Cybersicherheit in Unternehmen

Sonderauswertung zur IHK Digitalisierungsumfrage

#GemeinsamDigital

DIHK Deutsche Industrie- und Handelskammer

IHK Deutsche Industrie- und Handelskammern

Impressum

Ansprechpartner im DIHK:

Dr. Katrin Sobania
sobania.katrin@dihk.de
+49 30 20308-2109

Herausgeber und Copyright

© Deutsche Industrie- und Handelskammer
Berlin | Brüssel
Bereich Digitale Wirtschaft, Infrastruktur, Regionalpolitik (DIR)

DIHK Berlin
Postanschrift: 11052 Berlin | Hausanschrift: Breite Straße 29 | Berlin-Mitte
Telefon: 030 20308-0 | Telefax: 030 20308-100

DIHK Brüssel
Vertretung der Deutschen Industrie- und Handelskammer bei der Europäischen Union
19 A-D, Avenue des Arts | B-1000 Bruxelles
Telefon: +32-2-286-1611 | Telefax: +32-2-286-1605

@ *info@dihk.de*
www.dihk.de

Grafik
Friedemann Encke, DIHK

Bildnachweis
© Getty Images
Jasmin Merdan | Sean Gladwell | Volker Schlichting/EyeEm | Andriy Onufriyenko | Science Photo Library

Stand
Februar 2023

Cybersicherheit in Unternehmen – besseres Zusammenspiel Staat und Wirtschaft erforderlich

Sonderauswertung zur IHK Digitalisierungsumfrage zur Daten- und Informationssicherheit

Mangelnde Kompetenzen und sich verschärfende Bedrohungslage beunruhigen

Mit zunehmender Digitalisierung, Datennutzung und Vernetzung gibt es auch mehr Angriffsfläche im digitalen Raum. Das Risiko für Unternehmen, Opfer von digitaler Erpressung, Sabotage und Spionage zu werden, steigt. Das Bundesamtes für Sicherheit in der Informationstechnik (BSI) identifiziert in seinem aktuellen Lagebericht 2022 als Hauptbedrohungen u. a. Ransomware (Verschlüsseln von Daten in ausgefeilten mehrstufigen Angriffen, um Lösegeld zu erpressen), Angriffe auf externe IT-Lösungen, die Unternehmen einsetzen, bzw. Angriffe auf Cloud-Angebote, die von Unternehmen genutzt werden, sowie Schwachstellen in Produkten.

Die Bedrohungslage hat sich insbesondere im Kontext des russischen Angriffskrieges gegen die Ukraine weiter zugespitzt. Unter Experten nimmt die Sorge vor Angriffen vor allem auf die kritischen Infrastrukturen zu. Wenn Unternehmen nicht direkt Opfer gezielter Angriffe werden, können Folgeschäden drohen, etwa durch die Nichtverfügbarkeit von kritischen Infrastrukturen, oder weil viele Industrieunternehmen dieselben technischen Systeme wie die Betreiber kritischer Infrastrukturen nutzen. Sie können so zum Opfer von Angriffen werden. Darüber hinaus ist mit der Sabotage und Manipulation physischer (IT-)Infrastrukturen eine neue Dimension im Sinne „hybrider Bedrohungen" hinzugetreten.

In einer mehr und mehr vernetzten Gesellschaft sind alle Beteiligten – Staat, Wirtschaft und Gesellschaft – auf ein vertrauensvolles Miteinander angewiesen. Nicht jede Gruppe kann die komplexen Herausforderungen allein bewältigen. Sicherheitsrelevante Prozesse müssen übergreifend gedacht werden und erfordern neue Kooperationsformen, in denen jeder nach seinen Fähigkeiten einen Beitrag leisten muss.

Zwar haben die Unternehmen die Gefahren erkannt und häufig technische Vorkehrungen getroffen. Mit technischen Sicherheitsvorkehrungen allein ist es jedoch nicht getan. Der Staat sollte die Unternehmensbemühungen besser flankieren: So wünschen sich die Unternehmen passgenaue Informationen zur Sicherheitslage. Das ergab eine Umfrage, die die DIHK in Zusammenarbeit mit der Allianz für Cybersicherheit im Sommer 2022 durchgeführt hat. Das Lagebild sollte Informationen zu Cyber- und analogen Bedrohungen enthalten, verständlich sein und konkrete Handlungsempfehlungen enthalten. Ist ein IT-Notfall eingetreten, wissen die betroffenen Unternehmen häufig nicht, an wen sie sich um Hilfe wenden können. Hier sollten die Sicherheitsorgane deutlich besser qualitativ und quantitativ aufgestellt und das Zusammenspiel zwischen den Behörden verbessert werden.

Die Umsetzung der Sicherheitsmaßnahmen in den Unternehmen sollte durch entsprechende Unterstützungsleistungen flankiert werden. Dabei sind neben technischen Vorkehrungen vor allem organisatorisch-prozessuale Maßnahmen in den Unternehmen selbst erforderlich. Denn auch die Belegschaft spielt eine wichtige Rolle für Angreifer. Unsicherheiten im Umgang mit IT-Systemen, etwa die fehlende Kenntnis von Angriffsmustern, können Hackern in die Hände spielen. Insbesondere organisatorische Maßnahmen und Maßnahmen zur Erhöhung der Informationssicherheits-Kompetenzen der Geschäftsführungen und der Beschäftigten sind nach Angaben der Unternehmen jedoch weniger verbreitet als technische Sicherheitsmaßnahmen. Es gibt bei den Betrieben noch einiges zu tun: So haben viele Unternehmen keinen schriftlich festgehaltenen Plan für den Fall eines IT-Sicherheitsvorfalls. Auch Mitarbeiterschulungen, Nutzungsrichtlinien für die Mitarbeitenden oder die Einrichtung eines IT-Sicherheitsbeauftragten sind angesichts der zunehmenden Bedrohungslage von immer größerer Bedeutung. Werden aber noch nicht flächendeckend eingesetzt. Das zeigen die Ergebnisse der DIHK-Sonderauswertung der Digitalisierungsumfrage der IHKs zum Thema Daten- und Informationssicherheit unter mehr als 4.000 Unternehmen.

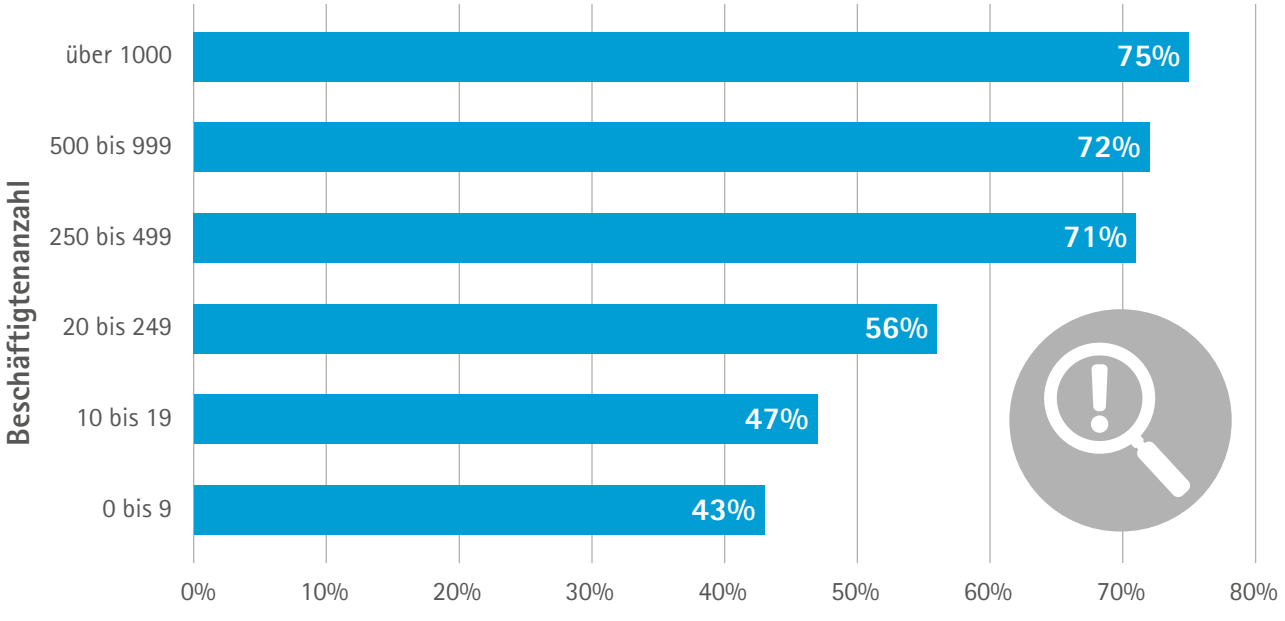
Maßnahmen Informationssicherheit in Unternehmen

Antwort	2022	2021	2020
Technische Maßnahmen			
Backups	91%	92%	91%
Laufende Aktualisierung der IT-Sicherheitsmaßnahme (z.B. Updates)	75%	-	-
Identitätsmanagement (z.B. Authentifikation via Passwort; Rechte-/Rollenverwaltung)	66%	62%	65%
Verschlüsselung (z.B. von E-Mails)	45%	55%	51%
Organisatorische Maßnahmen			
Risikoanalyse	53%	55%	54%
Nutzungs-Richtlinien für die Mitarbeitenden	53%	54%	51%
Regelmäßige Mitarbeiterschulungen	46%	47%	48%
Informationssicherheitsbeauftragter	33%	32%	35%
Notfallplan/-handbuch	30%	31%	30%
Cyberversicherungen	27%	23%	11%
Externer Sicherheitstest des Netzwerks (Penetrationstests)	26%	23%	19%

Systematischer Umgang mit Risiken im Cyber-Raum gefragt

Der Unternehmensleitung müssen die wesentlichen Risiken bekannt sein, damit sie die richtigen Entscheidungen treffen kann. Dafür müssen die Risiken zunächst erfasst und bewertet werden. Darauf aufbauend ist zu entscheiden, wie mit den Risiken umgegangen werden soll. Diesen Prozess mit Blick auf Cybersicherheit haben bisher hauptsächlich größere Unternehmen systematisch durchlaufen: drei Viertel der Unternehmen mit mehr als 1000 Mitarbeitenden haben eine entsprechende Risikoanalyse vor-

Risikoanalyse nach Größenklassen



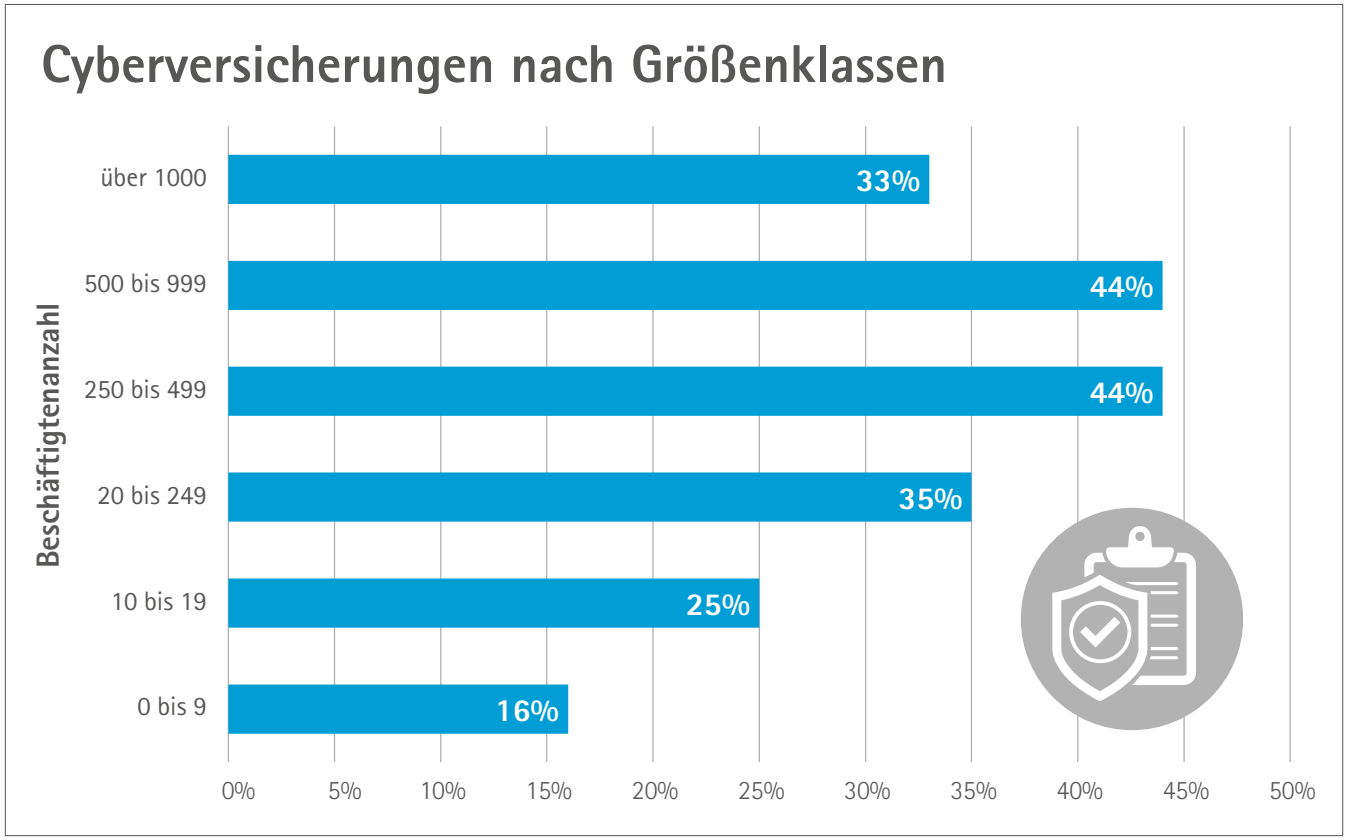
genommen. Bei den kleineren Unternehmen mit weniger als 10 Beschäftigten sind es hingegen weniger als die Hälfte.

Immer mehr Unternehmen unterziehen ihre IT-Systeme und Anwendungen zusätzlich Sicherheitstests. Die sogenannten Penetrationstests (Pentests) sorgen für Transparenz über ihre Sicherheitsrisiken. Waren es im Jahr 2020 noch 19 Prozent der Unternehmen und im Vorjahr 23 Prozent, so geben nun 25 Prozent der Befragten an, dieses Instrument als Teil einer allgemeinen Sicherheitsanalyse zu nutzen. Insbesondere in der Industrie (35 Prozent), in der Logistik (34 Prozent) und in der Finanzwirtschaft (37 Prozent) sind Pentests relativ verbreitet.

Cyberversicherungen auf dem Vormarsch

Immer mehr Unternehmen entscheiden sich, für die Absicherung von Risiken Cyberversicherungen abzuschließen. Diese haben im Laufe der letzten Jahre eine immer größere Bedeutung erlangt: 27 Prozent der Befragten geben an, eine Cyberversicherung abgeschlossen zu haben, gegenüber 23 Prozent im Jahr 2021 und 11 Prozent in 2020. Die meisten Cyberversicherungen wurden in der Finanzwirtschaft (49 Prozent) abgeschlossen. Nach Angaben der Versicherer gelten Netzattacken auf die Wirtschaft inzwischen als größtes Risiko. Das spiegelt sich zunehmend in der Höhe der Policen wider.

Zudem ist die Einhaltung gewisser Sicherheitsstandards Voraussetzung, um überhaupt eine Cyberversicherung abzuschließen. Eine Cyberversicherung geht demnach immer auch mit Umsetzungsanforderungen einher. Dies hat sich auch im kontinuierlichen Zuwachs bei der Einführung eines Informationssicherheitsmanagementsystems bzw. der Anwendung von IT-Sicherheitsstandards niedergeschlagen (33 Prozent gegenüber 25 bzw. 20 Prozent bei den Vorumfragen). Im Branchenvergleich liegt erneut die Finanzwirtschaft vorn (49 Prozent), wohingegen im Handel nur 22 Prozent entsprechende Prozesse etabliert haben.

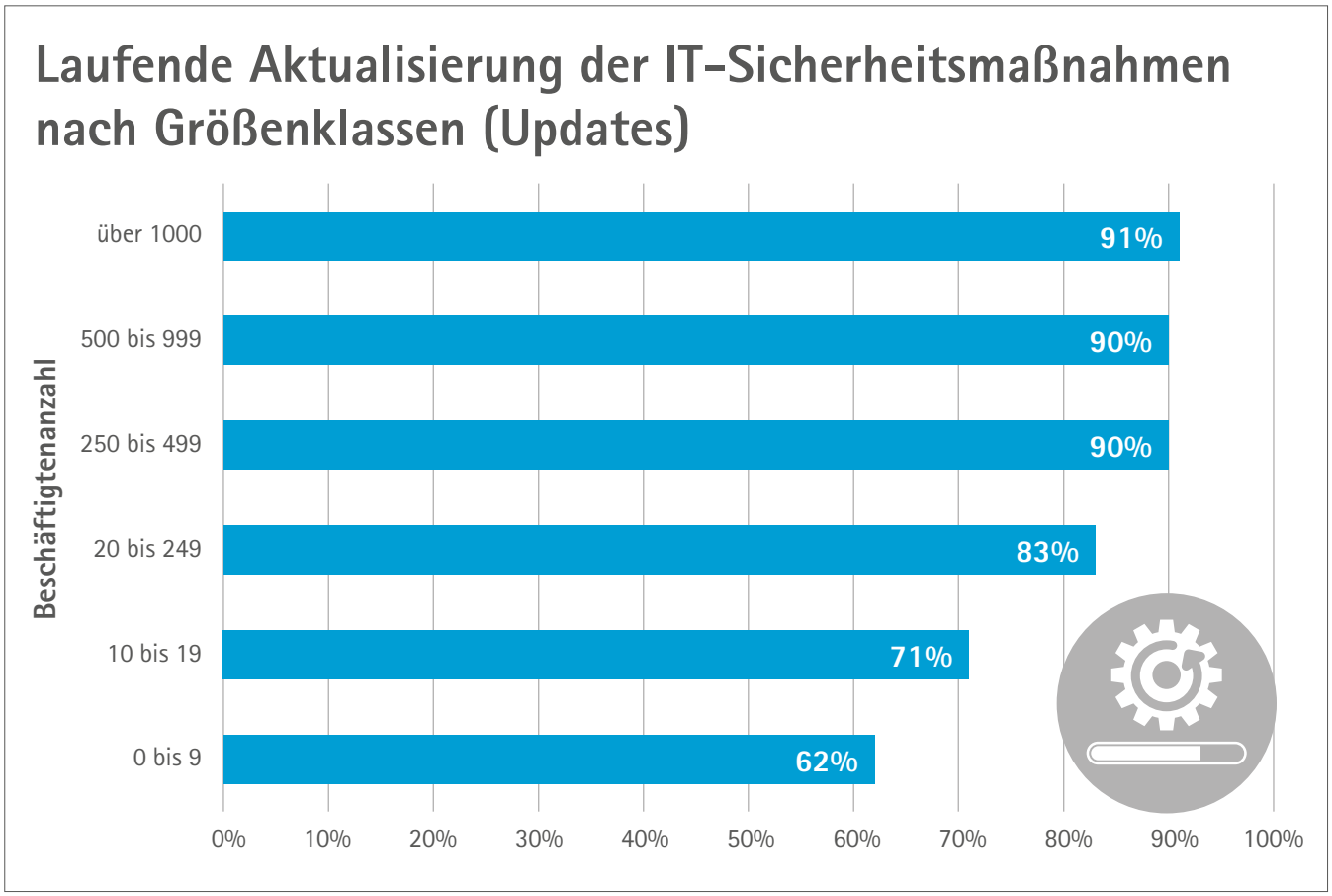


Sicherheits-Updates der Systeme und Infrastrukturen – Luft nach oben

Das BSI verweist in seinem aktuellen Lagebericht explizit auf die Gefahren, die von Software-Schwachstellen in Produkten ausgehen. Daher sollten Betriebssystem und jede verwendete Software möglichst aktuell gehalten werden. Die meisten Unternehmen spielen regelmäßig Sicherheits-Updates ein. Bei den Unternehmen mit mehr als 250 Mitarbeitenden geben dies mehr als 90 Prozent an. Doch gerade bei den kleinsten Unternehmen besteht weiterer Aufklärungs- und Umsetzungsbedarf: nur knapp zwei Drittel der Unternehmen mit weniger als 10 Mitarbeitenden nimmt laufend Sicherheitsupdates vor.

Gerade Unternehmen dieser Größenklasse nutzt vorranging Standardsoftware, für die die Anbieter im Regelfall Sicherheitsupdates anbieten.

Auch die Verschlüsselung, z. B. von E-Mails, spielt in kleineren Unternehmen noch weniger eine Rolle als in größeren. So geben 62 Prozent der kleinsten Unternehmen mit weniger 10 Mitarbeitenden an, Daten zu verschlüsseln, wohingegen dies 91 Prozent der großen Unternehmen mit mehr als 1000 Beschäftigten tun.

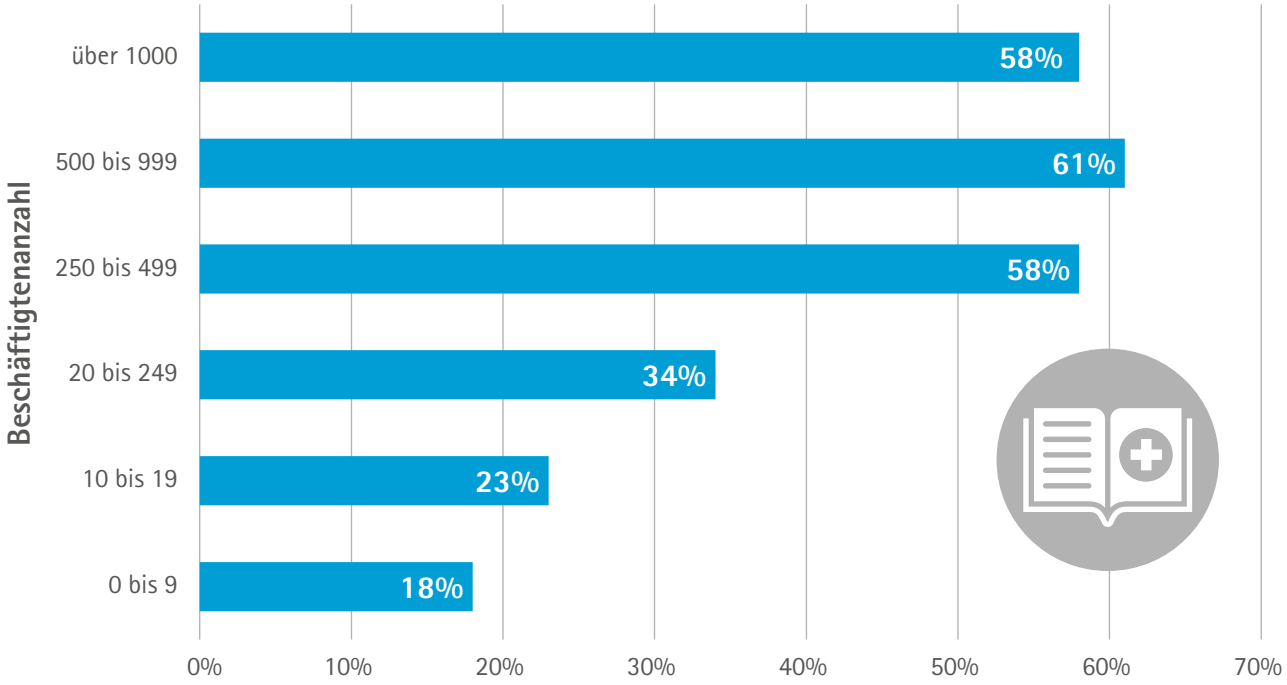


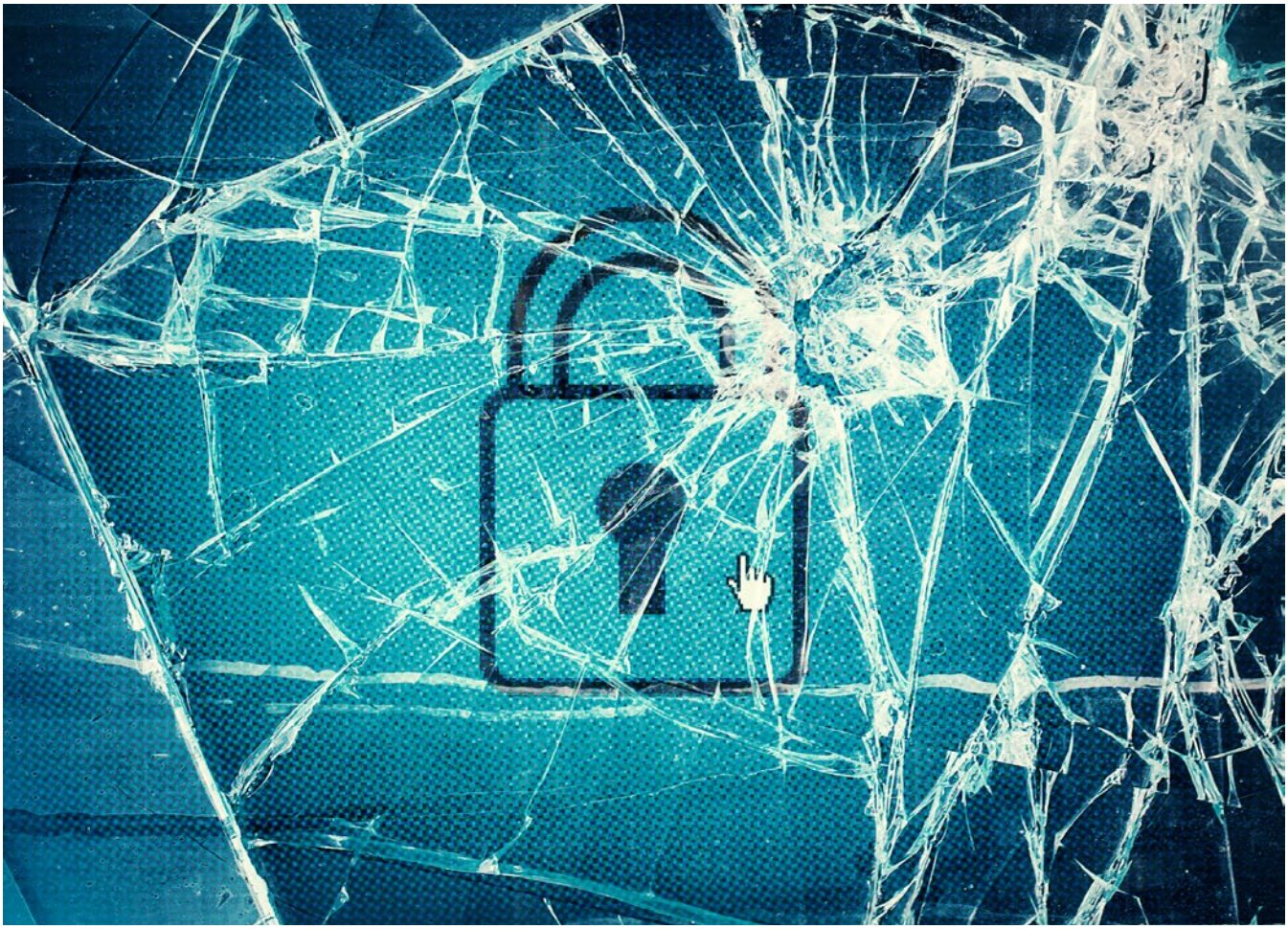
Vorbereitet sein auf Notfälle

Die Wirtschaft in der Breite muss davon ausgehen, dass ihre Systeme angegriffen werden – und dass Angriffe auch erfolgreich sein können. Funktionierende Backups helfen etwa, um Datenverluste zu vermeiden. Dies haben die meisten Unternehmen erkannt und sind gut aufgestellt: 91 Prozent der Befragten geben an, dass Backups in den Unternehmen vorhanden sind.

Auf einen erfolgreichen Cyber-Angriff, also einen IT-Notfall, sind hingegen weniger Unternehmen systematisch vorbereitet. Weniger als ein Drittel der Unternehmen verfügt über einen schriftlich fixierten Notfallplan – je kleiner das Unternehmen, desto seltener Notfallpläne in der Schublade. In der Finanzwirtschaft geben 47 Prozent der Befragten an, über einen Notfallplan zu verfügen, im Gastgewerbe 16 Prozent. Gegenüber den Vorjahresumfragen bleibt das Bild unverändert.

Notfallplan / Notfallhandbuch nach Größenklassen

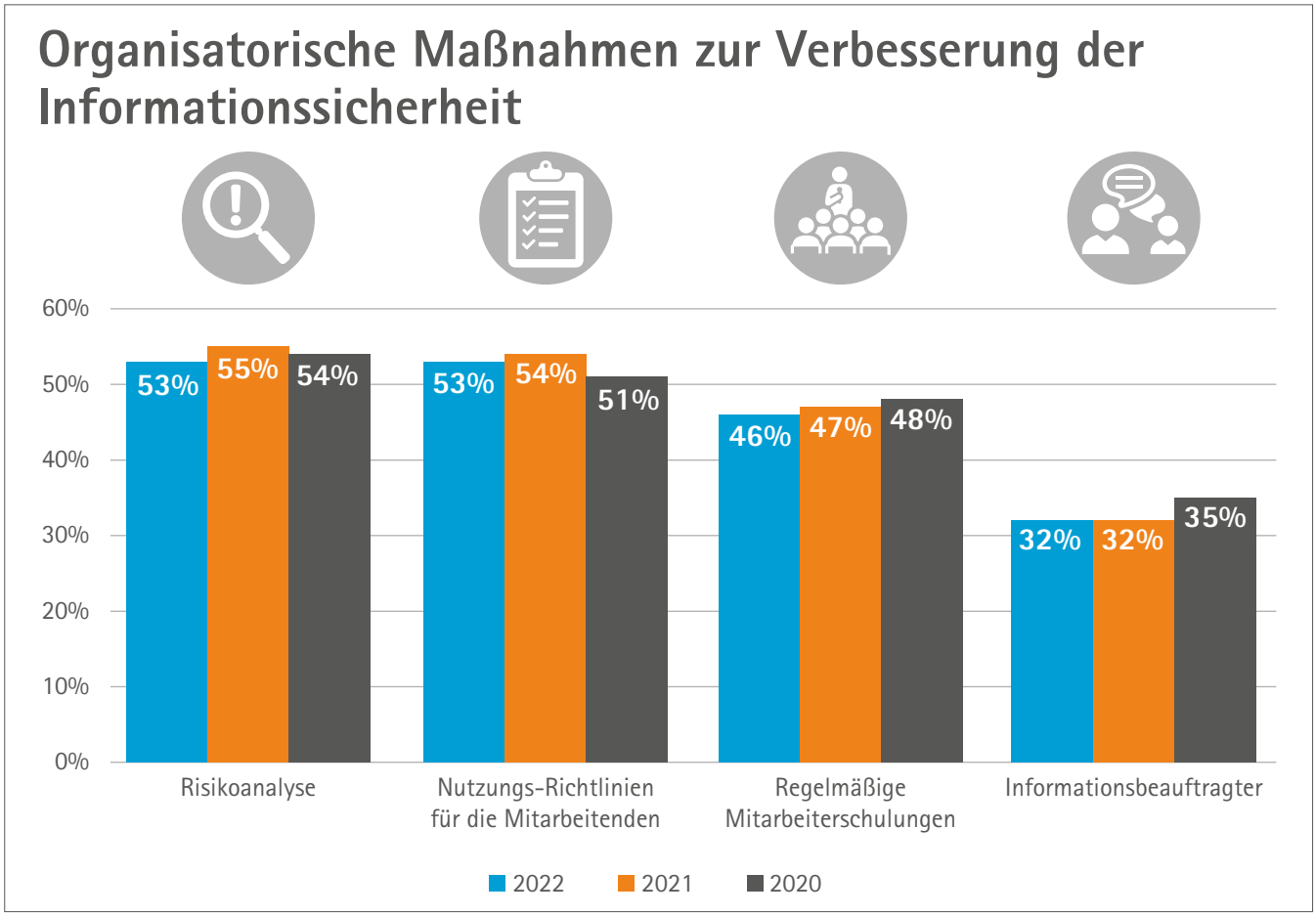


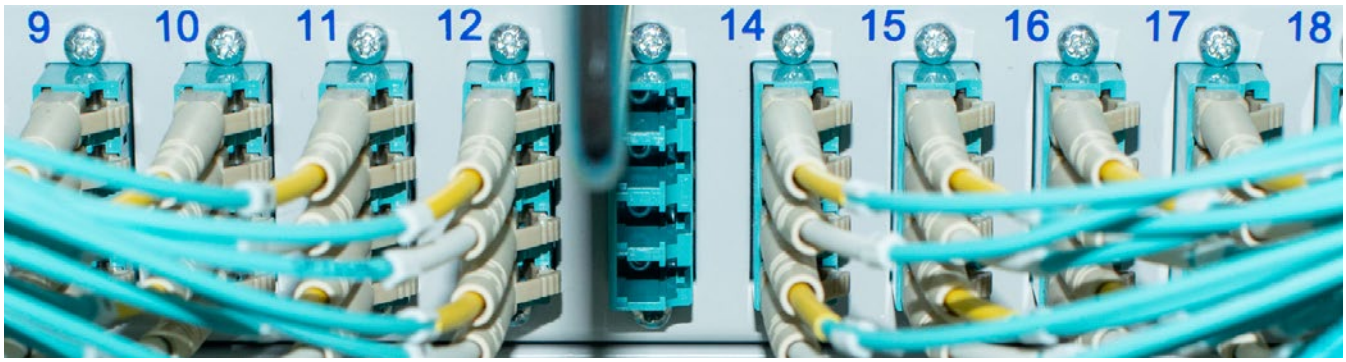


Mitarbeitende: Sicherheitsbewusstsein erforderlich

Zusätzlich zu strategischen und technischen Maßnahmen sind organisatorische Maßnahmen ein wesentlicher Erfolgsfaktor für die Informationssicherheit in Unternehmen. Denn allein mit dem Kauf der Technik ist es nicht getan. Begleitend müssen Prozesse etabliert und die Sensibilität für sicherheitsfördernde Verhaltensweisen gefördert und organisatorisch umgesetzt werden. Es gilt, Mitarbeitende etwa im Hinblick auf mögliche Angriffsmuster zu informieren, um angemessen reagieren zu können. Aktuell gibt es neben Cyberangriffen zahlreiche akute Herausforderungen wie die Energiepreiskrise etc., die Unternehmen dazu zwingen, ihre Aufmerksamkeit auf diese Themen zu lenken. Dementsprechend haben die Unternehmen ihre Aktivitäten im Vergleich zu den Vorumfragen insgesamt nicht weiter verstärkt, bzw. es sind teilweise sogar Rückgänge zu verzeichnen, etwa bei den Mitarbeiterschulungen.

Über alle Größenklassen hinweg geben zwei Drittel der Befragten an, in ihrem Unternehmen ein Identitätsmanagement, etwa Authentifizierung via Passwort, Rechte- und Rollenverwaltung, anzuwenden – genauso viele wie in den beiden Vorjahresumfragen. Regelmäßige Schulungen der Mitarbeitenden werden bei 46 Prozent aller Unternehmen durchgeführt, 33 Prozent haben einen Informationssicherheitsbeauftragten eingesetzt – jeweils geringere Werte als in den Vorjahren.



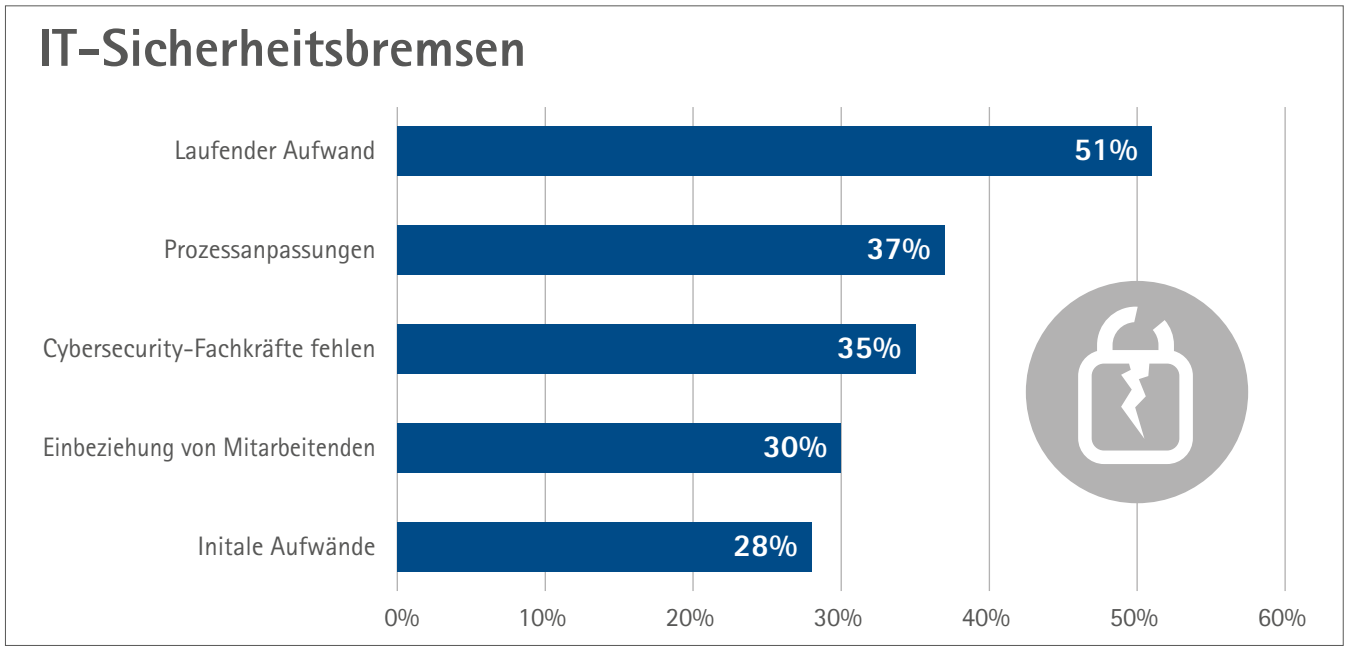


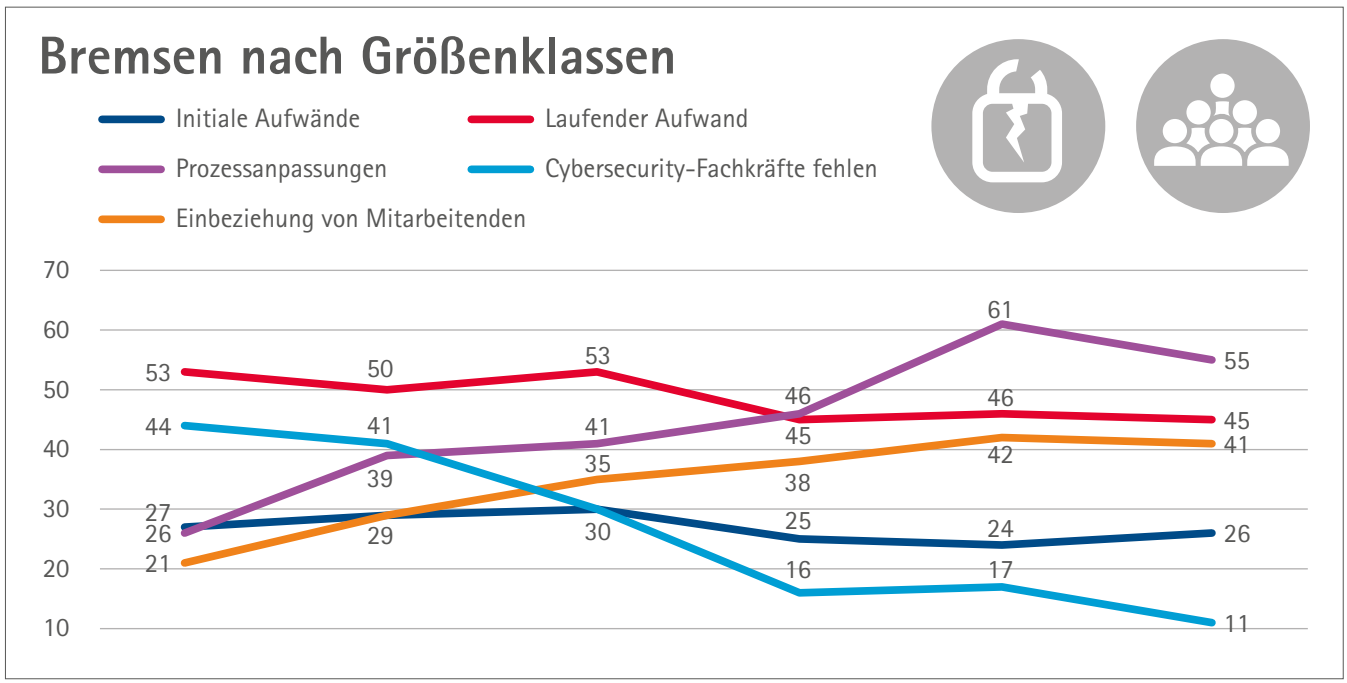
Laufender Aufwand und Prozessanpassungen als Herausforderungen

Als Bremsen für mehr Cybersichersicherheit fallen aus Sicht der Wirtschaft vor allem laufende technische Aufwände, Prozessanpassungen und fehlende IT-Sicherheitsfachkräfte ins Gewicht.

Je kleiner die Unternehmen sind, desto stärker bremst der laufende technische Aufwand. Bei den Kleinstunternehmen mit weniger als 10 Mitarbeitenden stehen die laufenden technischen Aufwände an erster Stelle (53 Prozent) gegenüber 45 Prozent bei den Großunternehmen mit mehr als 1000 Mitarbeitenden. Als zweitgrößtes Hemmnis beklagen die kleineren Unternehmen den Mangel an IT-Sicherheitsfachkräften (44 Prozent). Deren Fehlen haben hingegen nur 11 Prozent der Großunternehmen ab 1.000 Mitarbeitende als TOP3-Sicherheitsbremse angegeben.

Je größer das Unternehmen – und damit je komplexer die Prozesse – desto stärker werden Aufwände für Prozessanpassungen als eines der drei Haupthemmnisse für IT-Sicherheitsmaßnahmen betrachtet. Von den Großunternehmen mit über 1000 Mitarbeitenden haben 55 Prozent Prozessanpassungen als eines der Haupthemmnisse genannt.





Von denjenigen Unternehmen, die den **laufenden technischen Betrieb** als eines der drei Haupthemmnisse betrachten (insgesamt 51 Prozent), greifen bei den Unternehmen in der Größenordnung von 10 bis 249 Mitarbeitenden ca. zwei Drittel auf die Dienstleistungen externer Anbieter zurück. Hingegen nutzen ca. zwei Drittel der größeren Unternehmen ab 500 Mitarbeitenden dafür hauptsächlich eigenes Fachpersonal. Bei den Kleinstunternehmen, die Standardprodukte nutzen, zeigt sich ein gemischtes Bild: 53 Prozent geben an, sich selber um den laufenden Betrieb der IT-Sicherheitsmaßnahmen zu kümmern, 64 Prozent lagern dies an externe Dienstleister aus.

Laufende technische IT-Sicherheitsmaßnahmen werden erbracht durch...

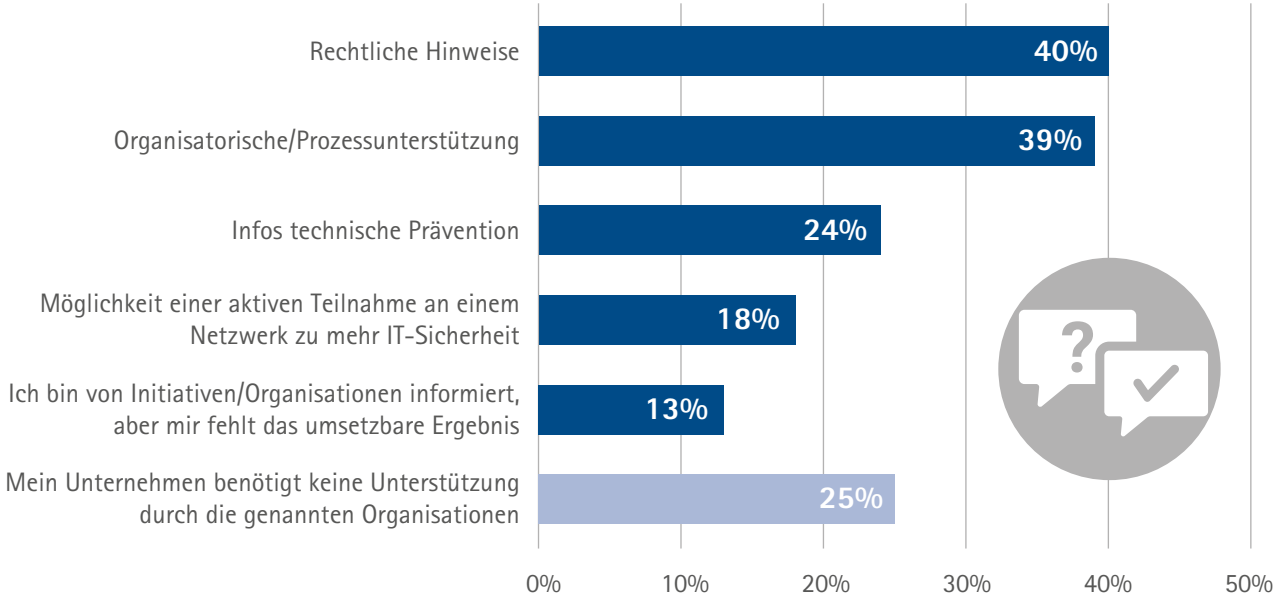
	Beschäftigtenanzahl					
Antwort	**0 - 9**	**10 - 19**	**20 - 249**	**250 - 499**	**500 - 999**	**über 1000**
Hauptsächlich durch externe Dienstleister	46%	66%	63%	50%	34%	34%
Hauptsächlich in Eigenleistung	53%	34%	36%	46%	66%	66%
Sonstiges	2%	0%	1%	4%	0%	0%

Viele Unternehmen melden Unterstützungsbedarf

Die Wirtschaftsbereiche, die zur kritischen Infrastruktur gehören und damit gesetzlichen Vorgaben wie dem IT-Sicherheitsgesetz unterliegen, haben höhere Umsetzungszahlen in Bezug auf die abgefragten Cybersicherheitsmaßnahmen. Dies betrifft etwa Teile der Finanzwirtschaft, der IKT-Wirtschaft, des Verkehrs- und Logistikbereichs oder der Industrie. Gesetzliche Vorgaben sind aber nicht für die gesamte Breite der Wirtschaft erforderlich. Vielmehr sollten Unterstützungsangebote immer vor neuen gesetzlichen Verpflichtungen stehen.

Die Unternehmen wurden befragt, in welchen Bereichen sie sich konkret Unterstützung durch den Staat, IHKs oder andere Organisationen wünschen.

Gewünschte Unterstützung beim Thema IT-Sicherheit

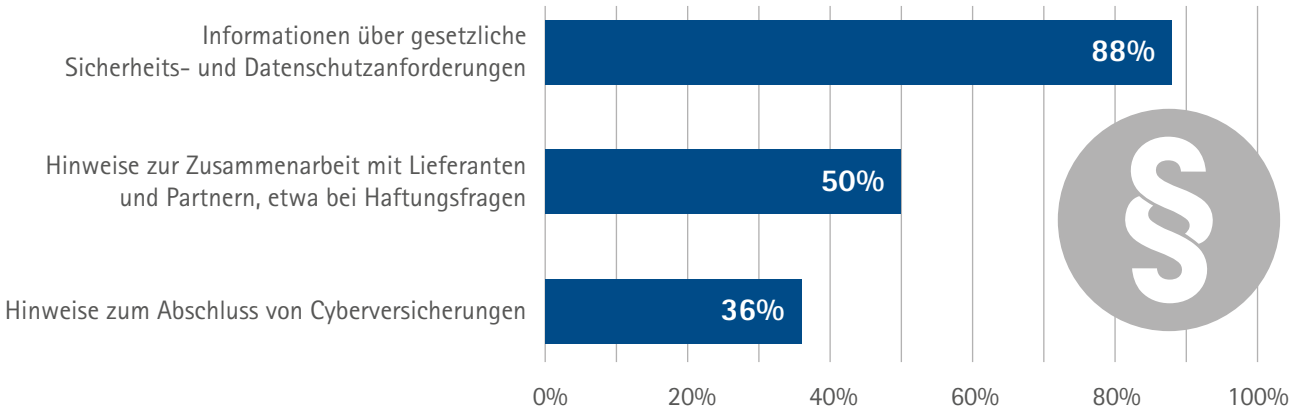


75 Prozent der Unternehmen haben Unterstützungsbedarf unterschiedlichster Art angemeldet. Von diesen wünschen sich 40 Prozent Unterstützung in Bezug auf rechtliche Fragestellungen und 39 Prozent haben Bedarf im Bereich Organisation und Prozesse. In den Freitextantworten wird häufiger aufgeführt, dass allein der Abbau bürokratischer Verpflichtungen, etwa im Bereich Datenschutz, sowie die eigene Digitalisierung der Verwaltungen eine Hilfe für die Unternehmen wäre. Darüber hinaus wäre vielen Unternehmen schon geholfen, wenn bessere Voraussetzungen für die Digitalisierung allgemein geschaffen würden, etwa eine leistungsfähige digitale Infrastruktur, und sie Unterstützung bei der Erlangung digitaler Kompetenzen hätten. Der Fachkräftemangel sollte aus Sicht der Befragten stärker adressiert werden. Gefordert wird auch, offene, sichere Standards zu unterstützen und staatlicherseits keine Hintertüren in Softwareprodukten offenzuhalten und so die IT-Sicherheit auszuhebeln. Genannt wird aber auch Unterstützungsbedarf zum Einsatz von Open Source Software oder zur Erlangung von Fördermitteln.

Von denjenigen Unternehmen, die Unterstützungsbedarf bei rechtlichen Fragestellungen haben, wünscht sich ein großer Anteil von 88 Prozent Informationen zu gesetzlichen Sicherheits- und Datenschutzanforderungen. Wie in den Vorjahresumfragen wird auch hier deutlich, dass die Umsetzung datenschutzrechtlicher Vorgaben für Verunsicherung in den Unternehmen aller Größenklassen sorgt und unverhältnismäßig viele Kapazitäten bindet. Dies gilt insbesondere auch für die Zusammenarbeit mit Unternehmen aus Drittstaaten. Unternehmen wünschen sich hier nicht nur rechtliche Vereinfachungen, sondern auch konkrete, einfach verständliche Umsetzungsempfehlungen.

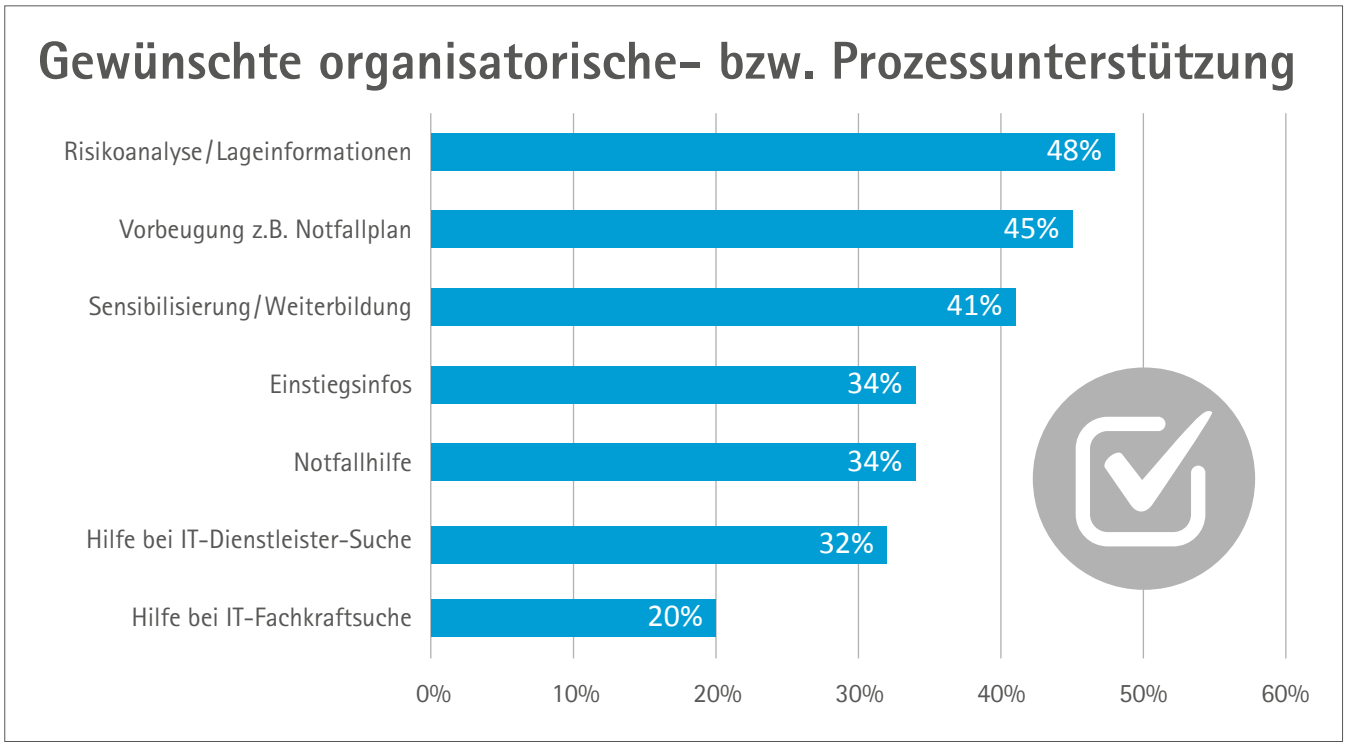
Die Hälfte der Unternehmen, die sich Unterstützung in rechtlichen Fragestellungen wünscht, hat Fragen zur Zusammenarbeit mit Lieferanten und Partnern, etwa zur Haftung. Mehr als ein Drittel hätte gern Hinweise zum Abschluss von Cyberversicherungen.

Gewünschte rechtliche Hinweise



Von denjenigen Unternehmen, die organisatorische bzw. Prozessunterstützung anmelden, wünschen sich 48 Prozent Unterstützung bei der Risikoanalyse im Unternehmen und fortlaufende Updates zu akuten Bedrohungssituationen für Unternehmen (Lageinformationen bzw. sog. Lagebild). Der Staat kann unterstützen, indem er passgenaue Informationen zur aktuellen Sicherheitslage zur Verfügung stellt. Das Lagebild sollte Informationen zu Cyber- und analogen Bedrohungen enthalten, verständlich sein und konkrete Handlungsempfehlungen enthalten. Ist ein IT-Notfall eingetreten, wünschen sich 34 Prozent Unterstützung durch staatliche Stellen. Die betroffenen Unternehmen wissen häufig nicht, an wen sie sich im Schadensfall um Hilfe wenden können. Hier sollten die Sicherheitsorgane deutlich besser qualitativ und quantitativ aufgestellt und das Zusammenspiel zwischen den Behörden verbessert werden.

Das Hauptaugenmerk der nachgefragten Unterstützungsleistungen bezieht sich jedoch auf präventive Maßnahmen: 45 Prozent der Unternehmen, die organisatorische bzw. Prozessunterstützung anmelden, sehen Bedarf an Informationen zur Vorbeugung bzw. zum Umgang mit IT-Sicherheitsvorfällen (z. B. Notfallplan). Jeweils 41 Prozent wünschen Unterstützung bei der Sensibilisierung für das Thema Informationssicherheit im Betrieb und bei der Weiterbildung von Mitarbeitenden.



Einerseits geht mit der Auslagerung der IT und der Umsetzung von IT-Sicherheitsanforderungen auf externe Dienstleister bzw. Cloud-Anbieter häufig ein Zuwachs an IT-Sicherheit einher. Andererseits identifiziert das BSI in seinem aktuellen Lagebericht Angriffe auf externe IT-Lösungen, die Unternehmen einsetzen bzw. Angriffe auf Cloud-Angebote, die von Unternehmen genutzt werden, als eine der drei Hauptbedrohungen für Unternehmen.

Von Seiten der Unternehmen ist Augenmerk gefragt bei der Auswahl sicherer Produkte, Cloudlösungen oder eines vertrauenswürdigen IT-Dienstleisters. Und so gibt auch ein knappes Drittel der Unternehmen an, dass sie Unterstützung bei der Suche nach einem vertrauenswürdigen IT-Dienstleister benötigen. In den Freitextantworten wird darauf hingewiesen, dass dazu auch Informationen etwa zu Lastenheften, Projektbegleitung etc. sinnvoll wären.

Ein Lösungsansatz wäre, dass Vorprodukte mit bereits „eingebauter Sicherheit" und ohne Sicherheitslücken hergestellt werden. Entsprechende gesetzliche Regelungen existieren bereits, sind verabschiedet und müssen noch in nationales Recht umgesetzt werden wie die NIS 2.0-Richtlinie, oder werden gerade erarbeitet wie der Cyber Resilience Act. Die gesetzlichen Vorgaben können ihre Wirkung nur dann entfalten, wenn sie als angemessen anerkannt und ernsthaft von allen Beteiligten umgesetzt werden. Der Staat sollte die Umsetzung der rechtlichen Vorgaben durch unterstützende Maßnahmen flankieren – etwa indem er keine Schwachstellen in Softwareprodukten offenhält und auch sonst alles tut, um das Vertrauensverhältnis zwischen Staat und Wirtschaft zu stärken und die Unternehmen in ihren Bemühungen unterstützt. Denn in einer vernetzten Gesellschaft sind alle Beteiligten auf ein vertrauensvolles Miteinander angewiesen. Das komplexe Thema Informationssicherheit erfordert neue Kooperationsformen, in denen jeder nach seinen Fähigkeiten einen Beitrag leisten muss.

Die IHK-Organisation unterstützt...

DIHK und IHKs vermitteln in zahlreichen Formaten Informationen zu möglichen Gefährdungen und geben praktische Hinweise, wie Unternehmen ihre Informationssicherheit verbessern können. Die IHK-Organisation engagiert sich u. a. im Beirat der Allianz für Cybersicherheit. Im Rahmen der Allianz für Cybersicherheit arbeiten wir an einer Verbesserung der Informationen zur Gefährdungslage und entsprechenden Handlungsempfehlungen.

https://www.dihk.de/de/themen-und-positionen/wirtschaft-digital/daten-und-informationssicherheit

Außerdem bieten wir im Rahmen unserer Webinarreihe #gemeinsamdigital jeden Monat Online-Informationsveranstaltungen zu diversen informationssicherheitsrelevanten Themen an.

https://www.dihk.de/de/themen-und-positionen/wirtschaft-digital/gemeinsamdigital

Fragebogen Schwerpunktthema Daten- und Informationssicherheit

Welche der aufgeführten Maßnahmen setzen Sie im Unternehmen ein, um den Herausforderungen der Daten- und Informationssicherheit zu begegnen? [Mehrfachauswahl]

Strategische Maßnahmen

- ☐ Risikoanalyse
- ☐ Anwendung von IT-Sicherheitsstandards/Informationssicherheitsmanagementsystem (z. B. VDS 10005, CISIS 12, ISA+ ISIS12, ISO/IEC 27001, BSI IT-Grundschutz)

Organisatorische Maßnahmen

- ☐ Informationssicherheitsbeauftragte(r)
- ☐ Nutzungs-Richtlinien für die Mitarbeitenden
- ☐ Regelmäßige Mitarbeiterschulungen
- ☐ Notfallplan/-handbuch • Externer Sicherheitstest des Netzwerks (Penetrationstests)
- ☐ Cyberversicherungen

Technische Maßnahmen

- ☐ laufende Aktualisierung der IT-Sicherheitsmaßnahmen
- ☐ Verschlüsselung (z.B. von E-Mails)
- ☐ Identitätsmanagement (z.B. Authentifikation via Passwort; Rechte-/Rollenverwaltung)
- ☐ Regelmäßige Sicherungskopien (Backups)

Was bremst aus Ihrer Sicht am meisten, mehr Cybersicherheit im Unternehmen zu implementieren? [TOP 3]

- ☐ Initiale Anschaffungskosten/Einführungsaufwand für IT-Sicherheitsmaßnahmen
  wenn ja; Pop-up: In Bezug auf die initiale Anschaffung der IT-Sicherheitsmaßnahmen:
  Wie hoch ist der Anteil, der an externe Dienstleister ausgelagert wurde bzw. wird?
  - ☐ die IT-Sicherheitsmaßnahmen wurden weitestgehend von der IT-Abteilung selbst realisiert
  - ☐ wir haben verfügbare Produkte am Markt eingekauft
  - ☐ wir haben einen externen Dienstleister mit dem überwiegenden Teil der Anschaffung beauftragt
- ☐ Aufwand/Kosten für laufenden technischen Betrieb/Anpassungen/Aktualisierungen
  wenn ja, Pop-up: Durch wen wird der laufende technische Betrieb der IT-Sicherheitsmaßnahmen erbracht?
  - ☐ hauptsächlich durch externen Dienstleister
  - ☐ hauptsächlich in Eigenleistung
  - ☐ Sonstiges (Freitext)

- ☐ Technisch-organisatorische Prozessanpassungen im Unternehmen
- ☐ Einbeziehung von Mitarbeitenden
- ☐ im Unternehmen gibt es keine IT-Fachkräfte für das Thema
- ☐ Sonstiges (Freitext)

Wobei wünscht sich Ihr Unternehmen Unterstützung durch den Staat, IHKs oder anderen Organisationen? [Mehrfachnennungen möglich]

- ☐ Informationen über technische Präventionsmaßnahmen (z.B. Ende-zu-Ende Verschlüsselungen)
- ☐ Rechtliche Hinweise
  wenn ja: Pop-up:
  - ☐ Informationen über gesetzliche Sicherheits- und Datenschutzanforderungen
  - ☐ zur Zusammenarbeit mit Lieferanten und Partnern etwa bei Haftungsfragen
  - ☐ Hinweise zum Abschluss von Cyberversicherungen
  - ☐ Sonstiges (Freitext)
- ☐ Organisatorische bzw. Prozessunterstützung
  wenn ja: Pop-up:
  - ☐ Unterstützung bei der Suche nach einem vertrauenswürdigen IT-Dienstleister
  - ☐ passgenau aufbereiteter Einstieg in das Thema IT-Sicherheit
  - ☐ Unterstützung bei der Risikoanalyse im Unternehmen, fortlaufende Updates zu akuten Bedrohungssituationen für Unternehmen (Lageinformationen bzw. sog. Lagebild)
  - ☐ Informationen zur Vorbeugung bzw. zum Umgang mit IT-Sicherheitsvorfällen (z.B. Notfallplan)
  - ☐ Unterstützung durch die öffentliche Hand bei Notfällen
  - ☐ Unterstützung bei der Suche nach IT-Sicherheits-Fachkräften
  - ☐ Sensibilisierung für das Thema im Betrieb, Unterstützung bei der Weiterbildung von Mitarbeitenden
  - ☐ Sonstiges (Freitext)
- ☐ Möglichkeit einer aktiven Teilnahme an einem Netzwerk zu mehr IT-Sicherheit
- ☐ Mein Unternehmen benötigt keine Unterstützung durch die genannten Organisationen
- ☐ Ich bin von Initiativen/Organisationen informiert, aber mir fehlt das umsetzbare Ergebnis
- ☐ Sonstiges: (Freitext)