KPMG

ZIA
DIE IMMOBILIENWIRTSCHAFT

Cyber Security in der Immobilienwirtschaft

Studie in Kooperation mit dem Zentralen Immobilien Ausschuss (ZIA)

Inhalt

Vorwort KPMG 4

Einführung ZIA 5

1. Management Summary 6

2. Überblick Studie 10

3. Handlungsfeld Unternehmen

3.1 Schützenswerte Unternehmens-IT 13
3.2 Strategische Awareness für das Unternehmen 14
3.3 Management von Cyber-Risiken im Unternehmen 16
3.4 Prozesse im Unternehmen 17
3.5 Ausgewählte Detailbetrachtungen 18

4. Handlungsfeld Immobilie

4.1 Schützenswerte Immobilien-Infrastruktur 23
4.2 Strategische Awareness für Immobilien 24
4.3 Management von Cyber-Risiken in der Immobilie 25
4.4 Notfallplan für kritische Technologie 26
4.5 Prozesse für die Immobilien 26

5. Handlungsfeld Mitarbeitende

5.1 Strategische Awareness der Mitarbeitenden 29
5.2 Organisation der Cyber Security 30
5.3 Management von Cyber-Risiken bei Mitarbeitenden 35
5.4 Informationssicherheitskultur und Weiterbildung bei Mitarbeitenden 37

6. Fazit 40

Vorwort KPMG

Immobilien und Cyber Security – was hat denn das miteinander zu tun? Bei vielen wird der erste Gedanke wahrscheinlich sein, dass diese beiden Begriffe wenig bis nichts miteinander zu tun haben, da mit dem Begriff Cyber Security eher technologische Themen wie zum Beispiel Computersysteme, Netzwerke und Software in Verbindung gebracht werden. In diesen Zusammenhängen lassen sich sofort potenzielle Bedrohungen (u. a. Datendiebstahl, Phishing, Malware oder Trojaner) ableiten und die Notwendigkeit von Cyber Security erschließt sich unmittelbar.

Wenn man sich die Fragestellung in unserer heutigen vernetzten Welt mit dem Aspekt der Digitalisierung in der Immobilienwirtschaft und Begrifflichkeiten wie Smart Home oder Smart Building jedoch erneut stellt, wird der Zusammenhang schnell deutlich. Mit sehr hoher Wahrscheinlichkeit ist man dann sogar je nach Wohnsituation nicht nur im beruflichen Umfeld, sondern persönlich direkt betroffen.

Wer nutzt als Privatperson nicht die Vorteile des Smart Home wie zum Beispiel mit dem Internet verbundene Haushaltsgeräte oder sensorgesteuerte Hausautomation? Welches Unternehmen setzt in seinen Objekten keine Sensorik für Wärmemessung oder Wartungsunterstützungen ein? Haben Sie sich hier privat oder aus Unternehmenssicht schonmal mit dem Thema Cyber Security aktiv befasst? In den meisten Fällen wird die Antwort wohl eher „Nein“ lauten, weil man die Risiken entweder nicht direkt sieht oder sich in den vielen Fällen auf den Hersteller der Lösung verlässt, frei nach dem Motto „Hier wird schon nichts passieren“.

Überträgt man diese Einstellung auf ein Immobilienunternehmen bewegt man sich jedoch unmittelbar in einem riskanten Umfeld. Sowohl im Unternehmen als auch bei den Beständen werden eine Vielzahl von Technologien unterschiedlichster Hersteller eingesetzt, die sowohl mittel- als auch unmittelbar einen konkreten Zusammenhang zum Thema Cyber Security ableiten lassen.

Die Digitalisierung ist in der Branche angekommen und schreitet weiter voran. Aus der Digitalisierung heraus ergeben sich jedoch Pflichten zur Minimierung der damit verbundenen Risiken, die eine erweiterte Sicht auf das Thema erfordern.

Neben den genutzten ERP-Systemen und weiteren IT-Applikationen und deren Betrieb sind unter anderem technische Einbauten in den Gebäuden, die über einen webbasierten Zugang verfügen relevant für die Betrachtung unter Cyber-Security-Aspekten. Einige mögliche Beispiele sind Lösungen für Verbrauchsmessungen (Smart Metering), Photovoltaikanlagen, Fernzugriffe für Heizungssteuerung oder Sensorik für Predictive Maintenance (vorausschauende Instandhaltung). Die Digitalisierung von Unternehmen und Gebäuden schreitet voran, der technische Standard entwickelt sich rasant, aber werden auch mögliche Risiken, die daraus entstehen, betrachtet? Wo sieht sich die Immobilienwirtschaft bei diesem Thema und wird es überhaupt als relevant angesehen?

Gemeinsam mit dem ZIA wollen wir diesen Fragen nachgehen und ermitteln, wo die Immobilienwirtschaft beim Thema Cyber Security steht. Durch diese Studie „Cyber Security in der Immobilienwirtschaft“, können wir mit Unterstützung der gesamten Branche ein übergreifendes Bild zum Thema Cyber Security schaffen und wesentliche Fragestellungen beantworten. Die Studie soll dabei unterstützen, eine Transparenz zum Thema herzustellen und eigene Ansätze zu hinterfragen oder weiterzuentwickeln.

Zu den Handlungsfeldern

- Unternehmen,
- Immobilie und
- Mitarbeitende

konnten Erkenntnisse gesammelt werden, die den aktuellen Status zum Umgang mit Cyber Security in der Branche transparent macht.

Wir danken allen Teilnehmenden für die rege Beteiligung und aktive Mitwirkung an der Studie und wünschen Ihnen eine spannende Lektüre, verbunden mit einem persönlichen Erkenntnisgewinn aus den vorliegenden Studienergebnissen.

Marco Müth
Partner
Head of Real Estate Germany

Robert Betz
Partner
EMA Head of Digital Real Estate

Einführung ZIA

Fast 140.000 Fälle von Cyber Crime in Deutschland 2022[1], 206 Milliarden Euro Schaden pro Jahr durch Datendiebstahl, Spionage und Sabotage[2] – eigentlich mehr als ein Grund also, sich des Themas Cyber Security anzunehmen.

Gerade in einer Welt, die zunehmend digital arbeitet und vernetzt ist, wird auch die Immobilienwirtschaft vermehrt zum Ziel von Cyber-Angriffen. Die Dynamik dieser Bedrohung wurde lange Zeit unterschätzt, da die Branche traditionell eher auf physische Sicherheitsmaßnahmen fokussiert war. Aufgrund des vermehrten Einsatzes von Smart-Building-Technologien ist die gebaute Umwelt jedoch nicht länger isoliert von Angriffen im Cyber-Raum. Die rasante Digitalisierung der Immobilienwirtschaft hat zu einem Paradigmenwechsel geführt, der die Notwendigkeit einer umfassenden Auseinandersetzung mit Cyber Security in der Branche unterstreicht.

Die Erkenntnis, dass Cyber Security in vielen Unternehmen oft noch nicht den Stellenwert einnimmt, der dem Thema gebührt, ist alarmierend. Um jedoch die Sicherheit unserer digitalen Infrastruktur zu gewährleisten, muss Cyber-Sicherheit zwangsläufig zur Top-Priorität in der obersten Führungsriege werden. Nur durch ein gemeinsames Verständnis und eine aktive Beteiligung der Führungsebene, kann das gesamte Unternehmen resilient gegen Cyber Crime aufgestellt werden.

Die Ergebnisse dieser Studie verdeutlichen, dass in jedem Unternehmen der Mensch als potenzielles Einfallstor für Cyber-Angriffe betrachtet werden muss. Daher sind eine weitreichende Risikoaufklärung und kontinuierliche Schulung der Mitarbeitenden von essenzieller Bedeutung. Die Sensibilisierung für Cyber-Sicherheit muss integraler Bestandteil unserer Unternehmenskultur werden, um die Widerstandsfähigkeit gegenüber Cyber-Bedrohungen zu stärken.

Die Studie unterstreicht ebenfalls, dass es keine „One Size Fits All"-Lösung für Cyber-Sicherheit gibt. Jedes Unternehmen muss seine eigenen Schwachstellen identifizieren und gezielt Maßnahmen ergreifen, um Cyber-Angriffe zu verhindern. Diese Erkenntnis erfordert eine individuelle und anpassungsfähige Herangehensweise an die Cyber-Sicherheit, die sich den spezifischen Bedürfnissen und Risiken eines jeden Unternehmens stellt.

Für Ihre aktive Beteiligung an unserer Studie möchte ich mich herzlich bedanken – Ihre Perspektiven und Einblicke sind für uns äußerst wichtig. Zudem geht mein Dank an KPMG für die produktive Zusammenarbeit an dieser aufschlussreichen Studie. Die gewonnenen Erkenntnisse bieten nicht nur wertvolle Einblicke in die aktuelle Lage der Cyber-Sicherheit in der Immobilienwirtschaft, sondern dienen auch als Handlungsgrundlage für zukünftige Strategien und Maßnahmen.

Ich hoffe, dass diese Studie dazu beiträgt, das Bewusstsein für Cyber-Sicherheit zu schärfen und unsere Branche auf dem Weg zu einer sicheren, digitalen Zukunft unterstützt.

Aygül Özkan
Stellvertretende Hauptgeschäftsführerin
ZIA Zentraler Immobilien Ausschuss e.V.

[1] Bundeskriminalamt (2023)
[2] Bitkom Research (2023)

1 | Management Summary

Handlungsfeld Unternehmen

Key Fact 1

Je größer das Unternehmen, desto wahrscheinlicher ist es, dass ein Cyber-Angriff erfolgt.

Die Untersuchung verdeutlicht, dass Cyber-Angriffe ein breites Spektrum von Unternehmen betreffen, unabhängig von ihrer Größe. Dennoch steigt mit der Unternehmensgröße die Wahrscheinlichkeit, Opfer von Cyber-Attacken zu werden. Die durchschnittlich geschätzte Anzahl von 282 Angriffen pro Jahr unterstreicht die Dringlichkeit, robuste Sicherheitsmaßnahmen zu implementieren, um sich vor diesen Bedrohungen zu schützen.

Key Fact 2

Unternehmen, welche die Relevanz von Cyber Security besonders hoch einschätzen, ergreifen dennoch seltener proaktive Maßnahmen zur Verbesserung.

Obwohl 93 % der teilnehmenden Unternehmenden eine Zunahme von Cyber-Angriffen erwarten und die Relevanz von Cyber Security hoch einschätzen (mit einem durchschnittlichen Wert von 8,4 von 10), bewerten Unternehmen, die lediglich ein grundlegendes Verständnis ihrer Cyber-Security-Lage haben und keine proaktiven Maßnahmen ergreifen, diese Relevanz noch höher (9 von 10). Dies verdeutlicht eine Diskrepanz zwischen der wahrgenommenen Bedeutung von Cyber Security und den tatsächlich ergriffenen proaktiven Schritten zur Verbesserung, was darauf hindeutet, dass eine bewusste Wahrnehmung nicht zwangsläufig zu entsprechenden Handlungen führt.

Key Fact 3

51 % der teilnehmenden Unternehmen haben bereits eine Cyber-Security-Strategie im Unternehmen etabliert, wohingegen 33 % sich in der Phase der Strategieumsetzung befinden.

Die Studie verdeutlicht, dass 51 % der teilnehmenden Unternehmen bereits eine Cyber-Security-Strategie etabliert haben, wobei 24 % eine bestehende Strategie kontinuierlich anpassen und etwa 27 % regelmäßige Überprüfungen zur Anpassung an Bedrohungsveränderungen durchführen. Allerdings befinden sich etwa 33 % der Unternehmen noch in der Phase der Strategieumsetzung, was den Willen zur Stärkung der Cyber-Sicherheit zeigt, jedoch auch darauf hinweist, dass viele noch keine abgeschlossene Strategie haben. Besonders Unternehmen mit weniger als 20 Mitarbeitenden sind noch in der Phase der Strategieentwicklung, wobei 55 % angeben, dass sie aktuell an einer solchen Strategie arbeiten.

Key Fact 4

Je höher die Relevanz von Cyber-Security in einem Unternehmen, desto eher werden Vorgaben und Richtlinien auf der Vorstandsebene verabschiedet.

Die Studie zeigt, dass etwa 60 % der Befragten, die die Bedeutung von Cyber Security in ihrem Unternehmen als besonders hoch einschätzen (Bewertung von 9 bis 10), Vorgaben und Richtlinien zur Cyber Security auf Vorstandsebene verabschiedet haben. Dies verdeutlicht eine starke Korrelation zwischen der Wahrnehmung der Relevanz von Cyber-Security und der Implementierung entsprechender Richtlinien auf höchster Führungsebene. Unternehmen, die die Bedeutung dieses Themas hoch bewerten, sind somit eher geneigt, gezielte Vorgaben und Richtlinien auf Vorstandsebene zu etablieren, um ihre Cyber-Sicherheit zu stärken.

Key Fact 5

Bei

60 % aller Unternehmen ist eine Sicherheitsüberprüfung von Software- und Hardwarekomponenten vorgeschrieben.

Eine festgelegte Prüfung der Komponenten minimiert das Risiko der Abweichung von den eigenen Sicherheitsanforderungen. Die Prüfung sollte daher bestenfalls nicht nur initial, sondern auch bei Updates vollzogen werden. Bei 40 % finden jedoch keine oder lediglich sporadische Prüfungen statt.

Key Fact 6

Zum Schutz der Unternehmens-IT hat sich die Zwei-Faktor-Authentisierung in den meisten Unternehmen etabliert.

Die Studie verdeutlicht, dass Unternehmen generell ein solides Verständnis von möglichen Log-In-Methoden aufweisen, wobei die Zwei-Faktor-Authentisierung als eine der am häufigsten genutzten Methoden zur Sicherung der Unternehmens-IT gilt. Durchschnittlich verwenden Unternehmen zwei verschiedene Log-In-Methoden, wobei einige sogar bis zu fünf Methoden simultan einsetzen. Die beliebteste Kombination ist die Nutzung der Zwei-Faktor-Authentisierung in Verbindung mit Single-Sign-On, was darauf hinweist, dass Unternehmen vermehrt auf multifaktorielle Sicherheitsansätze setzen, um ihre IT-Systeme zu schützen.

Key Fact 7

Nur

45 % der Unternehmen setzen auf eine zentrale und toolgestützte Lösung bei der Verwaltung und Nutzung mobiler Endgeräte.

Die Untersuchung zeigt, dass lediglich 45 % der Unternehmen eine zentrale, toolgestützte Lösung für die Verwaltung mobiler Endgeräte nutzen, was eine dezidierte Sicherheitsrichtlinie impliziert. Während etwa 30 % der teilnehmenden Unternehmen formelle Listen von mobilen Hard- und Softwarekomponenten überwachen, zeigen jeweils 7 % der Unternehmen eine fehlende oder nicht bekannte Richtlinie, was potenzielle Sicherheitslücken aufzeigt und die Notwendigkeit einer umfassenden Cyber-Sicherheitsrichtlinie betont.

Handlungsfeld Immobilie

Key Fact 8

Für

89 % **der Befragten spielen Smart-Building-Technologien eine Rolle. Bei 69 % der teilnehmenden Unternehmen ist in den Immobilien mindestens eine Smart Building-Technologie verbaut, die es zu schützen gilt.**

Die Studie betont, dass 89 % der Befragten die Bedeutung von Smart-Building-Technologien anerkennen, wobei bei 69 % der Unternehmen mindestens eine dieser Technologien in den Immobilien verbaut ist. Dies unterstreicht die Notwendigkeit, potenzielle Angriffsflächen dieser Technologien von Anfang an zu schützen, kontinuierlich zu überwachen und proaktiv zu verbessern, um möglichen Missbrauch zu verhindern.

Key Fact 9

Fast 80 % der Unternehmen haben keine portfolio-weite/unternehmensweite Strategie zum Schutz der Gebäudetechnik vor Cyber-Angriffen.

Nahezu 80 % der teilnehmenden Unternehmen haben keine unternehmensweite Strategie zur Absicherung ihrer Gebäudetechnik vor Cyber-Angriffen entwickelt. Lediglich 20 % geben an, Strategien zum Schutz dieser Technik implementiert zu haben, was auf eine erhebliche Lücke in den Sicherheitsvorkehrungen für Gebäudetechnik hinweist.

Handlungsfeld Mitarbeitende

Key Fact 10

Es ist eine Diskrepanz zwischen der Eigenwahrnehmung und der Fremdwahrnehmung bezüglich der Kenntnisse der nicht leitenden Mitarbeitenden zu Cyber-Risiken vorhanden. Die nicht leitenden Mitarbeitenden schätzen ihre Kenntnisse schlechter ein, wohingegen die Einschätzung durch die leitenden Mitarbeitenden höher ausfällt.

Die Studie betont eine klare Diskrepanz in der Wahrnehmung der Kenntnisse zu Cyber-Risiken zwischen nicht leitenden Mitarbeitenden und Führungspersonen, wobei die Einschätzungen der Führungsebene im Durchschnitt höher ausfallen als die Selbsteinschätzungen der nicht leitenden Mitarbeitenden.

Key Fact 11

Überwiegend kümmert sich nur ein Mitarbeitender um Cyber Security, circa 70 % der Unternehmen beauftragen externe Dienstleistende.

Über 70 % der befragten Unternehmen binden externe Dienstleistende in Fragen der Cyber Security ein. Interessanterweise zeigen die Ergebnisse keine eindeutigen Korrelationen zwischen Unternehmensstandort, Anzahl der für Cyber-Security-Verantwortlichen, der Beauftragung von externen Dienstleistenden und der Unternehmensgröße.

Key Fact 12

Für den Umgang mit Dienstleistenden geben nur 47 % der Unternehmen an, formelle Regelungen zur Einhaltung von Sicherheitsvorgaben getroffen zu haben.

Lediglich 47 % der teilnehmenden Unternehmen geben an, formelle Regelungen zur Einhaltung von Sicherheitsvorgaben mit ihren Dienstleistenden implementiert zu haben. Während einige Unternehmen strenge und vertraglich festgehaltene Sicherheitsstandards durchsetzen, gibt es wiederum auch Unternehmen, die keine spezifischen Regelungen oder informelle Vorgaben für ihre Dienstleistenden aufweisen.

Key Fact 13

In

79 %

der teilnehmenden Unternehmen werden Schulungen zur Cyber Security für die Mitarbeitenden anhand eines Schulungsplans durchgeführt.

Die Studie zeigt, dass in 79 % der teilnehmenden Unternehmen Schulungen zum Thema Cyber Security mithilfe von Schulungsplänen für die Mitarbeitenden zur Sensibilisierung und zur Awareness durchgeführt werden. Es besteht eine Vielfalt in den Ansätzen der Schulungspläne, wobei jedoch nur eine geringe Anzahl auf spezifische Kompetenzlücken in der Belegschaft abzielt.

2 | Überblick Studie

Datenbasis und Teilnehmende

Die vorliegende Studie wurde im zweiten Quartal 2023 vorbereitet und die Fragestellungen gemeinsam mit dem ZIA und ausgewählten Unternehmen der Immobilienbranche entwickelt und verprobt.

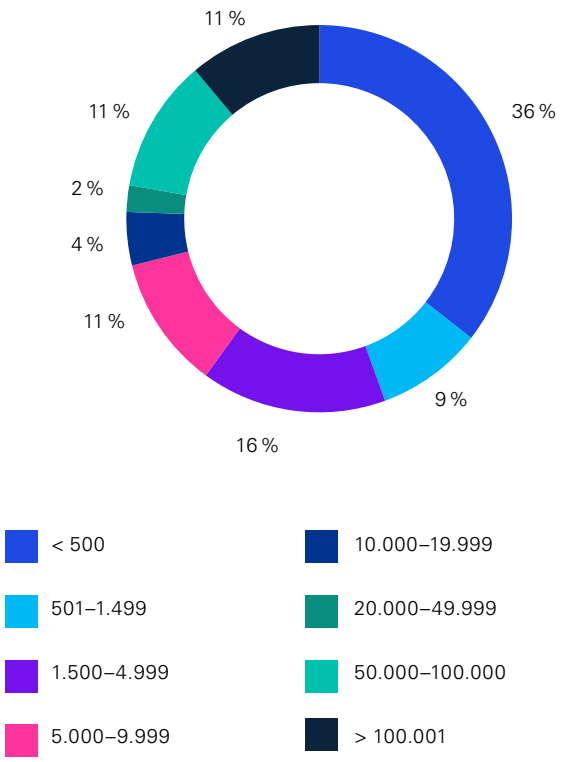
Aus diesen Ergebnissen wurde ein Online-Befragungsbogen entwickelt, den über 100 teilnehmende Personen aus allen Bereichen der Branche ausgefüllt haben. Neben den Asset-Klassen Wohnen, Handel und Büro sind auch Hotel/Gastgewerbe, Industrie/Produktion sowie Lager/Logistik, Gesundheit und Soziales vertreten.

Zudem bilden die teilnehmenden Unternehmen die Immobilienbranche nahezu ganzheitlich ab. Neben Fonds- und Asset Management, Banken, Versicherungen, Wohnungsunternehmen, Investoren und Facility-Management-Mitarbeitenden haben sich auch Property Management, Bauunternehmen und Projektentwicklungen an der Umfrage beteiligt.

Die Teilnehmenden an der Studie bilden zudem einen Querschnitt aus allen Führungs- und Fachebenen der Immobilienwirtschaft, wobei der Anteil von Mitarbeitenden in leitenden Funktionen mehr als 85 % der Teilnehmenden beträgt.

- Vorstand (C-Level), Geschäftsleitung 38 %
- Bereichs-/Abteilungs-/Teamleitung 49 %
- Mitarbeitende/Sonstiges 13 %

Abbildung 1:
Übersicht der Unternehmen nach Anzahl der verwalteten Objekte



Quelle: KPMG in Deutschland, 2023; Rundungsdifferenzen möglich

3 | Handlungsfeld Unternehmen

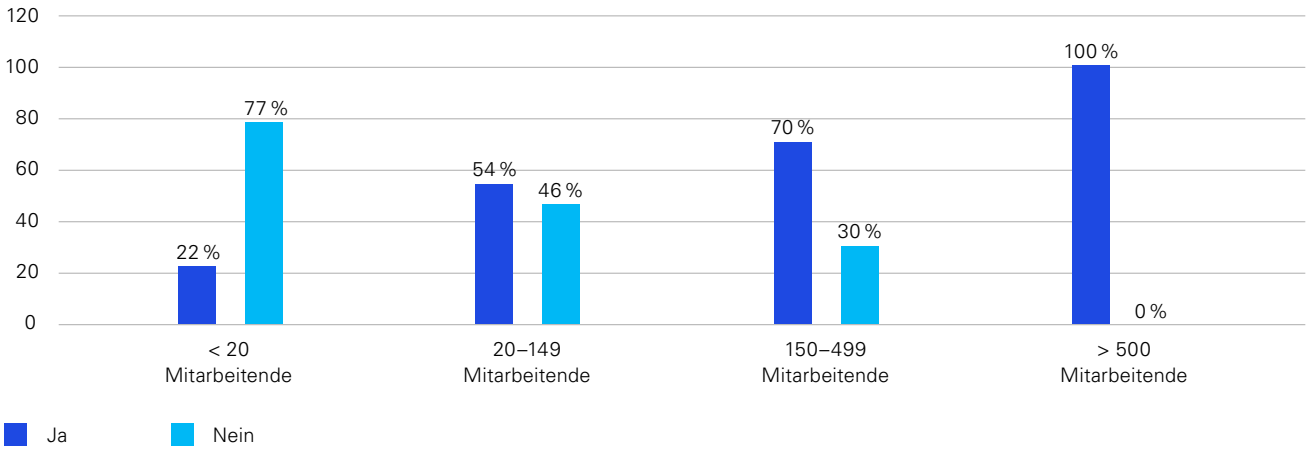
Die erste Betrachtungsebene von Cyber Security im Rahmen dieser Studie blickt auf das Unternehmen.

Hier stellen sich insbesondere Fragen zu der Lokalisation von Cyber Security im Unternehmensorganigramm, der Anzahl an Mitarbeitenden, welche sich mit Cyber Security beschäftigen, und der Bedrohungslage des Unternehmens. Die Antworten auf diese grundlegenden Fragen benötigt ein Unternehmen, um eine konsistente Cyber-Security-Strategie zu erstellen, Möglichkeiten der Gefahrenabwehr zu ermitteln und die Schutzmechanismen zu überprüfen und zu verbessern. Dieser iterative Prozess ermöglicht eine umfängliche Sicherung des Unternehmens, der verwalteten Immobilien und der Mitarbeitenden.

3.1 Schützenswerte Unternehmens-IT

Mehr als 55 % der teilnehmenden Unternehmen gaben an, dass sie Kenntnis von Cyber-Attacken auf die Systeme des Unternehmens oder auf die Systeme der (IT-)Dienstleistenden haben. Mehr als 50 % der Unternehmen mit mehr als 20 Mitarbeitenden haben Kenntnis über Cyber-Attacken auf die eigenen Systeme oder die der (IT-)Dienstleistenden. Dies zeigt, dass diese Gefahr nicht nur für große Unternehmen besteht, sondern auch kleinere Unternehmen als Angriffsziel ausgesucht werden. Dennoch nimmt die Kenntnis, und somit vermutlich auch das Risiko eines Angriffes, mit der Unternehmensgröße zu. Die durchschnittliche geschätzte Anzahl von Angriffen pro Jahr aller Unternehmen beläuft sich auf 282.

Abbildung 2:
Kenntnis über Cyber-Attacken auf die Unternehmen prozentual gruppiert nach Anzahl der Mitarbeitenden



Quelle: KPMG in Deutschland, 2023; Angaben in Prozent, Rundungsdifferenzen möglich

93 % der befragten Unternehmen prognostizieren, dass die Anzahl der Cyber-Attacken in den nächsten fünf Jahren steigen wird. Dementsprechend hoch wird auch die Relevanz von Cyber Security für das eigene Unternehmen eingeschätzt, der durchschnittliche Wert beträgt 8,4 auf einer Skala von eins bis zehn. Auffallend ist, dass dieser Wert steigt, wenn ausschließlich die Unternehmen betrachtet werden, die laut Aussage der Teilnehmenden lediglich ein „grobes Verständnis" der eigenen Cyber-Security-Lage haben und keine proaktiven Maßnahmen zur Verbesserung durchführen (9/10).

Key Fact 1

Je größer das Unternehmen, desto wahrscheinlicher ist es, dass ein Cyber-Angriff erfolgt.

Key Fact 2

Unternehmen, welche die Relevanz von Cyber Security besonders hoch einschätzen, ergreifen dennoch seltener proaktive Maßnahmen zur Verbesserung

3.2 Strategische Awareness für das Unternehmen

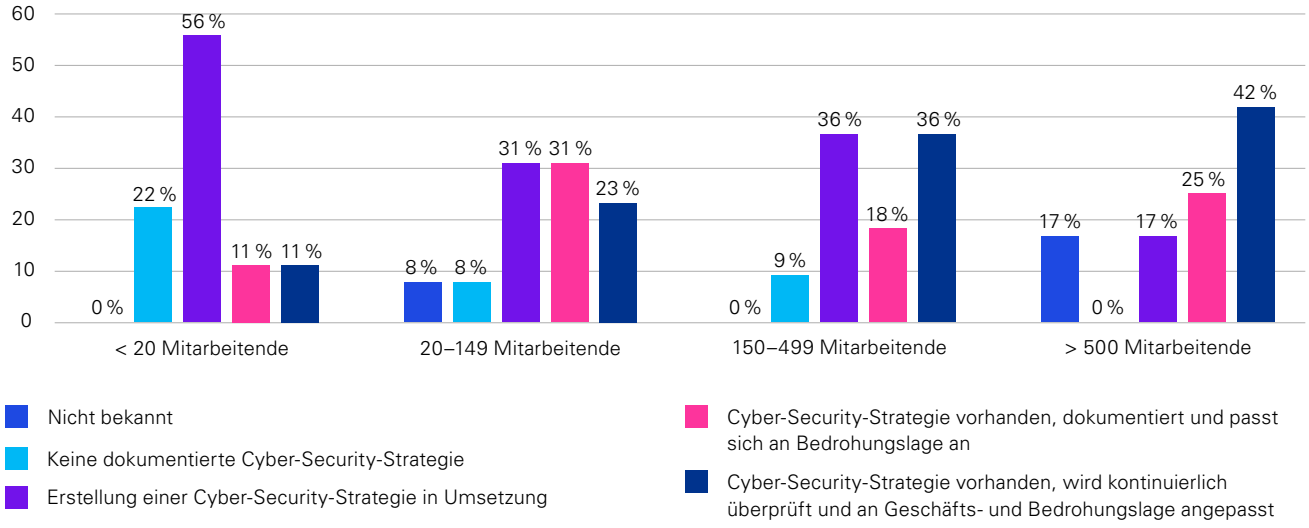
24 % der teilnehmenden Unternehmen geben an, dass sie eine vorhandene, dokumentierte Cyber-Security-Strategie haben, die kontinuierlich angepasst wird, um den Veränderungen in der Bedrohungslandschaft gerecht zu werden. Rund 27 % der teilnehmenden Unternehmen führen regelmäßige Überprüfungen ihrer Cyber-Security-Strategie durch und passen sie an Veränderungen an. Circa 33 % befinden sich in der Phase der Umsetzung einer Cyber-Security-Strategie. Dies zeigt den Willen, eine Strategie zu entwickeln, um die Cyber-Sicherheit zu stärken, jedoch deutet es auch darauf hin, dass viele noch nicht über eine abgeschlossene Strategie verfügen. Jedoch haben circa 9 % der Teilnehmenden keine dokumentierte Cyber-Security-Strategie, was auf potenzielle Schwächen oder fehlende Strukturen im Bereich der Cyber-Sicherheit hinweisen könnte. Wiederum weitere 7 % geben an, dass ihnen eine Strategie zur Cyber-Sicherheit nicht bekannt ist.

Wenn die vorliegenden Daten in Abhängigkeit zu der Unternehmensgröße betrachtet werden, wird deutlich, dass insbesondere die Unternehmen mit weniger Mitarbeitenden noch keine Cyber-Security-Strategie erstellt haben. Immerhin gaben 55 % der Teilnehmenden mit weniger als 20 Mitarbeitenden an, dass eine derartige Strategie aktuell in Umsetzung sei.-

Key Fact 3

51 % der teilnehmenden Unternehmen haben bereits eine Cyber-Security-Strategie im Unternehmen etabliert, wohingegen 33 % sich in der Phase der Strategieumsetzung befinden.

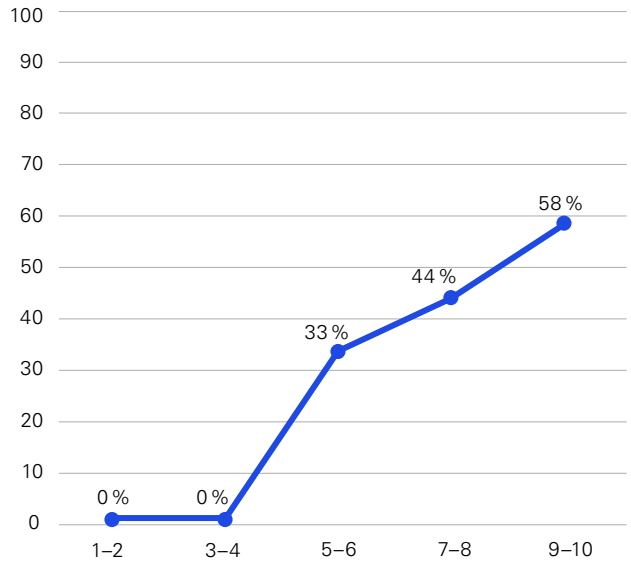
Abbildung 3:
Vorhandene Cyber-Security-Strategien nach Unternehmensgröße



Quelle: KPMG in Deutschland, 2023; Angaben in Prozent, Rundungsdifferenzen möglich

Von den Teilnehmenden, welche die Relevanz des Themas Cyber Security im Unternehmen hoch bewerten (9–10), haben circa 60 % eine Cyber-Security-Richtlinie auf Vorstandsebene verabschiedet.

Abbildung 4:
Verabschiedung einer Cyber-Security-Richtlinie auf Vorstandsebene gruppiert nach Einordnung der Cyber-Security-Relevanz



Quelle: KPMG in Deutschland, 2023; Angaben in Prozent, Rundungsdifferenzen möglich

Bei den Kenntnissen über die Cyber-Security-Lage haben 20 % der Befragten mit einer Bewertung von 10 angegeben, dass ihr Unternehmen nur ein grobes Verständnis seiner Cyber-Security-Lage aufweist. 80 % hingegen bezifferten dem Unternehmen ein tieferes Verständnis der eigenen Cyber-Security-Lage sowie die proaktive Ergreifung von Maßnahmen zur Verbesserung.

Obwohl 80 % der Teilnehmenden angeben, dass ihr Unternehmen ein Verständnis hat und keine proaktiven Maßnahmen zur Verbesserung der Cyber-Security-Lage betreibt, können lediglich 15 % die Frage nach konkreten Sicherheitsvorfällen (Datenverluste, Trojaner, Cyber-Attacken) in der Vergangenheit verneinen. Dies zeigt, dass auch hier weiterer Verbesserungsbedarf besteht und die bestehenden potenziellen Sicherheitsrisiken minimiert werden müssen.

Key Fact 4

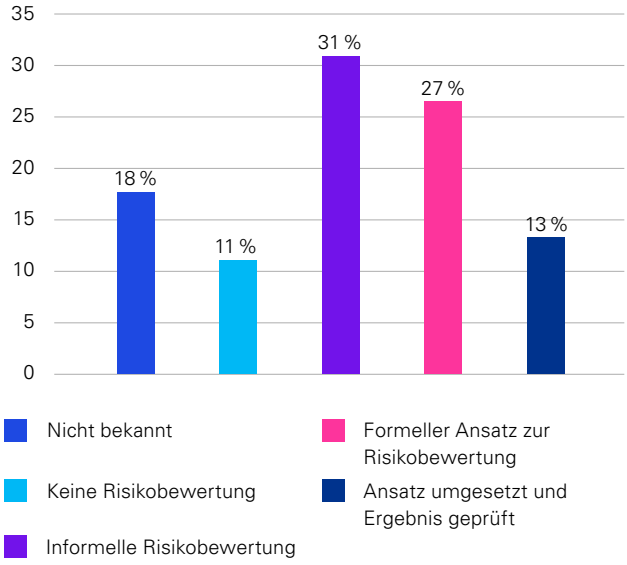
Je höher die Relevanz von Cyber Security in einem Unternehmen, desto eher werden Strategien, Vorgaben und Richtlinien auf der Vorstandsebene verabschiedet.

3.3 Management von Cyber-Risiken im Unternehmen

Im Rahmen der strategischen Ausarbeitungen sollte auch eine entsprechende Identifikation von Risiken stattfinden. Mehr als 82 % der Teilnehmenden führen in ihren Unternehmen eine solche Risikoidentifizierung durch. Auf Basis der durchgeführten Risikoidentifizierung erstellen jedoch nur rund 78 % einen Risikobericht, der anschließend dem Vorstand vorgelegt wird und eine Bewertung der identifizierten Risiken vornimmt.

Mehr als 70 % der Teilnehmenden geben an, mindestens eine informelle Risikobewertung im Unternehmen durchzuführen, bevor eine Entscheidung zur Auslagerung einer Dienstleistung oder Geschäftstätigkeit getroffen wird.

Abbildung 5:
Art und Weise der Risikobewertung der Unternehmen



Quelle: KPMG in Deutschland, 2023; Angaben in Prozent, Rundungsdifferenzen möglich

3.4 Prozesse im Unternehmen

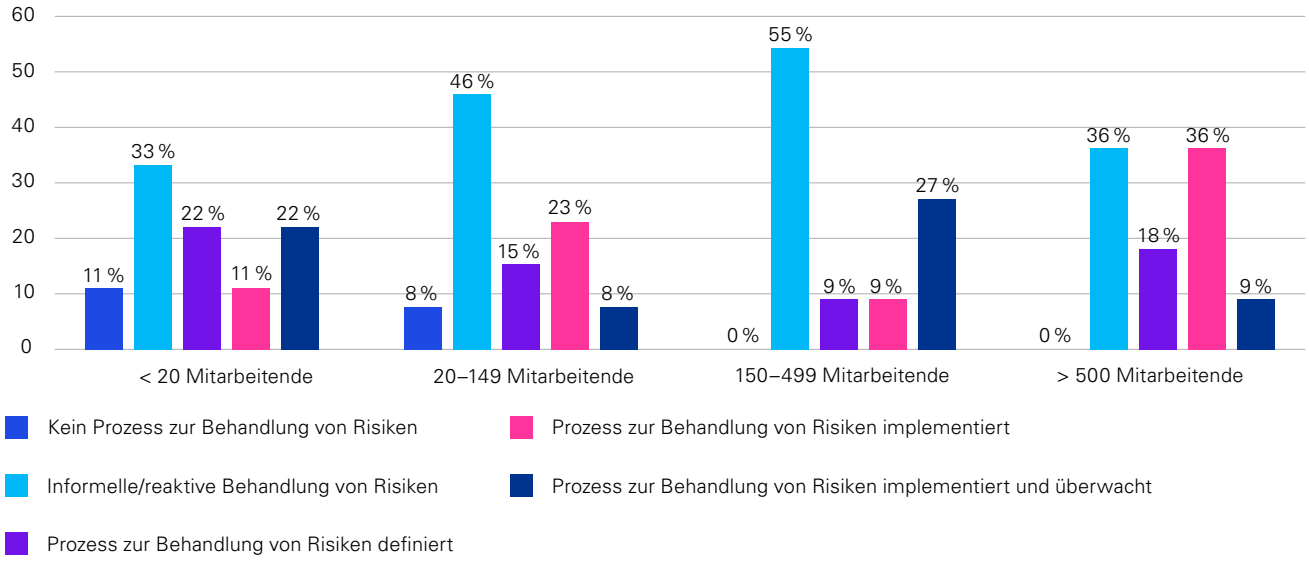
Sofern Risiken erkannt, bewertet und schriftlich festgehalten sind, stellt sich die Frage, wie die Unternehmen mit diesen Risiken umgehen. Dazu sollten interne Prozesse zum Umgang und zur Vorgehensweise definiert und implementiert sein.

- In Unternehmen mit 150 bis 499 Mitarbeitenden dominiert die informelle/reaktive Behandlung von Risiken mit circa 55 %.

- Über 35 % der Unternehmen mit mehr als 500 Mitarbeitenden haben bereits Prozesse zur Behandlung von Risiken implementiert, im Vergleich dazu jedoch nur circa 9 % Unternehmen mit 150 bis 499 Mitarbeitenden.

Die Auswertung der Daten zeigt, dass kleinere Unternehmen tendenziell weniger formelle Prozesse zur Risikobehandlung haben, während größere Unternehmen dazu neigen, formalisierte Ansätze zu implementieren. Eine bedeutende Anzahl von Unternehmen aller Größenkategorien bevorzugt nach wie vor informelle und reaktive Methoden zur Risikobehandlung. Dies unterstreicht die Notwendigkeit für Unternehmen, ihre Risikomanagementpraktiken zu überdenken und Risiken proaktiv anzugehen, um langfristigen Erfolg und Stabilität zu gewährleisten.

Abbildung 6:
Risikobehandlungsprozesse der Unternehmen prozentual gruppiert nach Anzahl der Mitarbeitenden



Quelle: KPMG in Deutschland, 2023; Angaben in Prozent, Rundungsdifferenzen möglich

3.5 Ausgewählte Detailbetrachtungen

Vorbeugende Sicherheitsaudits

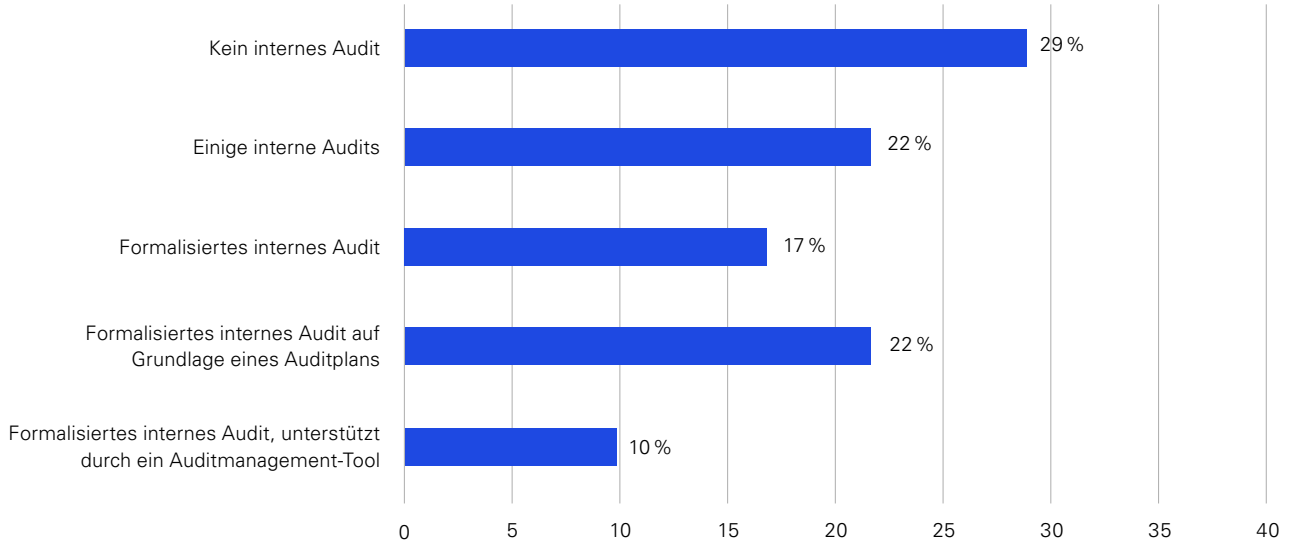
In der heutigen digital vernetzten Welt sind Immobilienunternehmen zunehmend komplexen Cyber-Bedrohungen ausgesetzt, die sowohl von internen als auch von externen Quellen stammen können. Externe Angreifer nutzen häufig ausgeklügelte Phishing-Techniken, Ransomware-Angriffe oder fortgeschrittene persistente Bedrohungen, um in die IT-Systeme einzudringen. Intern kann das Risiko durch unachtsames Personal, unzureichend geschulte Mitarbeitende oder durch Missbrauch von Zugriffsrechten entstehen. Darüber hinaus können Schwachstellen in der Lieferkette oder bei Drittanbietern, die mit kritischen Systemen verbunden sind, zusätzliche Einfallstore bieten. Diese Risiken werden durch die zunehmende Integration von IoT-Geräten in das Gebäudemanagement und die damit verbundene Erweiterung der Angriffsfläche noch verstärkt. Sicherheitsaudits sind daher ein unerlässliches Instrument, um die Resilienz von Immobilienunternehmen gegenüber diesen vielfältigen und sich ständig weiterentwickelnden Bedrohungen zu stärken.

Die ausgewerteten Daten bieten Einblicke in die Existenz und Struktur von internen Audits, die zur Beurteilung der Konzeption und Wirksamkeit von Sicherheitskontrollen in Unternehmen durchgeführt werden.

17 % der teilnehmenden Unternehmen geben an, dass ein formalisiertes internes Audit existiert, was eine klare Struktur und einen systematischen Ansatz aufzeigt. Weitere 22 % der teilnehmenden Unternehmen geben an, dass sie einige interne Audits durchführen. Jedoch scheinen die Struktur und Regelmäßigkeit der Audits unregelmäßig oder nicht standardisiert zu sein. Mit ebenfalls 22 % geben Unternehmen an, ein formalisiertes internes Audit durchzuführen, das auf einem spezifischen Auditplan basiert. 10 % sagen, dass sie für die Durchführung ihrer formalisierten internen Audits sogar ein Auditmanagement-Tool verwenden und damit die Effizienz und Effektivität der Überprüfungen steigern, indem es bei der Organisation, Durchführung und Nachverfolgung der Audits unterstützt.

Die Vielfalt in der Durchführung interner Audits zeigt, dass Unternehmen unterschiedliche Grade der Strukturierung und Planung in ihren Überprüfungen haben. Einige haben bereits feste Auditpläne und unterstützende Tools etabliert, während andere möglicherweise weniger strukturierte Ansätze verfolgen. Um die Effektivität der Sicherheitskontrollen zu gewährleisten, ist eine kontinuierliche und gut geplante Überprüfung erforderlich. Unternehmen, die weniger formale Ansätze nutzen, könnten von einer verstärkten Struktur und Planung in ihren Audits profitieren, um potenzielle Sicherheitslücken zu identifizieren, zu schließen und ihre Mitarbeitenden für die Thematik von Cyber Security zu sensibilisieren.

Abbildung 7:
Interne Audits für die Konzeption und Wirksamkeit der Sicherheitskontrollen



Quelle: KPMG in Deutschland, 2023; Angaben in Prozent, Rundungsdifferenzen möglich

Vorbeugende Software-Sicherheitsprüfung

Die sorgfältige Prüfung von Software- und Hardware-Komponenten vor deren Einsatz ist für die Cyber Security von entscheidender Bedeutung, da sie es ermöglicht, potenzielle Sicherheitslücken proaktiv zu identifizieren und zu schließen, bevor sie ausgenutzt werden können. Dies reduziert das Risiko von Cyber-Angriffen und Datenverlusten, die nicht nur finanzielle Verluste, sondern auch Reputationsschäden nach sich ziehen können. Zusätzlich fördert es ein tiefgreifendes Verständnis für die eigene Infrastruktur, was für eine effektive Reaktion auf das Management von Sicherheitsvorfällen unerlässlich ist.

Die vorliegenden Daten ermöglichen einen Einblick in die Praktiken der teilnehmenden Unternehmen bezüglich der Prüfung von Software- und Hardware-Komponenten hinsichtlich potenzieller Schwachstellen vor deren Implementierung. Die ausgewerteten Daten zeigen, dass die teilnehmenden Unternehmen verschiedene Methoden zur Überprüfung von Software- und Hardware-Komponenten auf Schwachstellen vor deren Implementierung anwenden.

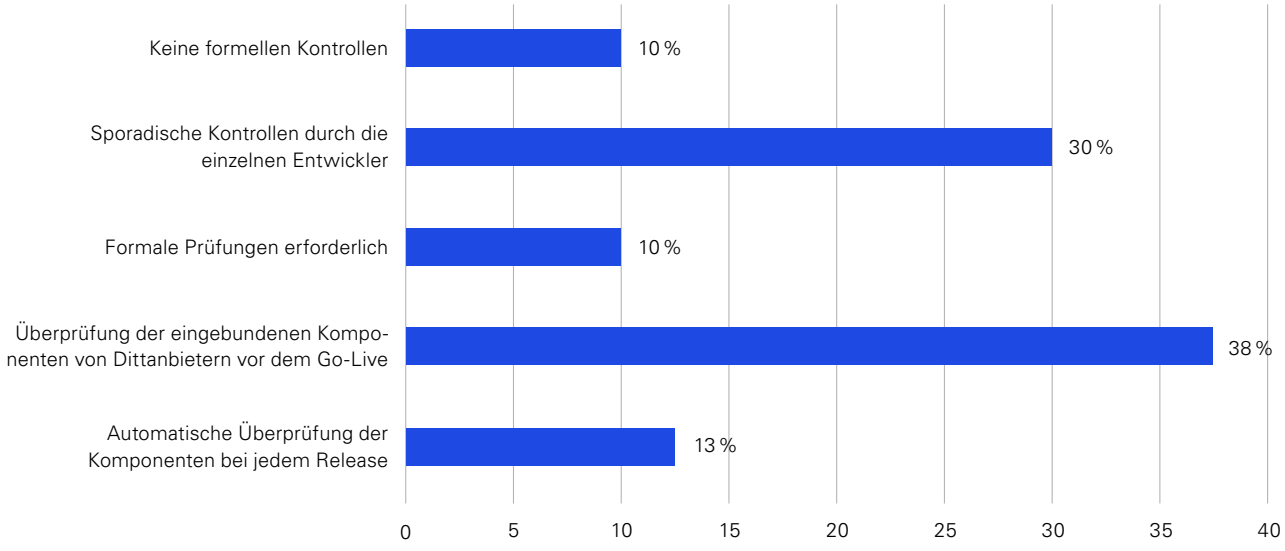
37,5 % der teilnehmenden Unternehmen überprüfen die eingebundenen Komponenten von Drittanbietern vor dem geplanten Go-Live. Ein beträchtlicher Anteil der teilnehmenden Unternehmen von 30 %, verlässt sich auf sporadische, einzelne Kontrollen durch die Entwickler. Jeweils 10 % haben formale Prüfverfahren etabliert, die bei der Implementierung neuer Komponenten vorgeschrieben sind, während die anderen 10 % keine formalen Kontrollmechanismen haben, um mögliche Schwachstellen vor der Implementierung zu überprüfen. Mit 12,5 % führt ein weiterer Teil der Unternehmen automatische Überprüfungen der Komponenten bei jeder Veröffentlichung durch.

Während einige Unternehmen automatisierte oder formale Prüfverfahren nutzen, verlassen sich wiederum andere Unternehmen auf sporadische oder keine formellen Kontrollen. Die Überprüfung von Drittanbieter-Komponenten vor dem Go-Live ist dabei die am häufigsten angewendete Methode.

Key Fact 5

Bei 60 % aller Unternehmen ist eine Sicherheitsprüfung von Software- und Hardwarekomponenten vorgeschrieben.

Abbildung 8:
Prüfung von Software- und Hardwarekomponenten auf Schwachstellen vor Implementierung



Quelle: KPMG in Deutschland, 2023; Angaben in Prozent, Rundungsdifferenzen möglich

Log-In

Die einfachste Art des Zugriffs auf die internen Systeme eines Unternehmens ist der Log-In. Dies kann über zusätzlich eingeführte Sicherheitsmethoden erschwert werden. Die Funktionsweise der Sicherheitsmethoden ist unterschiedlich. So wird bei einigen Unternehmen zusätzliche Hardware (z. B. Hardware-Token) benötigt.

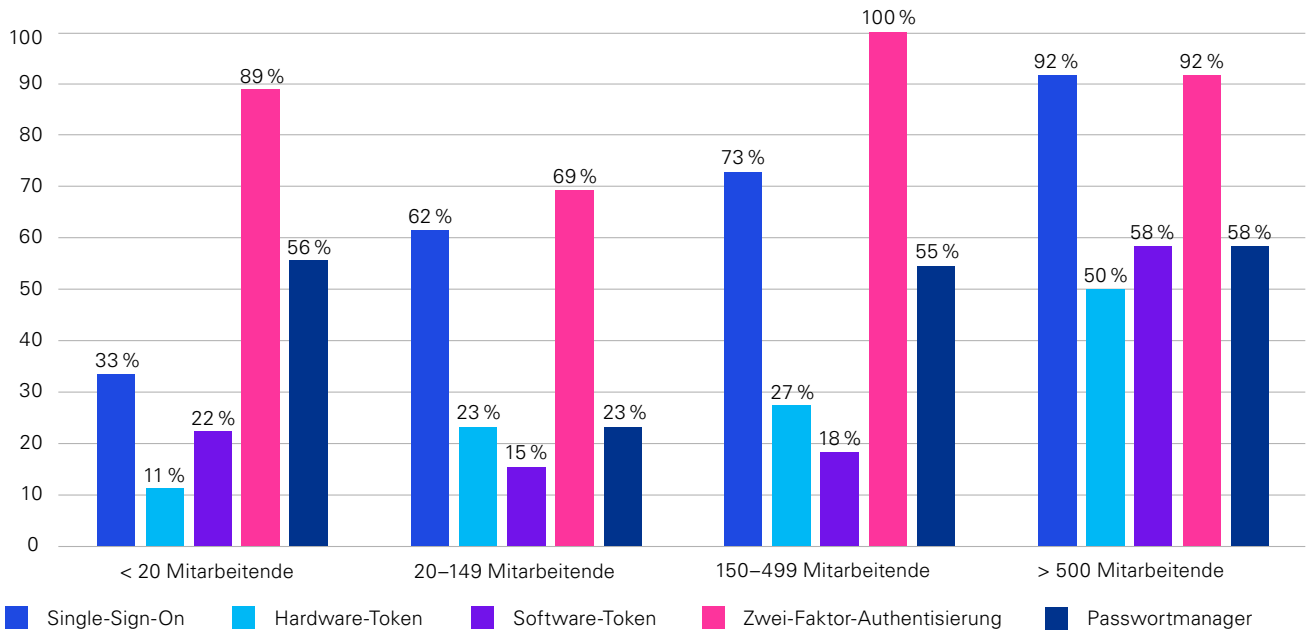
Die in der Umfrage erfassten Daten zu den eingesetzten Authentifizierungsmethoden verdeutlichen, dass Unternehmen im Cyber-Security-Bereich ein breites Spektrum an Verfahren zur Absicherung ihrer Log-in-Prozesse nutzen. Single-Sign-On wird häufig eingesetzt, um Nutzenden einen vereinfachten und dennoch sicheren Zugriff auf verschiedene Dienste zu ermöglichen, indem die Authentifizierungsinformationen zentral verwaltet werden. Hardware-Token bieten als Form der Zwei-Faktor-Authentifizierung eine physische Komponente, die die Sicherheit durch einen zusätzlichen Besitzfaktor erhöht. Software-Token, die oft in mobilen Anwendungen genutzt werden, fügen eine flexible und benutzerfreundliche Option hinzu, die dennoch eine starke Sicherheitsebene beibehält. Die Implementierung von 2FA (Zwei-Faktor-Authentifizierung) als Methode, bei der zwei verschiedene Authentifizierungsfaktoren kombiniert werden, stellt eine zusätzliche Hürde für unbefugte Zugriffe dar. Passwort-Manager werden immer mehr zur Norm, um die Komplexität und Einzigartigkeit von Passwörtern zu steigern und die Sicherheitsrisiken, die mit schwachen oder wiederverwendeten Passwörtern einhergehen, zu minimieren.

Die Auswertung der Befragung zeigt, dass grundsätzlich ein hoher Kenntnisstand zu möglichen Log-In-Methoden besteht. Nur eine Minderheit der Befragten konnte keine eindeutigen Aussagen zu den Methoden des Log-Ins benennen. Am häufigsten wird eine Zwei-Faktor-Authentisierung in den Unternehmen genutzt. Durchschnittlich werden zwei Log-In-Methoden je Unternehmen verwendet, einige Unternehmen benutzen fünf Methoden gleichzeitig. Die häufigste Kombination ist die Verwendung einer Zwei-Faktor-Authentisierung mit Single-Sign-On.

Key Fact 6

Zum Schutz der Unternehmens-IT hat sich die Zwei-Faktor Authentisierung in den meisten Unternehmen etabliert.

Abbildung 9:
Benutzte Log-In-Methoden der Unternehmen gruppiert nach Unternehmensgröße



Quelle: KPMG in Deutschland, 2023; Angaben in Prozent, Rundungsdifferenzen möglich

Mobile Endgeräte

Cyber Security für mobile Endgeräte hat in der heutigen Ära der ständigen Konnektivität höchste Priorität, da diese Geräte eine Fülle sensibler Daten enthalten und oft als Eintrittspunkte in Unternehmensnetzwerke dienen. Angesichts der Tatsache, dass mobile Plattformen zunehmend zum Ziel komplexer Cyber-Angriffe werden, ist es von entscheidender Bedeutung, robuste Sicherheitsprotokolle zu implementieren, um sowohl die Integrität als auch die Vertraulichkeit der auf diesen Geräten gespeicherten Informationen zu gewährleisten.

Die teilnehmenden Unternehmen weisen unterschiedliche Policies für mobile Endgeräte und die Beschaffenheit dieser auf.

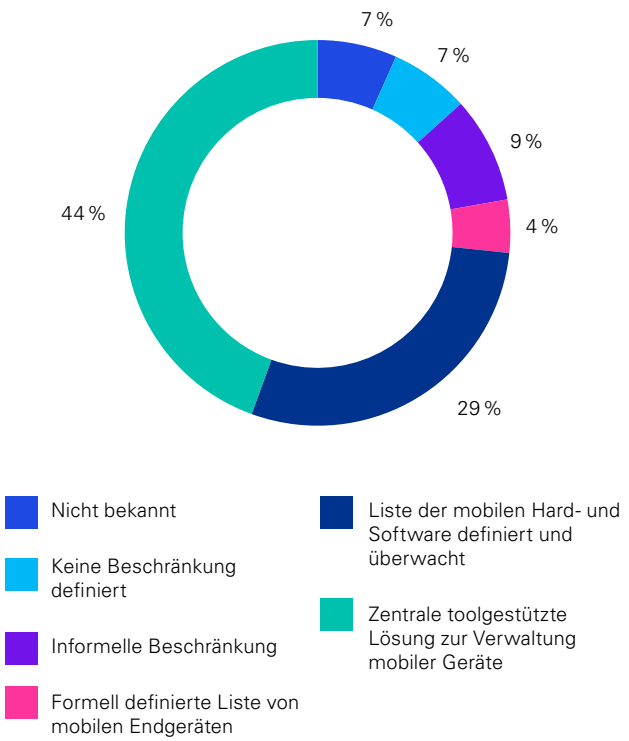
- Der Großteil, nämlich circa 45 % der Unternehmen, setzt auf eine zentrale und toolgestützte Lösung zur Verwaltung der im Einsatz befindlichen mobilen Geräte. Dies ist insofern positiv zu bewerten, da eine dezidierte Sicherheitsrichtlinie, die Risiken im Zusammenhang mit mobilen Endgeräten minimiert.

- Bei fast 30 % der Unternehmen wird eine Liste von mobiler Hard- und Software formell definiert und auch überwacht. Dies zeigt ein höheres Maß an Sicherheitskontrolle und Überwachung.

- Mit jeweils 7 % ist den Teilnehmenden eine Policy für mobile Endgeräte nicht bekannt bzw. keine Beschränkung definiert, was auf eine mögliche Schwachstelle in der Sicherheitsstruktur hinweisen kann.

Die dargestellten Ergebnisse unterstreichen die Bedeutung einer robusten Cyber-Sicherheitsrichtlinie für mobile Endgeräte. Während es teilweise noch Raum zur Verbesserung gibt, setzen die meisten Unternehmen auf strukturierte Ansätze, um die Sicherheit und Integrität ihrer mobilen Technologien zu gewährleisten. Eine umfassende und gut durchdachte Cyber-Sicherheitsrichtlinie ist entscheidend, um sich vor potenziellen Cyber-Bedrohungen zu schützen und die Vertraulichkeit sensibler Daten zu wahren.

Abbildung 10:
Definierter Umgang der Unternehmen mit mobilen Endgeräten



Quelle: KPMG in Deutschland, 2023; Rundungsdifferenzen möglich

Key Fact 7

Nur 45 % der Unternehmen setzen auf eine zentrale und toolgestützte Lösung bei der Verwaltung und Nutzung mobiler Endgeräte.

4 | Handlungsfeld Immobilie

Nachdem die Unternehmensebene betrachtet wurde, stellt sich die Frage nach dem Status quo von Cyber Security auf Ebene der Immobilien. Wer Gebäudetechnik in seinen Objekten installiert hat, sollte im Idealfall auch für den Schutz dieser Technik sorgen.

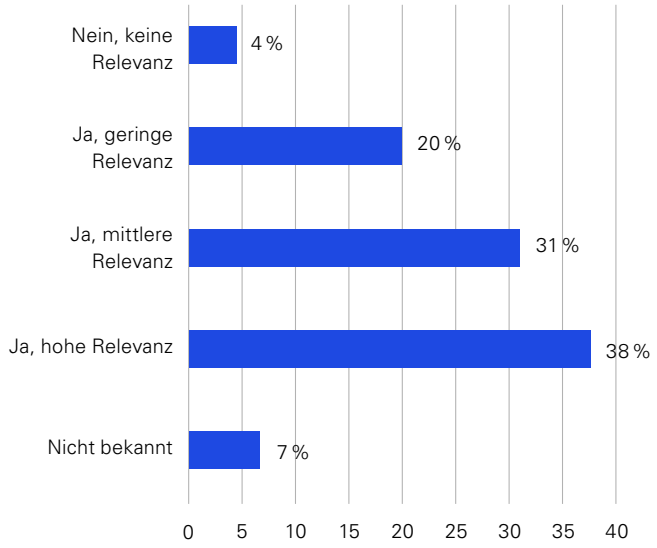
4.1 Schützenswerte Immobilien-Infrastruktur

Smart Building-Technologien werden von 89 % der Teilnehmenden als relevant eingestuft. Weniger als 5 % sagen aus, dass diese keine Relevanz besitzen. Circa 7 % der Teilnehmenden können überhaupt keine Aussage zum Einsatz von Smart-Building-Technologien treffen. Diese potenziellen Angriffsflächen müssen vor Missbrauch initial geschützt, laufend überprüft und proaktiv verbessert werden.

Die Umfrage zeigt eine klare Notwendigkeit, das Thema Cyber Security in den verwalteten Immobilien zu betrachten. Ein Großteil der Befragten erkennt mit fast 70 % einen notwendigen Bezug zwischen den verbauten Bestandteilen in den Immobilien und dem Thema Cyber Security. Lediglich eine Minderheit von circa 20 % sieht keinen direkten Bezug.

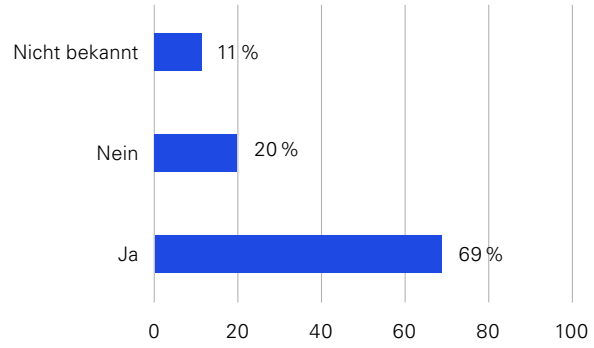
69 % der Teilnehmenden geben an, dass mindestens eine Smart-Building-Technologie in ihren verwalteten Immobilien enthalten ist, die aus Cyber-Security-Sicht zu den kritischen Systemen, wie zum Beispiel elektronische Zugangssysteme, Sensorik, Wärme-/Kältemesstechnik, Funk-/Internetbasierte Verbrauchszähler, Photovoltaik-Anlagen, Wallbox/Ladestationen, Smart Meter, Energiemanagement, Energiezentrale, Microgrid, auch Kameras und Alarm-/Einbruchmelde-/Überwachungsanlagen gehört.

Abbildung 11:
Bewertung der Relevanz von Smart Building für die verwalteten Immobilien bzw. das Unternehmen



Quelle: KPMG in Deutschland, 2023; Angaben in Prozent, Rundungsdifferenzen möglich

Abbildung 12:
Nutzung von Bauteilen in Immobilien für die Cyber Security relevant ist



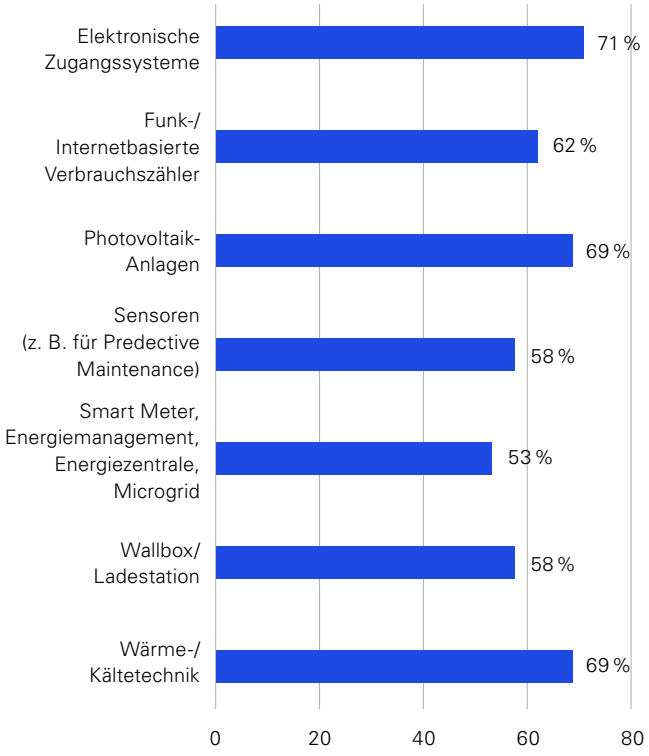
Quelle: KPMG in Deutschland, 2023; Angaben in Prozent, Rundungsdifferenzen möglich

71 % aller Unternehmen haben elektronische Zugangssysteme installiert, 68 % haben Wärme-/Kältemesstechnik und Photovoltaik-Anlagen verbaut. Rund 53 % der Teilnehmenden besitzen in ihren verwalteten Immobilien zudem weitere kritische Systeme.

4.2 Strategische Awareness für Immobilien

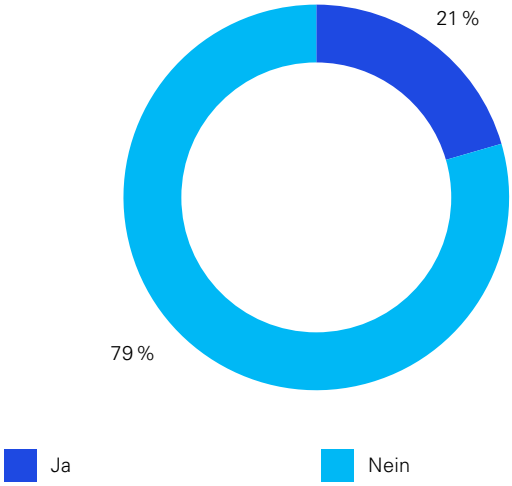
Leider hat nur eine Minderheit der Unternehmen eine Strategie erarbeitet, um die Gebäudetechnik vor Cyber-Security-Attacken zu schützen. Tatsächlich geben fast 80 % der Befragten an, dass ihre Unternehmen keine unternehmensweite/portfolioweite Strategie für den Schutz ihrer Gebäudetechnik entwickelt haben. Lediglich 20 % geben an, Strategien dafür entwickelt zu haben.

Abbildung 13:
Nutzung von kritischen Systemen in Immobilien aus der Cyber-Security-Sicht



Quelle: KPMG in Deutschland, 2023; Angaben in Prozent, Rundungsdifferenzen möglich

Abbildung 14:
Entwicklung einer portfolioweiten/unternehmensweiten Strategie zum Schutz der Gebäudetechnik



Quelle: KPMG in Deutschland, 2023; Rundungsdifferenzen möglich

Key Fact 8

Für 89 % der Befragten spielen Smart-Building-Technologien eine Rolle. Bei 69 % der teilnehmenden Unternehmen ist in den Immobilien mindestens eine Smart-Building-Technologie verbaut, die es zu schützen gilt.

Key Fact 9

Fast 80 % der Unternehmen haben keine portfolioweite/unternehmensweite Strategie zum Schutz der Gebäudetechnik vor Cyber-Angriffen.

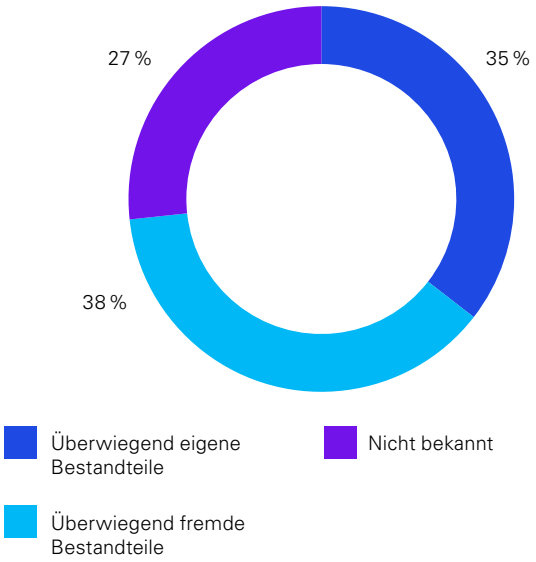
4.3 Management von Cyber-Risiken in der Immobilie

Das Zusammenspiel zwischen internem und externem Risikomanagement ist für Unternehmen von zentraler Bedeutung, um ein ganzheitliches Sicherheitskonzept zu gewährleisten. Durch die Kombination von internen Richtlinien und Kontrollmechanismen mit externen Risikobewertungen und Schutzmaßnahmen können Organisationen eine robuste Verteidigungslinie gegen ein breites Spektrum von Bedrohungen aufbauen. Diese integrierte Herangehensweise ermöglicht es, sowohl die internen Schwachstellen als auch die durch externe Partner und die Lieferkette eingebrachten Risiken effektiv zu managen und somit die Resilienz des Unternehmens gegenüber Cyber-Angriffen zu stärken.

Bei den Einbauten ist darauf zu achten, ein Register zu führen, in dem eindeutig identifizierbare Gebäude-bestandteile mit Relevanz für Cyber Security aufgeführt und bezüglich ihrer Risiken bewertet sind. Nur 18 % der Teilnehmenden führen ein solches Register. 44 % geben an, kein Register zu besitzen, während weitere 38 % keine Angabe zur Existenz eines solchen Registers treffen können.

Zum Teil befinden sich die risikorelevanten Bestandteile nicht immer im Besitz der Unternehmen. So kommt es vor, dass Technologien externer Dienstleistender verwendet werden. Circa 36 % der teilnehmenden Unternehmen geben an, dass sich die risikorelevanten Bestandteile überwiegend in ihrem Eigentum befinden. Circa 37 % nutzen überwiegend Technologien von externen Dienstleistenden. 27 % der Teilnehmenden können keine Aussage dazu treffen, ob sich die risikorelevanten Bestandteile in ihrem oder im Besitz Externer befinden.

Abbildung 15:
Besitzverhältnisse der verbauten risikorelevanten Bestandteile und Technologien



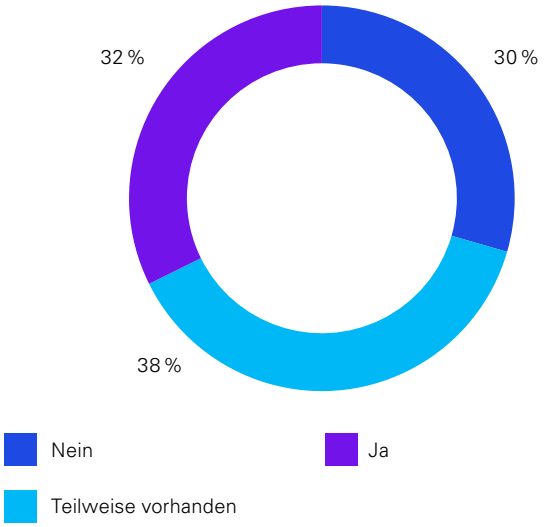
Quelle: KPMG in Deutschland, 2023; Rundungsdifferenzen möglich

4.4 Notfallplan für kritische Technologie

Insbesondere der Ausfall von kritischer Gebäudetechnologie birgt hohe Gefahren. Hier ist eine schnelle Reaktion des angegriffenen Unternehmens wichtig, um den resultierenden Schaden zu minimieren. Daher sollten sich Unternehmen frühzeitig Gedanken über den Umgang mit einem möglichen Angriff machen. In diesem Zuge wird ein Notfallplan für die kritische Technologie erstellt, welcher mit einer möglichst hohen Granularität das Vorgehen festlegt.

Tatsächlich haben lediglich 32 % der Unternehmen bereits einen solchen umfassenden Notfallplan erstellt. Weitere 38 % haben zumindest teilweise einen Notfallplan vorliegen, bei 30 % existiert noch gar kein Notfallplan. Eine Korrelation zu der Unternehmensgröße oder der Anzahl an verwalteten Objekten ist nicht erkennbar.

Abbildung 16:
Existenz eines Notfallplans für kritische Gebäudetechnologie



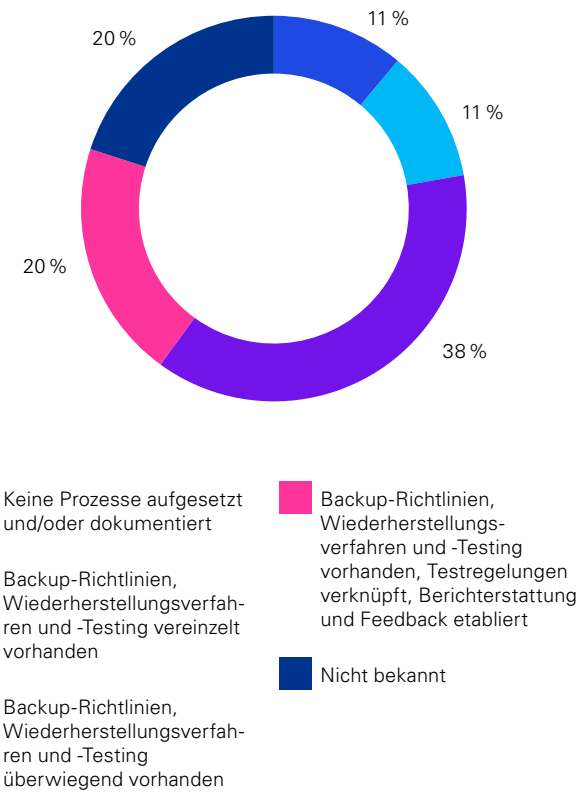
Quelle: KPMG in Deutschland, 2023; Rundungsdifferenzen möglich

4.5 Prozesse für die Immobilien

Sicherungs- und Wiederherstellungsprozesse in der Cyber Security sind essenziell, um die Kontinuität und Widerstandsfähigkeit von IT-Systemen sicherzustellen. Sie umfassen detaillierte Notfallpläne, die den Schutz kritischer Daten und die schnelle Wiederherstellung von Systemen im Falle eines Cyber-Angriffs gewährleisten sollen. Moderne Strategien beinhalten die Anwendung von End-to-End-Verschlüsselungstechnologien zur Sicherung der Datenintegrität und den Einsatz von automatisierten Backup-Lösungen, die eine regelmäßige und redundante Datensicherung ermöglichen. Darüber hinaus werden regelmäßige Tests und Bewertungen der Wiederherstellungspläne durchgeführt, um sicherzustellen, dass sie im Ernstfall effektiv umgesetzt werden können. Die Evaluierung dieser Prozesse bei den teilnehmenden Unternehmen zeigt auf, wie sie sich auf die unterschiedlichen Szenarien vorbereiten und ihre Anpassungsfähigkeit an potenzielle Cyber-Bedrohungen verstärken. Eine Bewertung dieser Prozesse zeigt, wie die teilnehmenden Unternehmen diese Herausforderungen angehen.

Mit 11 % hat ein Teil der teilnehmenden Unternehmen noch keine konkreten Sicherungs- und Wiederherstellungsprozesse für ihre vernetzten Geräte implementiert. Das Fehlen solcher Prozesse birgt erhebliche Risiken, da es im Falle eines Sicherheitsvorfalls schwierig sein kann, angemessen zu reagieren. In weiteren 11 % der Unternehmen sind teilweise Sicherungs- und Wiederherstellungsprozesse vorhanden. Mit überwiegend 38 % hat die Mehrheit der Teilnehmenden bereits Sicherungs- und Wiederherstellungsprozesse für ihre vernetzten Geräte eingerichtet. Dies zeigt eine gewisse Sensibilität für die Bedeutung von Sicherheit, auch wenn es noch Raum für Verbesserungen gibt. Ein mit 20 % bedeutender Anteil der teilnehmenden Unternehmen hat sogar umfassende Sicherungs- und Wiederherstellungsprozesse implementiert, diese mit Testregelungen verbunden und Feedbackmechanismen etabliert. Ein beträchtlicher Anteil von weiteren 20 % konnte allerdings keine genauen Informationen über ihre Sicherungs- und Wiederherstellungsprozesse für vernetzte Geräte liefern.

Abbildung 17:
Existenz und Art von Sicherungs- und Wiederherstellungsprozessen



Quelle: KPMG in Deutschland, 2023; Rundungsdifferenzen möglich

Die Implementierung von Sicherungs- und Wiederherstellungsprozessen bei vernetzten Geräten ist von entscheidender Bedeutung und bildet das Rückgrat für die Widerstandsfähigkeit gegenüber Bedrohungen und die Fähigkeit, im Falle eines Sicherheitsvorfalls schnell und effektiv zu reagieren. Die Unterschiede in der Umsetzung zeigen, dass trotz der Fortschritte noch Raum für Verbesserungen besteht, insbesondere bei der Entwicklung und Dokumentation umfassender Sicherheitsstrategien für vernetzte Geräte.

5 | Handlungsfeld Mitarbeitende

Eine unsachgemäße Handhabung der Systeme und Endgeräte durch Mitarbeitende kann eine Erleichterung für Angreifer zur Folge haben.

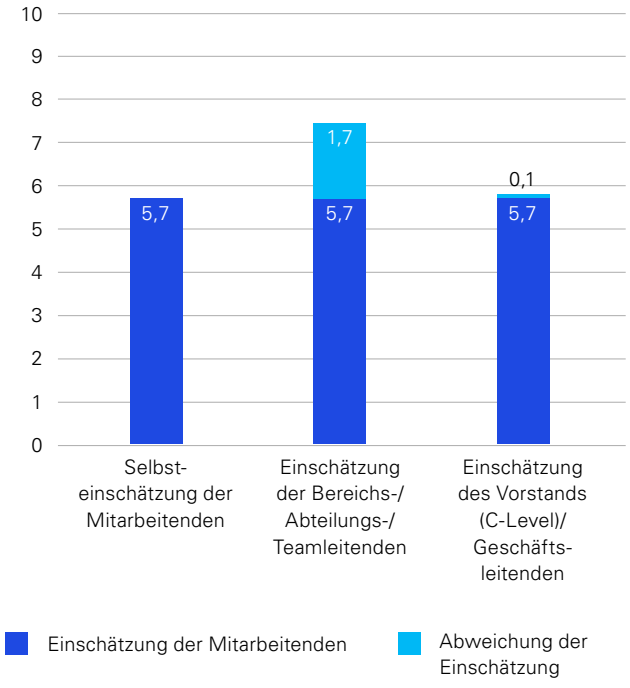
Der Zugriff auf die Systeme sowie auf die Technologien in den Immobilien wird ermöglicht und Schaden in Form von Datenlecks, Sabotage von Anlagen oder Erpressung des Unternehmens können die Folge sein. Diese Gefahr muss im Unternehmen erkannt und durch effiziente Schulungsmaßnahmen und klare Richtlinien minimiert werden.

5.1 Strategische Awareness der Mitarbeitenden

Nicht nur die mit Cyber Security betrauten Mitarbeitenden sind zuständig für diese Gefahrenabwehr. Auch die sonstigen Mitarbeitenden sowie die Managementebene sollte für diese Thematik sensibilisiert sein. Die Auswertung der Zahlen zeigt, dass eine unterschiedliche Einschätzung der Kenntnisse der Mitarbeitenden zu Cyber-Risiken besteht.

Die Mitarbeitenden schätzen ihre eigene Kenntnislage zu Cyber-Risiken auf einer Skala vonnull (niedrig) bis zehn (hoch) durchschnittlich mit einer 5,7 ein. Die Bereichs-, Abteilungs- und Teamleitenden trauen den Mitarbeitenden dabei deutlich mehr zu und schätzen ihre Kenntnislage auf eine 7,4. Die Einschätzung des Vorstands (C-Level)/der Geschäftsleitenden liegt mit einer Bewertung von 5,8 fast gleichauf wie die Selbsteinschätzung der Mitarbeitenden.

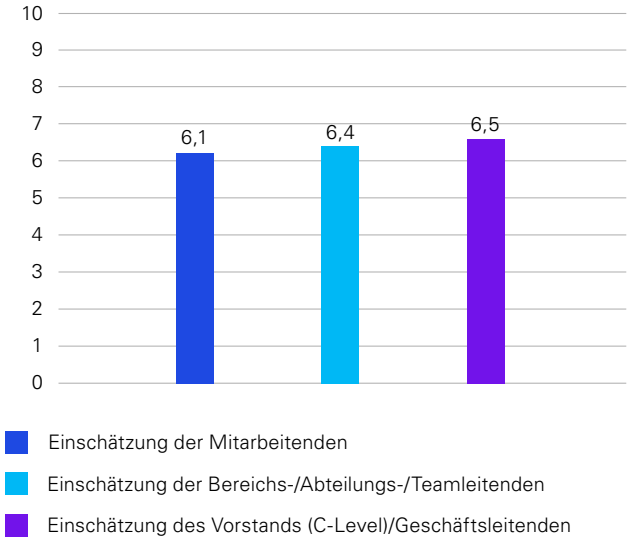
Abbildung 18:
Einschätzung der Kenntnisse zu Cyber-Risiken der Mitarbeitenden auf einer Skala von 1 bis 10



Quelle: KPMG in Deutschland, 2023

Fragt man bezüglich der Kenntnisse der Managementebene, so variieren die Einschätzungen nur minimal. Die Einschätzung der Mitarbeitenden beträgt auf der gleichen Skala 6,2. Die Bereichs-/Abteilungs-/Teamleitenden bewerten die Kenntnisse der Managementebene mit einer 6,4. Vorstände (C-Level)/Geschäftsleitende geben der Managementebene 6,5 der 10 möglichen Punkte.

Abbildung 19:
Einschätzung der Kenntnisse zu Cyber-Risiken der Managementebene auf einer Skala von 1 bis 10



Quelle: KPMG in Deutschland, 2023

Aus diesen Ergebnissen lässt sich ableiten, dass die nicht leitenden Mitarbeitenden sich selbst bezüglich ihrer Kenntnisse am schlechtesten bewerten. Die Bereichs-/Abteilungs-/Teamleitenden und die Vorstände (C-Level)/Geschäftsleitende gehen von einer höheren Fachkenntnis ihrer Mitarbeitenden aus. Die Bereichs-/Abteilungs-/Teamleitenden sind sogar der Meinung, dass die Cyber-Security-Kenntnisse ihrer Mitarbeitenden weitreichender als die eigenen Kenntnisse sind.

Da die sonstigen Mitarbeitenden den größten Anteil des Unternehmens ausmachen, ist eine Fehleinschätzung dieser Rollengruppe durch die Vorgesetzten und Geschäftsleitenden besonders kritisch zu bewerten. Eine Ursache dieser Diskrepanz in Außenwahrnehmung und Eigenwahrnehmung der Mitarbeitenden sollte besonders untersucht werden.

Zu beachten ist, dass eine effektive Cyber-Sicherheitsstrategie nicht nur von der Führung, sondern von allen Ebenen innerhalb des Unternehmens getragen werden sollte. Hierbei ist eine kontinuierliche Sensibilisierung und Schulung über Cyber-Sicherheitsrisiken für alle Ebenen von entscheidender Bedeutung, um ein umfassendes Verständnis und eine proaktive Herangehensweise zur Risikominimierung zu gewährleisten.

Key Fact 10

Es ist eine Diskrepanz zwischen der Eigenwahrnehmung und der Fremdwahrnehmung bezüglich der Kenntnisse der nicht leitenden Mitarbeitenden zu Cyber-Risiken vorhanden. Die nicht leitenden Mitarbeitenden schätzen ihre Kenntnisse schlechter ein, wohingegen die Einschätzung durch die leitenden Mitarbeitenden höher ausfällt.

5.2 Organisation der Cyber Security

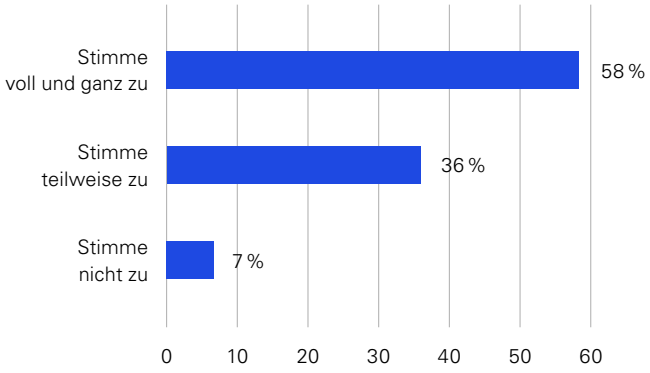
Die Abwehr von Cyber-Security-Bedrohungen sollte in einem Immobilienunternehmen sehr ernst genommen werden und mit einer entsprechenden Organisation unterlegt werden. In den befragten Unternehmen beschäftigt sich abhängig von der Unternehmensgröße eine unterschiedliche Anzahl von Mitarbeitenden mit dem Thema Cyber Security.

Ressourcenallokation

Unternehmen zwischen 150 bis 499 Mitarbeitenden sowie die großen Unternehmen mit mehr als 500 Mitarbeitenden beschäftigen die meisten Personen im Bereich Cyber Security. Auffällig ist, dass obwohl der Durchschnitt der Cyber-Security-Mitarbeitenden 8,5 beträgt, die Verantwortlichkeit am häufigsten bei einer einzigen Person liegt. In Unternehmen mit mehr als 500 Mitarbeitenden befassen sich rund 20 Mitarbeitende mit diesen Themen. Weniger verwunderlich ist die Tatsache, dass die Unternehmen, welche eine eigene Organisation bzw. Organisationseinheit für das Thema Cyber Security aufgebaut haben, oftmals eine deutlich höhere Anzahl an Cyber-Security-Mitarbeitenden beschäftigen.

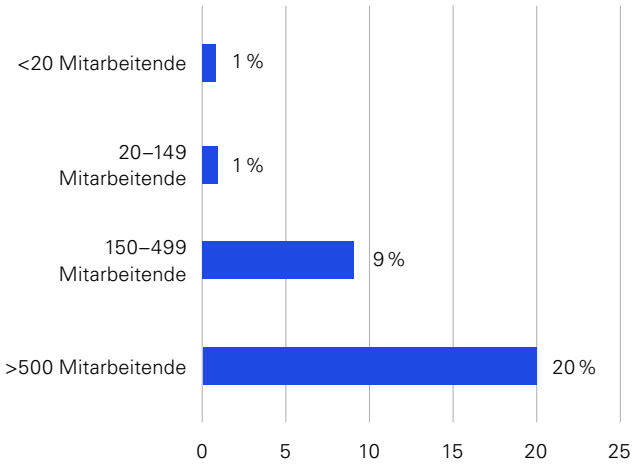
Abbildung 20:
Verantwortlichkeit der Führungskräfte zu rechtlichen und regulatorischen Cyber-Security-Anforderungen

Alle Führungskräfte sind dafür verantwortlich, rechtliche Anforderungen an Cyber Security zu verstehen und dahingehende Geschäftspraktiken einzuhalten.



Quelle: KPMG in Deutschland, 2023; Angaben in Prozent, Rundungsdifferenzen möglich

Abbildung 21:
Anzahl der Cyber-Security-Fachkräfte nach Anzahl der Mitarbeitenden im Unternehmen

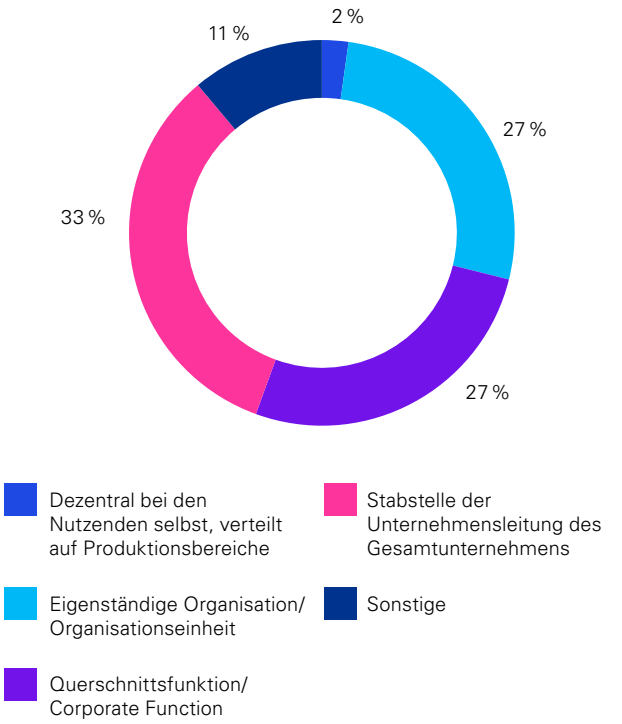


Quelle: KPMG in Deutschland, 2023

Wo diese Positionen genau verortet werden können, zeigen die Auswertungsergebnisse für die Cyber-Security-Organisationseinheit. Jeweils 27 % der teilnehmenden Unternehmen geben an, eine eigenständige Organisationseinheit oder eine Querschnittsfunktion/Corporate Function mit den Aufgaben betraut zu haben. Rund 33 % der teilnehmenden Unternehmen verorten diese Zuständigkeit als Stabstelle der Unternehmensleitung des Gesamtunternehmens.

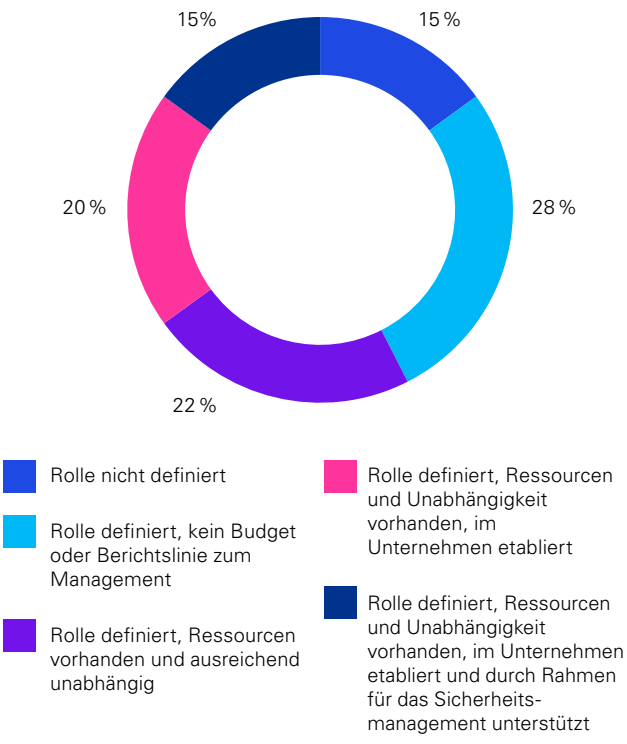
Die verschiedenen Rollenausprägungen innerhalb der Security-Organisationseinheit fallen sehr unterschiedlich aus. So geben 22 % an, eine definierte Rolle mit ausreichender Unabhängigkeit und Ressourcen zu haben, während circa 28 % eine definierte Rolle ohne Budget oder direkte Berichtslinie zum Management haben. Rund 20 % der teilnehmenden Unternehmen geben an, eine Rolle mit ausreichender Unabhängigkeit und Ressourcen definiert und vollständig im Unternehmen etabliert zu haben, circa 15 % werden zusätzlich durch einen zertifizierten Rahmen für das Sicherheitsmanagement unterstützt.

Abbildung 22:
Lokalisation der Zuständigkeit für Cyber Security im Unternehmen



Quelle: KPMG in Deutschland, 2023; Rundungsdifferenzen möglich

Abbildung 23:
Definition der Cyber-Security-Rolle im Unternehmen



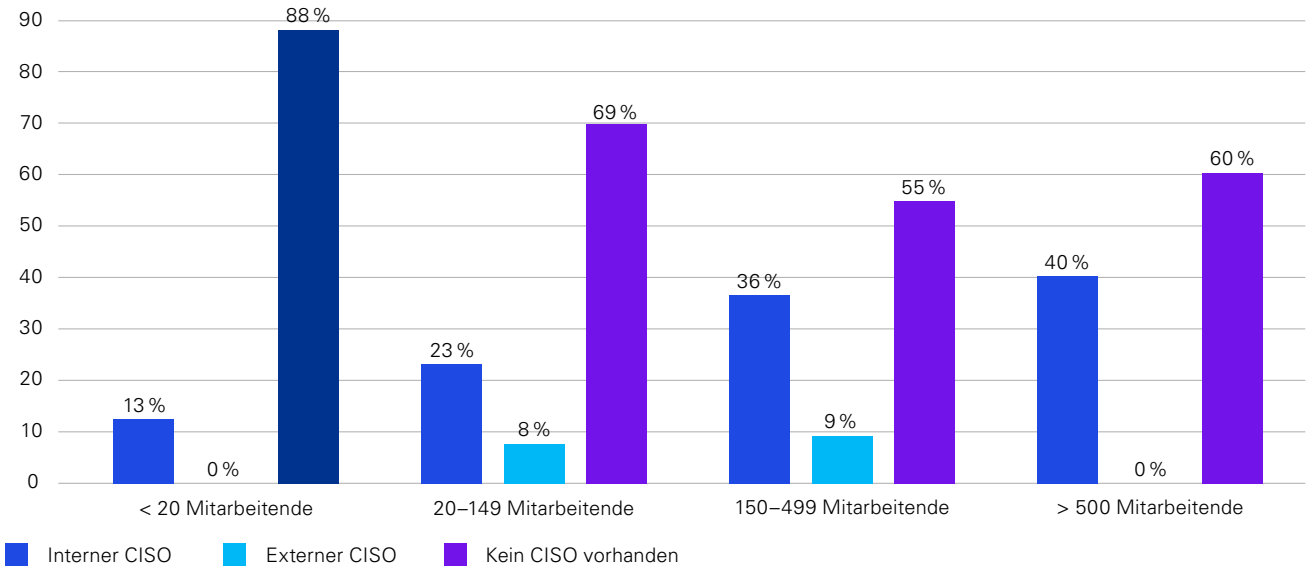
Quelle: KPMG in Deutschland, 2023; Rundungsdifferenzen möglich

Diese Angaben spiegeln eine breite Varianz in der organisatorischen Verankerung und Ressourcenausstattung von Sicherheitsrollen wider. Es zeigt sich, dass, während ein Teil der Unternehmen Sicherheitsfunktionen mit hinreichenden Kompetenzen und Mitteln ausstattet, ein signifikanter Anteil ohne wesentliche Budgets oder direkte Einflusslinien operieren muss. Die volle Etablierung und Unterstützung durch zertifizierte Rahmenwerke bei einer Minderheit der Unternehmen unterstreicht die Notwendigkeit einer stärkeren institutionellen Verankerung des Sicherheitsmanagements als integralen Bestandteil der Unternehmensführung.

Einsatz eines Chief Information Security Officers

Bei 31 % der Unternehmen ist ein Chief Information Security Officer (CISO) für die Security Themen verantwortlich. Bei größeren Unternehmen, mit mehr als 500 festangestellten Mitarbeitenden, sind interne CISO häufiger vertreten. Wenig verwunderlich ist, dass kleine Unternehmen mit weniger als 20 Mitarbeitenden in der Regel keinen CISO einsetzen. Hier stellt sich die Frage, ob diese kleinen Unternehmen tatsächlich keinen Bedarf für einen CISO sehen oder die Aufgabenstellung anderweitig übertragen haben (z. B. Beauftragte externe Dienstleistende). Dies ist insbesondere aus dem Aspekt wesentlich, da kleine Unternehmen die Relevanz von Cyber Security hoch und die Anzahl an Angriffen als steigend einschätzen.

Abbildung 24:
Einsatz und Art eines CISO der Unternehmen prozentual gruppiert nach Anzahl der Mitarbeitenden



Quelle: KPMG in Deutschland, 2023; Angaben in Prozent, Rundungsdifferenzen möglich

Externe Unterstützung

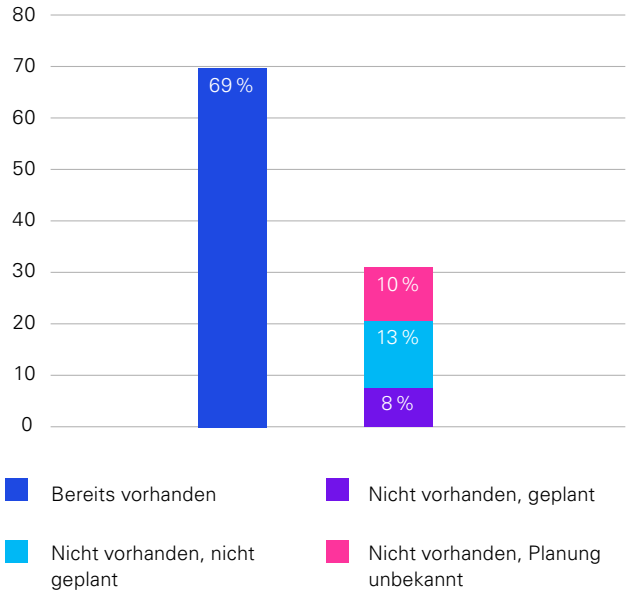
Bei mehr als 70 % der teilnehmenden Unternehmen unterstützen oder betreuen externe Dienstleistende bei Themen zur Cyber Security. Einen CISO (Chief Information Security Officer) im Unternehmen haben lediglich 31 % der teilnehmenden Unternehmen.

Interessant ist, dass Korrelationen zwischen Unternehmensstandort, Anzahl an Cyber-Security-Verantwortlichen, der Beauftragung von externen Dienstleistenden und der Größe des Unternehmens nicht erkennbar sind.

Key Fact 11

Überwiegend kümmert sich nur ein Mitarbeitender um Cyber Security, circa 70 % der Unternehmen beauftragen externe Dienstleistende.

Abbildung 25:
Übersicht über die aktuelle sowie geplante Nutzung von externen Cyber-Security-Dienstleistern



Quelle: KPMG in Deutschland, 2022; Angaben in Prozent, Rundungsdifferenzen möglich

Regelungen der Sicherheitsvorgaben mit Dienstleistenden

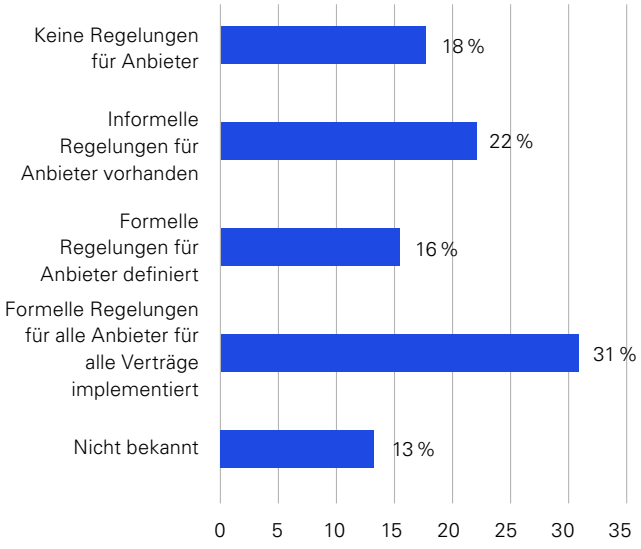
Die erhobenen Daten bieten Einblicke in die vielfältigen Sicherheitsregelungen, die von Unternehmen zur Überwachung und Sicherstellung der Sicherheitsstandards bei ihren Dienstleistenden implementiert werden. Die Auswertung verdeutlicht die Bandbreite an Ansätzen und Strukturen, die für die Kontrolle der Sicherheitsvorgaben bei externen Partnern existieren.

31 % der Unternehmen haben formelle Regelungen mit den Dienstleistenden getroffen, die vertraglich geregelt und festgehalten sind. So verfolgen diese Unternehmen eine stringente und standardisierte Herangehensweise, um die Sicherheit bei externen Partnern zu gewährleisten. Rund 16 % hat formelle Regelungen spezifisch für Dienstleistende definiert.

Ein Teil der Unternehmen, etwa 18 %, geben an, dass keine spezifischen Regelungen zur Überwachung der Einhaltung von Sicherheitsvorgaben bei Dienstleistenden existieren. Dies könnte jedoch potenzielle Lücken in der Kontrolle von Sicherheitsaspekten bei den externen Dienstleistenden aufzeigen. 22 % der Unternehmen haben lediglich informelle Regelungen für Anbieter. Weitere 13 % können keine Aussage zu Regelungen mit Dienstleistenden treffen bzw. Regelungen sind nicht bekannt.

Die Daten zeigen, dass Unternehmen unterschiedliche Ansätze für die Überwachung und Überprüfung von Dienstleistenden in Bezug auf Sicherheitsvorgaben haben. Ein Teil der Unternehmen hat formelle Regelungen für alle Verträge implementiert, während andere entweder informelle Regelungen oder keine spezifischen Vorgaben für Anbieter aufweisen.

Abbildung 26:
Regelungen zur Einhaltung von Sicherheitsvorgaben durch Dienstleistende



Quelle: KPMG in Deutschland, 2023; Angaben in Prozent, Rundungsdifferenzen möglich

Key Fact 12

Für den Umgang mit Dienstleistenden geben nur

47 % **der Unternehmen an, formelle Regelungen zur Einhaltung von Sicherheitsvorgaben getroffen zu haben.**

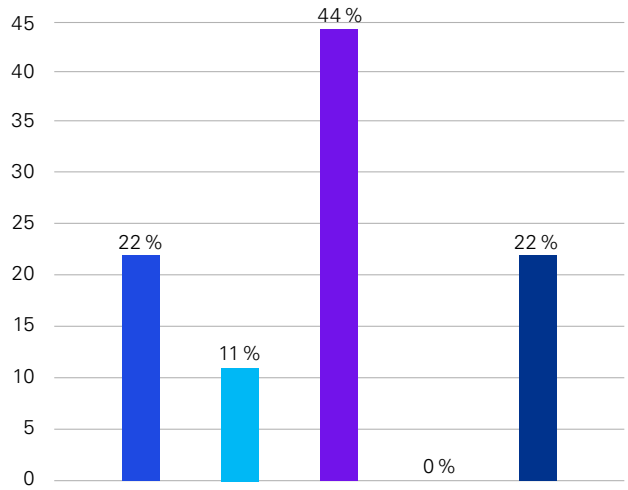
5.3 Management von Cyber-Risiken bei Mitarbeitenden

Die vorliegenden Daten zeigen eine Vielzahl von Herangehensweisen in Bezug auf den Zugang und die Einhaltung der Regelungen hinsichtlich Cyber Security innerhalb der Unternehmen. Während einige Unternehmen formalisierte Anforderungen und Überwachungen implementiert haben, gibt es andere, bei denen die Regelungen weniger strukturiert oder nicht klar kommuniziert sind. Die regelmäßige Einhaltung und die Sensibilisierungsprogramme variieren je nach Unternehmensgröße und internen Richtlinien. Es ist von großer Bedeutung, dass sämtliche Anweisungen, Richtlinien und Regeln der Organisation für die Mitarbeitenden zugänglich sind, aber gleichzeitig auch klare und überwachte Regelungen durch die Unternehmen eingeführt werden. Die Mitarbeitenden sollten die Sicherheitsrichtlinien verstehen, zustimmen und konsequent einhalten.

50 % der teilnehmenden Unternehmen mit mehr als 500 Mitarbeitenden haben eine formale Anforderung zur Beinhaltung einer Vereinbarung zur Einhaltung der Regelungen im Arbeitsvertrag verankert und Richtlinien werden unternehmensweit kommuniziert. 33 % der Mitarbeitenden werden regelmäßig aufgefordert die Einhaltung zu bestätigen und die Unternehmen führen Sensibilisierungsprogramme durch.

In Unternehmen mit weniger als 20 Mitarbeitenden geben 22 % der Teilnehmenden an, keine formalisierte Vereinbarung zur Einhaltung der Regelungen zu haben und die Mitarbeitenden haben nur begrenzten Zugang zu den Richtlinien. Weitere 22 % der Teilnehmenden geben an, die regelmäßige Einhaltung zu überprüfen und ein Sensibilisierungsprogramm durchzuführen. 11 % der teilnehmenden Unternehmen dieser Unternehmensgröße haben lediglich in einigen Arbeitsverträgen eine Vereinbarung über die Regeleinhaltung aufgenommen. Ein Anteil von 44 % der Teilnehmenden hat eine formale Anforderung zur Beinhaltung einer Vereinbarung zur Einhaltung der Regelungen im Arbeitsvertrag und Richtlinien werden in der gesamten Organisation kommuniziert.

Abbildung 27:
Anweisungen, Richtlinien und Regeln der Organisation hinsichtlich Cyber Security in Unternehmen bis 20 Mitarbeitende

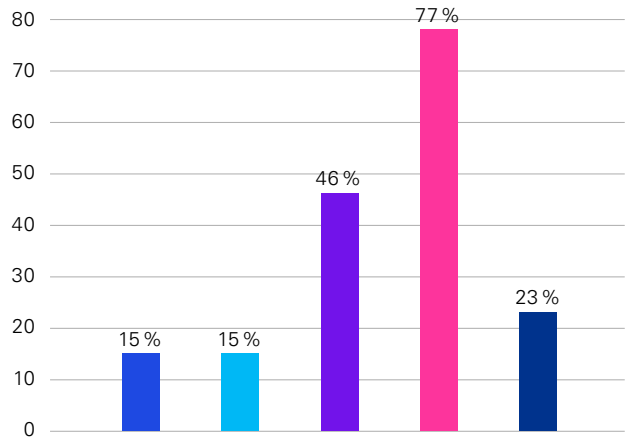


- Keine formalisierte Vereinbarung zur Einhaltung der Regelungen vorhanden, Mitarbeitende haben nur begrenzten Zugang zu den Richtlinien
- Einige Arbeitsverträge enthalten eine Vereinbarung über die Einhaltung der Regelungen
- Formale Anforderung zur Beinhaltung einer Vereinbarung zur Einhaltung der Regelungen im Arbeitsvertrag vorhanden, Richtlinien werden in der gesamten Organisation kommuniziert
- Anforderung ist verbindlich und wird überwacht
- Mitarbeitende werden regelmäßig aufgefordert, Einhaltung zu bestätigen und Sensibilisierungsprogramm wird durchgeführt

Quelle: KPMG in Deutschland, 2023; Angaben in Prozent, Rundungsdifferenzen möglich

77 % der Unternehmen mit einer Unternehmensgröße von 20 bis 149 Mitarbeitenden haben verbindliche Anforderungen definiert, die überwacht werden. 46 % der Unternehmen in dem Bereich halten formale Anforderung zur Beinhaltung einer Vereinbarung zur Einhaltung der Regelungen im Arbeitsvertrag fest und kommunizieren Richtlinien in der gesamten Organisation. Weitere 23 % werden regelmäßig dazu aufgefordert, die Einhaltung zu bestätigen und es wird ein Sensibilisierungsprogramm durchgeführt. 15 % haben in einigen Arbeitsverträgen eine Vereinbarung über die Einhaltung der Regelungen getroffen, während bei weiteren 15 % keine formalisierte Vereinbarung zur Einhaltung der Regelung vorhanden ist und die Mitarbeitenden nur einen begrenzten Zugang zu den Richtlinien haben.

Abbildung 28:
Anweisungen, Richtlinien und Regeln der Organisation hinsichtlich Cyber Security in Unternehmen mit 20 bis 149 Mitarbeitende



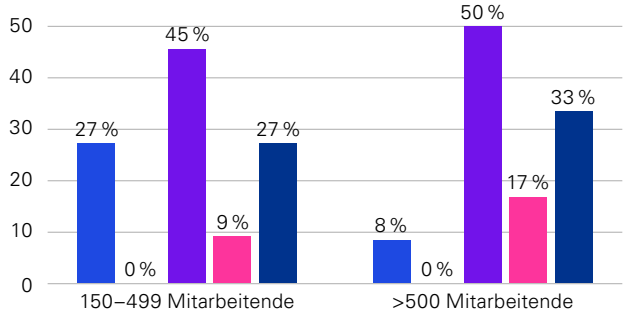
- Keine formalisierte Vereinbarung zur Einhaltung der Regelungen vorhanden, Mitarbeitende haben nur begrenzten Zugang zu den Richtlinien
- Einige Arbeitsverträge enthalten eine Vereinbarung über die Einhaltung der Regelungen
- Formale Anforderung zur Beinhaltung einer Vereinbarung zur Einhaltung der Regelungen im Arbeitsvertrag vorhanden, Richtlinien werden in der gesamten Organisation kommuniziert
- Anforderung ist verbindlich und wird überwacht
- Mitarbeitende werden regelmäßig aufgefordert, Einhaltung zu bestätigen und Sensibilisierungsprogramm wird durchgeführt

Quelle: KPMG in Deutschland, 2023; Angaben in Prozent, Rundungsdifferenzen möglich

In Unternehmen mit einer Unternehmensgröße von 150 bis 499 Mitarbeitenden geben 45 % an, dass formale Anforderungen zur Beinhaltung einer Vereinbarung zur Einhaltung der Regelungen im Arbeitsvertrag vorhanden seien, Richtlinien werden in der gesamten Organisation kommuniziert. Weitere 45 % enthalten eine Vereinbarung über die Einhaltung der Regelungen. 27 % der Unternehmen fordern ihre Mitarbeitenden in regelmäßigen Abständen dazu auf, die Einhaltung zu bestätigen und führen ein Sensibilisierungsprogramm durch. Weitere 9 % haben eine verbindliche Anforderung, die überwacht wird.

Bei den Unternehmen mit mehr als 500 Mitarbeitenden setzt sich der Trend fort. Die formalen Anforderungen zur Beinhaltung der Vereinbarung sind bereits bei 50 % vorhanden und sowohl der Anteil mit verbindlichen und überwachten Anforderungen steigt nochmals um circa 7 % an. Ebenfalls wird in dieser Unternehmensgröße der Höchstwert mit 33 % der Teilnehmenden erreicht, welche ihre Mitarbeitenden die Einhaltung regelmäßig bestätigen lassen und dahingehende Sensibilisierungsprogramme durchführen.

Abbildung 29:
Anweisungen, Richtlinien und Regeln der Organisation hinsichtlich Cyber Security in Unternehmen ab 150 Mitarbeitende



- Keine formalisierte Vereinbarung zur Einhaltung der Regelungen vorhanden, Mitarbeitende haben nur begrenzten Zugang zu den Richtlinien
- Einige Arbeitsverträge enthalten eine Vereinbarung über die Einhaltung der Regelungen
- Formale Anforderung zur Beinhaltung einer Vereinbarung zur Einhaltung der Regelungen im Arbeitsvertrag vorhanden, Richtlinien werden in der gesamten Organisation kommuniziert
- Anforderung ist verbindlich und wird überwacht
- Mitarbeitende werden regelmäßig aufgefordert, Einhaltung zu bestätigen und Sensibilisierungsprogramm wird durchgeführt

Quelle: KPMG in Deutschland, 2023; Angaben in Prozent, Rundungsdifferenzen möglich

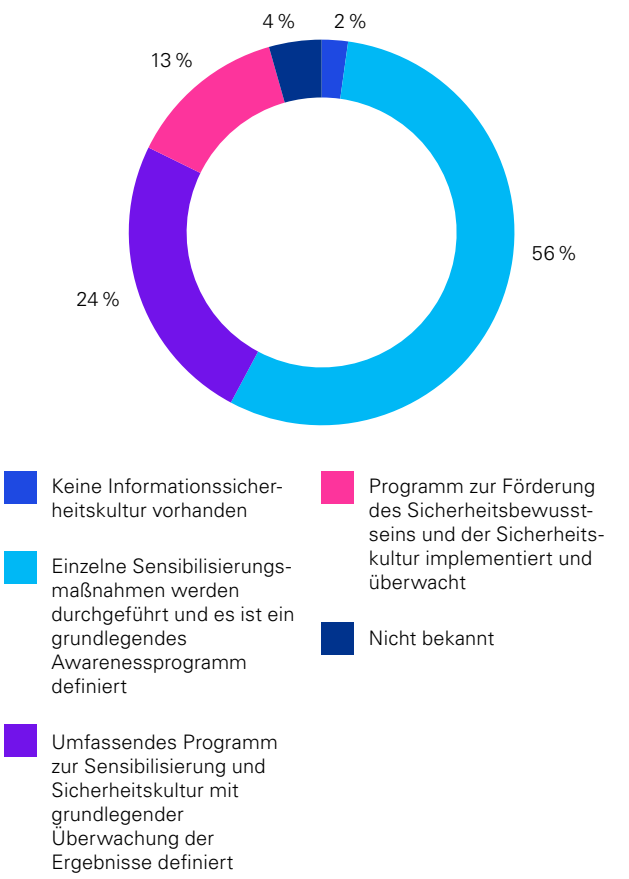
5.4 Informationssicherheitskultur und Weiterbildung bei Mitarbeitenden

Die vorliegenden Daten bieten Einblicke in die Existenz und Umsetzung einer Informationssicherheitskultur in Unternehmen sowie die Bereitstellung von Anleitungen für Mitarbeitende in ihrem täglichen Arbeitsumfeld und im Umgang mit Kunden:

56 % der teilnehmenden Unternehmen führen einzelne Sensibilisierungsmaßnahmen durch und haben ein grundlegendes Awareness-Programm definiert. Das zeigt, dass zumindest ein Basisniveau an Sensibilisierung für Informationssicherheit existiert, auch wenn es sich möglicherweise um verschiedene unabhängige Maßnahmen handelt. 24 % der teilnehmenden Unternehmen haben ein umfassendes Programm zur Sensibilisierung und zur Förderung einer Sicherheitskultur mit grundlegender Überwachung der Ergebnisse definiert. Nur 13 % der Unternehmen haben ein Programm zur Förderung des Sicherheitsbewusstseins und der Sicherheitskultur implementiert und überwachen aktiv dessen Wirksamkeit.

Die Mehrheit der teilnehmenden Unternehmen hat zumindest grundlegende Sensibilisierungsmaßnahmen und ein Bewusstsein für Informationssicherheit implementiert. Klar erkennbar ist, dass viele Unternehmen in irgendeiner Form an der Entwicklung einer Informationssicherheitskultur arbeiten. Einige Unternehmen haben spezifischere, umfassendere Programme zur Förderung des Sicherheitsbewusstseins und der Sicherheitskultur mit Überwachung implementiert, was auf einen strukturierteren und zielgerichteteren Ansatz hindeutet. Anzumerken ist, dass ein kleiner Prozentsatz von 6 % keine Informationssicherheitskultur definiert hat bzw. keine Kenntnis hierüber vorhanden ist.

Abbildung 30:
Informationssicherheitskultur der Unternehmen

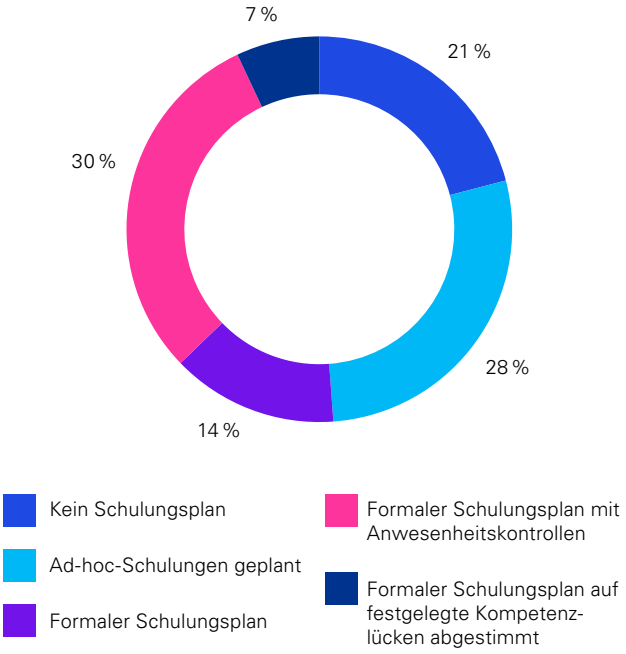


Quelle: KPMG in Deutschland, 2023; Rundungsdifferenzen möglich

Umfangreiche Schulungen und Informationsveranstaltungen sind oftmals ein adäquates Mittel zur Informationsvermittlung im Umgang mit Cyber-Security-Risiken. Rund 27 % der teilnehmenden Unternehmen planen Ad-hoc-Schulungen für ihre Mitarbeitenden im Bereich Cyber Security, während 30 % der Teilnehmenden sogar formale Schulungspläne mit Anwesenheitskontrollen ausgearbeitet haben. Dies deutet auf ein höheres Maß an Verpflichtung und auch auf eine höhere Bedeutung, die dem Schulungsprogramm beigemessen wird, hin. In 21 % der teilnehmenden Unternehmen sind derzeit keine Ad-hoc-Schulungen für die Mitarbeitenden geplant. Nur circa 7 % der teilnehmenden Unternehmen haben formale Schulungspläne entwickelt, die auf festgestellte Kompetenzlücken der Belegschaft abgestimmt sind.

Die Daten zeigen eine Vielfalt in den Ansätzen der Unternehmen hinsichtlich der Schulungspläne für Mitarbeitende im Bereich Cyber Security. Während einige der Unternehmen Schulungspläne mit Anwesenheitskontrollen implementieren, gibt es auch Unternehmen, die keine Pläne entwickelt haben oder nur Ad-hoc-Schulungen für die Mitarbeitenden durchführen. Gerade aufgrund der Diskrepanz bezüglich der Kenntniseinschätzung der nicht leitenden Mitarbeitenden sollte der Anteil an auf Kompetenzlücken abgestimmten Schulungen erhöht werden.

Abbildung 31:
Schulungspläne für Mitarbeitende zu Cyber Security



Quelle: KPMG in Deutschland, 2023; Rundungsdifferenzen möglich

Key Fact 13

In 79 % der teilnehmenden Unternehmen werden Schulungen für die Mitarbeitenden anhand eines Schulungsplans durchgeführt.

6 | Fazit

Die Studie zur Cyber Security in Unternehmen verdeutlicht die Vielfalt und Komplexität der Sicherheits-praktiken in verschiedenen Handlungsfeldern.

Einer der herausragenden Befunde ist, dass die Wahrscheinlichkeit von Cyber-Angriffen mit der Größe des Unternehmens zunimmt. Trotzdem sind von Cyber-Angriffen fast alle Unternehmen betroffen, was die Dringlichkeit von robusten Sicherheitsmaßnahmen unterstreicht. Überraschenderweise ergreifen Unternehmen, die die Relevanz von Cyber Security hoch einschätzen, seltener proaktive Maßnahmen zur Verbesserung, was die Diskrepanz zwischen wahrgenommener Bedeutung und tatsächlichen Handlungen verdeutlicht.

Die Ergebnisse zeigen zudem, dass viele Unternehmen eine Cyber-Security-Strategie etabliert haben oder sich in der Phase der Strategieumsetzung befinden, wobei der Entwicklungsstand der Strategien stark von der Unternehmensgröße abhängig ist. Die Implementierung von Richtlinien auf Vorstandsebene korreliert mit der Relevanz von Cyber Security.

Die Ergebnisse der Studie heben die Bedeutung hervor, die Unternehmen der Zwei-Faktor-Authentifizierung beimessen, um die Sicherheit ihrer Systeme zu erhöhen. Jedoch offenbart die geringe Verbreitung zentralisierter und toolgestützter Verwaltungssysteme für mobile Endgeräte eine mögliche Sicherheitslücke, die es zu schließen gilt. Die zunehmende Präsenz von Smart-Building-Technologien stellt eine Erweiterung der Angriffsfläche dar, die spezifische Schutzmaßnahmen erfordert. Trotz des offensichtlichen Risikopotenzials fehlt es in vielen Unternehmen an einer ganzheitlichen Strategie zur Sicherung ihrer Gebäudetechnik gegen Cyber-Bedrohungen, was eine kritische Lücke in der Sicherheitsarchitektur aufzeigt. Dies unterstreicht die Dringlichkeit für Organisationen, ihre Sicherheitsprotokolle zu überdenken und eine umfassende Strategie zu entwickeln, die sowohl herkömmliche IT-Systeme als auch die zunehmend verbreiteten smarten Komponenten ihrer Gebäudeinfrastruktur einschließt.

Darüber hinaus offenbart die Untersuchung eine klare Diskrepanz in der Wahrnehmung der Kenntnisse zu Cyber-Risiken zwischen leitenden und nicht leitenden Mitarbeitenden. Die Auslagerung der Cyber-Security-Aufgaben an externe Dienstleister ist weit verbreitet, wobei die Regelungen für diese Dienstleistenden nicht einheitlich sind. Schulungen zur Cyber Security werden zwar in den meisten Unternehmen durchgeführt, jedoch sind spezifisch auf Kompetenzlücken abzielende Schulungspläne nur begrenzt vorhanden.

Insgesamt zeigen die Ergebnisse der Studie, dass Cyber Security eine komplexe und vielschichtige Herausforderung für Unternehmen darstellt, die nicht nur technische Maßnahmen erfordert, sondern auch eine umfassende Sensibilisierung und Anpassung in verschiedenen Bereichen, um wirksame und robuste Sicherheitsmaßnahmen zu implementieren.

Angesichts der sich ständig wandelnden Cyber-Bedrohungslandschaft ist es unerlässlich, dass Unternehmen eine dynamische und ganzheitliche Sicherheitsstrategie verfolgen, die sowohl präventive als auch reaktive Elemente umfasst. Die Studie betont die Notwendigkeit einer kontinuierlichen Weiterentwicklung und Anpassung der Sicherheitsprotokolle, um den Schutz vor neuen und sich entwickelnden Bedrohungen aufrechtzuerhalten. Letztendlich erfordert die Gewährleistung einer robusten Cyber Security eine Unternehmenskultur, die Sicherheit als wesentlichen Bestandteil des Geschäftsalltags begreift und fördert, wodurch ein resilientes Umfeld gegenüber Cyber-Risiken geschaffen wird.

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft

Marco Müth
Partner, Head of Real Estate Germany
T +49 69 9587 3347
mmueth@kpmg.com

Robert Betz
Partner, EMA Head of Digital Real Estate
T +49 89 9282 6822
rbetz@kpmg.com

ZIA
Zentraler Immobilien Ausschuss e.V.

Aygül Özkan
Stellvertretende
Hauptgeschäftsführerin
T +49 30 20215-8562
ayguel.oezkan@zia-deutschland.de

Dr. Michael Hellwig
Abteilungsleiter
Innovation, Digitalisierung und Research
T +49 30 20215-8552
michael.hellwig@zia-deutschland.de

Tobias Payer
Referent
Digitalisierung und Innovation
T +49 30 20215-8540
tobias.payer@zia-deutschland.de

www.kpmg.de

www.kpmg.de/socialmedia