

KPMG-Umfrage deckt Schwächen bei Cybersicherheit auf

Smart Building-Technik ist die Achillesferse der Unternehmen

Die Immobilienwirtschaft wird digitaler. Damit wächst aber auch die Gefahr von Hacker-Angriffen. Der ZIA weist darauf hin, dass das Smart Building Cyberkriminellen praktisch noch ungeschützt ausgeliefert ist. Diese könnten sich beispielsweise über die digitale Aufzugssteuerung Zugang zu ERP-Systemen und sensiblen Daten verschaffen.

Es braucht nur durchschnittliche IT-Kenntnisse, aber ganz sicher keine kriminelle Energie, um sich in die digitale Haustechniksteuerung eines Hotels zu hacken. Robert Betz sitzt im Frühstücksraum eines Hotels und stellt fest, dass sein Handy über Bluetooth Verbindung zur Heizungspumpe des Gebäudes hat. Das Passwort des Gerätes hat er sich vom Hersteller der Pumpe besorgt. Er könnte, wenn er wollte, die Leistung der Pumpe manipulieren. Das will Robert Betz aber nicht. Er ist einer der Autoren der aktuellen Studie „Cyber Security in der Immobilienwirtschaft“, die die Wirtschaftsprüfungsgesellschaft KPMG in Kooperation mit dem Zentralen Immobilien Ausschuss (ZIA) durchgeführt hat. Bei der Vorstellung der Studienergebnisse berichtet Aygül Özkan, stellvertretende ZIA-Hauptgeschäftsführerin, vom Hacker-Angriff gegen die Hotel One-Kette. Am 30. September sei das geschütz-



FOTO: DENIS VETTERHOFF / STOCK.ADOBE.COM

Die Hardware eines Unternehmens vor Angriffen zu schützen ist nur ein Aspekt von Cybersicherheit. Immobilienunternehmen müssen auch die Smart Building-Anwendungen in ihren Gebäuden in ein Sicherheitskonzept einbeziehen.

te IT-System des Unternehmens gezielt angegriffen worden. Die Kriminellen hätten sechs Terrabyte Kundendaten gestohlen. Die erste Cybersecurity-Studie von KPMG zeige, dass das Thema Sicherheit in der Immobilienwirtschaft rasant an Bedeutung gewinne.

Die Immobilienwirtschaft ist verstärkt Cyberangriffen ausgesetzt

Die Branche habe sich lange nicht im Fokus der Cyberkriminalität gesehen. Das enorme Tempo der Digitalisierung der Immobilienwirtschaft habe jedoch zu einem Paradigmenwechsel geführt, der die Notwendigkeit einer umfassenden Auseinandersetzung mit Sicherheitsfragen unterstreiche. Immer öfter würden Smart-Building-Technologien eingesetzt, die auch die gebaute Umwelt mit dem Cyberraum verbinden und die Branche zum Ziel von Angriffen machten. „Die Dynamik dieser Bedrohung wurde lange Zeit unterschätzt, da die Branche traditionell eher auf physische Sicherheitsmaßnahmen fokussiert war. Doch die Tatsache, dass auch die Immobilienwirtschaft vermehrt von Cyberangriffen betroffen ist, unterstreicht die Notwendigkeit, dass sich auch diese Branche umfassend mit den Cyberrisiken auseinandersetzen sollte“, betont Robert Betz, KPMG, Partner, Management Consulting Real Estate & EMA Head of Digital Real Estate. ZIA-Geschäftsführerin Aygül Özkan zieht drei Schlüsse aus den Umfrageergebnissen:

- Sicherheit sei Chefsache und müsse in den Vorständen der Unternehmen angesiedelt werden. Häufig bestehe ein Bewusstsein für die Risiken, es fehle aber an der Umsetzung von Sicherheitsstrategien. Sicherheit müsse Teil der Unternehmenskultur werden.
- Der Mensch sei das Einfallstor für Hackerangriffe. Deshalb sei die kontinuierliche Schulung und Sensibilisierung der Mitarbeiter notwendig.
- Es gebe nicht eine universelle Sicherheitslösung. Jedes Unternehmen sei ge-



FOTO: ZIA

Aygül Özkan, ZIA-Hauptgeschäftsführerin, zeigt sich alarmiert über den geringen Stellenwert von Cybersicherheit in vielen Unternehmen der Immobilienwirtschaft.

fordert, Schwachstellen ausfindig zu machen und individuelle Sicherheitskonzepte zu entwickeln.

KPMG-Experte Betz betonte, dass Wohnungsunternehmen eine Vielzahl persönlicher Daten – auch zahlungsrelevante – von Mietern pflegen. „An diese Daten wollen die Kriminellen gelangen“, so seine Warnung. Die Studie basiert auf einer Online-Befragung, an der sich im dritten Quartal 2023 über 100 Personen aus allen Bereichen der Immobilienwirtschaft beteiligten. Es seien alle Größen- und Assetklassen vertreten.

Die Ergebnisse der Studie

Obwohl 93 Prozent der Unternehmen dem Thema Cybersecurity eine hohe Relevanz beimessen, ergreifen sie seltener aktiv Maßnahmen zur Verbesserung der Sicherheit. Von allen befragten Unternehmen der Immobilienbranche haben 51 Prozent bereits eine Cybersecurity-Strategie etabliert. 24 Prozent der Firmen passen eine bestehende Strategie kontinuierlich an und etwa 27 Prozent überprüfen sie regelmäßig, um sie an Bedrohungsveränderungen anzupassen. Nahezu 80 Prozent der teilnehmenden Immobilienunternehmen haben keine unternehmensweite Strategie zur Absicherung ihrer Gebäudetechnik vor Cyberangriffen entwickelt. Lediglich 20 Prozent geben an, Strategien zum Schutz dieser Technik implementiert zu haben. Das zeige einen erheblichen Nachholbedarf bei den Sicherheitsvorkehrungen für Gebäudetechnik. Überwiegend kümmert sich nur ein Mitarbeiter um IT-Sicherheit und etwa 70 Prozent der befragten Unternehmen binden externe Dienstleister in Fragen der Cybersicherheit ein. (Red.)

