REALITYCHECK: IT-SICHERHEIT IM ÖSTERREICHISCHEN MITTELSTAND

ELISABETH MAYERHOFER
FELIX STAHL
REINHARD PRÜGL

VORWORT

Sehr geehrte Leserinnen und Leser,

es freut uns, Ihnen die Ergebnisse der vorliegenden Studie „Realitycheck: IT-Sicherheit im österreichischen Mittelstand“ präsentieren zu dürfen. In einer zunehmend digitalisierten Welt sind Unternehmen jeder Größe mit einer stetig wachsenden Bedrohung durch Cyberkriminalität konfrontiert. Diese Bedrohungen nehmen nicht nur an Umfang, sondern auch an Raffinesse zu. Gerade für mittelständische Unternehmen, die aktuell im Fokus der Cyberkriminellen stehen, ist es daher von entscheidender Bedeutung, sich dieser Herausforderung bewusst zu sein und rechtzeitig angemessene Schutzmaßnahmen zu ergreifen.

Die vorliegende Studie ist das Ergebnis intensiver Forschungsarbeit in Verbindung mit einem einzigartigen Studiendesign. Diese Studie kombiniert Erkenntnisse aus einer repräsentativen Umfrage unter über 200 Geschäftsführern mittelständischer Unternehmen mit der Auswertung von Daten aus über 180 IT-Sicherheitsüberprüfungen (IT-Audits), die anonymisiert vom IT-Dienstleister techbold zur Verfügung gestellt wurden. Wesentliches Ziel dieser Initiative ist, heimische Unternehmen für die aktuelle und immanente Bedrohungslage zu sensibilisieren und bei der Identifizierung von Schwachstellen und der Bewertung von Risiken bzw. der Implementierung wirksamer Sicherheitsstrategien zu unterstützen. Wir haben uns darüber hinaus mit den neuesten Entwicklungen in der Welt der Cyberkriminalität auseinandergesetzt und untersucht, wie sich diese auf mittelständische Unternehmen auswirken.

Unsere Studie beinhaltet nicht nur eine Bestandsaufnahme der Schwachstellen, sondern bietet auch praxisnahe Empfehlungen für Wirtschaft, Politik und Gesellschaft, wie Unternehmen – und dabei insbesondere der Mittelstand – ihre Cybersicherheit verstärken können.

Denn der österreichische Mittelstand ist die tragende Säule der heimischen Wirtschaft.

Wir hoffen und sind zuversichtlich, dass diese Studie eine wertvolle Informationsquelle für Politik, Wirtschaft und Gesellschaft, aber vor allem für Führungskräfte und Entscheidungsträger in mittelständischen Unternehmen darstellt. Ihre Cybersecurity-Bemühungen sind von entscheidender Bedeutung, nicht nur für den Schutz Ihrer Daten und Ihres geistigen Eigentums, sondern auch für das Vertrauen Ihrer Kunden und den langfristigen Erfolg der Unternehmen.

Wir danken allen Beteiligten, die an dieser Studie mitgewirkt haben, für ihre wertvollen Beiträge. Es ist unser Ziel, einen Beitrag zur Stärkung der Cybersicherheit im Mittelstand zu leisten und Unternehmen dabei zu unterstützen, den digitalen Wandel sicher zu gestalten und im internationalen Wettbewerb weiterhin zu bestehen.

Wir wünschen eine anregende und interessante Lektüre.

Damian Izdebski
CEO und Gründer von techbold

Univ.-Prof. Dr. Reinhard Prügl
Studienautor und Inhaber des Lehrstuhls für Innovation,
Technologie und Entrepreneurship an der Zeppelin Universität

Reinhard Prügl
What`s Next Institute

Univ.-Prof. Dr. Reinhard Prügl ist österreichischer Wirtschaftswissenschaftler, akademischer Leiter des Friedrichshafener Instituts für Familienunternehmen (FIF) und Inhaber des Lehrstuhls für Innovation, Technologie und Entrepreneurship an der Zeppelin Universität in Friedrichshafen am Bodensee. Er ist außerdem mehrfacher Unternehmer mit Beteiligungen an Gründungen zwischen 2018 und 2020. Für seine Lehrtätigkeit wurde Prügl bereits mehrfach mit dem „Best Teaching Award“ der Zeppelin Universität ausgezeichnet.

Damian Izdebski
techbold CEO & Gründer

Damian Izdebski ist Gründer und CEO der techbold Gruppe. Damian verantwortet vor allem die Bereiche Strategie, Sales, Investor Relations und M&A. techbold ist spezialisiert auf hochsichere IT-Infrastrukturen für den Mittelstand und ist ein kompetenter Partner für alle Unternehmen, die sowohl IT-Lösungen als auch alle IT-Dienstleistungen und -services aus einer Hand beziehen möchten. Das über 150-köpfige techbold Team mit Standorten in Wien, Oberösterreich und im Burgenland verantwortet die IT-Sicherheit von über 800 Unternehmen in 10 europäischen Ländern.

ÜBERBLICK GESAMTGESELLSCHAFTLICHE EBENE

WAS WIR WISSEN: GESAMTGESELLSCHAFTLICHE EBENE

- Cyberangriffe werden von Wirtschaft und Politik – national wie international – gleichermaßen als ernstzunehmende Bedrohung angesehen, die weiterreichende Folgen sowohl für den/die einzelne Bürger:in, das einzelne Unternehmen aber auch die Gesellschaft an sich haben kann.
- Die Angreifer:innen verfolgen ganz unterschiedliche Ziele: von der Lösegelderpressung über den Diebstahl von Wissen oder der Schädigung eines Konkurrenten bis zu geopolitisch motivierten Zielen.
- Cyber Crime im engeren und weiteren Sinn nimmt in Österreich ebenfalls stark zu.

Quelle: Ergebnisse aus der Literaturrecherche

GLOBAL RISKS RANKED BY SEVERITY OVER THE SHORT AND LONG TERM

Der jährlich erscheinende Global Risk Report des **World Economic Forum** (WEF) zählt **Cyber Crime und Cyber Insecurity** sowohl für die nächsten zwei als auch für den nächsten zehn Jahre zu den **TOP 10 globalen Risiken.**

- Technological
- Societal
- Geopoitical
- Environmental
- Economic

	2 years	10 years
01	Cost-of-living crisis	Failure to mitigate climate change
02	Natural disasters and extreme weather events	Failure of climate-change adaptation
03	Geoeconomic confrontation	Natural disasters and extreme weather events
04	Failure to mitigate climate change	Biodiversity loss and ecosystem collapse
05	Erosion of social cohesion and societal polarization	Large-scale involuntary migration
06	Large-scale environmental damage incidents	Natural resource crises
07	Failure of climate change adaptation	Erosion of social cohesion and societal polarization
08	Widespread cybercrime and cyber insecurity	**08** Widespread cybercrime and cyber insecurity
09	Natural resource crises	Geoeconomic confrontation
10	Large-scale involuntary migration	Large-scale environmental damage incidents

Quelle: World Economic Forum (2022): Global Risk Report 2023

GLOBAL RISKS LANDSCAPE: AN INTER-CONNECTIONS MAP

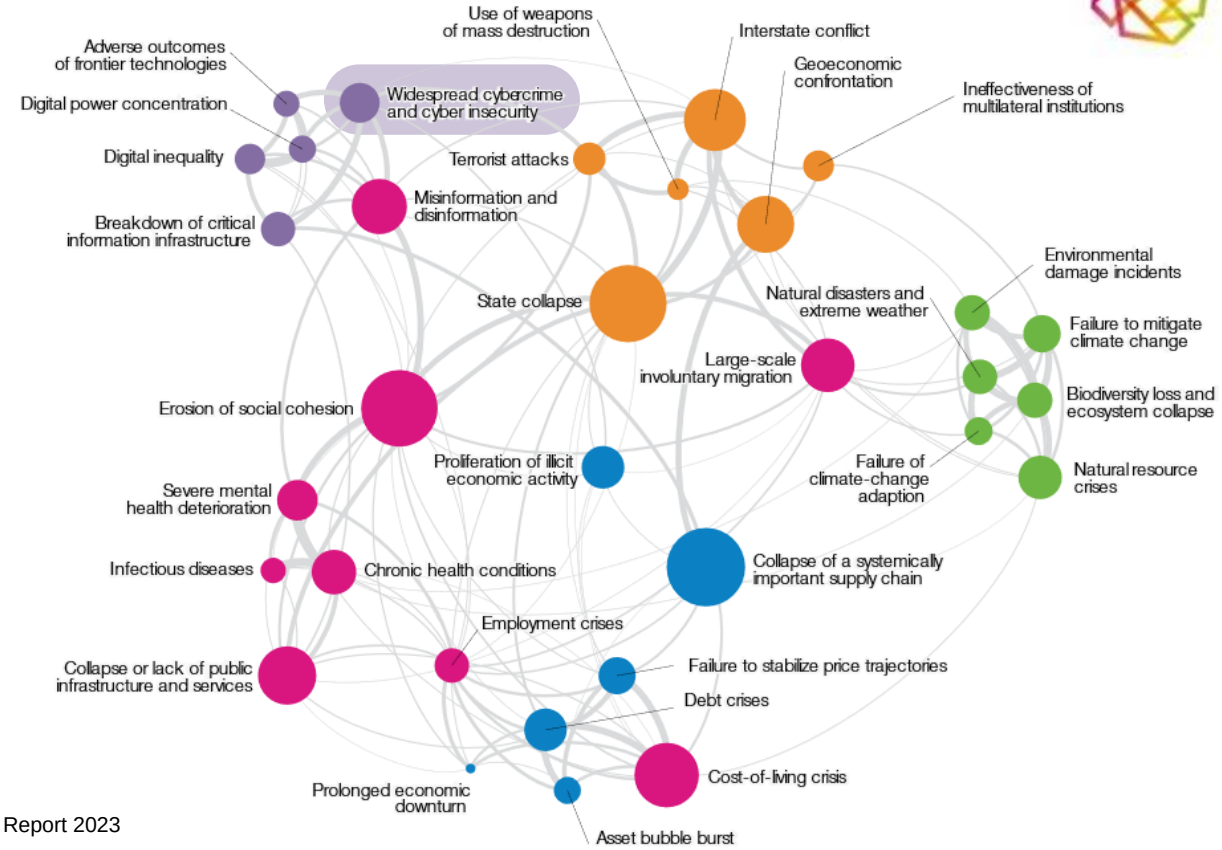
Nodes
Risk Influence

High
Medium
Low

Edges
Relative influence

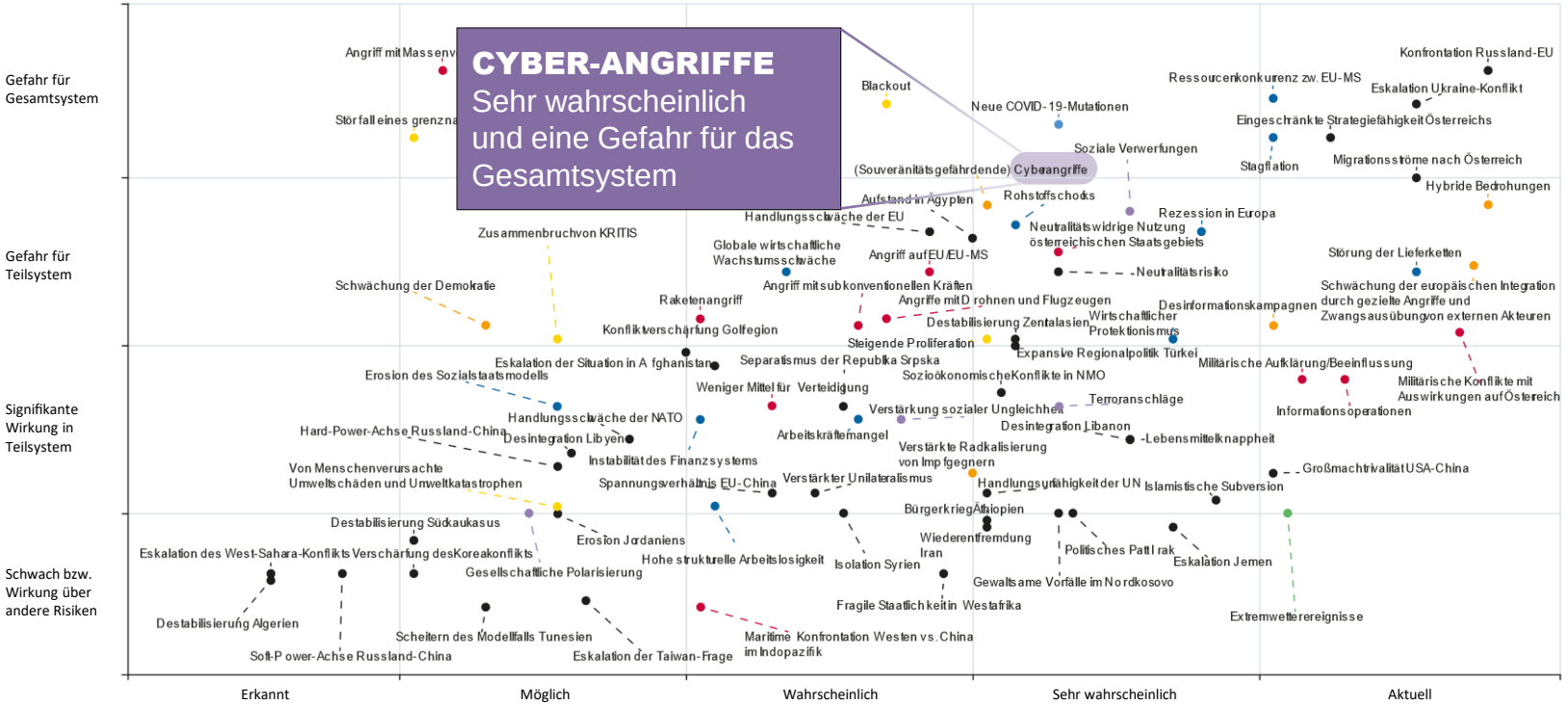
High
Medium
Low

- Technological
- Societal
- Geopoitical
- Environmental
- Economic



Quelle: World Economic Forum (2022): Global Risk Report 2023

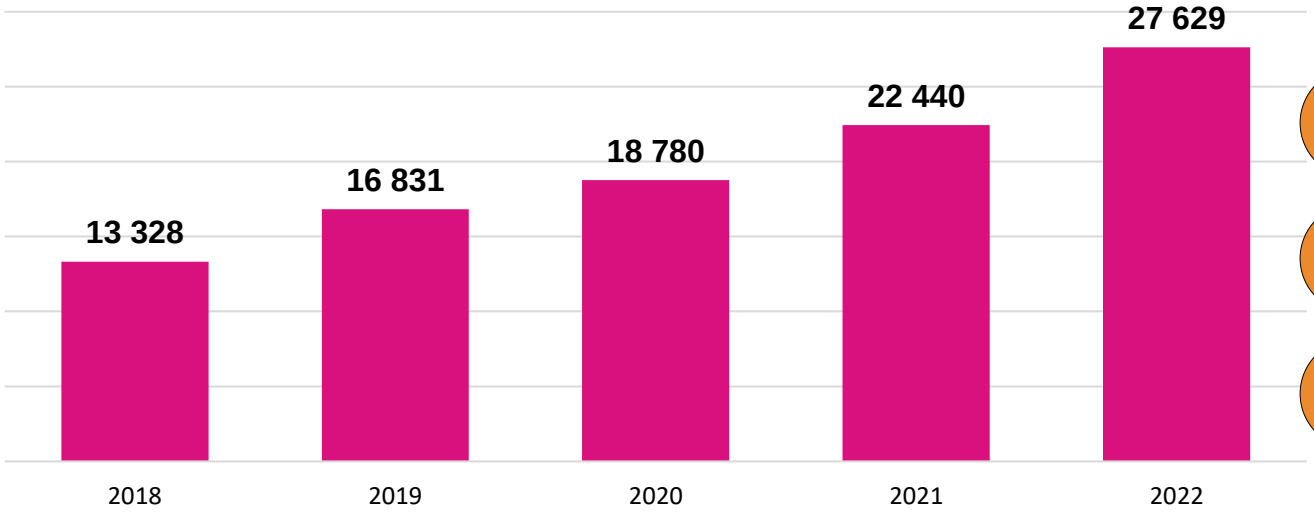
AUSZUG AUS DEM RISIKOBILD 2023



Quelle: Bundesministerium für Landesverteidigung (2022): Risikobild 2023

ENTWICKLUNG CYBERKRIMINALITÄT GESAMT

Anzeigen Cyberkriminalität im weiteren Sinne im Zeitraum 2018 – 2022
(Mehr als verdoppelt | Faktor 2,1)



§ 146 StGB
Betrug

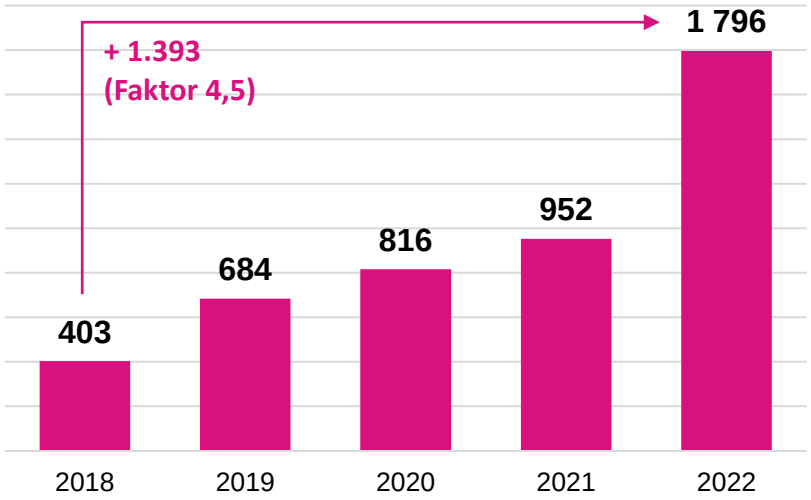
§ 147 StGB
Schwerer Betrug

§ 148 StGB
Gewerbsmäßiger Betrug

Quelle: Cybercrime Reports des Bundeskriminalamts 2018 - 2022

ENTWICKLUNG CYBERKRIMINALITÄT
WIDERRECHTLICHER ZUGRIFF AUF COMPUTERSYSTEME

Anzeigen nach § 118a im Zeitraum 2018 – 2022 (Mehr als vervierfacht)



Quelle: Cybercrime Reports des Bundeskriminalamts 2018 - 2022

§ 118a
Widerrechtlicher Zugriff auf ein Computersystem

Problem Dunkelziffer

„Die Dunkelziffer im Bereich der Internet-kriminalität ist unter Berücksichtigung internationaler Studien besonders hoch. Viele Betroffene scheuen die Anzeige bei der nächsten Polizeidienststelle, teils aus Scham, Angst vor Reputationsverlust oder weil angenommen wird, dass der Fall ohnehin nicht verfolgt werden könne."

Quelle: Cybercrime Report 2021 des Bundeskriminalamts, S. 31

ÜBERBLICK UNTERNEHMERISCHE EBENE

Key Findings Literatur-Recherche

Unternehmen jeder Größe sind betroffen

Viele Studien zeigen weiters, dass Unternehmen aller Größen Opfer von Cyber Crime werden können. Gerade kleine und mittlere Unternehmen - unabhängig davon ob sie Familienunternehmen sind oder nicht – sind schlechter auf Cyber-Attacken vorbereitet als größere Unternehmen.

Der Stellenwert von Digitalisierung ist zentral

Einige Studien weisen darauf hin, dass der Stellenwert von Digitalisierung im Unternehmen Auswirkungen auf die Bedeutung von Cyber Security hat. Dabei gilt die Faustregel: je zentraler die Rolle von Digitalisierung im Geschäftsmodell, desto eher gibt es Sensibilisierung für Cyber Security und die Bereitschaft entsprechende Maßnahmen zu setzen.

Cyber Security wird zur gesellschaftlichen Aufgabe

Der World Risk Report des World Economic Forum oder das Risikobild des Bundesheers nennen Cyber Crime als eine zentrale Bedrohung für Wirtschaft und Gesellschaft. Damit kommt Cyber Security in Unternehmen auch große gesellschaftspolitische Bedeutung zu, da etwa über Schulungsmaßnahmen und Bewusstseinsbildung in Unternehmen das Bewusstsein in der Bevölkerung insgesamt steigen kann.

AI wird zum zweiseitigen Turbo

Künstliche Intelligenz wird zum doppelten Turbo: KI ermöglicht neue Methoden für Cyber Crime genauso wie neue Optionen für Cyber Security.

Zu wenig Austausch und regelmäßige Überprüfung

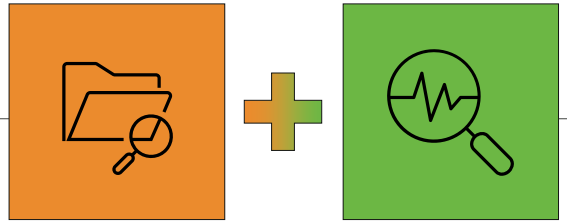
Es fehlt an strukturiertem Austausch zwischen Unternehmen und auch mit staatlichen Akteur:innen, um sich über Bedrohungslagen, mögliche Antworten etc. austauschen zu können und voneinander lernen zu können. Darüber hinaus fehlt eine regelmäßige kritische und externe Überprüfung der IT-Sicherheits-Strukturen.

12

BISHERIGE STUDIEN & VERWENDETE METHODEN

Studie	Methode
Deloite Private (2020): Cyber Security im Mittelstand	Online Fragebogen bei deutschen, mittelständischen Unternehmen (gem. EU-Definition) + 6 Expert:innen Interviews.
Berg, Archim (2022): Wirtschaftsschutz 2022, bitcom	Computergestützte telefonische Befragung/Computer Assisted Telephone Interview (CATI).
KPMG (2022): Cyber Security in Österreich	Online Fragebogen bei österreichischen Unternehmen aller Branchen und Größen + qualitative Interviews.
ESET (2022): Cybersicherheits-Umfrage: Die Stimmungslage bei KMUs. Wo der Schuh drückt. Warum EDR* eine Lösung darstellt. * Endpoint Detection Response	Keine konkreten Angaben zum Befragungsmodus, außer: Es wurden 1.212 IT-Sicherheits-Entscheider aus England, den USA, Kanada, Frankreich, Spanien, Italien, Polen, Schweden, Tschechien, den Niederlanden, Dänemark, Norwegen und Finnland interviewt. Die Befragten repräsentieren Unternehmen mit einer Größe von 25 bis 500 Mitarbeiter:innen sowie in puncto IT-Sicherheitsprozesse mit unterschiedlichen Reifegraden und Budgets.
KPMG (2022): Lünendonk® Studie: Von Cyber Security zu Cyber Resilienece – mehr Digitalisierung, mehr Cyber Bedrohung?	Telefoninterviews mit CIOs, CTOs, CISOs aus Unternehmen unterschiedlicher Branchen.
Bundesamt für Sicherheit in der Informationstechnik (2022): Die Lage der IT-Sicherheit in Deutschland 2022	Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet als nationale Cyber-Sicherheitsbehörde kontinuierlich die Gefährdungslage der IT-Sicherheit in Deutschland. Im Fokus des BSI stehen Cyber-Angriffe auf Unternehmen, staatliche sowie öffentliche Institutionen und Privatpersonen, aber auch Maßnahmen zur Prävention und Bekämpfung dieser Lagen. Der vorliegende Bericht zieht eine Bilanz für die Zeit vom 1. Juni 2021 bis zum 31. Mai 2022 (Berichtszeitraum). Damit greift der Bericht aktuelle und unter Umständen anhaltende Cyber-Bedrohungen auf.
Bundeskanzleramt (2022): Bericht Cybersicherheit für das Jahr 2021	Auswertung diverser Daten etwa aus der Kriminalstatistik, Experteninputs, Integration der KPMG-Studie „Cyber Security in Österreich“.

Studie	Methode
Bundesministerium für Inneres (2022): Cybercrime Report 2022. Lagebericht über die Entwicklung von Cybercrime	Auswertung diverser Kriminalitätsstatistiken, keine weiteren Angaben zur sonstigen Methodik.
Bundesministerium für Landesverteidigung (2022): Risikobild 2023	Keine Angabe zur Methodik.
World Economic Forum (2022): Global Risk Report 2023	Grundlage für diesen Report ist der Global Risks Perception Survey. Keine genauen Angaben zur Durchführung. Vermutlich Online-Umfage sowie Expert:inneninterviews.
European Union Agency for Cybersecurity (ENISA) (2022): ENISA Threat Landscape 2022	Auswertung von Sekundärdaten, qualitative Interviews.



NEUES STUDIENDESIGN: EINZIGARTIGE KOMBINATION VON ZWEI DATENBASEN (MIXED METHODS)

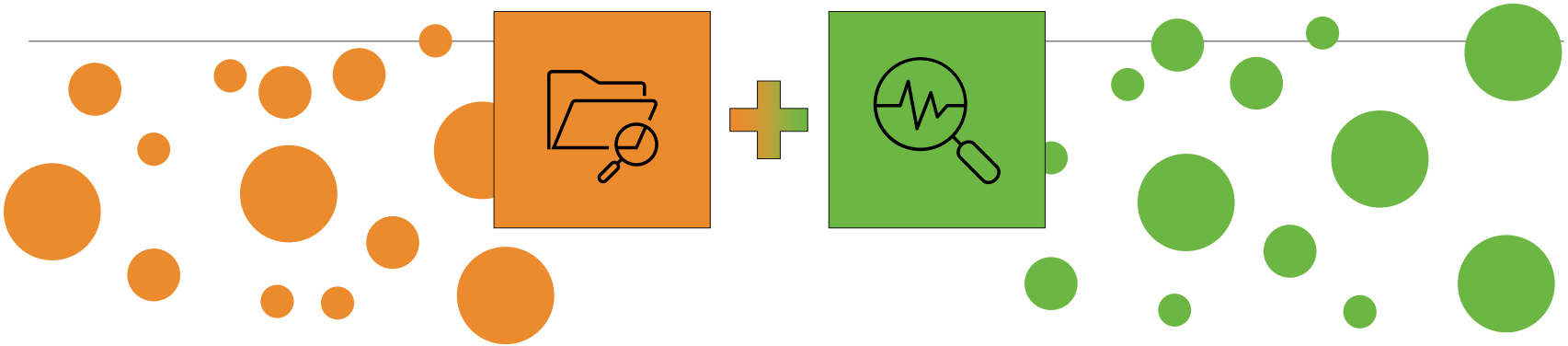
STUDIENDESIGN: EINZIGARTIGE KOMBINATION VON ZWEI DATENBASEN (MIXED METHODS)

Das sagt der Mittelstand

Auswertung von CATI-Daten aus dem Jahr 2023 von über 200 Geschäftsführer:innen die in mittelständischen Unternehmen in Österreich Verantwortung tragen; davon mehr als die Hälfte in mittelständischen Familienunternehmen.

Das macht der Mittelstand

Auswertung von Daten aus rund 180 IT-Audits aus den Jahren 2019 – 2023. Das techbold IT-Audit untersucht relevante Indikatoren in Bezug auf die IT-Sicherheit von Unternehmen. Unternehmens- und Personendaten über Matching mit COMPASS Datenbank.



DETAILS ZUR CATI BEFRAGUNG

Das sagt der Mittelstand

Auswertung von CATI-Daten aus dem Jahr 2023 von über 200 Geschäftsführer:innen die in mittelständischen Unternehmen in Österreich Verantwortung tragen; davon mehr als die Hälfte in mittelständischen Familienunternehmen.

Das macht der Mittelstand

Auswertung von Daten aus den Jahren 2019 – 2023. Das techbold-Audit untersucht relevante Indikatoren in Bezug auf die IT-Sicherheit von Unternehmen. Unternehmens- und Personendaten über Matching mit COMPASS Datenbank.

METHODISCHE VORGEHENSWEISE

Befragung von Geschäftsführung

Wie schätzt sich der österreichische Mittelstand in Bezug auf IT-Sicherheit ein und was sind die Pläne für die Zukunft?

Forschungsprojekt

Empirische Untersuchung der Einstellungen, Erfahrungen und unternehmerischen Pläne mittelständischer Unternehmen in Österreich in Bezug auf Themen der IT-Sicherheit im Rahmen eines langfristig angelegten Forschungsprojekts

Datenerhebung (Sommer 2023)

- Standardisierter Fragebogen, Telefoninterviews (CATI)

Zielgruppe und Stichprobe

- Zielgruppe: Mitglieder der Geschäfts-führung, die im österreichischen Mittelstand Verantwortung als Geschäftsführer und/oder Gesellschafter tragen (mit besonderer Berücksichtigung von Familienunternehmen)
- Umfangreiche Stichprobe mit 202 Befragten (n=202)

Sommer 2023

ZUSAMMENSETZUNG DER STICHPROBE CATI-BEFRAGUNG

Demografische Daten der Befragten

- **Geschlecht**
  k.A.
- **Alter**
  k.A.
- **Verweildauer im Unternehmen**
  Ø 21 Jahre
- **Rolle im Unternehmen**
  100% in der Geschäftsführung tätig

Eckdaten zu den Unternehmen

- **Mitarbeiter:innen**
  75% bis zu 30 Mitarbeiter:innen,
  17% bis zu 100 Mitarbeiter:innen,
  8% bis zu 350 Mitarbeiter:innen
- **Hauptsitz des Unternehmens**
  62% Ländlicher Raum/Kleinstadt (bis 100.000), 38% Großstadt (mehr als 100.000)
- **Unternehmenstyp**
  59% Familienunternehmen*,
  41% Nicht-Familienunternehmen

*Von einem Familienunternehmen spricht man, wenn (1) sich die Mehrheit der Entscheidungsrechte im Besitz der natürlichen Person(en), die das Unternehmen gegründet hat/haben, der natürlichen Person(en), die das Gesellschaftskapital des Unternehmens erworben hat/haben oder im Besitz ihrer Ehepartner, Eltern, ihres Kindes oder der direkten Erben ihres Kindes befindet, und (2) die Mehrheit der Entscheidungsrechte direkt oder indirekt besteht, und/oder (3) mindestens ein Vertreter der Familie oder der Angehörigen offiziell an der Leitung bzw. Kontrolle des Unternehmens beteiligt ist.

DETAILS ZU IT-AUDITS

Das sagt der Mittelstand

Auswertung von CATI-Daten aus dem Jahr 2023 von über 200 Geschäftsführer:innen die in mittelständischen Unternehmen in Österreich Verantwortung tragen; davon mehr als die Hälfte in mittelständischen Familienunternehmen.

Das macht der Mittelstand

Auswertung von Daten aus den Jahren 2019 – 2023. Das techbold-Audit untersucht relevante Indikatoren in Bezug auf die IT-Sicherheit von Unternehmen. Unternehmens- und Personendaten über Matching mit COMPASS Datenbank.

AUSWERTUNG DER TECHBOLD IT-SICHERHEITS-AUDITS IM ZEITRAUM 2019 – SOMMER 2023

IT-Sicherheits-Audits

Wie entwickelt sich der österreichische Mittelstand in Bezug auf IT-Sicherheit in den letzten Jahren (seit 2019)?

Forschungsprojekt

Empirische Untersuchung von IT-Sicherheits-Audits in mittelständischen Unternehmen in Österreich in Bezug im Rahmen eines langfristig angelegten Forschungsprojekts

Datenbasis (2019 – Sommer 2023)

- Standardisierte Analyse, umfassendes IT-Sicherheits-Audit **PLUS** unternehmens- und personenbezogene Daten aus COMPASS Datenbank (Matching)

Zielgruppe und Stichprobe

- Zielgruppe: Österreichischer Mittelstand (mit besonderer Berücksichtigung von Familienunternehmen)
- Umfangreiche Stichprobe mit 179 umfassenden IT-Sicherheits-Audits (n=179) in den letzten 5 Jahren (2019 bis Sommer 2023)

Zeitraum 2019 | Sommer 2023

ZUSAMMENSETZUNG DER STICHPROBE IT-AUDITS (MATCHING COMPASS-DATEN)

Demografische Daten der Personen

- **Geschlecht**
  85% männlich,
  15% weiblich
- **Alter**
  Ø 52 Jahre
- **Verweildauer im Unternehmen**
  Ø 18 Jahre
- **Rolle im Unternehmen**
  100% in der Geschäftsführung und/oder als Eigentümer tätig

Eckdaten zu den Unternehmen

- **Mitarbeiter:innen**
  73% bis zu 30 Mitarbeiter:innen,
  21% bis zu 100 Mitarbeiter:innen,
  6% bis zu 350 Mitarbeiter:innen
- **Hauptsitz des Unternehmens**
  67% Ländlicher Raum/Kleinstadt (bis 100.000), 33% Großstadt (mehr als 100.000)
- **Unternehmenstyp**
  74% Familienunternehmen*,
  26% Nicht-Familienunternehmen

*Von einem Familienunternehmen spricht man, wenn (1) sich die Mehrheit der Entscheidungsrechte im Besitz der natürlichen Person(en), die das Unternehmen gegründet hat/haben, der natürlichen Person(en), die das Gesellschaftskapital des Unternehmens erworben hat/haben oder im Besitz ihrer Ehepartner, Eltern, ihres Kindes oder der direkten Erben ihres Kindes befindet, und (2) die Mehrheit der Entscheidungsrechte direkt oder indirekt besteht, und/oder (3) mindestens ein Vertreter der Familie oder der Angehörigen offiziell an der Leitung bzw. Kontrolle des Unternehmens beteiligt ist.

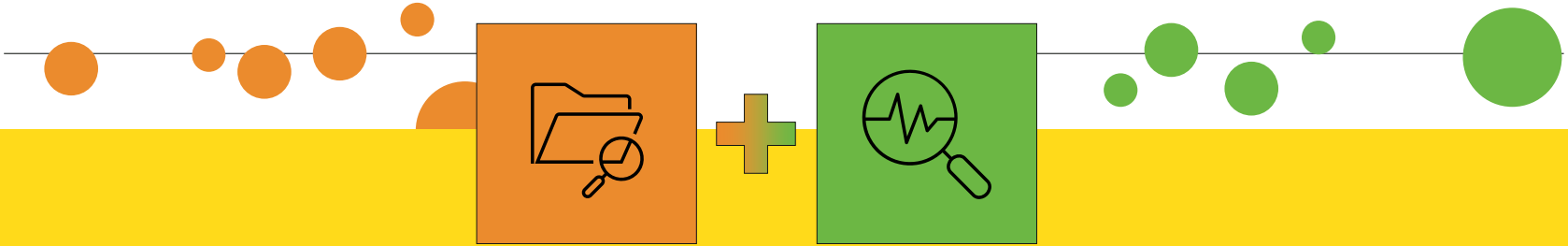
STUDIENDESIGN: EINZIGARTIGE KOMBINATION VON ZWEI DATENBASEN (MIXED METHODS)

Das sagt der Mittelstand

Auswertung von CATI-Daten aus dem Jahr 2023 von über 200 Geschäftsführer:innen die in mittelständischen Unternehmen in Österreich Verantwortung tragen; davon mehr als die Hälfte in mittelständischen Familienunternehmen.

Das macht der Mittelstand

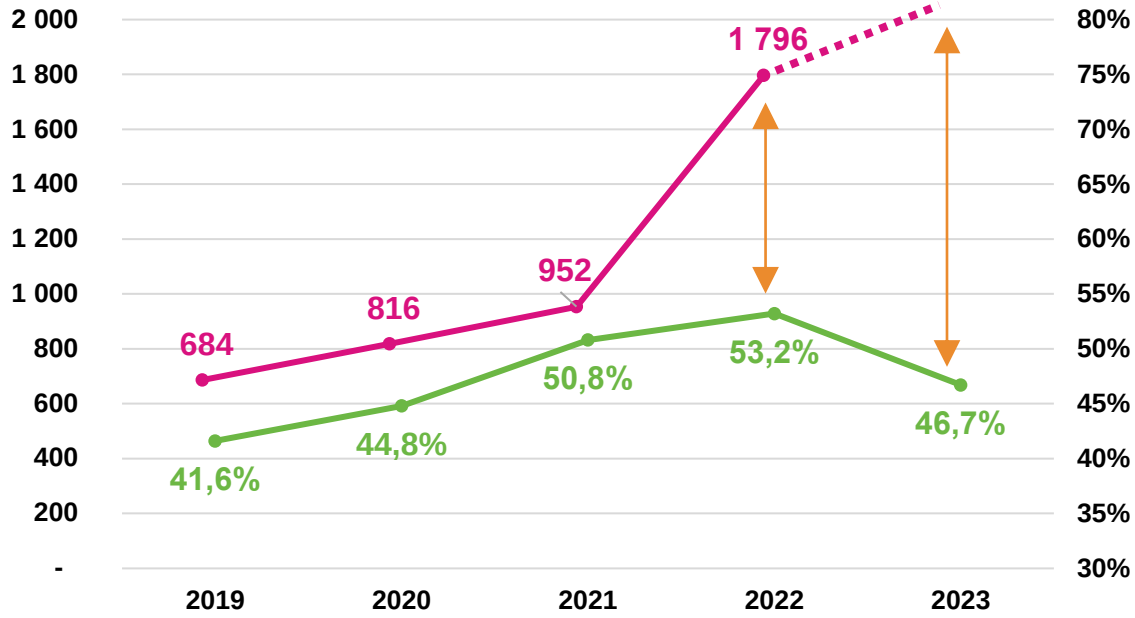
Auswertung von Daten aus rund 180 IT-Audits aus den Jahren 2019 – 2023. Das techbold-Audit untersucht relevante Indikatoren in Bezug auf die IT-Sicherheit von Unternehmen. Unternehmens- und Personendaten über Matching mit COMPASS Datenbank.



BIG PICTURE ERGEBNISSE: FAMILIENUNTERNEHMEN STECHEN BEI BEIDEN DATENQUELLEN HERVOR.

ÜBERBLICK ZENTRALE ERGEBNISSE

ENTWICKLUNG CYBERKRIMINALITÄT IM VERGLEICH ERGEBNISWERTE IT-AUDIT

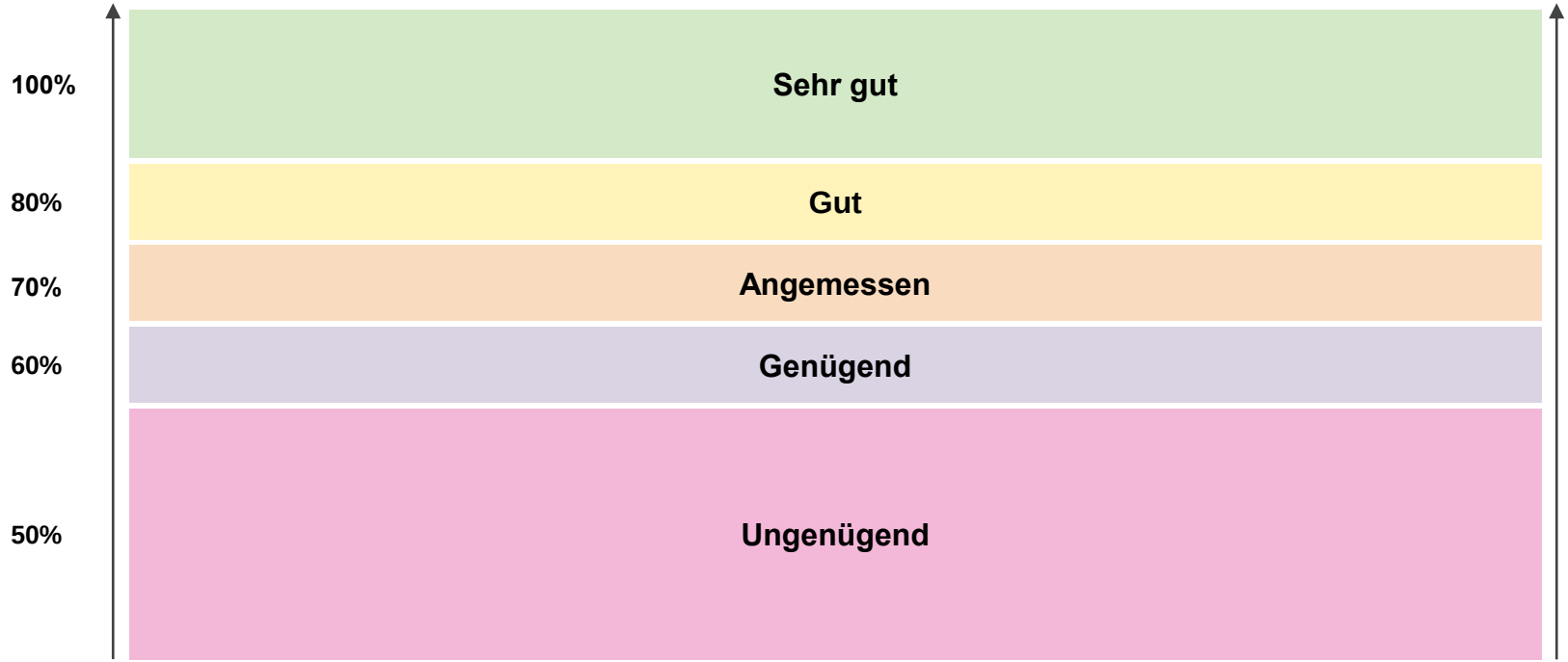


Während die Anzeigen im Cybercrime–Bereich deutlich steigen, sinken die Ergebniswerte der mittelständischen Unternehmen im Rahmen der techbold IT-Audits.

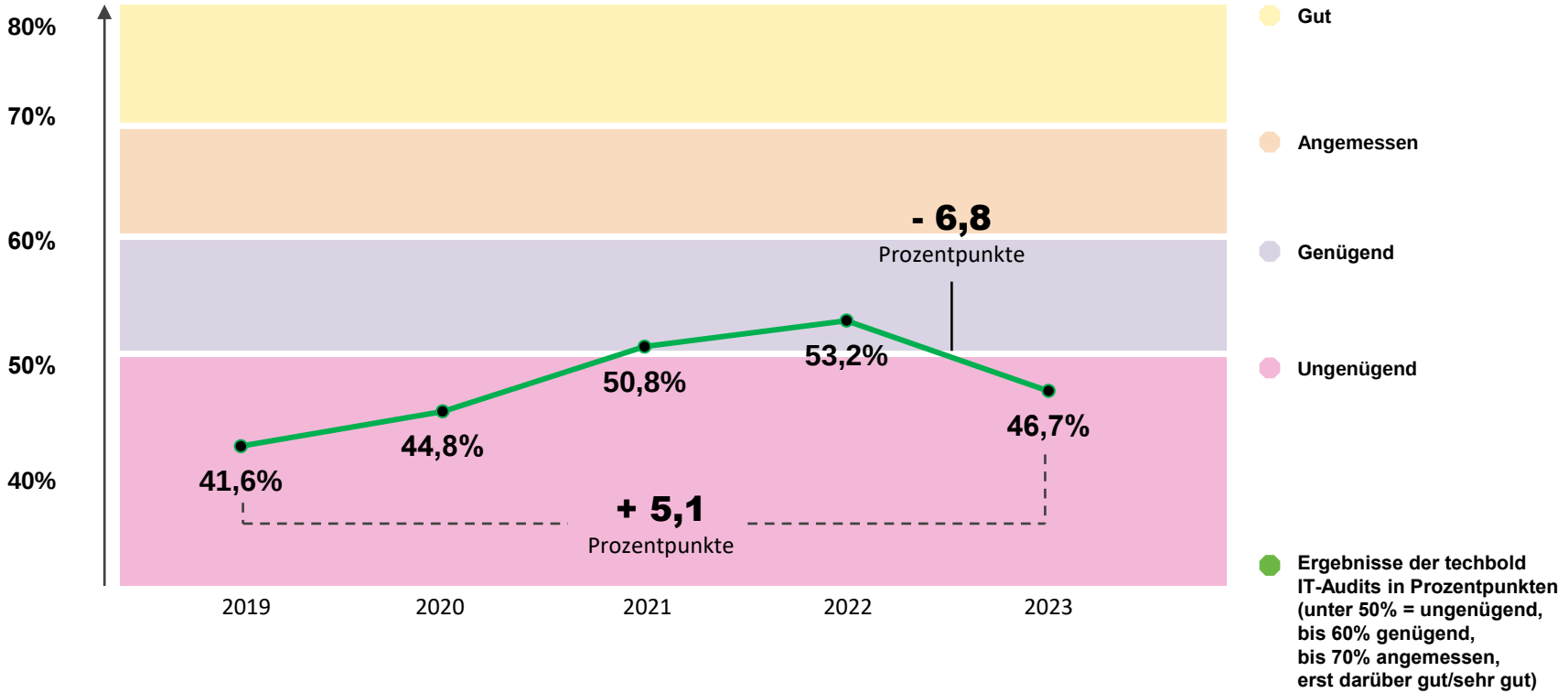
Anzahl der Cybercrime-Anzeigen

Ergebnisse der techbold IT-Audits in Prozentpunkten (unter 50% = unzureichend, bis 60% genügend, bis 70% angemessen, erst darüber gut/sehr gut)

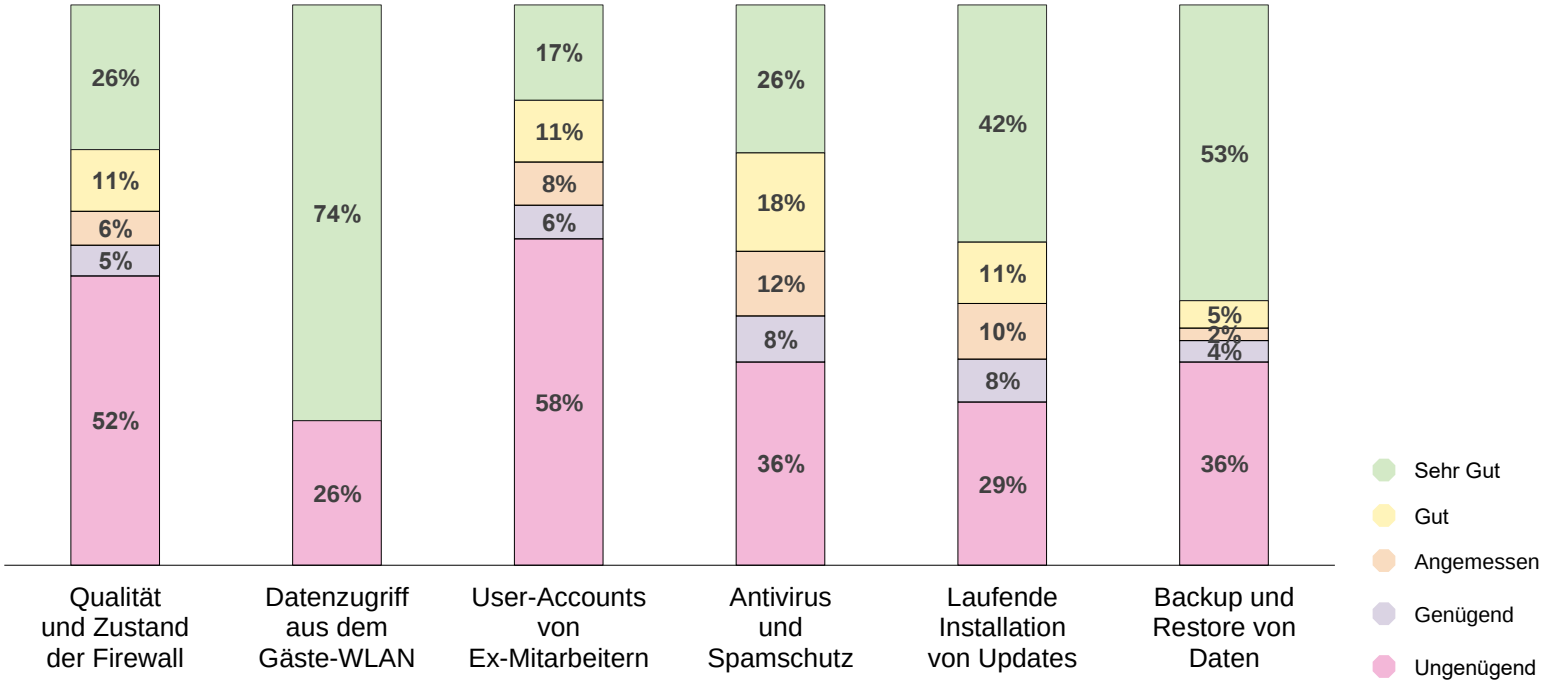
AUSWERTUNG DER IT-AUDITS – ERGEBNISSE IN PROZENT



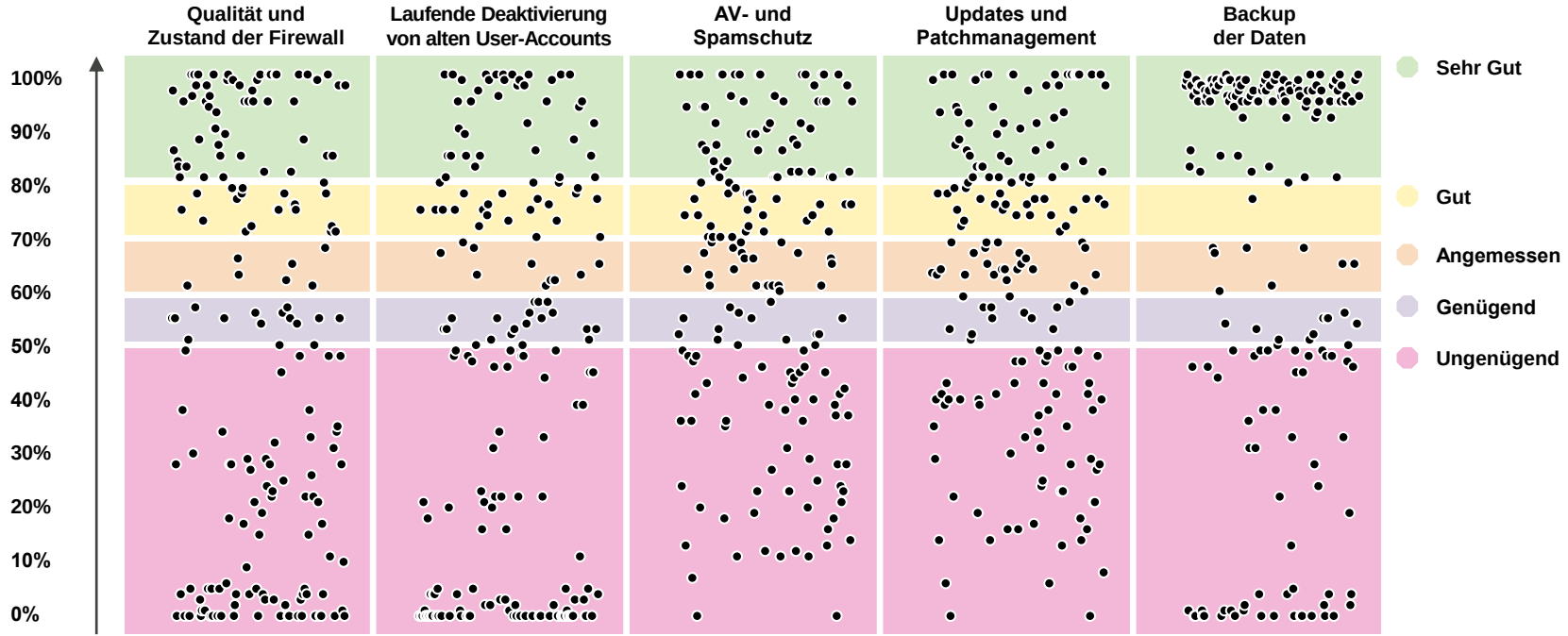
DETAILERGEBNISSE IT-AUDIT/FOKUSBEREICHE



DETAILERGEBNISSE
IT-AUDIT/FOKUSBEREICHE



DETAILERGEBNISSE
IT-AUDIT/FOKUSBEREICHE



DETAILERGEBNISSE IT-AUDIT (FOKUSBEREICHE)

Firewall
52 % der Unternehmen haben entweder gar keine Firewall oder eine Firewall, die überaltet oder falsch konfiguriert ist, so dass sie keinen Schutz bietet.

WLAN
Bei rund einem Viertel der Unternehmen (26 %) kann man relativ leicht aus dem öffentlichen Gäste-WLAN auf die Unternehmensdaten zugreifen.

Alte Accounts
Bei 58 % der Firmen bleiben User-Accounts aktiv, obwohl der/die Mitarbeiter:in das Unternehmen verlassen hat. In vielen Fällen verbinden sich ex-Mitarbeiter:innen noch Monate lang nach dem Ausscheiden aus dem Unternehmen mit dem Server ihres alten Arbeitgebers.

Antivirus und Anti Spam
36 % haben einen unzureichenden Schutz gegen Viren, Spam und Trojaner.

Updates
Bei 29 % der Firmen werden die Systeme nicht laufend mit Updates und Patches versorgt.

Backup
36 % der Unternehmen haben gar kein funktionierendes Backup oder eine Rücksicherung der Daten wäre in angemessener Zeit nicht möglich. Im Falle einer Datenverschlüsselung müssten diese Firmen ein Lösegeld bezahlen, um den Betrieb wiederherstellen zu können.

GRUNDSÄTZLICHE BEOBACHTUNGEN ANALYSE IT-AUDITS

Generell im Durschnitt recht niedriges Niveau sowohl beim Gesamtergebnis der IT-Audits (nie über 60 Prozent) als auch in Teilbereichen

- In Summe also viel Luft nach oben im österreichischen Mittelstand in Bezug auf das Thema IT-Sicherheit
- Manche Unternehmen schneiden sehr gut, viele andere sehr schlecht ab
- Hohe Varianz (SD: rund +/- 20%, Extremwerte von rund 5% bis 95%)

Trendanalyse in Bezug auf die letzten 5 Jahre: durchgängig ansteigende Werte sowohl beim Gesamtergebnis der IT-Audits als auch in Teilbereichen zwischen 2019 und 2022

- **Aber: ausgeprägter Rückgang der Ergebnisse der IT-Audits in 2023 (bis zu 9 Prozentpunkte im Vergleich zu 2022)**
- In manchen Bereichen nahezu Rückgang auf das Niveau von 2019 (insbesondere im Bereich regelmäßige Bewertung & Überprüfung)
- **ACHTUNG: Trendumkehr in Zeiten zunehmender Bedrohungen**

GEGENÜBERSTELLUNG ERGEBNISSE CATI & AUDIT NACH EINFLUSSFAKTOREN

SPEZIFIKA VON FAMILIENUNTERNEHMEN & IT SECURITY

Erkenntnisse aus der Online-Umfrage

Im Bereich IT-Security sind Familienunternehmen keine Vorreiter. Sie schätzen IT-Security Themen als weniger bedrohlich und wichtig ein

Je näher der Generationenwechsel im Familienunternehmen rückt, desto präsenter werden IT-Security Themen

Je älter das Familienunternehmen, desto bewusster sind Unternehmen sich der IT-Security-Risiken

Stadtluft macht Familienunternehmen IT-Security-bewusster

Eine lange Verweildauer der Geschäftsführung wirkt sich positiv auf die Wahrnehmung von IT-Security Risiken sowie auf Prozesse und Investitionen in die Prävention aus

Erkenntnisse aus dem techbold Reality-Check

Je operativer die Eigentümer:innen, desto schlechter schneiden Familienunternehmen bei den techbold IT-Audits ab

Je älter das Familienunternehmen, desto besser sind die Ergebnisse der techbold IT-Audits

Mehrere Personen in der Geschäftsführung hängen mit besseren Werten beim techbold IT-Audit zusammen

FAMILIENUNTERNEHMEN: NACHHOLBEDARF IM BEREICH IT-SECURITY

Erkenntnisse aus der Online-Umfrage

Einschätzung Bedrohungslage

Familienunternehmen nehmen seltener Angriffe wahr

Stellenwert / Wichtigkeit von IT-Security

Familienunternehmen nehmen das Thema IT Security als weniger wichtig wahr

Hemmnisse bei der Verbesserung der IT-Security

Familienunternehmen sehen seltener als Nicht-Familien-unternehmen Hemmnisse bei der Verbesserung der IT-Security

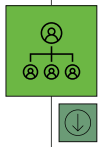
Qualität der definierten Prozesse

Familienunternehmen verfügen über kaum definierte oder gar keine Prozesse, wie im Fall eines IT-Sicherheitsvorfalls vorzugehen ist

Einschätzung des bestehenden Schutzes

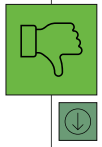
Familienunternehmen fühlen sich weniger gut vor internen/externen Angriffen und Datenverlust geschützt

Erkenntnisse aus dem techbold Reality-Check



Eigentümer:innen in der Ziehung

Eigentümergeführte Familienunternehmen weisen schlechtere Werte beim techbold IT-Audit auf



Je mehr Eigentümer:innen, desto schlechter

Mehrere Eigentümer:innen hängen mit schlechteren Werten beim Audit zusammen

DER UNTERNEHMENSSITZ: STADTLUFT MACHT IT-SECURITY-BEWUSSTER

Erkenntnisse aus der Online-Umfrage

Einschätzung Bedrohungslage

Je urbaner der Unternehmenssitz, desto häufiger werden Angriffe wahrgenommen

Stellenwert / Wichtigkeit von IT Security

Je urbaner der Unternehmenssitz, desto wichtiger wird das Thema IT Security wahrgenommen

Veränderung Sicherheitsrisiken in den nächsten 2 Jahren

Unternehmen mit einem Sitz im ländlichen Raum sehen eine stärkere Zunahme der Risiken im Bereich der IT-Security in den nächsten zwei Jahren

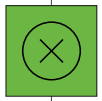
Kompetenz und Know-how rund um IT-Sicherheit

Unternehmen mit einem Sitz im ländlichen Raum schätzen sich als weniger kompetent im Bereich der IT-Security ein

Qualität der definierten Prozesse

Unternehmen mit einem Sitz in einer Großstadt verfügen über gut definierte Prozesse, wie im Fall eines IT-Sicherheitsvorfalls vorzugehen ist

Erkenntnisse aus dem techbold Reality-Check



Der Unternehmenssitz hat keinen signifikanten Einfluss auf die Ergebnisse der IT-Audits von techbold

IT-SECURITY: EINE FRAGE DER ERFAHRUNG IN FAMILIENUNTERNEHMEN

Erkenntnisse aus der Online-Umfrage

Einschätzung Bedrohungslage

Je älter des Familienunternehmen, desto häufiger werden Angriffe wahrgenommen

Stellenwert / Wichtigkeit von IT-Security

Je älter des Familienunternehmen, desto wichtiger wird das Thema IT-Security wahrgenommen

Einschätzung des bestehenden Schutzes

Ältere Familienunternehmen fühlen sich weit besser vor internen/ externen Angriffen und Datenverlust geschützt

Hemmnisse bei der Verbesserung der IT-Security

Ältere Familienunternehmen sehen öfter Hemmnisse bei der Verbesserung der IT-Security

Qualität der definierten Prozesse

Ältere Familienunternehmen verfügen über gut definierte Prozesse, wie im Fall eines IT-Sicherheitsvorfalls vor-zugehen ist

Ordnungsgemäße Datensicherung im Unternehmen

Ältere Familienunternehmen sind sich weniger sicher, dass alle wichtigen Daten im Unternehmen gesichert und wiederhergestellt werden können

Erkenntnisse aus dem techbold Reality-Check

Je älter das Familienunternehmen, desto besser sind die Ergebnisse der techbold IT-Audits.

IT-SECURITY: EINE FRAGE DER ERFAHRUNG IN FAMILIENUNTERNEHMEN AUCH AUF GESCHÄFTSFÜHRUNGSEBENE

Erkenntnisse aus der Online-Umfrage

Einschätzung Bedrohungslage

Je länger die GF bereits im Unternehmen ist, desto häufiger werden Angriffe wahrgenommen

Ordnungsgemäße Datensicherung im Unternehmen

Familienunternehmen mit einer längeren Verweildauer der GF sind sich weniger sicher, dass alle Daten im Unternehmen gesichert & wiederhergestellt werden können

Veränderung Sicherheitsrisiken in den nächsten 2 Jahren

Familienunternehmen mit einer längeren Verweildauer der GF sehen eine stärkere Zunahme der Risiken im Bereich der IT-Security in den nächsten zwei Jahren

IT-Security Vorfälle in den letzten zwei Jahren

Je länger die Verweildauer der GF, desto eher gab es keinen bzw. keinen registrierten IT-Security Vorfall in den letzten beiden Jahren

Investitionen in IT-Sicherheit in den nächsten zwei Jahren

Familienunternehmen mit einer längeren Verweildauer der GF planen höhere Investitionen in die IT-Security im kommenden Jahr (2024) im Vergleich zum aktuellen Jahr (2023)

Erkenntnisse aus dem techbold Reality-Check

Die Verweildauer der Geschäftsführung im Familienunternehmen hat keinen signifikanten Einfluss auf die Ergebnisse der techbold IT-Audits. Aber: Mehrere Personen in der Geschäftsführung hängen mit besseren Werten beim Audit zusammen

IT-SECURITY: DER GENERATIONENWECHSEL BRINGT IT SECURITY AUF DEN RADAR

Erkenntnisse aus der Online-Umfrage

Investitionen in IT-Sicherheit in den nächsten zwei Jahren

Familienunternehmen, in denen Generationswechsel nahe ist, planen höhere Investitionen in die IT-Security im kommenden Jahr (2024) im Vergleich zum aktuellen Jahr (2023)

Veränderung Sicherheitsrisiken in den nächsten 2 Jahren

Familienunternehmen, bei denen der Generationswechsel ansteht, erwarten eine höhere Zunahme der Risiken im Bereich der IT-Security in den nächsten zwei Jahren

Einschätzung Bedrohungslage

Je näher der Generationswechsel ist, desto häufiger werden Angriffe wahrgenommen

Erkenntnisse aus dem techbold Reality-Check

Keine Vergleichsdaten aus den techbold IT-Audits

EINFLUSSFAKTOREN IT-AUDITS: ZUSAMMENFASSUNG WESENTLICHE EINFLÜSSE

1

Familien-unternehmen:
Eigentümergeführte Familienunternehmen weisen **schlechtere Werte** beim Audit auf

2

Unternehmens-größe:
Je größer das Unternehmen, desto **besser die Werte** beim Audit

3

Unternehmens-alter:
Je älter das Unternehmen, desto **besser die Werte** beim Audit

4

Ein:e Eigentümer:in vs mehrere Eigentümer:innen:
Mehrere Eigentümer hängen im Vergleich zu Alleineigentümern mit **schlechteren Werten** beim Audit zusammen

5

Ein GF vs mehrere GF:
Mehrere Personen in der GF hängen mit **besseren Werten** beim Audit zusammen

Starker Zusammenhang Ausgeprägter Zusammenhang Moderater Zusammenhang

DAS KANN DER MITTELSTAND JETZT TUN

IT-Security als Querschnittsmaterie denken
Nicht nur die „Expert:innen, sondern sämtliche Mitarbeiter:innen sind gefordert.

Marathon kein Sprint
IT-Security ist ein laufender Prozess, man darf sich auf den Lorbeeren nicht ausruhen.

Dialog suchen, Erfahrungen austauschen
Cybercrime betrifft alle. Damit ist Cyber Security auch eine gemeinsame Aufgabe. Austausch zwischen Unternehmen fördern.

Stets kritisch bleiben
Der Kreativität an neuen Cyber-Bedrohungen sind keine Grenze gesetzt. Regelmäßig die eigenen Annahmen und Maßnahmen kritisch hinterfragen.

DAS SOLLTE DIE POLITIK JETZT TUN

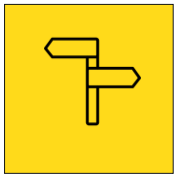
Stellenwert der IT grundlegend ändern
IT-Infrastruktur in der Jahresbilanz auf den Prüfstand stellen. Ähnlich wie Eigenkapitalquote oder Bonität.

Generationenwechsel nutzen
NextGen in Familienunternehmen als Gelegenheit zur Verbesserung der IT-Sicherheitskompetenzen.

Ländliche Unternehmen stärken
Einrichtung von IT-Security-Mentoring-Programmen, um Erfahrungen zwischen Unternehmen auszutauschen.

Bewusstsein schaffen
Förderung der Aufklärung über Cyberkriminalität und Schutzmaßnahmen in Bildungseinrichtungen und Unternehmen.

Sicherheit überprüfen
Betonung der Notwendigkeit regelmäßiger Sicherheitsüberprüfungen und Audits, besonders für kleinere Unternehmen.



Optionen statt Strafen
Umlenkung auffällig gewordener Jugendlicher in positive Bahnen und Nutzung ihres Talents.

REALITYCHECK: IT-SICHERHEIT IM ÖSTERREICHISCHEN MITTELSTAND

DANKE FÜR DIE AUFMERKSAMKEIT

NEXT: Q&A

ERGEBNISSE IM DETAIL

Legende:

FU: Familienunternehmen

NFU: kein Familienunternehmen

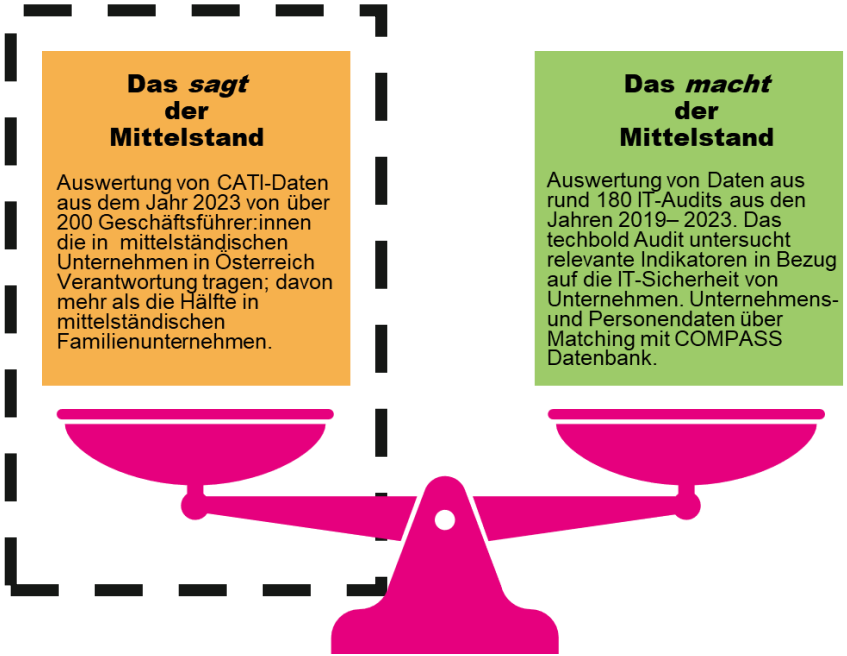
DETAIL-AUSWERTUNG CATI BEFRAGUNG

Das *sagt* der Mittelstand

Auswertung von CATI-Daten aus dem Jahr 2023 von über 200 Geschäftsführer:innen die in mittelständischen Unternehmen in Österreich Verantwortung tragen; davon mehr als die Hälfte in mittelständischen Familienunternehmen.

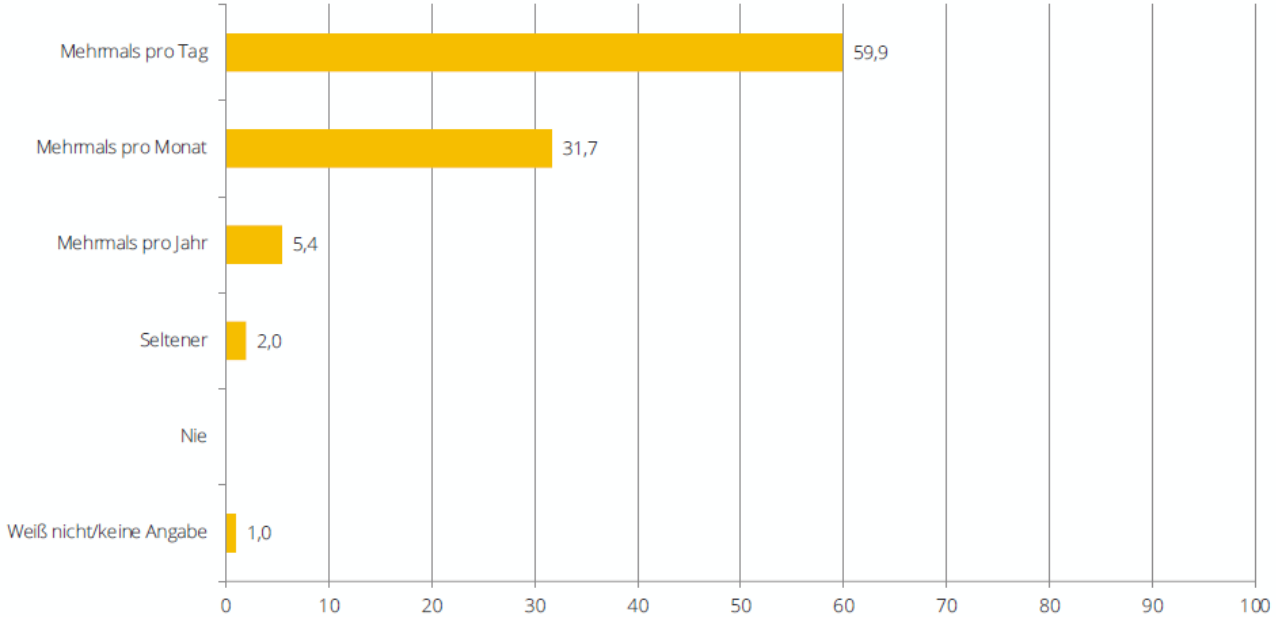
Das *macht* der Mittelstand

Auswertung von Daten aus rund 180 IT-Audits aus den Jahren 2019– 2023. Das techbold Audit untersucht relevante Indikatoren in Bezug auf die IT-Sicherheit von Unternehmen. Unternehmens- und Personendaten über Matching mit COMPASS Datenbank.



EINSCHÄTZUNG DER BEDROHUNGSLAGE

„Was schätzen Sie, wie oft werden österreichische Unternehmen im Durchschnitt (durch z.B. Hacker Malware, Pishing, usw) angegriffen?“

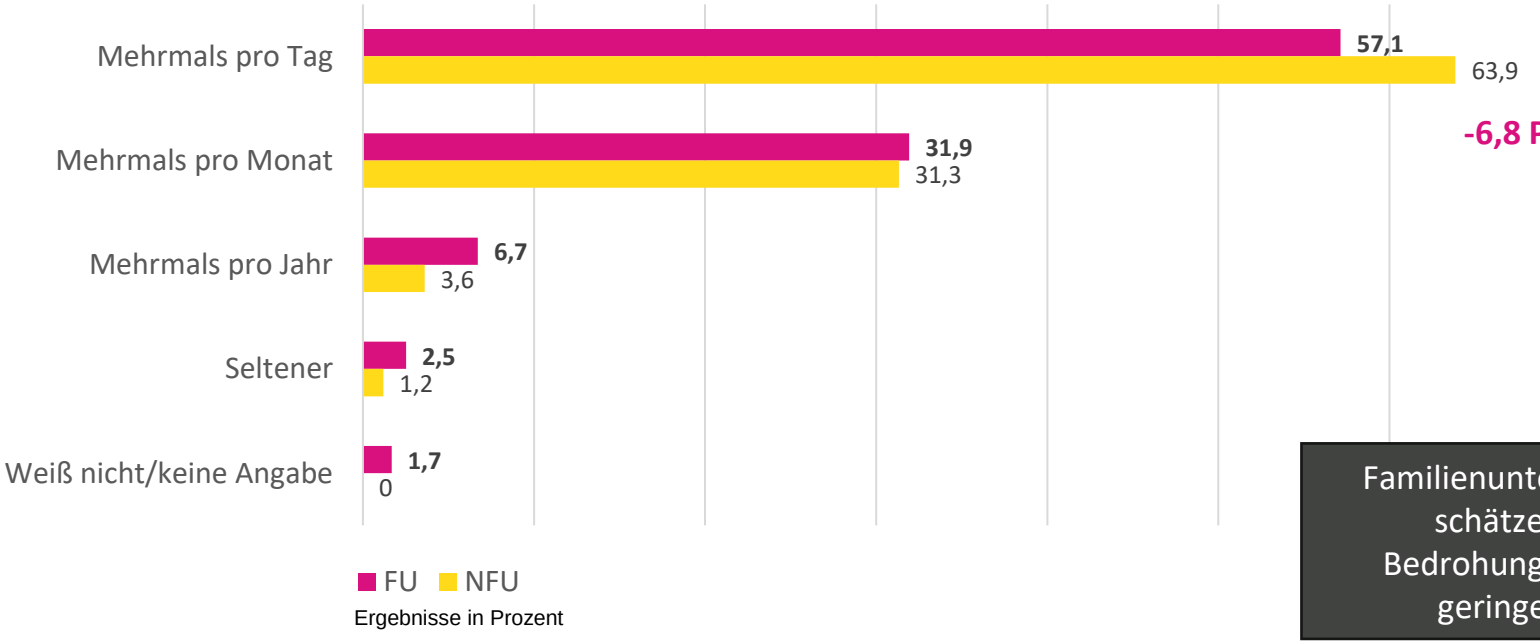


In %, Einfachantwort, n=202

Ausgeprägte Bedrohungslage (mehrheitlich mehrere Angriffe pro Tag)

EINSCHÄTZUNG DER BEDROHUNGSLAGE FU UND NFU IM VERGLEICH

„Was schätzen Sie, wie oft werden österreichische Unternehmen im Durchschnitt (durch z.B. Hacker Malware, Pishing, usw) angegriffen?“



Ergebnisse in Prozent

-6,8 Prozentpunkte

Familienunternehmen schätzen die Bedrohungslage als geringer ein

EINFLUSSFAKTOREN

Größe des Unternehmens: kein statistisch signifikanter Zusammenhang

Sitz des Unternehmens: ausgeprägter & statistisch signifikanter Zusammenhang (0,126**), d.h. je städtischer der Sitz des Unternehmens, desto häufiger werden Angriffe wahrgenommen

Familienunternehmen: erkennbarer & statistisch signifikanter Zusammenhang (-0,115**), d.h. Familienunternehmen nehmen seltener Angriffe wahr

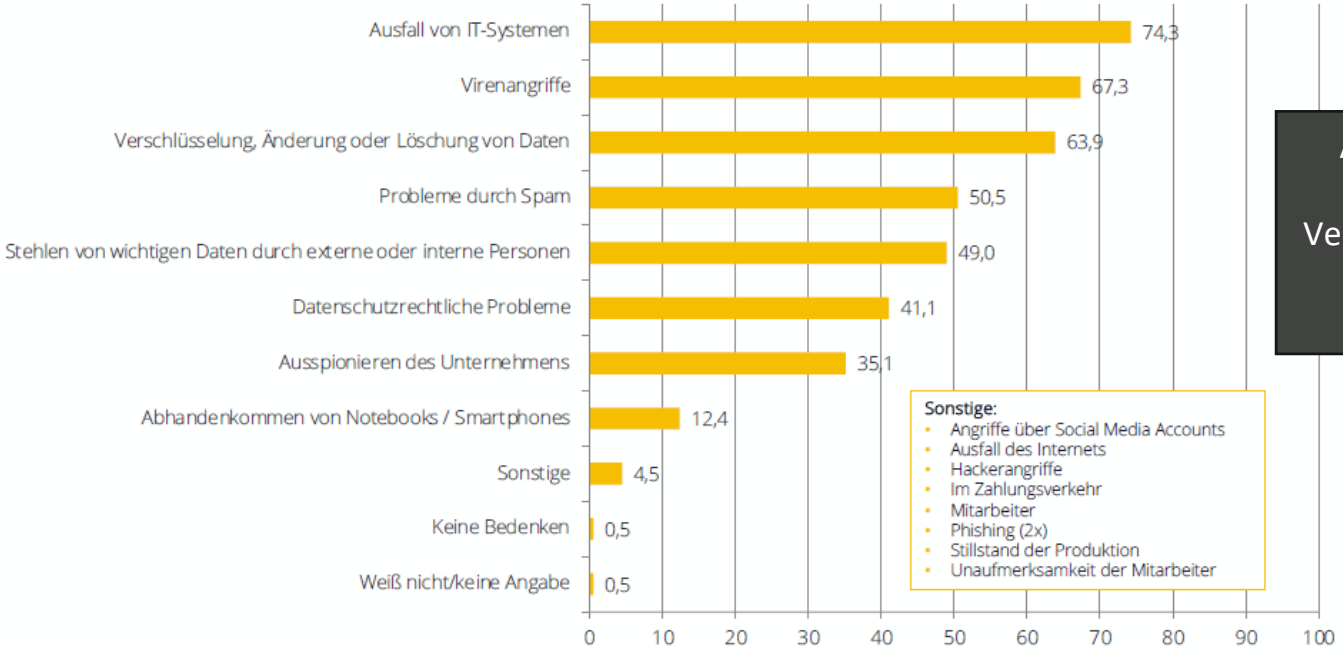
Alter des Familienunternehmens: tendenziell vorhandener Zusammenhang, d.h. desto älter des Familienunternehmen, desto häufiger werden Angriffe wahrgenommen

Verweildauer der GF im Familienunternehmen: ausgeprägter & statistisch signifikanter Zusammenhang (-0,161**), d.h. je länger bereits im Unternehmen, desto häufiger werden Angriffe wahrgenommen

Zeit bis zum nächsten Generationswechsel: starker & statistisch signifikanter Zusammenhang (0,235**), d.h. je länger es bis zum nächsten Generationswechsel dauert, desto seltener werden Angriffe wahrgenommen

BEDENKEN IM BEREICH IT-SECURITY

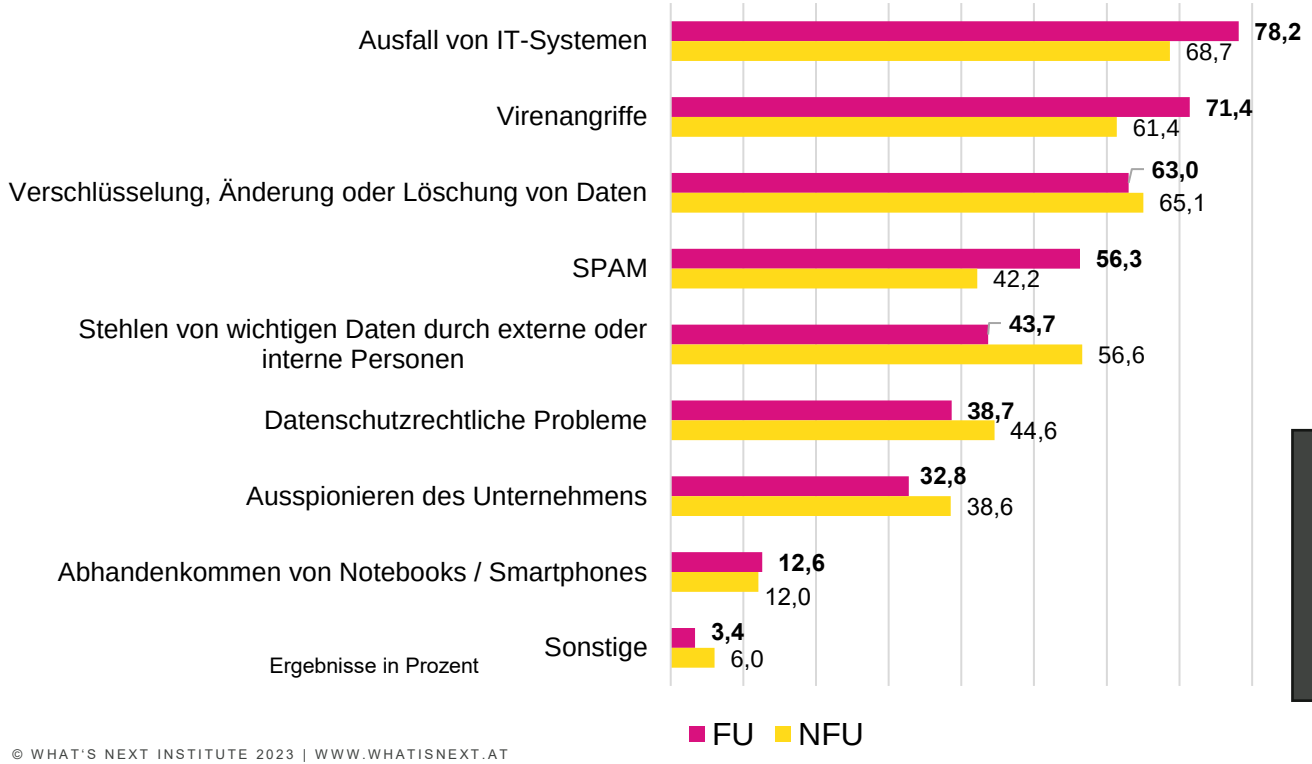
„Was sind Ihre größten IT-Sicherheit Bedenken in Ihrem Unternehmen?“



In %, Mehrfachantworten, n=202

Ausfall von Systemen, Virenangriffe und Verschlüsselung/Änderung von Daten sind Top 3 Bedenken

BEDENKEN IM BEREICH IT SECURITY
FU UND NFU IM VERGLEICH



+9,5 Prozentpunkte

+10,0 Prozentpunkte

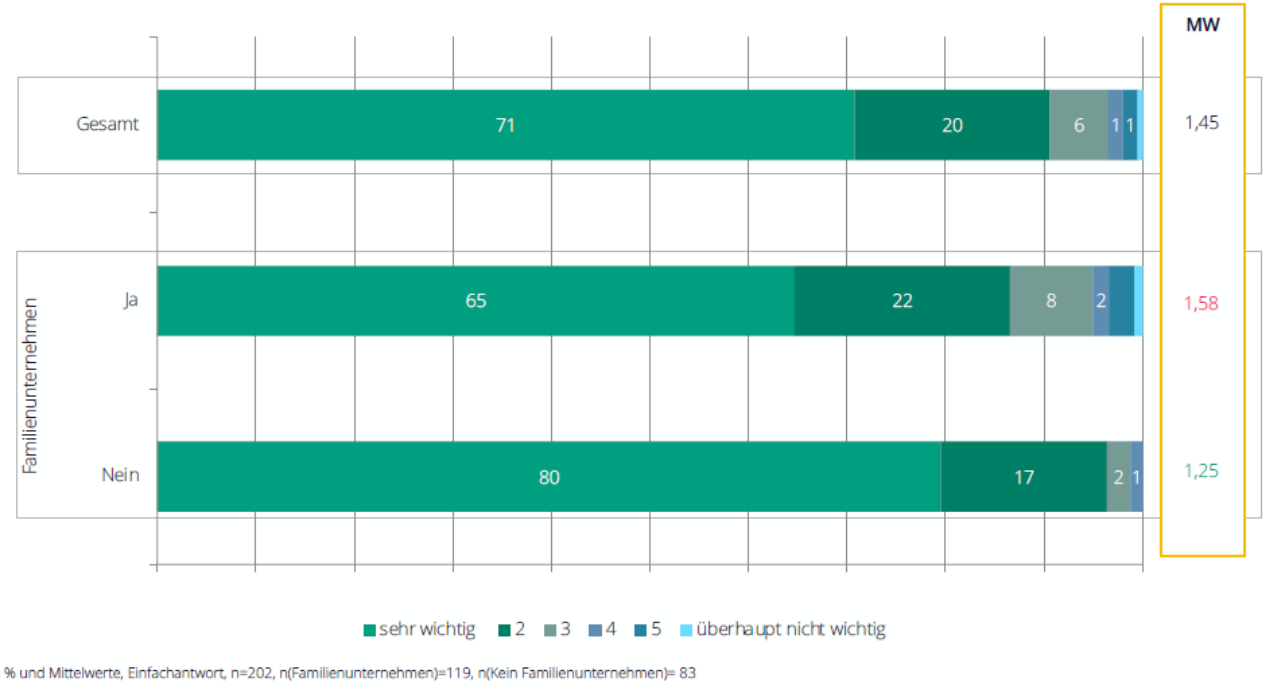
+14,1 Prozentpunkte

-12,9 Prozentpunkte

Familienunternehmen haben ausgeprägtere Wahrnehmung bei zentralen Bedenken – vor allem Ausfall von IT Systemen, Viren, Spam stärker als bei NFU – Datendiebstahl dafür weit weniger

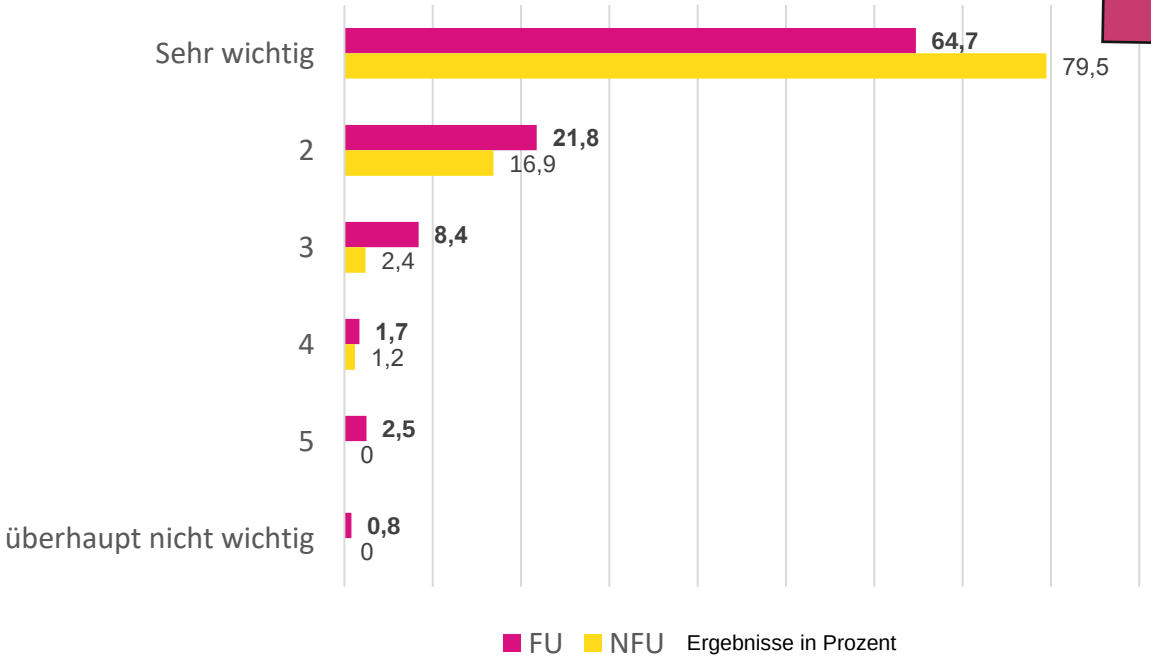
WICHTIGKEIT VON IT-SICHERHEIT IM UNTERNEHMEN

„Wie wichtig ist das Thema IT-Sicherheit innerhalb Ihres Unternehmens?“



In % und Mittelwerte, Einfachantwort, n=202, n(Familienunternehmen)=119, n(Kein Familienunternehmen)= 83

STELLENWERT VON IT-SECURITY IM UNTERNEHMEN FU UND NFU IM VERGLEICH



-14,8 Prozentpunkte

Für Familienunternehmen hat IT-Security einen deutlich geringeren Stellenwert

EINFLUSSFAKTOREN

Größe des Unternehmens: kein statistisch signifikanter Zusammenhang

Sitz des Unternehmens: moderater & statistisch signifikanter Zusammenhang (0,100*), d.h. je städtischer der Sitz des Unternehmens, desto wichtiger wird das Thema IT Security wahrgenommen (ländlicher Raum misst IT Security einen geringeren Stellenwert bei)

Familienunternehmen: ausgeprägter & statistisch hochsignifikanter Zusammenhang (-0,188***), d.h. Familienunternehmen nehmen das Thema IT Security als weniger wichtig wahr

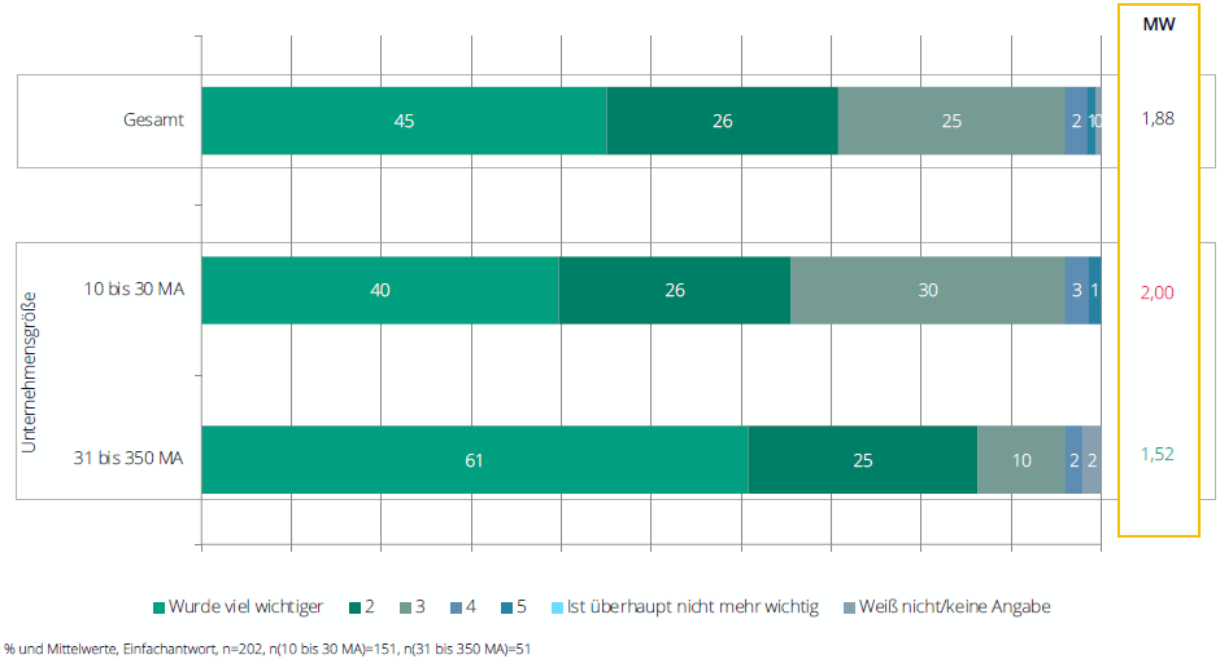
Alter des Familienunternehmens: ausgeprägter & statistisch signifikanter Zusammenhang (0,163**), d.h. desto älter des Familienunternehmen, desto wichtiger wird das Thema IT Security wahrgenommen

Verweildauer der GF im Familienunternehmen: kein statistisch signifikanter Zusammenhang

Zeit bis zum nächsten Generationswechsel: kein statistisch signifikanter Zusammenhang

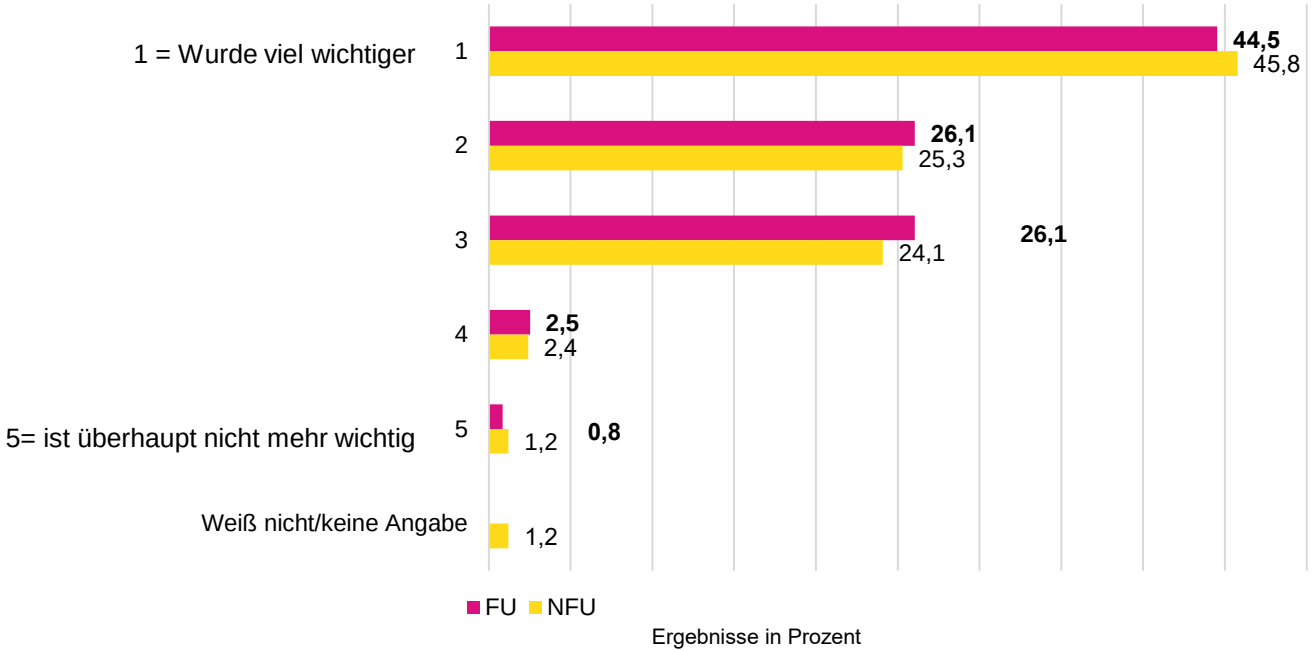
VERÄNDERUNG DER WICHTIGKEIT VON IT-SICHERHEIT IN UNTERNEHMEN

„Wie hat sich der Stellenwert der IT-Sicherheit in Ihrem Unternehmen in den letzten Jahren verändert?“



In % und Mittelwerte, Einfachantwort, n=202, n(10 bis 30 MA)=151, n(31 bis 350 MA)=51

VERÄNDERUNG DER WICHTIGKEIT VON IT-SECURITY IM UNTERNEHMEN FU UND NFU IM VERGLEICH



EINFLUSSFAKTOREN

Größe des Unternehmens: ausgeprägter & statistisch signifikanter Zusammenhang (-0,142**), d.h. größere Unternehmen nehmen das Thema IT Security in den letzten beiden Jahren als zunehmend wichtiger wahr

Sitz des Unternehmens: kein statistisch signifikanter Zusammenhang

Familienunternehmen: kein statistisch signifikanter Zusammenhang

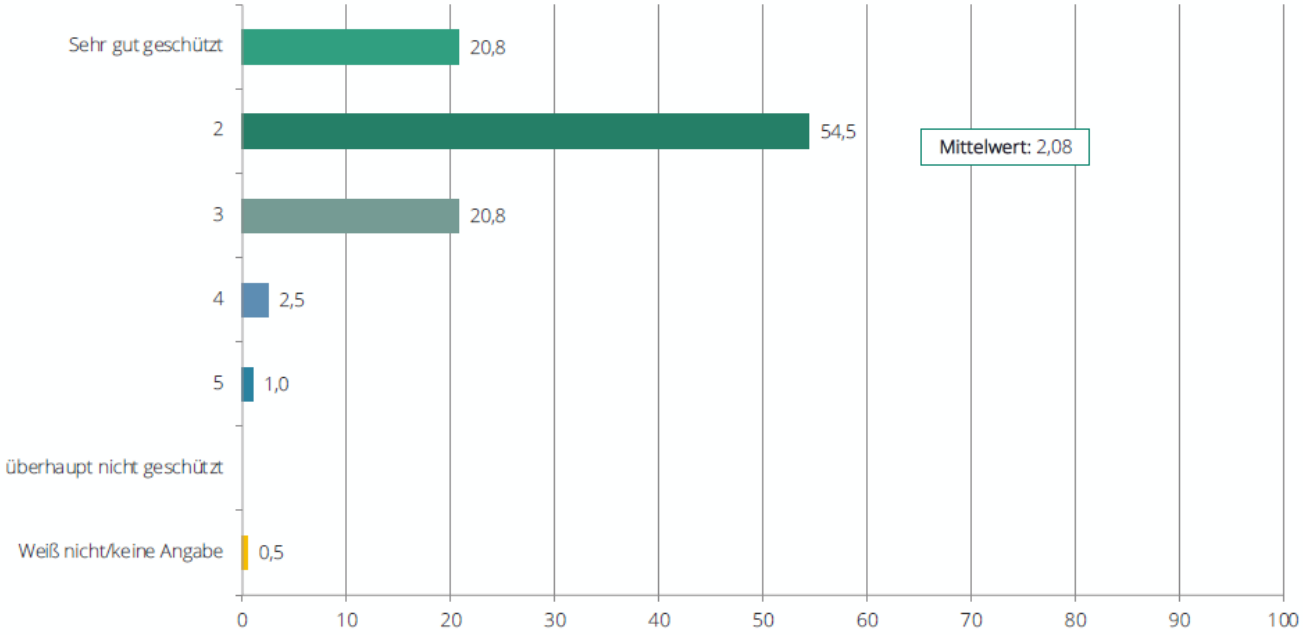
Alter des Familienunternehmens: kein statistisch signifikanter Zusammenhang

Verweildauer der GF im Familienunternehmen: kein statistisch signifikanter Zusammenhang

Zeit bis zum nächsten Generationswechsel: kein statistisch signifikanter Zusammenhang

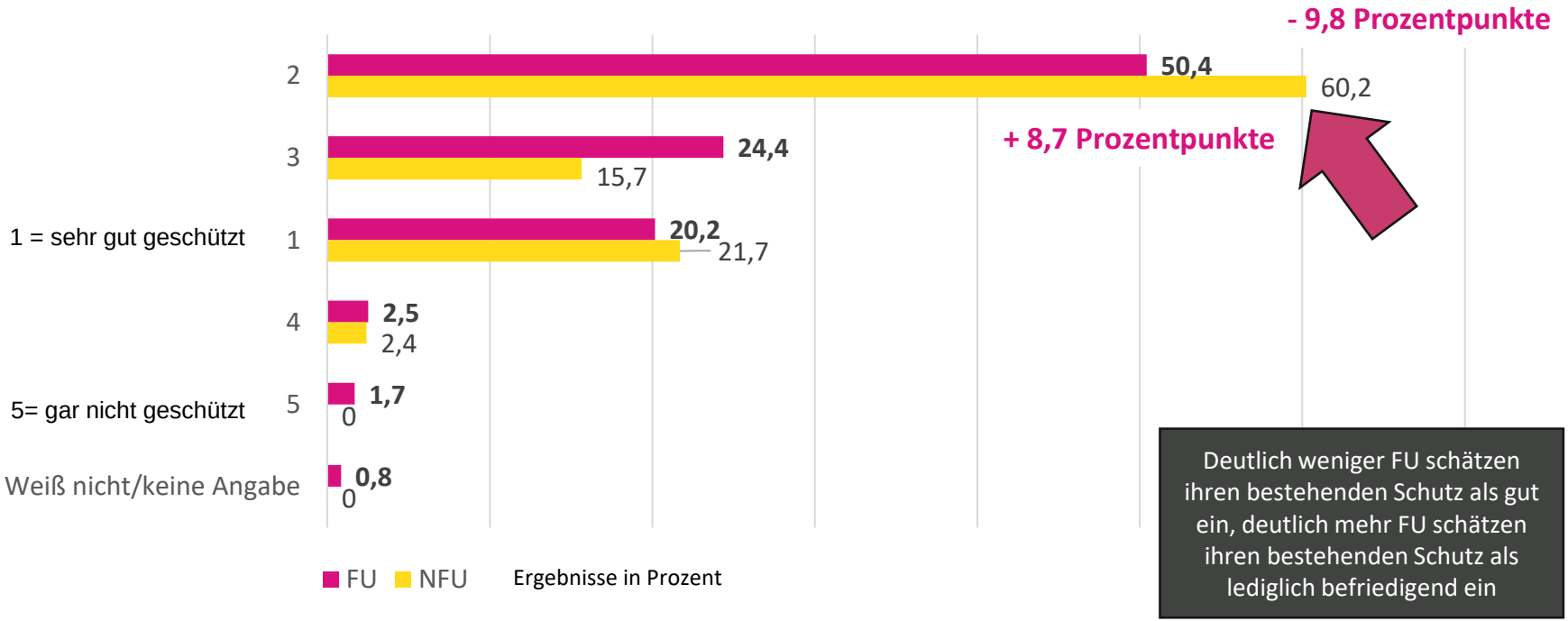
EINSCHÄTZUNG DES BESTEHENDEN SCHUTZES

„Was denken Sie, wie gut ist Ihr Unternehmen vor internen und externen Angriffen und Datenverlust geschützt?“



In % und Mittelwert, Einfachantwort, n=202

EINSCHÄTZUNG DES BESTEHENDE SCHUTZES FU UND NFU IM VERGLEICH



Deutlich weniger FU schätzen ihren bestehenden Schutz als gut ein, deutlich mehr FU schätzen ihren bestehenden Schutz als lediglich befriedigend ein

EINFLUSSFAKTOREN

Größe des Unternehmens: kein statistisch signifikanter Zusammenhang

Sitz des Unternehmens: kein statistisch signifikanter Zusammenhang

Familienunternehmen: moderater & statistisch signifikanter Zusammenhang (-0,114**), d.h. Familienunternehmen fühlen sich weniger gut vor internen/externen Angriffen und Datenverlust geschützt

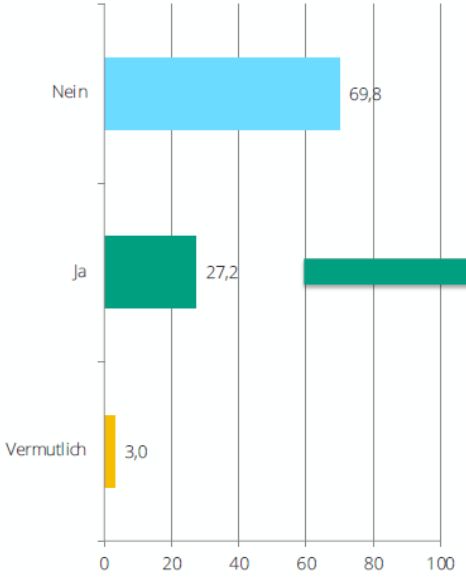
Alter des Familienunternehmens: ausgeprägter & statistisch hochsignifikanter Zusammenhang (0,245***), d.h. ältere Familienunternehmen fühlen sich weit besser vor internen/externen Angriffen und Datenverlust geschützt

Verweildauer der GF im Familienunternehmen: kein statistisch signifikanter Zusammenhang

Zeit bis zum nächsten Generationswechsel: kein statistisch signifikanter Zusammenhang

IT-SECURITY VORFÄLLE IN DEN LETZTEN 2 JAHREN

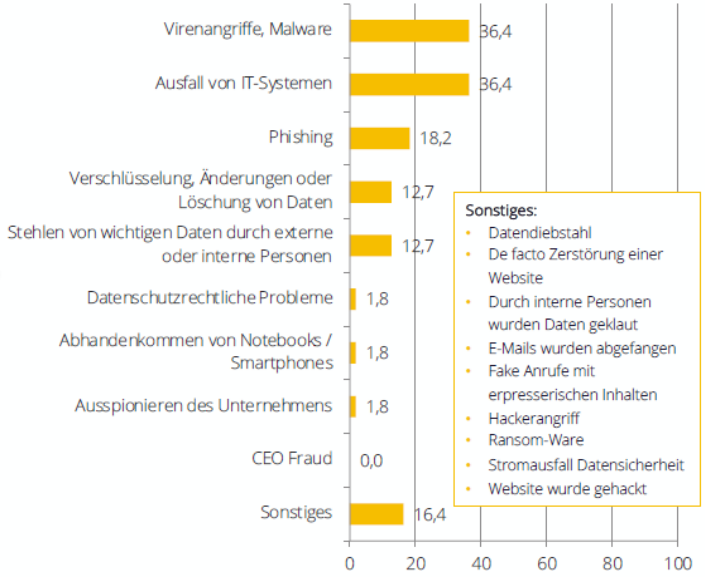
„Hat es in Ihrem Unternehmen in den letzten 2 Jahren einen IT-Security-Vorfall (wie z.B. Industriespionage, Virenangriffe, Ausfall von IT-Systemen, Datenverlust, Datenmanipulation, usw.) gegeben?"



In %, Einfachantwort, n=202

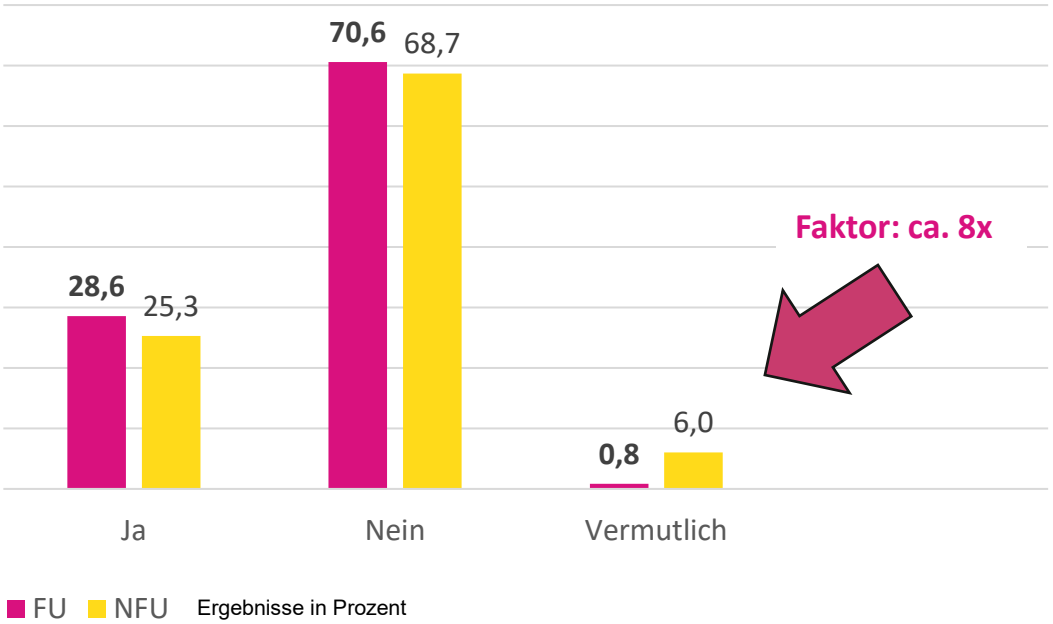
„Welche IT-Security-Vorfälle waren das?"

Frage wurde nur jenen gestellt, in deren Unternehmen es in den letzten 2 Jahren einen IT-Vorfall gab.



In %, Mehrfachantworten, n=55

IT-SECURITY VORFÄLLE IN DEN LETZTEN 2 JAHREN FU IM VERGLEICH ZU NFU



FU scheinen stärker davon auszugehen, dass sie wissen NICHT Opfer geworden zu sein. 0,8 % der Befragten FU geht davon aus vermutlich Opfer eines Angriffs geworden zu sein, während 6% der NFU davon ausgehen, vermutlich Opfer zu sein, es aber einfach nicht zu wissen. Nahezu Faktor 8 im Unterschied. könnte auf starke Unterschätzung der Gefahren durch FU hinweisen (‚trügerische Sicherheit').

EINFLUSSFAKTOREN

Größe des Unternehmens: starker & statistisch hochsignifikanter Zusammenhang (-0,246***), d.h. desto größer das Unternehmen desto eher gab es einen IT Security Vorfall in den letzten beiden Jahren

Sitz des Unternehmens: kein statistisch signifikanter Zusammenhang (spannend, weil offenbar oftmals vermutet dass am Land seltener Vorfälle passieren – scheint aber nicht so zu sein)

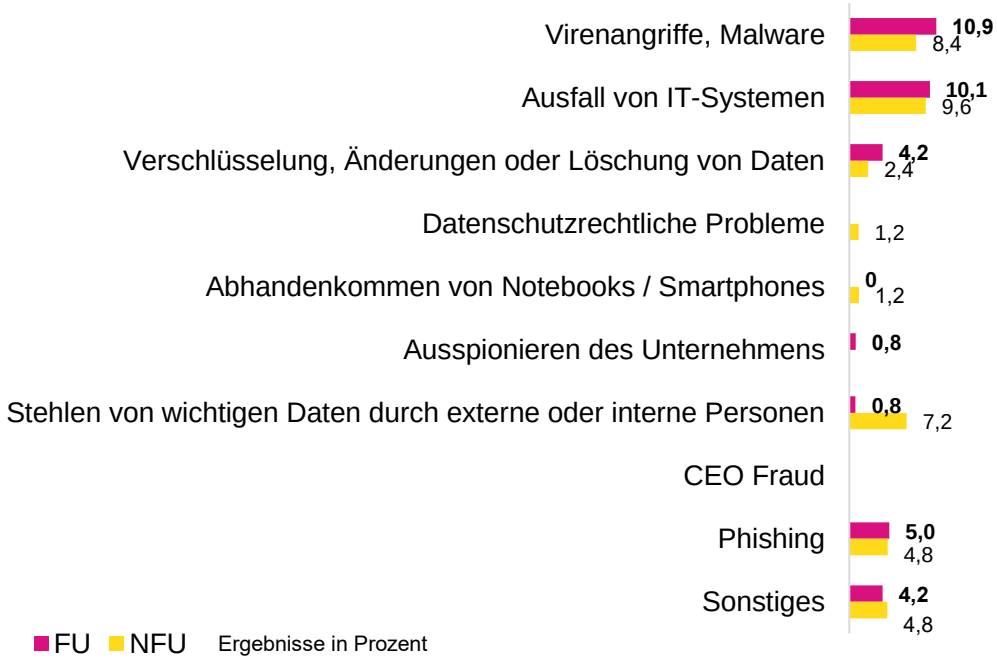
Familienunternehmen: kein statistisch signifikanter Zusammenhang

Alter des Familienunternehmens: kein statistisch signifikanter Zusammenhang

Verweildauer der GF im Familienunternehmen: starker & statistisch hochsignifikanter Zusammenhang (0,343***), d.h. desto länger die Verweildauer der GF desto eher gab es keinen bzw. keinen registrierten IT Security Vorfall in den letzten beiden Jahren

Zeit bis zum nächsten Generationswechsel: kein statistisch signifikanter Zusammenhang

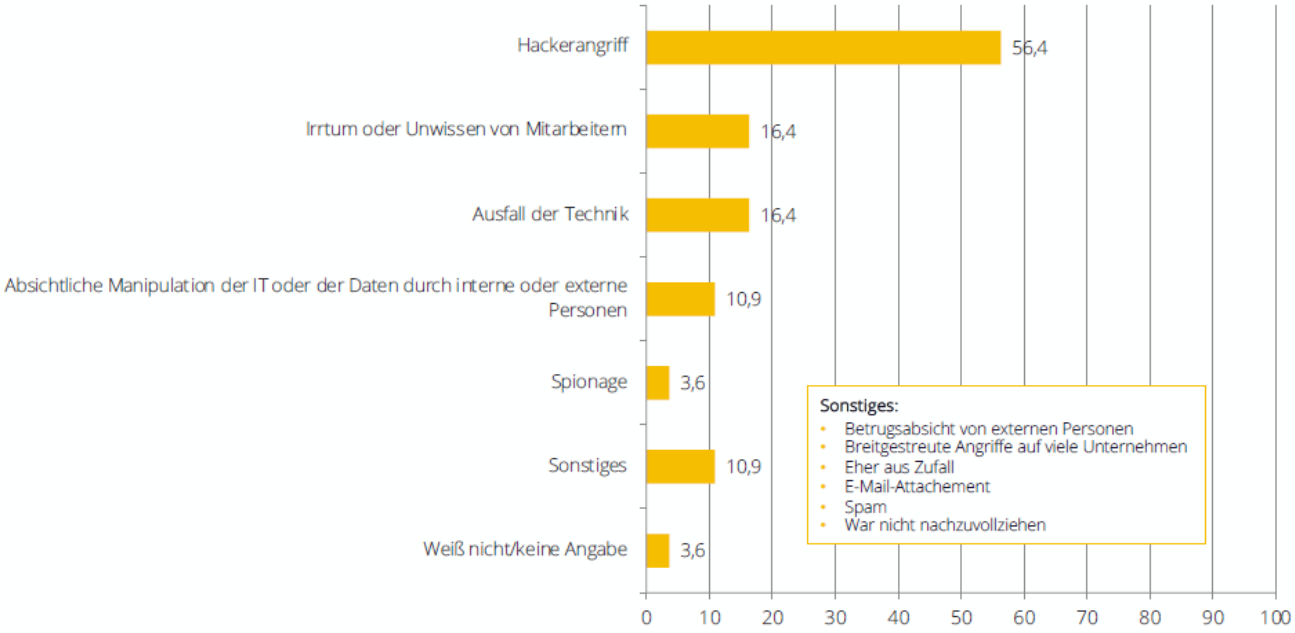
ARTEN VON IT-SECURITY VORFÄLLEN FU UND NFU IM VERGLEICH



URSACHEN FÜR IT-SECURITY-VORFÄLLE

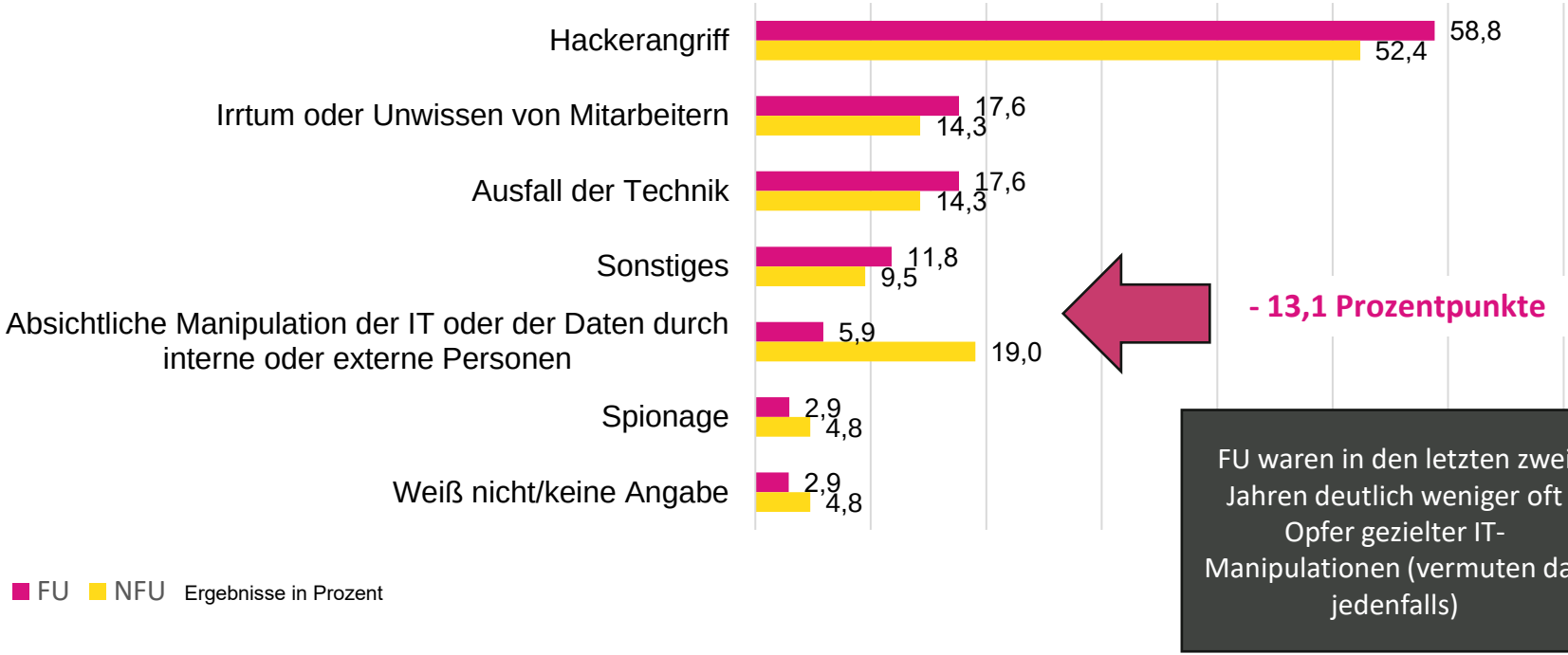
„Und was waren die Ursachen für diese IT-Security-Vorfälle?"

Frage wurde nur jenen gestellt, in deren Unternehmen es in den letzten 2 Jahren einen IT-Vorfall gab.



In %, Mehrfachantworten, n=55

URSACHEN FÜR IT-SECURITY VORFÄLLE FU UND NFU IM VERGLEICH

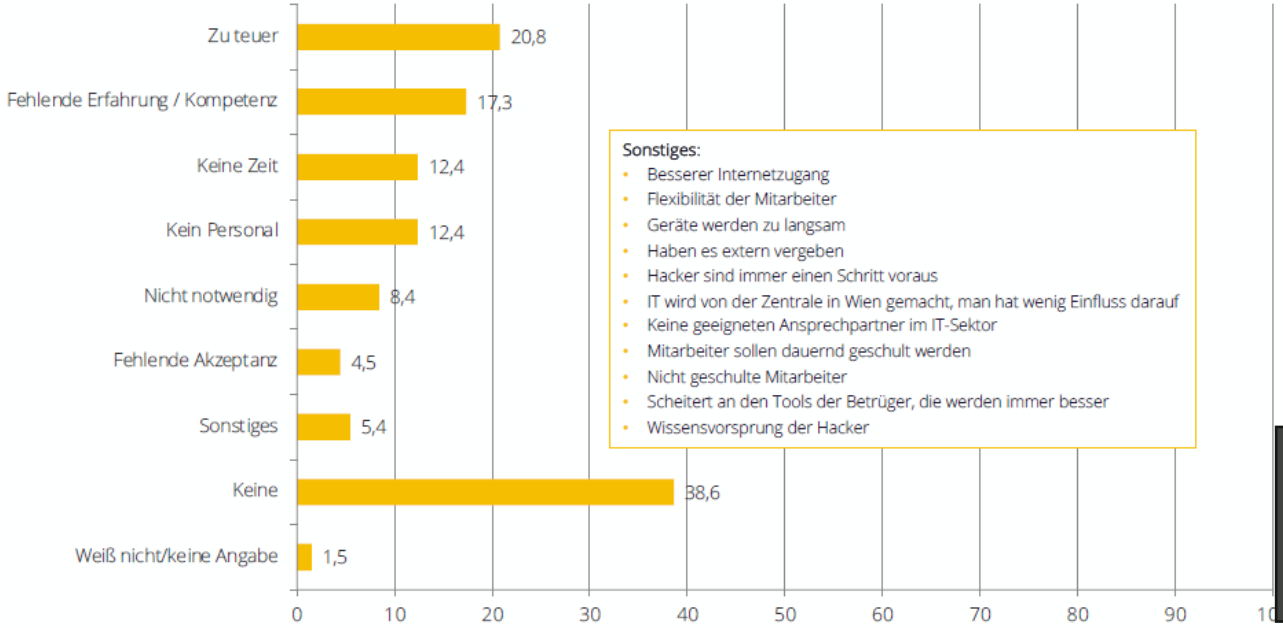


- 13,1 Prozentpunkte

FU waren in den letzten zwei Jahren deutlich weniger oft Opfer gezielter IT-Manipulationen (vermuten das jedenfalls)

HEMMNISSE BEI DER VERBESSRUNG DER IT-SECURITY

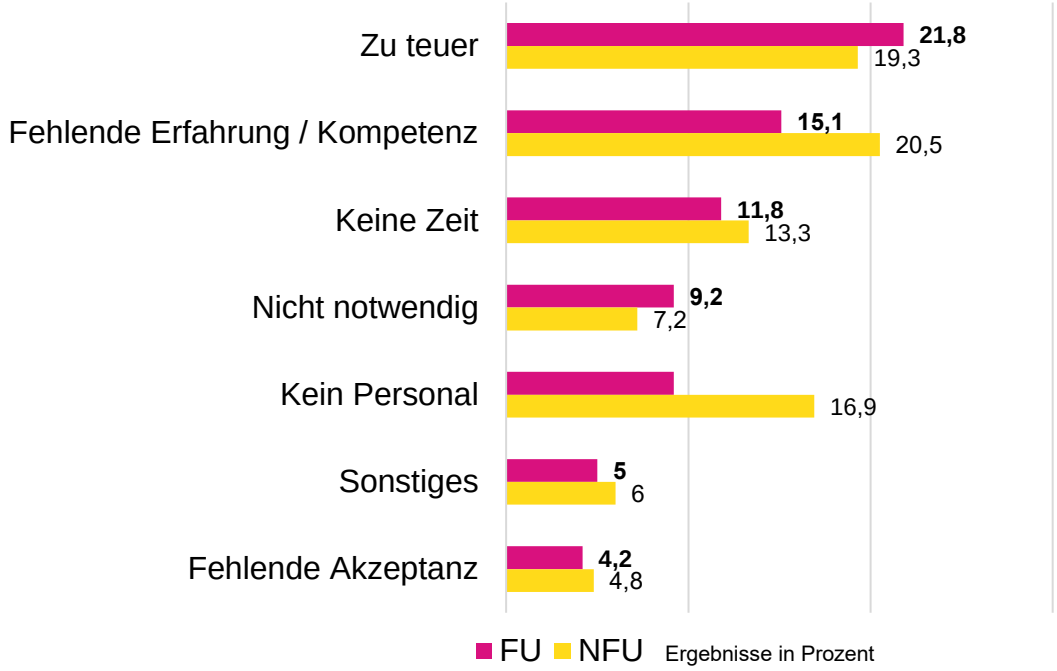
„Welche Hemmnisse sehen Sie in Ihrem Unternehmen, die einer Verbesserung der IT-Security entgegenwirken?"



Rund 40 Prozent der Mittelständler sehen KEINE Hemmnisse bei der Verbesserung der IT-Security

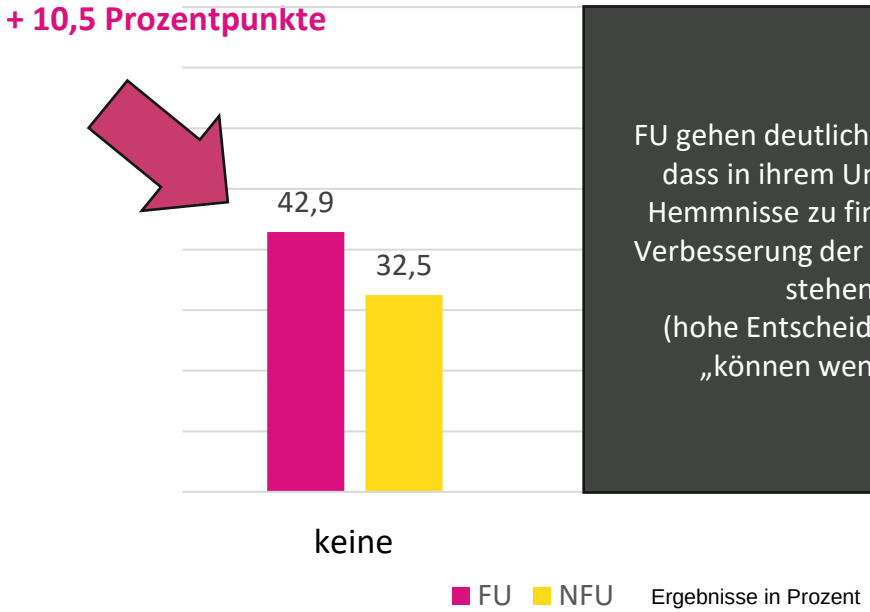
In %, Mehrfachantworten, n=202

HEMMNISSE BEI DER VERBESSRUNG DER IT-SECURITY FU UND NFU IM VERGLEICH



KEINE Hemmnisse: Detailanalyse (nächste Folie)

KEINE HEMMNISSE BEI DER VERBESSRUNG DER IT-SECURITY: FU UND NFU IM VERGLEICH



FU gehen deutlich häufiger davon aus, dass in ihrem Unternehmen keine Hemmnisse zu finden sind, die einer Verbesserung der IT-Security im Wege stehen als NFU
(hohe Entscheidungskompetenz – „können wenn wir wollen“).

EINFLUSSFAKTOREN

Größe des Unternehmens: kein statistisch signifikanter Zusammenhang

Sitz des Unternehmens: kein statistisch signifikanter Zusammenhang

Familienunternehmen: moderater & statistisch signifikanter Zusammenhang (-0,104*), d.h. Familienunternehmen sehen seltener Hemmnisse bei der Verbesserung der IT Security

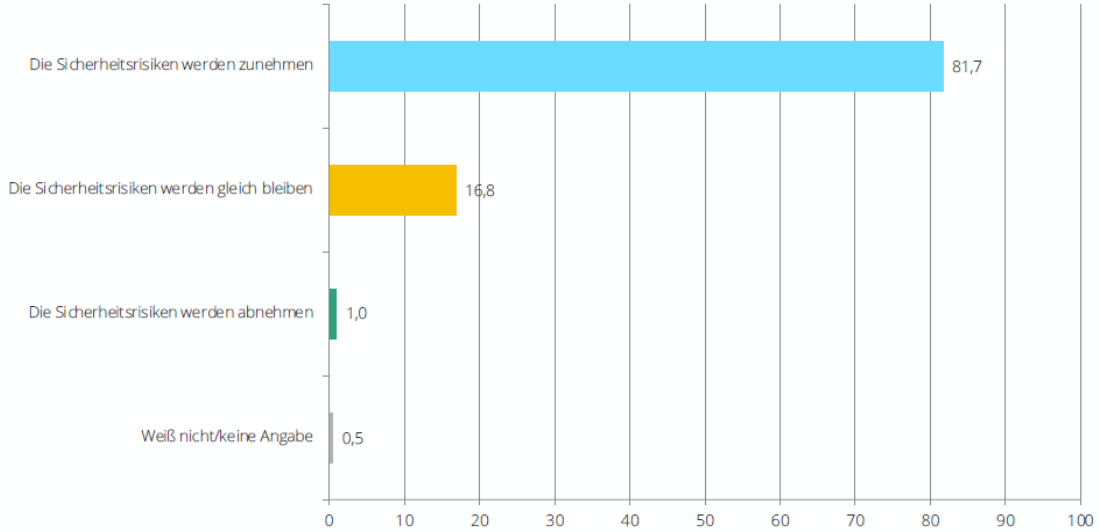
Alter des Familienunternehmens: moderater & statistisch signifikanter Zusammenhang (-0,132*), d.h. ältere Familienunternehmen sehen öfter Hemmnisse bei der Verbesserung der IT Security

Verweildauer der GF im Familienunternehmen: kein statistisch signifikanter Zusammenhang

Zeit bis zum nächsten Generationswechsel: kein statistisch signifikanter Zusammenhang

VERÄNDERUNG DER SICHERHEITSRISIKTEN IN DEN NÄCHSTEN ZWEI JAHREN

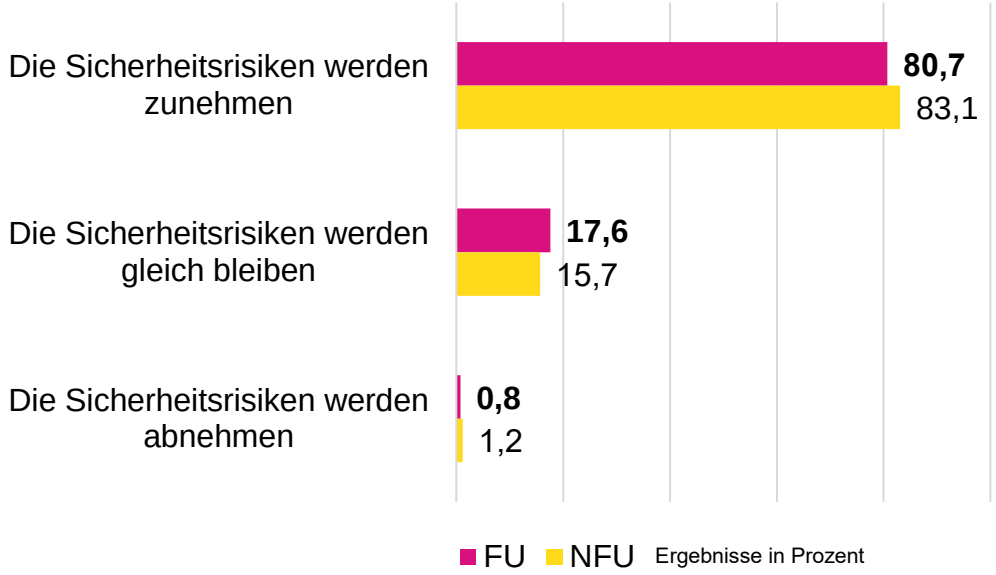
„Wie werden sich Ihrer Meinung nach die Sicherheitsrisiken im IT-Bereich in den nächsten zwei Jahren verändern?“



In %, Einfachantwort, n=202

Sicherheitsrisiken nehmen zu – überwiegende Mehrheit sieht das so

VERÄNDERUNG SICHERHEITSRISIKTEN IN DEN NÄCHSTEN ZWEI JAHREN FU UND NFU IM VERGLEICH



EINFLUSSFAKTOREN

Größe des Unternehmens: kein statistisch signifikanter Zusammenhang

Sitz des Unternehmens: moderater & statistisch signifikanter Zusammenhang (-0,129**), d.h. Unternehmen mit einem Sitz im ländlichen Raum sehen eine stärkere Zunahme der Risiken im Bereich der IT Security in den nächsten zwei Jahren

Familienunternehmen: kein statistisch signifikanter Zusammenhang

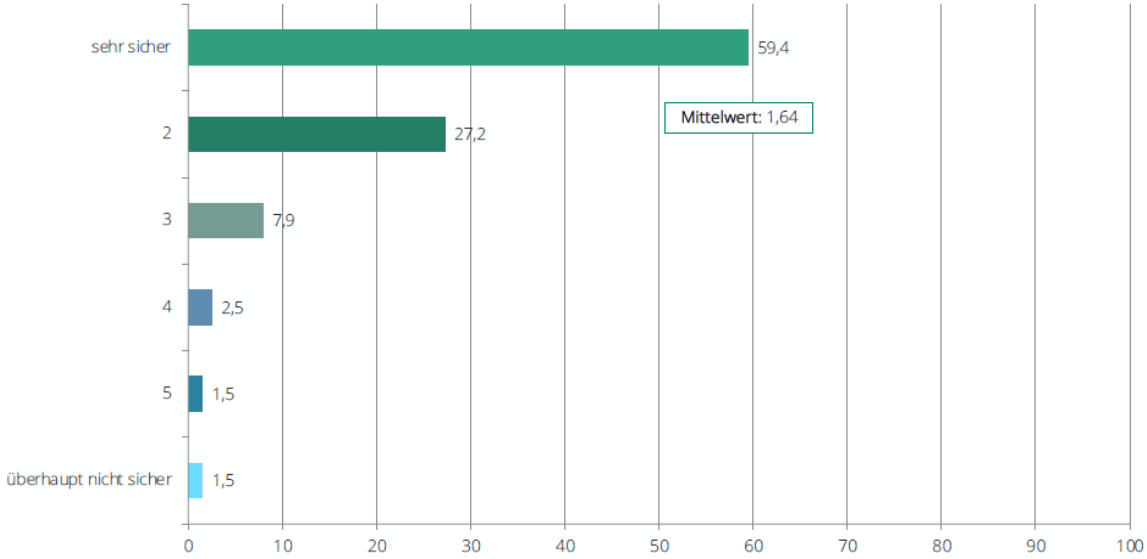
Alter des Familienunternehmens: kein statistisch signifikanter Zusammenhang

Verweildauer der GF im Familienunternehmen: moderater & statistisch signifikanter Zusammenhang (-0,141*), d.h. Familienunternehmen mit einer längeren Verweildauer der GF sehen eine stärkere Zunahme der Risiken im Bereich der IT Security in den nächsten zwei Jahren

Zeit bis zum nächsten Generationswechsel: starker & statistisch hochsignifikanter Zusammenhang (0,226***), d.h. Familienunternehmen mit einer längeren Zeitspanne bis zum nächsten Generationswechsel sehen eine geringere Zunahme der Risiken im Bereich der IT Security in den nächsten zwei Jahren

ORDNUNGSGEMÄSSE DATENSICHERUNG IM UNTERNEHMEN

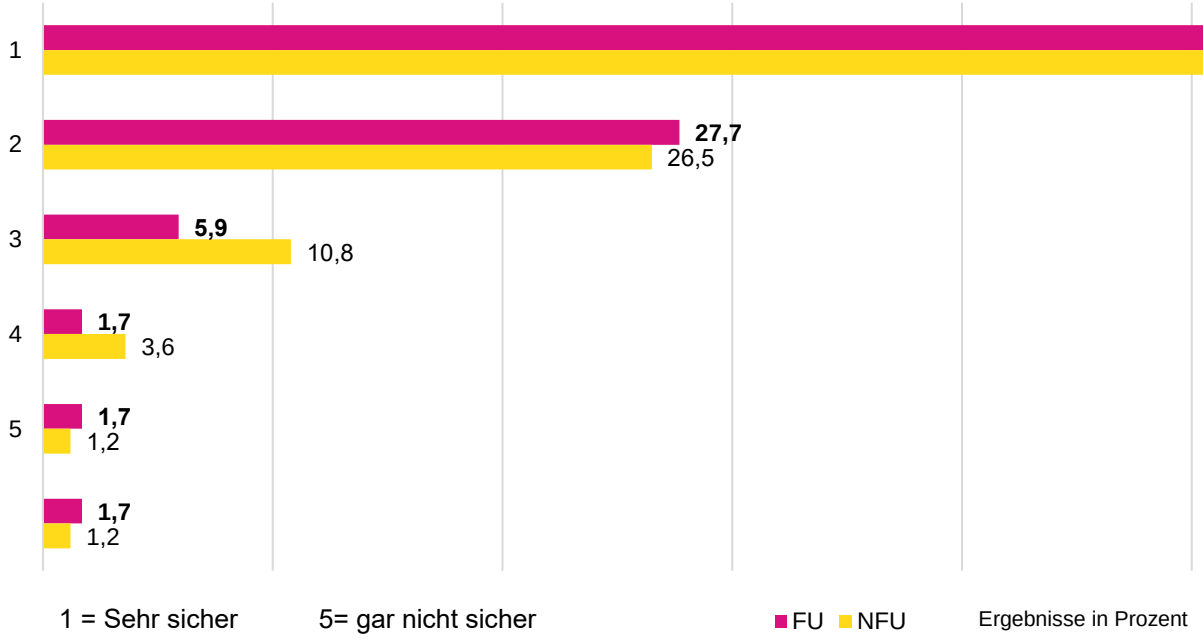
„Sind Sie sicher, dass alle wichtigen Daten in Ihrem Unternehmen ordnungsgemäß gesichert und im Ernstfall rasch wieder hergestellt werden können?“



In % und Mittelwert, Einfachantwort, n=202

Rund 60% sind sich sehr sicher, dass sie alle wichtigen Daten gut gesichert haben und wieder herstellen können

ORDNUNGSGEMÄSSE DATENSICHERUNG IM UNTERNEHMEN FU UND NFU IM VERGLEICH



+4,7 Prozentpunkte

Familienunternehmen sind sich besonders sicher dass Daten gut gesichert und wieder hergestellt werden können

EINFLUSSFAKTOREN

Größe des Unternehmens: kein statistisch signifikanter Zusammenhang

Sitz des Unternehmens: kein statistisch signifikanter Zusammenhang

Familienunternehmen: kein statistisch signifikanter Zusammenhang

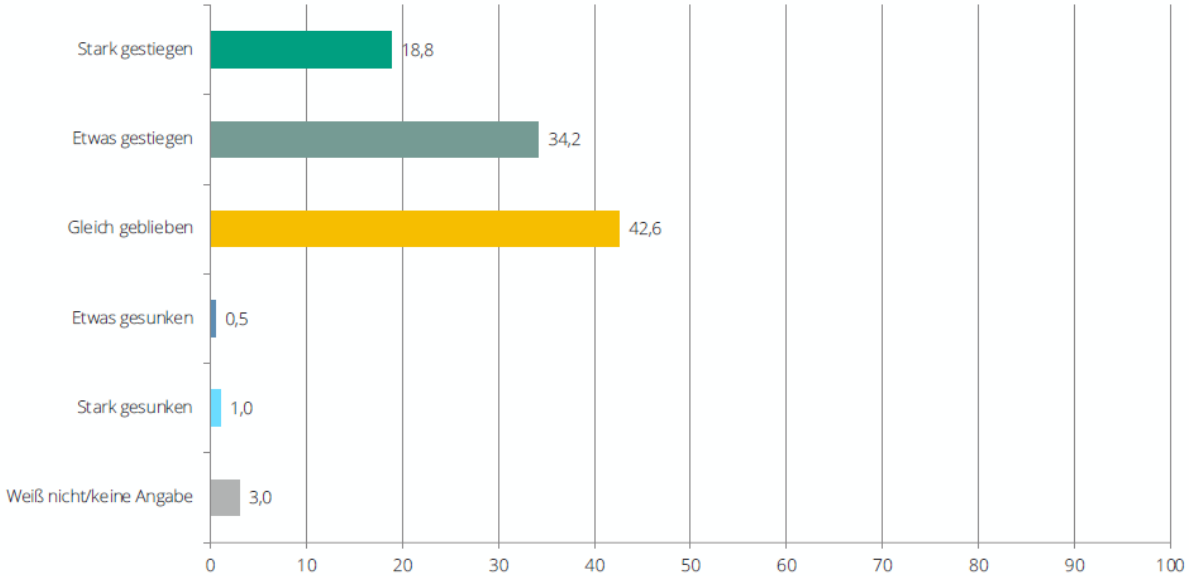
Alter des Familienunternehmens: starker & statistisch hochsignifikanter Zusammenhang (0,242***), d.h. ältere Familienunternehmen sind sich weniger sicher, dass alle wichtigen Daten im Unternehmen ordnungsgemäß gesichert und im Ernstfall wiederhergestellt werden können

Verweildauer der GF im Familienunternehmen: starker & statistisch hochsignifikanter Zusammenhang (0,276***), d.h. Familienunternehmen mit einer längeren Verweildauer der GF sind sich weniger sicher, dass alle wichtigen Daten im Unternehmen ordnungsgemäß gesichert und im Ernstfall wiederhergestellt werden können

Zeit bis zum nächsten Generationswechsel: kein statistisch signifikanter Zusammenhang

VERÄNDERUNG DES IT-BUDGETS IM LETZTEN JAHR

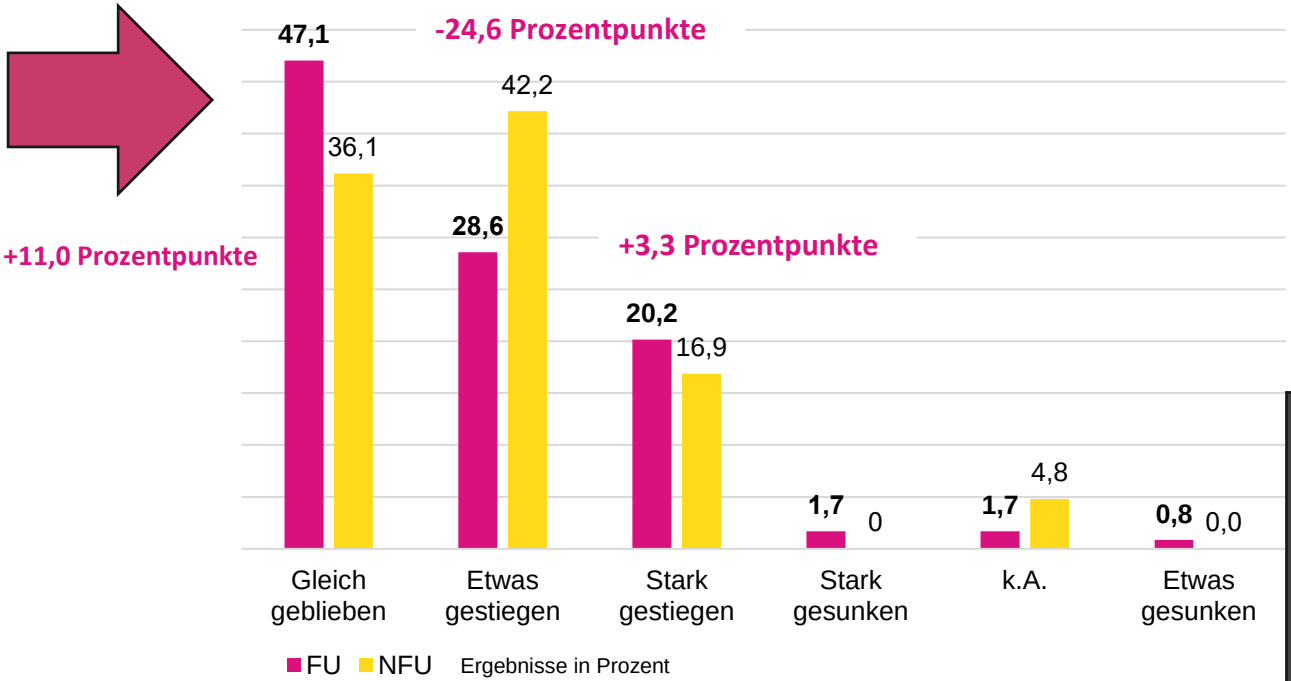
„Wie hat sich das IT-Budget in Ihrem Unternehmen im Vergleich zum Vorjahr verändert?“



In %, Einfachantwort, n=202

Die knappe Mehrheit (53%) gibt an das IT-Budget im letzten Jahr stark oder etwas erhöht zu haben

WIE HAT SICH DAS IT-BUDGET IN IHREM UNTERNEHMEN IM VERGLEICH ZUM VORJAHR VERÄNDERT?



Familienunternehmen haben das IT-Budget eher nicht verändert, während Nicht-Familienunternehmen eine leichte Steigerung des IT-Budgets im Vergleich zum Vorjahr verzeichnen

EINFLUSSFAKTOREN

Größe des Unternehmens: kein statistisch signifikanter Zusammenhang

Sitz des Unternehmens: kein statistisch signifikanter Zusammenhang

Familienunternehmen: kein statistisch signifikanter Zusammenhang

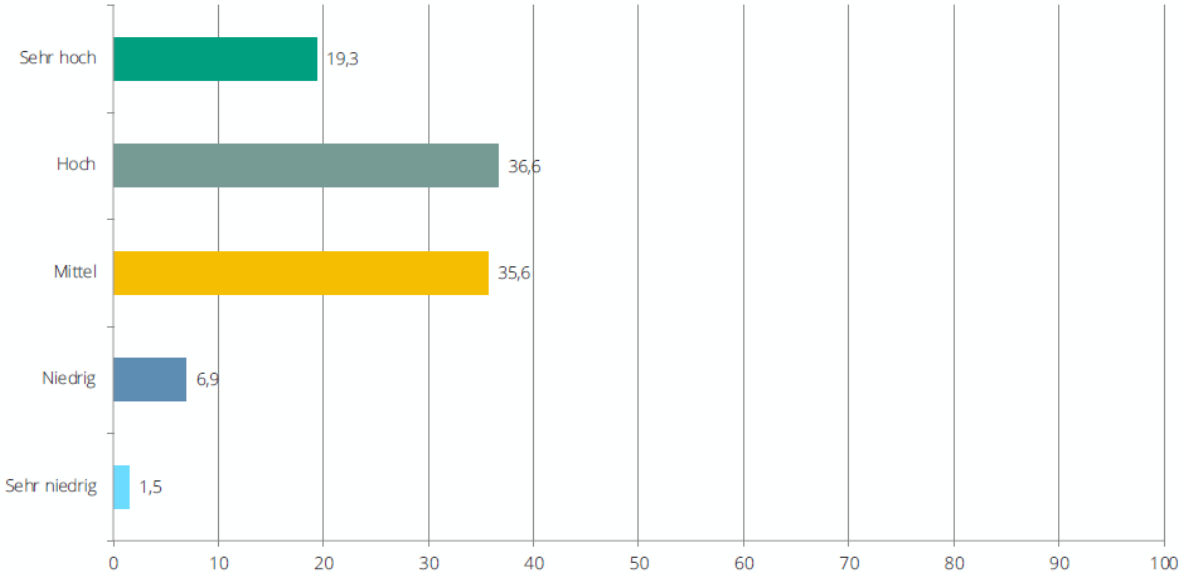
Alter des Familienunternehmens: kein statistisch signifikanter Zusammenhang

Verweildauer der GF im Familienunternehmen: kein statistisch signifikanter Zusammenhang

Zeit bis zum nächsten Generationswechsel: kein statistisch signifikanter Zusammenhang

KOMPETENZ UND KNOW-HOW ZUM THEMA IT-SICHERHEIT

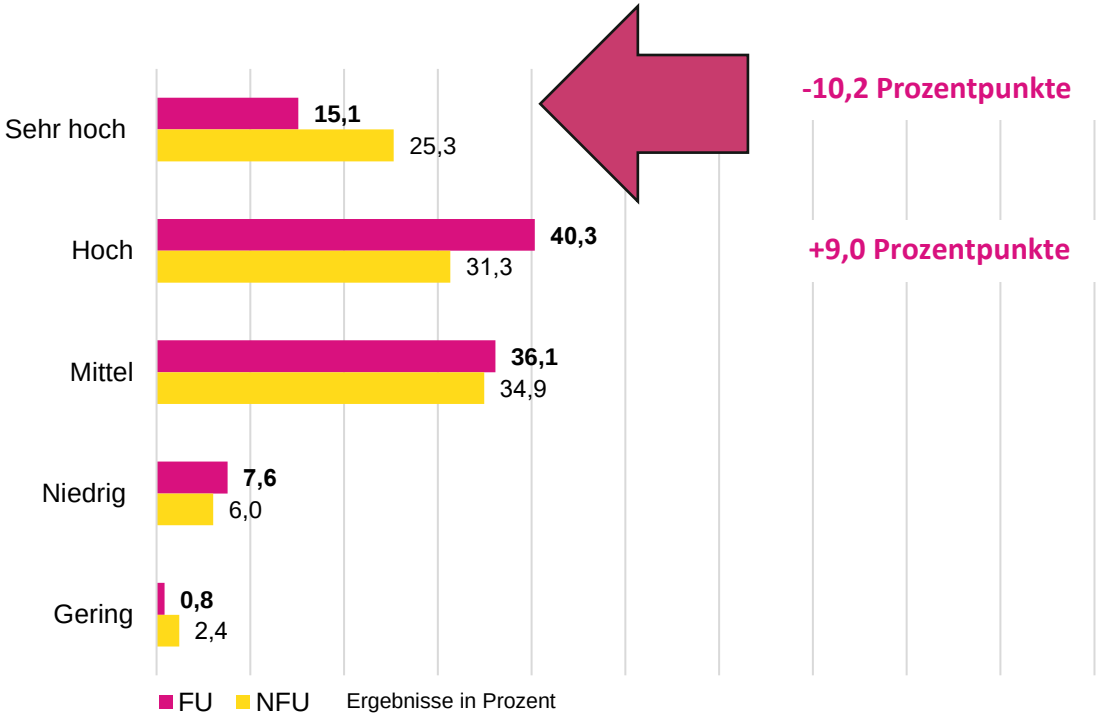
„Wie schätzen Sie die Kompetenz und das Know-How zum Thema IT-Sicherheit in Ihrem Unternehmen ein?“



In %, Einfachantwort, n=202

Die Mehrheit der Mittelständler (rund 56%) schätzt die Kompetenz im Bereich IT-Sicherheit als sehr hoch oder hoch ein

KOMPETENZ UND KNOW-HOW ZUM THEMA IT-SICHERHEIT: FU UND NFU IM VERGLEICH



-10,2 Prozentpunkte

+9,0 Prozentpunkte

Familienunternehmen schätzen ihre Kompetenz im Bereich IT-Sicherheit seltener als sehr hoch ein als Nicht-Familienunternehmen

EINFLUSSFAKTOREN

Größe des Unternehmens: kein statistisch signifikanter Zusammenhang

Sitz des Unternehmens: moderater & statistisch signifikanter Zusammenhang (0,149**), d.h. Unternehmen mit einem Sitz im ländlichen Raum schätzen ihre Kompetenz und ihr Know-how in Bezug auf IT-Security als geringer ein

Familienunternehmen: kein statistisch signifikanter Zusammenhang

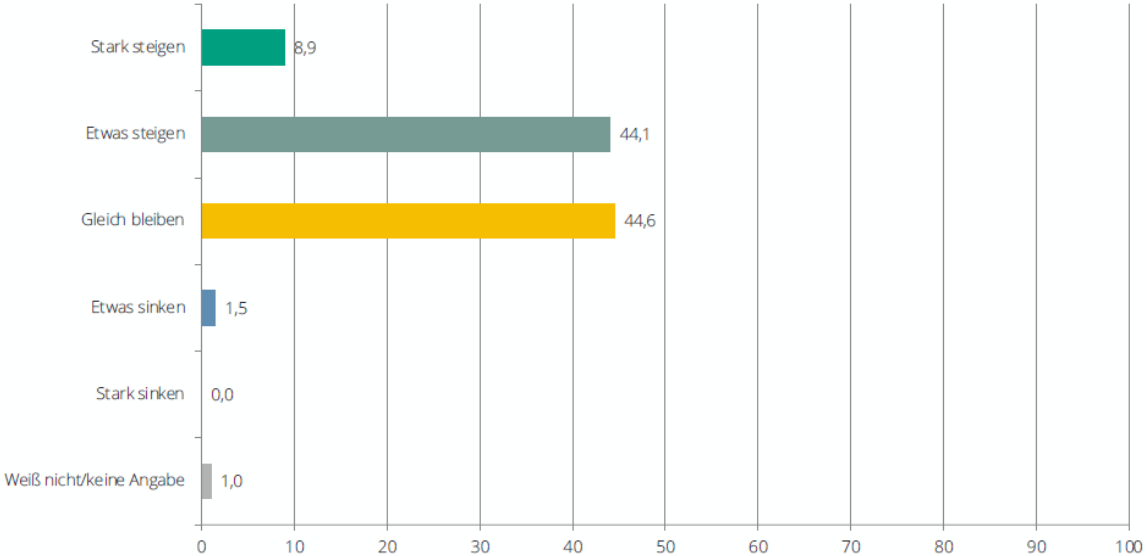
Alter des Familienunternehmens: kein statistisch signifikanter Zusammenhang

Verweildauer der GF im Familienunternehmen: kein statistisch signifikanter Zusammenhang

Zeit bis zum nächsten Generationswechsel: kein statistisch signifikanter Zusammenhang

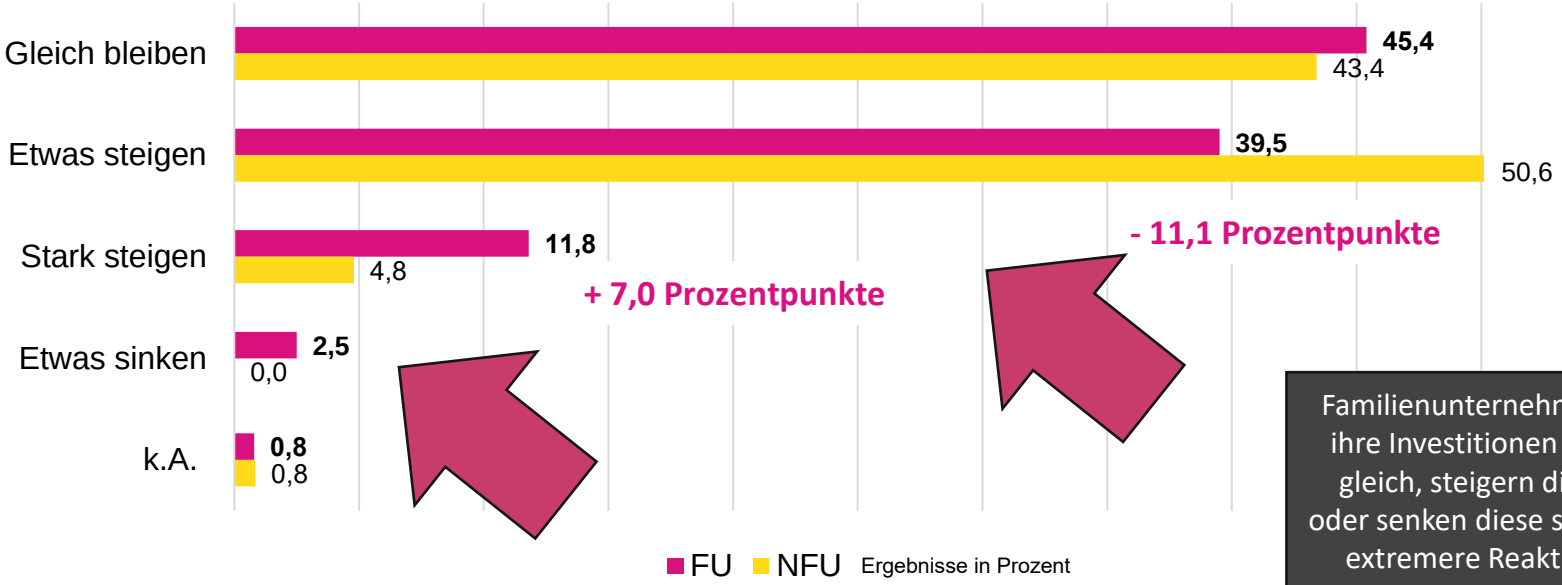
INVESTITIONEN IN DIE IT-SICHERHEIT IM KOMMENDEN JAHR

„Was schätzen Sie, wie werden sich die Investitionen in die IT-Sicherheit Ihres Unternehmens im Jahr 2024 gegenüber 2023 verändern?“



In %, Einfachantwort, n=202

INVESTITIONEN IN DIE IT-SICHERHEIT IN DEN KOMMENDEN ZWEI JAHREN FU UND NFU IM VERGLEICH



Familienunternehmen halten ihre Investitionen entweder gleich, steigern diese stark oder senken diese sogar – eher extremere Reaktionen im Vergleich zu NFU

EINFLUSSFAKTOREN

Größe des Unternehmens: kein statistisch signifikanter Zusammenhang

Sitz des Unternehmens: kein statistisch signifikanter Zusammenhang

Familienunternehmen: kein statistisch signifikanter Zusammenhang

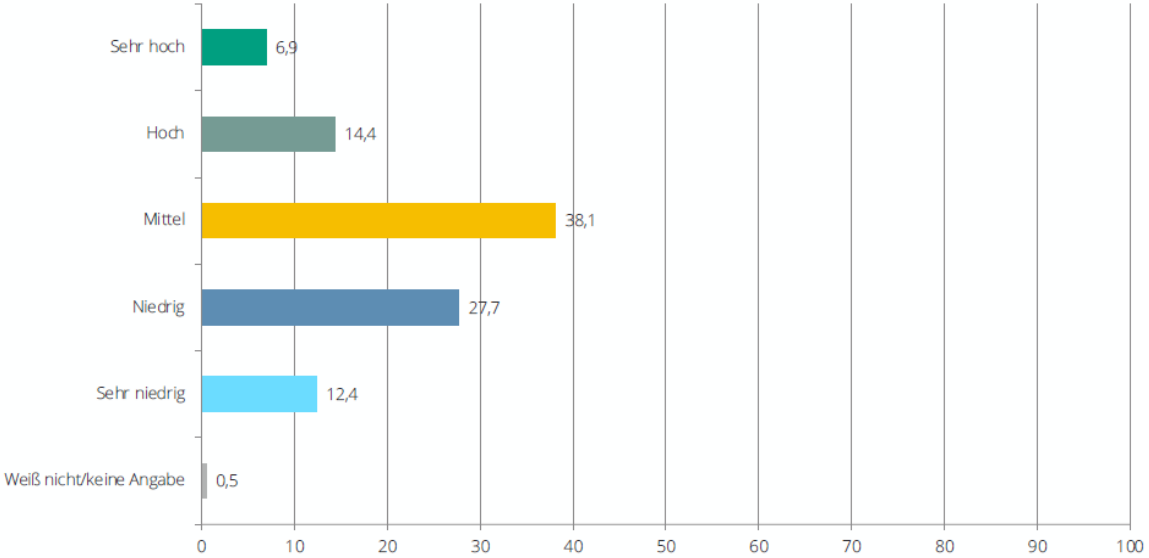
Alter des Familienunternehmens: kein statistisch signifikanter Zusammenhang

Verweildauer der GF im Familienunternehmen: starker & statistisch hochsignifikanter Zusammenhang (-0,256***), d.h. Familienunternehmen mit einem GF mit einer längeren Verweildauer planen **höhere Investitionen in die IT Security** im kommenden Jahr (2024) im Vergleich zum aktuellen Jahr (2023)

Zeit bis zum nächsten Generationswechsel: starker & statistisch hochsignifikanter Zusammenhang (0,245***), d.h. Familienunternehmen mit einer längeren Zeitspanne bis zum nächsten Generationswechsel planen **geringere Investitionen in die IT Security** im kommenden Jahr (2024) im Vergleich zum aktuellen Jahr (2023)

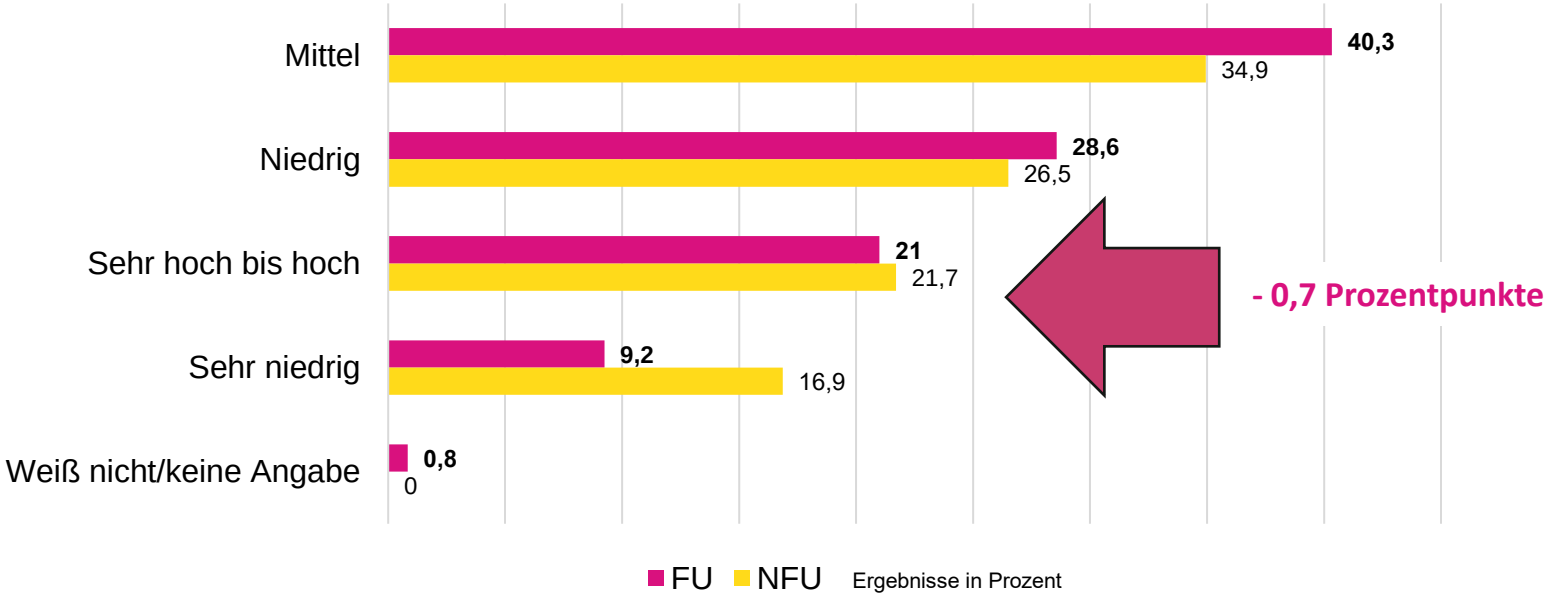
RISIKO FÜR CYBERKRIMINALITÄT ODER DATENKLAU

„Wie hoch schätzen Sie das Risiko ein, dass Sie in den nächsten 12 Monaten Opfer von Cyberkriminalität oder Datenklau werden (z.B. Identitätsdiebstahl, Diebstahl von Kreditkartendaten oder Unternehmensdaten, Internetbetrug, Cybererpressung, Cyberspionage)?“



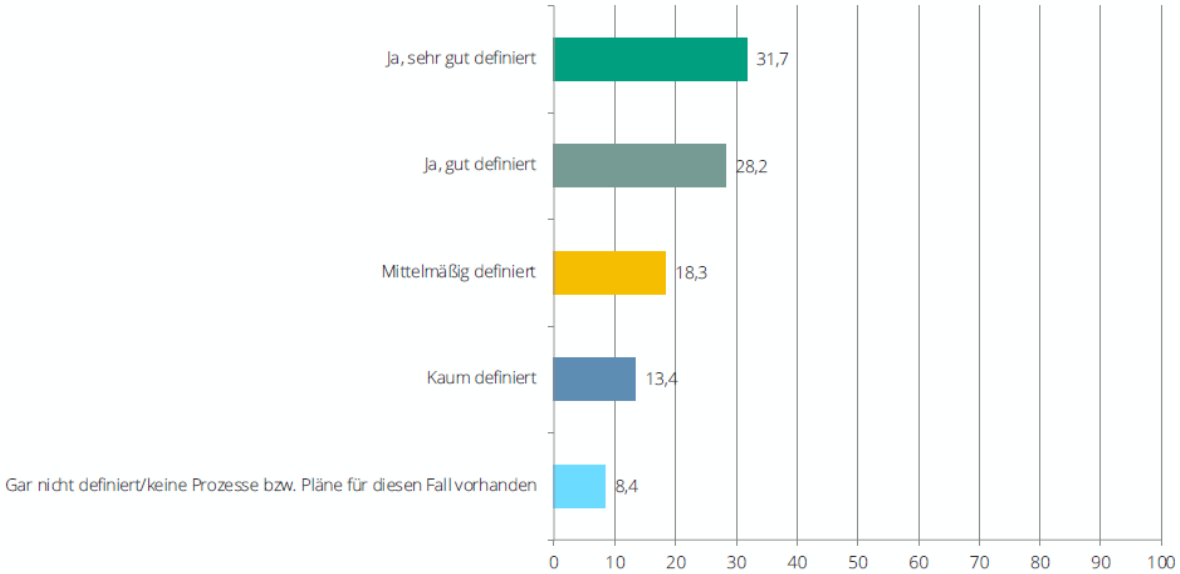
In %, Einfachantwort, n=202

WIE HOCH SCHÄTZEN SIE DAS RISIKO EIN, DASS SIE IN DEN NÄCHSTEN 12 MONATEN OPFER VON CYBERKRIMINALITÄT ODER DATENKLAU WERDEN?



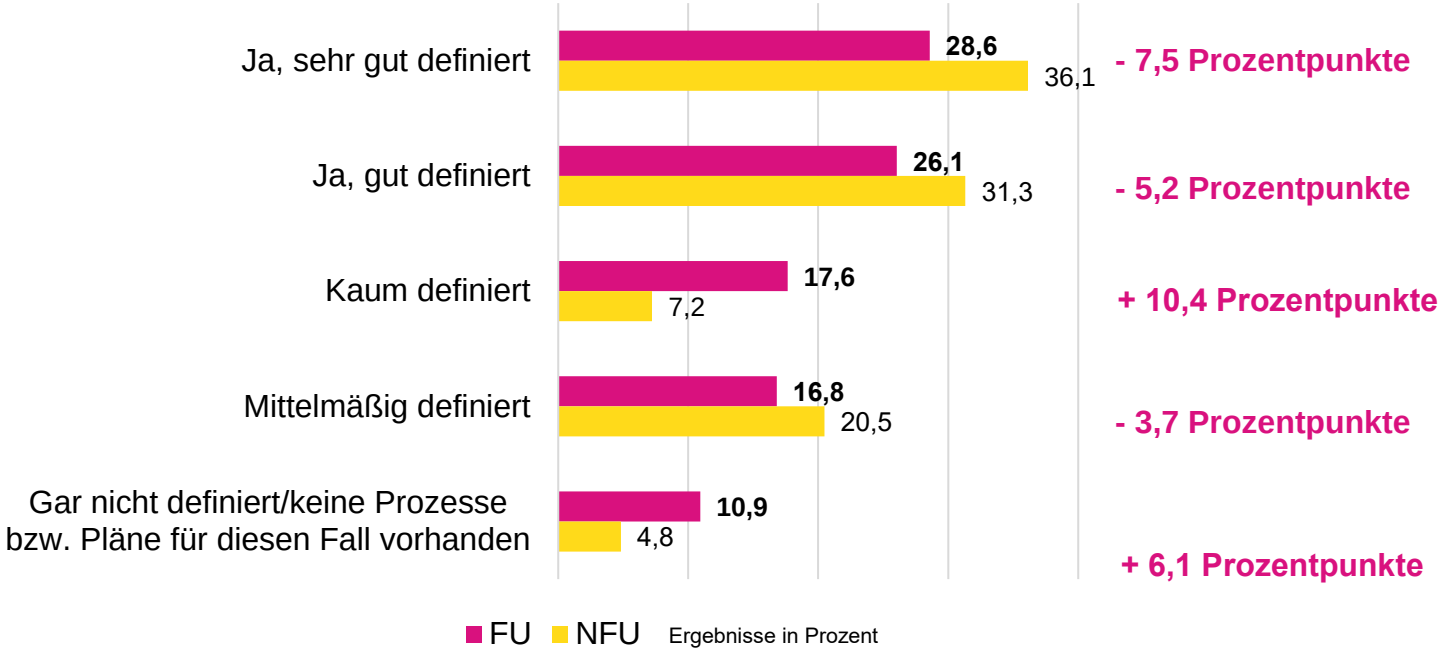
DEFINIERTE PROZESSE FÜR IT-SICHERHEITSVORFALL

„Sind in Ihrem Unternehmen Prozesse definiert, wie im Falle eines IT-Sicherheitsvorfalls vorzugehen ist?“



In %, Einfachantwort, n=202

DEFINIERTE PROZESSE FÜR IT-SICHERHEITSVORFALL: FU UND NFU IM VERGLEICH



EINFLUSSFAKTOREN

Größe des Unternehmens: moderater & statistisch signifikanter Zusammenhang (-0,147**), d.h. größere Unternehmen verfügen über **gut definierte Prozesse**, wie im Fall eines IT-Sicherheitsvorfalls vorzugehen ist

Sitz des Unternehmens: starker & statistisch hochsignifikanter Zusammenhang (0,210***), d.h. Unternehmen mit einem Sitz in einer Großstadt verfügen über **gut definierte Prozesse**, wie im Fall eines IT-Sicherheitsvorfalls vorzugehen ist

Familienunternehmen: moderater & statistisch signifikanter Zusammenhang (-0,165**), d.h. Familienunternehmen verfügen über **kaum definierte oder gar keine Prozesse**, wie im Fall eines IT-Sicherheitsvorfalls vorzugehen ist

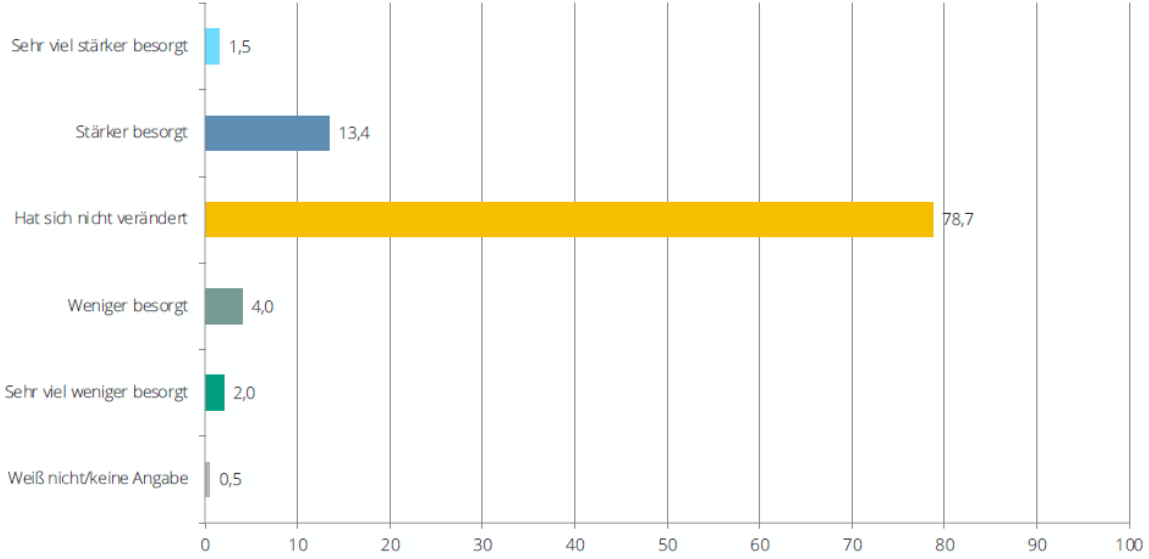
Alter des Familienunternehmens: moderater & statistisch signifikanter Zusammenhang (0,167**), d.h. ältere Familienunternehmen verfügen über **gut definierte Prozesse**, wie im Fall eines IT-Sicherheitsvorfalls vorzugehen ist

Verweildauer der GF im Familienunternehmen: kein statistisch signifikanter Zusammenhang

Zeit bis zum nächsten Generationswechsel: kein statistisch signifikanter Zusammenhang

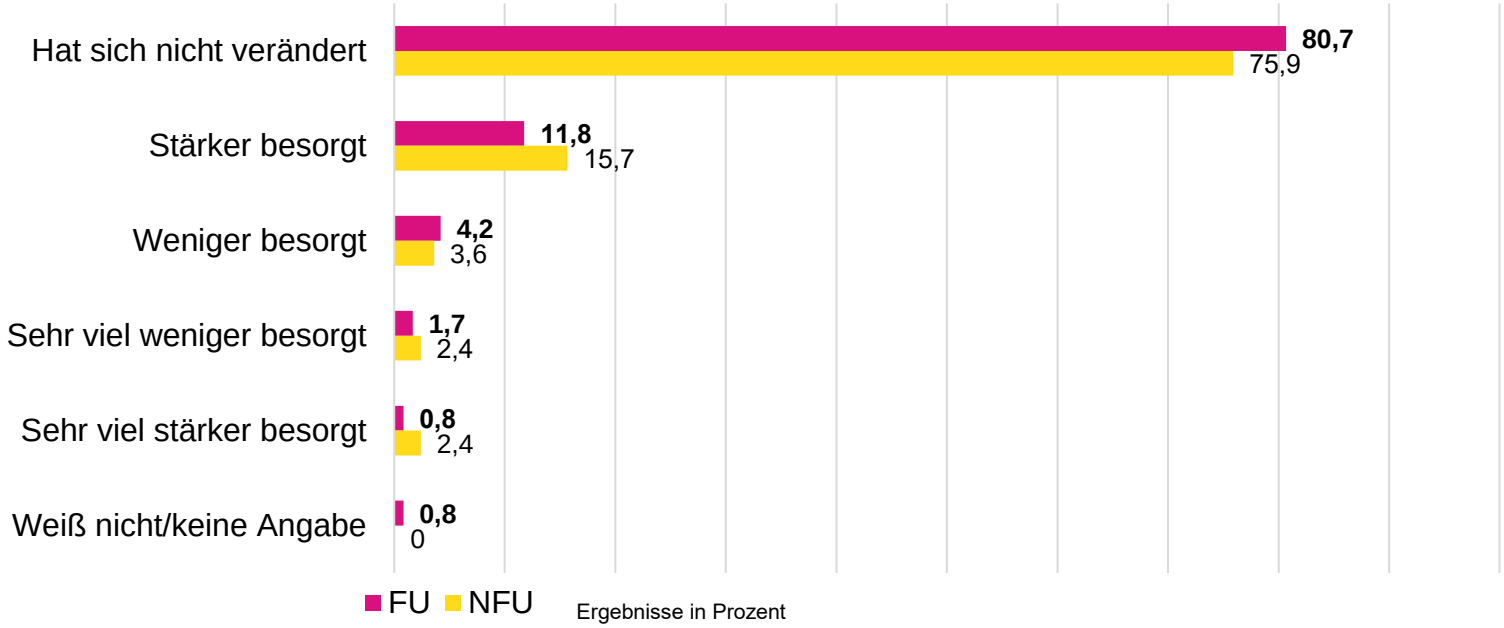
AKTUELLE WAHRNEHMUNG DER IT-SICHERHEIT

„Derzeit herrscht Krieg in der Ukraine. Wie hat sich Ihre Wahrnehmung bezüglich IT-Sicherheit seit dieser Zeit verändert? Ich bin aktuell in Bezug auf die IT-Sicherheit..."



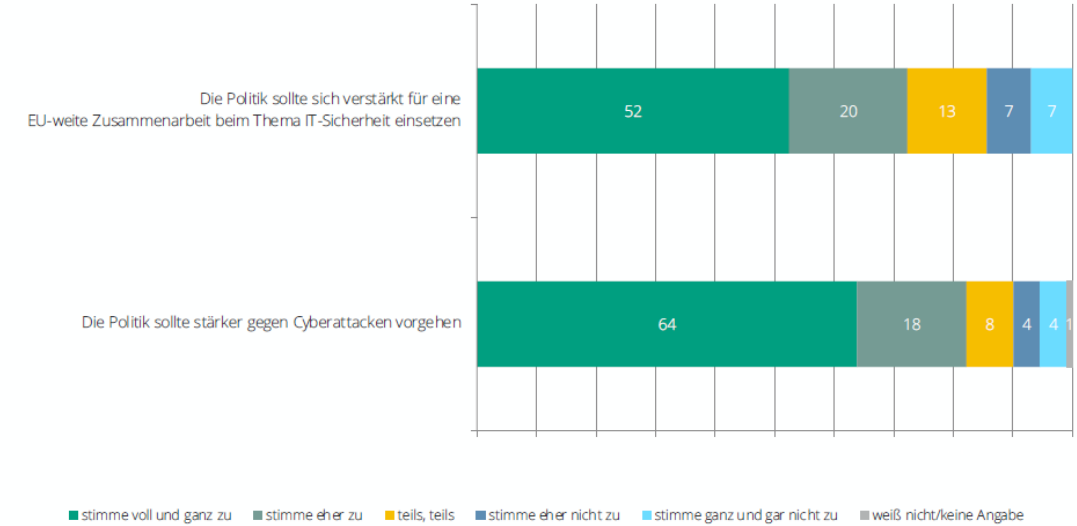
In %, Einfachantwort, n=202

DERZEIT HERRSCHT KRIEG IN DER UKRAINE. WIE HAT SICH IHRE WAHRNEHMUNG BEZÜGLICH IT-SICHERHEIT SEIT DIESER ZEIT VER-ÄNDERT? ICH BIN AKTUELL IN BEZUG AUF DIE IT-SICHERHEIT ...



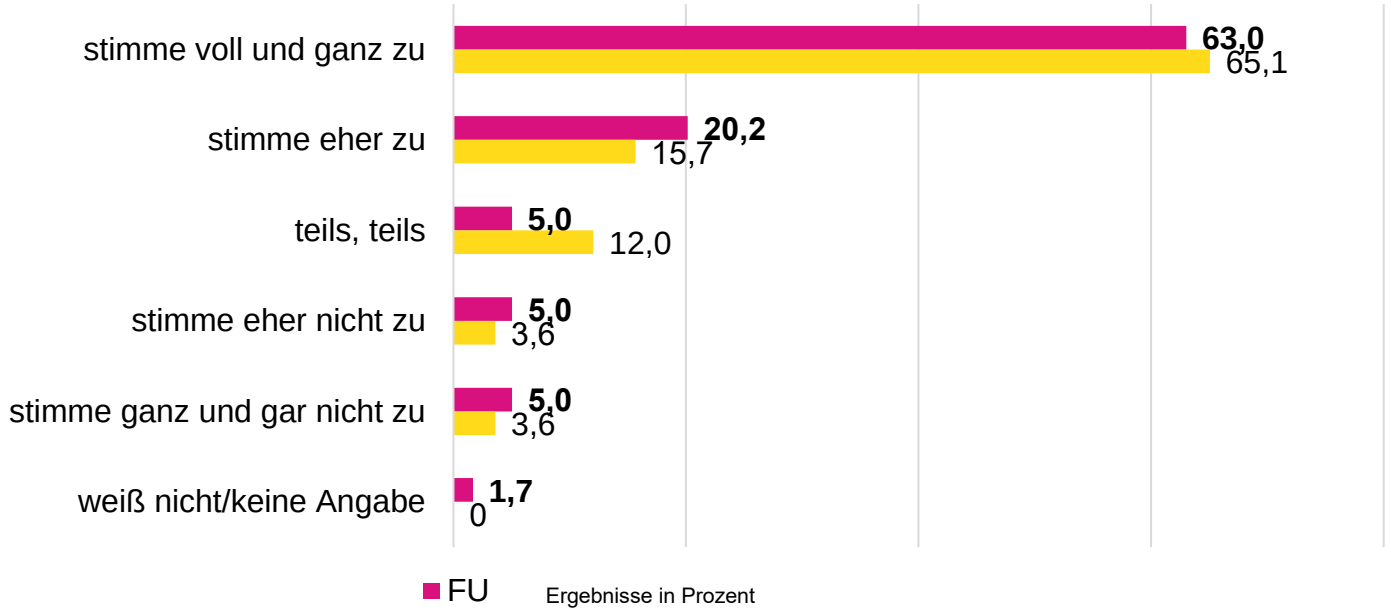
EINFLUSS DER POLITIK AUF DIE IT-SICHERHEIT

„Wie sehr stimmen Sie den folgenden Aussagen zu."

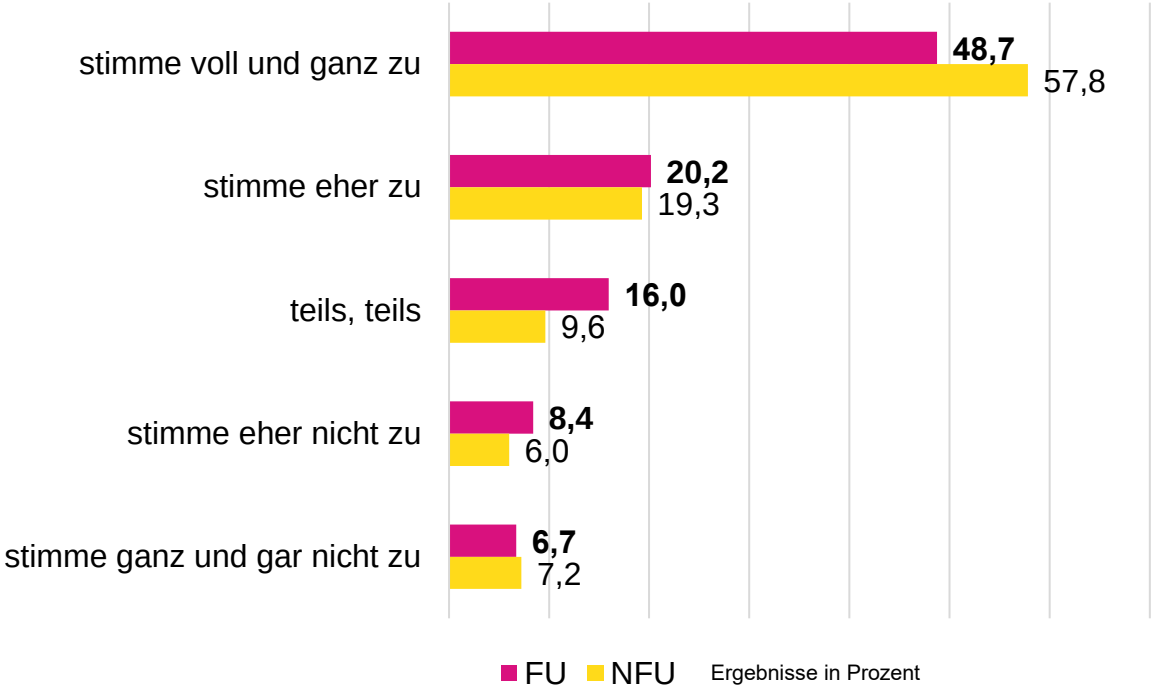


In %, Einfachantwort, n=202

WIE SEHR STIMMEN SIE DEN FOLGENDEN AUSSAGEN ZU: DIE POLITIK SOLLTE STÄRKER GEGEN CYBERATTACKEN VORGEHEN.

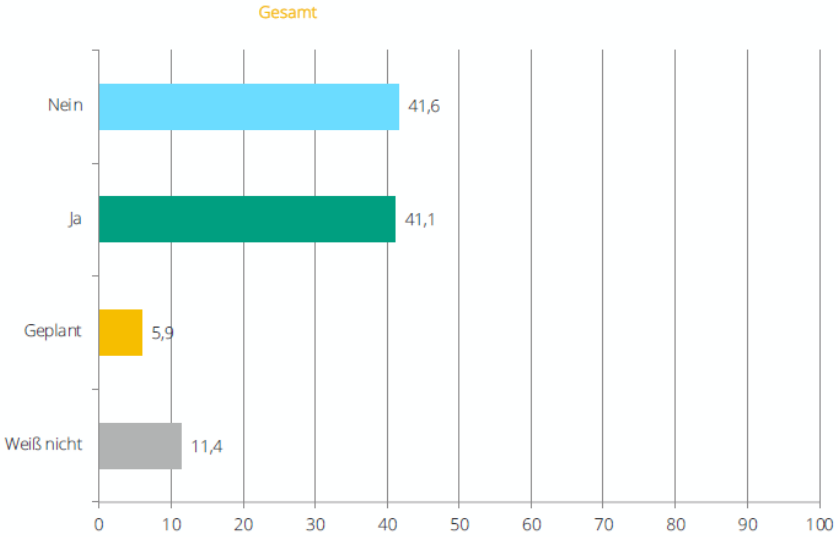


WIE SEHR STIMMEN SIE DEN FOLGENDEN AUSSAGEN ZU: DIE POLITIK SOLLTE SICH VERSTÄRKT FÜR EINE EU-WEITE ZUSAMMENARBEIT BEIM THEMA IT-SICHERHEIT EINSETZEN.



ABDECKUNG VON POTENTIELLEN SCHÄDEN DURCH CYBER-VERSICHERUNG

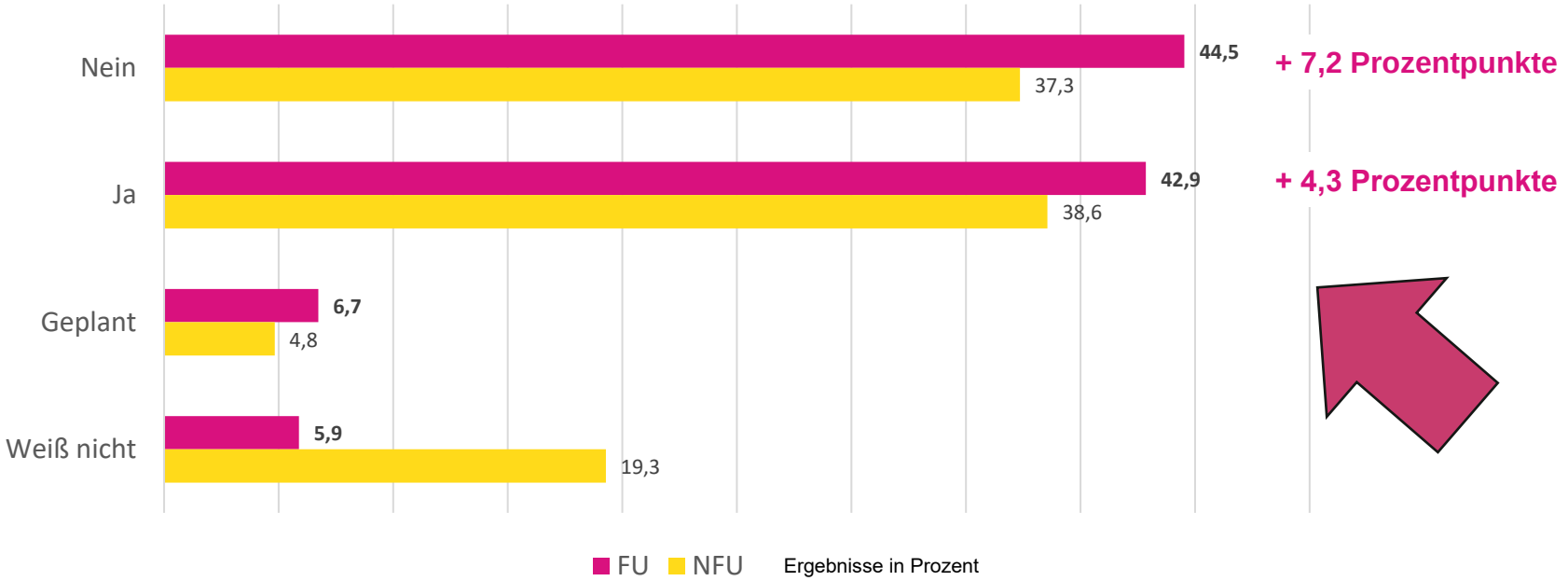
„Sind in Ihrem Unternehmen potentielle Schäden einer Cyberattacke durch eine Cyber-Versicherung abgedeckt (wie Kosten für Wiederherstellung der Systeme, Kosten von Lösegeldforderungen und Kosten für Schäden, die Dritten entstanden sind)?“



Familienunternehmen	
Ja	Nein
42,9	38,6
44,5	37,3
6,7	4,8
5,9	19,3

In %, Einfachantwort, n=202, n(Familienunternehmen)=119, n(Kein Familienunternehmen)= 83

ABDECKUNG POTENTIELLER SCHÄDEN DURCH CYBER-VERSICHERUNG FU UND NFU IM VERGLEICH



ÜBERBLICK:

ZENTRALE UNTERNEHMENS-MERKMALE UND IHR EINFLUSS AUF DIE WAHRNEHMUNG DES THEMAS IT-SICHERHEIT

UNTERNEHMENSGRÖßE

Veränderung der Wichtig von IT Security im Unternehmen	Gab es IT-Security Vorfälle in den letzten zwei Jahren	Qualität der definierten Prozesse
Größere Unternehmen nehmen das Thema IT Security in den letzten beiden Jahren als zunehmend wichtiger wahr	Je größer das Unternehmen desto eher gab es einen IT Security Vorfall in den letzten beiden Jahren	Größere Unternehmen verfügen über gut definierte Prozesse, wie im Fall eines IT-Sicherheitsvorfalls vorzugehen ist

Starker Zusammenhang | Ausgeprägter Zusammenhang | Moderater Zusammenhang

SITZ DES UNTERNEHMENS

Einschätzung der Bedrohungslage	Stellenwert und Wichtig von IT Security im Unternehmen	Veränderung der Sicherheitsrisiken in den nächsten zwei Jahren	Kompetenz und Know-how zum Thema IT-Sicherheit	Qualität der definierten Prozesse
Je städtischer der Sitz des Unternehmens, desto häufiger werden Angriffe wahrgenommen (ländlicher Raum wiegt sich in Sicherheit)	Je städtischer der Sitz des Unternehmens, desto wichtiger wird das Thema IT Security wahrgenommen (ländlicher Raum misst IT Security einen geringeren Stellenwert bei)	Unternehmen mit einem Sitz im ländlichen Raum sehen eine stärkere Zunahme der Risiken im Bereich der IT Security in den nächsten zwei Jahren	Unternehmen mit einem Sitz im ländlichen Raum schätzen ihre Kompetenz und ihr Know-how in Bezug auf IT-Security als geringer ein	Unternehmen mit einem Sitz in einer Großstadt verfügen über gut definierte Prozesse, wie im Fall eines IT-Sicherheitsvorfalls vorzugehen ist

Starker Zusammenhang | Ausgeprägter Zusammenhang | Moderater Zusammenhang

FAMILIENUNTERNEHMEN

Einschätzung der Bedrohungslage	Stellenwert und Wichtig von IT Security im Unternehmen	Einschätzung des bestehenden Schutzes	Hemmnisse bei der Verbesserung der IT Security im Unternehmen	Qualität der definierten Prozesse
Familienunternehmen nehmen seltener Angriffe wahr	Familienunternehmen nehmen das Thema IT Security als weniger wichtig wahr	Familienunternehmen fühlen sich weniger gut vor internen/externen Angriffen und Datenverlust geschützt	Familienunternehmen sehen öfter keine Hemmnisse bei der Verbesserung der IT Security	Familienunternehmen verfügen über kaum definierte oder gar keine Prozesse, wie im Fall eines IT-Sicherheits-vorfalls vorzugehen ist

Starker Zusammenhang | Ausgeprägter Zusammenhang | Moderater Zusammenhang

ALTER DES FAMILIENUNTERNEHMENS

Einschätzung der Bedrohungs-lage	Stellenwert und Wichtig von IT Security im Unternehmen	Einschätzung des bestehenden Schutzes	Hemmnisse bei der Verbesserung der IT Security im Unternehmen	Ordnungs-gemäße Datensicherung im Unternehmen	Qualität der definierten Prozesse
Je älter des Familien-unternehmen, desto häufiger werden Angriffe wahrgenommen	Je älter des Familien-unternehmen, desto wichtiger wird das Thema IT Security wahrgenommen	Ältere Familien-unternehmen fühlen sich weit besser vor internen/ externen Angriffen und Datenverlust geschützt	Ältere Familien-unternehmen sehen öfter Hemmnisse bei der Verbesserung der IT Security	Ältere Familien-unternehmen sind sich weniger sicher, dass alle wichtigen Daten im Unter-nehmen ordnungs-gemäß gesichert und im Ernstfall wiede-hergestellt werden können	Ältere Familien-unternehmen verfügen über gut definierte Prozesse, wie im Fall eines IT-Sicherheits-vorfalls vorzugehen ist

Starker Zusammenhang

Ausgeprägter Zusammenhang

Moderater Zusammenhang

VERWEILDAUER DER GF IM FAMILIENUNTERNEHMEN

Einschätzung der Bedrohungslage	IT-Security Vorfälle in den letzten zwei Jahren	Veränderung der Sicherheitsrisiken in den nächsten zwei Jahren	Ordnungsgemäße Datensicherung im Unternehmen	Investitionen in IT-Sicherheit in den nächsten zwei Jahren
Je länger die GF bereits im Unternehmen ist, desto häufiger werden Angriffe wahrgenommen	Je länger die Verweildauer der GF desto eher gab es keinen bzw. keinen registrierten IT Security Vorfall in den letzten beiden Jahren	Familienunternehmen mit einer längeren Verweildauer der GF sehen eine stärkere Zunahme der Risiken im Bereich der IT Security in den nächsten zwei Jahren	Familienunternehmen mit einer längeren Verweildauer der GF sind sich weniger sicher, dass alle wichtigen Daten im Unternehmen ordnungsgemäß gesichert und im Ernstfall wiederhergestellt werden können	Familienunternehmen mit mit einer längeren Verweildauer der GF planen höhere Investitionen in die IT Security im kommenden Jahr (2024) im Vergleich zum aktuellen Jahr (2023)

Starker Zusammenhang | Ausgeprägter Zusammenhang | Moderater Zusammenhang

ZEIT BIS ZUM NÄCHSTEN GENERATIONENWECHSEL

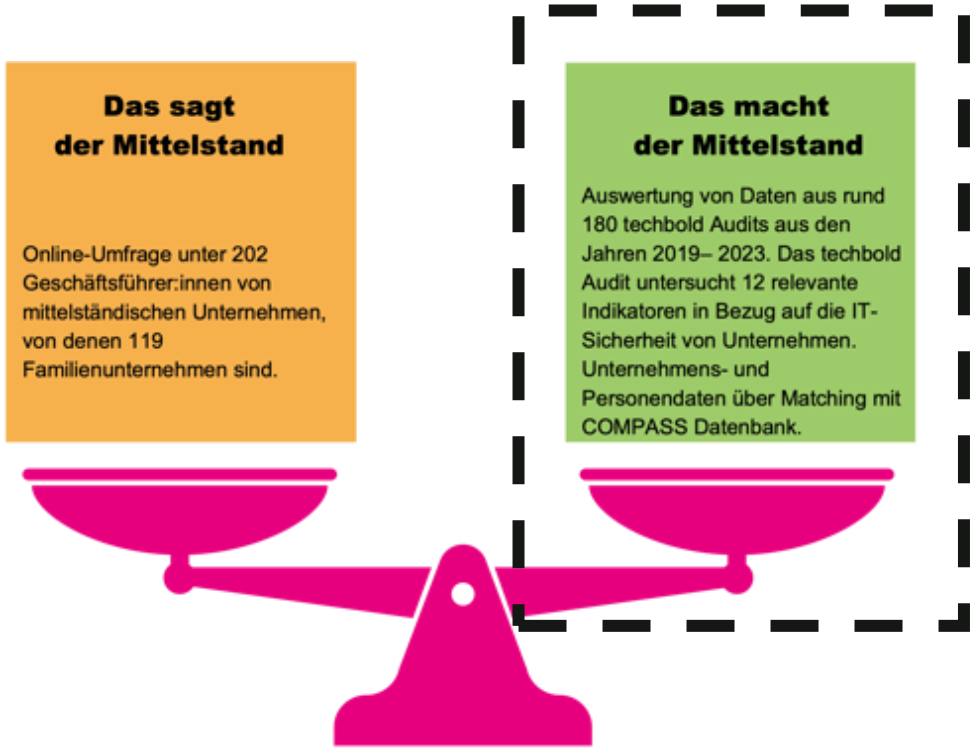
Einschätzung der Bedrohungslage	Veränderung der Sicherheitsrisiken in den nächsten zwei Jahren	Investitionen in IT-Sicherheit in den nächsten zwei Jahren
Je länger es bis zum nächsten Generationswechsel dauert, desto seltener werden Angriffe wahrgenommen	Familienunternehmen mit einer längeren Zeitspanne bis zum nächsten Generationswechsel sehen eine geringere Zunahme der Risiken im Bereich der IT Security in den nächsten zwei Jahren	Familienunternehmen mit einer längeren Zeitspanne bis zum nächsten Generationswechsel planen geringere Investitionen in die IT Security im kommenden Jahr (2024) im Vergleich zum aktuellen Jahr (2023)

(Im Umkehrschluss: je näher der Generationswechsel, desto stärker ist das Thema IT-Security auf dem Radar)

Starker Zusammenhang

TECHBOLD
REALITY CHECK

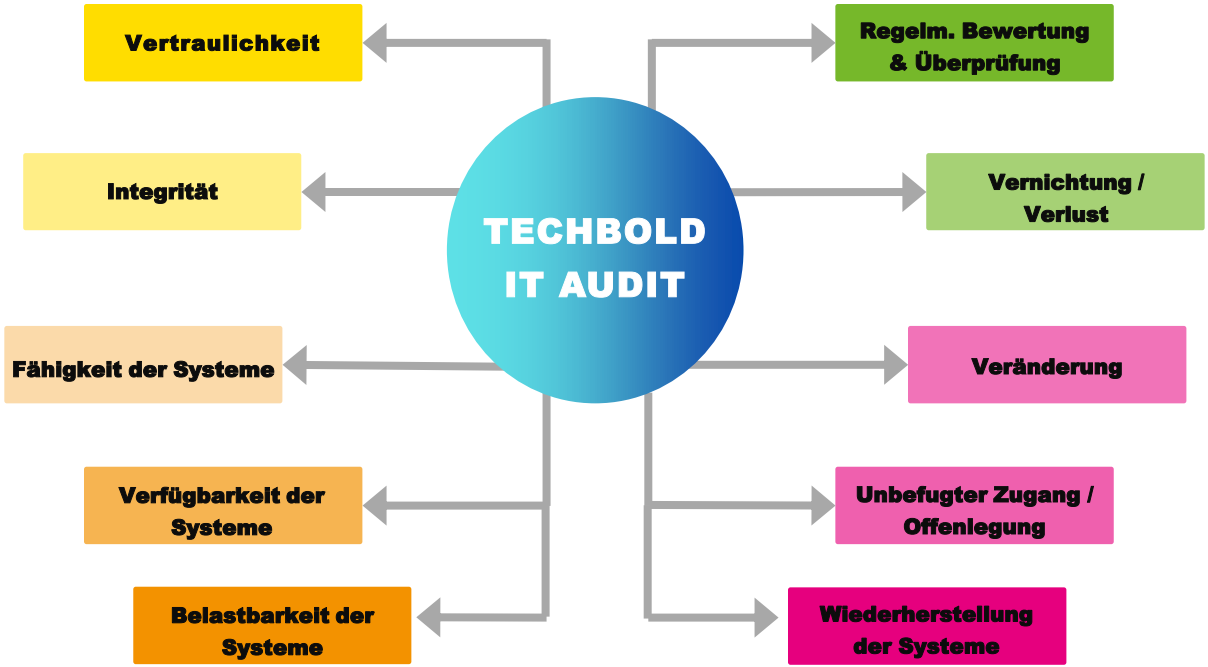
DETAIL-AUSWERTUNG IT-AUDITS



WAS IST DAS TECHBOLD IT AUDIT?

Das techbold IT-Audit ist eine unabhängige und umfassende IT-Analyse, die ein umfassendes Bild des Status Quo der IT-Sicherheit im Unternehmen ermittelt. Dabei werden alle Schwachstellen in den IT-Systemen aufgedeckt, bevor es zu Problemen und Datenverlusten kommt. Darüber hinaus dient das IT-Audit auch zum Nachweis der Sorgfaltspflicht für Geschäftsführer und IT-Verantwortliche laut DSGVO Art. 32

ELEMENTE DES TECHBOLD IT-AUDITS



Vertraulichkeit

Zustand der Firewall, Usermanagement, Alter der Passworte und Passwortrichtlinien, Absperrung Serverraum, Protokollierung der Zutritte zum Serverraum, Bildschirmschoner mit Passwortschutz, Sicherheit im WLAN, Antivirus, Antispam, laufende Sicherheitsupdates, laufende Berechtigungskontrolle

Integrität

Zustand der Firewall, Usermanagement, Alter und Qualität der Serverhardware, RAID-System im Server, Redundanz bei Speichermedien, Redundanz in der Stromversorgung, Redundanz in der Datenanbindung, Alter der Passworte und Passwortrichtlinien, Antivirus, Antispam, Backup, E-Mail-Archivierung

Fähigkeit der Systeme

Qualität der Firewall, Alter und Leistung der Serverhardware, Konzept der Benutzerverwaltung, Berechtigungen, Alter der Betriebssysteme, freie Kapazitäten, Antivirus, Antispam

Verfügbarkeit der Systeme

Qualität der Firewall, Alter und Leistung der Serverhardware, Konzept der Benutzerverwaltung, Berechtigungen, Alter der Betriebssysteme, freie Kapazitäten, Antivirus, Antispam

Belastbarkeit der Systeme

Zustand der Firewall, Alter und Leistung der Serverhardware, Redundanzen in den Systemen, verfügbare Systemreserven, Aktualität der Sicherheitsupdates auf den Servern und der Firewall

Wiederherstellbarkeit der Systeme

Alter und Qualität der Server und Firewalls, Backup-Konzept, Cloud Backup, Protokollierung der täglichen Backups, benötigte Zeit für Datenwiederherstellung

Unbefugter Zugang oder Offenlegung

Qualität des Servers und der Firewalls, Zutritt zum Serverraum, Passwortschutz, Benutzerberechtigungen, Anschluss externer Datenträger, Firewallkonzept, SSL-Zertifikat, Verschlüsselung der mobilen Geräte, Sicherheit des WLANs

Veränderung

Qualität der Firewalls, Benutzerberechtigungen, Passwortschutz, Verschlüsselung der mobilen Geräte, VPN, Monitoring der Zugriffe auf Dateien und Ordner

Vernichtung und Verlust

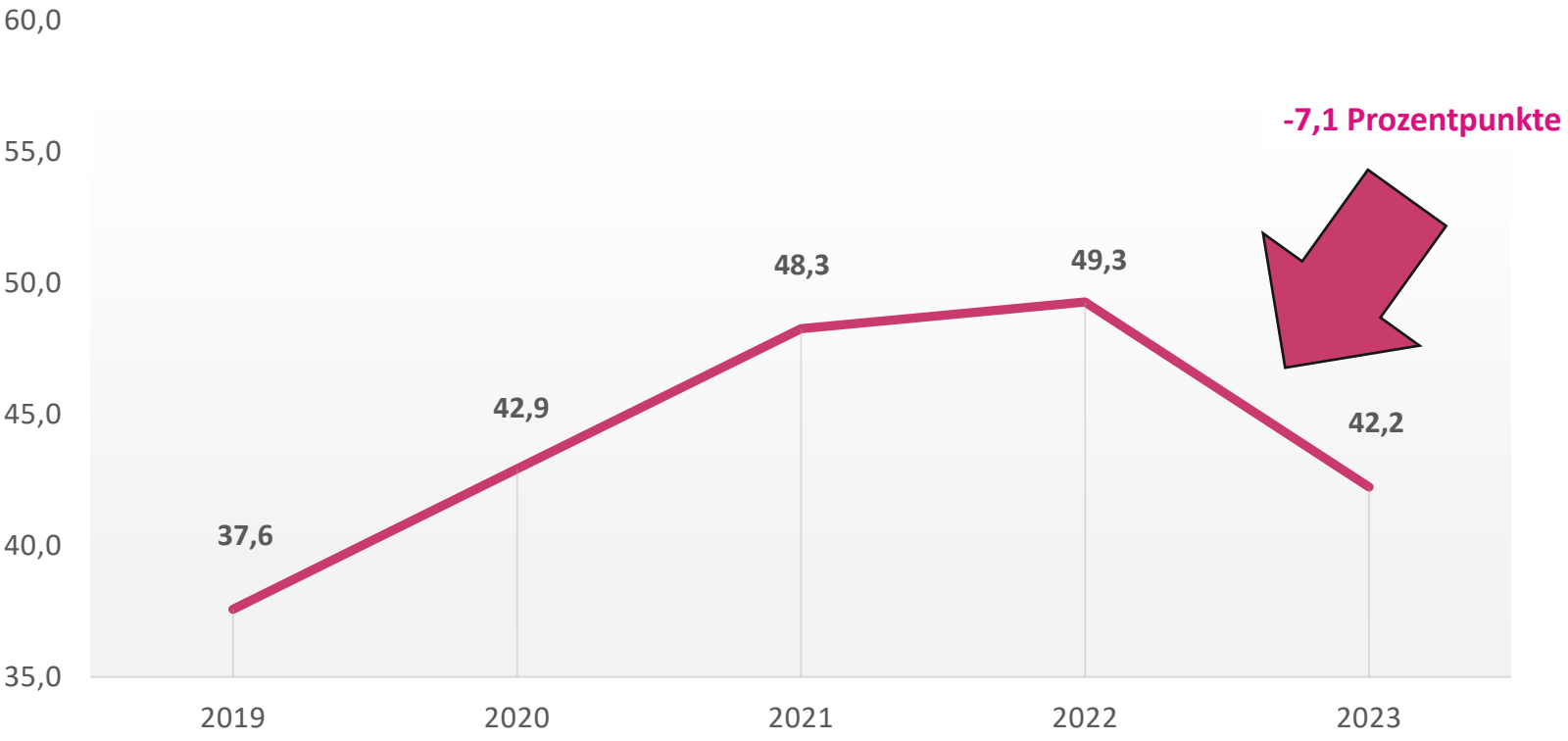
Zutritt zum Serverraum, Benutzerberechtigungen, Passwortschutz, laufende Kontrolle der Passworte und Accounts, Verschlüsselung der mobilen Geräte, redundandte Festplatten in den Server-Systemen, Backup-Konzept

Regelmäßige Bewertung und Überprüfung

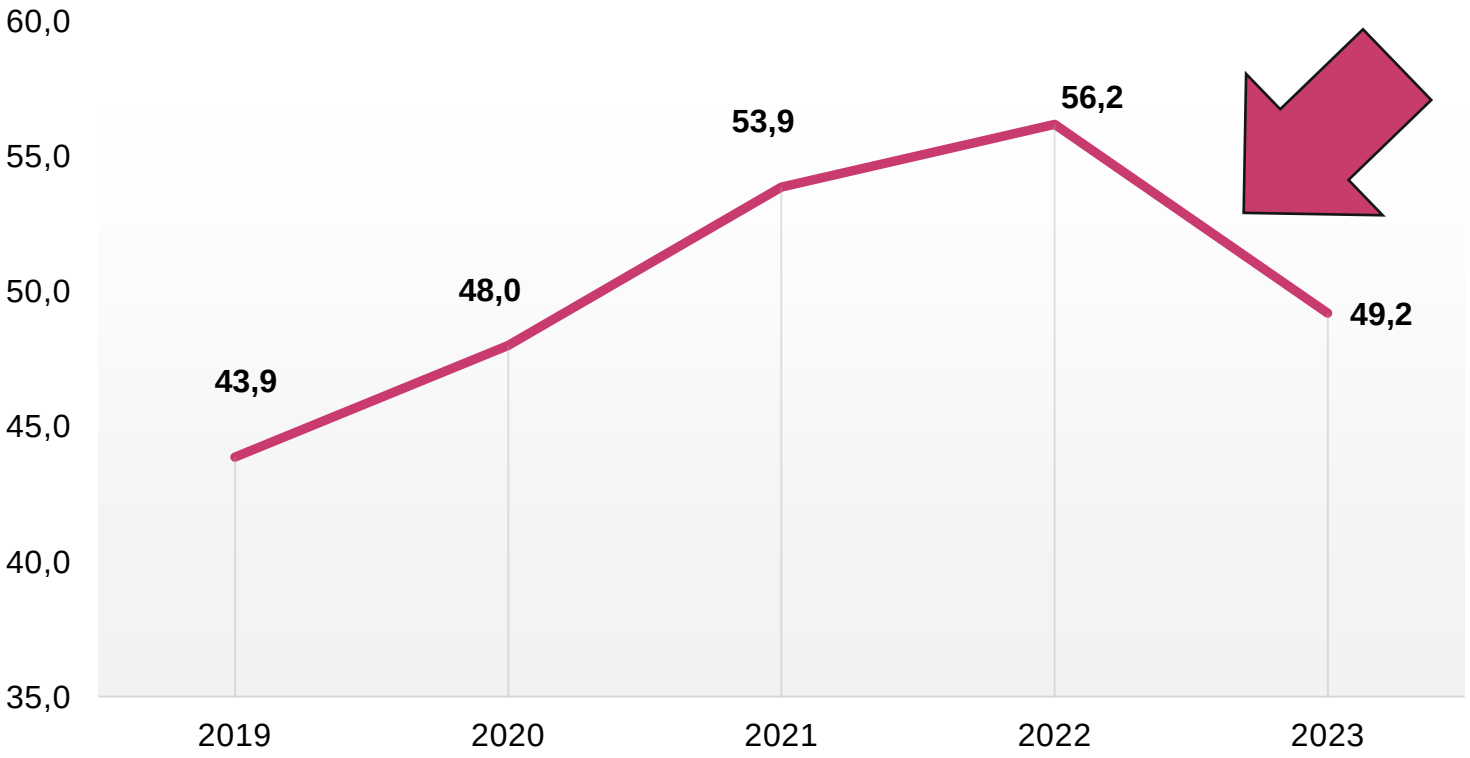
Laufendes Monitoring, laufende Kontrolle und Installation der Updates, laufende Kontrolle der Berechtigungen und aktiven User-Accounts, laufende Kontrolle der Passworte und Accounts, laufende Anpassung der Backup-Konzepte, Überwachung der Ressourcen

ANALYSE AUDITS IM DETAIL

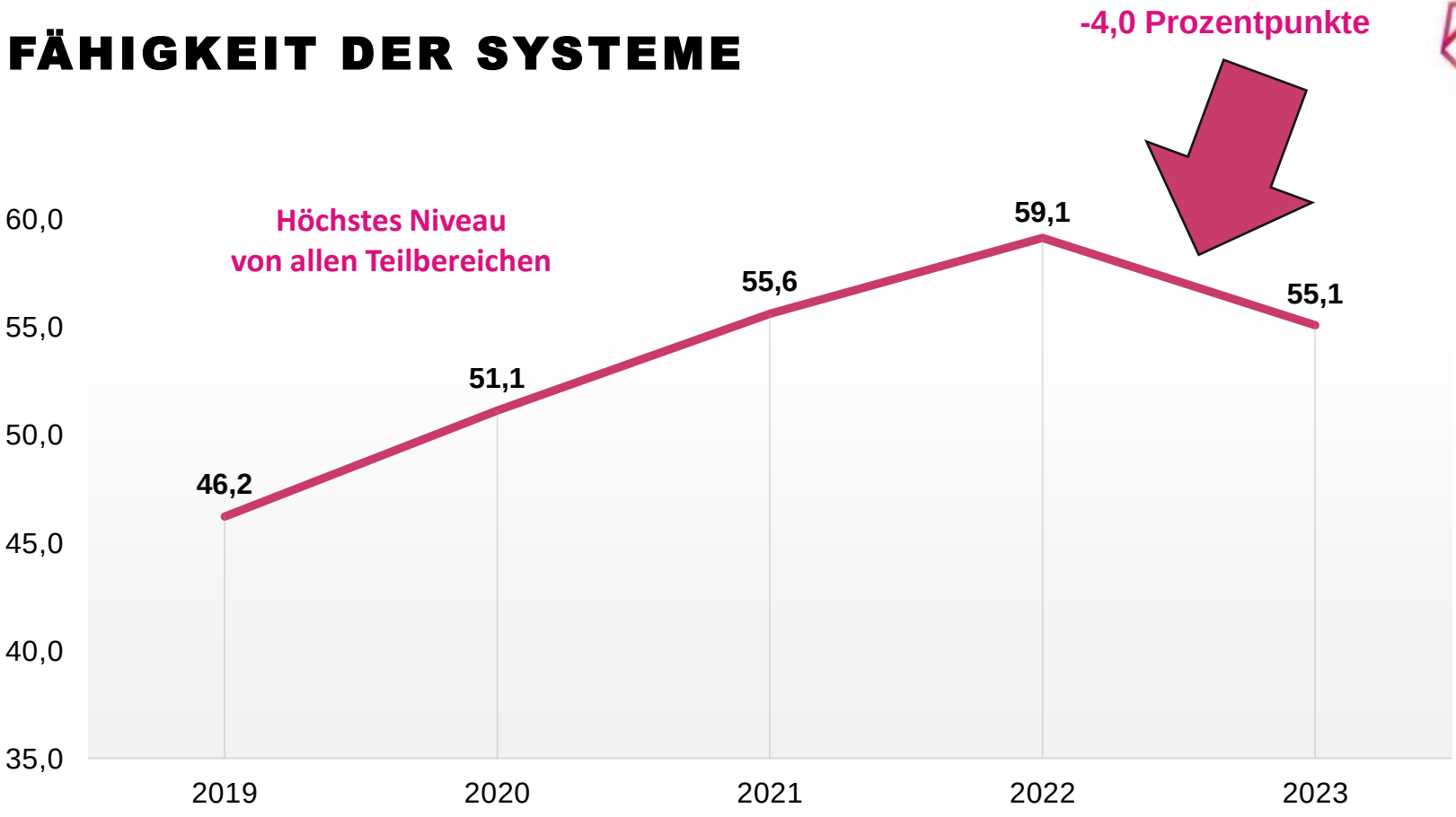
VERTRAULICHKEIT



INTEGRITÄT

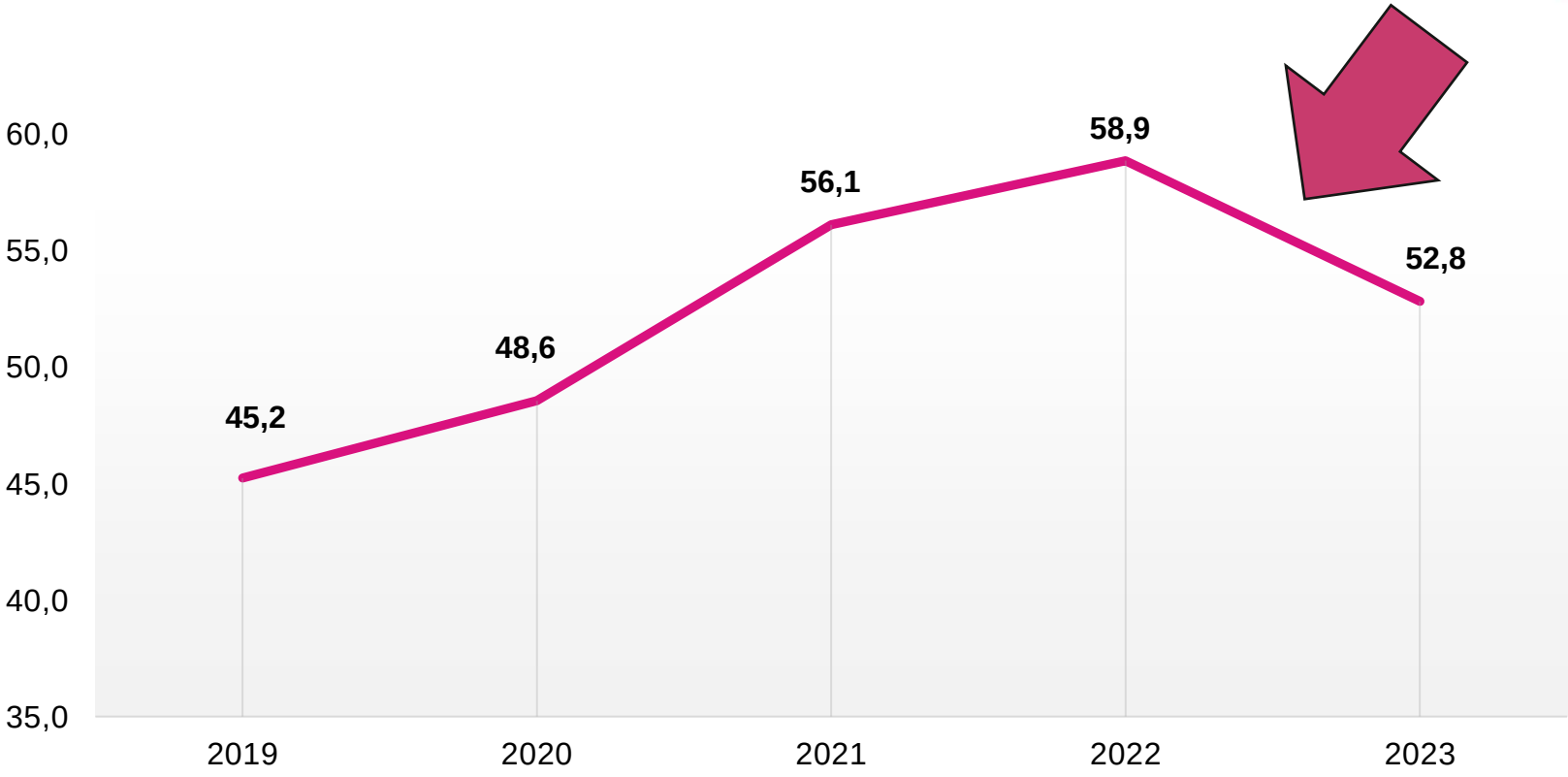


FÄHIGKEIT DER SYSTEME



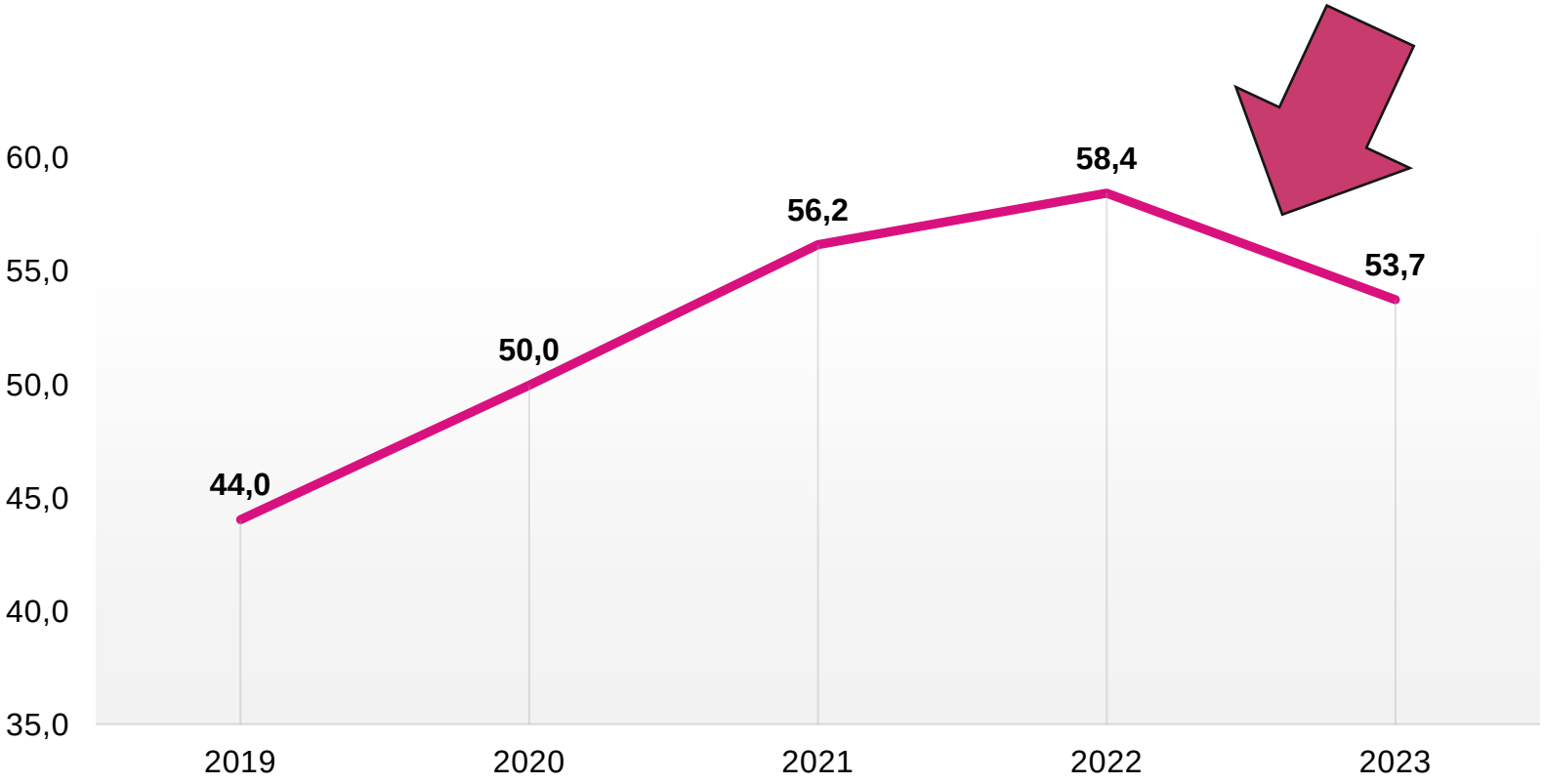
VERFÜGBARKEIT DER SYSTEME

-6,1 Prozentpunkte

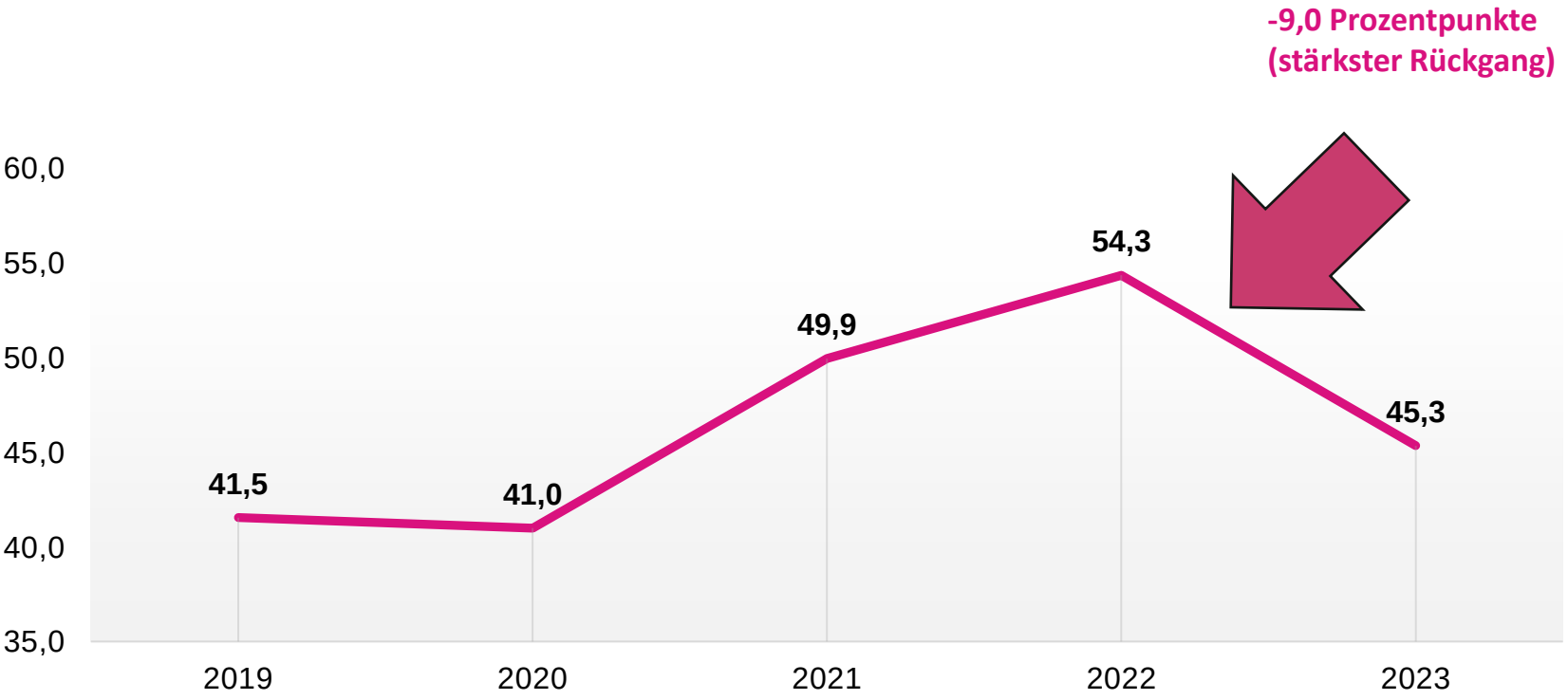


BELASTBARKEIT DER SYSTEME

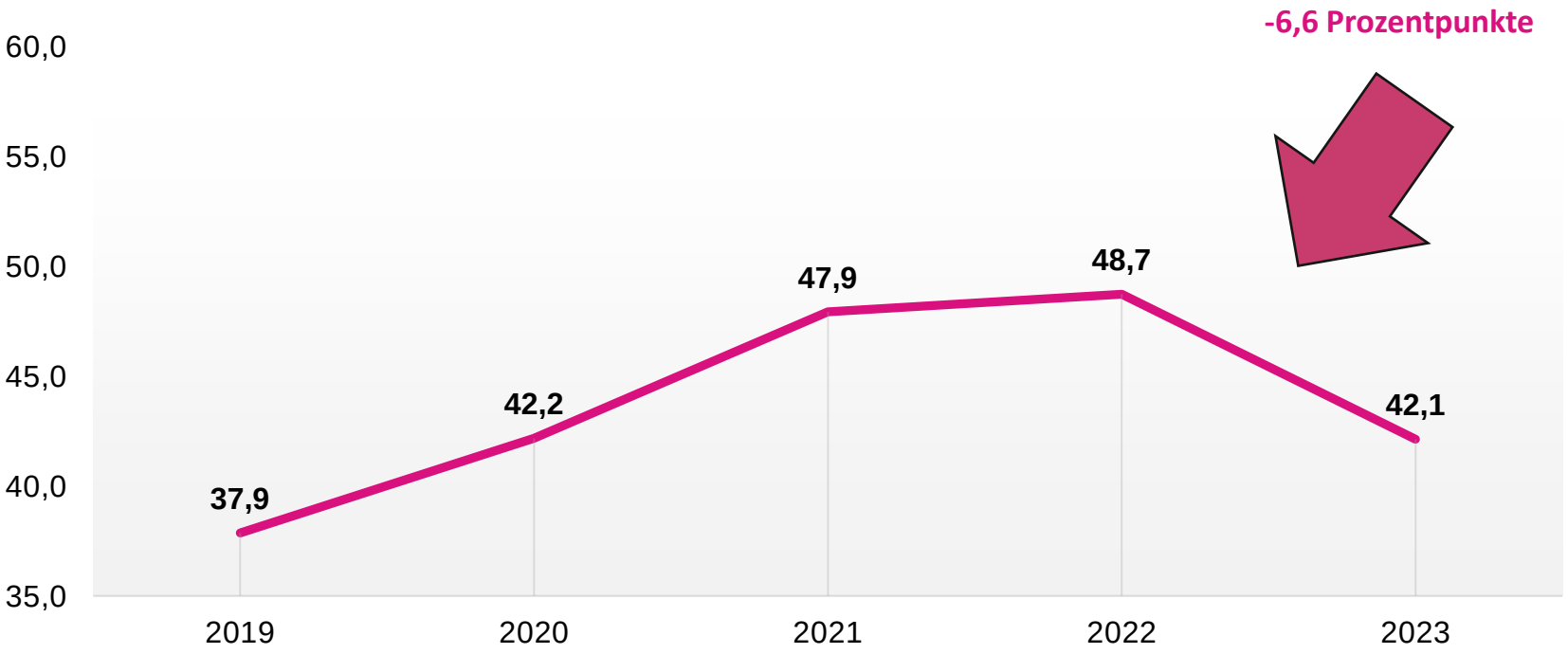
-4,7 Prozentpunkte



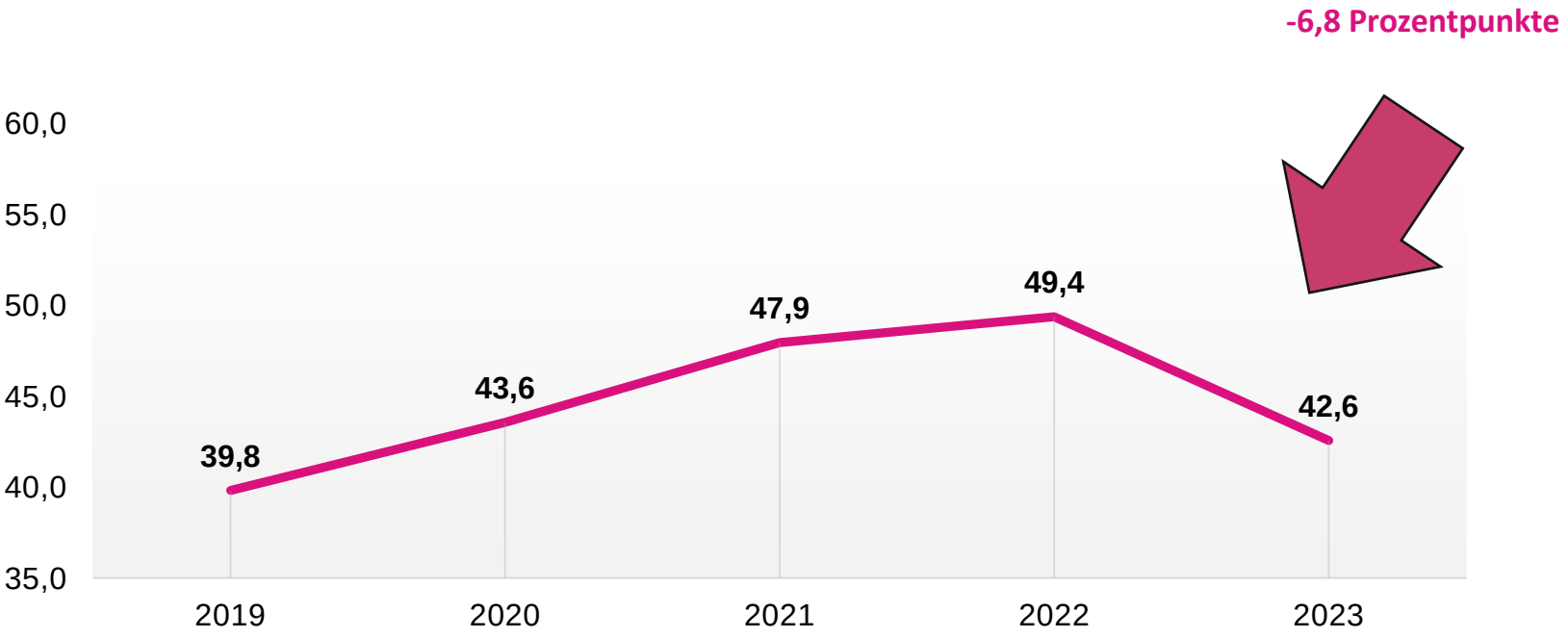
WIEDERHERSTELLBARKEIT



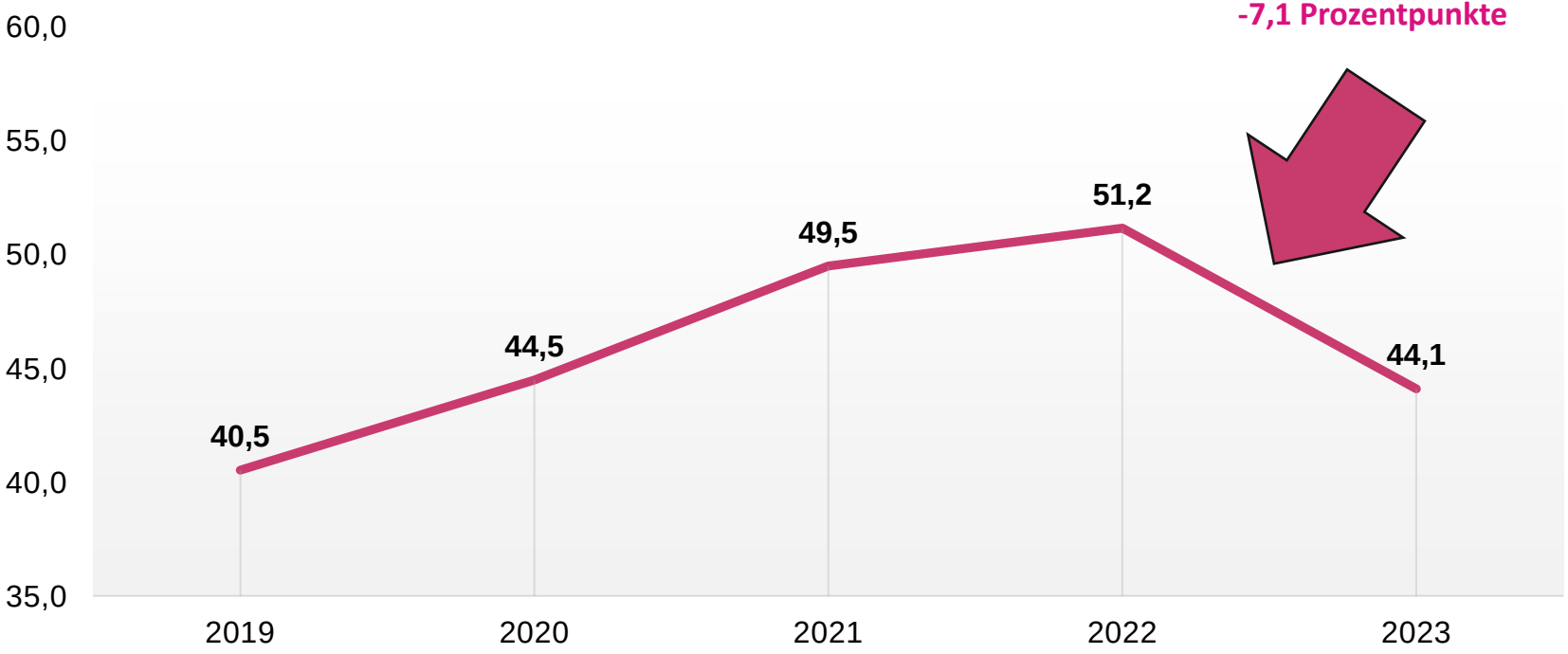
UNBEFUGTER ZUGANG



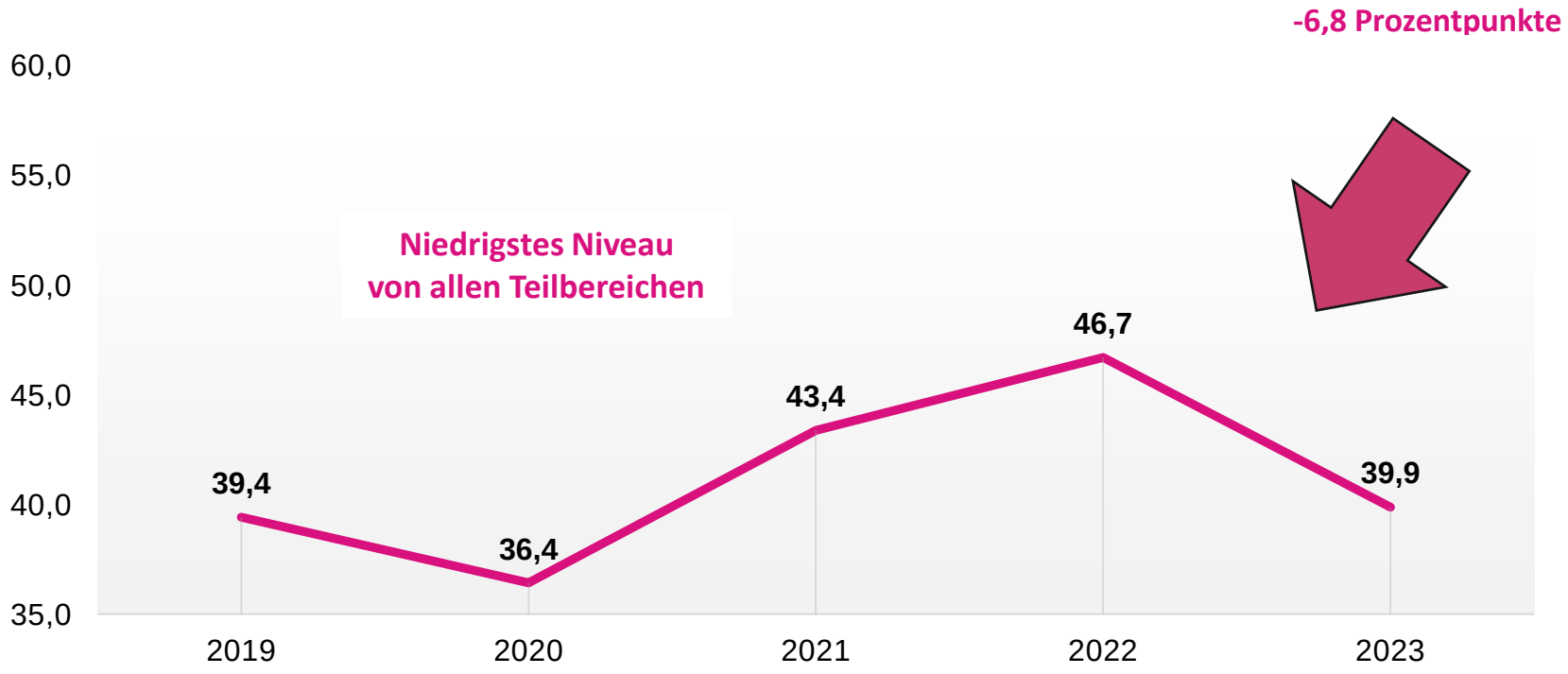
VERÄNDERUNG



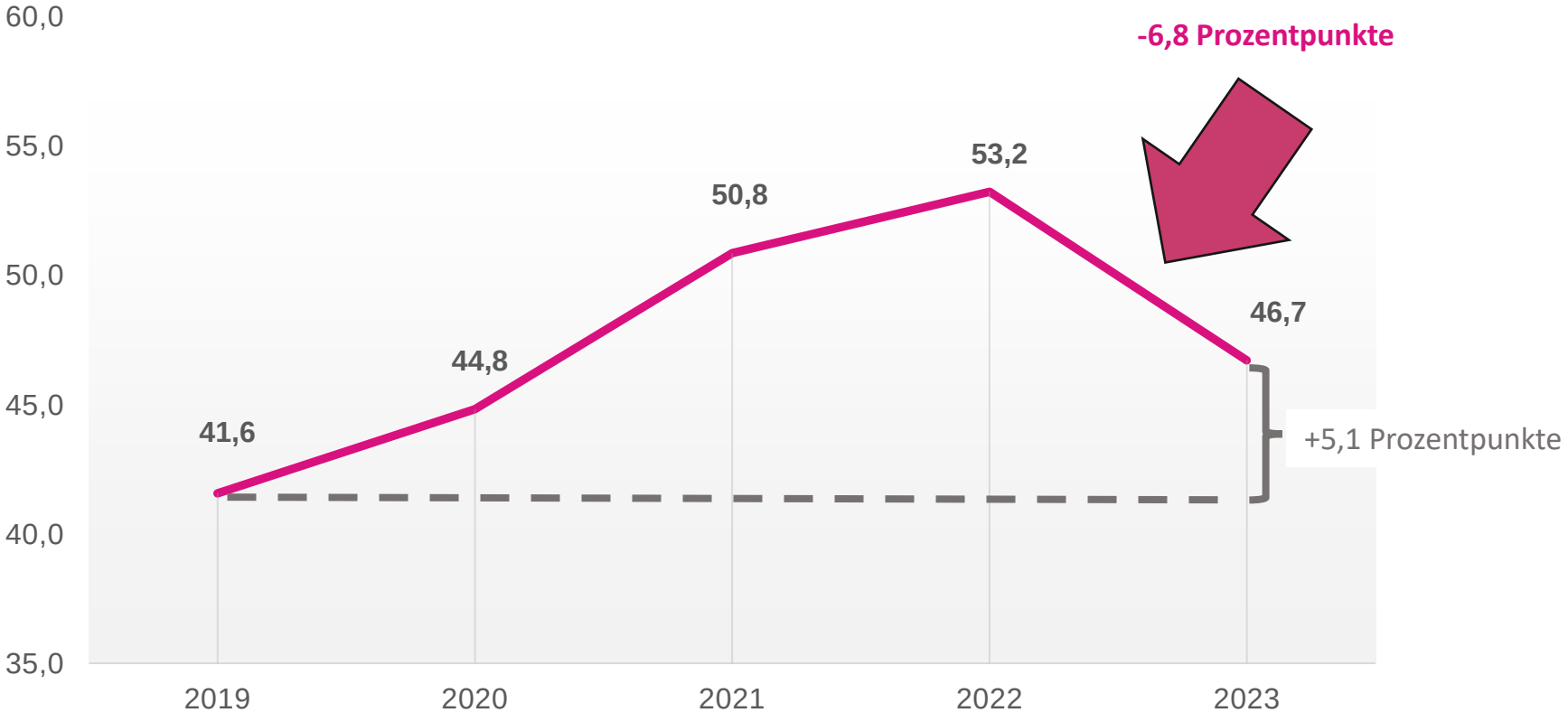
VERNICHTUNG / VERLUST



REGELMÄßIGE BEWERTUNG & ÜBERPRÜFUNG



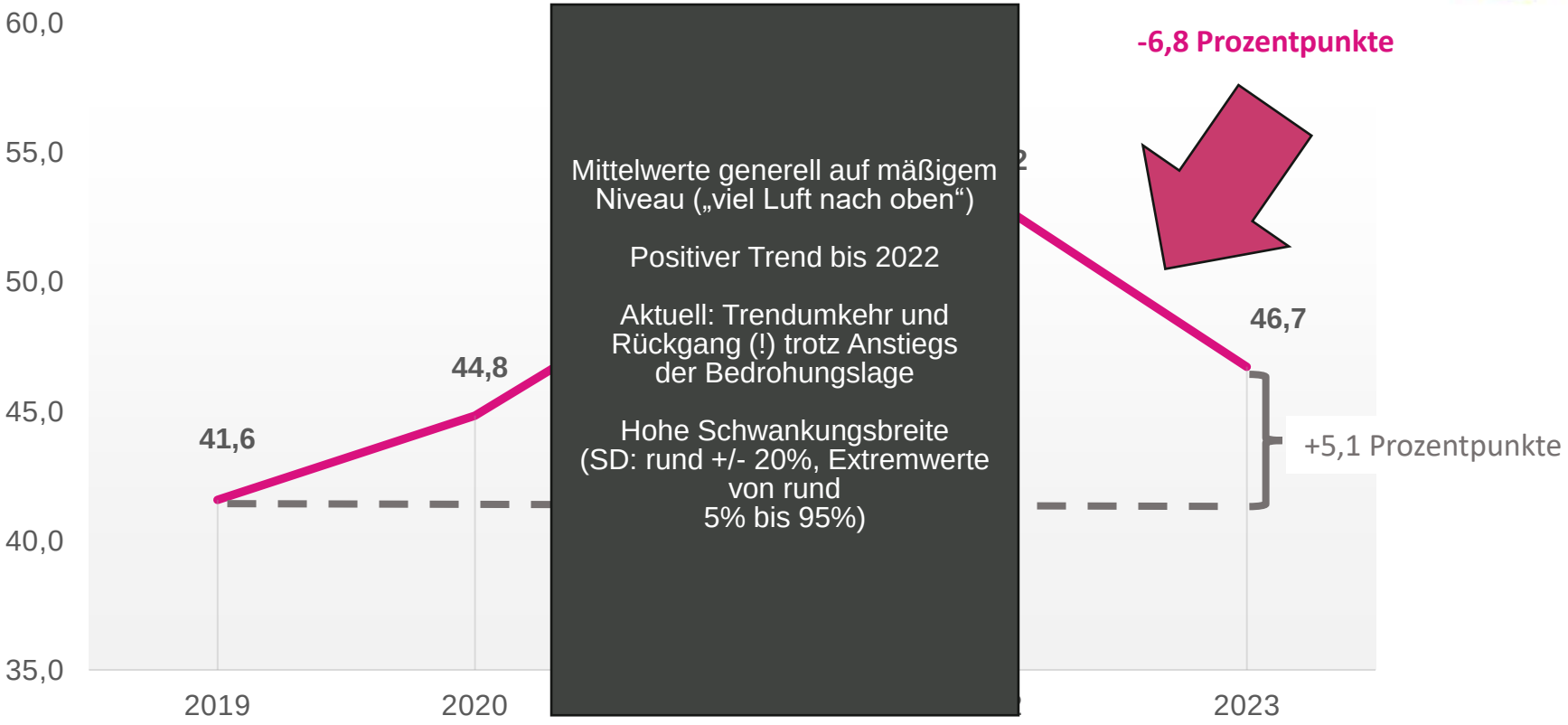
GESAMTERGEBNIS IT-AUDIT



GRUNDSÄTZLICHE BEOBACHTUNGEN

- Generell im Durschnitt recht niedriges Niveau sowohl beim Gesamtergebnis der IT-Audits als auch in Teilbereichen (nie über 60 Prozent)
  - In Summe also viel Luft nach oben im österreichischen Mittelstand in Bezug auf das Thema IT-Sicherheit
- Trendanalyse in Bezug auf die letzten 5 Jahre: durchgängig ansteigende Werte sowohl beim Gesamtergebnis der IT-Audits als auch in Teilbereichen zwischen 2019 und 2022
  - Aber: ausgeprägter Rückgang der Ergebnisse der IT-Audits in 2023 (bis zu 9 Prozentpunkte im Vergleich zu 2022)
  - In manchen Bereichen nahezu Rückgang auf das Niveau von 2019 (insbesondere im Bereich regelmäßige Bewertung & Überprüfung)
  - ACHTUNG: Trendumkehr in Zeiten zunehmender Bedrohungen

GESAMTERGEBNIS IT-AUDIT



EINFLUSSFAKTOREN

Unternehmensgröße: starker & statistisch hochsignifikanter positiver Zusammenhang (0,282***)

- Je größer das Unternehmen, desto besser die Werte beim Audit

Sitz des Unternehmens: kein statistisch signifikanter Zusammenhang

Familienunternehmen: starker & statistisch hochsignifikanter negativer Zusammenhang (-0,306***)

- Eigentümergeführte Familienunternehmen weisen schlechtere Werte beim Audit auf

Unternehmensalter: ausgeprägter & statistisch signifikanter positiver Zusammenhang (0,187**)

- Je älter das Unternehmen, desto besser die Werte beim Audit

EINFLUSSFAKTOREN

Verweildauer der GF an der Spitze: kein statistisch signifikanter Zusammenhang

Ein GF vs mehrere GF: tendenziell positiver moderater Zusammenhang (0,109)

- Mehrere Personen in der GF hängen mit besseren Werten beim Audit zusammen

Ein/e Eigentümer:in vs mehrere Eigentümer:innen: ausgeprägter & statistisch signifikanter negativer Zusammenhang (-0,122*)

- Mehrere Eigentümer:innen weisen im Vergleich zu Alleineigentümern schlechtere Werte beim Audit auf

***Alter und Geschlecht GF:** kein statistisch signifikanter Zusammenhang (konnte in CATI-Befragung aus Anonymitätsgründen nicht abgefragt werden)

EINFLUSSFAKTOREN: ZUSAMMENFASSUNG

1. **Familienunternehmen:** Eigentümergeführte Familienunternehmen weisen **schlechtere Werte** beim Audit auf
2. **Unternehmensgröße:** Je größer das Unternehmen, desto **besser die Werte** beim Audit
3. **Unternehmensalter:** Je älter das Unternehmen, desto **besser die Werte** beim Audit
4. **Ein/e Eigentümer:in vs mehrere Eigentümer:innen:** Mehrere Eigentümer:innen hängen im Vergleich zu Alleineigentümern mit **schlechteren Werten** beim Audit zusammen
5. **Ein GF vs mehrere GF:** Mehrere Personen in der GF hängen mit **besseren Werten** beim Audit zusammen

Starker Zusammenhang | Ausgeprägter Zusammenhang | Moderater Zusammenhang

ABLEITUNGEN

Familienunternehmen: Los geht‘s

Insgesamt schätzen Familienunternehmen die Bedrohungslage rund um IT Security weniger hoch ein, nehmen IT-Security auch als weniger wichtig wahr und verfügen kaum über definierte Prozesse für IT-Sicherheitsvorfälle. Sie fühlen sich insbesondere vor Datenverlusten und Angriffen weniger gut geschützt und geben allerdings auch häufiger an, keine Hemmnisse in Bezug auf die Verbesserung der IT-Security zu sehen (Möglichkeiten vorhanden, aber Wille zur Umsetzung wenig ausgeprägt durch fehlendes Bewusstsein).
Die Gruppe der Familienunternehmen braucht mehr Bewusstsein über die Risiken fehlender IT-Security. Darauf aufbauend brauchen sie mehr konkrete Unterstützung, da gerade Familienunternehmen häufiger eigentlich keine Hemmnisse in Bezug auf die Verbesserung von IT-Security sehen.

Alter des Familienunternehmens: Erfahrung zahlt sich aus

Unterscheidet man Familienunternehmen in jüngere und ältere Familienunternehmen zeigt sich, dass ältere Familienunternehmen IT-Angriffe häufiger vermuten, dem Thema einen höheren Stellenwert einräumen und sich weit besser vor Angriffen und Datenverlust geschützt fühlen. Sie sehen öfter Hemmnisse bei der Verbesserung der IT-Security. Ältere Familienunternehmen sind sich auch weniger häufig sicher, ob die Datensicherung im Unternehmen ordnungsgemäß ist. Sie gehen trotzdem davon aus, dass sie gut definierte Prozesse für IT-Sicherheitsvorfälle haben.
Jüngere Familienunternehmen könnten von älteren Familienunternehmen in Sachen IT-Security lernen. (→ Idee: Mentoring Programm)

ABLEITUNGEN

Unternehmensgröße: Vorbeugen ist besser als heilen

Bisher gab es eher IT-Security Vorfälle bei größeren Unternehmen. Diese nehmen das Thema daher auch zunehmend wichtiger war und verfügen über gut definierte Prozesse im Falle von IT-Sicherheitsvorfällen.

Kleinere Unternehmen, bei denen weniger häufig IT-Sicherheitsvorfälle auftraten, könnten sich in trügerischer Sicherheit wiegen. Vorbeugen ist besser als heilen – daher auch ohne Sicherheitsvorfälle in IT-Infrastruktur investieren.

Sitz des Unternehmens: Darf der Standort den Standpunkt bestimmen, wenn es um IT-Security geht?

Je städtischer der Sitz eines Unternehmens, desto häufiger kommen IT-Sicherheitsfälle vor. Dementsprechend ist bei städtischeren Unternehmen der Stellenwert und die Wichtigkeit von IT-Security im Unternehmen höher und sie gehen davon aus, dass IT-Risiken in den kommenden Jahren zunehmen werden. Sie verfügen daher auch über gut definierte Prozesse, die im Falle eines IT-Sicherheitsvorfalls zum Einsatz kommen.

Unternehmen im ländlichen Raum waren bisher zwar weniger häufig Opfer von IT-Angriffen als Unternehmen im städtischen Raum, sie sind aber schlechter vorbereitet und schätzen ihre Kompetenz und ihr Know-how im IT-Security Bereich auch schlechter ein. Unternehmen im ländlichen Raum müssen sich dringend mit ihrer IT-Security Infrastruktur beschäftigen sowie in den Ausbau der diesbezüglichen Kompetenz in ihrem Unternehmen investieren.

ABLEITUNGEN

Verweildauer der Geschäftsführung: Mehr Awareness

Je länger in Familienunternehmen eine Geschäftsführung in Funktion ist, desto seltener gab es in den letzten zwei Jahren IT-Sicherheitsvorfälle. Das könnte mit erhöhtem Bewusstsein zu tun haben: denn, je länger die GF bereits im Unternehmen ist, desto häufiger werden Angriffe vermutet. Ebenso wird in Familienunternehmen, deren GF schon länger im Unternehmen ist, eine stärkere Zunahme der Risiken im IT-Security Bereich vermutet. Passend dazu planen Familienunternehmen, der GF schon länger im Unternehmen ist, in den kommenden zwei Jahren höhere Investitionen in IT-Security. Ist die GF schon länger im Unternehmen, geben Familienunternehmen an, weniger sicher zu sein ob die Datensicherung im Unternehmen ordnungsgemäß ist.
Ein erhöhtes Risikobewusstsein führt zu mehr Investitionen und auch zu einer kritischeren Betrachtung einzelner Prozesse, wie etwa der Datensicherung.

Zeit bis zum nächsten Generationenwechsel: Next Gen früh einbinden

Je näher der Generationenwechsel rückt, desto höher scheint das Risikobewusstsein in Bezug auf IT-Security zu sein. Das könnte unter anderem auch daran liegen, dass hier auch die Entwicklung der IT-Sicherheitsrisiken als weniger stark gesehen wird.
Dem entsprechend investieren Familienunternehmen, bei denen der nächste Generationenwechsel noch weiter entfernt ist, auch weniger in IT-Security. Im Umkehrschluss scheint ein nahender Generationswechsel – unter Umständen auch durch die verstärkte Präsenz der Next Gen – das Risikobewusstsein zu schärfen.

DAS KANN DER MITTELSTAND JETZT TUN (1)

IT-Security als Querschnittsmaterie denken

IT-Security darf nicht nur als Experte:innen-Thema verstanden werden. IT-Security ist eine Querschnittsmaterie, die Wissen, Aufmerksamkeit und Weiterbildung aller Mitarbeiter:innen erfordert.

Dialog suchen

Cyber Crime betrifft alle. Damit ist Cyber Security auch eine gemeinsame Aufgabe. Wer sich mit anderen Unternehmen über Bedrohungen, Präventionsmaßnahmen und Erfahrungen in Bezug auf IT-Sicherheitsvorfälle austauscht kann daher nur profitieren. Auch ein regelmäßiger Austausch mit Expert:innen ist sinnvoll und wichtig.

DAS KANN DER MITTELSTAND JETZT TUN (2)

Dran bleiben

IT-Security ist für viele Unternehmen mit hohem Aufwand verbunden. Gerade wenn Digitalisierung nicht Teil des Geschäftsmodells ist, besteht die Gefahr, dass Unternehmen sich auf ihren IT-Security-Lorbeeren ausruhen. Es braucht Bewusstsein dafür, dass IT Security kein einmaliges Projekt ist, sondern ein andauernder Prozess, der permanent Aufmerksamkeit und Ressourcen benötigt. Regelmäßige Sicherheitsüberprüfungen und externe Audits sind sinnvoll und wichtig.

Kritisch bleiben

Der Kreativität an neuen Cyber-Bedrohungen ist keine Grenze gesetzt. Alleine 2021 sind 144 Millionen neue Schadsoftware-Varianten hinzugekommen (KPMG 2022). Wer sicher bleiben will, muss daher auch bereit sein die eigenen Annahmen und Maßnahmen regelmäßig kritisch zu hinterfragen. Regelmäßige Sicherheitsüberprüfungen und externe Audits sind sinnvoll und wichtig.

DAS SOLLTE DIE POLITIK JETZT TUN (1)

Cyber Security geht alle an
Es braucht mehr Bewusstseinsbildung und Aufklärung in Wirtschaft und Gesellschaft über die Bedeutung von Cyber Crime sowie mögliche Schutzmaßnahmen. Maßnahmen wie der **Cyber-Security Month** soll sich in den Schulen, Hochschulen sowie Erwachsenenaus- und Weiterbildungseinrichtungen durch zahlreiche Maßnahmen stark spürbar sein. Auch Unternehmen könnten, etwa über die Wirtschaftskammer aufgerufen werden, Veranstaltungen in ihrer Organisation umzusetzen und Cyber Security regelmäßig zum Thema zu machen.

Die kleineren Unternehmen aus dem ländlichen Raum drohen durch den Rost zu fallen
Unternehmen aus dem ländlichen Raum scheinen IT-Security Risiken und deren Entwicklung zu unterschätzen. Hier braucht es Bewusstseinsbildung und die Möglichkeit sich mit Unternehmen, die mehr Erfahrung im Bereich IT-Security haben, auszutauschen. Nach dem Vorbild von Start-Up Mentoring Programmen, könnte ein **Mentoring Programm für IT-Security** ins Leben gerufen werden in dem erfahrene Geschäftsführer:innen junge Geschäftsführer:innen bzw. ältere Familienunternehmen jüngere Familienunternehmen in Sachen IT-Security begleiten.

Regelmäßige Sicherheitsüberprüfungen und externe Audits fördern
Regelmäßige Sicherheitsüberprüfungen und externe Audits sind sinnvoll und wichtig. Insbesondere bei kleineren Unternehmen fehlt es vielfach nicht nur an Bewusstsein, sondern auch an Ressourcen. Hier ist die Politik gefordert, um entsprechende Fördermaßnahmen zu setzen.

DAS SOLLTE DIE POLITIK JETZT TUN (2)

NextGen in Familienunternehmen als Chance begreifen
Der Übergang von einer Generation auf die andere ist auch eine Chance für IT-Security: Nachfolger:innen und Übernehmer:innen brauchen Bewusstsein und ein Mindestmaß an Grundkompetenzen, wenn es um das IT-Security in Unternehmen geht. Nach dem Beispiel „NextGen 4 Bavaria“ könnte auch in Österreich ein **Programm für Nachfoger:innen/Übernehmer:innen eingerichtet werden, das unter anderem eine Grundqualifizierung im Bereich IT-Security** beinhaltet.

Optionen aufzeigen statt kriminalisieren und damit auch den Fachkräftemangel smart adressieren
Nach dem Vorbild der britischen Organisation „Cyber Choices“ könnten minderjährige oder junge Personen, die im Zusammenhang mit Cyber Crime auffällig wurden nicht nur aufgeklärt werden, welchen desaströsen Karrierepfad sie – oft unwissentlich – einschlagen, sondern ihr Talent auch gezielt für die Wirtschaft gescouted werden.

Stellenwert der IT grundlegend ändern
Die Sicherheit der IT-Infrastruktur in der Jahresbilanz auf den Prüfstand stellen. Ähnlich wie die Eigenkapitalquote oder die Bonität.

GOOD PRACTICE BEISPIEL „CYBER SECURITY MONTH“ /EU

„For the 10th consecutive year the European Union Agency for Cybersecurity (ENISA) is partnering with the Commission and Member States in carrying out #CyberSecMonth: the EU’s annual campaign dedicated to promoting cybersecurity among EU citizens and organisations and providing up-to-date online security information through awareness raising activities and sharing of good practices.“

https://cybersecuritymonth.eu/

GOOD PRACTICE BEISPIEL „NEXTGEN FÜR BAVARIA“ /DE

Die digitale Transformation stellt die nächste Generation des Mittelstands in Bayern vor ihre bisher größte Herausforderung: Kompetenzen im Bereich Digitalisierung und Innovation auf- und auszubauen, um ihre Unternehmen zukunftsfähig zu machen. Dafür ist der Zugang zu Digitalisierungsexpertise dringend erforderlich. Deshalb hat das Digitalministerium die Digitalinitiative NextGen4Bavaria für Unternehmensnachfolge ins Leben gerufen: NextGen4Bavaria schafft ein exklusives und professionelles Umfeld, das die digitale Aus- und Weiterbildung der Teilnehmenden in den Mittelpunkt stellt und bayerische Unternehmen so fit für die digitale Zukunft macht.

https://www.stmd.bayern.de/themen/nextgen4bavaria/

GOOD PRACTICE BEISPIEL „CYBER CHOICES“ /UK

In Großbritannien sind zahlreiche der Personen, die wegen Cyber Crime Delikten mit dem Gesetz in Konflikt kommen, noch minderjährig. Um insbesondere diese Gruppe nicht zu kriminalisieren hat die Polizei in England einen anderen Weg eingeschlagen:

Mit der Gründung der Organisation Cyber Choices wurde eine Stelle geschaffen, die die auffällig gewordenen Jugendlichen u.a. über den Karrierepfad aufklären, den sie mit ihren illegalen Aktivitäten einschlagen und sie informiert, welche Konsequenzen ihre Aktivitäten in weiterer Folge haben könnten.

Gleichzeitig wird aber ihr Potenzial erkannt und Cyber Choices versucht diese Jugendlichen als Fachkräfte für die „gute Seite“ als etwa IT-Security-Abteilungen staatliche Organisationen oder von Unternehmen zu gewinnen. So wird nicht nur weiteren kriminellen Taten vorgebeugt sondern auch ein Beitrag zur Milderung des Fachkräftemangels in diesem Bereich beigesteuert.

https://nationalcrimeagency.gov.uk/cyber-choices


WHAT'S
NEXT
INSTITUTE

UNSER ANGEBOT

WIR BEGLEITEN ORGANISATIONEN IN WIRTSCHAFT, POLITIK UND GESELLSCHAFT DABEI SICH STRUKTURIERT MIT DER ZUKUNFT ZU BESCHÄFTIGEN.

WIRTSCHAFT

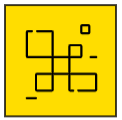
(Familien-) Unternehmen I Social Businesses

NEXT GENs

Nachfolger:innen in (Familien)Unternehmen I Nächste Generation in politischen Organisationen und NGOs

POLITIK

Ministerien I Verwaltung I Parteien I Politische Vorfeldorganisationen



NGOs

Think Tanks I Interessenvertretungen I Vereine