Grant Thornton

# Cybersecurity in der deutschen Immobilien-wirtschaft.

## Ein unterschätztes Risiko

# Inhalt

# Ausgangslage

Unser Wirtschaftsleben ist heutzutage ohne Internet und digitale Arbeit undenkbar geworden. Gerade auch in der Bau- und Immobilienbranche sind die Arbeit am PC, der Austausch von Daten über das Internet und die Nutzung verschiedener Softwares grundlegend. Das wissen auch Kriminelle: Cyberkriminalität, Hacking und Internet-Betrug nehmen immer mehr zu. Während zu früheren Zeiten geschädigte Unternehmen bewusst die Information der Öffentlichkeit vermieden, steigt die Zahl der publik gewordenen Cyberangriffe.

So wächst die branchenübergreifende Sensibilisierung für mögliche Gefahren – wenngleich weiterhin eine hohe Dunkelziffer betroffener Unternehmen besteht. Daher schätzt der Branchenverband Bitkom in seiner aktuellen im September 2023 veröffentlichten Studie die in diesem Jahr durch Cyberattacken entstandenen Schäden für die deutsche Wirtschaft auf rund 206 Milliarden Euro.

Zunehmende Fälle und eine immer stärkere Professionalisierung der Täter spiegeln sich in den Sorgen der Unternehmen wider. Sprunghaft von neun auf 45 Prozent stieg die Zahl der Firmen, die eine massive Störung ihrer Geschäftsprozesse durch Hackerangriffe befürchten.

Für die deutsche Immobilienwirtschaft fehlte bislang ein transparentes Bild über die Risiken und existierende Schutzmaßnahmen. Unsere Studie untersucht daher als Pionierprojekt die Gefahreneinschätzung und die bislang registrierten Schäden in den Unternehmen. Aus der Befragung ergibt sich ein transparentes Bild über die Sensibilisierung der Immobilienwirtschaft für Cybersecurity, die bereits getroffenen Schutzmaßnahmen und die Beurteilung möglicher zukünftiger Risiken.

# Methodik

Die Studie baut auf den Ergebnissen einer Online-Umfrage unter Führungskräften und Entscheidern der Bau- und Immobilienbranche auf. Als Umfragetool wurde Qualtrics genutzt. **Die Befragung umfasste zwölf Fragen und wurde von März bis Juli 2023 durchgeführt. 64 Unternehmen haben sich an der Umfrage beteiligt.** Nach einleitenden Informationen zum jeweiligen Teilsegment innerhalb der Immobilienwirtschaft und der Unternehmensgröße anhand der Mitarbeiterzahl wurde die Gefahrenlage anhand bereits registrierter Angriffe und ihrer Folgen abgefragt. In einem weiteren Teil wurden die teilnehmenden Unternehmen gebeten, die bereits getroffenen sowie die zukünftig geplanten Schutzmaßnahmen anzugeben. Es folgten Selbsteinschätzungen zur bestehenden IT-Sicherheit und der Sensibilisierung der Belegschaft für mögliche Cyberrisiken. Die Umfrage wurde über die Verteiler von Grant Thornton und des Fachmagazins „Immobilien Aktuell“ sowie über LinkedIn geteilt.

Zu den Teilnehmern zählten größtenteils Geschäftsführer, CEOs oder Vorstandsmitglieder sowie Angestellte auf Abteilungsleiterebene. Mehrheitlich nahmen Unternehmen aus der Projektentwicklung und dem Asset Management teil. Die Antworten und Rückmeldungen der Teilnehmer wurden mithilfe der qualitativen Inhaltsanalyse geclustert und ausgewertet.

# Executive Summary

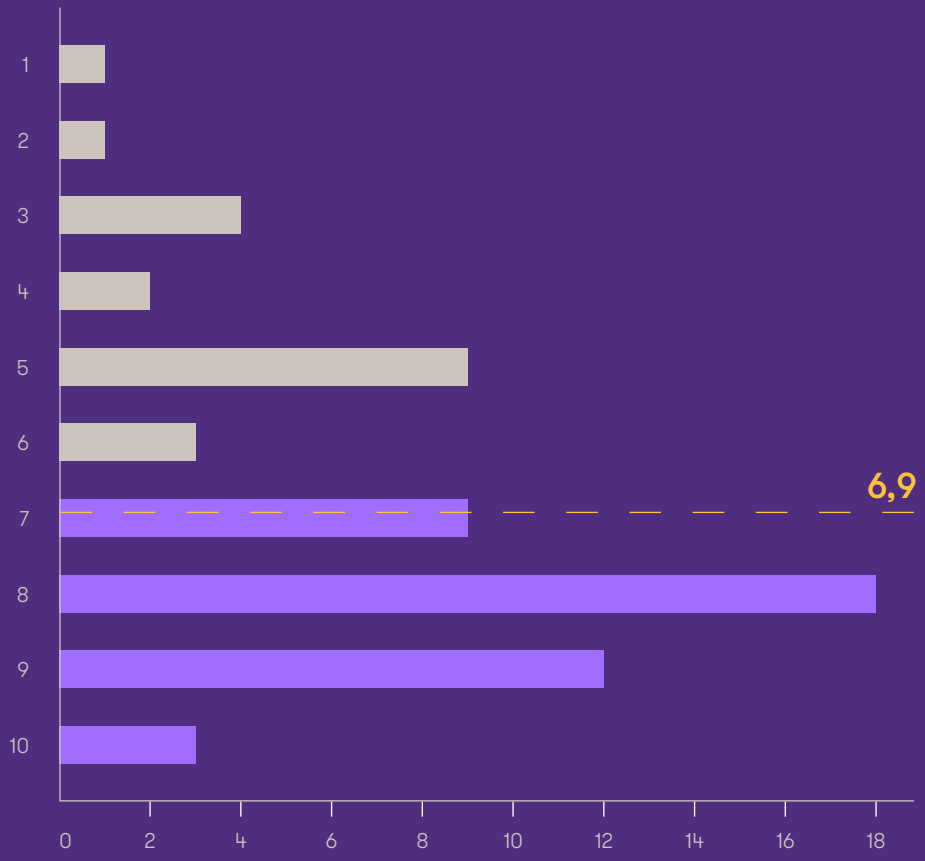
Cyberkriminalität ist im Alltag der Immobilienwirtschaft angekommen. **45 Prozent der Immobilienunternehmen in Deutschland stellten in den vergangenen zwölf Monaten mindestens eine Cyberattacke fest. Nur 23 Prozent verzeichneten keinen Angriff aufs IT-System, jedes zehnte Unternehmen meldete sogar über 50 Angriffe pro Jahr. Dementsprechend schätzen 37 Prozent die Gefahr von Cybercrime als hoch bis sehr hoch ein.**

Es gibt erheblichen Bedarf an fortschrittlicher Sicherheitsarchitektur: Nur etwa jedes zehnte Unternehmen nutzt beispielsweise Verschlüsselungs- und Authentifizierungssoftware. Sicherheitsmaßnahmen wie Zwei-Faktor-Authentifizierungen oder Mitarbeiterschulungen finden nur bei einer Minderheit der Unternehmen Anwendung.

Zwar sind die etablierten Sicherheitsstandards auch in der Immobilienwirtschaft angekommen. Dementsprechend findet Cybercrime in den Unternehmen kein offenes Einfallstor. Doch die in der Befragung sich ergebene Unwissenheit vieler befragter Unternehmen deutet darauf hin, dass die Sensibilisierung für IT-Sicherheit noch nicht zufriedenstellend ausgeprägt ist. Es ist davon auszugehen, dass die Dunkelziffer für Cyberattacken höher ist als die Rückmeldungen der Unternehmen es widerspiegelt.

# 1. Wie sicher schätzen Sie Ihre IT-Infrastruktur ein?

10 = sehr sicher
1 = sehr unsicher



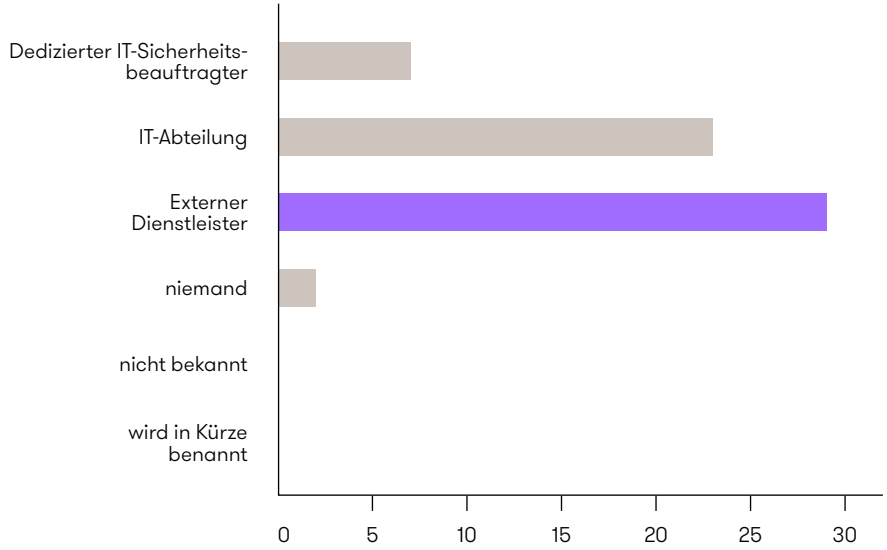

## Die Unternehmen schätzen ihre IT-Infrastruktur als sehr sicher ein.

Ein **Mittelwert von 6,9 von 10** zeigt, dass ein Grundbewusstsein um Sicherheit vorhanden ist. 28 Prozent sehen mit einem Wert von 5 und weniger ihre IT-Infrastruktur noch nicht ausreichend geschützt.

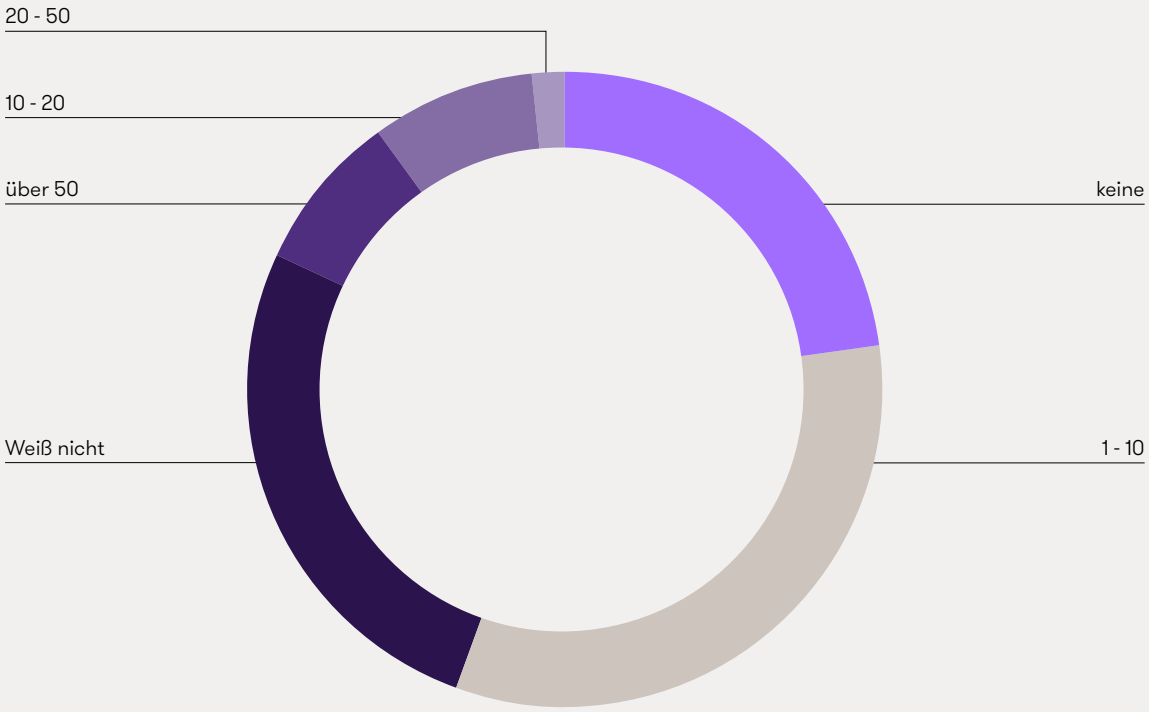
# 2. Wer verantwortet in Ihrem Unternehmen die IT-Security?

**Cybersecurity findet in der Regel nicht im Unternehmen selbst statt. Gut die Hälfte der Unternehmen hat IT-Sicherheit extern vergeben.**

Nur knapp über elf Prozent verfügen über einen dedizierten IT-Sicherheits-beauftragten: Cybersecurity – so liegt es nahe – ist also ein Thema unter vielen innerhalb der IT-Strategie der Unternehmen.



# 3. Wie viele Cyberangriffe haben Sie in den letzten zwölf Monaten in Ihrem Unternehmen registriert?




**Nur 23 Prozent können belegen, dass es im vergangenen Jahr keinen registrierten Angriff auf ihre IT gab. Bei rund 18 Prozent gibt es praktisch jeden Monat mindestens eine IT-Attacke.**

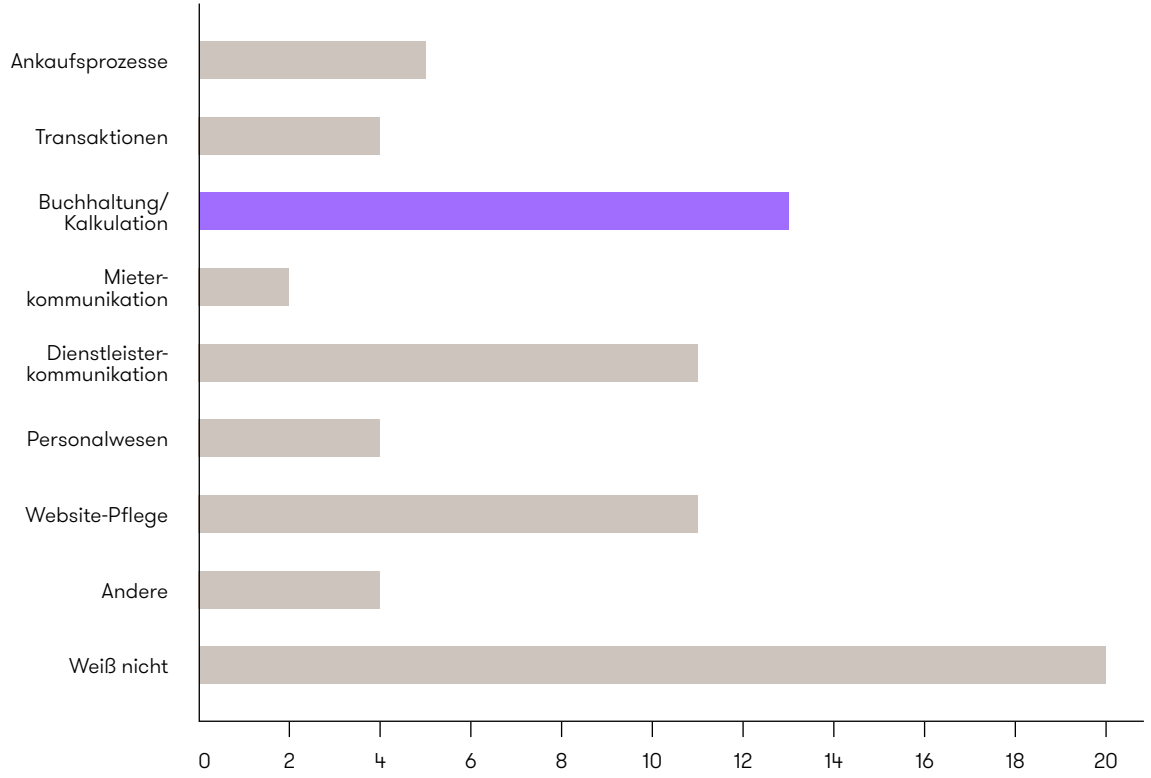
Rund jedes vierte Unternehmen misst keine Daten zu Cyberattacken – ein Indiz für Scheinsicherheit.

# 4. Welche Geschäftsbereiche haben sich im Rahmen der IT-Sicherheit als anfällig erwiesen?

(Mehrfachantworten möglich)

**Hacker-Angriffe haben vor allem die Finanzen der Unternehmen im Visier: Mit 18 Prozent ist die Buchhaltung der vulnerabelste Geschäftsbereich.**

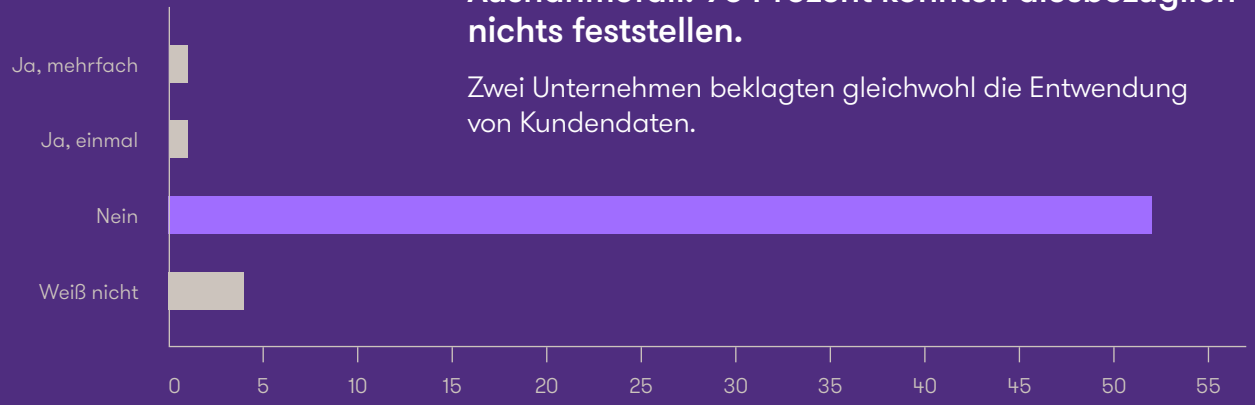
Webbasierte Anwendungen sind ein logisches Einfallstor für Cyberattacken: Rund 15 Prozent der Unternehmen nennen die Website-Pflege und die webbasierte Dienstleisterkommunikation als gefährdete Geschäftsprozesse.



# 5. Wurden in den letzten 36 Monaten im Rahmen von Cyberangriffen Kundendaten bei Ihnen entwendet?

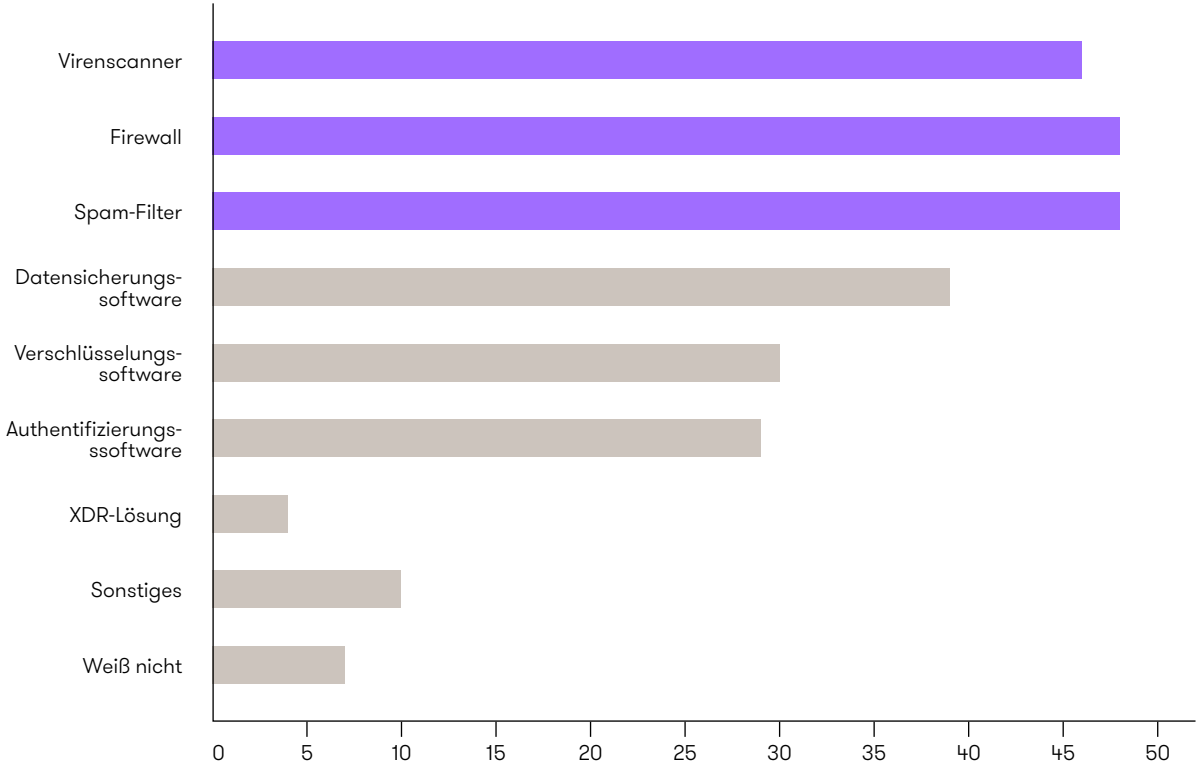
**Die Entwendung von Kundendaten bleibt ein Ausnahmefall. 90 Prozent konnten diesbezüglich nichts feststellen.**

Zwei Unternehmen beklagten gleichwohl die Entwendung von Kundendaten.



# 6. Welche Lösungen nutzen Sie im Rahmen Ihrer IT-Security?

(Mehrfachantworten möglich)

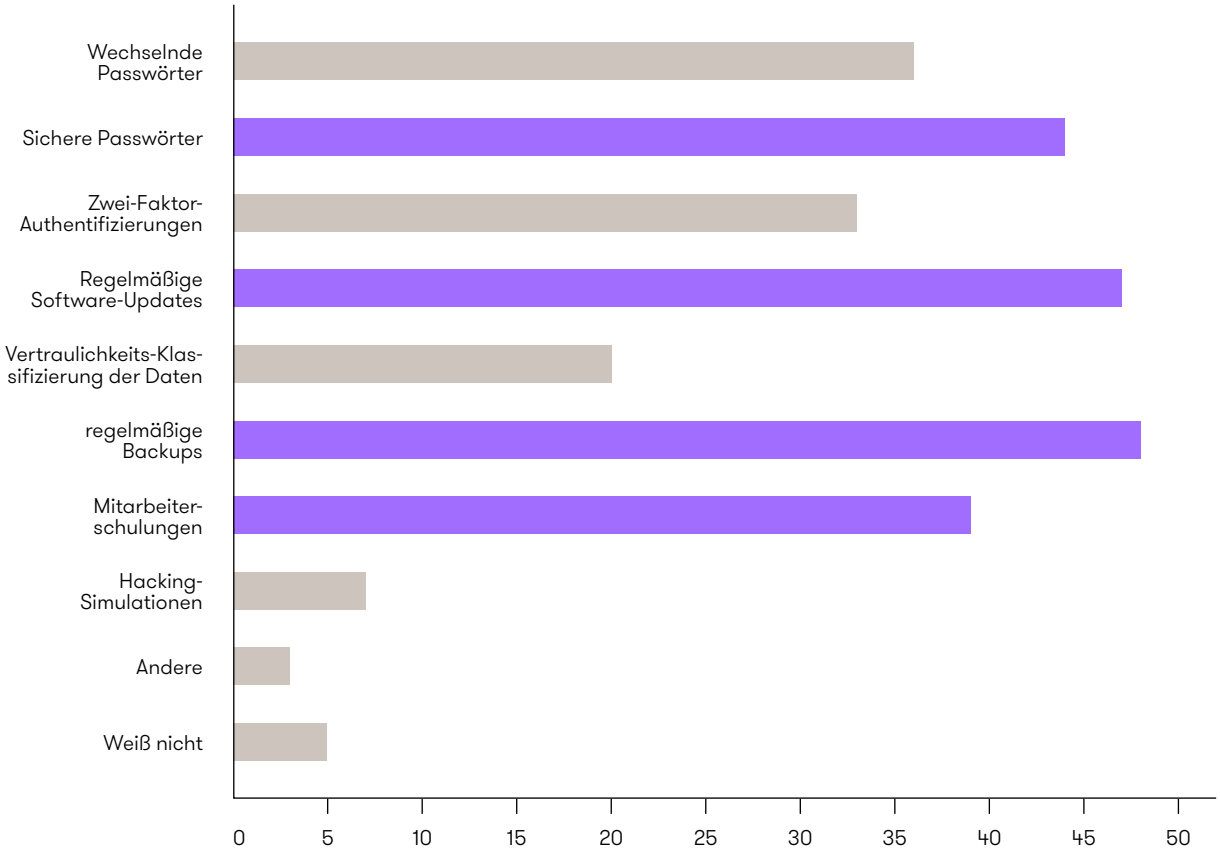



## Virenscanner, Firewall und Spam-Filter zählen mittlerweile zur Standardausstattung der IT-Sicherheit.

Darüber hinaus gehende Lösungen wie Authentifizierungs- oder Verschlüsselungssoftware sind jedoch noch selten in der Immobilienbranche im Einsatz. Mehrfach gesicherte Zugänge wie beispielsweise im Online-Banking sind also eine Seltenheit in den Unternehmen.

# 7. Welche Maßnahmen haben Sie im Rahmen Ihrer IT-Security bereits umgesetzt?

(Mehrfachantworten möglich)

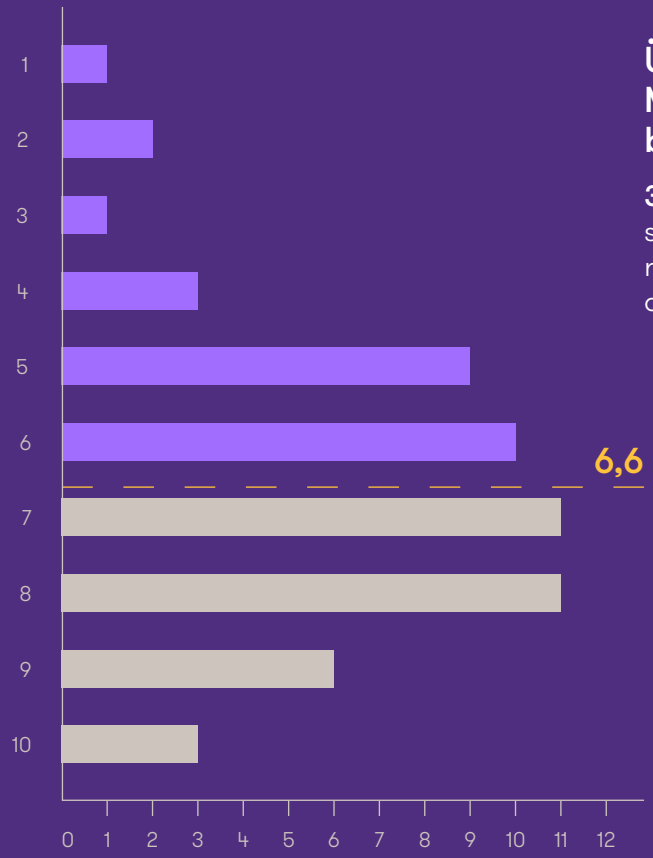



**Die Standard-Sicherheitsmaßnahmen wie regelmäßige Updates, Backups, Mitarbeiterschulungen oder sichere Passwörter sind bei der großen Mehrheit der Unternehmen etabliert.**

Weitaus seltener verbreitet sind wechselnde Passwörter, eine Kategorisierung der Daten nach Vertraulichkeit und Hacking-Simulationen.

# 8. Wie schätzen Sie die aktuelle Sensibilisierung Ihrer Mitarbeiter für Cyberattacken ein?

10 = stark sensibilisiert
1 = überhaupt nicht sensibilisiert

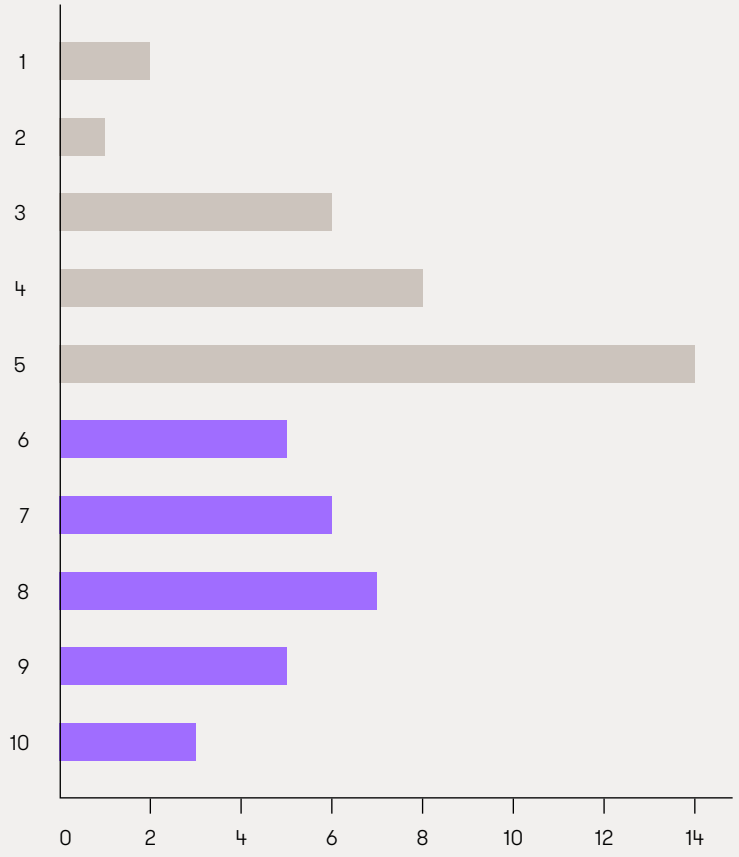



**Über 40 Prozent der Unternehmen schätzen ihre Mitarbeiter im Bereich Cybersecurity als mäßig bis nicht geschult ein.**

**35 Prozent** hingegen halten ihre Mitarbeiter für sehr gut sensibilisiert. Mit einem **Mittelwert von 6,6 von 10** besteht eine relativ hohe Sensibilisierung der Mitarbeiter, die allerdings auf der Selbsteinschätzung der Unternehmen beruht.

# 9. Wie hoch schätzen Sie die Gefahr von Cybercrime für Ihre Geschäftsprozesse ein?

10 = sehr hoch
1 = nicht vorhanden

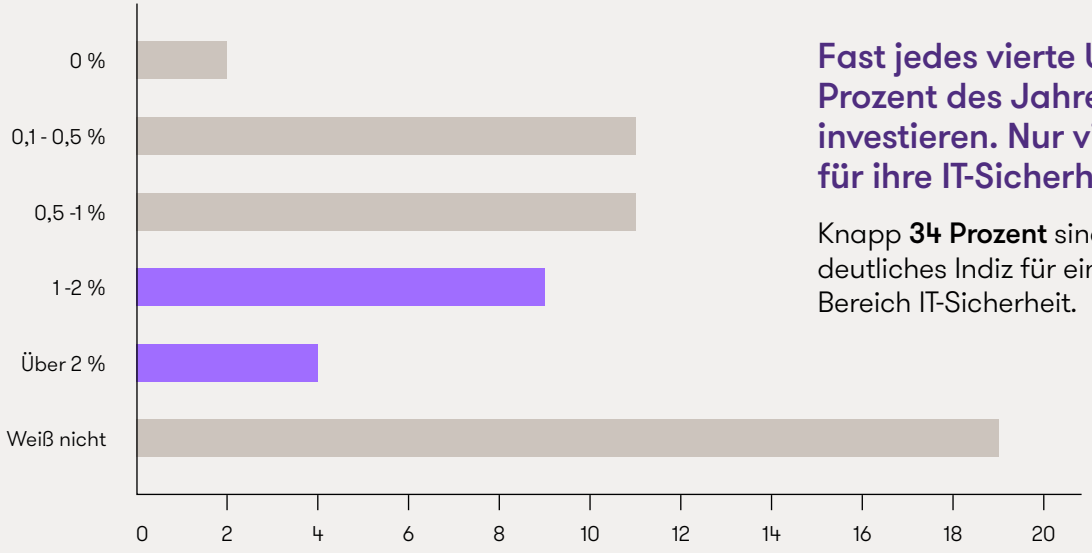



## Über jedes dritte Unternehmen sieht IT-Attacken als hohes bis sehr hohes Risiko für das gesamte Geschäftsmodell an.

Nur rund **15 Prozent** sehen eine geringe bis gar keine Gefahr durch Cyberkriminalität.

# 10. Wie viel Prozent Ihres Jahresumsatzes möchten Sie in den nächsten zwei Jahren in Ihre IT-Sicherheit investieren?

(inklusive Personalkosten)




**Fast jedes vierte Unternehmen plant, mehr als ein Prozent des Jahresumsatzes in Cybersecurity zu investieren. Nur vier Prozent wollen keine Ausgaben für ihre IT-Sicherheit tätigen.**

Knapp **34 Prozent** sind zu dieser Frage noch unentschieden – ein deutliches Indiz für eine notwendige höhere Sensibilisierung im Bereich IT-Sicherheit.

# Handlungsempfehlungen

**Das Bewusstsein um die IT-Sicherheit gehört ganz oben auf die Agenda. Mangelnde Informationen auf Entscheiderebene um Angriffe auf die IT-Infrastruktur sind ein deutlicher Beleg für eine noch unterentwickelte Sensibilisierung für die Gefahren von Cyberkriminalität. Es wäre wünschenswert, dass mehr betroffene Unternehmen den mutigen Gang an die Öffentlichkeit wagen.**

Gerade Bestandshalter und Asset Manager sind aufgrund der zunehmenden webbasierten Gebäudeautomation besonders gefordert, geeignete Maßnahmen für eine effektive IT-Sicherheit zu treffen.

Die Ausgliederung der IT-Sicherheit an einen externen Spezialisten ist naheliegend. Dabei ist eine enge Wechselwirkung zwischen Dienstleister und Entscheidern auf Unternehmensseite wichtig. Sind auch beim Auftraggeber Risikobewusstsein und entsprechende Expertise vorhanden, gehören solche Partnerschaften zu den besonders wirksamen Schutzmaßnahmen gegen oft verheerende Angriffe.

Mitarbeiterschulungen sind und bleiben ein einfacher und sehr wirksamer Bestandteil der Cybersecurity. Sie sollten mögliche Risikoszenarien bis hin zu Hacking-Simulationen umfassen.

Perspektivisch ist es für die Immobilienwirtschaft ratsam, besonders sensible Daten mittels einer Zwei-Faktor-Authentifizierung abzusichern.

Jedes Immobilienunternehmen benötigt eine Datenstrategie, um eine Priorisierung der jeweiligen Daten vorzunehmen und exklusive Zugriffsrechte zu etablieren.

## Sprechen Sie mit unseren Experten

**Dr. Florian Scheriau**
Partner, Risk Advisory
Düsseldorf
T +49 211 9524 8625
M +49 172 8245 859
E florian.scheriau@de.gt.com

Grant Thornton

**grantthornton.de**

© 2023 Grant Thornton AG Wirtschaftsprüfungsgesellschaft. Alle Rechte vorbehalten.

„Grant Thornton" bezieht sich auf die Marke, unter der Mitgliedsfirmen der Grant Thornton International Ltd („GTIL"), je nach Kontext eine oder mehrere, Prüfungs-, Steuerberatungs- und andere Beratungsleistungen (insgesamt „Leistungen") für ihre Mandanten erbringen. Die Grant Thornton AG Wirtschaftsprüfungsgesellschaft ist die deutsche Mitgliedsfirma von GTIL. GTIL und deren Mitgliedsfirmen sind keine weltweite Partnerschaft, sondern rechtlich selbständige Gesellschaften. Die Mitgliedsfirmen erbringen ihre Leistungen eigenverantwortlich und unabhängig von GTIL oder anderen Mitgliedsfirmen. Als operativ nicht tätige Dachorganisation erbringt GTIL keine Leistungen gegenüber Mandanten. Sämtliche Bezeichnungen richten sich an alle Geschlechter.
Stand 10/2023