



LAGEBILD WIRTSCHAFTSSCHUTZ NRW 2021/22 KOMPAKT

Die ist eine Kompaktversion des Lagebilds. Bei Interesse an der Komplettfassung wenden Sie sich bitte an die E-Mail Adresse **wirtschaftsschutz@im1.nrw.de**.

Erstellt durch die
Fachhochschule des Mittelstands (FHM)

Auf Initiative der
Sicherheitspartnerschaft NRW

unter Federführung des
Ministeriums des Innern
des Landes Nordrhein-Westfalen

Ausschließlich zum Zweck der besseren Lesbarkeit wird auf eine geschlechtsspezifische Schreibweise verzichtet.
Alle personenbezogenen Bezeichnungen sind genderneutral und beziehen sich auf Angehörige aller Geschlechter.

Zur besseren Lesbarkeit des Berichts werden nicht alle Textteile grafisch belegt.
Bei Fragen zu Grafiken wenden Sie sich gerne an lagebild-ws@fh-mittelstand.de

VORWORT



Die vergangenen Monate und Jahre waren mit extremen Herausforderungen für die Gesellschaft, aber auch für jedes einzelne Wirtschaftsunternehmen verbunden. Die Folgen des Ukraine-Krieges, einschneidende Auswirkungen der Corona-Pandemie und steigende Bedrohungen durch weltweit agierende Cyberkriminelle versetzen große Teile der Wirtschaft bis heute in einen andauernden Krisenmodus. In einer solchen Situation ist es wichtig, dass Unternehmen Orientierung und Unterstützung erfahren.

Die Sicherheitspartnerschaft Nordrhein-Westfalen bietet dies. Sie bildet ein starkes Bündnis gegen Wirtschaftsspionage, Sabotage und Wirtschaftskriminalität. Und sie hat den Fokus auf dem Schutz kleiner und mittlerer Unternehmen in Nordrhein-Westfalen.

Mit dem Lagebild Wirtschaftsschutz hat die Sicherheitspartnerschaft im Jahr 2019 erstmals den Status des Schutzniveaus mittelständischer Unternehmen in NRW durch die Fachhochschule des Mittelstands in Bielefeld erheben lassen. Wir wollen damit feststellen, in welchen Bereichen es konkrete Unterstützungsbedarfe bei der Unternehmenssicherheit gibt. Unternehmen können dabei ihre eigenen Akti-

vitäten im Bereich Sicherheit einordnen und mögliche Handlungsbedarfe erkennen. Mit regelmäßiger Wiederholung der Befragung lassen sich so Entwicklungen nachvollziehen und es kann entsprechend gegengesteuert werden.

Ein erstes Update liegt nun mit dem „Lagebild Wirtschaftsschutz NRW 2021/22“ vor. Ich bedanke mich bei den mehr als eintausend Unternehmen, die bei der Befragung mitgemacht und einen wichtigen Beitrag zum Schutz unserer Wirtschaft geleistet haben.

Leider ist der Gesamtindexwert für das Schutzniveau von 2019 bis 2021 gesunken. Der Schutzstatus über alle Branchen und Größen mittelständischer Unternehmen in NRW hinweg ist damit im Jahr 2021 weiterhin als eher gering zu bezeichnen. Dies ist alarmierend. Es macht mir Sorge, dass beispielsweise der Nachholbedarf beim Thema Schulung und Sensibilisierung immer noch sehr groß ist, vor allem bei kleinen Unternehmen. Obwohl es zahlreiche, teils kostenlose Sensibilisierungsangebote im Bereich Unternehmenssicherheit gibt, werden diese offenbar zu wenig genutzt. Wir müssen und werden uns als Sicherheitspartner noch stärker bemühen, die Unternehmen auf diese Angebote aufmerksam zu machen. Das von der Landesregierung im Jahr 2021 eingerichtete Kompetenzzentrum für Cybersicherheit in der Wirtschaft Digital.Sicher.NRW kann dabei gut unterstützen. Ein wichtiger Schritt war zudem die Einrichtung der Koordinierungsstelle für Cybersicherheit NRW im Ministerium des Innern. Sie schafft einen Überblick über die Aktivitäten innerhalb der Landesregierung und bildet eine Plattform für ein abgestimmtes Vorgehen.

Meine Bitte an alle Unternehmen in Nordrhein-Westfalen: Nutzen Sie die kostenfreien Unterstützungs- und Präventionsangebote von Verfassungsschutz und Polizei in NRW sowie die entsprechenden Angebote der übrigen Sicherheitspartner. Und geben Sie der Unternehmenssicherheit den Stellenwert, der ihr gebührt, damit Ihr Unternehmen auch in Zukunft sicher ist.

A handwritten signature in black ink, which appears to read 'Herbert Reul'.

Herbert Reul MdL
Minister des Innern des Landes Nordrhein-Westfalen

INHALTSVERZEICHNIS

I	Ergebnisse im Überblick und Handlungsempfehlungen	
1.1	Ergebnisse im Überblick	6
1.2	Kennzahlen zum Gesamtindex	8
1.3	Handlungsempfehlungen der Sicherheitspartnerschaft	10
II	Einleitung und Grundlagen	
2.1	Einleitung	14
	Wirtschaftsschutz im Innenministerium	14
	Sicherheitspartnerschaft Nordrhein-Westfalen	15
	Ganzheitlicher Ansatz	15
	Lagebild Wirtschaftsschutz NRW	16
	Ziele	16
2.2	Grundlage der Untersuchung	18
	Kleine und mittlere Unternehmen	18
	Wirtschaftsschutz im Lagebild	18
III	Lage des Wirtschaftsschutzes bei KMU in NRW 2021	
3.1	Übergreifende Indexwerte und Aussagen	22
	Gesamtindex	24
	Branchenindex	26
	Indexwerte von KRITIS-Unternehmen	30
	Schutzstatus nach Wichtigkeit des Schutzes von Betriebs- und Geschäftsgeheimnissen	32
	Aufteilung der Unternehmen nach Schutzstatus	38
	Index nach Unternehmensgröße	40
3.2	Fokus: Mobiles Arbeiten und Homeoffice	44
	Entwicklung von mobiler Arbeit und Homeoffice im Vergleich zu Vor-Corona-Zeiten	46
	Digitalisierungsstand in den Unternehmen	48
	Veränderung der Unternehmenssicherheit durch mobiles Arbeiten und Homeoffice	50
3.3	Dimension 1: Organisatorische Schutzmaßnahmen	54
	Richtlinien und Anweisungen	56
	Passwortrichtlinie	58
	Notfall- und Krisenkonzepte	60
	Monitoring sicherheitsrelevanter Prozesse	62
	Schriftliches Sicherheitskonzept	64
	Externe Absicherungsmaßnahmen	66
	Cyberversicherungen	68
3.4	Dimension 2: Personenbezogene Schutzmaßnahmen	70
	Unternehmenssicherheit als Chefsache	72
	Operative Zuständigkeit für Unternehmenssicherheit	74
	Integrität	76
	Sensibilisierung und Schulung	78

3.5 Dimension 3: Cyberangriffsschutz	82
Cyberangriffe und Angriffsversuche bei den Unternehmen	84
Verschlüsselung mobiler Endgeräte und des Datenaustausches	86
Verschlüsselung der Kommunikation	88
Verschlüsselung des externen Zugriffs auf Systeme	90
Zugriffsschutz	92
Firewall und Antivirenprogramme	94
Backups	96
Aktuelle Patches und Updates bei Software	98
Regelmäßige Sicherheitstests	100
3.6 Dimension 4: Physischer Gebäudeschutz	102
Gebäudeschutz und Schutz sensibler Bereiche vor unerlaubtem Eindringen	104
Videogestützte oder akustische Einbruchmeldeanlagen	106
Kontrolle des Betriebsgeländes durch Sicherheitspersonal	108
Sicherheitsvorkehrungen für sensible Besprechungen	110
Aufbewahrung sensibler und wichtiger Dokumente	112
3.7 Informationsquellen zum Thema Unternehmenssicherheit	116
IV Methodik der Untersuchung	
4.1 Zielgruppeninformationen	120
Kleine und mittlere Unternehmen	120
Branchendifferenzierung	120
Wirtschaftsregionen	121
4.2 Stichprobe und Durchführung der Studie	122
4.3 Rücklaufquote und Repräsentativität	124
4.4 Auswertung der Erhebung	126
Allgemeines	126
Einschränkung von Aussagen bei Großunternehmen und der Branche „Sonstiges“	126
Aussagen zur Indexwerten und dem Status des Schutzniveaus	126
Verzeichnisse	
Abbildungsverzeichnis	128
Tabellenverzeichnis	130
Literaturverzeichnis	131
Impressum / Rechtliche Hinweise	
Impressum	132

I

ERGEBNISSE IM ÜBERBLICK UND HANDLUNGSEMPFEHLUNGEN

1.1 Ergebnisse im Überblick

Die vorliegende Studie liefert wichtige neue Erkenntnisse zum aktuellen Stand des Wirtschaftsschutzes bei kleinen und mittleren Unternehmen (KMU) in Nordrhein-Westfalen. Es können folgende Ergebnisse festgehalten werden:

Das Lagebild Wirtschaftsschutz bietet einen ganzheitlichen Blick auf das Schutzniveau der kleinen und mittleren Unternehmen in Nordrhein-Westfalen.

Es zeigt anhand von vier Schutzdimensionen (Organisatorische und *Personenbezogene Schutzmaßnahmen*, *Cyberangriffsschutz* und *Physischer Gebäudeschutz*) auf, wie umfassend mittelständische Unternehmen mit einer Größe von 0 bis 499 Mitarbeitern die Umsetzung ihrer Unternehmensschutzmaßnahmen auf einer Skala von 0 bis 10 einschätzen.

Mittelständische Unternehmen in NRW sind nur teilweise geschützt. Das Schutzniveau ist im Vergleich zu 2019 noch geringer.

Der Schutzstatus mittelständischer Unternehmen in NRW ist auch im Jahr 2021 noch eher gering. Es wird ein Gesamtindexwert von 4,41 erzielt (2019: 4,81), was der Aussage ‚teilweise geschützt‘ entspricht. Einzelne Branchen erweisen sich als besonders wenig geschützt. ‚Eher wenig geschützt‘ sind vor allem die ‚Gastronomie/Hotellerie‘ (3,12) sowie das ‚Handwerk‘ (3,80). Keine Branche erreicht 2021 das Ergebnis ‚eher gut geschützt‘. Insgesamt sind größere Mittelständler besser geschützt. Während ‚Kleinstunternehmen‘ (0-9 Mitarbeiter) auf einen Wert von 3,79 kommen und damit ‚wenig geschützt sind‘, erzielen Unternehmen mit 10 bis 249 Mitarbeitern Werte zwischen 4 und 6. Dies entspricht der Aussage ‚teilweise geschützt‘. Lediglich Unternehmen ab 250 Mitarbeitern gelten mit einem Wert von 6,18 als ‚eher geschützt‘.

Cyberangriffsschutz ist im Fokus der Unternehmen. Der Schutzfaktor Mensch wird vernachlässigt.

Eine erhöhte Sensibilität in Bezug auf Maßnahmen ist bei allen *Cyberangriffsschutzindikatoren* feststellbar. Eine geringe Relevanz wird hingegen den Bereichen *Schulung und Sensibilisierung*, *Integritätsprüfungen* sowie *externen Absicherungsmaßnahmen* zugemessen. Die geringere Relevanzwahrnehmung spiegelt sich in der geringen Umsetzung konkreter Maßnahmen in diesen Kategorien wider. Damit wird ein erhöhtes Gefährdungspotenzial deutlich. Zum einen fehlt das Wissen und die Sensibilität für die Notwendigkeit des Unternehmensschutzes, zum anderen sind entsprechende Unternehmen im Falle eines Angriffs nicht hinreichend abgesichert. Vor allem die Bedeutung des Schutzfaktors Mensch wird noch zu wenig gesehen.

Ein geringer Unternehmensschutz ist vor allem in „Gastronomie/Hotellerie“, „Handwerk“ und „Handel“ erkennbar.

Insgesamt zeigt sich, dass vor allem kleine Unternehmen noch wenige Schutzmaßnahmen umsetzen. In diesem Bereich sollten die Maßnahmen zur *Sensibilisierung und Schulung* verstärkt und genau auf diese Unternehmensgröße abgestimmt werden. Ein besonderer Fokus der Prävention sollte sich zudem auf die Branchen ‚Gastronomie/Hotellerie‘, ‚Handwerk‘ und ‚Handel‘ richten. Ein umfassendes Schutzniveau weist kein Unternehmen auf. Mittelständler sind vorrangig auf einem intermediären Niveau. **Kein Unternehmen aus dem Bereich der KMU in NRW ist nach eigener Einschätzung ‚umfassend‘ geschützt** und weist einen Indexwert von 10 auf (0 < 2 = ‚Schutzlos‘; 2 < 4 = ‚Einsteiger‘; 4 < 6 = ‚Intermediär‘; 6 < 8 = ‚Fortgeschrittener‘; 8 < 10 ‚Experte‘). **Die Mehrheit der Unternehmen bewegt sich beim Thema Wirtschaftsschutz auf dem Niveau ‚Einsteiger‘ (31,6 %) oder ‚Intermediär‘ (32,1 %)**. Der durchschnittliche Gesamtindexwert beträgt bei Berücksichtigung aller Unternehmen 4,41 und liegt damit im Bereich eines ‚teilweisen‘ Schutzes. Lediglich 3,1 Prozent aller Unternehmen sind auf der Grundlage eigener Angaben dem Schutzstatus ‚Experte‘ zuzurechnen. 13,1 Prozent aller Unternehmen sind als ‚schutzlos‘ zu bezeichnen. Jedes fünfte Unternehmen (20,1 %) ordnet sich in die Kategorie ‚Fortgeschrittene‘ ein.

Unternehmen fühlen sich selbst zu gut geschützt.

Die Unternehmen überschätzen ihren Schutz in allen vier abgefragten Dimensionen. Dies deutet auf ein trügerisches Sicherheitsgefühl bei den Unternehmen hin. Lediglich im Bereich *Cyberangriffsschutz* liegt die Selbstwahrnehmung mit einem Indexwert von 6,51 nahe am tatsächlichen Indexwert von 6,20. Es ist zu vermuten, dass die Unternehmen hier mehr sensibilisiert sind und daher zu einer realistischeren Einschätzung kommen.

Relevanz von ganzheitlichen Maßnahmen wird erst mit zunehmender Größe des Unternehmens gesehen.

Die ‚Relevanz‘ ganzheitlicher Schutzmaßnahmen steigt mit der Unternehmensgröße. „Große Mittelständische“ Unternehmen mit 250 bis 499 Beschäftigten erzielen einen Indexwert von 6,18 und sind damit als ‚eher geschützt‘ zu bezeichnen. „Kleinunternehmen“ mit 10 bis 49 Beschäftigten und „größere Mittelständler“ mit 50 bis 249 Mitarbeitern haben mit Indexwerten von 4,30 und 5,54 nur einen ‚teilweisen‘ Schutz. „Kleinstunternehmen“ mit 0 bis 9 Mitarbeitern sind mit einem Wert von 3,79 ‚eher wenig‘ geschützt.

Ein Blick auf die einzelnen Zahlen ermöglicht zudem folgende detaillierte Feststellungen:

- Je kleiner ein Unternehmen ist, desto größer ist die Gefahr, dass ein breit angelegter, unspezifischer Angriff, der nicht gezielt auf ein Unternehmen abgestimmt ist, sondern sich auf eine unbestimmte Anzahl von Unternehmen bezieht, erfolgreich verläuft.
- KRITIS-Unternehmen sind mit einem Indexwert von 5,04 nur wenig besser geschützt als Nicht-KRITIS-Unternehmen (4,22). Der Schutz von KRITIS-Unternehmen fällt deutlich geringer aus als noch 2019 (Indexwert 7,2).
- Der „Schutzfaktor Mensch“ findet bei den Unternehmen noch zu wenig Berücksichtigung. Die Dimension *Personenbezogene Schutzmaßnahmen* weist nur einen Gesamtindexwert von 4,22 auf.

- Schulungen und Sensibilisierungen werden als wichtige präventive Maßnahme des Unternehmensschutzes im Mittel deutlich vernachlässigt (Indexwert 3,43).
- Unternehmen haben ein erhöhtes Risiko für schwere Beeinträchtigungen der Betriebsfähigkeit oder finanzielle Schäden bei erfolgreichen Angriffen. Zum einem sind *Notfall- und Krisenkonzepte* (3,47) sowie Sicherheitsanalysen und -konzepte (3,35) kaum existent und vollständig ausgearbeitet. Zum anderen sind Unternehmen für den Fall von finanziellen Folgen eines Angriffs kaum extern abgesichert (2,46).
- Der *Cyberangriffsschutz* ist über alle Branchen und Unternehmensgrößen hinweg die am stärksten ausgeprägte Dimension der Unternehmenssicherheit.
- Am meisten werden Schutzmaßnahmen in den Indikatorbereichen *Schutz vor Cyberattacken und Datenverlust* (Indexwert 7,10, Rangplatz 1), *Zuständigkeiten* (6,30, 2) und *Zugriffsschutz* (6,04, 3) umgesetzt. Dies sind die einzigen Indikatoren bei denen ein ‚eher hoher‘ Schutz erkennbar wird.
- Indikatoren mit erkennbarem Nachholbedarf (Indexwert < 4,0), was dem Niveau ‚eher wenig‘ geschützt entspricht, gibt es in allen Dimensionen. Die Indikatoren mit den niedrigsten Schutzwerten sind: *Externe Absicherungsmaßnahmen* (2,46), *Integritätsprüfungen* (2,93), *Sicherheitsanalysen und -konzepte* (3,35), *Sensibilisierungen und Schulungen* (3,43), *Notfall- und Krisenkonzepte* (3,47), *Äußerer Gebäude- und Betriebsgeländeschutz* (3,48), *Richtlinien und Anweisungen* (3,63).
- Unternehmen aller Branchen und Größen sind potenzielle Angriffsopfer. Jede beziehungsweise jeder Verantwortliche sollte dem Schutz des eigenen Unternehmens hohe Aufmerksamkeit widmen.

Das Lagebild Wirtschaftsschutz NRW 2021 zeigt, dass in den vier Schutzdimensionen *Organisation*, *Personal*, *Cyberangriffsschutz* und *Gebäudeschutz* in Teilen deutlicher Handlungs- und Aufholbedarf besteht. Dabei hat sich der Schutzstatus in den letzten beiden Jahren kaum verändert, beziehungsweise hat er sich sogar in einzelnen Bereichen verschlechtert. Branchen- und größenbezogen bestehen weiterhin große Unterschiede. Es erweist sich, dass für die Resilienz eines gesamten Wirtschaftssystems Unternehmensschutz von einem größeren Anteil von Unternehmen als eigenständiges und zentrales Handlungsfeld verstanden werden sollte.

1.2 Kennzahlen zum Gesamtindex

Die folgende Tabelle gibt einen Überblick über die wichtigsten Kennzahlen des Lagebilds Wirtschaftsschutz NRW 2021.

Tabelle 1: Kennzahlen Gesamtindex 2021 und 2019

Kennzahl	Werte 2021	Werte 2019
Gesamtindex Wirtschaftsschutz KMU in NRW 2021	4,41	4,81
Indexwerte nach Dimensionen		
Indexwert <i>Organisatorische Schutzmaßnahmen</i>	3,23	3,82
Indexwert <i>Personenbezogene Schutzmaßnahmen</i>	4,22	5,24
Indexwert <i>Cyberangriffsschutz</i>	6,20	6,37
Indexwert <i>Physischer Gebäudeschutz</i>	4,00	3,82
Indexwerte nach Indikatoren		
<i>Richtlinien und Anweisungen</i>	3,63	4,63
<i>Notfall- und Krisenkonzepte</i>	3,47	3,13
<i>Sicherheitsanalysen und -konzepte</i>	3,35	4,22
<i>Externe Absicherungsmaßnahmen</i>	2,46	3,30
<i>Zuständigkeiten</i>	6,30	7,25
<i>Integritätsprüfungen</i>	2,93	4,25
<i>Sensibilisierungen und Schulungen</i>	3,43	4,21
<i>Verschlüsselung</i>	5,47	5,29
<i>Zugriffsschutz</i>	6,04	7,18
<i>Schutz vor Cyberattacken und Datenverlust</i>	7,10	6,65
<i>Schutz innerhalb des Gebäudes</i>	4,53	4,36
<i>Äußerer Schutz des Gebäudes und Betriebsgeländes</i>	3,48	3,28
KRITIS/ Nicht-KRITIS		
Indexwert KRITIS-Unternehmen	5,04	7,20
Indexwert Nicht-KRITIS-Unternehmen	4,22	4,70
Branchenbezogene Indexwerte		
Indexwert Finanzen/Versicherungen	5,21	6,26
Indexwert Handel	4,30	4,42
Indexwert Energie/Wasser/Abwasser/Entsorgung	5,30	7,34
Indexwert Gastronomie/Hotellerie	3,12	3,95
Indexwert Gesundheit/Soziales	4,88	5,42
Indexwert Industrie	4,82	5,10
Indexwert Handwerk	3,80	4,04
Indexwert Industrienaher Dienstleistungen	4,52	5,49

Kennzahl	Werte 2021	Werte 2019
Anteil der Unternehmen nach Schutzstatus		
Schutzlose (Indexwert 0<2)	13,1 %	7,1 %
Einsteiger (Indexwert 2<4)	31,6 %	28,4 %
Intermediäre (Indexwert 4<6)	32,1 %	36,1 %
Fortgeschrittene (Indexwert 6<8)	20,1 %	20,5 %
Experten (Indexwert>8)	3,1 %	7,9 %
Größenbezogene Indexwerte		
Kleinstunternehmen (0-9 Mitarbeiter)	2,42	4,41*
Kleinunternehmen (10-49 Mitarbeiter)	3,35	4,88*
Größere Mittelständler (50-249 Mitarbeiter)	5,45	5,76
Große Mittelständler (250-499 Mitarbeiter)	5,45	6,95

* Hinweis: 2021 wurde in die Größenkategorien 0 bis 9 Mitarbeiter und 10 bis 49 Mitarbeiter unterschieden. 2019 lagen die Kategorien bei 0 bis 19 und 20 bis 49 Mitarbeiter.

1.3 Handlungsempfehlungen der Sicherheitspartnerschaft

Das Lagebild Wirtschaftsschutz NRW 2021 spiegelt die Selbsteinschätzung und den Schutzstatus kleiner und mittlerer Unternehmen (KMU) in Nordrhein-Westfalen wider. Aus den Ergebnissen der Befragungen leitet die Sicherheitspartnerschaft Nordrhein-Westfalen folgende Empfehlungen ab:

- Die beiden vorliegenden Lagebilder 2019 und 2021 belegen, dass die kleinen und mittleren Unternehmen in Nordrhein-Westfalen ihr Schutzniveau in den Bereichen *Organisatorische Schutzmaßnahmen*, *Personenbezogene Schutzmaßnahmen* und *Physischer Gebäudeschutz* weiterhin zum Teil deutlich höher einschätzen, als es die jeweiligen Indexwerte bei den Schutzmaßnahmen widerspiegeln. Möglicherweise ist dies auf eine zu geringe Sensibilität für diese Schutzbereiche zurückzuführen. Der präventive Wirtschaftsschutz sollte seinen Fokus bei der Sensibilisierung daher verstärkt auf eine ganzheitliche Betrachtung der Unternehmenssicherheit richten, die ausdrücklich alle vier Dimensionen der Unternehmenssicherheit in den Blick nimmt.
- Beim Schutzniveau sind die einzelnen Branchen weiterhin sehr unterschiedlich aufgestellt. Insbesondere bei den Unternehmen der Branchen Handwerk und Handel ist der Schutz besonders niedrig ausgeprägt. Zur gezielten Stärkung der Resilienz der Unternehmen empfiehlt die Sicherheitspartnerschaft, die Unterstützung der Branchen Handel und Handwerk durch die in der Prävention aktiven Akteure kurzfristig zu intensivieren, um den Grundschutz zu verbessern.
- Die Ergebnisse der Studie deuten darauf hin, dass viele vor allem kleinere Unternehmen Schwierigkeiten haben, ihre besonders schützenswerten Betriebs- und Geschäftsgeheimnisse zu identifizieren, das konkrete Bedrohungspotential zu analysieren und systematisch ganzheitliche Sicherheitskonzepte zu entwerfen. Der präventive Wirtschaftsschutz sollte seine Bemühungen verstärkt darauf ausrichten, den Unternehmen Methoden und Werkzeuge nahezubringen, mit denen sich diese Aufgaben leichter und individuell angepasst umsetzen lassen.
- Zahlreiche kleine und mittlere Unternehmen in Nordrhein-Westfalen unterstützen ihre Beschäftigten offensichtlich immer noch nicht hinreichend bei der Anwendung grundlegender Schutzmaßnahmen wie dem Passwortschutz. Regelmäßige Schulungen und Sensibilisierungen finden gerade bei kleineren Unternehmen teilweise bis gar nicht statt. Die Sicherheitspartnerschaft sieht hier einen weiteren, konkreten Unterstützungsbedarf für die KMU durch Informationen zu entsprechend niederschweligen Methoden und Instrumenten. Das Angebot an Lern- und Vermittlungsinhalten in einer modernen Form (z.B. Videos, Podcasts) sollte ausgebaut und Kleinstunternehmen möglichst kostenlos zur Verfügung gestellt werden.
- Fast die Hälfte aller Unternehmen nutzen ein Monitoring sicherheitsrelevanter Prozesse eher nicht bis gar nicht. Gerade bei kleinen Unternehmen ist der Anteil besonders hoch und sogar rückläufig. Die Sicherheitspartnerschaft rät dringend dazu, neben der Implementierung von Schutzvorkehrungen auch ein kontinuierliches, aktives Monitoring zu betreiben. Angriffe und Angriffsversuche lassen sich damit sehr frühzeitig erkennen und abwenden oder zumindest das Ausmaß möglicher Schäden begrenzen.
- Der Anteil der KMU, die *Notfall- und Krisenkonzepte* nutzen, ist zwar leicht gestiegen, er liegt aber immer noch auf einem sehr niedrigen Niveau. Dabei lassen sich bei einer frühzeitigen und zielgerichteten Reaktion im Angriffsfall in vielen Fällen größere Schäden für das betroffene Unternehmen abwenden. Die im Wirtschaftsschutz aktiven Akteure sollten kleine und mittlere Unternehmen verstärkt für die Notwendigkeit einer Vorbereitung auf jederzeit zu erwartende erfolgreiche Angriffe sensibilisieren. Dies sollte mit Informationen zu konkreten Unterstützungsangeboten für die Erstellung von Notfall- und Krisenplänen verbunden werden.
- Das Schutzniveau der Unternehmen, die sich selbst der KRITIS-Kategorie zuordnen, ist gegenüber dem Lagebild 2019 deutlich gesunken. Die vorliegenden Zahlen geben keinen weiteren Aufschluss über mögliche Gründe für diese Entwicklung. In Anbetracht der zunehmenden Bedrohungslage gerade auch für den besonders sensiblen KRITIS-Bereich, sieht die Sicherheitspartnerschaft NRW einen dringenden Bedarf, diese Entwicklung näher zu beleuchten.





II

EINLEITUNG UND GRUNDLAGEN

2.1 Einleitung

In Nordrhein-Westfalen (NRW) gibt es ca. 730.600 kleine und mittlere Unternehmen (KMU). Mittelständische Unternehmen stellen 99,3 % aller Unternehmen in NRW dar und gelten damit als Stütze der Wirtschaft.¹ Gerade durch die Covid19-Pandemie haben digitale Formen der Zusammenarbeit und die Umsetzung von Online-Vertriebsmöglichkeiten an Bedeutung gewonnen. Auch wenn die Digitalisierung im Mittelstand bislang noch deutlich langsamer voranschreitet als in großen Unternehmen,² stellen soziotechnische Entwicklungen wie insbesondere „Industrie 4.0“, „virtuelle Zusammenarbeit“, „Big Data“ und „Künstliche Intelligenz“ Unternehmen vor neue und zunehmende Herausforderungen. Alle direkten und indirekten wertschöpfenden Aktivitäten sind davon betroffen. Zudem wird die interne Wertschöpfungskette um eine fortschreitende digitale Vernetzung mit Lieferanten und Kunden erweitert. Im Zuge dieser zunehmenden Digitalisierung bieten sich potenziellen Angreifern von innen wie von außen vielfältige neue Möglichkeiten.

Laut einer Studie von Bitkom, des Branchenverbandes der deutschen Informations- und Telekommunikationsbranche, entsteht der deutschen Wirtschaft jährlich ein Schaden von 223 Milliarden Euro durch Diebstahl, Sabotage und Spionage. Rund neun von zehn Unternehmen wurden bereits Opfer. Gerade das Homeoffice stellt ein neues Einfallstor dar. 59 Prozent der befragten Unternehmen, bei denen das Arbeiten im Homeoffice grundsätzlich möglich ist, gaben in der Bitkom-Studie an, von Sicherheitsvorfällen betroffen gewesen zu sein, die im Zusammenhang mit der Arbeit in den heimischen Büros entstanden sind.³ Wie das Lagebild Wirtschaftsschutz NRW 2019 aufgezeigt hat, sind mittelständische Unternehmen häufig noch sehr wenig vor Angriffen geschützt. 68,5 % der KMU sind gar nicht oder eher wenig geschützt und sind damit hoch gefährdet, selbst Opfer von Angriffen zu werden.⁴

Wirtschaftsschutz im Innenministerium

Zum Aufgabenspektrum des Verfassungsschutzes gehört der Wirtschaftsschutz. Wirtschaftsschutz im Sinne der eng gefassten Aufgabenbeschreibung des verantwortlichen Referates umfasst ausgehend vom Aufklärungsauftrag des Verfassungsschutzes insbesondere die Präventionsarbeit zu Bedrohungen, die sich aus Spionageaktivitäten fremder Nachrichtendienste ergeben. Die Dienste anderer Staaten handeln insbesondere aus politischen Interessen oder mit dem Ziel, der eigenen Wirtschaft durch Ausforschung von Unternehmen einen Wettbewerbsvorteil zu verschaffen.

Die kostenfreien Präventionsangebote des Referates Wirtschaftsschutz richten sich an nordrhein-westfälische Unternehmen aller Branchen und Größenordnungen, an wissenschaftliche Einrichtungen sowie an Verwaltung und Politik. Insoweit stellen sie ein gezieltes Sensibilisierungsprogramm dar, mit dem Bedrohungen durch Ausspähungen, insbesondere Wirtschaftsspionage, und speziell durch Cyberattacken, begegnet wird. Der präventive Wirtschaftsschutz setzt zudem auf Informationsvermittlung zum Schutz vor Bedrohungen durch Sabotage, Extremismus und Terrorismus. Er geht von der Grundannahme aus, dass Unternehmenssicherheit zuerst ein Handlungsfeld der unternehmerischen Eigenverantwortung ist. Darauf aufbauend berät und unterstützt der Verfassungsschutz Unternehmen und andere Zielgruppen, auch auf Nachfrage, zur Notwendigkeit ganzheitlicher *Sicherheitskonzepte* und gibt praktische Hilfestellungen bei den ersten Schritten zu deren Aufstellung. Das Referat Wirtschaftsschutz führt derzeit zudem die Geschäfte der Sicherheitspartnerschaft Nordrhein-Westfalen.

1 Vgl. Wirtschaft NRW. Web: <https://www.wirtschaft.nrw/daten-und-fakten-zum-mittelstand-nrw>

2 Vgl. Werning et al.: Digitalisierungsindex von KMU in NRW. Digitalisierungsstand in den Branchen Industrie, industriennahe Dienstleistungen und Handwerk, hrsg. Sparkassenverband Westfalen-Lippe, Münster 2020.

3 Bitkom (2021): Web: <https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr>

4 Vgl. Werning et al. (2019): Lagebild Wirtschaftsschutz NRW 2019. Web: https://www.wirtschaftsschutz.info/SharedDocs/Studien/DE/Lagebild_NRW.html (Abruf: 23.09.2021)

Sicherheitspartnerschaft Nordrhein-Westfalen

Unter dem erweiterten Begriff „Wirtschaftsschutz“, der dem Lagebild zugrunde liegt, leisten zahlreiche Akteure insbesondere der Wirtschaft, der Wissenschaft und des Staates einen Beitrag, um Unternehmen für die Gefahren von Angriffen zu sensibilisieren, sie präventiv zu beraten oder ihnen in Fällen erfolgreicher Attacken bei der Eingrenzung möglicher Schäden zu helfen.

Mit diesen Zielsetzungen wurde im Jahr 2001 die „Sicherheitspartnerschaft Nordrhein-Westfalen“ gegründet. Im Fokus dieser Partnerschaft liegt ein gemeinsames Vorgehen gegen Wirtschaftsspionage und Wirtschaftskriminalität. Mitglieder der Sicherheitspartnerschaft NRW sind derzeit

- das Ministerium des Innern des Landes Nordrhein-Westfalen mit dem Landeskriminalamt und dem Verfassungsschutz,
- die Allianz für Sicherheit in der Wirtschaft West e.V.,
- die IHK NRW - Industrie- und Handelskammern in Nordrhein-Westfalen e.V.,
- das Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen und
- der Verband der Wirtschaftsförderungsgesellschaften NRW.

Unter den Sicherheitspartnern besteht Einigkeit, dass eine vernetzte Zusammenarbeit zwischen Wirtschaft und Staat für einen umfassenden Wirtschaftsschutz unentbehrlich ist. Innerhalb der Sicherheitspartnerschaft drückt sich dies durch einen kontinuierlichen Austausch, gegenseitige Information, Beratung und Unterstützung, aber auch gemeinsame Projekte und Aktivitäten zu sicherheitsrelevanten Themen aus. Die Partnerschaft profitiert dabei von der Expertise der einzelnen Mitglieder.

Konkrete Angebote der Sicherheitspartnerschaft für Unternehmen sind:

- umfassende Sensibilisierungen zu aktuellen Entwicklungen, Gefährdungen und Gegenstrategien,

- aktuelle unternehmensbezogene Informationen zur Gefährdung durch Wirtschaftsspionage, Wirtschaftskriminalität, Produkt- und Markenpiraterie, Cybercrime, politisch motivierte Kriminalität und IT-Sicherheit,
- aktuelle Lagebilder,
- Fortbildungsveranstaltungen, Beratungsgespräche und Sicherheitstagungen.
- umfassende Informationsmaterialien,
- Hinweise auf Informationsveranstaltungen.⁵

Ganzheitlicher Ansatz

Beim Thema Unternehmenssicherheit ist eine ganzheitliche Betrachtungsweise notwendig. Der technische *Schutz vor Cyberangriffen und Datenverlust* stellt zwar eine wesentliche Säule des Unternehmensschutzes dar, dennoch sind die betrieblich existentiellen Daten und Informationen von Unternehmen Gefahren durch Ausspähung und Abschöpfung ausgesetzt. Und die Radikalisierung von Beschäftigten kann Abläufe im Unternehmen erheblich stören und den wirtschaftlichen Erfolg sowie das Außenbild eines Unternehmens beeinträchtigen.

Der Sicherheitsfaktor „Mensch“ ist daher die entscheidende zweite Schutzsäule. Denn die Beschäftigten sind sowohl Gestalterinnen und Gestalter sowie Managerinnen und Manager als auch Administratorinnen und Adressaten der Maßnahmen zur Unternehmenssicherheit. Darüber hinaus benötigen Mitarbeiterinnen und Mitarbeiter Handlungssicherheit. Diese sind über *Richtlinien und Anweisungen, Notfall-, Krisen und Sicherheitskonzepte* sowie durch *externe Absicherungsmaßnahmen* umzusetzen. Dies stellt die dritte Säule eines ganzheitlichen Unternehmensschutzes dar. Die vierte Säule bildet der *äußere und innere Gebäudeschutz*.

Ein ganzheitlicher Wirtschaftsschutz verfolgt über allem das Ziel, die Resilienz der Unternehmen gegen Angriffe verschiedenster Art und Motivation zu festigen. Die damit verbundenen Gefahren haben gerade kleine und mittlere Unternehmen nicht immer fest im Blick. Wer seinen Betrieb jedoch umfassend gesichert und die Beschäftigten umfassend eingebunden hat, gewinnt damit einen wichtigen Wettbewerbsvorteil.

5 Vgl. <https://www.im.nrw/themen/verfassungsschutz/schutz-von-behoerden-und-unternehmen/sicherheitspartnerschaft-nordrhein>. (Stand: 01.12.2021).

Lagebild Wirtschaftsschutz NRW

Die Digitalisierung der Wertschöpfungsprozesse, die Zunahme an mobiler Arbeit sowie die Verzahnung von analoger und virtueller Lebenswelt stellen eine zunehmende Herausforderung für den Schutz von Daten, Informationen und Know-how in allen Gesellschaftsbereichen dar.⁶ Der hohe Anteil mittelständischer Unternehmen an der deutschen Wirtschaft gebietet es, diese in besonderem Maße und vor allem vorsorgend dabei zu unterstützen, sich und damit die Resilienz des gesamten deutschen Wirtschaftssystems zu stärken.

Daher ist es wichtig, neben aktuellen Bedrohungsformen auch das Schutzniveau in den Unternehmen zu kennen. Daraus lassen sich Handlungserfordernisse für den präventiven Wirtschaftsschutz ableiten, mit dem Ziel, bei den Unternehmen das Bewusstsein für Sicherheitsbedrohungen und -maßnahmen zu erhöhen.⁷ Der präventive staatliche Wirtschaftsschutz in seiner konkreten Ausformung muss sich demzufolge an dem tatsächlichen Zustand der Unternehmenssicherheit orientieren. Das Augenmerk der vorliegenden Untersuchung liegt deshalb, wie bereits 2019, auf der Erhebung des Schutzniveaus, das die Unternehmen zur Vermeidung von Sicherheitsrisiken umsetzen. Abzuleiten sind ebenso besondere Aufgabenstellungen und neuen Herausforderungen für den präventiven Wirtschaftsschutz. Ein besonderer Fokus wird aufgrund der aktuellen Situation dem Thema „Mobiles Arbeiten und Homeoffice“ gewidmet. Zusammengefasst ergibt sich daraus das „Lagebild Wirtschaftsschutz NRW 2021“. Es konzentriert sich auf die größte Zielgruppe der im Wirtschaftsschutz engagierten Akteure, die knapp 730.600 kleinen und mittleren Unternehmen in Nordrhein-Westfalen.

Ziele

Die Fachhochschule des Mittelstandes (FHM) hat von Anfang September 2021 bis Ende November 2021 im Auftrag der Sicherheitspartnerschaft NRW und unter der Projektleitung des Ministeriums des Innern des Landes Nordrhein-Westfalen die vorliegende Studie zum „Lagebild Wirtschaftsschutz NRW

2021“, bezogen auf die KMU in Nordrhein-Westfalen, durchgeführt. Die Studie verfolgt vier wesentliche Ziele:

1. Aufbau einer fundierten empirischen Basis zum IST-Stand des Sicherheitsniveaus (auf einer Skala von 0 bis 10) in mittelständischen Unternehmen mit einem besonderen Fokus im Jahr 2021 auf das Thema „Mobiles Arbeiten und Homeoffice“
2. Überführung der Ergebnisse in ein „Lagebild Wirtschaftsschutz NRW 2021“. Dies gibt Aufschluss darüber, welche Schutzdimensionen und Indikatoren für den Wirtschaftsschutz als staatliche Aufgabe der Prävention aktuell relevant sind sowie gezielt und verstärkt in den Fokus seiner Aktivitäten genommen werden sollten.
3. Vergleich der Ergebnisse der Lagebilder 2019 und 2021, um Entwicklungen beim Schutzstatus darstellen zu können.
4. Schaffung eines Analyseinstruments für unternehmerische Handlungsfelder. Das Wissen über die Anwendung bestimmter Maßnahmen ermöglicht nicht nur das Abbild eines konkreten unternehmerischen Schutzniveaus, sondern bietet damit auch Aufschlüsse über erforderliche Entwicklungsschritte.

Das Lagebild stellt im Folgenden die wesentlichen Erkenntnisse zu den Schutzdimensionen zusammen. Nach einer Zusammenfassung folgen jeweils die Ergebnisse zu den einzelnen Schutzaspekten sowie deren Einordnung.

6 <https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf>.

7 Bitkom (2016) <https://www.bitkom.org/sites/default/files/file/import/181106-Studie-Wirtschaftsschutz.pdf>. (Abruf: 01.12.2021)

2.2 Grundlage der Untersuchung

Im Folgenden werden die Grundlagen der Untersuchung dargestellt. Tiefergehende Informationen zur Methodik der Untersuchung enthält das Kapitel IV.

Kleine und mittlere Unternehmen

Zielgruppe der Untersuchung sind kleine und mittlere Unternehmen in NRW, die so genannten KMU. Die Einordnung der Unternehmen in die Gruppe der KMU erfolgt in Anlehnung an die Definition des Instituts für Mittelstandsforschung (IfM) und der KMU-Definition der Europäischen Kommission⁸.

Tabelle 2: Definition KMU (IfM Bonn 2018)

Unternehmensgröße	Zahl der Beschäftigten	€ Umsatz/Jahr
Kleinstunternehmen	bis 9	bis 2 Mio.
Kleinunternehmen	bis 49	bis 10 Mio.
Größerer Mittelstand	bis 249	bis 43 Mio.
Großer Mittelstand	bis 499	bis 50 Mio.

Für die Untersuchung wird die Dimension „Umsatz“ nicht weiter betrachtet.

Branchendifferenzierung

Die im Lagebild vorgenommene Differenzierung der Branchen erfolgt in Anlehnung an die vom Statistischen Bundesamt festgelegten Branchencodes C-Q. Diese wurden den im Lagebild betrachteten Branchen zugeordnet.⁹

Tabelle 3: Branchenbezeichnungen Lagebild Wirtschaftsschutz

Kategorie	Branchenbezeichnung
1	Finanzen/Versicherungen
2	Handel
3	Energie/Wasser/Abwasser/Entsorgung
4	Gastronomie/Hotellerie
5	Gesundheit/Soziales
6	Industrie
7	Handwerk
8	Industrienaher Dienstleistungen
9	Sonstiges

Die teilnehmenden Unternehmen haben sich bei der Befragung selbst der jeweiligen Branche zugeordnet.

Wirtschaftsschutz im Lagebild

Wirtschaftsschutz ist grundsätzlich auf Unternehmen jeder Größenordnung in Deutschland ausgerichtet. Er umfasst in erster Linie alle Rahmenbedingungen und Maßnahmen, die der Unternehmenssicherheit dienen. Für den Wirtschaftsschutz tragen die Unternehmen genauso wie unterschiedliche Akteure vornehmlich aus den Bereichen Staat, Wissenschaft und Gesellschaft Verantwortung. Die maßgebliche Verantwortung für die Unternehmenssicherheit tragen jedoch die Unternehmen selbst. Das tatsächliche Schutzniveau lässt sich deshalb nur dort erheben.

Der Fokus dieses Lagebildes liegt demnach nicht auf dem Gesamtfeld des Wirtschaftsschutzes aus Sicht von Staat und Gesellschaft, sondern betrachtet unter dem Begriff

⁸ <https://www.ifm-bonn.org/definitionen/kmu-definition-des-ifm-bonn/>

⁹ vgl. Kapitel 4.1 Zielgruppeninformationen, S. 122

Wirtschaftsschutz die Summe aller Schutzmaßnahmen, die Unternehmen zur Vermeidung von Sicherheitsrisiken umsetzen.

Die relevanten Maßnahmen werden als Lagebild Wirtschaftsschutz NRW 2021 über vier Dimensionen erschlossen:

Dimension 1 - Organisatorische Schutzmaßnahmen

Die Grundlage für alle Maßnahmen des Wirtschaftsschutzes in dieser Dimension besteht in der organisatorischen Ausrichtung und Verankerung von *Richtlinien und Anweisungen*, von *Notfall- und Krisenkonzepten*, von allgemeinen *Sicherheitsanalysen und -konzepten* sowie von *externen Absicherungsmaßnahmen*.

Dimension 2 - Personenbezogene Schutzmaßnahmen

Die Sicherheit in Unternehmen ist entscheidend von den Mitarbeitern, deren Umgang mit technischem Equipment, Daten und Informationen sowie der Zuordnung von Verantwortung für Sicherheitsthemen abhängig. Für die Sicherstellung wirtschaftlicher Wettbewerbsfähigkeit haben *Zuständigkeiten*, *Integritätsprüfungen* sowie Personalentwicklung bzw. *Sensibilisierung und Schulung* eine wichtige Bedeutung.

Dimension 3 - Cyberangriffsschutz

Die zunehmende Globalisierung und Digitalisierung stellt die Unternehmen vor neue Sicherheitsanforderungen. Durch neue digitale Techniken, die vielseitig einsetzbar sind und Prozesse im Unternehmen effizienter gestalten, rückt sowohl der Schutz durch *Verschlüsselung* als auch der *Zugriffsschutz* in den Fokus der Unternehmen. Das gilt auch für den *Schutz vor Cyberattacken und Datenverlust* durch z.B. Wirtschaftsspionage oder Cyberkriminalität.

Dimension 4 - Physischer Gebäudeschutz

Eine ganzheitliche Betrachtung der Unternehmenssicherheit umfasst zudem den *physischen Gebäudeschutz*. Es gilt, den physischen Schutz des Gebäudes und des Betriebsgeländes nach außen sicherzustellen. Daneben spielt der Schutz sensibler Bereiche innerhalb des Unternehmens eine wichtige Rolle.

Jeder Dimension wurden Indikatoren zugeordnet, die einzelne Schutzmaßnahmenbereiche beschreiben. Die Zuordnung der Indikatoren zu den Dimensionen zeigt die folgende Tabelle.

Tabelle 4: Dimensionen und Indikatoren des Lagebildes Wirtschaftsschutz

Dimension	Indikator
1. Organisatorische Schutzmaßnahmen	1.1 <i>Richtlinien und Anweisungen</i>
	1.2 <i>Notfall- und Krisenkonzepte</i>
	1.3 <i>Sicherheitsanalyse und -konzepte</i>
	1.4 <i>Externe Absicherungsmaßnahmen</i>
2. Personenbezogene Schutzmaßnahmen	2.1 <i>Zuständigkeiten</i>
	2.2 <i>Integritätsprüfung</i>
	2.3 <i>Sensibilisierung und Schulung</i>
3. Cyberangriffsschutz	3.1 <i>Verschlüsselung</i>
	3.2 <i>Zugriffsschutz</i>
	3.3 <i>Schutz vor Cyberattacken und Datenverlust</i>
4. Physischer Gebäudeschutz	4.1 <i>Schutz innerhalb des Gebäudes</i>
	4.2 <i>Äußerer Schutz des Gebäudes</i>

III

LAGE DES WIRTSCHAFTSSCHUTZES BEI KMU IN NRW 2021

3.1 Übergreifende Indexwerte und Aussagen

Wesentliche Erkenntnisse

Das Lagebild Wirtschaftsschutz NRW 2021 zeigt deutliche Branchenunterschiede beim Schutzniveau. KRITIS-Unternehmen schneiden nur leicht besser ab als die übrigen Unternehmen.

Das Lagebild zeigt abermals, dass die Branchen „Gastronomie/Hotellerie“ (Indexwert 3,13), „Handwerk“ (3,80) und „Handel“ (4,30) am wenigsten geschützt sind. KRITIS-Unternehmen sind mit einem Indexwert von 5,04 nur noch leicht besser geschützt als Nicht-KRITIS-Unternehmen (4,22). Im Vergleich zu 2019 lässt sich sogar ein deutlich niedrigeres Schutzniveau erkennen (2019: 7,2).

Eine Relevanz von Schutzmaßnahmen wird vor allem beim Cyberangriffsschutz gesehen. Unternehmenssicherheit wird von den Unternehmen noch nicht als ganzheitliches Thema verstanden.

Die Basisschutzmaßnahmen zur Vermeidung von Cyberangriffen wie Backups, Firewalls, Antivirenprogramme oder Passwortschutz werden von mehr als 85 Prozent der Unternehmen als ‚eher‘ bis ‚sehr relevant‘ bewertet. Schulungen und Sensibilisierung, Integritätsprüfungen sowie externen Absicherungsmaßnahmen werden hingegen von mehr als der Hälfte der Unternehmen als ‚eher nicht‘ bis ‚gar nicht relevant‘ bewertet. Die Bedeutung einer ganzheitlichen Betrachtung von Unternehmenssicherheit ist vielen Unternehmen noch nicht bewusst.

Kleine und mittlere Unternehmen in NRW überschätzen ihren Schutzstatus.

In allen vier Dimensionen schätzen die Unternehmen sich besser ein, als sie tatsächlich geschützt sind. Insgesamt sind 43,7 % der Unternehmen als ‚Schutzlos‘ oder ‚Einstieger‘ zu bezeichnen und weisen damit nur einen geringen Unternehmensschutz auf.

Mit zunehmender Unternehmensgröße und Bedeutung von Betriebs- und Geschäftsheimnissen wächst das Schutzniveau.

Je größer ein Unternehmen ist, desto mehr Schutzmaßnahmen setzt es um. Daneben ist für den Umfang des Unternehmensschutzes die Bedeutung von Betriebs- und Geschäftsheimnissen relevant. Je mehr Bedeutung Unternehmen diesen zumessen, desto stärker ist der Unternehmensschutz ausgeprägt.



Gesamtindex

i [4,41]

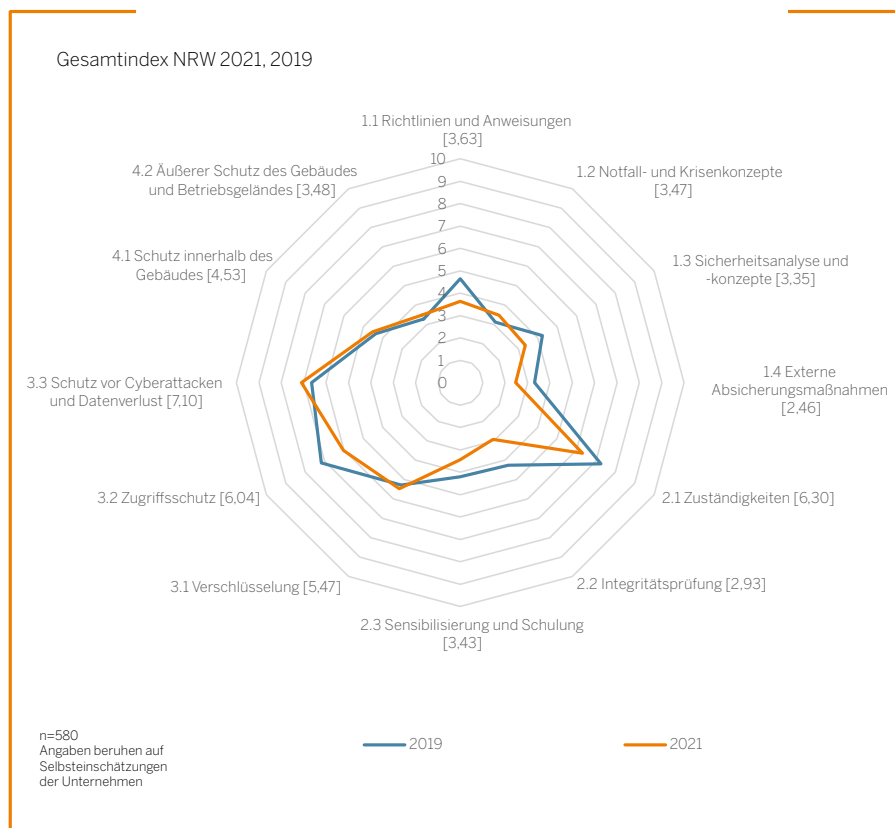


Abbildung 1: Gesamtindex NRW im Vergleich 2019/2021

Schutzbereich / Betrachtungsfeld

Der Gesamtindex von mittelständischen Unternehmen in NRW misst auf der Basis einer Selbsteinschätzung aller teilnehmenden Unternehmen, wie umfassend Schutzmaßnahmen in den einzelnen Dimensionen umgesetzt werden. Der Gesamtindex ergibt sich aus den gewichteten Branchenindizes.

Zentrale Ergebnisse

Der Gesamtindexwert der Unternehmenssicherheit bei KMU in Nordrhein-Westfalen liegt bei 4,41 von 10. NRW-Unternehmen bewerten sich damit im Durchschnitt als ‚teilweise geschützt‘.

Es zeigen sich deutliche Unterschiede bei den einzelnen Wirtschaftsschutzdimensionen. Über dem durchschnittlichen Gesamtindexwert von 4,41 findet sich einzig der Durchschnittswert der Dimension *Cyberangriffsschutz* (Indexwert 6,20). Dagegen liegen die Werte der übrigen Dimensionen *Organisatorische Schutzmaßnahmen* (3,23), *Personenbezogene Schutzmaßnahmen* (4,22) sowie *Physischer Gebäudeschutz* (4,00) unter dem durchschnittlichen Gesamtindexwert.

Im Berichtsjahr 2021 erzielen die Unternehmen den höchsten Indexwert in der Dimension *Cyberangriffsschutz* (6,20). Die Indikatoren *Schutz vor Cyberattacken und Datenverlust* (7,10) sowie *Zugriffsschutz* (6,04) stechen besonders positiv hervor.

Bei den *Personenbezogenen Schutzmaßnahmen* sind die Unternehmen mit einem Indexwert von 4,22 ‚mittelmäßig‘ aufgestellt. Besonders hervorzuheben ist der Indikator *Zuständigkeiten* mit einem Indexwert von 6,30. Die Festlegung einer Zuständigkeit für Sicherheitsthemen scheint bei den Unternehmen somit am ehesten umgesetzt zu sein.

Der *Physische Gebäudeschutz* weist bei Unternehmen in NRW einen geringen Indexwert von 4,00 auf. Insbesondere der *Äußere Schutz des Betriebsgeländes* zeigt sich mit einem Wert von 3,48 als ‚teilweise‘ vorhanden, liegt jedoch an der Grenze zu ‚eher wenig‘ vorhandenen Schutzmaßnahmen.

Tabelle 5: Schutzindikatoren nach Indexwert absteigend

Indikatorenranking (Rang und Bezeichnung)	2021	2019
1. Schutz vor Cyberattacken und Datenverlust	7,10	6,65
2. Zuständigkeiten	6,30	7,25
3. Zugriffsschutz	6,04	7,18
4. Verschlüsselung	5,47	5,29
5. Schutz innerhalb des Gebäudes	4,53	4,36
6. Richtlinien und Anweisungen	3,63	4,63
7. Äußerer Schutz des Gebäudes und Betriebsgeländes	3,48	3,28
8. Notfall- und Krisenkonzepte	3,47	3,13
9. Sensibilisierung und Schulung	3,43	4,21
10. Sicherheitsanalyse und -konzepte	3,35	4,22
11. Integritätsprüfung	2,93	4,25
12. Externe Absicherungsmaßnahmen	2,46	3,30
Gesamtindex 2021	4,41	4,81

Die Dimension *Organisatorische Schutzmaßnahmen* nimmt mit einem Wert von 3,23 mit etwas Abstand den letzten Platz bei den Dimensionen ein. Es zeigt sich, dass Unternehmen in Bezug auf *Externe Absicherungsmaßnahmen* ‚eher wenig‘ Maßnahmen ergreifen. *Dieser Indikator hat mit einem Indexwert von 2,46 die geringste Ausprägung im gesamten Lagebild.*

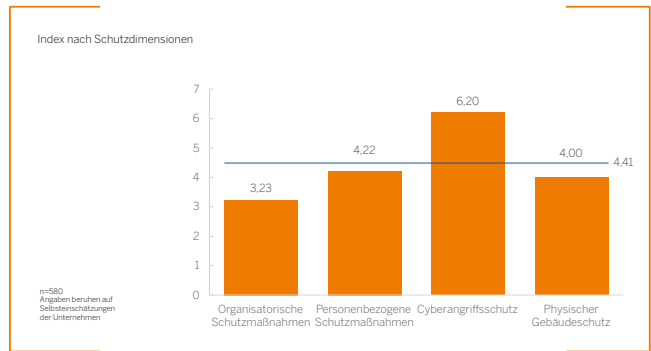


Abbildung 2: Durchschnittindexwert und Indexwerte der vier Dimensionen

Einordnung

Insgesamt hat sich der Schutz der Unternehmen in allen Dimensionen im Vergleich zu 2019 leicht verschlechtert. Der Gesamtindex liegt 0,4 Punkte niedriger als vor zwei Jahren (2019: 4,81; 2021: 4,41). Diese kritischere Einschätzung der eigenen Schutzmaßnahmen mag mit einer gestiegenen Sensibilität für die Gefahren einhergehen. Gerade bei den *Zuständigkeiten* schätzen sich die Unternehmen deutlich zurückhaltender ein als noch 2019. Der Indexwert sinkt von 7,25 auf 6,30. Möglicherweise sind durch die Corona-Pandemie in Beziehung auf die *Zuständigkeiten* Unklarheiten gewachsen, die sich in einem gesunkenen Sicherheitsempfinden ausdrückt.

Die Corona-Pandemie könnte auch einen Sondereffekt bei den Indikatoren *Integritätsprüfungen* sowie *Sensibilisierungen und Schulungen* bewirkt haben. Möglicherweise ist durch eine Verringerung der Besucherzahlen, weniger neue Mitarbeiter oder auch seltenere direkte Kontakte mit Geschäftspartnern die Wahrnehmung der Bedeutung einer *Integritätsprüfung* für Unternehmen gesunken. Lag der Wert 2019 noch bei 4,25, beträgt er im Jahr 2021 nur noch 2,93. Der Wert der *Sensibilisierungen und Schulungen* sinkt von 4,21 auf 3,40, was mit einem geringen Angebot von Schulungen oder dem vielfach erfolgten Aussetzen von Unternehmensschulungen in Zeiten der Pandemie einhergehen kann.

Branchenindex

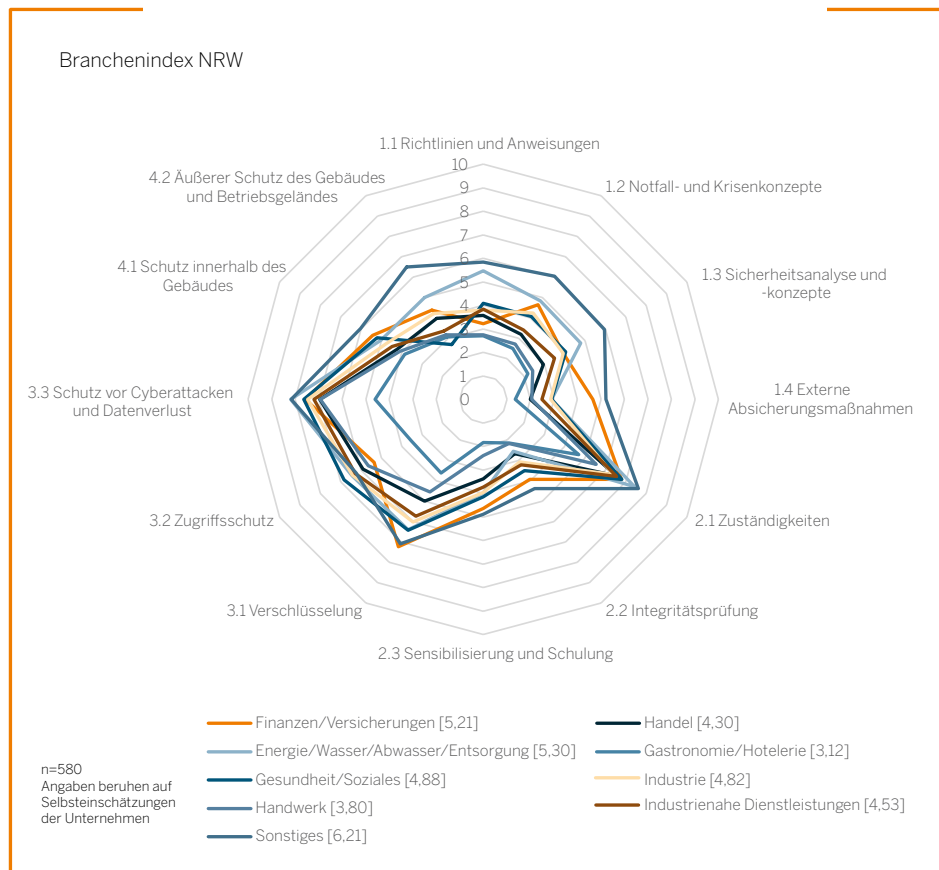


Abbildung 3: Branchenindex NRW

Schutzbereich / Betrachtungsfeld

Der Branchenindex für mittelständische Unternehmen in NRW gibt auf der Basis einer Selbsteinschätzung wieder, wie umfassend Schutzmaßnahmen in einzelnen Branchen umgesetzt werden. Betrachtet werden die Branchen „Finanzen/Versicherungen“, „Handel“, „Energie/Wasser/Abwasser/Entsorgung“, „Gastronomie/Hotellerie“, „Gesundheit/Soziales“, „Industrie“, „Handwerk“ und „Industrienahe Dienstleistungen“. Auf die aus methodischen Gründen hinzugefügte Kategorie „Sonstiges“ wird nicht weiter eingegangen.

Zentrale Ergebnisse

Die vier Branchen „Gesundheit/Soziales“, „Industrienahe Dienstleistungen“, „Industrie“ „Finanzen/Versicherungen“ und „Energie/Wasser/Abwasser/Entsorgung“ sind mit Gesamtindexwerten zwischen 4,53 und 5,30

überdurchschnittlich aufgestellt. Die Werte der drei Branchen „Gastronomie/Hotellerie“ (3,12), „Handwerk“ (3,80) und „Handel“ (4,30) liegen demgegenüber unterhalb des Branchendurchschnitts.

In der Dimension Organisatorische Maßnahmen zeigt sich, dass Sicherheitsmaßnahmen am stärksten in der „Finanz- und Versicherungsbranche“ (4,11) und in der Branche „Energie/Wasser/Abwasser/Entsorgung“ (4,49) umgesetzt sind, wengleich in der Aussage nur ‚teilweise‘. Die Bereiche „Gastronomie/Hotellerie“, „Handel“ und „Handwerk“ weisen Organisatorischen Schutzmaßnahmen weniger Relevanz zu. Hier liegen die Indexwerte zwischen 2,19 und 2,92. Insbesondere in der „Gastronomie/Hotellerie“ und im „Handwerk“ fehlen in weiten Teilen Notfall- und Krisenkonzepte sowie Externe Absicherungsmaßnahmen.

Tabelle 6: Indexwerte nach Branche und Gesamtindex

Dimensionen und Indikatoren	01	02	03	04	05	06	07	08	09	Gesamt
1. Organisatorische Schutzmaßnahmen	4,11	2,92	4,49	2,19	3,77	3,71	2,49	3,31	5,76	3,23
1.1 Richtlinien und Anweisungen	3,21	3,56	5,47	2,71	4,08	3,80	2,75	3,83	5,83	3,63
1.2 Notfall- und Krisenkonzepte	4,64	3,18	4,84	2,50	4,08	4,25	2,73	3,41	6,04	3,47
1.3 Sicherheitsanalyse und -konzepte	3,93	2,95	4,77	2,19	4,03	3,93	2,42	3,49	5,94	3,35
1.4 Externe Absicherungsmaßnahmen	4,64	1,99	2,89	1,35	2,90	2,85	2,06	2,49	5,21	2,46
2. Personenbezogene Schutzmaßnahmen	5,12	4,19	4,65	2,89	4,81	4,46	3,36	4,50	5,63	4,22
2.1 Zuständigkeiten	6,79	6,53	7,42	4,69	6,79	6,38	5,53	6,54	7,60	6,30
2.2 Integritätsprüfungen	3,93	2,68	2,55	2,15	3,50	3,07	2,16	3,22	4,38	2,93
2.3 Sensibilisierung und Schulung	4,64	3,37	3,98	1,84	4,15	3,95	2,40	3,73	4,90	3,43
3. Cyberangriffsschutz	6,72	5,96	7,02	3,92	6,97	6,64	5,71	6,42	7,17	6,20
3.1 Verschlüsselung	7,23	4,99	6,41	3,61	6,42	6,01	4,54	5,73	7,08	5,47
3.2 Zugriffsschutz	5,36	5,92	6,46	3,54	6,85	6,43	5,65	6,31	6,25	6,04
3.3 Schutz vor Cyberattacken und Datenverlust	7,57	6,96	8,19	4,60	7,64	7,47	6,93	7,21	8,17	7,10
4. Physischer Gebäudeschutz	4,91	4,11	5,02	3,46	3,96	4,49	3,63	3,92	6,28	4,00
4.1 Schutz innerhalb des Gebäudes	5,45	4,25	5,04	3,85	5,23	4,76	4,10	4,48	6,04	4,53
4.2 Äußerer Schutz des Gebäudes und Betriebsgeländes	4,38	3,97	5,00	3,07	2,69	4,21	3,17	3,36	6,51	3,48
Gesamtindex pro Branche	5,21	4,30	5,30	3,12	4,88	4,82	3,80	4,53	6,21	4,41*

*Gesamtbranchenindexwerte ergeben sich aus der Gewichtung der Werte der Branchen

01 Finanzen/Versicherungen
02 Handel
03 Energie/Wasser/Abwasser/Entsorgung

04 Gastronomie/Hotellerie
05 Gesundheit/Soziales
06 Industrie

07 Handwerk
08 Industriennahe Dienstleistungen
09 Sonstiges

In der Dimension *Personenbezogene Schutzmaßnahmen* wird in allen Branchen der Schutz durch die Klärung von *Zuständigkeiten* am weitesten umgesetzt. Die meisten Branchen weisen hier einen Indexwert über 6 auf und sind damit ‚eher geschützt‘. Ausnahmen bilden die Gastronomie/Hotellerie (Indexwert 4,69) sowie das Handwerk (5,53). *Integritätsprüfungen* spielen für die meisten Unternehmen nur eine sehr geringe Rolle. Die Indexwerte liegen je nach Branche zwischen 2,15 und 3,93. *Integritätsprüfungen* haben den zweitschlechtesten Indexwert bei allen Indikatoren. Deutliche Unterschiede ergeben sich im Bereich *Sensibilisierung und Schulung*. Während die Branchen „Energie/Wasser/Abwasser/Entsorgung“ (4,64) und „Gesundheit/Soziales“ (4,15) ‚teilweise geschützt‘ sind, werden in der Branche „Gastronomie/Hotellerie“ sehr wenige *Sensibilisierungen und Schulungen* durchgeführt. Der Indexwert beträgt dort 1,85, was so viel wie ‚eher nicht geschützt‘ bedeutet. Alle anderen Branchen liegen im Bereich ‚wenig geschützt‘ und damit unter einem

Wert von 4. Eine *Sensibilisierung und Schulung* zum Schutz des Unternehmens findet im „Gastronomie/Hotellerie“ und „Handwerk“ den Werten zufolge kaum statt. Erstaunlicherweise werden solche Maßnahmen auch bei den Unternehmen, die sich der Branche Industrie zurechnen, eher wenig durchgeführt.

In der Dimension *Cyberangriffsschutz* zeigen alle Branchen bei den Indikatoren *Zugriffsschutz* und *Schutz vor Cyberattacken und Datenverlust* hohe Indexwerte. Sie sind in diesem Bereich durchweg ‚eher gut‘ aufgestellt und weisen Indexwerte von 6,93 bis 8,19 auf. Lediglich die „Gastronomie/Hotellerie“ ist mit einem Wert von 4,60 deutlich schlechter geschützt. Den höchsten Wert erreicht die Branche „Energie/Wasser/Abwasser/Entsorgung“ beim *Schutz vor Cyberattacken und Datenverlust* (8,19). Dies ist auch insgesamt der höchste Wert über alle Indikatoren und Branchen. Werte über 8 lassen sich als ‚eher hoher‘ Schutz bezeichnen. Beim *Zugriffsschutz* sind

die Branchen „Energie/Wasser/Abwasser/Entsorgung“, „Gesundheit/Soziales“ sowie „Industrie“ ‚eher gut‘ geschützt. Sie kommen allesamt auf Werte von mehr als sechs. Im Bereich der *Verschlüsselung* gibt es starke Unterschiede zwischen den Branchen. Die Branche „Finanzen/Versicherungen“ setzt sehr häufig *Verschlüsselungen* ein (7,23). Demgegenüber setzen der „Handel“, die „Gastronomie/Hotellerie“ und das „Handwerk“ diese Schutzmaßnahmen kaum ein, so dass diese Branchen in der Gesamtbetrachtung nur als ‚teilweise geschützt‘ bezeichnet werden können.

In der Dimension *Physischer Gebäudeschutz* zeigt sich generell, dass der *Innere Gebäudeschutz* (4,53) besser bewertet wird als der *äußere Schutz* (3,48). Es gibt jedoch starke *Branchenunterschiede*: So hat etwa die Branche „Gesundheit/Soziales“ einen sehr geringen Indexwert beim *Äußeren Gebäudeschutz* (2,69). Dies ist vor dem Hintergrund der besonders schützenswerten Informationen überraschend. Die Branche legt hingegen Wert auf einen relativ ausgeprägten Inneren Gebäudeschutz mit einem deutlich höheren Wert von 5,23. Es ist anzunehmen, dass eine geringe Umsetzung von *äußerem Gebäudeschutz* nicht notwendigerweise aus fehlendem Bewusstsein für diese Schutzmaßnahme resultiert. Vermutlich ist weniger die Branchenzugehörigkeit, sondern vielmehr die Größe des Unternehmens ausschlaggebend.

Einordnung

Betrachtet man den jeweiligen Durchschnittswert der Indikatoren, weisen alle Branchen insgesamt einen niedrigeren Indexwert auf als 2019. Folgende Kernerkenntnisse ergeben sich aus der Branchenbetrachtung

01 Finanzen/Versicherungen (Indexwert 2021: 5,21; 2019: 6,26) Die Branche „Finanzen/Versicherungen“ ist schlechter geschützt als noch 2019 und ist damit nur noch in der Kategorie ‚teilweise geschützt‘ zugeordnet. Insbesondere im Indikatorenbereich *Richtlinien und Anweisungen* gibt es deutlichen Nachholbedarf (3,21) bei den sonst eher formalisierten Finanz- und Versicherungsunternehmen.

02 Handel (Indexwert 2021: 4,30; 2019: 4,42): Der „Handel“ gehört, wie auch schon 2019, zu den drei am wenigsten geschützten Branchen. Das Schutzniveau ist jedoch nahezu gleichgeblieben. Die Chancen des Schutzes durch *organisatorische Schutzmaßnahmen* werden nicht vollumfänglich genutzt. Und auch der *Cyberangriffsschutz* befindet sich auf dem Niveau ‚teilweise geschützt‘. Mit einem Indexwert von 1,99 bei den *externen Absicherungsmaßnahmen* erreicht die Branche einen auffallend niedrigen Wert. Gerade durch die zunehmende Bedeutung des Online-Handels sind diese Werte kritisch zu betrachten.

03 Energie/Wasser/Abwasser/Entsorgung (Indexwert 2021: 5,30; 2019: 7,34): Im Branchenvergleich erzielt die Branche „Energie/Wasser/Abwasser/Entsorgung“ den besten Indexwert mit 5,30. Der Gesamtindexwert der Branche liegt jedoch um zwei Punkte niedriger als noch 2019. 62,5 Prozent der teilnehmenden Unternehmen dieser Branche ordnen sich der KRITIS-Kategorie zu. Das deutlich geringere Schutzniveau als 2019 ist damit kritisch zu sehen, auch wenn vor allem der *Cyberangriffsschutz* überdurchschnittlich ist. Er befindet sich jedoch im Vergleich zu 2019 ebenfalls auf dem niedrigeren Niveau ‚eher stark geschützt‘ statt ‚stark geschützt‘.

04/Gastronomie/Hotellerie (Indexwert 2021: 3,12; 2019: 4,82): Die Branche „Gastronomie-/ Hotellerie“ bleibt die am geringsten geschützte Branche. Insbesondere in den beiden Dimensionen *Personenbezogene Schutzmaßnahmen* und *Cyberangriffsschutz* liegen die Unternehmen dieser Branche bis zu 2,28 Indexpunkten unter dem Durchschnitt. Bessere Werte erzielt die Branche beim *äußeren Gebäudeschutz*.

2019 wurde hier noch ein Indexwert von 1,60 erzielt. 2021 steigt der Wert auf 3,07.

05 Gesundheit/Soziales (Indexwert 2021: 4,88; 2019: 5,42): Unternehmen des Gesundheits- und Sozialsektors gehören zu den besser aufgestellten Unternehmen. Die Branche erzielt hohe Werte im *Cyberangriffsschutz* (6,97) und schützt damit insbesondere sensible Daten. Im Vergleich zu 2019 werden trotz vieler Regulationen, die dieser Branche unterworfen ist, jedoch weniger *Organisatorischen Schutzmaßnahmen* ergriffen (Indexwert 2021: 3,74,84)

06 Industrie (Indexwert 2021: 4,82; 2019: 5,10): Die „Industrie“ liegt in allen Dimensionen des Wirtschaftsschutzes leicht über dem Durchschnitt. Ihr Schutzstatus hat sich insgesamt im Vergleich zu 2019 nur leicht verschlechtert. Im Bereich *Schutz vor Cyberattacken und Datenverlust* erzielt die „Industrie“ 2021 (7,47) sogar leicht bessere Werte als noch 2019 (7,08). Es zeigt sich jedoch auch, dass die Schulungsaktivitäten und damit die Stärkung des Schutzfaktors Mensch kaum intensiviert wurden (2021: 3,95; 2019: 3,88).

07 Handwerk (Indexwert 2021: 3,80; 2019: 4,04): Das „Handwerk“ landet auch 2021 auf dem vorletzten Platz beim Schutzniveau. Es fehlt insbesondere an *organisatorischen Schutzmaßnahmen*. Auch die Aufstellung im Bereich der *Personenbezogenen Schutzmaßnahmen* (3,36), z.B. bei *Sensibilisierung und Schulung* (2,40), bietet viel ungenutztes Potential. Der *Schutz vor Cyberattacken und Datenverlust* wurde jedoch im Vergleich zu 2019 leicht verbessert (2021: 6,93; 2019: 6,13).

08 Industrienaher Dienstleistungen (Indexwert 2021: 4,53; 2019: 5,49): Auch die Industrienahen Dienstleistungen sind leicht überdurchschnittlich aufgestellt. Die Branche hat im Bereich *Sensibilisierungen und Schulungen* im Vergleich zu 2019 leicht bessere Werte und scheint damit den Fokus auf diese Schutzmaßnahme zu erhöhen (2021: 3,73; 2019: 3,11). Neben ‚eher vielen‘ Schutzmaßnahmen im Bereich *Schutz vor Cyberattacken und Datenverlust* (7,21) legt die Branche viel Wert auf die Klärung von *Zuständigkeiten* (6,54). Dies war auch bereits 2019 so, jedoch mit einem deutlich höheren Wert bei *Zuständigkeiten* (2019: 7,33)

Insgesamt zeigen sich somit branchenbezogene Unterschiede, die in den einzelnen Geschäftsmodellen begründet sein können.

Indexwerte von KRITIS-Unternehmen

i [5,04]

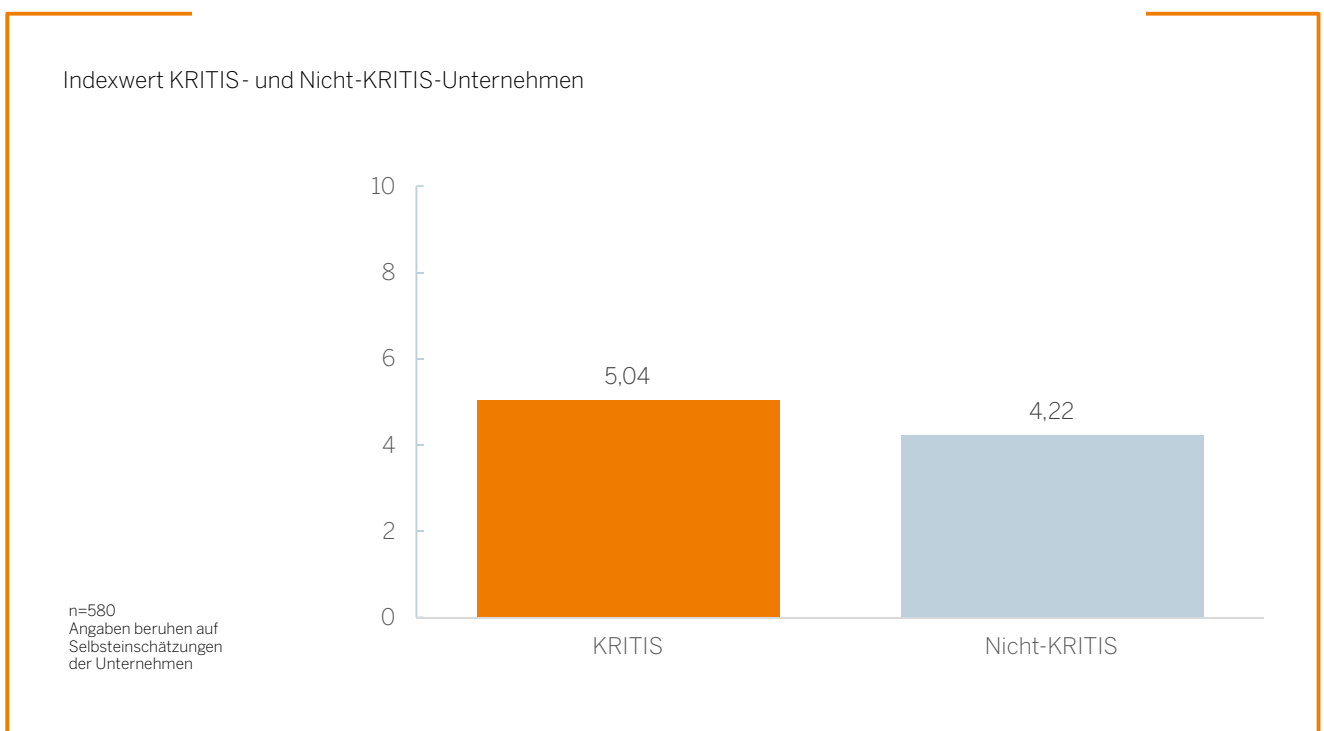


Abbildung 4: Indexwerte KRITIS- und Nicht-KRITIS-Unternehmen

Schutzbereich / Betrachtungsfeld

Die Bezeichnung „KRITIS“ steht für „Kritische Infrastruktur“. KRITIS-Unternehmen sind von besonderer Bedeutung für das staatliche Gemeinwesen. Kommt es bei Unternehmen dieser Kategorie zu einem Ausfall oder einer Beeinträchtigung, können nachhaltig wirkende Versorgungsengpässe entstehen, die im schlimmsten Fall zu erheblichen Störungen der öffentlichen Sicherheit führen oder mit anderen dramatischen Folgen einhergehen können.

Zentrale Ergebnisse

Gehört ein Unternehmen der KRITIS-Kategorie an, werden höhere Indexwerte erzielt als bei Nicht-KRITIS-Unternehmen. KRITIS-Unternehmen weisen einen durchschnittlichen Index von 5,04 auf, Nicht-KRITIS-Unternehmen von 4,22. Beide

Kategorien von Unternehmen sind damit jedoch lediglich ‚teilweise geschützt‘. Insgesamt machen die KRITIS-Unternehmen etwas mehr als ein Fünftel (21,7 %) aller Teilnehmer an der Befragung aus.

Einordnung

Der Indexwert der KRITIS-Unternehmen fällt mit 5,04 im Jahr 2021 deutlich niedriger aus als 2019 (7,20). Der Indexwert der KRITIS-Unternehmen ist damit stark gesunken. Die Tatsache, dass KRITIS-Unternehmen lediglich einen ‚teilweisen‘ Schutz aufweisen, ist bedenklich. Die Mehrheit der KRITIS-Unternehmen ist wie bereits schon 2019 den Kleinst- und Kleinunternehmen zuzuordnen (2021: 71,4 %, 2019: 85,0 %). Ob diese Unternehmen wirklich zur KRITIS-Kategorie gehören, kann nicht nachvollzogen werden. Auffällig ist im Jahr 2021, dass

KRITIS-Kleinstunternehmen mit bis zu neun Mitarbeitern auf einen Indexwert von 4,21 kommen, während 2019 die Werte in der kleinsten Unternehmenskategorie bereits bei 6,45 lagen. 2021 erzielte die Unternehmenskategorie 250-499 Mitarbeiter innerhalb der KRITIS-Unternehmen mit 5,22 die höchsten Indexwerte und ist damit schlechter geschützt als die Kleinstunternehmen 2019. Im Rahmen der Studie wurde überprüft, ob dies mit einer veränderten Branchenzugehörigkeit der KRITIS-Unternehmen zu erklären ist. Hieraus ergeben sich jedoch keine Anhaltspunkte. Grundsätzlich steigt wie bereits im Jahr 2019 das Schutzniveau der KRITIS-Unternehmen mit der Unternehmensgröße. „Große Mittelständler“ kommen auf einen Indexwert von 5,22. Im Lagebild Wirtschaftsschutz NRW 2019 lagen bereits KRITIS-Kleinstunternehmen mit einem Indexwert von 6,45 über dem Wert der „großen Mittelständler“ von 2021. Auch aus der Branchenanalyse ergeben sich keine Begründungen zur Veränderung des Schutzniveaus von KRITIS-Unternehmen. *Weitergehende Analysen zu möglichen Ursachen und zur Überprüfung der nun vorliegenden Ergebnisse sind daher sehr zu empfehlen.*

Schutzstatus nach Wichtigkeit des Schutzes von Betriebs- und Geschäftsgeheimnissen

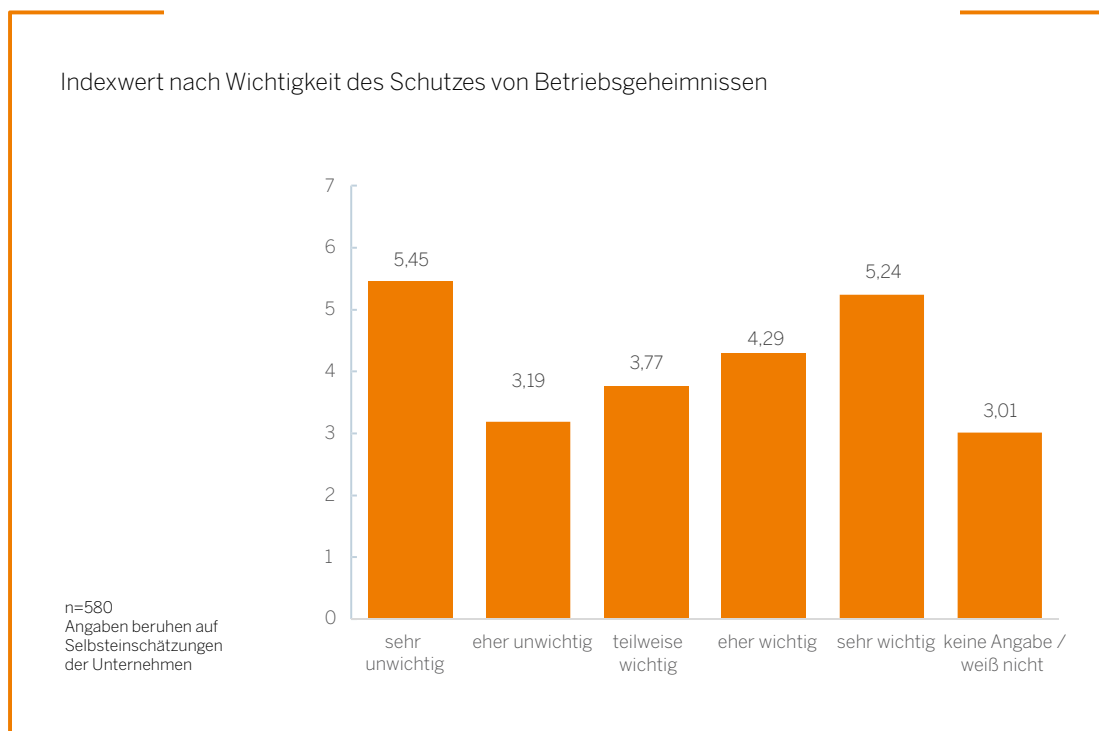


Abbildung 5: Durchschnittlicher Indexwert der Befragten je nach zugeschriebener Wichtigkeit von Betriebs- und Geschäftsgeheimnissen des Unternehmens

Schutzbereich / Betrachtungsfeld

Betriebs- und Geschäftsgeheimnisse gehören zu den sogenannten „Kronjuwelen“ eines Unternehmens. Sie gelten als besonders schützenswert. Die Studie zeigt auf, (1) ob Betriebs- und Geschäftsgeheimnissen je nach Branchen oder Unternehmensgrößen eine unterschiedliche Bedeutung zugemessen wird und (2) ob der Indexwert mit steigender Bedeutung von Betriebs- und Geschäftsgeheimnissen zunimmt.

„Energie/Wasser/Abwasser/Entsorgung“ (56,3 %, ‚eher unwichtig‘ bis ‚sehr unwichtig‘) wird die Wichtigkeit am geringsten eingeschätzt. Vor allem bei letzterer Branche ist dies bemerkenswert und es signalisiert Handlungsbedarf.

Zentrale Ergebnisse

Betriebs- und Geschäftsgeheimnissen wird in den meisten Branchen eine hohe Wichtigkeit zugemessen. Mit Ausnahme von vier Branchen, zu denen erstaunlicherweise die „Finanz- und Versicherungsbranche“ gehört, liegt die Zustimmung über 60 Prozent. In den Branchen „Gastronomie/Hotellerie“ (58,3 % ‚eher unwichtig‘ bis ‚sehr unwichtig‘), aber auch

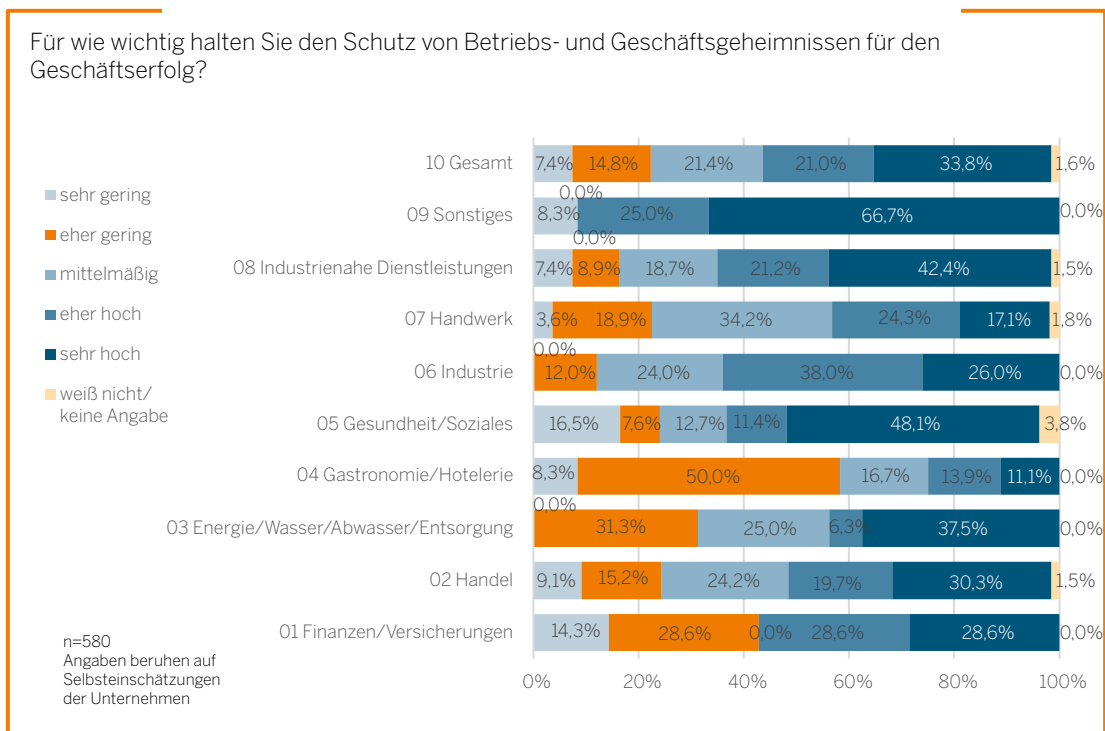


Abbildung 6: Branchenauswertung zur Wichtigkeit des Schutzes von Betriebs- und Geschäftsgeheimnissen

Besonders hoch (Antworten im Bereich ‚eher wichtig‘ bis ‚sehr wichtig‘) schätzen die Branchen „Industrie“ (64,0 %), „Industrienaher Dienstleistungen“ (63,6 %) „Gesundheit/Soziales“ (59,5 %) sowie „Handel“ (50,0 %) die Wichtigkeit von Betriebs- und Geschäftsgeheimnissen für den Unternehmenserfolg ein. 48,1 Prozent der Unternehmen aus der „Gesundheits- und Sozialbranche“ geben die Wichtigkeit im Durchschnitt sogar mit ‚sehr hoch‘ an. Ebenso stimmen 42,4 Prozent der Unternehmen der „Industrienahen Dienstleistung“ einer ‚sehr hohen‘ Wichtigkeit zu. In der „Gastronomie/Hotellerie“ sieht mehr als die Hälfte aller Unternehmen ‚keine‘ oder eine ‚eher geringe‘ Wichtigkeit von Betriebs- und Geschäftsgeheimnissen für den Unternehmenserfolg. **Insgesamt gesehen stimmen nur gut die Hälfte aller befragten Unternehmen der Aussage zu, dass Betriebs- und Geschäftsgeheimnisse ‚eher‘ oder ‚sehr wichtig‘ für den Unternehmenserfolg sind.**

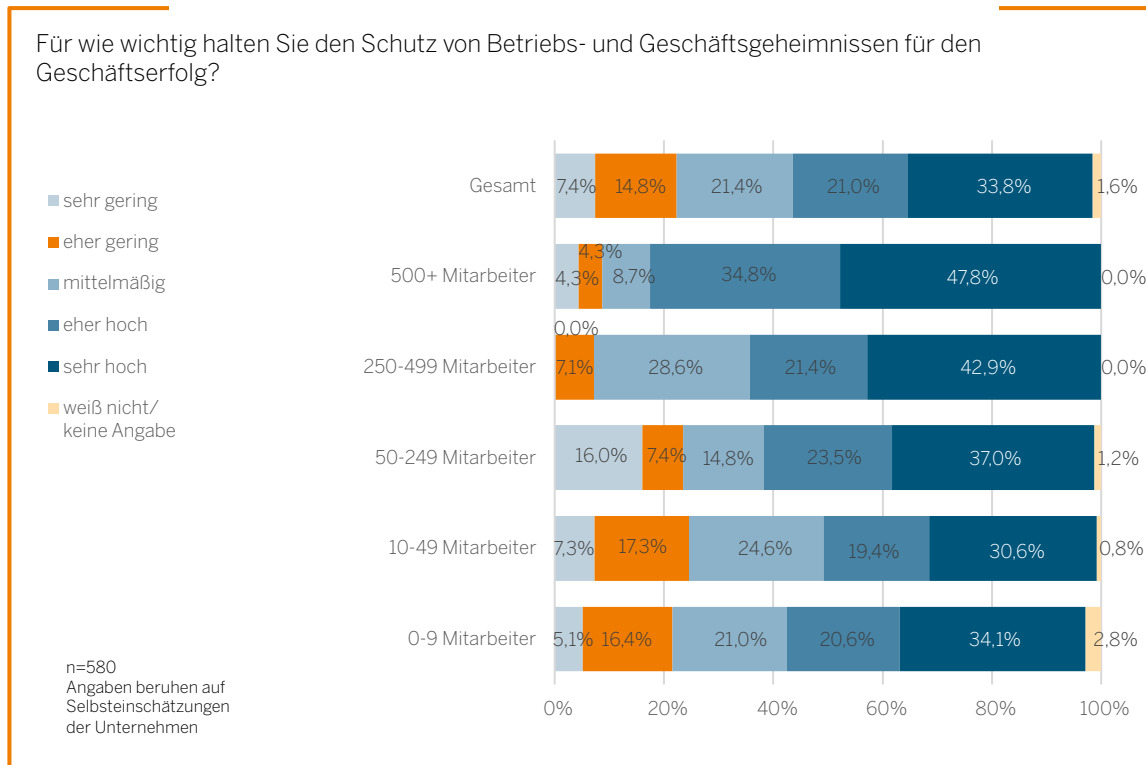


Abbildung 7: Unternehmensgrößenauswertung zur Wichtigkeit des Schutzes von Betriebs- und Geschäftsgeheimnissen

Die Wichtigkeit nach Unternehmensgröße lässt erkennen, dass die Betriebe mit einer Beschäftigtenzahl im Bereich 250-499 der Wichtigkeit mit insgesamt 64,3 % Zustimmung einen ‚eher hohen‘ (21,4 %) bis ‚sehr hohen‘ (42,9 %) Stellenwert einräumen. Die Werte sinken mit der Unternehmensgröße auf eine ‚eher hohe‘ bis ‚sehr hohe‘ Zustimmung von 50,0 Prozent. Der Wert steigt jedoch in der Kategorie der „Kleinstunternehmen“ (0-9 Mitarbeiter) wieder auf insgesamt 54,7 % an.

Je wichtiger der Schutz von Betriebs- und Geschäftsgeheimnissen für ein Unternehmen ist, desto höher ist in der Regel das Schutzniveau. Unternehmen, die nicht einschätzen können wie wichtig ihnen der Schutz dieser Geheimnisse ist, haben mit 3,01 den geringsten Indexwert. Unternehmen, die den Schutz von Betriebs- und Geschäftsgeheimnissen für ‚sehr wichtig‘ halten, weisen hingegen einen durchschnittlichen Indexwert von 5,24 auf. Sie kommen damit aber dennoch nicht über die Einstufung als ‚intermediär‘ hinaus. Eine Abweichung von der Grundtendenz gibt es bei Unternehmen, die die Bedeutung von Betriebs- und Geschäftsgeheimnissen mit ‚sehr gering‘ angeben. Sie weisen mit 5,45 sogar noch einen

höheren Indexwert auf als diejenigen, die diesem Aspekt eine ‚sehr hohe‘ Wichtigkeit beimessen.

Einordnung

Insgesamt zeigt sich, dass diejenigen Unternehmen, die Betriebs- und Geschäftsgeheimnisse für ihren Erfolg als ‚sehr gering‘ oder ‚eher gering‘ einschätzen, sich ihrer Betriebs- und Geschäftsgeheimnisse offenbar nicht bewusst sind und sie diese möglicherweise noch nicht identifiziert haben. Dies spiegelt sich in geringeren Indexwerten dieser Unternehmen wider. Die Verteilung der Indexwerte hat sich 2021 im Vergleich zum Jahr 2019 nicht verändert. In beiden Jahren hatten diejenigen Unternehmen, die Betriebs- und Geschäftsgeheimnissen eine höhere Bedeutung zumaßen, einen höheren Indexwert. Ebenso zeigte sich auch 2019 die Auffälligkeit, dass Unternehmen, die Betriebs- und Geschäftsgeheimnissen ‚gar keine‘ Bedeutung zumessen, höhere Indexwerte aufweisen als andere Unternehmen. 2021 nimmt diese Kategorie mit 5,45 sogar den höchsten Indexwert ein und weist einen höheren Wert auf als 2019 (4,76).

Selbstwahrnehmung der Unternehmen und tatsächlicher Indexwert

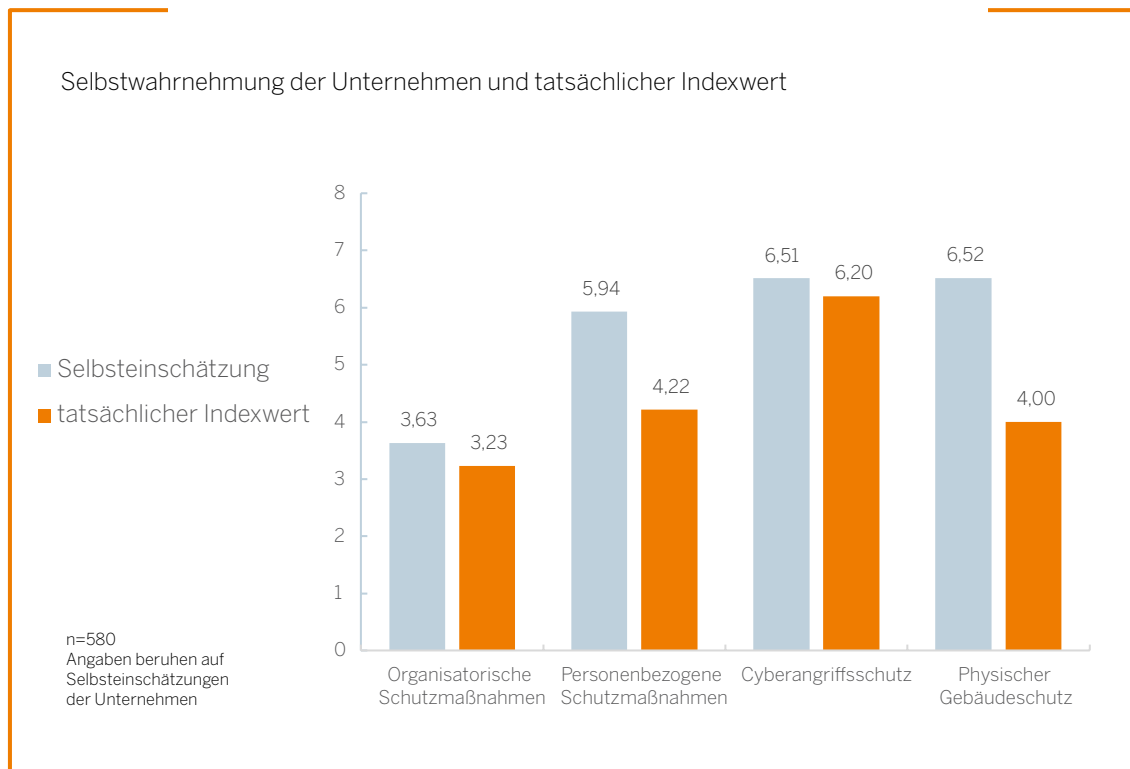


Abbildung 8: Gegenüberstellung der Selbstwahrnehmung der Unternehmen und des tatsächlichen Indexwertes

Schutzbereich / Betrachtungsfeld

Die Unternehmen wurden, bevor sie Fragen zur Umsetzung einzelner konkreter Schutzmaßnahmen erhielten, nach ihrer Selbsteinschätzung des Schutzniveaus in den einzelnen Dimensionen gefragt. Diese Selbsteinschätzung wird den Indexwerten gegenübergestellt, die aus den jeweils folgenden Fragen nach konkreten Umsetzungsmaßnahmen ermittelt wurden.

Selbstwahrnehmung und der tatsächliche Indexwert deutlich näher beieinander.

Zentrale Ergebnisse

Die Selbstwahrnehmung der Unternehmen spiegelt nicht immer den tatsächlichen Schutzstatus wider. Vielmehr überschätzt sich die Mehrheit der Unternehmen in allen vier Dimensionen. Dies wird insbesondere in den Dimensionen *Personenbezogene Schutzmaßnahmen* und *Physischer Gebäudeschutz* deutlich. Beim *Cyberangriffsschutz* und bei *Organisatorischen Schutzmaßnahmen* liegen der Wert der

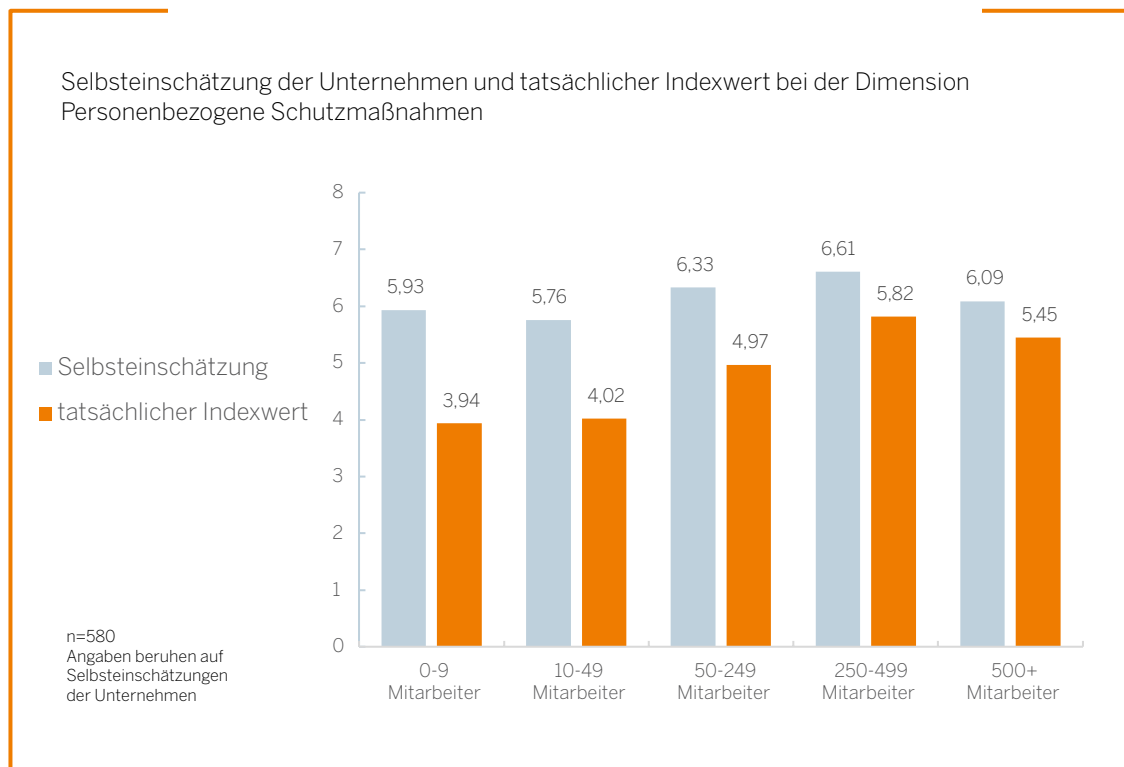


Abbildung 9: Unternehmensgrößenauswertung der Selbstwahrnehmung der Unternehmen und des tatsächlichen Indexwertes bei der Dimension *Personenbezogene Schutzmaßnahmen*

Am Beispiel der *Personenbezogene Schutzmaßnahmen* ist zudem zu erkennen, dass die Unternehmensgröße in diesem Punkt keinen Ausschlag gibt. **Unternehmen überschätzen ihren tatsächlichen Schutz unabhängig von der Zahl der Beschäftigten.** Das gleiche Ergebnis zeigt sich bei den anderen Schutzdimensionen.

Unternehmen schätzen die Bedrohung deswegen eventuell realistischer ein.

Bei den *personenbezogenen Schutzmaßnahmen* überschätzen sich die Unternehmen deutlich. Die wesentlichen Schutzfaktoren, die den Schutzfaktor Mensch wirksam werden lassen, sind offensichtlich nicht ausreichend bekannt.

Einordnung

Die Tendenz, dass Unternehmen sich besser geschützt fühlen, als es der Indexwert tatsächlich widerspiegelt, setzt sich auch im Jahr 2021 fort. Im Jahr 2019 schätzten Unternehmen sich lediglich in der Dimension *Cyberangriffsschutz* schlechter ein als der tatsächliche Indexwert. Dies hat sich **im Jahr 2021 nivelliert.** Ein Erklärungsansatz könnte sein, dass das Thema Cyberkriminalität und die damit einhergehende Alltäglichkeit von Cyberbedrohungen aktuell sehr präsent sind. Die Gefahrenwahrnehmung konzentriert sich dadurch möglicherweise verstärkt auf das Thema Cyberangriffe und

Relevanz der Wirtschaftsschutzindikatoren

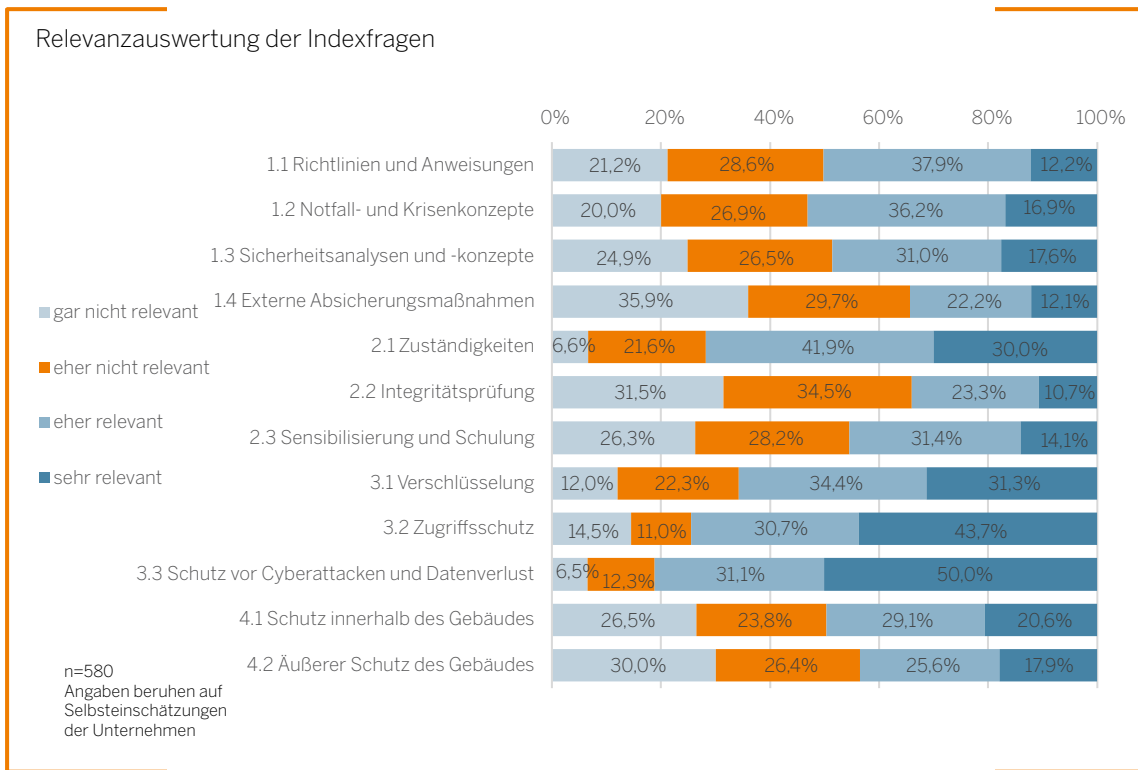


Abbildung 10: Relevanzwahrnehmung von KMU zu Themen des Wirtschaftsschutzes

Schutzbereich / Betrachtungsfeld

Die Relevanz der einzelnen Wirtschaftsschutzindikatoren spiegelt wider, welche Bedeutung die Unternehmen einzelnen Schutzmaßnahmen zuschreiben. Sie ergibt sich aus den Mittelwerten aller zugeschriebenen Relevanzbewertungen der einzelnen Fragestellungen zum jeweiligen Indikator.

Zentrale Ergebnisse

In der Summe wird deutlich, dass vor allem Maßnahmen des Cyberangriffsschutzes als besonders relevant angesehen werden. Hier liegt die Zustimmung, dass dies ‚eher‘ bis ‚sehr relevant‘ ist bei 65,7 Prozent (Verschlüsselung) bis 81,1 Prozent (Schutz vor Cyberattacken und Datenverlust). Externen Absicherungsmaßnahmen wie einer Cyberversicherung oder auch Sicherheitsaudits wird kaum Relevanz beigemessen. Hier liegt die Einschätzung, dass dies ‚gar nicht‘ bis ‚eher nicht‘ relevant ist bei 65,6 Prozent. Ebenso wenig relevant werden Integritätsprüfungen gesehen. Hier liegt die Negativzuschreibung bei 66,0 Prozent. Auch Maßnahmen

der Schulung und Sensibilisierung, Sicherheitsanalysen und -konzepte, sowie der Gebäudeschutz insgesamt werden mit einem hohen Anteil als ‚eher wenig‘ bis ‚gar nicht‘ relevant eingestuft. Eine hohe Zustimmung zur Relevanz besteht neben dem Cyberangriffsschutz beim Thema Zuständigkeiten. Dies wird von 71,9 Prozent der Unternehmen als ‚eher‘ bis ‚sehr relevant‘ eingestuft.

Einordnung

Die Relevanz wurde 2021 differenzierter erfragt als bei der ersten Ausgabe des Lagebilds. 2019 standen lediglich die Kategorien ‚relevant‘ oder ‚nicht relevant‘ zur Auswahl. 2021 konnten die Unternehmen die Relevanz anhand einer Vierskala (‚gar nicht relevant‘, ‚eher nicht relevant‘, ‚eher relevant‘ und ‚sehr relevant‘) bewerten. Die Vermutung ist naheliegend, dass die tatsächliche Umsetzung von Schutzmaßnahmen in einer direkten Korrelation zur Wahrnehmung der Relevanz von Indikatoren steht.

Aufteilung der Unternehmen nach Schutzstatus

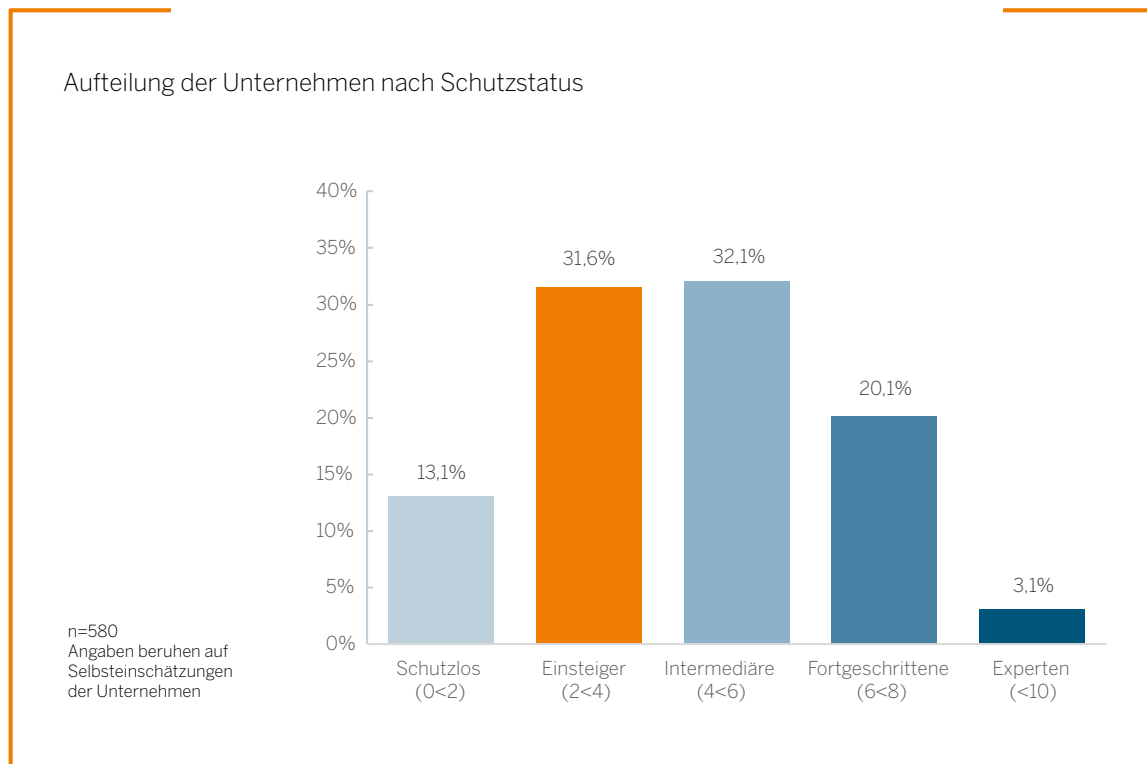


Abbildung 11: Aufteilung der Unternehmen nach Schutzstatus

Schutzbereich / Betrachtungsfeld

Die Unternehmen werden anhand der ermittelten Indexwerte einem bestimmten Schutzstatus zugeordnet. Als ‚Schutzlos‘ werden diejenigen Unternehmen bezeichnet, die einen Indexwert von weniger als 2 aufweisen, ‚Einsteiger‘ kommen auf Indexwerte zwischen 2 und 4, ‚Intermediäre‘ auf Werte im Bereich 4 bis 6, ‚Fortgeschrittene‘ weisen Indexwerte zwischen 6 und 8 auf und Experten liegen mit ihren Indexwerten zwischen 8 und 10.

Zentrale Ergebnisse

Die Einordnung der Unternehmen zeigt: **Gut drei Viertel aller Unternehmen (76,8 %) sind lediglich ‚teilweise‘ bis ‚gar nicht‘ geschützt. Ein knappes Drittel der Unternehmen ist als ‚intermediär‘ zu bezeichnen. Ein Fünftel (20,1 %) der nordrhein-westfälischen KMU sind im Sinne eines ganzheitlichen Unternehmensschutzes auf ‚fortgeschrittenem Niveau‘. Lediglich drei von zehn Unternehmen sind als ‚Experten‘ zu bezeichnen. Mehr als jedes achte Unternehmen ist ‚schutzlos‘.** Insgesamt

kann festgehalten werden, dass ein Viertel (23,2 %) aller befragten Unternehmen in die Kategorien ‚Fortgeschrittene‘ und ‚Experten‘ beim Thema Wirtschaftsschutz fällt. Aber selbst bei diesen Unternehmen besteht noch Optimierungspotenzial. Bei den Unternehmen und Betrieben, die den ‚intermediären‘ Status repräsentieren oder als ‚Einsteiger‘ und vor allem ‚Schutzlose‘ einzustufen sind, ist der Bedarf nach einer Erhöhung des Schutzniveaus jedoch ungleich höher.

Es zeigt sich, dass die Mehrheit der Branchen ‚Finanzen/Versicherungen‘, ‚Energie/Wasser/Abwasser/Entsorgung‘ und ‚Industriennahe Dienstleistungen‘ einen hohen Schutzstatus (Kategorien ‚Fortgeschrittene‘ und ‚Experten‘) aufweisen, während der überwiegende Teil der Unternehmen in den Branchen ‚Handel‘, ‚Gastronomie/Hotellerie‘ und ‚Handwerk‘ in die Kategorien ‚Schutzlose‘ oder ‚Einsteiger‘ fallen. Ein Drittel der insgesamt als ‚schutzlos‘ bezeichneten Unternehmen gehören in die Rubrik ‚Handwerk‘. Die Branchen ‚Industrie‘ sowie ‚Gesundheit/Soziales‘ weisen am meisten ‚Intermediäre‘ aus. Hier finden sich darüber hinaus

zu ähnlichen Anteilen gut geschützte und schlecht geschützte Unternehmen.

Einordnung

Die grundsätzliche Tendenz, dass bestimmte Branchen besser geschützt sind als andere, besteht auch im Jahr 2021 fort. Insgesamt hat im Vergleich zum Jahr 2019 der Anteil der „Schutzlosen“ zugenommen. Er steigt von 7,1 Prozent um sechs Prozent auf 13,1 Prozent. Diese Entwicklung ist vor dem Hintergrund einer steigenden Bedrohungslage durch Angriffe auf Unternehmen bedenklich. Die Wahrscheinlichkeit, dass ein Angriff bei „schutzlosen“ Unternehmen erfolgreich verläuft und ein ernsthafter Schaden in den Unternehmen entsteht, ist hoch. Letztlich zeigt sich, dass gut drei Viertel aller Unternehmen stark gefährdet sind, da auch der Anteil der „Experten“ und „Fortgeschrittenen“ nur noch bei 23,2 Prozent statt 28,4 Prozent in 2019 liegt. Es findet damit eine Verschiebung hin zu Einsteigern und Intermediären statt. Insgesamt haben 76,8 Prozent aller kleinen und mittleren Unternehmen in NRW Nachholbedarf in den vier Dimensionen und den dazugehörigen Indikatoren der Unternehmenssicherheit.

Index nach Unternehmensgröße

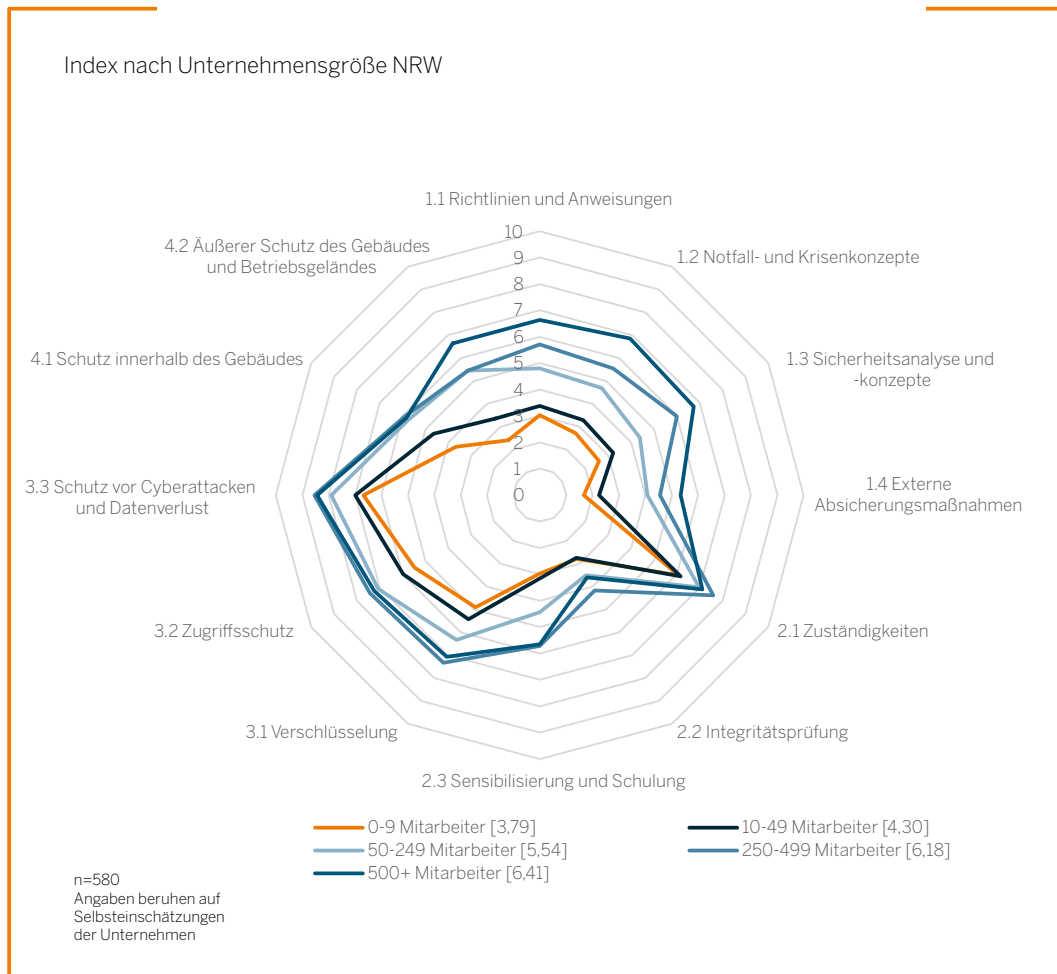


Abbildung 12: Index nach Unternehmensgröße NRW

Schutzbereich / Betrachtungsfeld

Der Größenindex mittelständischer Unternehmen in NRW gibt auf Basis von Selbsteinschätzungen wieder, wie umfassend Schutzmaßnahmen in den einzelnen Dimensionen bei Unternehmen unterschiedlicher Größen umgesetzt werden. Betrachtet werden die Unternehmensgrößen „Kleinstunternehmen“ (0-9 Mitarbeiter), „Kleinunternehmen“ (10-49 Mitarbeiter), „Größere Mittelständler“ (50-249 Mitarbeiter) und „Große Mittelständler“ (250-499 Mitarbeiter).

Zentrale Ergebnisse

Die generalisierende Betrachtung nach Unternehmensgrößen zeigt deutlich: Je kleiner ein Unternehmen, desto weniger

Maßnahmen werden in Bezug auf den Wirtschaftsschutz ergriffen. Mit zunehmender Größe steigt der Indexwert. „Kleinstunternehmen“ sind mit einem Indexwert von 3,79 ‚eher wenig geschützt‘, während „große Mittelständler“ auf einen Indexwert von 6,18 kommen und damit ‚eher geschützt‘ sind. Deutlich wird zudem, dass der Indexwert mit steigender Unternehmensgröße bei allen Indikatoren zunimmt. Die Linien im Netzdiagramm bewegen sich mit zunehmender Größe gleichmäßig nach außen. Die Verteilung der Umsetzung einzelner Maßnahmen bleibt damit jeweils auf einem anderen Niveau gleich.

Tabelle 7: Indexwerte der Dimensionen und Indikatoren nach Unternehmensgröße

Dimensionen und Indikatoren	000 -009	010 -049	050 -249	250 -499	500 und mehr
1. Organisatorische Schutzmaßnahmen	2,50	3,03	4,49	5,45	6,39
1.1 Richtlinien und Anweisungen	3,03	3,38	4,81	5,71	6,63
1.2 Notfall- und Krisenkonzepte	2,72	3,29	4,69	5,54	6,85
1.3 Sicherheitsanalyse und -konzepte	2,59	3,20	4,38	5,98	6,74
1.4 Externe Absicherungsmaßnahmen	1,65	2,24	4,07	4,55	5,33
2. Personenbezogene Schutzmaßnahmen	3,94	4,02	4,97	5,82	5,45
2.1 Zuständigkeiten	6,05	6,14	6,98	7,59	7,12
2.2 Integritätsprüfungen	2,78	2,74	3,50	4,17	3,59
2.3 Sensibilisierung und Schulung	2,98	3,17	4,43	5,71	5,65
3. Cyberangriffsschutz	5,69	6,14	7,11	7,77	7,58
3.1 Verschlüsselung	4,89	5,43	6,34	7,32	7,07
3.2 Zugriffsschutz	5,48	5,99	7,09	7,44	7,25
3.3 Schutz vor Cyberattacken und Datenverlust	6,68	6,99	7,90	8,54	8,43
4. Physischer Gebäudeschutz	3,05	4,00	5,59	5,69	6,24
4.1 Schutz innerhalb des Gebäudes	3,69	4,66	5,74	5,94	5,84
4.2 Äußerer Schutz des Gebäudes und Betriebsgeländes	2,42	3,35	5,45	5,45	6,63
Index nach Größe	3,79	4,30	5,54	6,18	6,41

Betrachtet man in der Dimension *Organisatorische Schutzmaßnahmen* das Thema *Richtlinien und Anweisungen* nach Unternehmensgröße, fällt auf: „Kleinstunternehmen“ weisen deutlich geringe Indexwerte auf als „große Mittelständler“. Sie stellen ‚eher wenige‘ *Richtlinien und Anweisungen* auf und kommen auf einen Indexwert von 2,50, während dieses Thema mit zunehmender Unternehmensgröße an Bedeutung gewinnt. „Große Mittelständler“ kommen auf einen Wert von 5,45. Darüber hinaus sind „Kleinstunternehmen“ kaum im Falle eines Angriffs durch externe Maßnahmen abgesichert. Hier wird gerade einmal ein Indexwert von 1,65 erreicht. Auch „Kleinunternehmen“ kommen lediglich auf einen Wert von 2,24. Dies ist kritisch, da die Auswertung zu erfolgreichen Angriffen zeigt, dass auch unter den teilnehmenden Unternehmen einzelne „Kleinst- und Kleinunternehmen“ bereits Opfer erfolgreicher Ransomware-Angriffe geworden sind (vgl. Abschnitt „Cyberangriffe und -angriffsversuche“). Entsprechend gering fallen bei den kleineren Unternehmen auch die Werte zu *Notfall- und Krisenkonzepten* (2,72 und 3,29) sowie *Sicherheitsanalysen und -konzepten* (2,59 und 3,20) aus.

63,5 Prozent der „Kleinstunternehmen“ sehen sich bei den Schutzmaßnahmen *Richtlinien und Anweisungen* ‚schlecht‘ aufgestellt. Bei den „großen Mittelständlern“ ist dies immerhin noch ein Viertel der Unternehmen (28,6 %).

In der Dimension der *Personenbezogenen Schutzmaßnahmen* sind alle Unternehmensgrößen beim Indikator *Zuständigkeiten* besonders gut aufgestellt. Sie fallen durchweg in die Kategorie ‚eher gut geschützt‘. Gerade bei „Kleinst- und Kleinunternehmen“ zeigt sich jedoch, dass sehr wenig Maßnahmen zur *Sensibilisierung und Schulung* von Mitarbeitern für mögliche Angriffe und Bedrohungen stattfinden. Mit Werten von 2,98 und 3,17 sind diese Unternehmen in dem Bereich ‚eher schlecht‘ aufgestellt. Aber auch die „größeren“ und „großen Mittelständler“ kommen hier lediglich auf Werte von 4,43 und 5,71 und sind damit nur ‚mittelmäßig‘ aufgestellt. Da der Mensch einen entscheidenden Faktor bei der Vermeidung von Angriffen oder Bedrohungen für Unternehmen darstellt, sind diese Werte kritisch zu sehen.

„Große Mittelständler“ sind besonders gut in der Dimension *Cyberangriffsschutz* aufgestellt. Bei einem Indexwert von 7,77 sind sie ‚eher gut‘ und fast schon ‚sehr gut‘ aufgestellt. Insbesondere im Bereich *Schutz vor Cyberattacken und Datenverlust* erzielen „große Mittelständler“ einen Wert von 8,52, was bereits einem ‚sehr hohen‘ Schutz entspricht. Vor dem Hintergrund rasant steigender Zahlen erfolgreicher Cyberangriffe muss diesem Punkt eine erhebliche Bedeutung zugemessen werden und verlangt insgesamt sicherlich noch größere Anstrengungen.

Selbst die „Kleinunternehmen“ mit 10 bis zu 49 Mitarbeitern geben an, beim *Cyberangriffsschutz* überdurchschnittlich gut aufgestellt zu sein (6,14). Dies stellt jedoch lediglich den technischen Schutz dar. Betrachtet man den geringen Wert bei *Sensibilisierungen und Schulungen* von Mitarbeitern (3,17), können sich trotz gezielter Investitionen in die IT Lücken für die Angreifer ergeben. „Kleinstunternehmen“ mit bis zu neun Mitarbeitern sind lediglich ‚teilweise‘ geschützt (5,69).

Der *Physische Gebäudeschutz* ist bei kleineren Unternehmen oft nur schwach ausgeprägt. Viele Unternehmen dieser Größenkategorie haben ihr Gebäude bzw. das Betriebsgelände kaum vor äußeren Angriffen geschützt (Indexwerte 2,42 und 3,35 bei *Äußerer Gebäudeschutz*). Je größer das Unternehmen ist, desto mehr Wert wird auf *äußeren und inneren Gebäudeschutz* gelegt.

Einordnung

Insgesamt ist die Tendenz der Schutzniveaus geordnet nach Unternehmensgrößen im Vergleich von 2021 zu 2019 gleichgeblieben. Je kleiner Unternehmen sind, desto schlechter ist der Schutz. In der Kategorie *Schutz vor Cyberattacken und Datenverlust* haben sich die „Klein- und Kleinstunternehmen“ jedoch leicht verbessert. Sie kommen 2021 auf Werte von 6,68 und 6,99 im Vergleich zu 6,34 und 6,83 im Jahr 2019.¹⁰ Bei den „großen Mittelständlern“ ist der Wert nahezu unverändert bei 8,54 statt 8,50.

Während 2019 der *Physische Gebäudeschutz* bei „Kleinst- und Kleinunternehmen“ die Dimension mit der insgesamt

geringsten Ausprägung darstellte, ist dies 2021 die Dimension *Organisatorische Schutzmaßnahmen*.

Bei den „großen Mittelständlern“ fallen vor allem die Werte in den Bereichen *Verschlüsselung* mit 7,32 (2019: 8,01) und *Zugriffsschutz* mit 7,44 (2019: 8,75) schlechter aus. Gerade die Unternehmen mit 50 bis 249 Mitarbeitern weisen deutlich weniger Schutz im Bereich der *Personenbezogenen Schutzmaßnahmen* auf. 2019 lag der Wert hier bei 5,84. 2021 wird nur noch ein Wert von 4,97 erreicht. Insgesamt kann gerade bei der Kategorie *Personenbezogene Schutzmaßnahmen* ein Pandemie-Effekt nicht ausgeschlossen werden. Gestützt auf vermehrtes Homeoffice oder mobiles Arbeiten, weniger Schulungs- und Weiterbildungsangebote sowie weniger Neueinstellungen, Besucher und Kontakte zu Geschäftspartnern kann angenommen werden, dass den Unternehmen generell weniger Maßnahmen in diesen Bereichen notwendig erscheinen.

¹⁰ Hinweis: 2021 wurde zwischen den Größenkategorien 0-9 Mitarbeiter und 10 bis 49 Mitarbeiter unterschieden. 2019 lagen die Kategorien bei 0-19 und 20 bis 49 Mitarbeiter. Insgesamt gesehen hat sich der Indexwert jedoch verbessert.

3.2 Fokus: Mobiles Arbeiten und Homeoffice

Wesentliche Erkenntnisse

Mobiles Arbeit und Homeoffice als neue Arbeitsform in der Corona-Pandemie.

Die Corona-Pandemie hat viele Unternehmen gezwungen, neue Wege der Zusammenarbeit zu finden. Vielfach wird von einem Digitalisierungsschub gesprochen. Durch die Verlagerung von Arbeit in das Homeoffice oder durch die Nutzung des mobilen Arbeitens stellen sich verstärkt Sicherheitsfragen wie der Schutz mobiler Endgeräte, des öffentlichen oder häuslichen WLANs, der Zugriff von außen auf Systeme und Programme und die Sicherheit genutzter Plattformen oder Kommunikationswege. Der Fokusteil beleuchtet, inwiefern die Unternehmen ihren Digitalisierungsstand und entsprechend auch den Unternehmensschutz auf diese Situationen hin angepasst haben bzw. zukünftig anpassen wollen.

Mobiles Arbeiten oder Homeoffice werden bei der Mehrheit der Unternehmen fester Bestandteil. Digitalisierungsstand und Sicherheit gewinnen nur sehr verhalten an Bedeutung.

Vor Beginn der Corona-Pandemie hat die Mehrheit der mittelständischen Unternehmen ‚gar kein‘ oder ‚eher wenig‘ Homeoffice oder mobiles Arbeiten ermöglicht (62,4 %). Dies hat sich durch die teilweise erzwungene Erfahrung in der Pandemie deutlich verändert. Bei mehr als 60 Prozent der Unternehmen wird dies zukünftig zumindest teilweise möglich sein. Auch wenn dann deutlich mehr räumlich flexibel gearbeitet werden kann, geben mehr als die Hälfte der Unternehmen an, dass das Thema IT-Sicherheit im Unternehmen ‚gar nicht‘ oder ‚eher wenig‘ an Bedeutung gewonnen hat. Dies überrascht vor dem Hintergrund, dass von der Mehrheit der Unternehmen zumindest ‚teilweise‘ in neue IT-Infrastruktur oder auch die Digitalisierung interner Prozesse investiert wurde. Unternehmen begegnen dieser Veränderung mit der Aufstockung von Ressourcen (finanziell, zeitlich und personell) für die Unternehmenssicherheit.

Unternehmen setzen auf technischen Schutz. Sie widmen dem Schutzfaktor Mensch immer noch keine hinreichende Aufmerksamkeit.

Während im *Cyberangriffsschutz* eine zunehmende Bedeutung gesehen wird, wird dem Schutzfaktor Mensch immer noch eine deutlich geringere Bedeutung zugemessen. Dass erfolgreiche Cybersicherheit neben dem technischen Schutz in einem hohen Maße von der Sensibilisierung und Handlungssicherheit der Mitarbeiter abhängt, wird von den Unternehmen noch nicht immer erkannt. Jedes vierte Unternehmen ermittelt zwar kontinuierlich Handlungsbedarfe für die Unternehmenssicherheit und stellt mehr Ressourcen bereit, jedoch wird der Fokus deutlich auf den technischen Schutz gelegt, während Schulungen und Sensibilisierungen bei Mitarbeitern nur in einem geringen Maße stattfinden. Der Schutzfaktor Mensch, der bei mobilem Arbeiten und im Homeoffice noch stärker an Bedeutung gewinnt, wird damit zu wenig berücksichtigt.

Eine Sensibilisierung für Sicherheitsrisiken bei flexiblen Arbeitsorten gewinnt an Bedeutung.

Es zeigt sich, dass es wichtig ist, Unternehmen für neue Angriffsmöglichkeiten, die durch mobiles Arbeiten und Homeoffice entstehen können, zu sensibilisieren. Daher empfiehlt es sich, Schulungen anzubieten, die dieses Thema fokussieren. Des Weiteren erscheint eine Sensibilisierung der Unternehmen mit schriftlichen Informationen oder Vortragsveranstaltungen durch unternehmensnahe Institutionen hilfreich. Ein großer Teil der Unternehmen bevorzugt mobile Formate für diese Themen.



Entwicklung von mobiler Arbeit und Homeoffice im Vergleich zu Vor-Corona-Zeiten

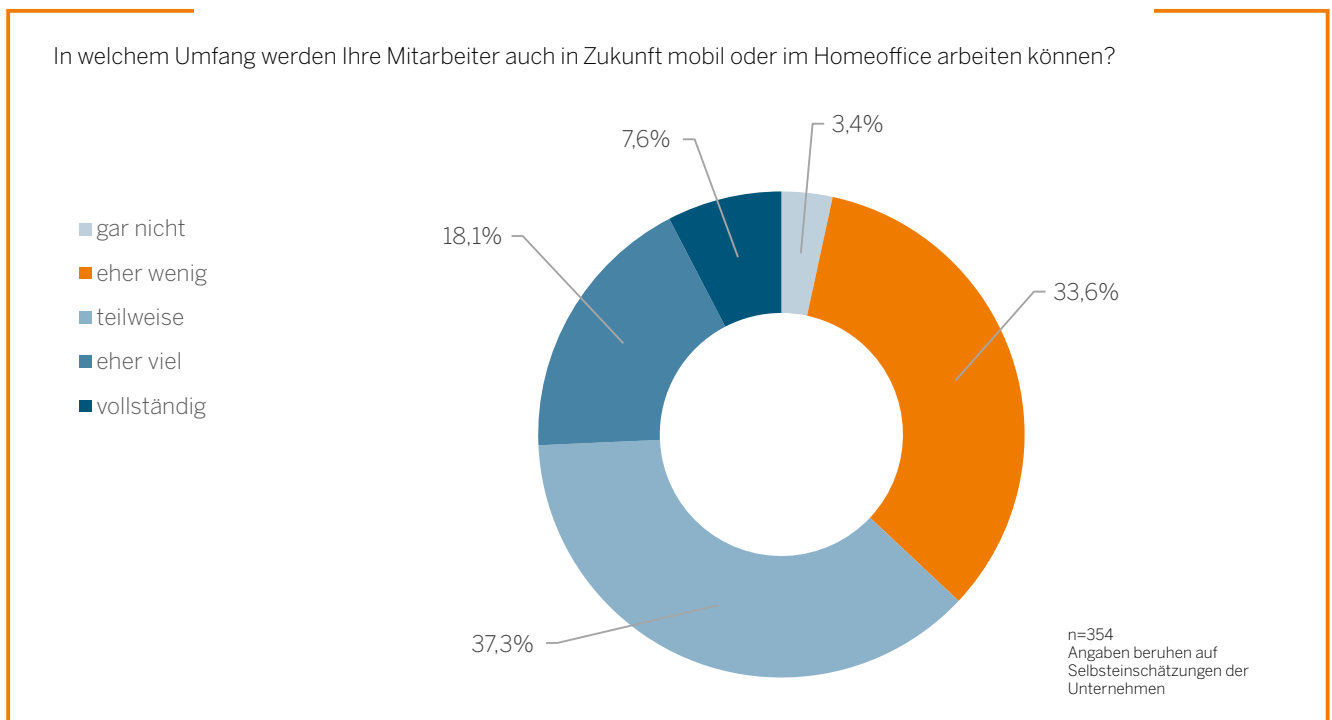


Abbildung 13: Allgemeine Auswertung zum zukünftigen Angebot von mobilem Arbeiten und Homeoffice

Schutzbereich / Betrachtungsfeld

Um während der Corona-Pandemie arbeitsfähig zu bleiben, waren und werden Unternehmen teil- und zeitweise gezwungen, Homeoffice oder mobiles Arbeiten zu ermöglichen. Im Rahmen der Studie wurde danach gefragt, inwiefern das mobile Arbeiten oder Homeoffice ein fester Bestandteil in Unternehmen bleiben wird. Da sich durch die Verlagerung des Arbeitsortes neue Sicherheitsrisiken ergeben können, sind Erkenntnisse darüber wichtig, wie hoch der Anteil betroffener Unternehmen sein wird.

Zentrale Ergebnisse

Das Ausmaß mobilen Arbeitens und der Nutzung von Homeoffice hat sich durch die Corona-Pandemie verändert.¹¹

Machten vor der Pandemie noch 62,4 Prozent der Unternehmen ‚kaum‘ oder ‚gar keinen‘ Gebrauch von diesen Arbeitsformen, wollen zukünftig nur noch 37,0 Prozent der Unternehmen diese ‚gar nicht‘ oder ‚kaum‘ nutzen.

Der Anteil der Unternehmen, die Homeoffice oder mobiles Arbeiten künftig ‚eher viel‘ bis ‚umfassend‘ anbieten wollen, weitet sich von 17,2 Prozent, die dies schon vor Ausbruch der Pandemie praktizierten, auf insgesamt 25,7 Prozent aus. Damit wird zukünftig jedes vierte Unternehmen flexible Möglichkeiten des Arbeitens nutzen. Rechnet man die Unternehmen

¹¹ Unter mobilem Arbeiten wird ein freies, ortsunabhängiges Arbeiten verstanden, unter Homeoffice ein fester, eingerichteter Arbeitsplatz beim Mitarbeiter zuhause.

hinzu, die dies künftig zumindest ‚teilweise‘ anbieten wollen (37,3 %), ergibt sich eine deutliche Mehrheit von 65,0 Prozent. Flexibles Arbeiten wird somit zur Unternehmensrealität in rund zwei Dritteln aller Unternehmen.

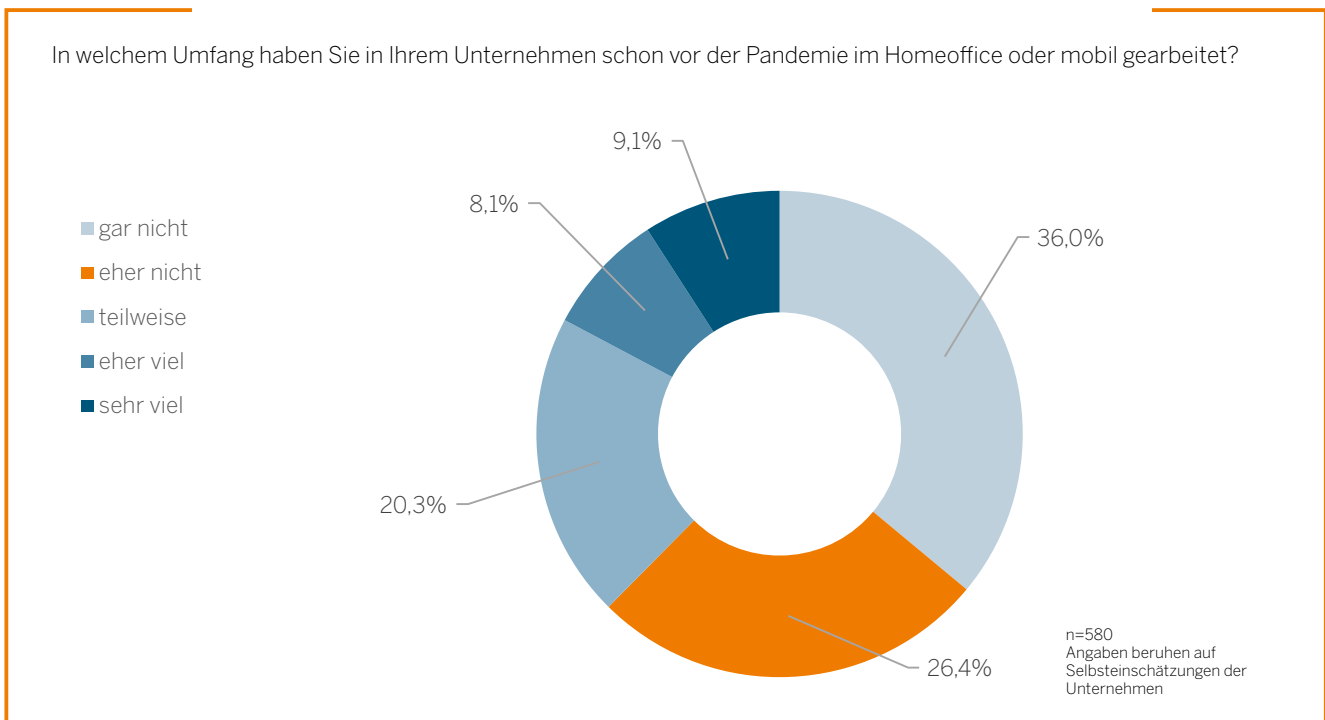


Abbildung 14: Allgemeine Auswertung zu mobilem Arbeiten und Homeoffice vor der Pandemie

Einordnung

Das Ergebnis zeigt, dass der diesjährige Fokus auf das Thema „Mobiles Arbeiten und Homeoffice“ für die Unternehmen zunehmend relevant sein wird und Unternehmenssicherheit verstärkt außerhalb der physischen Grenzen von Unternehmen gedacht werden muss.

Digitalisierungsstand in den Unternehmen

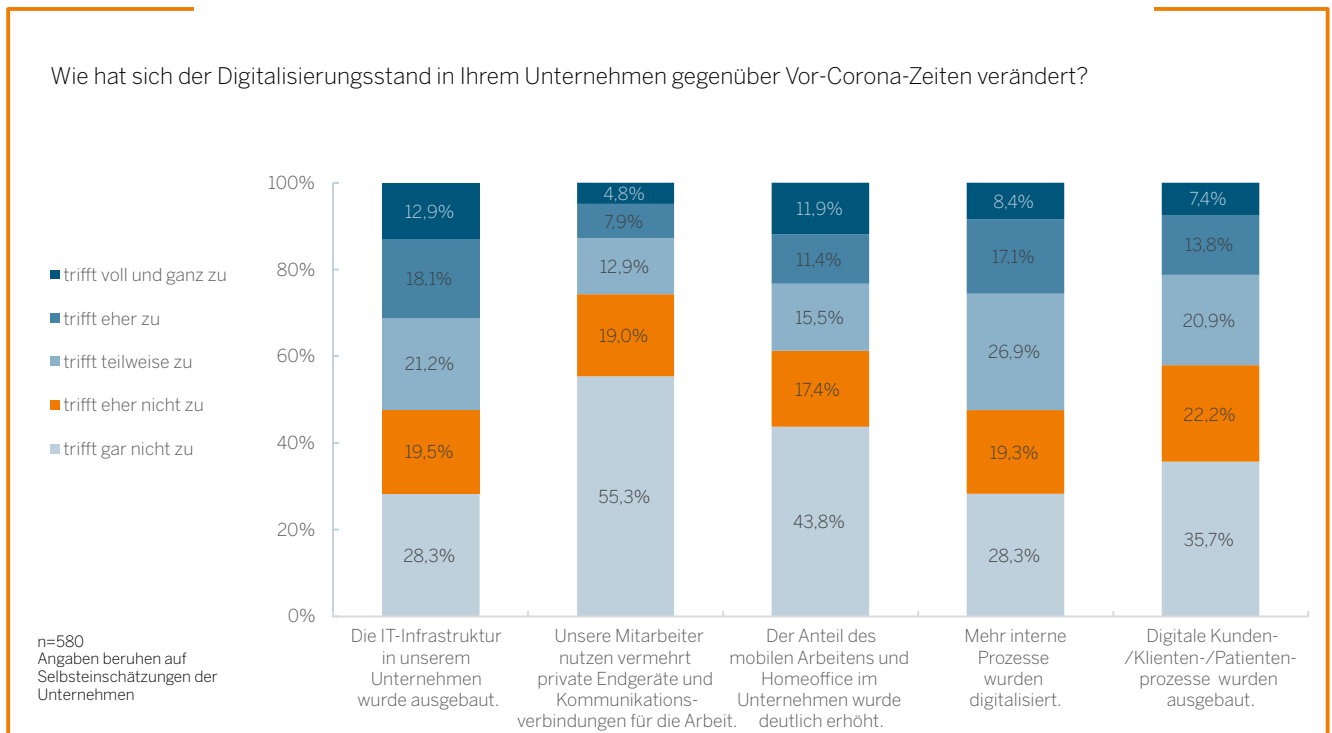


Abbildung 15: Allgemeine Auswertung zur Veränderung des Digitalisierungsstands durch die Corona-Pandemie

Schutzbereich / Betrachtungsfeld

Im Zuge der Corona-Pandemie wurde vielfach ein Digitalisierungsschub bei Unternehmen proklamiert. Dies erscheint vor allem vor dem Hintergrund des mobilen Arbeitens oder der Arbeit im Homeoffice nachvollziehbar. Da Digitalisierung und Unternehmensschutz Hand in Hand gehen, ist die Frage, ob Unternehmen tatsächlich vermehrt Prozesse oder Strukturen digitalisiert haben. Die Studie zeigt daher auf, ob Unternehmen ihren Digitalisierungsstand nach eigenen Angaben tatsächlich verändert haben.

Zentrale Ergebnisse

Die Flexibilisierung des Arbeitens hat nach Angaben der Unternehmen nur bedingt Auswirkungen auf deren Digitalisierungsstand gehabt. Im Wesentlichen wurde von fast jedem dritten Unternehmen mit Beginn der Pandemie ‚eher viel‘ oder ‚sehr viel‘ in den Ausbau der IT-Infrastruktur, also mehr Hardware, Software, Cloudlösungen oder auch IT-Sicherheitssysteme, investiert (31,0 %). Jedes vierte Unternehmen widmete sich ‚eher viel‘ oder ‚sehr viel‘ der Digitalisierung

interner Prozesse wie z. B. dem Aufbau des so genannten papierlosen Büros, der Digitalisierung von Buchhaltung, Personalprozessen, Terminverwaltungen, Auftragsmanagement oder der Digitalisierung von Wertschöpfungsprozessen wie Materialwirtschaft, Logistik und Produktion. Je größer das Unternehmen desto eher wird eine Relevanz für diese Themen gesehen. In Bezug auf die IT-Infrastruktur geben drei Viertel der großen Mittelständler mit mehr als 250 Mitarbeitern an, dass dies ‚sehr relevant‘ sei (78,9 %). Die Digitalisierung interner Prozesse halten 71,4 Prozent der großen Mittelständler für ‚eher‘ bis ‚sehr relevant‘. Bei den Klein- und Kleinunternehmen wird lediglich von 44,4 bzw. 53,6 Prozent eine ‚hohe Relevanz‘ gesehen.

Wenn flexible Arbeitsmöglichkeiten geboten werden, stehen offensichtlich auch mobile Endgeräte zur Verfügung. Das Thema „Bring Your Own Device“, die Nutzung privater Endgeräte für Zwecke der Unternehmen, spielt zumindest für knapp drei Viertel der Befragten (74,3%) ‚kaum‘ oder ‚gar keine‘ Rolle. Unternehmen aller Größen geben gleichermaßen an, keine

Relevanz für das Thema zu sehen bzw. sie lassen eine entsprechende Nutzung nicht zu.

Kundenprozesse wurden bei der Mehrheit der Unternehmen nicht angepasst, jedoch hat mehr als jedes fünfte Unternehmen Änderungen an der Schnittstelle zu den Kunden vorgenommen. 57,9 Prozent der Unternehmen geben an, keine Veränderungen bei der Möglichkeit zu Online-Bestellungen, digitalen Paymentlösungen, Help-Desks sowie virtuellen Beratungen umgesetzt zu haben. Immerhin haben aber 21,2 Prozent der Unternehmen ‚eher viele‘ oder ‚sehr viele‘ Anpassungen umgesetzt. Die Unternehmen, die viel in Kundenprozesse investiert haben, sind dabei zu 85,7 Prozent den Kleinst- und Kleinunternehmen mit bis zu 49 Mitarbeitern zuzuordnen. Kein einziger großer Mittelständler mit mehr als 250 Mitarbeitern bestätigt entsprechende Investitionen.

Einordnung

Das Ergebnis zeigt, dass vor allem die IT-Infrastruktur sowie interne Prozesse angepasst wurden. Dies betrifft insbesondere den Bedarf des Schutzes von Endgeräten, den Zugriffsschutz von außen auf Systeme sowie den sicheren Umgang mit Daten und Informationen. Private Endgeräte, Kommunikationsverbindungen, mobiles Arbeiten oder auch digitale Kunden-/Klienten-/Patientenprozesse wurden hingegen von der Mehrheit ‚gar nicht‘ oder ‚eher nicht‘ angepasst. Zwischen 12,9 und 20,9 Prozent der Unternehmen haben hier zumindest in Teilen eine Anpassung vorgenommen, was zumindest eine Weiterentwicklung auf dem Weg der Digitalisierung andeutet.

Auffällig ist, dass „Kleinst- und Kleinunternehmen“ den höchsten Anteil derjenigen bilden, die Kundenprozesse ‚viel‘ bis ‚eher viel‘ digitalisiert haben. Einige der Klein- und Kleinstunternehmen scheinen die Notwendigkeit neuer Vertriebs- oder Kommunikationskanäle mit Kunden, Klienten oder Patienten erkannt zu haben.

Dennoch ist eine verstärkte Digitalisierung bei den Unternehmen auch trotz der Erfahrungen der Corona-Pandemie grundsätzlich noch nicht im Fokus. Es besteht weiterhin Nachholbedarf im Mittelstand.

Veränderung der Unternehmenssicherheit durch mobiles Arbeiten und Homeoffice

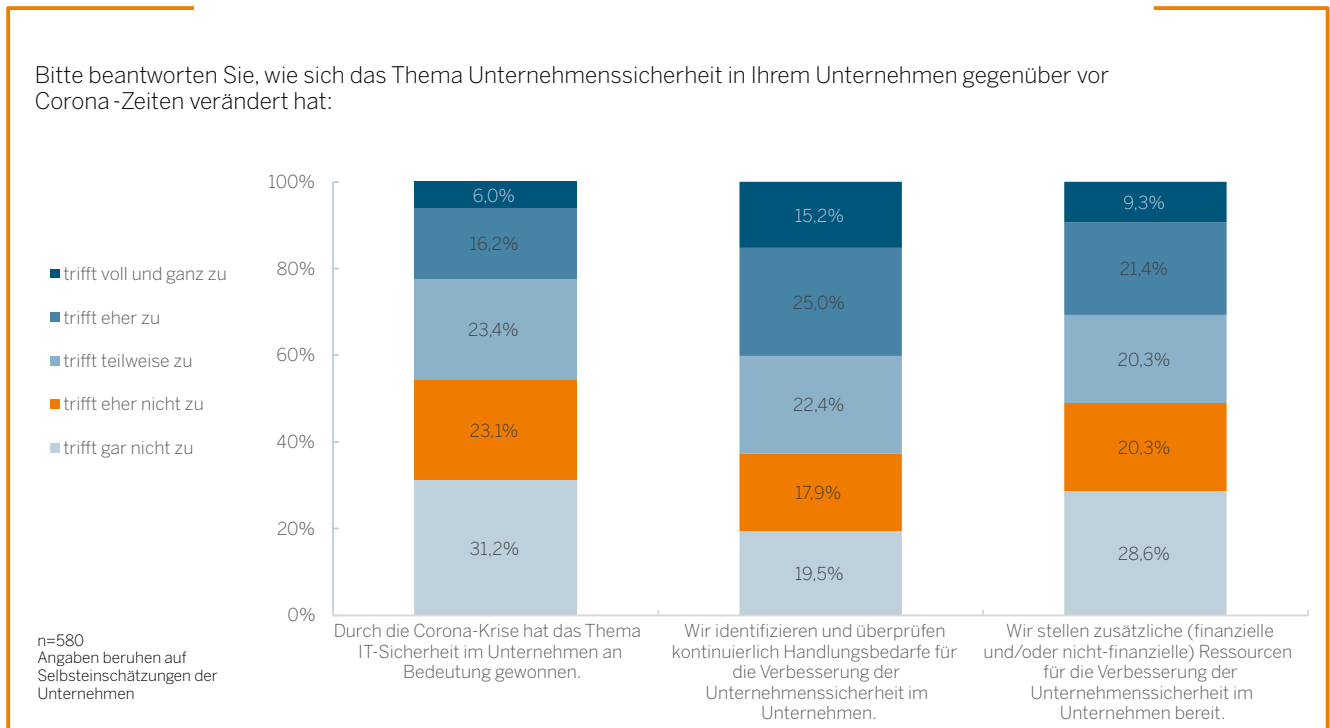


Abbildung 16: Allgemeine Auswertung zur Veränderung des Themas Unternehmenssicherheit durch die Corona-Pandemie

Schutzbereich / Betrachtungsfeld

Einhergehend mit der zunehmenden Digitalisierung und der Ausweitung von Arbeit auf Distanz, die durch die Corona-Pandemie forciert wurde, gewinnt der über die Grenzen des Unternehmens hinausgehende Schutzbedarf an Bedeutung. Die vorliegende Studie untersucht, inwiefern Unternehmen tatsächlich ihre Sicherheitsmaßnahmen an die neuen Herausforderungen des mobilen Arbeitens und des Homeoffice angepasst haben.

Zentrale Ergebnisse

Trotz der Zunahme von ortsungebundenem Arbeiten hat bei der Mehrheit der Unternehmen das Thema Unternehmenssicherheit nicht an Bedeutung gewonnen. Mehr als die Hälfte der Unternehmen (54,3 %) geben an, dass das Thema IT-Sicherheit keine größere Bedeutung durch die Einführung des mobilen Arbeitens und des Homeoffice erhalten hat. Von den 22,2 Prozent der Unternehmen, die angeben, dass die

IT-Sicherheit ‚eher viel‘ oder ‚sehr viel‘ an Bedeutung gewonnen hat, sind 72,8 Prozent „Kleinst- oder Kleinunternehmen“. Damit zeigt sich, dass zumindest einige „Kleinst- und Kleinunternehmen“ (18,6 %) die Bedeutung der IT-Sicherheit erkannt haben. „Größere Mittelständler“ sehen keinen gestiegenen Handlungsbedarf bei der IT-Sicherheit, was damit zu erklären ist, dass diese Unternehmenskategorie bereits ohnehin einen hohen Schutz aufweist (vgl. Kapitel 3.5 Auswertungen Dimension 3 Cyberangriffsschutz).

40,2 Prozent aller Unternehmen überprüfen ‚eher viel‘ oder ‚sehr viel‘ kontinuierlich Handlungsbedarfe für die Verbesserung der Unternehmenssicherheit. Die Verteilung nach Größen ist hier jedoch deutlich. Während dies nur 30,3 bzw. 38,3 Prozent der „Kleinst- und Kleinunternehmen“ machen, identifizieren 64,2 Prozent aller „großen Mittelständler“ kontinuierlich Handlungsbedarfe. „Klein- und Kleinunternehmen“

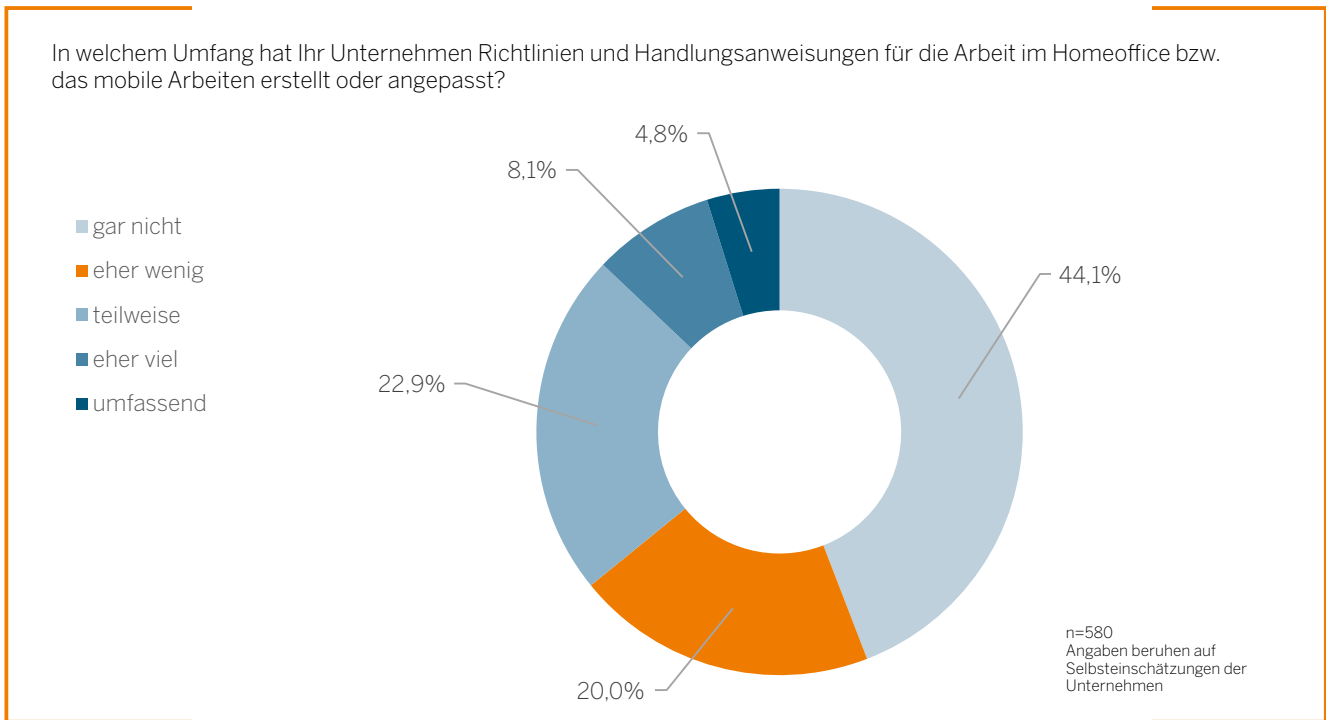


Abbildung 17: Allgemeine Auswertung zu Richtlinien und Anweisungen für mobiles Arbeiten oder Homeoffice

scheinen eher auf Sicherheitsthemen zu reagieren, während größere Unternehmen proaktiv agieren. Dies zeigt sich auch darin, dass 49,1 Prozent der „Kleinstunternehmen“ und 41,2 Prozent der „Kleinunternehmen“ diesem Thema ‚kaum‘ oder ‚gar keine‘ Relevanz zusprechen, bei den „großen Mittelständlern“ (250-499) sind es hingegen 92,9 Prozent und bei den „größeren Mittelständler“ (50-249 Mitarbeiter) 71,6 Prozent, die bei diesem Thema eine ‚eher hohe‘ bis ‚sehr hohe‘ Relevanz sehen.

Insgesamt stellen 30,7 Prozent der Unternehmen ‚eher viel‘ oder ‚sehr viel‘ mehr Ressourcen für die Unternehmenssicherheit bereit. Mehr als ein Viertel der Unternehmen (28,6 %) gibt jedoch auch an, dies ‚gar nicht‘ zu tun. „Größere Unternehmen“ sehen hier ohnehin eine hohe Relevanz und setzen Unternehmensschutz, wie auch die Indexdarstellungen zeigen, bereits mehr um als kleinere Unternehmen. „Kleinstunternehmen“ sehen zu mehr als der Hälfte (58,0 %) keine Relevanz dafür. Und auch bei „Kleinunternehmen“ von 10 bis 49 Mitarbeitern geben 49,2 Prozent an ‚eher wenig‘ bis ‚gar keine‘ Relevanz dafür zu sehen.

Dass Homeoffice oder mobiles Arbeiten zusätzliche Sicherheitsrisiken verursachen können, ist unumstritten. Umso wichtiger ist es, Mitarbeiter zu informieren und zu sensibilisieren, wie sie mögliche Risiken reduzieren können. Ein wesentlicher Baustein sind schriftliche *Richtlinien und Anweisungen*, die den Mitarbeiter Handlungssicherheit bieten.

Die Antworten der Unternehmen zeigen jedoch, dass 64,1 Prozent der Unternehmen ihre *Richtlinien und Anweisungen* für das mobile Arbeiten und das Homeoffice nicht aktualisiert haben. Einfache Möglichkeiten zur Vermeidung von Sicherheitsrisiken wie die Hinweise zu Absicherung des häuslichen WLANs, Vorgaben zur Übermittlung sensibler Daten, Anweisungen zum Zugriffsschutz für mobile Endgeräte oder auch Richtlinien zum sicheren Zugriff auf Programmen und Dateien werden damit nicht genutzt. Gerade einmal jedes achte Unternehmen (12,9 %) hat *Richtlinien und Anweisungen* entsprechend angepasst.

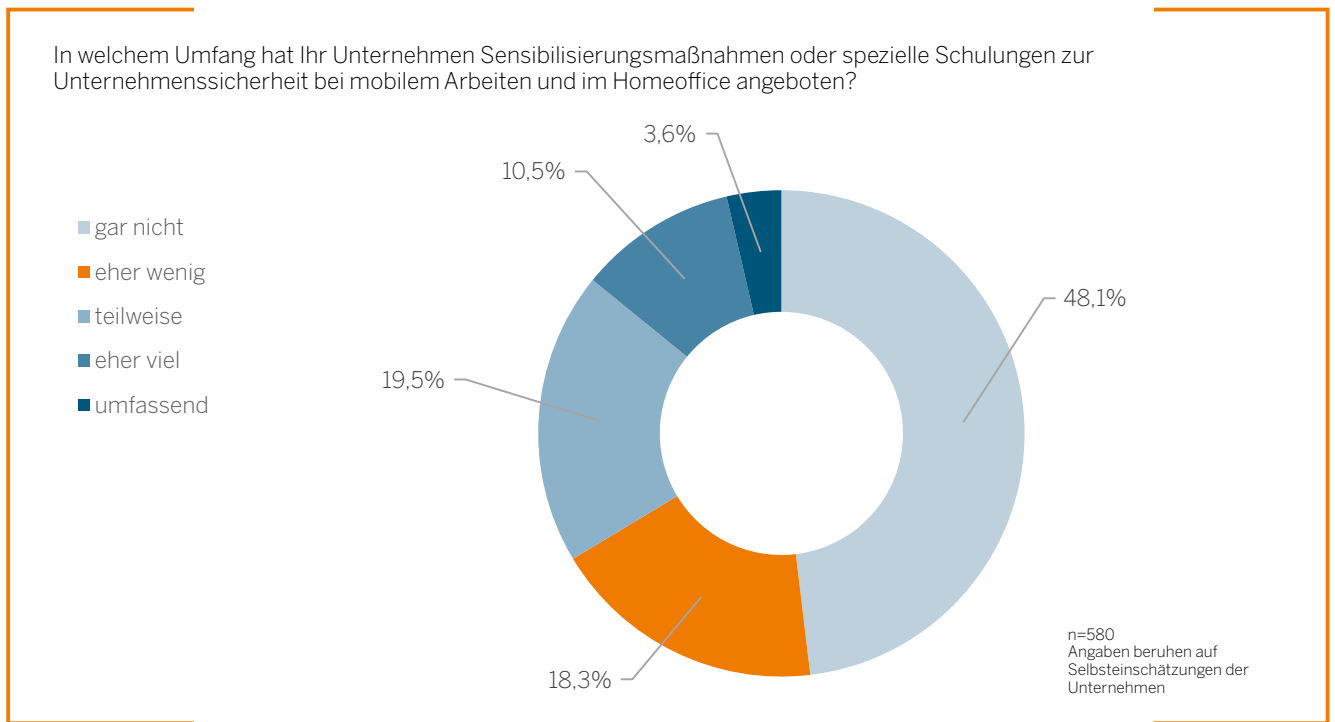


Abbildung 18: Allgemeine Auswertung zu Sensibilisierungen oder Schulungen zur Unternehmenssicherheit bei mobilen Arbeiten und im Homeoffice

Beschäftigte werden zudem ‚kaum‘ oder ‚gar nicht‘ für neue Risiken geschult oder sensibilisiert. 64,4 Prozent der Unternehmen führen keine entsprechenden Maßnahmen durch. Lediglich 14,1 Prozent der Unternehmen reagieren proaktiv und bieten *Sensibilisierungen und Schulungen* zu dem Thema Sicherheit beim mobilen Arbeiten oder im Homeoffice an.

Einordnung

Insgesamt ist festzuhalten, dass die Flexibilisierung von Arbeitsorten nur eingeschränkt mit einer Erhöhung der Schutzmaßnahmen von Unternehmen einhergeht. Zwar werden grundsätzlich mehr Ressourcen bereitgestellt, aber vorrangig wird die Notwendigkeit des Schutzes vor allem bei größeren Unternehmen gesehen. Bei den „Klein- und Kleinstunternehmen“ zeigt sich eine kleine Gruppe von Vorreitern, die dem Thema eine höhere Bedeutung zuschreibt.

3.3 Dimension 1: Organisatorische Schutzmaßnahmen

i [3,23]

Wesentliche Erkenntnisse

Organisatorische Schutzmaßnahmen als Handlungsrahmen für den Unternehmensschutz.

Die *Organisatorischen Schutzmaßnahmen* behandeln die Themen *Richtlinien und Anweisungen, Notfall- und Krisenkonzepte, Sicherheitsanalysen und -konzepte* sowie *Externe Absicherungsmaßnahmen*. Sie bilden die Handlungsgrundlage für wirksame Schutzmaßnahmen. Ohne konkrete *Richtlinien und Anweisungen* besteht Handlungsunsicherheit bei den Beschäftigten. Ein optimales Erkennen von Bedrohungen setzt sorgfältige Sicherheitsanalysen voraus. Ein umfassendes schriftliches Sicherheitskonzept ermöglicht einen ganzheitlichen Blick auf die Unternehmenssicherheit, es beschreibt Verantwortlichkeiten und die notwendigen Schutzmaßnahmen. Im Falle eines akuten Angriffs sind insbesondere *Notfall- und Krisenkonzepte* wichtig, um schnell handeln und so früh wie möglich Gegenmaßnahmen ergreifen zu können. Sollte im schlimmsten Fall ein Angriff erfolgreich gewesen sein, sind *externe Absicherungsmaßnahmen* wie eine Cyberversicherung wichtig, um finanzielle Folgen einzudämmen und eine mögliche Existenzgefährdung des betroffenen Unternehmens zu verhindern.

Organisatorische Schutzmaßnahmen sind am schlechtesten ausgeprägt. Ein großer Teil der Unternehmen misst schriftlichen Regelungen und Konzepten zum Unternehmensschutz keine besondere Bedeutung zu.

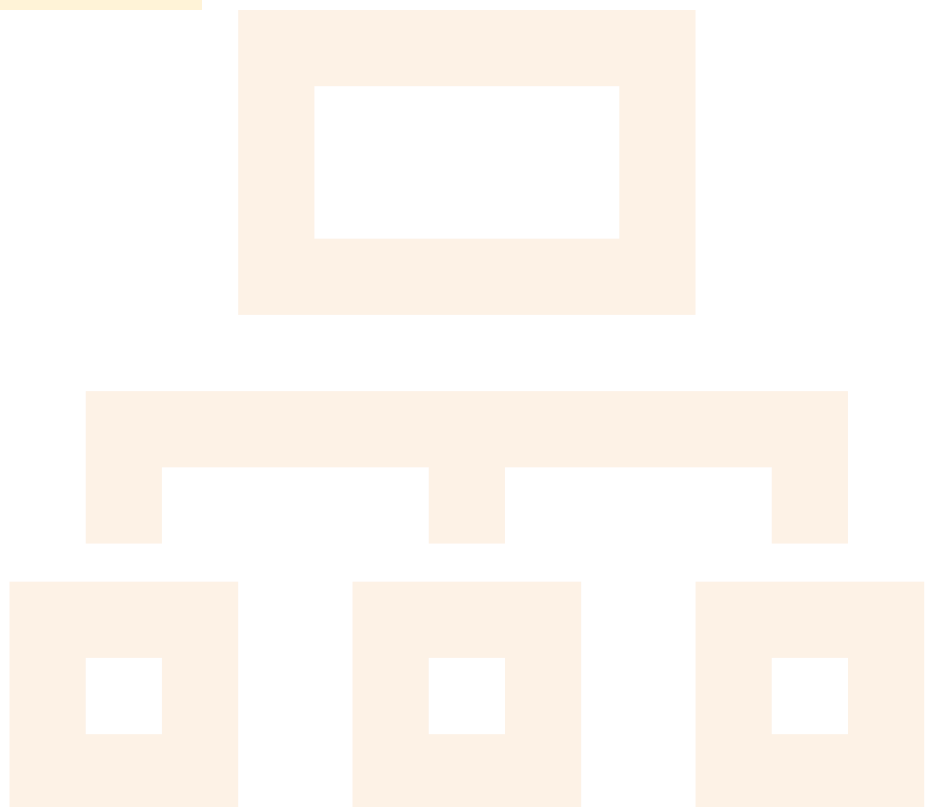
Insgesamt zeigt sich, dass *externe Absicherungsmaßnahmen* in Unternehmen kaum umgesetzt werden. Mit einem Indexwert von 2,46 ist dieser Indikator von allen am geringsten ausgeprägt. Darüber hinaus werden *Richtlinien und Anweisungen* von mehr als der Hälfte der Unternehmen nur eine geringe Relevanz zugeschrieben. Selbst Passwortrichtlinien existieren bei fast einem Drittel der Unternehmen nicht. Allenfalls Richtlinien mit Bezug zum Thema Datenschutz und Informationssicherheit werden von der Mehrheit der Unternehmen umgesetzt. *Notfall- und Krisenkonzepte* existieren bei mehr als der Hälfte der Unternehmen nicht. Schriftliche Sicherheitskonzepte sind bei mehr als 60 Prozent der Unternehmen ‚kaum‘ bis ‚gar nicht‘ vorhanden.

Eine Unterschätzung der Relevanz organisatorischer Schutzmaßnahmen erhöht das Gefährdungspotenzial.

Der Nutzen von *organisatorischen Schutzmaßnahmen* als wichtige Säule in einem ganzheitlichen Unternehmensschutz ist den Unternehmen offenbar nicht hinreichend bewusst. Dies zeigt die geringe Relevanzzuschreibung der untersuchten Aspekte. Damit ergibt sich ein erhöhtes Gefahrenpotenzial. Es werden nicht genug Maßnahmen ergriffen, um Mitarbeitern Handlungssicherheit zu geben. Bedrohungen werden nicht aufgespürt und selbst wenn sie erkannt werden, ist aufgrund fehlender *Notfall- und Krisenkonzepte* ein schnelles Handeln kaum möglich. Die Gefahr, dass Angriffe erfolgreich verlaufen, steigt dadurch. Gegen mögliche Schäden sind Unternehmen wiederum nicht abgesichert. Gerade kleinere Unternehmen scheinen die beschriebenen Maßnahmen als bürokratische Hindernisse zu sehen.

Eine gezielte Sensibilisierung insbesondere bei Kleinst- und Kleinunternehmen erscheint dringend notwendig.

Die Umsetzung von *organisatorischen Schutzmaßnahmen* ist im Vergleich zu 2019 um 0,4 Indexpunkte gesunken. Eine gewisse Relevanz derartiger Maßnahmen wird lediglich bei „großen Mittelständlern“ gesehen. Die Gefahr eines Angriff besteht jedoch bei jeder Unternehmensgröße. Deshalb sollten „Kleinst- und Kleinunternehmen“ insbesondere die Bedeutung von Sicherheitsanalysen und -konzepten und von *Notfall- und Krisenkonzepten* nähergebracht werden. Dafür bieten sich spezielle Beratungen und Sensibilisierungsmaßnahmen für Kleinst- und Kleinunternehmen, aber auch für größere Mittelständler an.



3.4 Dimension 2: Personenbezogene Schutzmaßnahmen

i [4,22]

Wesentliche Erkenntnisse

Personenbezogene Schutzmaßnahmen als Stärkung des Schutzfaktors Mensch.

Die *Personenbezogenen Schutzmaßnahmen* umfassen Schutzmaßnahmen, die sich auf den Menschen als wesentlichen Akteur des Unternehmensschutzes beziehen. Die Dimension umfasst Themen wie die Regelung von *Zuständigkeiten*, *Integritätsprüfungen* unterschiedlicher Personengruppen sowie *Schulungen und Sensibilisierungen*. Unternehmensschutz ist Chefsache. Nur wenn die strategische Zuständigkeit im Top-Management liegt, wird dem Thema die notwendige Bedeutung zugemessen. Daneben gilt es, die operativen *Zuständigkeiten* internen oder externen Spezialisten zuzuweisen. Das Handeln von Menschen kann einen entscheidenden Risikofaktor darstellen, wenn es darum geht, Betriebs- und Geschäftsgeheimnisse oder auch Hardware im Unternehmen zu schützen. Daher ist es wichtig, die Integrität neuer Mitarbeiter und Besucher sowie von Geschäftspartnern zu prüfen. Darüber hinaus können Menschen Schutzmaßnahmen nur dann optimal umsetzen, wenn sie für mögliche Bedrohungen und Angriffsformen sensibilisiert werden und entsprechende Schulungen für die richtige Anwendung der Schutzmaßnahmen erhalten.

Zuständigkeiten gut geregelt. Schulungen und Sensibilisierungen finden kaum statt.

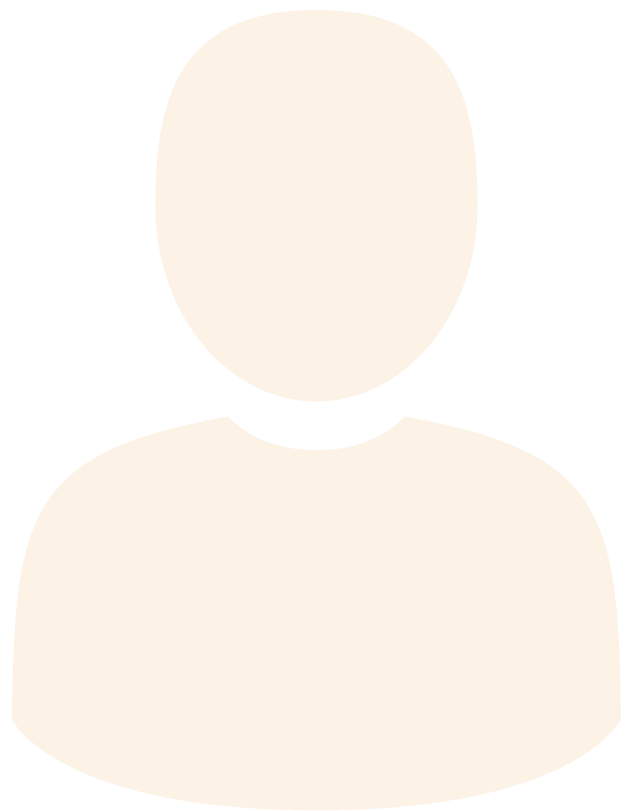
Bei der Umsetzung personenbezogener Schutzmaßnahmen zeigt sich insgesamt ein sehr ambivalentes Bild. Während die *Zuständigkeiten* in den Unternehmen ‚eher gut‘ geregelt sind (Indexwert: 6,30), sensibilisieren und schulen viele Unternehmen ihre Beschäftigten nicht hinreichend (Indexwert: 3,43). Damit wird eine wesentliche Ressource zum Schutz der Unternehmen kaum genutzt. *Integritätsprüfungen* sind für die meisten Unternehmen ‚eher wenig‘ bis ‚gar nicht relevant‘, daher werden in diesem Bereich auch kaum Maßnahmen ergriffen.

Unternehmen unterschätzen die Bedeutung des Schutzfaktors Mensch.

Der Nutzen von *Sensibilisierungen und Schulungen*, um beispielsweise der Gefahr des Social Engineerings zu begegnen, ist den Unternehmen kaum bewusst. Beinahe jedes vierte Unternehmen hält *Schulungen und Sensibilisierungen* für ‚gar nicht relevant‘ (26,3%). Dies ist umso bedenklicher, weil 54,5 Prozent der Unternehmen angeben, dass ihre Mitarbeiter nur ‚teilweise‘ bis ‚gar nicht‘ über mögliche Schutzmaßnahmen informiert sind. Dieser Wert ist im Vergleich zu 2019 noch einmal um sieben Prozent gestiegen. Je weniger Mitarbeiter über potentielle Bedrohungen und Schutzmaßnahmen wissen, umso leichter haben es Angreifer mit Methoden, die sich die Gutgläubigkeit und Unbedarftheit von Beschäftigten zunutze machen.

Diebstahl in den Unternehmen kein Thema.

90 Prozent der Teilnehmer geben an, dass bei ihnen noch nie Hardware, Unterlagen oder Werkzeuge entwendet wurden.



3.5 Dimension 3: Cyberangriffsschutz

i [6,20]

Wesentliche Erkenntnisse

Cyberangriffsschutz als technischer Schutzwall vor Angriffen über IT-Systeme.

Der *Cyberangriffsschutz* umfasst technische Schutzmaßnahmen mit denen Unternehmen sich vor Angriffen auf IT-Systeme schützen können. Dazu gehören beispielsweise Verschlüsselungstechnologien, der technische *Zugriffsschutz* von Systemen und Anwendungen, spezielle Schutzsoftware sowie gezielte Maßnahmen zum *Schutz vor Cyberattacken und Datenverlust*. Die *Verschlüsselung* soll sicherstellen, dass nur autorisierte Personen auf Daten, Informationen, Systeme und Kommunikation zugreifen können. Die Autorisierung wird mit Hilfe von technischen Barrieren überprüft. Der *Zugriffsschutz* regelt, wer welche Zugriffsrechte erhält und dementsprechend autorisiert ist. Der *Schutz vor Cyberattacken und Datenverlust* geschieht auf mehreren Ebenen. Zum einen gilt es mittels Firewalls und Antivirenprogrammen das Einschleusen von Schadsoftware in die eigene IT-Infrastruktur zu verhindern. Sensible Systeme sollten mehrfach geschützt werden. Um einen Angriff über Sicherheitslücken innerhalb genutzter Software in Unternehmen zu verhindern, ist es wichtig, regelmäßige Updates durchzuführen und Patches aufzuspielen. Sicherheitstests dienen dazu, rechtzeitig mögliche Einfallstore für Angreifer aufzuspüren. Neben dem technischen Schutz vor Angreifern ist als zweite Säule die Sicherung von Daten relevant. Regelmäßige Backups gewährleisten, Daten im Falle eines Datenverlusts schnell wiederherstellen zu können und so die Betriebsfähigkeit des Unternehmens aufrechtzuerhalten.

Jedes vierte Unternehmen sieht sich nur ‚teilweise‘ bis ‚gar nicht‘ geschützt.

Auch wenn die Dimension *Cyberangriffsschutz* mit einem Indexwert von 6,20 die am besten ausgeprägte Schutzdimension ist und einem Schutzstatus von ‚eher geschützt‘ entspricht, geben 41,3 Prozent der Unternehmen an, lediglich ‚teilweise‘ bis ‚gar nicht‘ vor Cyberangriffen geschützt zu sein. Lediglich 14,1 Prozent betrachten sich selbst als sehr gut geschützt und 44,7 Prozent halten ihren *Cyberangriffsschutz* für ‚eher hoch‘. Das zeigt, dass bei den Unternehmen bei technischen Schutzmaßnahmen ebenfalls noch deutlicher Optimierungsbedarf besteht. Dies ist gravierend, weil die Studie zeigt, dass Unternehmen jeglicher Größe bereits Opfer von Angriffen mit Ransomware geworden sind. Diese Art von Schadsoftware verschlüsselt die Daten oder Systeme des angegriffenen Unternehmens und bietet damit eine Möglichkeit zur Erpressung der Opfer.

Technischer Schutz vor Cyberattacken und Datenverlust wird am häufigsten umgesetzt. Backups, Firewalls und Antivirenprogramme sind die häufigsten Schutzinstrumente.

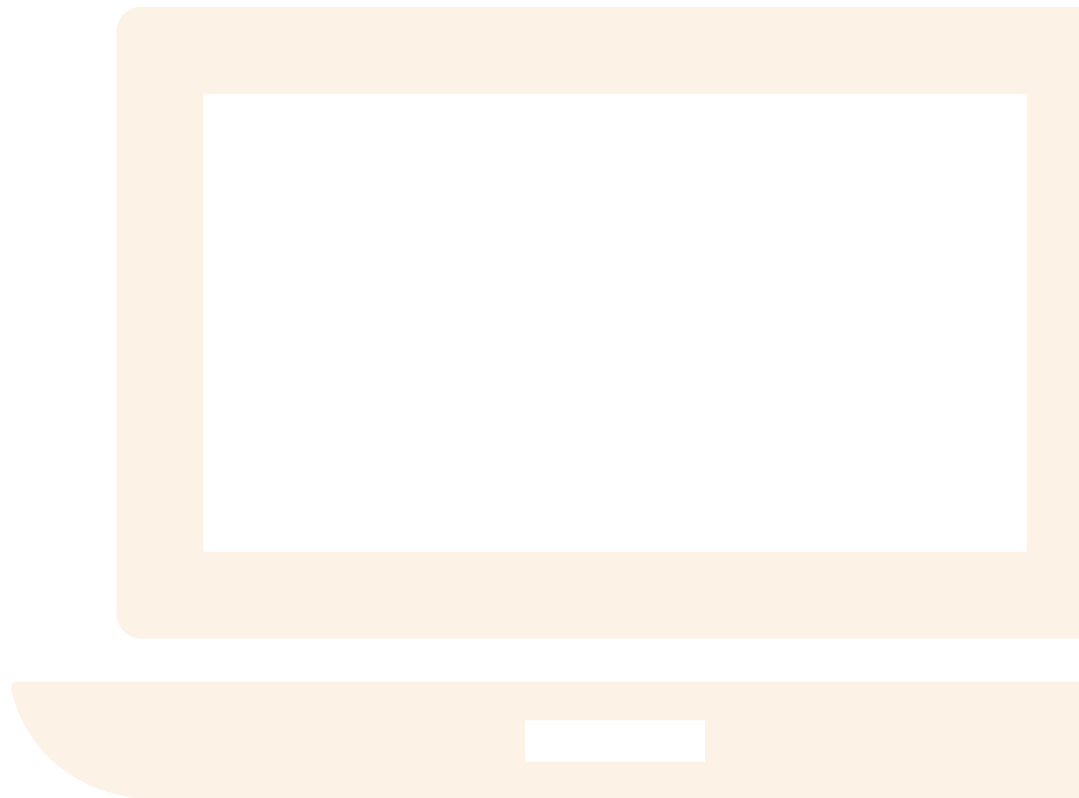
Unternehmen setzen beim Thema Sicherheit vor allem auf die Basisschutzmaßnahmen wie Backups, Firewalls und Antivirenprogramme. Je komplexer Schutzmaßnahmen werden, desto geringer wird die Umsetzung und die wahrgenommene Relevanz. Deutlich wird dies vor allem beim Thema Sicherheitstests. Während alle anderen Maßnahmen des Indikators *Schutz vor Cyberattacken und Datenverlust* auf Indexwerte von 8,00 bis 8,47 kommen, liegt der Wert für Sicherheitstests bei 4,27.

Trotz einer Zunahme des mobilen Arbeitens und Homeoffice gibt es kaum mehr Schutz durch Verschlüsselungen.

Obwohl die Unternehmen das Arbeiten in der Pandemie flexibler gestaltet haben, hat sich das Thema *Verschlüsselung* kaum weiterentwickelt. Der gegenwärtige Zustand ist nahezu identisch mit dem 2019 festgestellten Status. Am ehesten wird noch ein Schutz des externen Zugriffs auf Systeme durch den Einsatz von VPN-Lösungen umgesetzt. In Bezug auf diese Maßnahme sind die Unternehmen als ‚eher geschützt‘ einzuordnen.

Passwortschutz ist als Basisschutzmaßnahme immer noch nicht durchgängig umgesetzt.

Auch wenn der Passwortschutz zu den am häufigsten genutzten Schutzmaßnahmen gehört, wird diese Maßnahme dennoch nicht in allen Unternehmen konsequent umgesetzt. 58,4 Prozent aller Unternehmen schützen ihre sensiblen Daten immer noch nicht ‚umfassend‘.



3.6 Dimension 4: Physischer Gebäudeschutz

i [4,00]

Wesentliche Erkenntnisse

Die meisten Unternehmen fühlen sich in ihrem Gebäude gut geschützt.

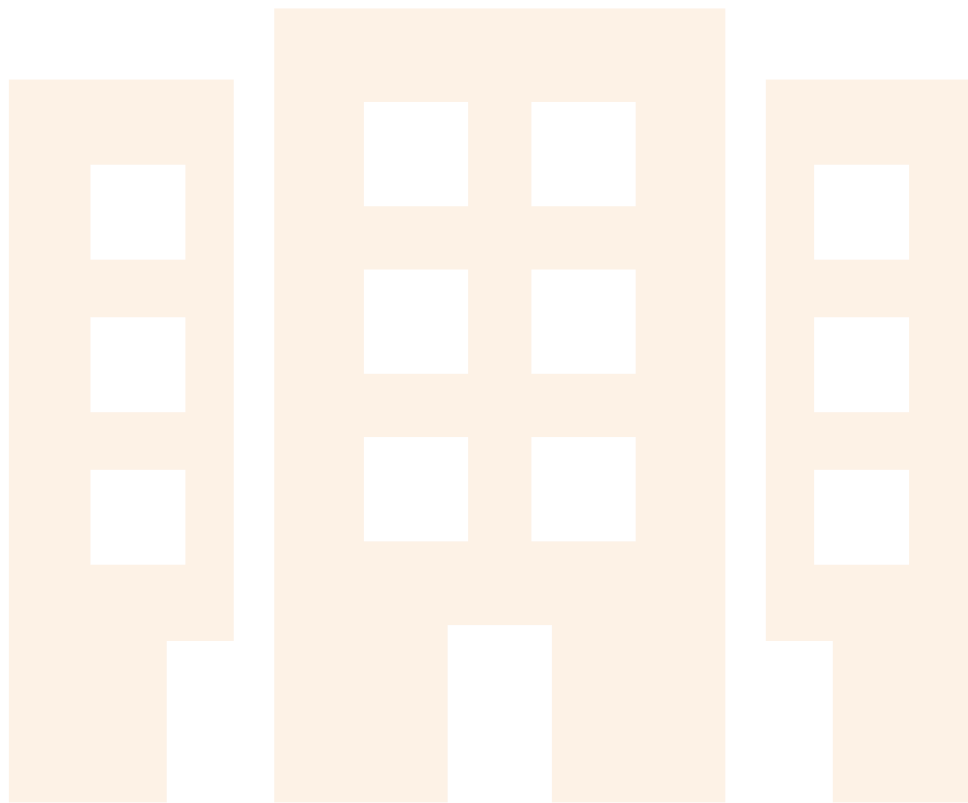
Der Schutz von Betriebs- und Geschäftsgeheimnissen sollte sich nicht nur auf den einzelnen Arbeitsplatz beschränken. Eine ganzheitliche Betrachtung muss auch den Physischen Gebäudeschutz mit seinen äußeren und betriebsinternen Schutzbereichen einbeziehen. Die Unternehmen bewerten den Schutz des eigenen Gebäudes vorrangig als ‚sehr gut‘ oder ‚eher gut‘.

Zu viele Unternehmen schützen sensible Besprechungen ungenügend.

Insgesamt wird bei knapp der Hälfte der Unternehmen kaum darauf geachtet, gezielte Vorkehrungen zum Schutz sensibler Besprechungen zu treffen. Damit entsteht ein Risiko, dass Angreifer sensible Informationen von innen oder außen abhören können. Lediglich jedes zehnte Unternehmen schützt sensible Besprechungen ‚umfassend‘ durch gezielte Vorkehrungen.

Unternehmen dürfen den Schutz wichtiger physischer Dokumente und Wertgegenstände nicht aus dem Blick verlieren.

Der Schutz digitalisierter Daten und Dokumente ist wichtig. Doch auch physisch vorhandene sensible Dokumente und Wertgegenstände gilt es mit Tresoren oder anderen Schutzschränken oder -räumen vor Diebstahl zu schützen. Fast jedes fünfte Unternehmen (18,4 %) nutzt diese Möglichkeit ‚gar nicht‘, weitere 15,2 Prozent kaum. Möglicherweise ist nicht allen Unternehmen der Schutzbedarf bestimmter Dokumente oder Wertgegenstände bewusst.



ABBILDUNGSVERZEICHNIS

Abbildung 1:	Gesamtindex NRW im Vergleich 2019/2021	24
Abbildung 2:	Durchschnittindexwert und Indexwerte der vier Dimensionen	25
Abbildung 3:	Branchenindex NRW	26
Abbildung 4:	Indexwerte KRITIS- und Nicht-KRITIS-Unternehmen	30
Abbildung 5:	Durchschnittlicher Indexwert der Befragten je nach zugeschriebener Wichtigkeit von Betriebs- und Geschäftsgeheimnissen des Unternehmens	32
Abbildung 6:	Branchenauswertung zur Wichtigkeit des Schutzes von Betriebs- und Geschäftsgeheimnissen	33
Abbildung 7:	Unternehmensgrößenauswertung zur Wichtigkeit des Schutzes von Betriebs- und Geschäftsgeheimnissen	34
Abbildung 8:	Gegenüberstellung der Selbstwahrnehmung der Unternehmen und des tatsächlichen Indexwertes	35
Abbildung 9:	Unternehmensgrößenauswertung der Selbstwahrnehmung der Unternehmen und des tatsächlichen Indexwertes bei der Dimension Personenbezogene Schutzmaßnahmen	36
Abbildung 10:	Relevanzwahrnehmung von KMU zu Themen des Wirtschaftsschutzes	37
Abbildung 11:	Aufteilung der Unternehmen nach Schutzstatus	38
Abbildung 12:	Index nach Unternehmensgröße NRW	40
Abbildung 13:	Allgemeine Auswertung zum zukünftigen Angebot von mobilem Arbeiten und Homeoffice	46
Abbildung 14:	Allgemeine Auswertung zu mobilem Arbeiten und Homeoffice vor der Pandemie	47
Abbildung 15:	Allgemeine Auswertung zur Veränderung des Digitalisierungsstands durch die Corona-Pandemie	48
Abbildung 16:	Allgemeine Auswertung zur Veränderung des Themas Unternehmenssicherheit durch die Corona-Pandemie	50
Abbildung 17:	Allgemeine Auswertung zu Richtlinien und Anweisungen für mobiles Arbeiten oder Homeoffice	51
Abbildung 18:	Allgemeine Auswertung zu Sensibilisierungen oder Schulungen zur Unternehmenssicherheit bei mobilen Arbeiten und im Homeoffice	52
Abbildung 19:	Branchenauswertung zum durchschnittlichen Vorhandensein von Richtlinien und Anweisungen	56
Abbildung 20:	Rangfolge vorhandener Richtlinien und Anweisungen in den Unternehmen	57
Abbildung 21:	Allgemeine Auswertung zu Richtlinien und Anweisungen zur Zeichenanzahl und -zusammensetzung von Passwörtern	58
Abbildung 22:	Allgemeine Auswertung zu Richtlinien und Anweisungen zur Änderungshäufigkeit von Passwörtern	59
Abbildung 23:	Branchenauswertung zu Krisen- und/oder Notfallplänen	60
Abbildung 24:	Unternehmensgrößenauswertung zur Relevanz von Monitoring sicherheitsrelevanter Prozesse	62
Abbildung 25:	Unternehmensgrößenauswertung zum Monitoring sicherheitsrelevanter Prozesse	63
Abbildung 26:	Branchenauswertung zum Vorhandensein eines aktuellen, schriftlich dokumentierten Sicherheitskonzepts	64
Abbildung 27:	Unternehmensgrößenauswertung zum Vorhandensein eines aktuellen, schriftlich dokumentierten Sicherheitskonzepts	65
Abbildung 28:	Branchenauswertung zu externen Sicherheitsaudits oder -zertifizierungen	66
Abbildung 29:	Unternehmensgrößenauswertung zu externen Sicherheitsaudits oder -zertifizierungen	67
Abbildung 30:	Unternehmensgrößenauswertung zu externer Absicherung durch eine Cyberversicherung	68
Abbildung 31:	Branchenauswertung zu externer Absicherung durch eine Cyberversicherung	69
Abbildung 32:	Unternehmensgrößenauswertung zur strategischen Verortung des Themas Unternehmenssicherheit auf der Leitungsebene	72
Abbildung 33:	Relevanzauswertung zur strategischen Verortung des Themas Unternehmenssicherheit auf der Leitungsebene	73
Abbildung 34:	Branchenauswertung zur operativen Verantwortung für Sicherheitsthemen	74

Abbildung 35: Allgemeine Auswertung der operativen Zuständigkeit für Unternehmensschutz	75
Abbildung 36: Relevanzauswertung zur Überprüfung sicherheitsrelevanter Aspekte von zukünftigen Mitarbeitern	76
Abbildung 37: Branchenauswertung zur Überprüfung sicherheitsrelevanter Aspekte von zukünftigen Mitarbeitern	77
Abbildung 38: Unternehmensgrößenauswertung zu Schulungen über Sicherheitsanforderungen	78
Abbildung 39: Relevanzauswertung zu Schulungen über Sicherheitsanforderungen	79
Abbildung 40: Branchenauswertung zu Schulungen über Sicherheitsanforderungen	80
Abbildung 41: Allgemeine Auswertung zu Opfern von Cyberangriffen oder -angriffsversuchen	84
Abbildung 42: Allgemeine Auswertung zu Opfer eines erfolgreichen Ransomwareangriffs	85
Abbildung 43: Unternehmensgrößenauswertung zur Verschlüsselung mobiler Geräte und Datenträger	86
Abbildung 44: Relevanzauswertung zur Verschlüsselung mobiler Geräte und Datenträger	87
Abbildung 45: Unternehmensgrößenauswertung zur Verschlüsselung der Kommunikation	88
Abbildung 46: Relevanzauswertung zur Verschlüsselung der Kommunikation	89
Abbildung 47: Unternehmensgrößenauswertung zur Verschlüsselung des externen Zugriffs auf Systeme	90
Abbildung 48: Branchenauswertung zur Verschlüsselung des externen Zugriffs auf Systeme	91
Abbildung 49: Unternehmensgrößenauswertung zu verbindlichem Passwortschutz sicherheitsrelevanter Daten	92
Abbildung 50: Unternehmensgrößenauswertung zu aktuellen Firewalls und Antivirenprogrammen	94
Abbildung 51: Relevanzauswertung zu aktuellen Firewalls und Antivirenprogrammen	95
Abbildung 52: Unternehmensgrößenauswertung zu regelmäßigen Backups der Daten	96
Abbildung 53: Unternehmensgrößenauswertung zu aktuellen Patches und Updates bei Software	98
Abbildung 54: Branchenauswertung zu aktuellen Patches und Updates bei Software	99
Abbildung 55: Branchenauswertung zu regelmäßigen Sicherheitstests	100
Abbildung 56: Relevanzauswertung zu regelmäßigen Sicherheitstests	101
Abbildung 57: Allgemeine Auswertung zum Schutz des Gebäudes vor unerlaubtem Eindringen	103
Abbildung 58: Allgemeine Auswertung zum Schutz sensibler Unternehmensbereiche vor unerlaubtem Eindringen	105
Abbildung 59: Unternehmensgrößenauswertung zu Einbruchmeldeanlagen	106
Abbildung 60: Branchenauswertung zu Einbruchmeldeanlagen	107
Abbildung 61: Branchenauswertung zu Kontrollen des Betriebsgeländes durch Sicherheitspersonal	108
Abbildung 62: Relevanzauswertung zu Kontrollen des Betriebsgeländes durch Sicherheitspersonal	109
Abbildung 63: Unternehmensgrößenauswertung zu Sicherheitsvorkehrungen bei sensiblen Besprechungen	110
Abbildung 64: Unternehmensgrößenauswertung zur Aufbewahrung sensibler und wichtiger Dokumente	112
Abbildung 65: Relevanzauswertung zur Aufbewahrung sensibler und wichtiger Dokumente	113
Abbildung 66: Branchenauswertung zu festgelegten Prozessen der Schlüsselvergabe	114
Abbildung 67: Unternehmensgrößenauswertung zu festgelegten Prozessen der Schlüsselvergabe	115
Abbildung 68: Allgemeine Auswertung zum Bezug von Wissen zum Thema Unternehmenssicherheit	116
Abbildung 69: Verteilung der effektiven Stichprobe nach Branche	124
Abbildung 70: Verteilung der effektiven Stichprobe nach Unternehmensgröße	125
Abbildung 71: Verteilung der effektiven Stichprobe nach KRITIS/ Nicht-KRITIS-Unternehmen	125

TABELLENVERZEICHNIS

Tabelle 1: Kennzahlen Gesamtindex 2021 und 2019	8
Tabelle 2: Definition KMU (IfM Bonn 2018)	18
Tabelle 3: Branchenbezeichnungen Lagebild Wirtschaftsschutz	18
Tabelle 4: Dimensionen und Indikatoren des Lagebildes Wirtschaftsschutz	19
Tabelle 5: Schutzindikatoren nach Indexwert absteigend	25
Tabelle 6: Indexwerte nach Branche und Gesamtindex	27
Tabelle 7: Indexwerte der Dimensionen und Indikatoren nach Unternehmensgröße	41
Tabelle 8: Definition KMU (IfM Bonn 2018)	120
Tabelle 9: Branchenbezeichnungen Lagebild Wirtschaftsschutz	120
Tabelle 10: Zuordnungen der Unternehmensaussagen in den Wirtschaftsschutzstand	126
Tabelle 11: Zuordnungen zum Wirtschaftsschutzniveau	126

LITERATURVERZEICHNIS

Bitkom (2016). Web: <https://www.bitkom.org/sites/default/files/file/import/181106-Studie-Wirtschaftsschutz.pdf> (Abruf: 01.12.2021).

Bitkom (2018). Web: <https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf> (Abruf: 01.12.2021).

Bitkom (2021). Web: <https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr> (Abruf: 01.12.2021).

Destatis (2008): Klassifikation der Wirtschaftszweige mit Erläuterungen. Web: <https://www.destatis.de/DE/Methoden/Klassifikationen/textbaustein-klassifikationen.html> (Abruf: 01.12.2021).

Institut für Mittelstandsforschung. Web: <https://www.ifm-bonn.org/definitionen-/kmu-definition-des-ifm-bonn> (Abruf: 22.12.2021).

IT-NRW (2021). Web: <https://www.it.nrw/nrw-wirtschaftsleistung-im-jahr-2020-um-44-prozent-niedriger-als-ein-jahr-zuvor-103118> (Abruf:23.09.2021).

Landesdatenbank NRW Auszug aus dem Unternehmensregister ab 2019. Web: <https://www.landesdatenbank.nrw.de/ldbnrw/online/> (Abruf:01.12.2021).

Sicherheitspartnerschaft NRW. Web: <https://www.im.nrw/themen/verfassungsschutz/schutz-von-behoerden-und-unternehmen/sicherheitspartnerschaft-nordrhein> (Stand: 01.12.2021).

Skillsoft 2021: Anstieg der Nachfrage für Sicherheitstrainings. Web: <https://www.it-daily.net/it-sicherheit/cloud-security/30996-anstieg-in-der-nachfrage-fuer-sicherheitstrainings> (Abruf: 22.12.2021).

Taubitz, T. (2020): Weiterbildung nach Corona. Grün, digital, on demand. Web: <https://www.humanresourcesmanager.de/news/weiterbildung-nachcorona-gruen-digital-on-demand.html> (Abruf: 22.12.2021).

Werning et al. (2019): Lagebild Wirtschaftsschutz NRW 2019. Web: https://www.wirtschaftsschutz.info/SharedDocs/Studien/DE/Lagebild_NRW.html (Abruf: 01.12.2021).

Werning et al. (2020): Digitalisierungsindex von KMU in NRW. Digitalisierungsstand in den Branchen Industrie, industrienaher Dienstleistungen und Handwerk, hrsg. Sparkassenverband Westfalen-Lippe, Münster 2020.

Wirtschaft NRW. Web: <https://www.wirtschaft.nrw/daten-und-fakten-zum-mittelstand-nrw> (Abruf: 01.12.2021).

IMPRESSUM

Herausgeber

Ministerium des Innern des Landes NRW
Friedrichstraße 62-80
40217 Düsseldorf
Telefon 0211/871-01
Telefax 0211/871-3355
E-Mail poststelle@im.nrw.de

Ansprechpartner

Referat Wirtschaftsschutz
E-Mail wirtschaftsschutz@im1.nrw.de
Internet www.im.nrw

Fachliche Bearbeitung

Prof. Dr. Ellena Werning
Fachhochschule des Mittelstands (FHM) GmbH
– University of Applied Sciences –
Ravensberger Str. 10 G
33602 Bielefeld
Telefon (0521) 96655-283
Telefax (05 21).96655-11
E-Mail werning@fh-mittelstand.de
Internet www.fh-mittelstand.de

Elisa Goldmann MBA
Wissenschaftliche Mitarbeiterin
Telefon (0521) 96655-260
Telefax (05 21).96655-11
E-Mail goldmann@fh-mittelstand.de
Internet www.fh-mittelstand.de

Unterstützung bei der technischen Datenverarbeitung und Auswertung

Kommunales Rechenzentrum Minden-Ravensberg/Lippe
Bismarckstraße 23, 32657 Lemgo
Telefon (05261) 252-0
Telefax (05261) 252-200
Internet www.krz.de

Layout, Gestaltung und Satz

Fachhochschule des Mittelstands (FHM) GmbH
Telefon (0521) 96655-222
Telefax (05 21).96655-11
E-Mail marketing@fh-mittelstand.de
Internet www.fh-mittelstand.de

Bildnachweis

Titelbild © Adobe Stock: #207941548

HINWEIS

Diese Druckschrift wird im Rahmen der Öffentlichkeitsarbeit des Ministeriums des Innern des Landes Nordrhein-Westfalen herausgegeben. Sie darf weder von Parteien noch von Wahlbewerberinnen und Wahlbewerbern oder Wahlhelferinnen und Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für die Landtags-, Bundestags- und Kommunalwahlen sowie für die Wahl der Mitglieder des Europäischen Parlaments. Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist gleichfalls die Weitergabe an Dritte zum Zwecke der Wahlwerbung. Eine Verwendung dieser Druckschrift durch Parteien oder sie unterstützende Organisationen ausschließlich zur Unterrichtung ihrer eigenen Mitglieder bleibt hiervon unberührt.

Unabhängig davon, wann, auf welchem Weg und in welcher Anzahl diese Schrift dem Empfänger zugegangen ist, darf sie auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl nicht in einer Weise verwendet werden, die als Parteinahme des Ministeriums des Innern Nordrhein-Westfalen zugunsten einzelner politischer Gruppen verstanden werden könnte.

