Rudel, Steffi; Steinle, Nora; Kolb, Lisa

Working Paper

IT-Sicherheit im Human Resource Management: Kenntnisstand und Kompetenzaufbau

IT-Sicherheit im Human Resource Management: Kenntnisstand und Kompetenzaufbau

Steffi Rudel, Nora Steinle, Lisa Kolb

Universität der Bundeswehr München

Zusammenfassung

Aufgrund der exponierten Stellung im Unternehmen sowie der Verarbeitung von personenbezogenen und vertraulichen Daten sind Personalabteilungen (Human Resource Management, HRM) einem erhöhten Risiko für Cyberangriffe ausgesetzt. Das Ziel der vorgestellten Forschung ist es, die IT-Sicherheit im HRM zu untersuchen und zu erhöhen, wobei der Fokus dieses Beitrags auf dem Faktor Mensch liegt. Es wird eine Umfrage zum Kenntnisstand der IT-Sicherheit im HRM sowie ein Training zur Verbesserung der IT-Sicherheitskompetenz von HRM-Mitarbeitenden vorgestellt.

1 Einführung

Gemäß dem jährlichen Lagebericht des BSI zur IT-Sicherheit (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2022) ist das Risiko für Unternehmen, Opfer eines Cyberangriffs zu werden, in den letzten Jahren kontinuierlich gestiegen. Angreifer nutzen immer neue Angriffsmuster, um unberechtigt in die IT-Infrastruktur von Unternehmen einzudringen und dort illegale Aktivitäten (Sabotage, Spionage, Datendiebstahl etc.) durchzuführen.

Dies birgt gerade für das Human Resource Management (HRM), insbesondere im Rahmen der Personalbeschaffung (Recruiting), ein hohes Risiko. Als zentrale Abteilung sind für das HRM offene Schnittstellen zu externen, dem Unternehmen zumeist unbekannten Personen nötig, um Interaktionen zu ermöglichen (Riepen, A., 2019; Zafar et al., 2011). Auch wenn die Mitarbeitenden im HRM im Umgang mit externen Kontakten erfahren sind, sollte immer wieder das Bewusstsein für IT-Sicherheit geschärft werden, um ein gewisses Maß an Skepsis und Vorsicht aufrecht zu erhalten. So können potenzielle Risiken bei der Personalbeschaffung besser erkannt und der sog. Overtrust-Effekt (Verhoeven, 2020) reduziert werden.

Wichtig ist es beim Thema IT-Sicherheit, sich nicht alleine auf technische Maßnahmen zu verlassen – vielmehr müssen die drei Faktoren *Mensch – Technik – Organisation* gleichermaßen im Blick behalten werden. Die Mensch-Technik-Organisations-Analyse (MTO-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 Beitrags wird der Fokus zur IT-Sicherheit auf den Faktor Mensch gelegt, um durch gezielte Aus- und Weiterbildung die Kompetenz zur Erkennung und zur Abwehr von Angriffen im HRM zu fördern und so die IT-Sicherheit des gesamten Unternehmens zu erhöhen.

Folgende Forschungsfragen leiten den vorliegenden Beitrag:

1. Was ist der Kenntnisstand von Mitarbeitenden und Führungskräften im HRM in Bezug auf IT-Sicherheit?
2. Wie kann ein zielgruppenorientierter Kompetenzaufbau im HRM hinsichtlich IT-Sicherheit ermöglicht werden?

2 Kenntnisstand zur IT-Sicherheit im HRM

Um den Kenntnisstand zur IT-Sicherheit im HRM zu erheben (Forschungsfrage 1), wurde Mitte 2022 eine Online-Umfrage durchgeführt. Der Fragebogen der Umfrage wurde basierend auf *ISCA* zur Messung der IT-Sicherheits*kultur* (Da Veiga, 2018) sowie *HAIS-Q* zur Messung von IT-Sicherheits*bewusstsein* (Parsons et al., 2017) erstellt.

Die Befragung fand vom 01. Juni bis zum 31. Juli 2022 statt und wurde über drei Mittelstandsverbände in Deutschland, das Netzwerk LinkedIn sowie gezielt an einige ausgewählte Personen mit Personalverantwortung verteilt. Der Fragebogen wurde im gesamten Zeitraum 109-mal ausgefüllt, wovon nach anschließender Bereinigung $n=78$ Datensätze verwertbar waren.

Bei 30 % der Befragten handelte es sich um Führungskräfte, die restlichen 70 % waren Mitarbeitende. Im Folgenden werden einige ausgewählte Erkenntnisse präsentiert.

In einer der ersten Fragen wurde um eine Einschätzung gebeten, wie sicher sich die Befragten sind, den Unterschied zwischen *Datenschutz* und *IT-Sicherheit* zu kennen (Abbildung 1). Gerade bei den Mitarbeitenden zeigt die deutliche verneinende Einschätzung (22 Antworten bei 0 %), dass Ansätze zum Kompetenzaufbau in diesem Bereich zielführend sind.

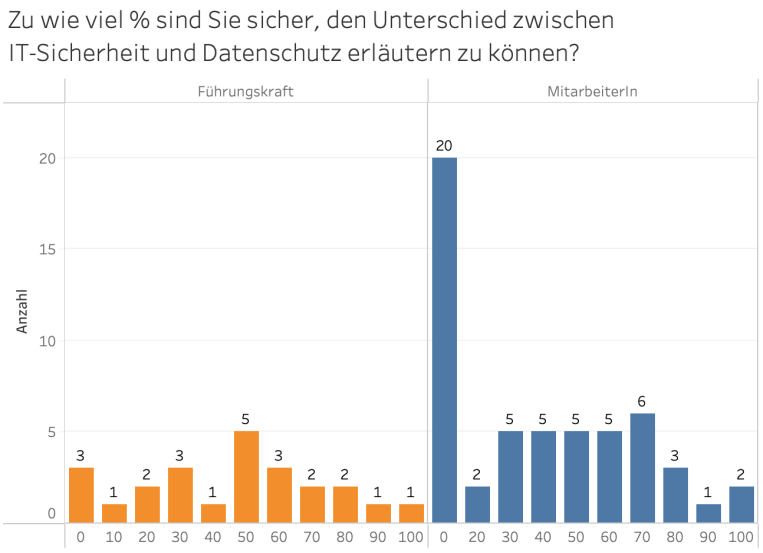

Abbildung 1: Sicherheit in der Unterscheidung IT-Sicherheit – Datenschutz

Die nachfolgenden Fragen (Abbildung 3 bis Abbildung 7) sollten anhand einer Likert-Skala von 0-5 beantwortet werden (Abbildung 2).

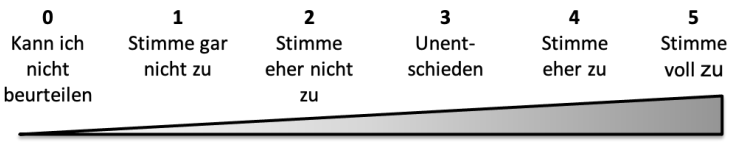

Abbildung 2: Likert-Skala

Einig sind sich die Meisten bei der Frage, ob die Verantwortlichkeit für IT-Sicherheit formell geregelt sein sollten. So stimmten mehr als 60 % der Führungskräfte und annähernd 50 % der Mitarbeitenden der Aussage voll und ganz zu (Abbildung 3).

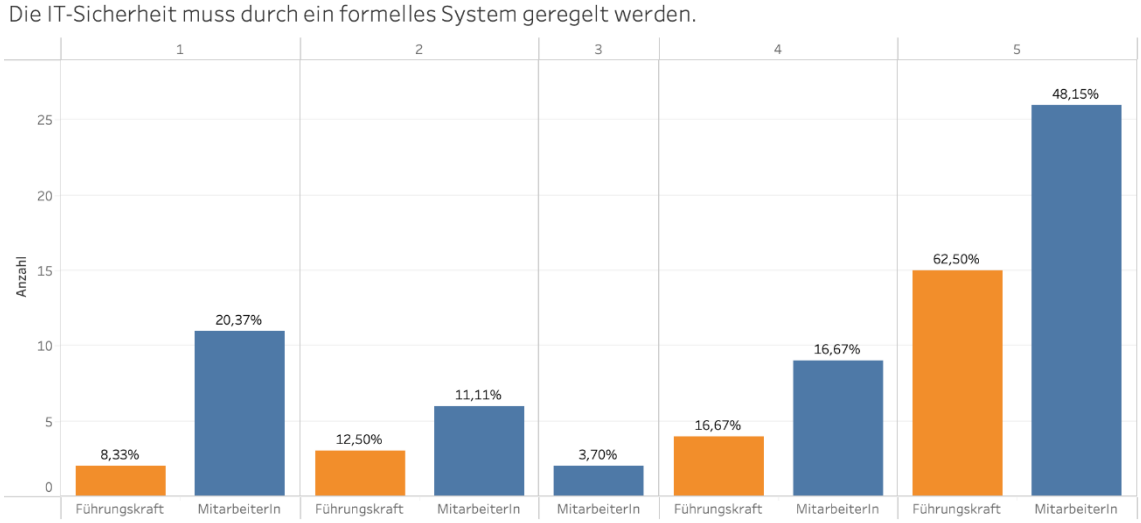

Abbildung 3: Regelung der IT-Sicherheit durch ein formelles System

Interessante Ergebnisse lieferten die Fragen zu den IT-Sicherheitsrichtlinien, also zu den formalen Vorgaben der IT-Sicherheit im Unternehmen. Dabei wurde unter anderem hinterfragt, ob die bestehende IT-Sicherheitsrichtlinie verständlich ist (Abbildung 4). Sowohl bei den Führungskräften als auch bei den Mitarbeitenden gaben mehr als 37% an, dies nicht beurteilen zu können – daraus lässt sich schlussfolgern, dass sie entweder die IT-Sicherheitsrichtlinie nicht kennen oder diese nicht existiert.

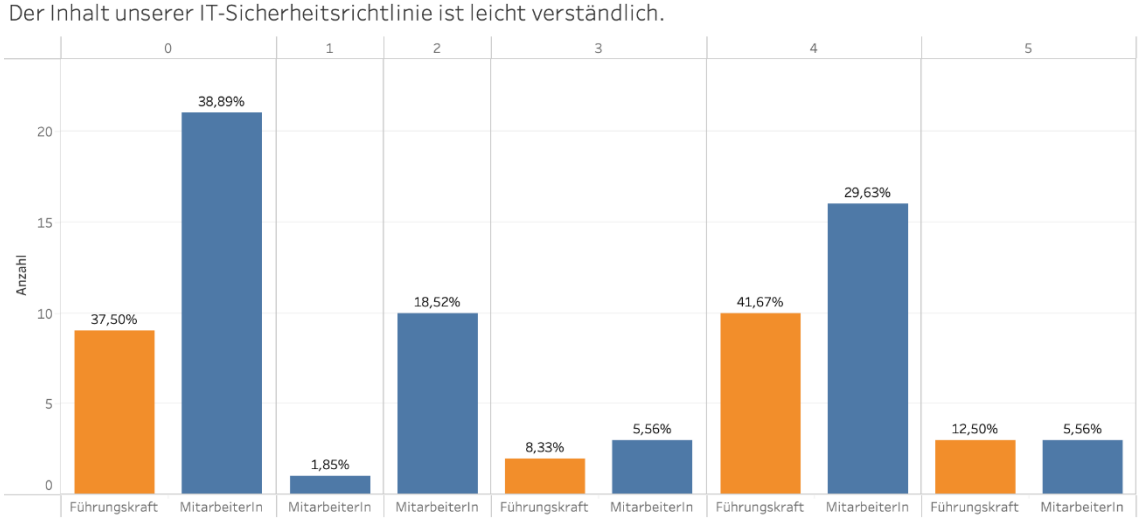

Abbildung 4: Frage nach der Verständlichkeit der IT-Sicherheitsrichtlinie im Unternehmen

Etwas besser sieht es bei der Frage nach dem Schutz sensibler/vertraulicher Daten von Mitarbeitenden aus. Die Antworten zeigen, dass über 57 % der Mitarbeitenden und über 75 % der Führungskräfte eher oder voll und ganz der Meinung sind, dass ihr Unternehmen diese Daten durch klare Richtlinien schützt (Abbildung 5).

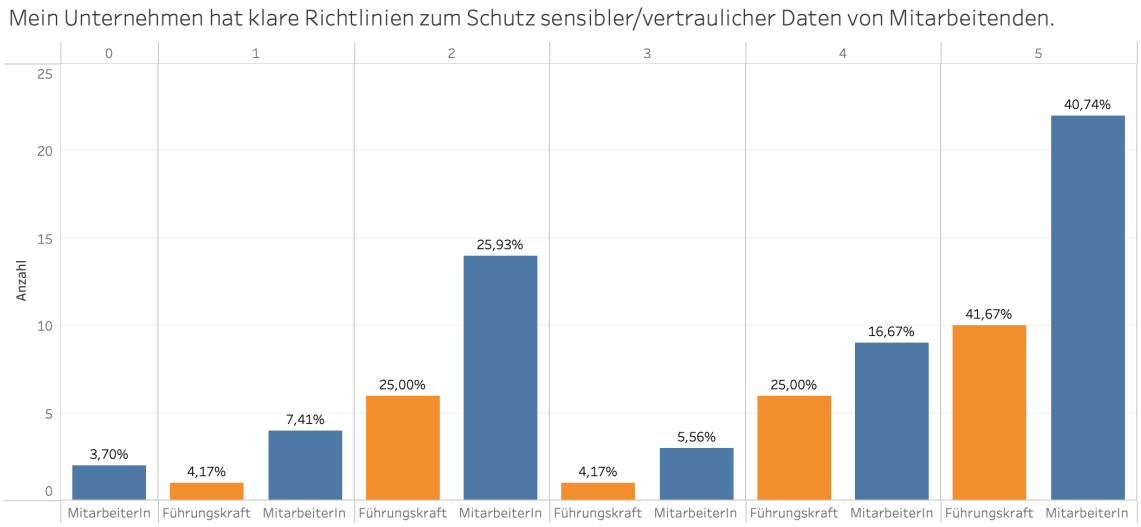

Abbildung 5: Frage nach klaren Richtlinien zum Schutz sensibler/vertraulicher Daten von Mitarbeitenden

Im nächsten Punkt wurde ein grundlegender Aspekt der IT-Sicherheit hinterfragt – denn einen USB-Stick mit Malware „absichtlich zu verlieren“ ist eine gängige Methode von Angreifern (Tischer et al., 2016). Wird der gefundene 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 6 ist zu erkennen, dass immerhin fast 30% der Führungskräfte und über 35% der Mitarbeitenden den Stick eher oder bestimmt anschließen würden, wodurch die IT-Sicherheit des Unternehmens gefährdet wäre.

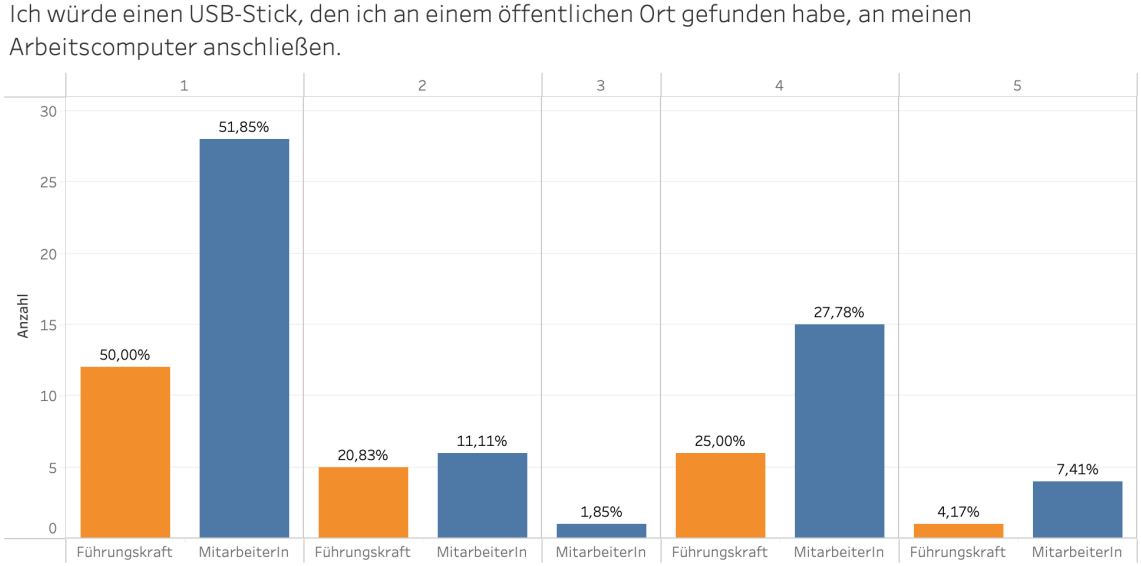

Abbildung 6: Unbekannten USB-Stick an PC anschließen

Nicht viel besser sieht es beim Klick-Verhalten auf Hyperlinks in E-Mails unbekannter Absender aus – ein Umstand, mit dem das Recruiting (als Teilbereich des HRM) fast täglich konfrontiert ist. Hier geben über 48 % der Mitarbeitenden und über 40 % der Führungskräfte an, solche Links eher oder bestimmt anzuklicken, wenn der Absender „interessant aussieht“ (Abbildung 7). Auch dieses Verhalten kann gerade für das HRM sehr gefährlich sein, da über einen angeklickten Link unbemerkt Schadsoftware auf dem Zielsystem platziert werden kann.

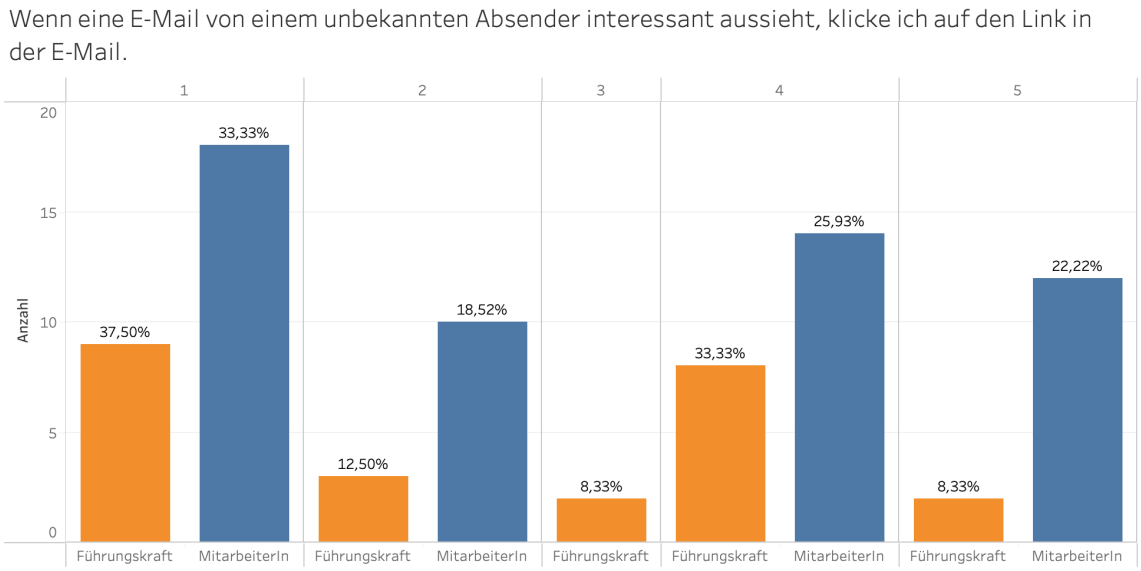

Abbildung 7: Klickverhalten auf Links in E-Mails unbekannter Absend

Zuletzt wurde danach gefragt, ob zusätzliche Schulungen zum Einsatz von IT-Sicherheitsinstrumenten als zielführend erachtet werden; über 57 % der Mitarbeitenden und mehr als 87 % der Führungskräfte stimmten dem zu.

Bei der Frage nach der gewünschten Methode (Mehrfachnennung möglich) erhielt das *praktische Training* mit Abstand die meisten Stimmen (Abbildung 8) – entsprechend wurde als Methode zum Kompetenzaufbau (Forschungsfrage 2) ein praktisches Training gewählt.

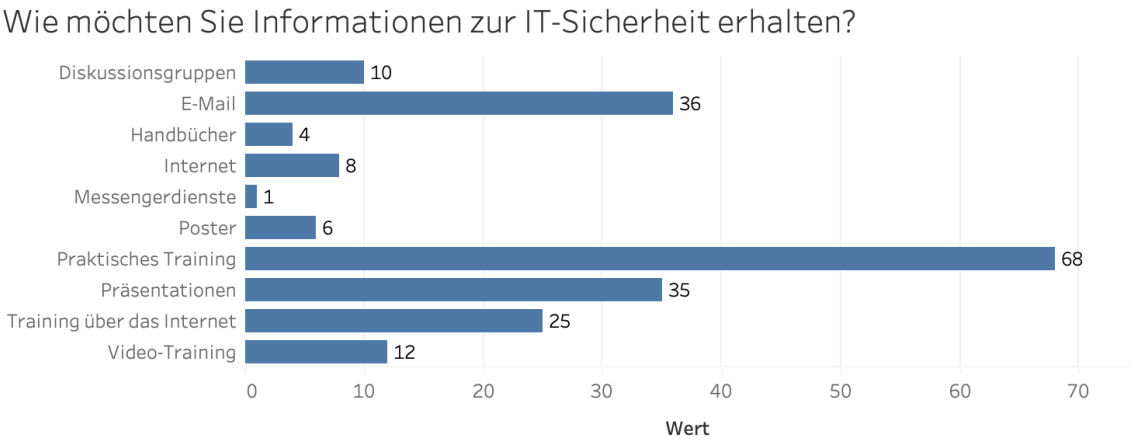

Abbildung 8: Wie sollen die Informationen vermittelt werden? (Mehrfachnennung möglich)

3 Kompetenzaufbau durch Training

Die fortschreitende Digitalisierung hat die Anforderung an die Weiterbildung von Mitarbeitenden grundlegend verändert; die Qualifizierung von digitalen Schlüsselkompetenzen sowie transformativer Kompetenzen („Future Skills“) gewinnt zunehmend an Bedeutung (Suessenbach, F. et al., 2021). Praktische Trainings sind eine Maßnahme, um die Mitarbeitenden beim Erwerb dieser Future Skills zu unterstützen (Kauffeld, S., 2016). Da darüber hinaus die Maßnahme „Praktische Trainings“ in der Umfrage die meisten Stimmen erhielt (Kapitel 2, Abbildung 8), wurde diese Methode zum Kompetenzaufbau der Mitarbeitenden im HRM bezüglich IT-Sicherheit (Forschungsfrage 2) ausgewählt.

Es sollte ein praxisnahes Trainingskonzept entwickelt werden, welches den bereits angesprochenen Dreiklang Technik, Mensch und Organisation in Bezug auf den Kompetenzaufbau von IT-Sicherheit im HRM vereint. Dabei galt es, den Grad der Sensibilisierung (Awareness) bezüglich der Sicherheitsgefahren auf die IT zu erhöhen und einen wirksamen Kompetenzaufbau bei den Mitarbeitenden im HRM zu ermöglichen.

Die Basis bildeten theoretische Grundlagen der IT-Sicherheit, der aktuelle Wissensstand von HRM zur IT-Sicherheit sowie die theoretischen Grundlagen von Trainingsmaßnahmen. Im Fokus der Konzipierung steht der Faktor Mensch, welcher nicht als Sicherheitsr*isik*o, sondern als Sicherheits*sensor* angesehen werden soll. Die Konzeption der praktischen Ausbildung basiert auf dem konstruktivistischen Lernansatz, der den aktiven Lernenden, welcher das Wissen selbst konstruiert, in den Mittelpunkt stellt (Kauffeld, S., 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, S, 2016). Um all diese Faktoren zu vereinen und den sonst eher abstrakten sowie technischen Konzepten und Modellen in der TI-Sicherheit zu trotzen, wurde auf der Basis des spielbasierten Ansatzes von Serious Games ein Kartenspiel entwickelt (Yasin, A. 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 für IT-Sicherheit, wie z. B. Riskio (Hart, S. 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 9).

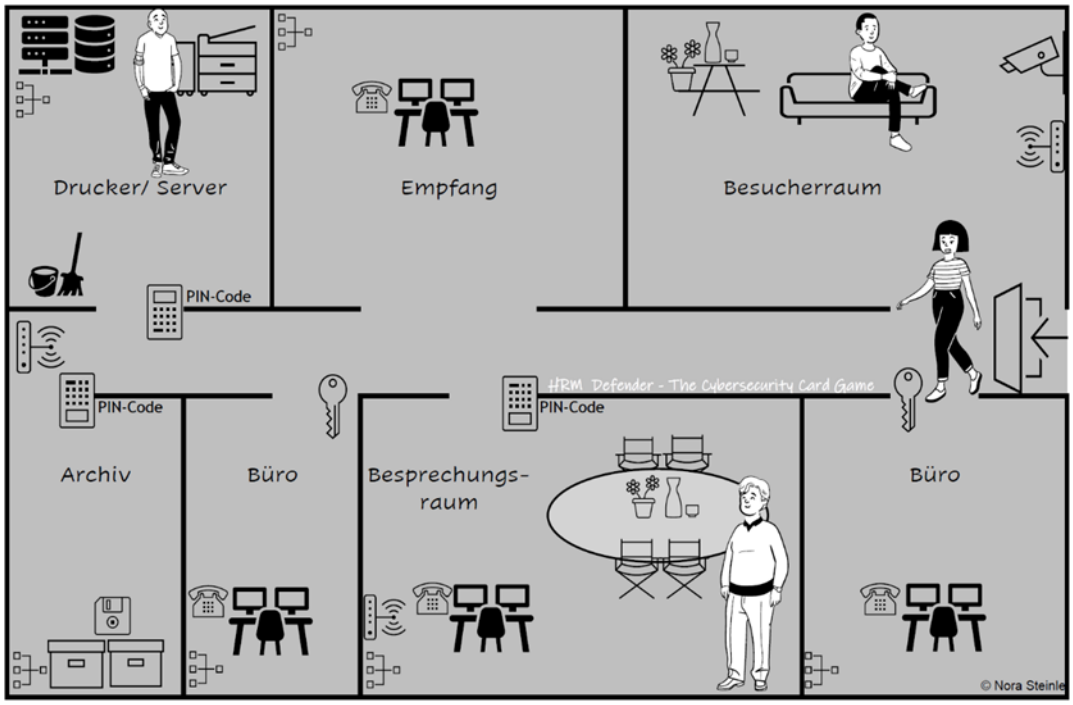

Abbildung 9: Prototyp des Spielfeldes HRM Defender - The Cybersecurity Card Game (eigene Darstellung)

Die folgende Abbildung 10 zeigt jeweils eine Beispielkarte der verschiedenen Kategorien.

Abbildung 10: Beispiele einer Verteidigungs-, Angriffs- sowie Informationskarte (v.l.n.r)

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, wird nach dem Training jeweils eine zweistufige Befragung auf der Basis von Grohmanns und Kauffelds *Questionnaire for Professional Training Evaluation* (Grohmann, A. & Kauffeld, S., 2013) durchgeführt.

Das Kartenspiel wird mit einem Spielleiter, sechs Spielern sowie einem Beobachter Ende April 2023 in einer Bundesbehörde als Pilot durchgeführt und anschließend evaluiert. Die gewonnenen Erkenntnisse fließen in die Verbesserung des Trainingskonzeptes ein.

4 Zusammenfassung & Ausblick

Einleitend wurde festgestellt, dass die Cyber-Bedrohungen für Unternehmen stetig zunehmen. Gerade der Bereich HRM ist aufgrund seiner exponierten Stellung und der verarbeiteten Daten besonders gefährdet. Da die IT-Sicherheit (neben technischen und organisatorischen Aspekten) stark von menschlichen Faktoren beeinflusst wird, wurde der Fokus in diesem Beitrag auf die Mitarbeitenden des HRM gelegt. Geleitet wurde der Beitrag durch zwei Forschungsfragen, die Frage nach dem Kenntnisstand zur IT-Sicherheit im HRM (Forschungsfrage 1) sowie einem Konzept zum Kompetenzaufbau im HRM hinsichtlich IT-Sicherheit (Forschungsfrage 2).

Zunächst wurde der Kenntnisstand im HRM zum Thema IT-Sicherheit in einer Online-Umfrage untersucht und in Kapitel 2 wurden ausgewählte Ergebnisse dargestellt. Als Ergebnis lässt sich festhalten, dass das Schaffen von Bewusstsein für IT-Sicherheitsrisiken und Maßnahmen von großer Notwendigkeit im HRM ist und die Mehrheit der Befragten praktische Trainings bevorzugen.

Anschließend wurde in Kapitel 3 das Kartenspiel *HRM Defender – The Cybersecurity Card Game* als ein solches praktisches Training vorgestellt. Da das Training als Pilot zeitlich erst nach der Einreichung dieses Beitrages durchgeführt wird, werden die Ergebnisse im Rahmen des Vortrages beim VHB-Workshop vorgestellt.

Im weiteren Verlauf der Forschung soll das Training in den nächsten Monaten mehrfach mit Unternehmen gespielt, evaluiert und so schrittweise weiterentwickelt werden.

5 Danksagung

Wir danken Bayern Innovativ für die Förderung des Projektes „Federated Learning Enhancing IT Security (FLEIS)“, Fördernummer DIK 0241-2104-0080, unseren Projekt- und Forschungspartnern, Herrn León Schwarz für die Durchführung der Online-Umfrage im Rahmen seiner Masterarbeit sowie den anonymen Reviewern des VHB-Herbstworkshops 2023 für das konstruktive Feedback.

Literatur

Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.). (2022). Die Lage der IT-Sicherheit in Deutschland 2022. Zugriff am 17.4.2023. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.html?nn=129410

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.

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.

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

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

Riepen, A. (2019). Warum IT-Sicherheit ein Thema für HR ist. *Personalmagazin*, (5/2019), 68–70.

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

Suessenbach, F., Winde, M., Klier, J., & Kirchherr, J. (2021). Future Skills 2021: 21 Kompetenzen für eine Welt im Wandel. Stifterverband für die Deutsche Wissenschaft e. V. Zugriff am 18.4.2023. Verfügbar unter: https://www.stifterverband.org/medien/future-skills-2021

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

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

Yasin, A., Liu, L., Li, T., & Fatima, R. (2019). Improving Software Security Awareness Using a Serious Game. *IET Software*, *13* (2), 159–169.

Zafar, H., Clark, J. G. & Ko, M. S. (2011). An Exploration of Human Resource Management Information Systems Security. *Journal of Emerging Knowledge on Emerging Markets*, *3* (1), 489–510.