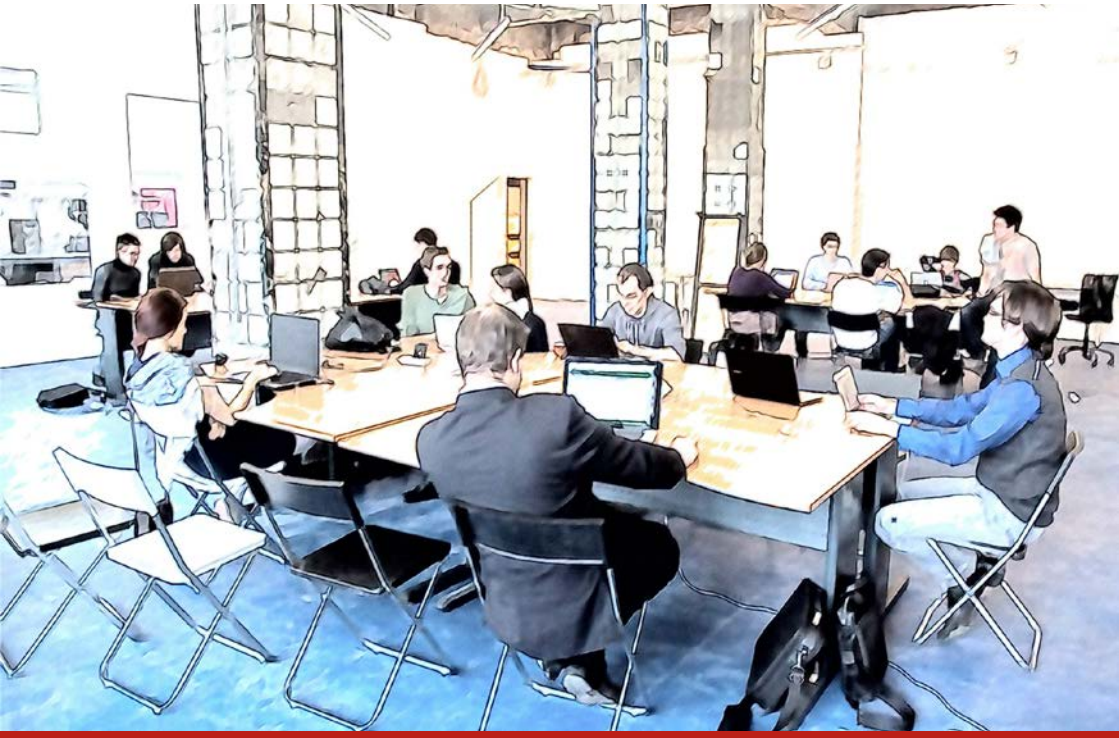
Mittelstand 4.0
Kompetenzzentrum
Cottbus



AUF DIE MITARBEITENDEN KOMMT ES AN

Die drei **B**s der Informationssicherheit – **B**ewusstsein, **B**efähigung, **B**efolgung

www.kompetenzzentrum-cottbus.digital

Mittelstand-
Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

IMPRESSUM

Herausgeber:
Mittelstand 4.0-Kompetenzzentrum Cottbus
c/o IHP GmbH - Innovations for High Performance Microelectronics/
Leibniz-Institut für innovative Mikroelektronik
Im Technologiepark 25
15236 Frankfurt (Oder)
info@kompetenzzentrum-cottbus.digital
Telefon: +49 335 5625 683

Vertreten durch: Geschäftsführer Prof. Dr.-Ing. Gerhard Kahmen und Manfred Stöcker

Autoren:
Dr. Erik Hermann

Satz/Layout:
maerkbar – Cottbus

Bildnachweis:
Umschlag: © geralt – www.pixabay.com
Seite 1: © TheDigitalWay – www.pixabay.com
Seite 2: © xresch – www.pixabay.com
Seite 7: © viarami – www.pixabay.com
Abbildungen 1–3/Tabelle 1: © Erik Hermann

MITARBEITENDE UND INFORMATIONSSICHERHEIT

„Das Prinzip Hoffnung regiert … Den meisten kleinen und mittelständischen Unternehmen in Deutschland ist bewusst, wie sehr ihre Arbeit mittlerweile von funktionierenden Computersystemen abhängig ist. Sie wissen auch, dass Cyberkriminalität eine Gefahr darstellt. Doch das Risiko, selbst einmal Opfer eines Cyberangriffs zu werden, verdrängen viele – es trifft ja immer nur die anderen."

Dieses Zitat stammt aus dem Leitartikel des Berichtes „Cyberrisiken im Mittelstand 2020" des Gesamtverbandes der Deutschen Versicherungswirtschaft[1] und zeichnet ein relativ düsteres Bild der Risikowahrnehmung mittelständischer Unternehmen. Diesen Aussagen liegen die Ergebnisse einer Forsa-Umfrage unter 300 kleinen und mittleren Unternehmen (KMU) aus dem Jahr 2020 zugrunde.
So gaben 69 Prozent der befragten KMU an, dass das Risiko von Cyberkriminalität für mittelständische Firmen in Deutschland eher hoch bis sehr hoch sei, für das eigene Unternehmen schätzten jedoch nur 28 Prozent der Befragten das Risiko eher hoch bis sehr hoch ein. Es lässt sich also eine gewisse Erwartungslücke feststellen, d. h. KMU scheinen das eigene Sicherheitsrisiko zu unterschätzen. Das könnte einem mangelnden oder zumindest der Realität nicht angemessenem Risikobewusstsein geschuldet sein. Damit ist bereits der erste zentrale Erfolgsfaktor für mehr Informationssicherheit in Ihrem Unternehmen angesprochen – das Bewusstsein für Sicherheitsbedrohungen und Gefährdungslagen. Dies bezieht sich jedoch nicht nur auf Sie – als Geschäftsführer/in, IT-Verantwortliche/r und/oder Administrator/in, sondern gilt vielmehr für alle Mitarbeitenden Ihres Unternehmens. Denn: „Auf die Mitarbeitenden kommt es an".

1 Gesamtverband der Deutschen Versicherungswirtschaft e. V. (2020). Cyberrisiken im Mittelstand 2020.

Im Folgenden zeigen wir, welche Faktoren und Ansätze das Verhalten Ihrer Mitarbeitenden im Hinblick auf Informationssicherheit und die Einhaltung von Sicherheitsvorgaben beeinflussen können. Dabei werden wir uns der drei **B**s bedienen. Das **B**ewusstsein und die **B**efähigung von Mitarbeitenden führen im Idealfall zur **B**efolgung von Sicherheitsvorgaben und -regelungen. Wir bevorzugen in dieser Broschüre den Begriff Informationssicherheit gegenüber den oftmals synonym verwendeten Begriffen IT-Sicherheit bzw. Cyber-Sicherheit. Der Begriff Informationssicherheit ist umfassender und beinhaltet alle Arten von Informationen und Daten (elektronisch und nicht-elektronisch verarbeitet und gespeichert).[2]

Informationssicherheit
Schutz aller Arten von Informationen, die sowohl in IT-Systemen elektronisch als auch nicht-elektronisch (Papierform, Wissen der Mitarbeitenden) gespeichert und verarbeitet werden[2]

IT-Sicherheit
Teilbereich der Informationssicherheit, der sich auf den Schutz elektronisch gespeicherter und verarbeiteter Informationen bezieht[2]

Cyber-Sicherheit
Schutz sämtlicher mit dem Internet und vergleichbaren Netzen verbundener IT und darauf verarbeiteter Informationen[2]

2 Bundesamt für Sicherheit in der Informationstechnik (2017). BSI Standard 200-2. IT-Grundschutz-Methodik.

MITARBEITENDE ALS TEIL DES PROBLEMS?

Allgemein lassen sich Gefährdungen der Informationssicherheit nach der Quelle der Gefährdung, d. h. intern oder extern und menschlich oder nichtmenschlich unterscheiden (siehe Abbildung 1).[3] Weiterhin können Gefährdungen unabsichtlich/zufällig auftreten oder absichtlich/vorsätzlich herbeigeführt werden.[3] Obwohl alle Arten von Gefährdungen (z. B. Cyber-Kriminalität, Hardware- und Softwarefehler) die Informationssicherheit Ihres Unternehmens beeinträchtigen und zum Verlust von Daten und Informationen führen können, konzentrieren wir uns vorliegend auf interne, menschliche Gefährdungen.

Diese Art der Gefährdungen kann von allen Mitarbeitenden ausgehen. In der Literatur wird mitunter von der Insider-Bedrohung („insider threat“) oder dem schwächsten Glied („weakest link“) der Informationssicherheitskette gesprochen.[4] Oftmals geschieht dies unabsichtlich oder zufällig, z. B. durch unbedachtes Öffnen eines E-Mail-Anhangs, der Schadsoftware enthält. Dementsprechend ist es wichtig, alle Mitarbeitenden für Gefährdungen einerseits und geltende Sicherheitsvorgaben andererseits zu sensibilisieren (**B**ewusstsein). Ob Sicherheitsvorgaben letzten Endes befolgt werden („Compliance“), kann von einer Vielzahl von Faktoren abhängen.

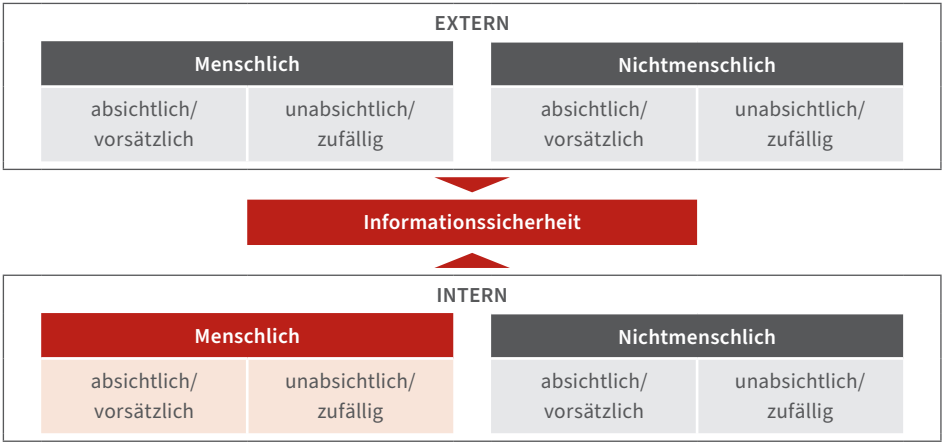


Abbildung 1 Gefährdungstypologie[3]

3 Loch, K. D., Carr, H. H., & Warkentin, M. E. (1994). Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly*, 16, 173–186. 4 Warkentin, M. E. & Willison, R. (2008). Behavioral and Policy Issues in Information Systems Security: The Insider Threat. *European Journal of Information Systems*, 18, 101–105.

Organisationale Einflussfaktoren

Unternehmensführung

Einen hohen Stellenwert für die Informationssicherheit nimmt die Unternehmensführung in zweierlei Hinsicht ein. Zum einen sollte die Geschäftsführung den Sicherheitsprozess initiieren, Strategien und Ziele definieren, finanzielle, zeitliche und personelle Ressourcen zur Verfügung stellen und die Gesamtverantwortung übernehmen.[5]

Zum anderen spielt Führung im Hinblick auf die Mitarbeitenden eine zentrale Rolle. So sollte sich die Geschäftsführung bewusst sein, dass:

a. Mitarbeitende der wichtigste und gleichzeitig schwächste Bestandteil von Informationssicherheitssystemen sind
b. das eigene Engagement, die eigene Beteiligung sowie Unterstützung von Mitarbeitenden die Einhaltung von Sicherheitsvorgaben verstärken
c. geeignete Führungsstrukturen und -praktiken Informationssicherheit fördern können.[6]

Der Führungsstil kann sich ebenfalls positiv auf die **B**efolgung von Sicherheitsvorgaben auswirken. Insbesondere ein transformativer Führungsstil, der durch Einflussnahme, durch Vorbildfunktion und Inspiration, intellektuelle Stimulierung und individuelle Förderung der Mitarbeitenden gekennzeichnet ist, entfaltet eine vorteilhafte Wirkung.[7] Eher passive und antiautoritäre Führungsstile hingegen sind weniger zielführend.[6, 8]

Unternehmenskultur

Neben dem Führungsstil kann auch die Unternehmenskultur Einfluss auf die Informationssicherheit und das Verhalten von Mitarbeitenden ausüben. Ähnlich wie ein antiautoritärer Führungsstil ist eine Unternehmenskultur, die Flexibilität zulasten eines gewissen Kontrollfokus (z. B. einheitliche, konsistente Regeln) (über-)betont, nicht zwangsläufig von Vorteil für ein effektives Informationssicherheitsmanagement.[9]

Regelungskomplexität

Regelungen – wie Sicherheitsvorgaben und -leitlinie – sollten also nicht nur strukturelle Elemente des Informationssicherheitsmanagements sein, sondern auch Elemente der Unternehmensführung und -kultur beinhalten. Bei den Sicherheitsvorgaben ist darauf zu achten, dass diese nicht zu komplex gestaltet sind. Sowohl die Regelungstiefe (die Anzahl der Komponenten, die einer Vorgabe/Regel untergeordnet sind) als auch die Anzahl der Regelungsverweise beeinflussen das Verständnis und die Einhaltung von Vor-

5 Bundesamt für Sicherheit in der Informationstechnik (2017). BSI Standard 200-2. IT-Grundschutz-Methodik. 6 Paliszkiewicz, J. (2019). Information Security Policy Compliance: Leadership and Trust, *Journal of Computer Information Systems*, 59, 211–217. 7 Guhr, N., Lebek, B., & Breitner, M. H. (2019). The Impact of Leadership on Employees' Intended Information Security Behaviour: An Examination of the Full-Range Leadership Theory. *Information Systems Journal*, 29, 340–362. 8 Feng, G., Zhu, J., Wang, N., & Liang, H. (2019). How Paternalistic Leadership Influences IT Security Policy Compliance: The Mediating Role of the Social Bond. *Journal of the Association for Information Systems*, 20, 1650–1691. 9 Ernest Chang, S. & Lin, C. (2007). Exploring Organizational Culture for Information Security Management. *Industrial Management & Data Systems*, 107, 438–458. 10 Lehmann, D. W., Cooil, B., & Ramanujam, R. (2020). The Effects of Rule Complexity on Organizational Noncompliance and Remediation: Evidence from Restaurant Health Inspections. *Journal of Management*, 46, 1436–1468.

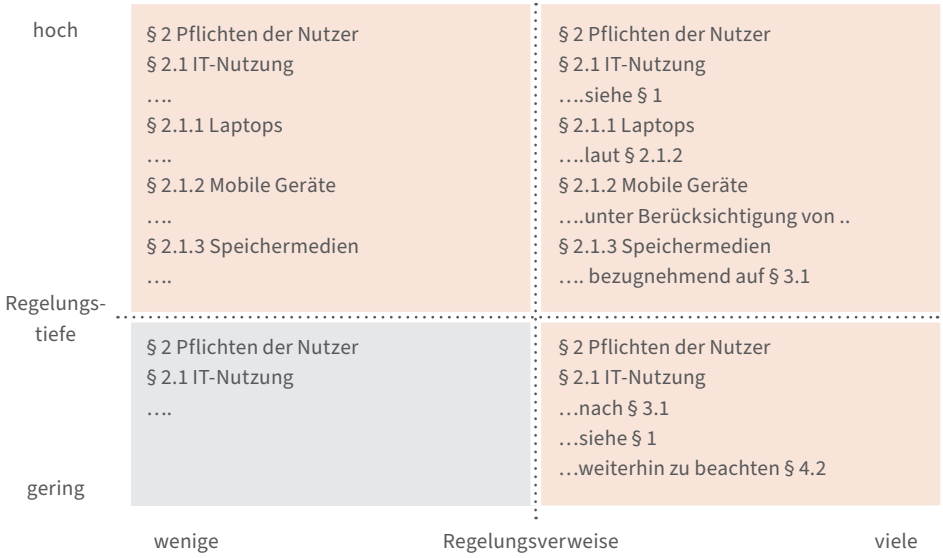


Abbildung 2 Regelungskomplexität

gaben.[10] Wie in Abbildung 2 dargestellt, sind Vorgaben und Regelungen mit eher geringer Regelungstiefe und wenigen Verweisen gegenüber komplexeren Regelungsstrukturen zu bevorzugen.

Personelle Einflussfaktoren

Ein zentraler, wenn nicht der zentrale Schritt zur Einhaltung von Informationssicherheitsvorgaben und sicherheitskonformen Verhaltensweisen ist das **B**ewusstsein für Informationssicherheit.[11] Eine vorhandene Sicherheitsleitlinie, Schulungen, die Sichtbarkeit von Sicherheitsmaßnahmen und die Beteiligung des Managements stärken dieses **B**ewusstsein rund um alle Regeln und Fragen der Informationssicherheit.[10]

Darüber hinaus sind verschiedene Erwartungen und Wahrnehmungen der Mitarbeitenden mit der **B**efolgung von Sicherheitsregelungen verbunden. Insbesondere fördern:

- der wahrgenommene Nutzen von Vorgaben und Maßnahmen
- die mit Sicherheitsmaßnahmen einhergehende wahrgenommene Nutzerfreundlichkeit bzw. Praktikabilität und

11 Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2019). Security Awareness: The First Step in Information Security Compliance Behavior. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2019.1650676.

- die Erwartung, bei Nichteinhaltung entdeckt oder sanktioniert zu werden das informationssicherheitskonforme Verhalten der Mitarbeitenden.[12]

Sehr umfangreiche und komplexe Sicherheitsregelungen wiederum können Mitarbeitende unter Druck setzen, sogenannten Technostress hervorrufen und das Gegenteil bewirken.[13] Es besteht die Gefahr, dass sich Mitarbeitende im Resultat moralisch von ihrer Verantwortung lösen und gegen Regelungen verstoßen. Dies kann auf unterschiedliche Art und Weise geschehen (siehe Tabelle 1).

Nicht zuletzt haben auch soziale Einflüsse[14, 15] (z. B. die Nachahmung der Verhaltensweisen von anderen Mitarbeitenden) und subjektive Normen[16] (z. B. die vermittelte Notwendigkeit, Regeln zu befolgen) Auswirkungen auf die **B**efolgung von Sicherheitsvorgaben.

Im Folgenden stellen wir Ihnen verschiedene Ansätze vor, die das Bewusstsein der Mitarbeitenden schärfen, sie befähigen und die **B**efolgung von Regelungen begünstigen. Unsere Überzeugung: Mitarbeitende sind ein Teil der Lösung und nicht ausschließlich ein Teil des Problems.

Moralische Rechtfertigung	Rechtfertigung von Verstößen durch Arbeitsaufkommen, Deadlines etc.
Herunterspielen	Darstellung von Verstößen als keine „große Sache“ oder irrelevant
Beschönigung	Rechtfertigung durch Vergleich mit gravierenderen Verstößen
Verantwortungsverweigerung	Begründung durch Arbeitsaufkommen
Verantwortungsverschiebung	Verantwortung eher bei Management, IT, anderen Mitarbeitenden
Verharmlosung	Verharmlosung des Schades von Verstößen für das Unternehmen
Fokusverschiebung	Schäden betreffen DAS Unternehmen, nicht die Mitarbeitenden
Schuldzuweisung	Darstellung von Verstößen als Folge von Unangemessenheit der Regeln

Tabelle 1 Formen der moralischen Loslösung[15]

12 Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly*, 43, 525–554. 13 D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, 31, 285–318. 14 Gwebu, K. L., Wang, J., & Hu, M. Y. (2020). Information Security Policy Noncompliance: An Integrative Social Influence Model. *Information Systems Journal*, 30, 220–269. 15 Veladi, A. & Warkentin, M. E. (2020). Can Secure Behaviors Be Contagious? A Two-Stage Investigation of the Influence of Herd Behavior on Security Decisions. *Journal of the Association for Information Systems*, 21, 428–459. 16 D'Arcy, J. & Lowry, P. B. (2019). Cognitive-Affective Drivers of Employees' Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study, *Information Systems Journal*, 29, 43–69.

MITARBEITENDE ALS TEIL DER LÖSUNG!

Sicherheitsleitlinie

Zunächst einmal sollten Sicherheitsziele, -vorgaben und -regelungen in einer Informationssicherheitsleitlinie festgehalten und offen kommuniziert werden. Die Leitlinie stellt Ihr Grundsatzdokument dar und sollte den Stellenwert der Informationssicherheit für Ihr Unternehmen, Ihre Geschäftstätigkeit und -prozesse unterstreichen. Weiterhin sollten:

- der Geltungsbereich der Leitlinie und Vorgaben beschrieben
- Ihre Verantwortung – als Geschäftsführung – für den Sicherheitsprozess und die Informationssicherheit allgemein betont und
- die Organisationsstruktur für die Umsetzung des Sicherheitsprozesses (welche Mitarbeitende werden wie eingebunden, wer ist der Informationssicherheitsbeauftrage) erläutert werden.

Schulungen

Die Sicherheitsleitlinie bildet schließlich die Grundlage für die Sensibilisierung und Schulung Ihrer Mitarbeitenden. Schulungen sollten jedoch nicht nur einmalig stattfinden, z. B. bei Verabschiedung der Sicherheitsleitlinie oder Einführung eines Informationssicherheitsmanagementsystems, sondern in regelmäßigen Abständen angeboten werden. Die in der Fachliteratur auch als SETA – **S**ecurity **E**ducation, **T**raining, **A**wareness[17] (Sicherheitsschulung, -training und -bewusstsein) bezeichneten Schulungsprogramme sollten:

- Bewusstsein für Sicherheitsrisiken und Gefährdungen schaffen
- verantwortungsvolles Verhalten aller Mitarbeitenden fördern
- Regelungsinhalte und entsprechende Anforderungen für alle Mitarbeitenden verständlich und nachvollziehbar vermitteln
- Mitarbeitende befähigen und trainieren, um Regelungen einzuhalten
- Problemstellungen, Herausforderungen und Widersprüche diskutieren

17 D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, 20, 79–98.

Für die Ausgestaltung und die Häufigkeit von Schulungen gibt es kein Patentrezept, vielmehr hängen diese von Ihrem Unternehmen (Prozesse, Strukturen, Unternehmensumfeld, Schutzbedarf etc.), Ihren Mitarbeitenden und dem Umfang der Informationssicherheitsvorgaben und -maßnahmen ab. Sie sollten also Schulungsformate an den Bedürfnissen Ihrer Mitarbeitenden ausrichten. Regelmäßige E-Mail-Newsletter und interne Briefings können Seminar- und Workshop-Formate ergänzen.

- Worauf muss ich achten?
- Welche Gefährdungen oder Risiken bestehen im Rahmen meiner (individuellen) Arbeit?
- An wen kann ich mich allgemein und speziell bei Sicherheitsvorfällen wenden?
- Wie verfahre ich bei Sicherheitsvorfällen?
- Was ändert sich?
- Welche Konsequenzen hätte mein Fehlverhalten?

Kommunikation

Für Schulungsformate, aber auch allgemein für die Vermittlung jeglicher Inhalte im Zusammenhang mit Informationssicherheit, sind zielgerichtete und adressatengerechte Sprache zentral.[18] Dementsprechend sollten Sie Kommunikationsbotschaften an Ihre Mitarbeitenden (Adressaten) anpassen. Da Informationssicherheit alle Mitarbeitenden in Ihrem Unternehmen betrifft, sollten die Inhalte selbst unverändert bleiben. Wie die Inhalte kommuniziert werden, kann sich jedoch unterscheiden. Vereinfacht gesagt: Sprechen Sie die Sprache Ihrer Mitarbeitenden. Einfache und verständliche Botschaften sind oft zielführender als umfangreiche technische Details oder Regelungskataloge. Ihre Kommunikation sollte die wesentlichen und relevanten Botschaften enthalten, die zu den betreffenden Mitarbeitenden passen. Mitarbeitende sollten beispielsweise Antworten auf die folgenden Fragen erhalten:

Zudem können Sie zwischen **du/ihr, wir** oder **Sie** bei der Ansprache Ihrer Mitarbeitenden unterscheiden. Außerdem können Sie explizit auf Gefährdungen, Bedrohungen und Risiken eingehen, um das Bewusstsein Ihrer Mitarbeitenden und die Einhaltung von Regelungen zu fördern.[19]
Wie bereits ausgeführt, unterliegt die Einhaltung von Informationssicherheitsregelungen unterschiedlichen personellen Einflüssen. Diese können Sie sich zunutze machen, um Ihre Kommunikationsmaßnahmen effektiver zu gestalten. So sollte für Mitarbeitende der persönliche Nutzen, Sicherheitsregeln zu befolgen, eindeutig hervorgehen. Weiterhin können Sie verdeutlichen, dass und wie sich andere Mitarbeitende bzw. die Belegschaft allgemein an Vorgaben halten und damit von subjektiven Normen und sozialen Einflüssen profitieren.

18 Johnston, A. C., Warkentin, M. E., Dennis, A. R., & Siponen, M. (2019). Speak their Language: Designing Effective Messages to Improve Employees' Information Security Decision Making. *Decision Sciences*, 50, 245–284. 19 Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly*, 39, 837–864.

Befähigung

Um einen Lernprozess einzuleiten und nachhaltige Lerneffekte zu erzielen, bedarf es der **B**efähigung Ihrer Mitarbeitenden. Dafür können Sie sich unterschiedlicher Instrumente und Methoden bedienen.
Einerseits können bestimmte Grundeinstellungen in Ihren IT-Systemen Fehlverhalten und Verstöße Ihrer Mitarbeitenden minimieren. Bevor Mitarbeitende E-Mail-Anhänge herunterladen oder speichern, könnte beispielsweise eine Abfrage zur Vertrauenswürdigkeit des Absenders erfolgen. Bei der Passwortvergabe können personalisierte Hinweise zur Passwortsicherheit und -anforderungen Mitarbeitende ebenfalls sensibilisieren und Lerneffekte ermöglichen.[20] Dies kann auch über Selbsteinschätzungen geschehen („Wie sicher würden Sie Ihr Passwort einschätzen?").[20] Um Selbstlernprozesse zu initiieren, können Sie Ihren Mitarbeitenden darüber hinaus einfache Entscheidungshilfen[21] zur Verfügung stellen. Entscheidungsbäume (siehe Abbildung 3) können aus einfachen Fragen mit Ja-Nein-Antwortmöglichkeiten bestehen und in verschiedenen Bereichen Anwendung finden, z. B. E-Mails und Anhänge und Verwendung externer Speichermedien.

Letzen Endes sollten alle Methoden und Schulungsmaßnahmen Ihre Mitarbeitenden befähigen, Sicherheitsrisiken selbst zu erkennen und entsprechend der Sicherheitsvorgaben zu handeln und/oder Rat bei den Sicherheitsexperten Ihres Unternehmens einzuholen.

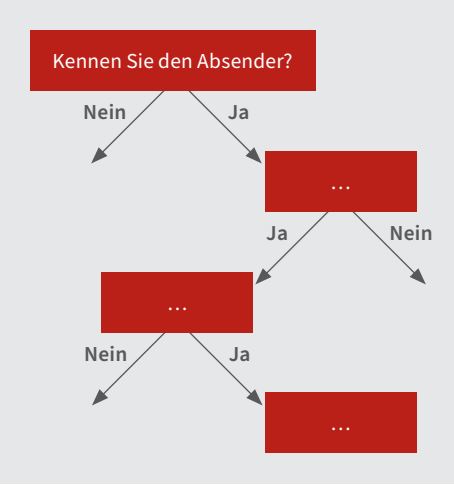


Abbildung 3 Entscheidungsbaum

20 Renaud, K. & Zimmermann, V. (2019). Nudging Folks towards Stronger Password Choices: Providing Certainty is the Key. *Behavioural Public Policy*, 3, 228–258. 21 Kozyreva, A., Lewandowsky, S., & Hertwig, R. (2020). Citizens versus the Internet: Confronting digital challenges with cognitive tools. *Psychological Science in the Public Interest*, 21, 103–156.

WAS IST MITTELSTAND-DIGITAL?

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.
Der DLR Projektträger begleitet im Auftrag des BMWi die Projekte fachlich und sorgt für eine bedarfs- und mittelstandsgerechte Umsetzung der Angebote. Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) unterstützt mit wissenschaftlicher Begleitung, Vernetzung und Öffentlichkeitsarbeit. Weitere Informationen finden Sie unter www.mittelstand-digital.de

Was ist das Mittelstand 4.0-Kompetenzzentrum Cottbus

Das Mittelstand 4.0-Kompetenzzentrum Cottbus setzt sich aus den fünf Partnern BTU Cottbus-Senftenberg (Projektleitung), Technische Hochschule Wildau, Hochschule für nachhaltige Entwicklung Eberswalde, IHP GmbH Leibniz-Institut für innovative Mikroelektronik Frankfurt (Oder) sowie IHK Cottbus als Vertreterin der Landesarbeitsgemeinschaft der Industrie- und Handelskammern in Brandenburg zusammen. Dabei stehen die Schwerpunkte Arbeit 4.0, Digitalisierung in Logistik und Produktion, IT-Sicherheit, Assistenzsysteme, Automatisierungstechnik, Robotik sowie Sozialpartnerschaften im Mittelpunkt. Das Zentrum gehört zu Mittelstand-Digital. Mit Mittelstand-Digital unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

KONTAKT

Mittelstand 4.0-Kompetenzzentrum Cottbus
c/o IHP GmbH - Innovations for High Performance Microelectronics/
Leibniz-Institut für innovative Mikroelektronik
Im Technologiepark 25
15236 Frankfurt (Oder)
Tel.: +49 335 5625 683
info@kompetenzzentrum-cottbus.digital
www.kompetenzzentrum-cottbus.digital

Folgen Sie uns: