bei der Gestaltung von neuen Systemen gibt es im Hinblick auf die Usability mit "User Centered Design", "Participative Design" und "Iterative Design" einige bewährte Konzepte[8], welche auch im Rahmen dieser Arbeit aufgegriffen wurden. User Centered Design erfasst die Notwendigkeit, die Nutzenden und deren Feedback in den Entwurfsprozess einzubinden, da diese die Zielgruppe des Systems repräsentieren. Das Konzept des Participative Design bedeutet, dass Personen mit fachlicher Expertise in den Entwurfsprozess involviert sind. In unserem Fall wird diese Rolle durch den Informationssicherheitsbeauftragten eingenommen, welcher die fachliche Sicht bei der Erarbeitung des Dokuments eingebracht hat. Letztendlich gibt es noch das Konzept des Iterative Design, welches sich auf das Wiederholen von einzelnen Entwurfsprozessen bezieht, um eine kontinuierliches Verbesserung des Systems zu ermöglichen. In der vorliegenden Arbeit wurde sich für einen iterativen Entwurfsprozess entschieden, da das Übersichtsdokument in mehreren Stufen evaluiert und verbessert wurde.

Volkamer und Sasse [15] behandeln einen Leitfaden für effektivere IT-Security-Awareness, welcher ebenfalls als Grundlage für diese Arbeit gedient hat. Dieser Leitfaden erfasst mit der Definition der Zielgruppe, der Zielsetzung, der Inhalte, des Formats, der Sprache und der Evaluation viele der bereits genannten Ansätze der Usability-Forschung.

Unsere Ergebnisse zeigen, dass die Forschung in einer Organisation sowohl methodisch konzeptionell, als auch in der Anwendung der Ergebnisse besondere Schwierigkeiten aufweist. Durch die Befragung zu einer geeigneten Methode zur Kommunikation von Informationen mit Bezug zur Informationssicherheit und der tatsächlichen Umsetzung, konnten erste Erkenntnisse über eine solche Maßnahme im Umfeld einer Organisation gewonnen werden. Bereits die wissenschaftliche Arbeit in der Organisation kann einen Einfluss auf diese nehmen und sollte in ein ausführliches Briefing und On-boarding der Beschäftigten (auch wenn diese nicht direkt in die Studie involviert sind) eingebettet werden. Zunächst ist die Erhebung des Ist-Zustand in einer heterogenen Organisation mit sehr unterschiedlichen Abteilungen mit einer Methode kompliziert. Wenn das Arbeitsumfeld bzw. der Arbeitskontext für manche Beschäftigten eine Erhebung erschwert bis unmöglich macht, kann die Umsetzung auf Basis der Ergebnisse zu neuen Schwierigkeiten führen. Zum einen stellt sich die Frage, welche Wünsche umgesetzt werden und zum anderen wie die Kommunikation bezüglich des Umsetzens und nicht Umsetzens gestaltet werden muss.

2 VERWANDTE ARBEITEN

Der Bereich Richtlinien zur Informationssicherheit wurde bereits in einigen Studien genauer untersucht. Die Abhängigkeit von verschiedenen, sich verändernden Informationstechnologien, die Einbindung von Cloudanbietern und die Bedeutung des Internets als Kommunikationskanal wächst und bietet somit zunehmend vielfältigere Möglichkeiten, dass sensible Informationen durch einen Fehler oder durch Angreifer offengelegt werden [12]. Sicherheitsrichtlinien sind ein häufig genutztes Mittel um die Beschäftigten auf die Einhaltung entsprechende Verhaltensregeln hinzuweisen. 98% der großen Organisationen und 60% der kleinen Unternehmen verwenden dokumentierte Informationssicherheitsrichtlinien[2]. Soomro et al. [10] weisen in diesem Zusammenhang darauf hin, dass die reine Existenz von Richtlinien nicht ausreicht, um das Sicherheitsniveau im Unternehmen effektiv zu steigern. Hierzu ist es notwendig, dass diese mit entsprechenden Trainings und Awarenessmaßnahmen begleitet werden, um ein Bewusstsein für die Richtlinien zu schaffen. In einer Arbeit von Beautement et al. [4] wurden 17 Beschäftigte von zwei großen Organisationen befragt, weshalb manche Regeln eingehalten werden und andere wiederum nicht. Im Ergebnis stellten die Forschenden fest, dass die Entscheidung der Beschäftigten, eine Richtlinie zu befolgen, davon abhängt, welcher Aufwand und welche Vorteile damit verbunden sind. Dieser Vergleich von Aufwand und Vorteilen ist jedoch individuell, da unterschiedliche Faktoren die Wahrnehmung beeinflussen können. Durch das Beachten dieser Abwägung und Verwendung von Awareness-Maßnahmen, lässt sich der Vergleich beeinflussen und die Einhaltung der Richtlinien verbessern. Alotaibi et al. [2] haben die bestehende Literatur zum Themengebiet untersucht und verweisen unter anderem auf die Herausforderung durch die sogenannten Shadow Security. Demnach gibt es bei Sicherheitsrichtlinien neben dem Befolgen und Ignorieren grundsätzlich ein drittes mögliches Verhalten. Hierbei missachten Beschäftigte absichtlich Richtlinien, wenn diese als zu aufwendig wahrgenommen werden oder hierdurch die Produktivität vermindert wird. Die Shadow Security kann das Einführen von Richtlinien erschweren und im schlimmsten Fall zu einer Kultur des Nichtbefolgens

führen, wodurch weitere Beschäftigte ein Missachten der Richtlinien tolerieren und selbst praktizieren. Bauer et al. [3] haben insgesamt 33 Interviews an drei verschiedenen Banken durchgeführt, um die erfolgreichsten Awarenessmethoden zur Bekanntmachung von Sicherheitsrichtlinien zu finden. Alohali et al. [1] beschäftigen sich in ihrer Arbeit unter anderem mit dem Thema der Kommunikation von Risiken im Umfeld der IT-Sicherheit. Demnach ist es wichtig, bei der Vermittlung von Informationen die unterschiedlichen Wissensstände und vorhandenen IT-Kenntnisse sowie kulturelle Hintergründe mit einzubeziehen. Ebenfalls soll nach Möglichkeit auf die Verwendung von Fachsprache verzichtet werden, da diese für weniger erfahrene Empfänger eine Barriere darstellt. Die Forschenden schlagen hierzu die Strukturierung von Informationen in verschiedene Gruppen vor, abhängig vom Grad des Vorwissens des Empfängers. Bei der Gestaltung von Inhalten sollten unterschiedliche Arten der Präsentation (z.B. Video, Audio, Text, etc.) in Betracht gezogen werden. Eine gute und verständliche interne Kommunikation führt laut Tkalac Verčič et al. [13] zu höherem Engagement der Beschäftigten und somit zu insgesamt zu einem höheren Sicherheitsniveau. Ein wichtiges Element ist demnach die Möglichkeit zur informellen Kommunikation, beispielsweise in Rahmen von Meetings.

3 RELEVANTE CHARAKTERISTIKA DES UNTERNEHMENS

Die Stadtwerke Ettlingen (SWE) ist als kommunales Energieversorgungs- und Dienstleistungsunternehmen in Baden-Württemberg tätig und beschäftigt konzernweit rund 240 Arbeitnehmende. Ein großer Anteil der Beschäftigten von Stadtwerke Ettlingen (SWE)ist hierbei nicht in der Verwaltung tätig, sondern verantworten beispielsweise in den Werkstätten, der Lagerverwaltung oder dem Netzmanagement das operative Geschäft. Der Grad der IT-Nutzung der Mitarbeitenden ist daher stark von der jeweiligen Abteilung sowie dem Aufgabengebiet abhängig. So haben beispielsweise Mitarbeitende der Werkstätten keinen dauerhaften Internetzugang, sowie keine individuellen betrieblichen E-Mail-Adressen, was sich jedoch in naher Zukunft durch weitere Digitalisierung innerhalb des Unternehmens ändern soll. Erschwerend kommt hinzu, dass für unterschiedliche Abteilungen zum Teil verschiedene Dienst- und Arbeitsanweisungen existieren. Die interne Kommunikation erfolgt weitestgehend über E-Mail, das Intranet sowie dem Umlauf - eine papiergebundene Verteilung an alle Mitarbeitenden mit Empfangsbestätigung per Unterschrift. Über das Intranet wird den Nutzenden - geordnet nach verschiedenen Rubriken - betriebsinterne Informationen wie beispielsweise Telefonlisten oder Veranstaltungstermine mitgeteilt. Innerhalb des Intranet gibt es eine Rubrik "Dokumente", die in verschiedene Unterordner gegliedert ist. Diese Rubrik dient als zentrale Ablage für Dateien, die die Mitarbeitenden benötigen. An dieser Stelle existiert auch der Unterordner "IT-Sicherheit", welcher diverse Dokumente aus dem Themenbereich IT- und Informationssicherheit enthält. Weiterhin wurde ein externer Dienstleister mit der Bereitstellung eines Awareness-Portals zum Thema Informationssicherheit und Cybersecurity beauftragt, welches über das Firmennetzwerk erreichbar und dessen regelmäßige Nutzung für alle Mitarbeitenden verbindlich ist. Für das Unternehmen wurde ein interner Informationssicherheitsbeauftragter bestellt, dieser ist unabhängig von der bereits existierenden separaten IT-Abteilung, welche für die technische Umsetzung und Verwaltung der IT zuständig ist. Das Unternehmen unterhält seit November 2017 ein nach ISO/IEC 27001 zertifiziertes Informationssicherheitsmanagementsystem (ISMS), das sich an den Vorgaben der Bundesnetzagentur orientiert.

4 ENTWICKLUNG EINES ERSTEN VORSCHLAGS

Zu Beginn wurde mit dem Informationssicherheitsbeauftragten des Unternehmens der Aufbau, sowie mögliche Optionen zur Speicherung und Verteilung des Übersichtsdokuments diskutiert, mit dem sich Mitarbeitende bei Bedarf einen Überblick über die relevanten Dokumente verschaffen können. Das so entwickelte Dokument umfasst insgesamt vier Seiten, wobei die erste Seite als Deckblatt fungiert und nur eine kurze Erklärung zum Dokument selbst enthält. Auf der zweiten und dritten Seite werden zu neun Themengebieten (z.B. Mobile Geräte) insgesamt 34 Einzeldokumente bzw. -ressourcen aufgeführt. Hierbei handelt es sich beispielsweise um Dienstanweisungen, Betriebsvereinbarungen, Checklisten oder Verweise auf das Awareness-Portal. Die letzte Seite enthält Name, Kontaktdaten und ein Bild des Informationssicherheitsbeauftragten sowie des Leiters der IT-Abteilung. Als Speicherort für das Übersichtsdokument kamen verschiedene Optionen in Frage, wie beispielsweise im Intranet, auf dem Netzlaufwerk, als Aushang in öffentlichen Räumen des Unternehmens sowie innerhalb des Awareness-Portals. Da das Netzlaufwerk nicht mehr für derart Angelegenheiten genutzt werden sollte, das schwarze Brett nicht regelmäßige Aufmerksamkeit erhält und das Awareness-Portal zu spezifisch ist, fiel die Wahl letztendlich auf das Intranet als zentraler Speicherort für das Übersichtsdokument.

5 ETHIK

Die durchgeführten Studien in dieser Arbeit sind an den ethischen Standard des KITs angepasst. Die Teilnehmenden wurden vollständig über die Studien aufgeklärt und durften zu jeder Zeit und ohne Angabe eines Grunds die Studie abbrechen, in welchem Fall die bisher gesammelten Daten gelöscht wurden. Die Daten wurden anonym erhoben, sodass spezifische Antworten nicht auf einzelne Teilnehmende zurückverfolgt werden könnten. Ebenso wurden die Aufnahmen der durchgeführten Interviews nach Abschluss der Transkription gelöscht, um mögliche Wiedererkennung der Stimme auszuschließen. Dem Unternehmen wurden nur aggregierte Daten bereitgestellt, sodass keine Möglichkeit für die Identifizierung einzelner Beschäftigter bestand.

6 QUALITATIVES FEEDBACK MITTELS INTERVIEWS

Das Ziel der Interviews war es, mehr Erkenntnisse zur geplanten Verteilung des Übersichtsdokuments im Unternehmen zu erlangen.

6.1 Methodik Interview

Um auf die unterschiedlichen Antworten der Teilnehmenden besser eingehen zu können, wurde ein semistrukturiertes Interview gewählt. Hierbei werden zentrale Fragen in einer festen Reihenfolge abgehandelt, wobei für den Interviewenden die Möglichkeit zur Nachfrage

besteht. Die Interviews wurden aufgezeichnet, transkribiert und anschließend gelöscht, um die Anonymität der Teilnehmenden zu gewährleisten. Zur Auswertung wurden die Interviews im offenen Codierungsverfahren analysiert, wobei zwei Forschende jeweils ein eigenständiges Codebuch erstellt haben. Im Anschluss wurde deren Inhalt verglichen zusammengeführt, wobei bestehende Abweichungen in der Diskussion aufgelöst wurden. Das hiermit gemeinsam erstellte Codebuch wurde als Grundlage für die folgende Analyse der Interviews verwendet. Um sicher zu gehen, dass beide Forschende dasselbe Verständnis bezüglich der unterschiedlichen Codes haben, wurde die Übereinstimmung der Codierung mittels Cohen's Kappa überprüft. Hierbei wurde eine Übereinstimmung von $\kappa = 0.94$ erreicht, was laut McHugh und Mary einer hohen Übereinstimmung entspricht [7]. Das finale Codebuch befindet sich zur Vollständigkeit und Möglichkeit einer Replikation im Anhang (siehe 10.5). Das Interview begann mit einer kurzen Erklärung des Themas, sowie dem Hinweis, dass die Dauer ungefähr 30 Minuten beträgt und die Antworten aufgezeichnet werden. Hierbei wurde besonders hervorgehoben, dass die Daten des Interviews streng vertraulich behandelt und nur in anonymisierter Form veröffentlicht werden. Zudem konnten die Teilnehmenden jederzeit und ohne Angabe eines Grundes das Interview abbrechen, wodurch alle bis dahin gesammelten Daten gelöscht werden. Danach bekamen die Teilnehmenden die Möglichkeit, Fragen zum Ablauf zu stellen. Die Zustimmung zur Aufzeichnung wurde vor und nach dem Start der Aufnahme eingeholt. Erst nach der Zustimmung wurde mit der Aufnahme begonnen. Im Anschluss wurde die Aufzeichnung gestartet und das Interview begonnen. Das Interview umfasst drei Teile (siehe Fig. 2), die im Folgenden erläutert werden:

(1) Im ersten Teil "Begriffsbestimmung", wurden die Teilnehmenden gefragt, ob ihnen ein Unterschied zwischen IT- und Informationssicherheit bekannt sei, da sich die beiden Begriffe ähneln und die Nutzenden verwirren könnten. Da es jedoch im Unternehmen wichtig ist, einen IT- oder Informationssicherheitsvorfall richtig zu erkennen und zu melden, sollte der derzeitige Wissensstand abgefragt werden. Falls die Teilnehmenden diese Frage bejahten, wurde danach gefragt, welcher der beiden Begriffe geläufiger sei und worin der Unterschied besteht. Falls die Frage verneint wurde, so wurde gefragt, ob einer der beiden Begriffe bekannt sei.

(2) Im zweiten Teil "Verhalten", lag der Fokus auf dem derzeitigen Verhalten bei der Suche nach Informationen im Kontext von IT- und Informationssicherheit. Die Teilnehmenden wurden gefragt, wie sie nach Informationen zum Thema IT- oder Informationssicherheit suchen. Falls die Teilnehmenden dies noch nie gemacht haben, sollte ein hypothetisches Vorgehen erläutert werden.

(3) Der dritte Teil "Zukunft", befasst sich mit dem Inhalt des erstellten Übersichtsdokuments zur Informationssicherheit. Die Fragestellung war, an welcher Stelle dieses gespeichert werden sollte und wie es am effektivsten verteilt werden könnte. Bei der ersten Frage sollten die Teilnehmenden Ideen nennen, an welcher Stelle das Dokument im Intranet im besten Fall abgelegt werden sollte. Falls die Teilnehmenden hierzu keine Idee nennen konnten, wurde ihnen ein Mock-Up mit einer Stelle im Intranet präsentiert, welche dem existierenden Unterordner 'IT-Sicherheit' entsprach. Daraufhin sollten die Teilnehmenden angeben, ob ihnen dieser Ort bekannt sei und wie geeignet sie diesen Ort empfinden. Die zweite Frage behandelt die Verteilung des Übersichtdokuments, wobei

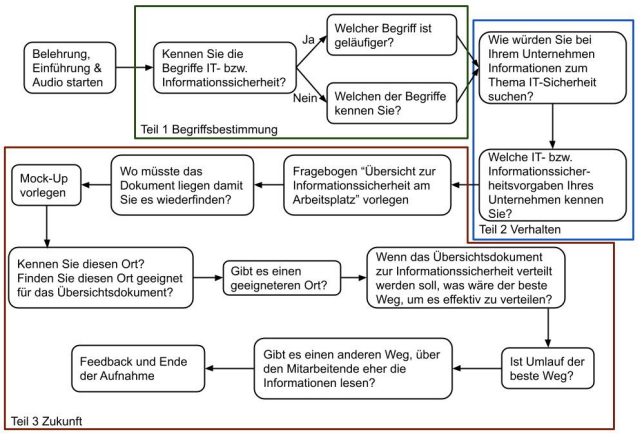

Figure 2: Ablauf des Interviews, aufgeteilt in die drei Teile Begriffsbestimmung, Verhalten und Zukunft.

die Teilnehmenden möglichst effektive Verteilungsmöglichkeiten benennen sollten. Falls hierbei der bisher übliche Verteilungsweg (sog. Umlauf) genannt wurde, wurde nachgefragt weshalb speziell dieser Weg geeignet ist. Zusätzlich wurde nach alternativen Wegen gefragt, über welche den Mitarbeitenden Informationen zugänglich gemacht werden können. Zum Abschluss wurde nach Feedback zum Inhalt des Übersichtsdokument sowie generell zur Informationssicherheit am Arbeitsplatz gebeten. Nach der Beantwortung der letzten Frage, wurde die Aufnahme gestoppt, für die Teilnahme gedankt und die Teilnehmenden verabschiedet.

6.2 Rekrutierung von Teilnehmenden

Da der Digitalisierungsgrad der Abteilungen variiert, wurden Teilnehmenden aus unterschiedlichen Abteilungen für das Interview rekrutiert. Insgesamt haben sich 18 Mitarbeitende der Stadtwerke Ettlingen (SWE) aus 16 unterschiedlichen Abteilungen an dem Interview beteiligt. Die Teilnehmenden wurden mit Hilfe des Informationssicherheitsbeauftragten akquiriert, wobei die Teilnahme an der Studie freiwillig erfolgte.

6.3 Ergebnis und Analyse

Im ersten Teil (Begriffsbestimmung) des Interviews gaben elf der Befragten an, dass ihnen der Begriff IT-Sicherheit im Vergleich zu Informationssicherheit geläufiger ist. Die gegenteilige Aussage wurde von keinem der Teilnehmenden getroffen. Sieben Befragte bezeichneten beide Begriffe als gleich geläufig. Im zweiten Teil (Verhalten) des Interviews wurden die Teilnehmenden zuerst gefragt, wie sie bei der Suche nach Informationen im Bereit IT- und Informationssicherheit vorgehen. 15 der 18 Befragten gaben an, sich telefonisch an die IT-Abteilung zu wenden. Das vom Informationssicherheitsbeauftragten gewünschte Verhalten (Recherche Intranet und Anfrage über Ticketsystem) wurde lediglich von zwei Teilnehmenden genannt. Eine Person konnte hierzu keine Angaben machen. Auf Nachfrage, warum die Teilnehmenden die telefonische Anfrage gegenüber dem Ticketsystem bevorzugen, antworteten diese, dass hierdurch wesentlich schneller eine Antwort zu erhalten ist. Das Intranet als Informationsquelle war vielen Befragten

bekannt, bleibt häufig jedoch ungenutzt. Im dritten Teil (Zukunft) des Interviews wurde in der ersten Frage nach geeigneten Stellen zur Ablage des Übersichtsdokuments im Unternehmensnetz gefragt. Elf Teilnehmenden sahen hierzu das Intranet als geeignet an. In sieben bzw. einem Fall wurde auf die Ablage im Netzlaufwerk bzw. innerhalb der Zeiterfassungssoftware verwiesen. Die im Mockup vorgeschlagene Stelle (Unterordner IT-Sicherheit) im Intranet war lediglich 13 Befragten bekannt, wobei nur acht in der Vergangenheit bereits auch darauf zugegriffen hatten. In Anbetracht des Mockups, wurde das Intranet von den Befragten überwiegend als geeignet empfunden. Gleichzeitig wurde dessen komplizierte Bedienung sowie teilweise veralteten Inhalte kritisiert. Ebenfalls wurde angeregt, die Nutzenden nach der Einstellung neuer Inhalte beispielsweise per E-Mail zu benachrichtigen. Bei der folgenden Frage wurden die Teilnehmenden des Interviews gebeten, möglichst effektive Varianten zur Verteilung des Übersichtsdokuments zu nennen. In 13 Fällen wurde hierbei die Verteilung mittels E-Mail empfohlen. Die Verwendung des unternehmensinternen Umlaufs wurde von sechs Teilnehmenden genannt. Eine Person regte die Verteilung während Schulungsveranstaltungen an. Generell wünschten sich die meisten Teilnehmenden eine digitale Verteilung des Übersichtsdokuments, wobei vereinzelt auch eine Mischform (digital + Umlauf) gefordert wurde. Als Vorteile der Verteilung über den Umlauf wurden der garantierte Erhalt sowie die empfunden höhere Wichtigkeit im Vergleich zu E-Mails genannt. Nachteile sahen die Teilnehmenden in der langen Dauer des Verfahrens, sowie der hierdurch begünstigten Informationsflut. Nach anderen Wegen zur Verteilung der Informationen gefragt, wurde beispielsweise auf die stärkere persönliche Ansprache durch Abteilungsleiter und die Erläuterung während Betriebsversammlung verwiesen. Zum Abschluss des dritten Teils wurde nach Feedback zum Inhalt des Übersichtsdokuments sowie generell zur Informationssicherheit am Arbeitsplatz gefragt. Die Teilnehmenden merkten hierbei insbesondere die große Anzahl unterschiedlicher Dokumente zu verschiedenen Themen an, die sich teilweise inhaltlich überschneiden sowie Inkonsistenzen und Unklarheiten enthalten. Ebenfalls werden nicht alle verfügbaren Dokumente nachvollziehbar an der gleichen Stelle des Intranets zur Verfügung gestellt. Weiterhin gibt es nur wenige Informationen zu direkten Ansprechpartnern im Unternehmen. Inwieweit neue Mitarbeitende nach Einstellung derartige Informationen vermittelt bekommen, wurde von den Teilnehmenden ebenfalls in Frage gestellt.

7 IMPLEMENTIERUNG VON MASSNAHMEN DURCH INFORMATIONSSICHERHEITS-BEAUFTRAGTEN

Basierend auf den Ergebnissen des Interviews wurden durch den Informationssicherheitsbeauftragten des Unternehmens verschiedene Maßnahmen abgeleitet und umgesetzt. Das Übersichtsdokument wurde von sieben auf vier Seiten gekürzt, sodass es lediglich als Übersicht über alle existierenden Einzeldokumente dient und keine eigenen Erklärungen beinhaltet. Hierdurch soll beispielsweise das Auftreten von Inkonsistenzen vermieden und die Übersichtlichkeit des Dokuments gesteigert werden. Zusätzlich zur Nennung von Namen und Kontaktdaten des Informationssicherheitsbeauftragten sowie des Leiters der IT-Abteilung wurde jeweils ein Bild der Person ergänzt, um die Ansprechbarkeit im Unternehmensalltag zu verbessern. Die Struktur des Ordners "IT-Sicherheit" im Intranet wurde angepasst, sodass nun verschiedene Unterordner mit allen relevanten Dokumenten existieren, wobei das Übersichtsdokument innerhalb der Hauptebene abgelegt ist. Die Verteilung des Übersichtsdokuments erfolgte durch den Informationssicherheitsbeauftragten an alle registrierten E-Mail-Adressen mittels einer sogenannten AllUsers-Mail. Hierbei wurde kurz der Hintergrund des Dokuments erläutert und auf den Ablageort innerhalb des Intranets verwiesen. Um das Finden des Dokuments zu vereinfachen, wurde das Dokument selbst, ein Link und ein Screenshot eingefügt. Weiterhin wurden die Empfangenden gebeten, die Informationen auch an andere Mitarbeitende weiterzugeben, die selbst keinen direkten PC-Zugang haben.

8 EVALUIERUNG DER UMSETZUNG MITTELS UMFRAGE

Die zweite Befragung wurde auf Grund der COVID-19-Pandemie über einen Online-Fragebogen durchgeführt, dessen Aufbau Abbildung 3 entnommen werden kann.

8.1 Methodik Umfrage

Die technische Umsetzung des Fragebogens erfolgte über SoSciSurvey, mit Servern innerhalb der Europäischen Union. Das Unternehmen stellt hierdurch die datenschutzkonforme Verarbeitung der Daten im Sinne der Datenschutzgrundverordnung sicher. Der Fragebogen enthält sowohl qualitative als auch quantitative Fragen mit dem Ziel, die Verteilung und Wahrnehmung des Übersichtsdokuments beurteilen zu können. Die Teilnehmenden erhielten zu Beginn eine kurze Erklärung der Hintergründe der Studie sowie Informationen über die Anonymität der Datenverwertung sowie die Freiwilligkeit der Teilnahme. Somit fungierte die Einleitung gleichzeitig als Einwilligung zur Teilnahme. Am Ende der Einleitung wurde hervorgehoben, dass mit Klicken auf den Knopf "Einverstanden", der Einleitungstext gelesen wurde und die Teilnehmenden mit diesem einverstanden sind. Alle Teilnehmenden wurden zunächst befragt, wie sie im Unternehmen bei der Suche nach Informationen zum Thema IT- oder Informationssicherheit vorgehen. Im Anschluss wurde der Erhalt des Übersichtsdokuments abgefragt, wobei die Teilnehmenden abhängig von der Antwort danach in zwei Gruppen aufgeteilt wurden. Die erste Gruppe, bei der die Teilnehmenden angegeben haben, dass sie das Dokument erhalten hatten, wurde zusätzlich gefragt, wie und wann genau sie das Dokument erhalten haben. Anschließend wurde die Frage gestellt, inwieweit das Übersichtsdokument verwendet wurde und ob sich die Teilnehmenden das Dokument bereits genauer angeschaut haben. In Abhängigkeit von der Antwort auf die letztgenannte Frage, erhielten die Teilnehmenden daraufhin eine unterschiedliche Folgefrage. Wenn angegeben wurde, dass das Dokument genauer betrachtet wurde, sollte ein generelles Meinungsbild dazu abgegeben werden. Falls die Teilnehmenden das Dokument noch nicht genau angeschaut haben, sollte hierfür eine Erklärung gegeben werden. Unabhängig von der vorherigen Frage, wurden anschließend alle Teilnehmenden der Gruppe gefragt, wie sie das Übersichtsdokument in der Zukunft nutzen werden. Die letzten Fragen für diese

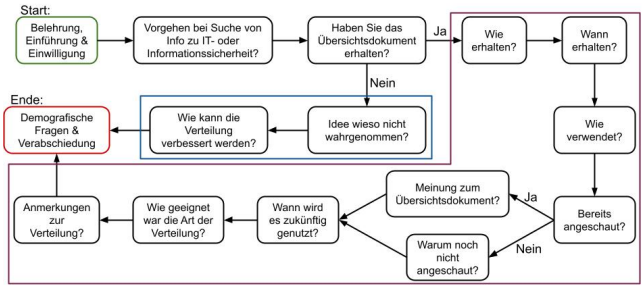

Figure 3: Aufbau des Online-Fragebogens zur Evaluierung der Umsetzung.

Gruppe bezogen sich auf die Art der Verteilung, wie geeignet diese empfunden wurde und ob es generell noch Anmerkungen zu der Verteilung des Dokuments gab. Die zweite Gruppe, bei der die Teilnehmenden angegeben haben, dass sie das Dokument nicht erhalten hatten, wurde nach möglichen Gründen gefragt, weshalb sie das Dokument vermutlich nicht wahrgenommen haben. Als nächstes konnten die Teilnehmenden Verbesserungsmöglichkeiten nennen, um die Aufmerksamkeit solcher Dokumente bei der Verteilung über E-Mail zu erhöhen. Abschließend sollten die Teilnehmenden beider Gruppen noch einige demografische Fragen beantworten.

8.2 Rekrutierung und Teilnehmende

Nach der Verteilung des Übersichtsdokuments im März, wurde im Zeitraum Juni bis Juli des Jahres die Umfrage gestartet. Hierzu wurden die Beschäftigten durch den Informationssicherheitsbeauftragten des Unternehmens um Teilnahme gebeten, wobei diese ebenfalls freiwillig war. Der Fragebogen wurde insgesamt von 40 Teilnehmenden ausgefüllt. Von den 40 Teilnehmenden der Umfrage mussten zwei auf Grund unvollständiger Angaben von der Auswertung ausgeschlossen werden. Von den übrigen 38 Befragten waren 29 männlich und neun weiblich. Das Alter der Teilnehmenden war zwischen 20 und 59 Jahren verteilt, wobei die meisten Teilnehmenden die Altersklasse 50-59 Jahre angaben. Als höchster Bildungsabschluss wurde hauptsächlich das Abitur sowie der Realschulabschluss genannt. Elf der 38 Teilnehmenden gaben darüber hinaus Bachelor, Master oder Diplom als Hochschulabschluss an.

8.3 Ergebnis und Analyse

In der Umfrage gaben 20 Teilnehmenden an, bei der Suche nach Informationen im Bereich IT- bzw. Informationssicherheit auf das unternehmenseigene Intranet zurückzugreifen. In 16 bzw. neun Fällen wurde hierbei die Ansprache des Informationssicherheitsbeauftragten bzw. der IT-Abteilung genannt. Lediglich eine teilnehmende Person erwähnte das zur Verfügung stehende Ticketsystem. 22 der 38 Teilnehmenden (bilden Gruppe 1) gaben an, das Übersichtsdokument erhalten zu haben. Dem entgegen haben 16 der Befragten (bilden Gruppe 2) das Dokument entweder nicht erhalten oder nicht wahrgenommen. 20 der 22 Teilnehmenden aus Gruppe 1 gaben an, das Übersichtsdokument seit Erhalt zumindest geöffnet zu haben, wobei zwei Befragte diese Frage mit Nein beantworteten. Auf die Frage, über welchen Weg sie das Dokument erhalten haben, gab der überwiegende Teil der Befragten (19) den Empfang per E-Mail an. Lediglich einzelne Teilnehmer nannten hierbei die Weitergabe durch Vorgesetzte oder Kollegen sowie den unternehmensinternen Umlauf. 14 der Teilnehmenden aus Gruppe 1 gaben an, das Dokument tatsächlich bereits in der Praxis verwendet zu haben, wobei neun Befragte vorgaben, das Dokument ausführlich gelesen zu haben. Dem entgegen haben fünf Teilnehmende das Übersichtsdokument lediglich überflogen oder nannten eine andersartige Verwendung. Von den 20 Teilnehmenden, die das Dokument seit Erhalt geöffnet haben, bewerteten es 18 generell als positiv. Sechs Befragte gaben zusätzlich oder stattdessen eine negative Meinung, sowie Verbesserungsmöglichkeiten an. Die beiden Teilnehmenden, die das Dokument seit Erhalt nicht geöffnet haben nannten hierfür mangelnde Zeit, sowie fehlenden Bedarf als Ursache. Ein Großteil der Befragten (17) aus Gruppe 1 beabsichtigte die zukünftige Nutzung des Übersichtsdokuments bei der Suche nach Informationen. Lediglich vier Teilnehmende gaben an, das Dokument in Zukunft nicht nutzen zu wollen. Zwei der 24 Befragten nannten darüber hinaus andere Verwendung, wie beispielsweise die Unterstützung bei der Bearbeitung eingehender E-Mails. Die Art der Verteilung des Dokuments wurde von den Mitgliedern der Gruppe 1 tendenziell als positiv bewertet. Auf der 7-Punkt Likert Skala (1: stimme gar nicht zu, 7: stimme voll zu) wurde hierbei ein Mittelwert von 5,0 mit einem Median von 6,0 erreicht. Die 16 Teilnehmenden aus Gruppe 2 wurden nach Gründen gefragt, weshalb sie das Übersichtsdokument nicht erhalten bzw. nicht wahrgenommen haben. Zehn Befragte sahen als möglichen Grund die geringe Auffälligkeit von E-Mails als wahrscheinlich an. Vereinzelt nannten hierbei Teilnehmende auch ein Mangel an Zeit, fehlende Relevanz, sowie die lange Zeitspanne zwischen Verteilung und Umfrage. Einer Person fehlte der persönliche Hinweis auf die E-Mail durch einen Vorgesetzten. Vier Teilnehmende konnten keine Gründe für die fehlende Wahrnehmung nennen. Alle Befragten aus Gruppe 2 wurden daraufhin um Vorschläge zur Verbesserung der Verteilung gebeten. Vier der 16 Teilnehmenden schlugen die Verwendung weitere Kommunikationskanäle vor, wie beispielsweise eine unternehmensinterne Kommunikationsplattform. Ebenfalls rieten vier Befragte zur mehrfachen Aussendung der E-Mail, sowie zur Anforderung einer Lesebestätigung durch den Informationssicherheitsbeauftragten. In drei Fällen wurde eine bessere Kennzeichnung der E-Mail zur Steigerung der Aufmerksamkeit angeregt. Eine Person empfahl einen Hinweis durch die Vorgesetzten, beispielsweise während Besprechungen der Abteilungen.

9 DISKUSSION

Im folgenden Kapitel werden die Ergebnisse des Interviews und des Online-Fragebogens diskutiert und mögliche Implikationen für die Studie erörtert.

9.1 Diskussion Interview

Das Interview umfasste mit der Begriffsbestimmung, dem Verhalten beim Suchen von Informationen zum Thema IT-Sicherheit und dem Thema Zukunft drei Teile, wobei es um einen möglichen Speicherort, sowie Verteilung von wichtigen Dokumenten ging. Die Ergebnisse zeigen, dass der Begriff IT-Sicherheit im Vergleich zu Informationssicherheit geläufiger ist. Generell stellt sich hier jedoch die Frage, wie gut die eigentlichen Definitionen bekannt sind,

da dies für die Erkennung von IT- und Informationssicherheitsproblemen notwendig ist. Die Teilnehmenden sollten beschreiben, wie sie im Falle eines Informationssicherheitsvorfalles vorgehen würden. Hier zeigt sich, dass ein Großteil die einfachere Variante des telefonischen Kontakts, statt die vom Informationssicherheitsbeauftragten und der IT-Abteilung gewünschte Nutzung des Ticketsystems, bevorzugt. Da dieses jedoch mehr Zeit in Anspruch nimmt oder es sich oftmals nur um "kleinere" Anliegen handelt, ist es für die Beschäftigten einfacher und schneller direkt mit den Verantwortlichen zu sprechen. Dieses Vorgehen unterbricht die Arbeit der IT-Abteilung und kann so ein effektives Bearbeiten der Tickets verhindern. Jedoch sollte das Feedback der Teilnehmenden ernst genommen und überprüft werden, welche Möglichkeiten zur Verbesserung des Ticketsystem bestehen. Eine schnellere Bearbeitung der Tickets, könnte zu einer vermehrten Nutzung führen und somit Unterbrechungen durch kurze Anfragen reduzieren.

Die Mitarbeitenden werden ebenfalls dazu angehalten das Intranet für die Suche nach Informationen zu verwenden. Den meisten Beschäftigten ist das Intranet bekannt, jedoch verwendet es nur ein kleiner Teil, da die Nutzung laut Aussagen für manche zu umständlich gestaltet ist. Beautmeant et al. [4] haben herausgefunden, dass das Befolgen von Regeln und Vorgaben für die anwendenden Personen abhängig von einer Kosten-Nutzenrechnung ist. Daher sollte die Struktur und Verwendung des Intranets genau untersucht werden, um mögliche Fehlerquellen zu identifizieren und die Usability zu steigern. Bei der Überarbeitung des Intranets sollte vor allem auf die Art der Präsentation geachtet (Alohali et al. [1]) sowie die Kommunikation möglichst einfach und verständlich gehalten werden (Tkalac Verčič et al. [13]).

Ein Großteil der Teilnehmenden emopfanden das Intranet als Speicherort für das Übersichtdokument am geeignetsten. Als Alternative wurde ebenfalls von einigen Beschäftigten das Netzlaufwerk des Unternehmens genannt. Jedoch wurde diese Option durch den Informationssicherheitsbeauftragten ausgeschlossen, da nicht alle Mitarbeitende Zugriff auf das Laufwerk haben, sowie der Ausbau und die Nutzung des Intranet in der Zukunft weiter forciert werden soll. Ebenfalls wurde das Zeiterfassungssystem als Option genannt, welches aber für die Bereitstellung von Dokumente technisch nicht geeignet ist. Eine teilnehmende Person gab an, dass viele Beschäftigte das Intranet nicht verwenden, obwohl es eine Suchfunktion beinhaltet. Dieser Kommentar könnte ein Hinweis dafür sein, dass noch keine ausreichende Aufklärung zum Thema Intranet und dessen Verwendung betrieben wurde. In diesem Zusammenhang könnte es sinnvoll sein, den Beschäftigten einen kurzen Einführungskurs oder ein Tutorial zur Verfügung zu stellen. Da der Großteil der Teilnehmenden das Übersichtsdokument im Intranet erwarten würde, ist es naheliegend, dieses auch dort zu platzieren. Die Tatsache, dass ein Großteil der Teilnehmenden die im Mockup angegebene Stelle (Unterordner IT-Sicherheit im Intranet) bekannt war, ist ein weiteres Argument für die Verwendung des Intranets zur Bereitstellung des Übersichtsdokuments.

Auch bei der Art der Verteilung des Übersichtsdokuments waren sich die Teilnehmenden größtenteils dahingehend einig, dass die Prozesse durch Digitalisierung schneller und umweltschonender gestaltet werden können und sollten. So wurde die E-Mail als Verteilungsmedium am häufigsten genannt. Um die Digitalisierung weiter voranzutreiben besteht, seitens des Unternehmens, derzeit auch die Idee, einen digitalen Umlauf zu kreieren. Dieser digitale Umlauf soll die gleiche Funktion wie der papiergebundene aufweisen, jedoch über eine Software erreichbar sein. Vereinzelt wurden auch persönliche Kommunikationswege genannt, wie zum Beispiel Versammlungen oder Besprechungen. Die Bedeutung dieser Kommunikationskanäle sollte nicht unterschätzt werden, vor allem für Beschäftigte außerhalb der Verwaltung, die nur über einen begrenzten Computerzugang verfügen. Da viele Maßnahmen der Informationssicherheit (z.B. Zutrittsschutz) sich nicht nur auf Computerarbeitsplätze beschränken, ist es besonders wichtig, dass auch diese Abteilung alle notwendigen Informationen erhalten. Auf Grund des mehrheitlichen Meinungsbildes, wurde das Übersichtsdokument mittels E-Mail verteilt und der Erfolg über den Online-Fragebogen ermittelt.

Die Teilnehmenden gaben an, dass es zu viele Dokumenten mit Richtlinien gibt und sich diese Informationen teilweise überschneiden oder veraltet seien. Diese Tatsache zeigt die Bedeutung auf, wichtige Dokumente regelmäßig zu erneuern und gegebenenfalls zu entfernen, wenn Informationen veraltet sind. Insbesondere möchten wir hier erneut auf Kosten-Nutzenrechnung verweisen, welche nachweislich das Befolgen von Vorgaben und Richtlinien beeinflusst ([13]). Weiterhin gaben die Teilnehmenden an, nicht ausreichend Informationen über die möglichen Ansprechpartner im Unternehmen zu haben. Aus diesem Grund hat die angepasste Version des Übersichtsdokuments eine Infoseite mit Ansprechpartnern inklusive Kontaktinformationen und Bilder der Personen. Ebenfalls gaben die Teilnehmenden an, dass wichtige Dokumente derzeit zu dezentralisiert seien, somit die Übersicht erschwert wird und daher das Übersichtsdokument ein geeigneten Überblick liefert.

9.2 Diskussion Onlineumfrage

Die Onlineumfrage ergab weitere Einblicke in den Verteilungsprozess von wichtigen Dokumenten und vor allem deren Wahrnehmung. Auf die Frage der Informationsbeschaffung im Bereich IT- und Informationssicherheit zeigte sich, dass sich die meisten Beschäftigten direkt an die IT-Abteilung wenden würde und nicht das Ticketsystem verwenden. Dies stellt laut den Teilnehmenden die schnellste Variante dar, jedoch kommt es so für die IT-Abteilungen immer zu Unterbrechungen der eigentlichen Tätigkeiten. Entsprechend muss hier in Zukunft untersucht werden wie es möglich wäre, die Mitarbeitenden zur vermehrten Nutzung des Ticketsystems zu bringen. Etwa die Hälfte der Teilnehmenden hat angegeben, das Übersichtsdokument per E-Mail erhalten zu haben. Für ein solch wichtiges Dokument ist diese Rate nicht akzeptabel und sollte verbessert werden. Weiter ist fraglich, wie umfangreich und genau das Dokument von den Teilnehmenden gelesen wurde. Dies stellt jedoch auch für die alte Art der Verteilung ein Risiko dar, da es nicht möglich ist festzustellen, wie genau die Informationen gelesen wurden. Der papiergebundene Umlauf bietet derzeit noch den möglichen Vorteil, dass die Beschäftigten den Erhalt per Unterschrift bestätigen und so die Verantwortung übernehmen. Durch das Unterschreiben, könnten die Beschäftigten eine größeres Verantwortungsgefühl entwickeln und so eher zum Lesen der Dokumente angehalten sein. Aus diesem Grund soll auch ein digitalisierter Umlauf entstehen, bei dem die Beschäftigten den Erhalt ebenfalls bestätigen müssen. Auf die Nachfrage, wieso die E-Mail nicht wahrgenommen wurde,

gaben viele Beschäftigte das zu große Aufkommen an E-Mails an. Hierduch würden einzelne E-Mails übersehen werden und untergehen oder zu sehr von der aktuellen Arbeit ablenken. Auch sei die Wichtigkeit der E-Mail nicht auf den ersten Blick ersichtlich. Ebenfalls hätten sich die Teilnehmenden hier eine Kommunikation über unterschiedliche Kanäle gewünscht. Die Ergebnisse zeigen, dass das Medium E-Mail in seiner aktuell verwendeten Form, für die Verteilung wichtiger Dokumente nicht geeignet ist. Die mangelnde Wahrnehmung kann verschiedene Gründe haben. Beispielsweise war es im Unternehmen das erste Mal, dass ein wichtiges Dokument mittels E-Mail statt Umlauf verteilt wurde, weshalb Mitarbeitenden unter Umständen nicht auf diese Art der Verteilung vorbereitet waren. So war es uns jedoch möglich einen unverfälschten Einblick in den Verteilungsprozess mittels E-Mail zu erhalten. Weitere Verbesserungen der Wahrnehmung und Verteilung werden im folgenden Kapitel besprochen.

10 FAZIT UND LESSON LEARNED

Im Verlauf dieses Forschungsvorhabens haben sich verschiedene Punkte ergeben, die für die zukünftige Forschung relevant sind und helfen können, das Themengebiet noch besser zu ergründen.

10.1 Beteiligung von Beschäftigten

Im Zuge der Auswertung der Daten stellte sich die Frage, ab wann Vorschläge von Beschäftigten für die Umsetzung berücksichtigt werden können und sollten. Kann hierfür beispielsweise die einmalige Nennung eines Vorschlags genügen oder muss ein bestimmter Anteil der Antworten ein Thema abbilden, bevor es als Vorschlag für die Umsetzung in Betracht kommt. Ebenfalls stellte sich die grundsätzliche Frage, wie man mit Vorschlägen von Beschäftigten umgeht, die aus Sicht der Forschenden im Anwendungsfall unmöglich umsetzbar sind oder nach deren Einschätzung sogar gegenteilige Wirkung entfalten könnten. Bei der Beteiligung von Beschäftigten muss also das Ziel sein, eine gute Balance zwischen realistischer Umsetzung und Wertschätzung jedes einzelnen Beitrags zu finden. Im konkreten Anwendungsfall wurde daher entschieden, im Nachgang zur Datenerhebung einen kurzen Text an alle Beschäftigten des Unternehmens zu versenden, mit dem auf die Abwägungen und Ergebnisse der Studie eingegangen wird. Hierdurch sollte auch die Akzeptanz der Studie und die Bereitschaft zur Teilnahme an zukünftigen weiteren Studien erhöht werden.

10.2 E-Mail als Medium zur Verteilung

Der untersuchte Ansatz, Informationen in Form eines Übersichtsdokuments per E-Mail zu verteilen, wurde von den Beschäftigten allgemein positiv aufgenommen, bietet jedoch in der Praxis einige Vor- und Nachteile. Teilnehmende nannten die Schnelligkeit sowie die Möglichkeit, alle Beschäftigten unabhängig vom Arbeitsort zu erreichen, als klaren Vorteil dieses Kommunikationswegs. Besonders durch die zunehmende Verbreitung von flexiblen Arbeitsmodellen und der räumlichen Verteilung von Beschäftigten, besteht hierin ein deutlicher Vorteil im Vergleich zu klassischen Ansätzen der Verteilung von Informationen. Weiterhin bieten E-Mails die Möglichkeit, zugehörige Inhalte unmittelbar als Anhang oder beispielsweise als Verweis auf ein Netzlaufwerk oder das Intranet verfügbar zu machen. Auch Welch et al. [17] schlussfolgern in ihrer Arbeit, dass es besser ist, Links zu Dokumenten zu versenden, statt die Beschäftigten selbstständig im internen Netz suchen zu lassen. Der Kommunikationsweg hat sich vor allem während der COVID-19-Pandemie als besonders wichtig erwiesen, aber auch einige Schwächen und Nachteile aufgezeigt. In einem Unternehmensumfeld, in dem viele Beschäftigte beispielsweise einer Tätigkeit in Werkstätten nachgehen, ist unter Umständen nicht jeder Beschäftigte gleichermaßen gut mittels E-Mail erreichbar. Auch durch das Einrichten von Postfächern für alle Beschäftigten, lässt sich das Problem nur bedingt auffangen, da für diese die Bearbeitung von E-Mails in der Regel nicht zum Arbeitsalltag gehört oder hierfür kein geeignetes Zugriffsgerät am Arbeitsplatz zur Verfügung steht. In einem derartigen Umfeld kommt der Informationsverbreitung über unterschiedliche Kanäle besondere Bedeutung zu.

10.2.1 Erhöhung der Wahrnehmung. Viele Beschäftigte gaben an, dass durch die Anzahl an täglich empfangenen E-Mails sowie die Tatsache, dass die Wichtigkeit einer Nachricht für die empfangende Person nicht direkt erkennbar ist, die Gefahr besteht, dass Informationen leicht übersehen werden oder in Vergessenheit geraten. Gleichzeitig ist die Erinnerung an eine E-Mail nur mittels einer weiteren E-Mail möglich, wodurch ein möglicher Überfluss an Nachrichten noch weiter verstärkt wird.

Folglich stellt sich die Frage, wie man die Aufmerksamkeit der Empfangenden auf - aus Sicht des Unternehmens - wichtige E-Mails lenken kann, ohne die Anzahl an Nachrichten und die damit einhergehende Unübersichtlichkeit zu steigern. Einige Studien haben sich mit diesem Thema befasst und zum Beispiel die Organisation von Postfächern [9, 11], Design des Posteingangs [5] sowie spezielle Programme betrachtet, die wichtige Informationen automatisch hervorheben sollen [16]. Fehlende Hinweise auf Nachrichten können eine mögliche Ursache für unzureichende Wahrnehmung von E-Mails sein. Iqbal und Horvitz [6] haben in diesem Zusammenhang untersucht, wie mögliche Benachrichtigungen wahrgenommen werden und wie sehr diese in der Praxis von der eigentlichen Hauptaufgabe ablenken. Beispielsweise können gewisse Informationen (Reize) gefiltert und ausgeblendet werden, um die Konzentration für eine bestimmte Aufgabe zu erhöhen. Im Falle der E-Mail können beispielsweise als erster mögliche Filter der Betreff und die Sender-Information dienen, auf deren Grundlage die Wichtigkeit einer Nachricht bestimmt werden kann. Ein weiterer möglicher Ansatz für eine Verbesserung der Kommunikation wäre, das einzelne Abteilungen innerhalb einer Organisation die eigenen versendeten E-Mails entsprechend unterschiedlich visuell kennzeichnen (z.B. durch verschiedene Einfärbung), sodass diese bereits auf den ersten Blick im Posteingang auf den Absendenden hinweisen.

10.2.2 Anforderung von Empfangsbestätigung. Im Anwendungsfall der Stadtwerke Ettlingen (SWE) wird der sogenannte Umlauf eingesetzt, um wichtige Informationen oder verbindliche Dienstanweisungen innerhalb des Unternehmens zu verbreiten und die Kenntnisnahme der Beschäftigten durch Unterschrift nachzuweisen. Der vorherrschende Prozess ist papiergebunden und daher langsam und unflexibel, weswegen der Wunsch nach einem digitalen Umlauf

auf Basis der bestehenden IT-Infrastruktur besteht. Grundsätzlich bietet sich beim Versand einer E-Mail die Möglichkeit, Empfangsbestätigungen einzuholen. Besonders beim Versand an eine große Zahl von Personen besteht das Problem, die Empfangsbestätigungen sinnvoll zu verwalten. Ein möglicher Ansatz wäre der Einsatz eines Systems, bei dem entsprechende E-Mails (neben einer visuellen Kennzeichnung) einen gesonderten Link enthalten, über den die Kenntnisnahme des Inhalts bestätigt werden kann. Hierdurch kann einerseits eine interne Liste über den Erhalt der Informationen geführt werden, ohne ein Papier von Arbeitsplatz zu Arbeitsplatz wandern zu lassen. Andererseits kann auf fehlende Bestätigungen zielgerichtet und automatisch mit einer Erinnerung reagiert werden, ohne den Posteingang aller Beschäftigten überfüllen zu müssen. Eine Verteilung über einen solchen digitalen Umlauf wäre wesentlich schneller und flexibler als der bisherige Prozess und ermöglicht es, alle Mitarbeitenden gleichzeitig zu erreichen.

10.3 Gestaltung von Richtlinien

Besonders bei Organisationen mit sehr heterogener Struktur und diversen unterschiedlichen Abteilungen, ergeben sich grundsätzliche Herausforderungen an die Gestaltung und Ausrichtung von Richtlinien zur IT-Sicherheit. So sollte bei der Erstellung und Pflege von Richtlinien der unterschiedliche Fokus von Abteilungen betrachtet werden, da nicht alle Informationen oder Richtlinien für alle Mitarbeitenden von gleicher Bedeutung sind. Beispielsweise sind Richtlinien im Bezug auf Datenschutz für Beschäftigte der Personalabteilung relevanter, als für Beschäftigte in der Produktion. Durch ein vorheriges Filtern und Anpassen der Informationen an die einzelnen Abteilungen, könnte sich die Informationsaufnahme durch die Beschäftigten insgesamt verbessern lassen.

10.4 Studiendesign bei heterogener Organisation

Im Laufe der Studiendurchführung hat sich gezeigt, dass durch die Diversität der verschiedenen Gruppen an Beschäftigten im Unternehmen ein einfacher Querschnitt womöglich nicht allen Gruppen im gleichen Maße gerecht werden kann. Dementsprechend könnte hier eine erweiterte Zielgruppenanalyse mit Identifikation der zu unterscheidenden Gruppen zielführend sein. Ebenfalls könnte man durch noch spezifischeres Zuschneiden von Interviews und Umfragen auf die Zielgruppen, einen positiven Effekt auf die Akzeptanz der Teilnahme erreichen. Beispielsweise könnte hierzu die Diskussionsform der Fokusgruppe mit verschiedenen Personen aus verschiedenen Abteilungen durchgeführt werden. Beschäftigte mit wenig Erfahrung bei der Teilnahme an Studien, sollten eine besonders intensive Einführung erhalten. Insgesamt sollte mehr Zeit und Mühe in den Studienabschnitt des Briefings fließen, womit beispielsweise die Erklärung zur Verarbeitung von Daten im Rahmen von wissenschaftlichen Studien oder die ethischen Grundsätze (Anonymität der Daten, Verpflichtung gegenüber den Teilnehmenden und nicht der Führung der Organisation, physische Sicherheitsrisiken, etc.) adressiert werden. Dies könnte ebenfalls dabei helfen, potentiell vorhandene Ängste zu reduzieren und damit insgesamt zu besseren Ergebnissen führen. Dieser Artikel soll einen erster Baustein für zukünftige Forschung und eine Verfeinerung der Methodik darstellen.

Im Sinne der Usability und des iterativen Designs, gilt es die neuen Umsetzungen weiter zu evaluieren und mittels Feedback durch Nutzende weiter zu verbessern. Erst wenn das System als einfach angesehen wird und die Informationen verständlich genug sind, kommt es zu einer Adaption durch die Nutzenden. In diesem Sinne gilt diese Studie als weitere Grundstein zur Verständnis der Kommunikation über E-Mail, sowie die Verbreitung von wichtigen betriebsinternen Richtlinien.

10.5 Ausblick

Auf Basis unserer Forschung ergeben sich verschiedene Ansatzpunkte für zukünftige Forschung, beispielsweise das Thema der Kommunikation mit den Beschäftigten. Die E-Mail wurde zwar von der Mehrheit als das geeignete Mittel genannt, jedoch ergeben sich durch die Verwendung der E-Mail in der üblichen Form der Organisation Probleme. Hierbei stellt sich die Frage, wie ohne Einführung eines neuen System, das bekannte System E-Mail weiterhin verwendet und trotzdem genug Aufmerksamkeit erzeugt werden kann, dass ein höherer Anteil der Beschäftigten die Informationen wahrnehmen. Mögliche Ansatzpunkte sind die Gestaltung der E-Mail, Erweiterung des System z.B. durch Anforderung von Lesebestätigungen oder die Kombination der E-Mail mit anderen Kanälen. Dabei sollten andere Kanäle lediglich zum Hinweis auf die E-Mail und nicht als paralleler Kanal zur gleichen Vermittlung verwendet. Auch in der grundsätzlichen Durchführung von Forschung direkt innerhalb von Organisationen sind noch methodische Fragen offen. Wie kann der Hintergrund, die Relevanz und der Ablauf eine Studie in einer Organisation gegenüber Beschäftigten kommuniziert werden. Welchen Einfluss hat alleine die Studiendurchführung auf die Beschäftigten selbst wenn diese nicht alle direkt beteiligt sind und wie können Organisationen mit sehr heterogenen Strukturen (Abteilungen/Tochter-Organisationen) erforscht werden. Wie können hier Mixed-Method Ansätze Anwendung finden und helfen, mit verschiedenen Methoden in den heterogenen Strukturen die gleiche Frage, anstelle unterschiedlicher Fragen in der gleichen Gruppe, zu beantworten.

ACKNOWLEDGEMENTS

This research was supported by funding from the topic Engineering Secure Systems, subtopic 46.23.01 Methods for Engineering Secure Systems, from the Helmholtz Association (HGF) through the Competence Center for Applied Security Technology (KASTEL) and from KASTEL Security Research Labs.

Wir möchten uns auch bei für die Zusammenarbeit mit den Stadtwerken Ettlingen und insbesondere dem Informationssicherheitsbeauftragten bedanken, da ohne diese Kooperation und Hilfsbereitschaft, diese Studie nicht möglich gewesen wäre.

REFERENCES

[1] Manal Alohali, Nathan Clarke, Steven Furnell, and Saad Albakri. 2017. Information security behavior: Recognizing the influencers. In *2017 Computing Conference*. IEEE, ., 844–853. https://doi.org/10.1109/SAI.2017.8252194

[2] Mutlaq Alotaibi, Steven Furnell, and Nathan Clarke. 2016. Information security policies: A review of challenges and influencing factors. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, ., 352–358.

[3] Stefan Bauer, Edward WN Bernroider, and Katharina Chudzikowski. 2017. Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *computers & security* 68 (2017), 145–159.
[4] Adam Beautement, M Angela Sasse, and Mike Wonham. 2008. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop*. ACM, ., 47–58.
[5] Jacek Gwizdka. 2002. Reinventing the inbox: supporting the management of pending tasks in email. In *CHI'02 Extended Abstracts on Human Factors in Computing Systems*. ACM, ., 550–551.
[6] Shamsi T Iqbal and Eric Horvitz. 2010. Notifications and awareness: a field study of alert usage and preferences. In *Proceedings of the 2010 ACM conference on Computer supported cooperative work*. ACM, ., 27–30.
[7] Mary L McHugh. 2012. Interrater reliability: the kappa statistic. *Biochemia medica* 22, 3 (2012), 276–282.
[8] Brian Shackel. 2009. Usability–Context, framework, definition, design and evaluation. *Interacting with computers* 21, 5-6 (2009), 339–346.
[9] Nikash Singh, Martin Tomitsch, and Mary Lou Maher. 2013. Understanding the management and need for awareness of temporal information in email. In *Proceedings of the Fourteenth Australasian User Interface Conference-Volume 139*. Australian Computer Society, Inc, ., 43–51.
[10] Zahoor Ahmed Soomro, Mahmood Hussain Shah, and Javed Ahmed. 2016. Information security management needs more holistic approach: A literature review. *International Journal of Information Management* 36, 2 (2016), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009
[11] Agnieszka Matysiak Szóstek. 2011. 'Dealing with My Emails': Latent user needs in email management. *Computers in Human Behavior* 27, 2 (2011), 723–729.
[12] Todor Tagarev and Dimitrina Polimirova. 2019. Main Considerations in Elaborating Organizational Information Security Policies. In *Proceedings of the 20th International Conference on Computer Systems and Technologies*. ACM, ., 68–73.
[13] Ana Tkalac Verčič and Nina Pološki Vokić. 2017. Engaging employees through internal communication. *Public Relations Review* 43, 5 (2017), 885–893. https://doi.org/10.1016/j.pubrev.2017.04.005
[14] Melanie Volkamer and Benjamin Bachmann. 2021. Security Sensibilisierung für Beschäftigte: Empfehlungen für Informationssicherheitsbeauftragte. https://publikationen.bibliothek.kit.edu/1000132482
[15] Melanie Volkamer and Martina Angela Sasse. 2022. Leitfaden des workstreams „effektive it-security- awareness: Wirksam ... https://www.dialog-cybersicherheit.de/storage/uploads/ws21-endprodukte/WS4%20-%20Effektive%20IT-Security%20Awareness.pdf
[16] Wei Wang, Saghar Hosseini, Ahmed Hassan Awadallah, Paul N Bennett, and Chris Quirk. 2019. Context-aware intent identification in email conversations. In *Proceedings of the 42nd International ACM SIGIR Conference on Research and Development in Information Retrieval*. ACM, ., 585–594.
[17] Mary Welch. 2012. Appropriateness and acceptability: Employee perspectives of internal communication. *Public Relations Review* 38, 2 (2012), 246–254. https://doi.org/10.1016/j.pubrev.2011.12.017 Strategically Managing International Communication in the 21st Century.

ANHANG

Codebook Interview

Bekanntheit von IT-Sicherheit und Informationssicherheit	
Code Bezeichnung	Definition
1 Begriff bekannt	Die Begriffe IT-Sicherheit und Informationssicherheit sind dem Teilnehmer bekannt
2 IT-Sicherheit geläufiger	Dem Teilnehmer ist der Begriff IT-Sicherheit geläufiger.
3 Nicht beantwortet	Die Frage wurde durch den Teilnehmer nicht beantwortet.
4 Missverständnis IT	Der Teilnehmer hat missverstanden, dass es sich bei der Frage um IT- und Informationssicherheit handelt. Dementsprechend denkt der Teilnehmer lediglich an IT.
5 Beides geläufig	Dem Teilnehmer ist sowohl IT- als auch Informationssicherheit geläufig.

Begriffsbestimmung, gleich oder unterschiedlich:	
Code Bezeichnung	Definition
6 Unterschied unbekannt	Der Unterschied zwischen IT-Sicherheit und Informationssicherheit, ist dem Teilnehmer nicht bekannt.
7 Kein Unterschied	Der Teilnehmer gibt an, dass zwischen den beiden Begriffen IT- und Informationssicherheit kein Unterschied besteht.
8 Unterschied	Der Teilnehmer gibt an, dass zwischen den beiden Begriffen IT- und Informationssicherheit ein Unterschied besteht.
9 Definition falsch	Der Unterschied zwischen IT-Sicherheit und Informationssicherheit wurde durch den Teilnehmer falsch definiert. à Nicht verwenden wenn Code 11 verwendet wurde.
10 Definition richtig	Der Unterschied zwischen IT- und Informationssicherheit wurde von dem Teilnehmer richtig definiert/ beschrieben.
11 Missverständnis IT	Der Teilnehmer hat missverstanden, dass es sich bei der Frage um IT- und Informationssicherheit handelt. Dementsprechend denkt der Teilnehmer lediglich an IT.
12 Unzureichende Information Definition	Der Teilnehmer nennt eine scheinbar richtige Definition, es fehlen jedoch Informationen um zu bestimmen ob diese auch komplett richtig ist.

Verhalten, Vorgehen bei Suche von Informationen:	
Code Bezeichnung	Definition
13 Suchvorgang unbekannt	Der Teilnehmer weiß nicht wie man vorgehen sollte um Informationen zum Thema IT- und Informationssicherheit zu erhalten.
14 Schulung ausreichend	Der Teilnehmer empfindet die Sicherheitsschulungen als ausreichend, um Informationen über das Thema IT- und Informationssicherheit zu erhalten.
15 Suchvorgang falsch	Das genannte Vorgehen durch den Teilnehmer um an Informationen zum Thema IT- und Informationssicherheit zu kommen ist nicht wie geplant.
16 Suchvorgang richtig	Das genannte Vorgehen durch den Teilnehmer um an Informationen zum Thema IT- und Informationssicherheit zu kommen ist wie geplant.
17 Kontaktieren IT	Der Teilnehmer würde die IT (Herr G.) kontaktieren um Informationen zum Thema IT- und Informationssicherheit zu erhalten.

Verhalten, Welche Informationssicherheitsvorgaben bekannt:	
Code Bezeichnung	Definition
18 E-Mails	Der Teilnehmer nennt Informationssicherheitsvorgaben mit Fokus auf E-Mails.
19 Authentifizierung	Der Teilnehmer nennt Informationssicherheitsvorgaben mit Fokus auf Authentifizierung.
20 Surfen und Downloaden	Der Teilnehmer nennt Informationssicherheitsvorgaben mit Fokus auf Surfen und Downloaden.
21 Mobile Geräte	Der Teilnehmer nennt Informationssicherheitsvorgaben mit Fokus auf mobile Geräte.
22 Mobile Datenträger	Der Teilnehmer nennt Informationssicherheitsvorgaben mit Fokus auf mobile Datenträger.
23 Social Engineering	Der Teilnehmer nennt Informationssicherheitsvorgaben mit Fokus auf Social Engineering.
24 Clean Desk und Betriebsfremde	Der Teilnehmer nennt Informationssicherheitsvorgaben mit Fokus auf Clean Desk und Betriebsfremde.
25 Datenschutz	Der Teilnehmer nennt Informationssicherheitsvorgaben mit Fokus auf Datenschutz.
26 Klassifizierung von Dokumenten	Der Teilnehmer nennt Informationssicherheitsvorgaben mit Fokus auf Klassifizierung von Dokumenten.
27 Andere Vorgaben	Der Teilnehmer nennt Informationssicherheitsvorgaben mit einem nicht aufgeführten Fokus.

Verhalten, Vorgehen bei IT-Sicherheitsvorfall:	
Code Bezeichnung	Definition
28 Vorgehen korrekt	Der Teilnehmer nennt die vorgegeben Vorgehensweise bei einem IT-Sicherheitsvorfall. Gerät abschalten, Netzkabel rausziehen und die Verbindung zum Netzwerk trennen. Danach Meldung bei der IT-Abteilung.
29 Vorgehen inkorrekt	Der Teilnehmer nennt nicht die vorgegebene Vorgehensweise.
30 IT-Abteilung informieren	Der Teilnehmer nennt als Teil des Vorgehens bei einem IT-Sicherheitsvorfall, diesen der IT zu melden nachdem die anderen beiden Schritte abgeschlossen wurden.
31 Netzstecker	Der Teilnehmer nennt als Teil des Vorgehens bei einem IT-Sicherheitsvorfall den Netzstecker zu ziehen.
32 Netzwerkkabel	Der Teilnehmer nennt als Teil des Vorgehens bei einem IT-Sicherheitsvorfall das Netzwerkkabel zu ziehen.
33 Gerät ausschalten	Der Teilnehmer nennt das Gerät auszuschalten, jedoch ohne dabei zu erwähnen, das der Netzstecker gezogen werden würde.

Zukunft, wo müssen Dokumente liegen:	
Code Bezeichnung	Definition
34 Intranet korrekt	Der Teilnehmer nennt explizit das Intranet und den Dokument Ordner, ich welchem die Dateien liegen.
35 IT-Sicherheit Ordner	Der Teilnehmer schlägt einen IT-Sicherheit Ordner im Intranet vor, oder sagt, dass dieser existiert.
36 Nur Intranet	Der Teilnehmer nenn lediglich das Intranet als Suchoption, die Nennung des speziellen Dokument-Ordners fehlt.
37 Laufwerk	Der Teilnehmer spricht von einem gewissen Laufwerk, auf dass er während der Arbeit Zugriff hat. Intranet wird hierbei nicht spezifisch erwähnt.

Zukunft, Kennen sie den Ort:	
38 IT-Sicherheit im Intranet unbekannt	Dem Teilnehmer ist nicht bekannt, dass dort auch Informationen zum Thema IT-Sicherheit zu finden sind.
39 Intranet/ Dokumente bekannt	Dem Teilnehmer ist die Stelle Intranet/Dokument bekannt
40 Intranet bekannt	Dem Teilnehmer nennt, dass ihm das Intranet bekannt ist.

Zukunft, finden sie diesen Ort geeignet + besserer Ort:	
Code Bezeichnung	Definition
41 Nie zugegriffen	Der Teilnehmer gibt an, im Intranet noch nicht unter Dokumente gewesen zu sein.
42 Intranet/ Dokumente als Stelle ungeeignet	Der Teilnehmer gibt an, dass die Stelle ungeeignet ist um die Informationen zu platzieren.
43 Besserer Ort genannt	Der Teilnehmer nennt einen besseren Ort für das Dokument

Zukunft, wie verteilen:	
Code Bezeichnung	Definition
44 Verteilen E-Mail	Der Teilnehmer nennt die E-Mail als Verteiloption.
45 Umlauf	Der Teilnehmer nennt den Umlauf als passenden Verteiler.
46 Verbesserung	Der Teilnehmer nennt einen Verbesserungsvorschlag, mit welchem die Informationen besser wahrgenommen werden können.
47 Schulung	Der Teilnehmer benennt die Schulung als eine gute Option, um die Leute auf das Intranet und deren Inhalt aufmerksam zu machen.
48 Persönliche Ansprache	Der Teilnehmer nennt, dass eine persönliche Ansprache in Form einer Betriebsversammlung, durch den Vorgesetzten oder Tag der Sicherheit am besten wäre, um auf die Informationen aufmerksam zu machen.
49 Intranet Verteilung	Der Teilnehmer nennt das Intranet als ein gutes Mittel um die Informationen an alle zu Verteilen.

Zukunft, Umlauf der beste Weg:	
Code Bezeichnung	Definition
50 Umlauf beste	Der Teilnehmer, nennt den Umlauf als da bessere Mittel um die Mitarbeiter über das Dokument zu berichten, oder würde dies über andere Möglichkeiten präferieren.
51 Digital beste	Der Teilnehmer würde einen digitalen Weg bevorzugen, wobei hier kein spezifischer Weg beschrieben wurde.
52 Umlauf + Digital	
53 Umlauf nicht beste Weg	Der Teilnehmer gibt an, dass der Umlauf nicht der beste Weg ist, gibt jedoch auch keine bessere Variante an.

Zukunft, anderer Weg:	
Code Bezeichnung	Definition
54 Kein besserer Weg	Der Teilnehmer kann keinen besseren Weg, über welchen wie Mitarbeiter mehr Information erhalten könnten.
55 Newsletter (neg/pos)	Der Teilnehmer nennt den Newsletter als Möglichkeit über neue Dokumente aufzuklären.
56 Schwarzes Brett (neg/pos)	Der Teilnehmer nennt das schwarze Brett als Informationskanal.
57 Monitor (neg/pos)	Der Teilnehmer empfindet die Monitore als keinen guten Kanal, um
58 Poster (neg/pos)	Der Teilnehmer nennt Poster als Kanal, entweder im positiven oder negativen Zusammenhang.
59 Genug Kanäle	Der Teilnehmer gibt an, dass es genug Kanäle gibt, über die Informationen verteilt werden.
60 E-Mail (pos/neg)	Der Teilnehmer gibt E-Mail als möglichen Kanal im positiven oder negativen Sinne an.
61 Papier (pos/neg)	Der Teilnehmer merkt an, dass Papier immer noch ein guter Weg sei, oder schlecht.
62 Umlauf (pos/neg)	Der Teilnehmer nennt den Umlauf als positiv oder negative Weg um auf Informationen hinzuweisen.
63 Awareness Maßnahme (neg/pos)	Die Awarenessmaßnahme wurde negativ oder positiv von dem Teilnehmer erwähnt um Informationen zu verbreiten.
64 Andere Maßnahme (neg/pos)	Der Teilnehmer nennt eine andere Maßnahme bei der die Information verbreitet werden kann.

Codebook Umfrage

Wie gehen Sie vor, wenn Sie in Ihrem Unternehmen Informationen im Bereich IT-Sicherheit oder Informationssicherheit suchen?	
Code	Beschreibung
1 Intranet	Es wird das Intranet genannt um Informationen zu suchen.
2 Kollegen	Die Person gibt an, sich bei Fragen an Kollegen oder Vorgesetzte zu wenden.
3 Sicherheitsbeauftragter	Die Person würde sich bei Fragen an den IT-Sicherheitsbeauftragten wenden.
4 Internet	Es wird das Internet verwendet um mögliche Informationen zu erhalten.
5 IT	Bei Fragen, würde sich die Person mit der IT-Abteilung des Unternehmens in Verbindung setzen.
6 Betriebsvereinbarung	Es werden Informationen in der Betriebsvereinbarung gesucht.
7 HumHub	Die Person würde Informationen über das HumHub suchen.
8 E-Mails	Es wird angegeben, Informationen in vorhandenen E-Mails zu suchen.
9 Ticket	Die Person würde ein Ticket bei der IT öffnen.
10 Laufwerk	Es werden nach Informationen in dem Laufwerk gesucht.
11 Awareness-Portal	Informationen werden über das Awareness-Portal gesucht.
12 Verantwortliche Person	TeilnehmerIn gibt an, sich an die verantwortliche Person zu wenden, wobei nicht genau gesagt wird, wer diese Person ist.

In wie weit haben Sie das Übersichtdokument bisher genutzt?	
Code	Beschreibung
13 Verwendet	Das Dokument wurde bereits in irgendeiner Form verwendet.
14 Nicht verwendet	Das Dokument wurde bisher noch nicht verwendet.
15 Gelesen	Das Dokument wurde gelesen. Wird nur in Verbindung mit „Verwendet" kodiert.
16 Überflogen	Das Dokument wurde überflogen. Wird nur in Verbindung mit „Verwendet" kodiert.
17 Andere Verwendung	Es werden Beispiele für eine andersartige Verwendung des Dokuments gegeben.
18 Keine Angabe	

Sie haben angegeben, sich bereits das Übersichtsdokument angeschaut zu haben. Was ist Ihre generelle Meinung zu dem Übersichtdokument?	
Code	Beschreibung
19 Positiv	Das Übersichtsdokument wird als positiv wahrgenommen und mögliche Erklärungen gegeben.
20 Negativ	Das Übersichtsdokument wird als negativ wahrgenommen und mögliche Erklärungen gegeben.
21 Verbesserung	Es werden mögliche Verbesserungen für das Übersichtsdokument genannt.

In welcher Situation würden Sie zukünftig das Übersichtsdokument nutzen?	
Code	Beschreibung
22 Informationssuche	TeilnehmerIn gibt an eine Frage zu haben und/oder das Dokument zur Suche von Informationen zu verwenden.
23 Nie	Es wird angegeben, dass das Dokument in Zukunft nie verwendet werden würde.
24 Keine Ahnung	Es wird explizit angegeben, dass die Person keine Ahnung hat, ob das Dokument in Zukunft verwendet wird.
25 E-Mail	TeilnehmerIn gibt an, das Dokument zur Verarbeitung von E-Mails zu verwenden.
26 Anders	Es werden andere Situationen oder Gründe zu Verwendung genannt.

Sie haben angegeben, das Dokument noch nicht angeschaut zu haben. Warum haben Sie sich das Übersichtsdokument noch nicht angeschaut?	
Code	Beschreibung
27 Zeit	Es wird angegeben, dass Zeit ein Grund für das Nichtanschauen ist.
28 Kein Bedarf	Es wird angegeben, dass bisher kein Bedarf bestand das Dokument zu lesen.

Haben Sie Anmerkungen zu der Art der Verteilung? Was hat Ihnen gefallen?	
Code	Beschreibung
29 Positiv	TeilnehmerIn empfindet die Verteilung als positiv, nennt jedoch explizit keine genauen Gründe. Wird nicht in Verbindung mit anderen Codes wie z.B. „Schnell" kodiert.
30 Schnell	Verteilung wird als schnell wahrgenommen.
31 Nonsense	Die eigentliche Frage wurde falsch verstanden und/oder falsch beantwortet. Antwort bezieht sich nicht auf Verteilung.
32 Keine Meinung / Nichts	Es werden keine positiven Punkte genannt, oder die Person hat keine Meinung.
33 Erreichbarkeit	Es wird hervorgehoben, dass durch die Art der Verteilung viele Adressaten erreicht werden können. Kann in Verbindung mit Code „All-Users" stehen.
34 All-Users	Der Kommunikationsweg über All-Users wird explizit (d.h. benannt) hervorgehoben.
35 Verweis	Der Verweis auf die Dokumente im Intranet wird als positiv empfunden.
36 Anhang	Es wird als positiv empfunden, dass die E-Mail das Dokument ebenfalls als Anhang enthält.
37 Starterpaket	Bei Arbeitseinstieg das Dokument erhalten.

Haben Sie Anmerkungen zu der Art der Verteilung? Was hat Ihnen nicht so gut gefallen?	
Code	Beschreibung
38 Nichts	Es werden keine Anmerkungen gemacht.
39 Fehlende Aufmerksamkeit	Die E-Mail geht in den ankommenden E-Mails oder Arbeitsaufträgen „unter"/wird nicht wahrgenommen.
40 Medium E-Mail	Das Medium E-Mail wird als negativ empfunden. Schließt auch Aussagen zu AllUser mit ein.
41 Verteilungsprozess	Das Vorgehen der Verteilung (z.B. nur einmalige Sendung) wird als negativ empfunden.

Haben Sie Anmerkungen zu der Art der Verteilung? Was könnte verbessert werden?	
Code	Beschreibung
42 Nichts	Keine Anmerkungen zur Verbesserung.
43 Informationen	Es wird angemerkt, dass einige Informationen fehlen oder mehr Informationen gegeben werden könnten.
44 Humhub	Es soll das HumHub zur Verteilung der Informationen verwendet werden.
45 Umlauf	Es soll der Umlauf verwendet werden.
46 Persönlicher Hinweis	Es soll persönlich in Teambesprechungen oder Abteilungstreffen auf das Dokument hingewiesen werden.
47 Persönlichere Gestaltung	Die Nachricht sollte persönlich an die Kollegen gerichtet sein.
48 Wichtigkeit hervorheben	Die Wichtigkeit der Nachricht sollte hervorgehoben werden.
49 Mehrere Kommunikationskanäle	Es sollen mehrere Kommunikationskanäle verwendet werden.
50 Erinnerungsmail	Die Mail soll mehrfach verschickt werden.
51 Awareness-Portal	In dem Awareness-Portal sollte auf die Informationen hingewiesen werden.
52 Automatisch	Die Verteilung derartiger Informationen sollte automatisiert erfolgen.

Haben Sie eine Idee, woran es liegen könnte, dass Sie die E-Mail nicht wahrgenommen haben bzw. dass Sie sich vorhin nicht erinnern konnten, dass Ihnen das Dokument zugeschickt wurde?	
Code	Beschreibung
53 Keine Ahnung	TeilnehmerIn gibt keine Ahnung zu haben, wieso die E-Mail nicht erhalten oder gelesen wurde.
54 Zeitmangel	Es wird angegeben, dass fehlende Zeit ein Faktor für das Nichtlesen sein könnte.
55 Zu lange her	Es wird angegeben, dass die lange Zeitspanne zwischen E-Mail und Fragebogen ein Faktor für die fehlende Erinnerung sein könnte.
56 Auffälligkeit	Es wird angegeben, dass die E-Mail in dem Postfach nicht auffällt und/oder „untergegangen" ist.
57 Kein persönlicher Hinweis	Es wird angegeben, dass der zusätzliche Hinweis z.B. eines Vorgesetzten die Wahrnehmung verstärken könnte.
58 Nicht erhalten / gelöscht	Es wird angegeben, dass die Nachricht nicht erhalten oder (versehentlich) gelöscht wurde.
59 Unnötig	Der Inhalt der Nachricht wurde als unnötig empfunden und daher nicht wahrgenommen. Nur wenn Dokument explizit als unnötig bezeichnet wird, keine Interpretation der Aussage.
60 Link	Ein Link in der E-Mail, der direkt zu der Seite führt wäre vorteilhaft.

Wie könnte die Verteilung von wichtigen Dokumenten (insbesondere über E-Mail) in Zukunft verbessert werden?	
Codes	Beschreibung
61 HumHub	Es kann/sollte das HumHub zur Verteilung von Informationen verwendet werden.
62 E-Mail	Es wird eine Verbesserung mit E-Mail genannt.
63 Newsletter	Es wird der Newsletter als zusätzliche Informationsquelle genannt.
64 Kennzeichnung	Die E-Mail sollte besser gekennzeichnet sein, um die Wichtigkeit hervorzuheben.
65 Dokument an sich	Problem ist das Dokument an sich.
66 Keine Ahnung	Keine Nennung von möglichen Verbesserungen.
67 Lesebestätigung	Es wird eine Lesebestätigung zum Erhalt als Kontrolle vorgeschlagen.
68 Ansprache	Die Informationen sollten in einer Ansprache durch Vorgesetzte oder Kollegen hervorgehoben werden.
69 Abteilungsaddresse	Anstelle des All-Users, sollte die Abteilungsaddresse verwendet werden.
70 Mehrfachsendung	Die E-Mail sollte mehrfach verschickt werden.
71 IT-Awareness bereits OK	Es bedarf keine weitere Verbesserungen, da für die IT-Awareness bereits genug getan wird.
72 Link	Die E-Mail sollte verbessert werden und einen Direkten Link zu dem Dokument im Intranet bereitstellen.
73 Extra Intranet	TeilnehmerIn gibt an, dass die Dokumente einen speziellen Bereich im Intranet erhalten sollten.