CYBER-SICHERHEIT IN DER WOHNUNGS-WIRTSCHAFT

Aktuelle Bedrohungen und Schutzmaß-nahmen für eine sichere digitale Zukunft.

DGC AG

24/7 High Performance Cybersecurity

1 Die Bedeutung von Cybersecurity für die Wohnungswirtschaft

» Kurze Übersicht über die wachsende digitale Vernetzung in der Wohnungswirtschaft (Smart Home, Gebäudemanagement-Systeme).

» Warum Unternehmen in der Wohnungswirtschaft anfällig für Cyberangriffe sind.

Digitalisiert – und damit im Visier.

» Gefahren: Die Wohnungswirtschaft digitalisiert sich stark, z.B. durch Smart-Home-Technologien und vernetzte Gebäudeverwaltungssysteme. Dies schafft neue Angriffs-flächen, da viele dieser Systeme oft nicht ausreichend abgesichert sind. Unternehmen unterschätzen oft die Bedrohung, die von veralteter Technologie oder schwachen Zugangskontrollen ausgeht.

» Beispiel: Smarte Heizsysteme, die über das Internet gesteuert werden, könnten bei einem Angriff ungewollt abgeschaltet oder missbraucht werden, um Mietern Schaden zuzufügen.

2 Aktuelle Cybersecurity-Lage in Deutschland

- Zahlen und Fakten (2024): Rund 70% der Unternehmen in Deutschland wurden in den letzten zwei Jahren Opfer von Cyberangriffen.
- Die durchschnittlichen Kosten eines Cyberangriffs betragen in Deutschland 4.9 Millionen Euro (Quelle: Bitkom).
- In der Wohnungswirtschaft sind besonders IoT-Geräte, Cloud-Systeme und ungesicherte Netzwerke Angriffspunkte.
- Gefahrenquellen: Phishing, Ransomware, unsichere Software und schwache Passwörter.

Gefährliche Lücken im Smart Home

- IoT-Geräte und Wohnungswirtschaft: In Deutschland sind zahlreiche vernetzte Geräte in Gebäuden im Einsatz, von Sicherheitskameras bis hin zu Smart-Thermostaten. Diese sind oft schlecht gesichert und werden zu beliebten Zielen für Angreifer.
- Zahlreiche Schwachstellen: Sicherheitsforscher haben in den letzten Jahren regelmäßig Schwachstellen in IoT-Geräten aufgedeckt, die Cyberkriminellen den Zugang ermöglichen.
- Schwache Passwörter und fehlende Sicherheitsupdates: Viele Geräte in der Wohnungswirtschaft laufen über Jahre hinweg ohne Updates. Diese Systeme verwenden oft Standardpasswörter oder schwache Authentifizierungen, die leicht gehackt werden können.
- Beispiel: Ein Fall aus Deutschland, bei dem Sicherheitskameras in Wohnanlagen gehackt wurden, weil sie mit Standardpasswörtern betrieben wurden.

3 Spezifische Risiken für die Wohnungswirtschaft

- IoT- und Smart Home-Geräte: Schwachstellen in Smart-Home-Systemen und Gebäudeverwaltung (Beispiele: Fernsteuerung von Heizung, Licht, Sicherheitssystemen).
- Datenschutz: Die Speicherung sensibler Mieterdaten und die Gefahr durch Datenlecks.
- Cloud-basierte Anwendungen: Angriffe auf Immobilienmanagement-Software oder Cloud-Dienste, die von Immobilienunternehmen genutzt werden.

Verwundbare Wohnsysteme

- IoT- und Smart Home-Geräte: Diese Geräte haben oft unzureichende Sicherheitsvorkehrungen, da der Fokus eher auf Benutzerfreundlichkeit und Kostenersparnis liegt. Hacker können diese Geräte als Einstiegspunkte nutzen, um Netzwerke zu kompromittieren oder sogar physische Schäden zu verursachen (z.B. Heizungsausfälle).
- Gefahr durch DDoS-Angriffe: IoT-Geräte werden häufig in Botnetze eingebunden, die für Distributed-Denial-of-Service (DDoS)-Angriffe genutzt werden, was große Netzwerkausfälle verursachen kann.
- Datenschutzverletzungen: Wohnungswirtschaftsunternehmen sammeln und speichern eine Vielzahl sensibler Daten, z.B. über Mieter, deren Mietverträge, Zahlungsinformationen und sogar Bewegungsprofile (z.B. durch Smart-Metering oder Zugangskontrollen). Bei Datenlecks könnten diese Informationen an die Öffentlichkeit gelangen oder verkauft werden.
- Datenlecks: Das Offenlegen persönlicher Informationen wie Mietvertragsdaten oder Zahlungsverläufe kann schwerwiegende Folgen wie Identitätsdiebstahl nach sich ziehen.
- Cloud-basierte Anwendungen: Viele Unternehmen der Wohnungswirtschaft nutzen cloudbasierte Verwaltungssoftware, um ihre Gebäude und Mietverhältnisse zu managen. Diese Cloud-Systeme sind oft schlecht konfiguriert und anfällig für Angriffe.
- Gefahr durch unzureichende Cloud-Sicherheit: Eine fehlerhafte Konfiguration kann zu offenen Zugangspunkten führen, die Angreifer nutzen können, um auf Daten oder Steuerungssysteme zuzugreifen.
- Risikofaktor Drittanbieter: Wohnungsbauunternehmen arbeiten oft mit einer Vielzahl von Dienstleistern (Facility Management, IT-Dienstleister, Handwerksfirmen) zusammen. Jede dieser Firmen stellt ein potenzielles Einfallstor dar, insbesondere, wenn deren Sicherheitsstandards niedriger sind. Angriffe über diese Lieferketten könnten verheerend sein.

4 Cyberangriffe der letzten Zeit und ihre Auswirkungen auf Unternehmen

- Beispiele aus der Wohnungswirtschaft oder verwandten Branchen (z.B. Hacks von IoT-Geräten in Mietshäusern oder Datenlecks bei Immobilienverwaltern).
- Kurzer Überblick über Ransomware-Angriffe, die Unternehmen in der Wohnungswirtschaft schwer getroffen haben.
- Folgen solcher Angriffe: Betriebsunterbrechungen, finanzielle Verluste, Reputationsschäden, regulatorische Sanktionen (DSGVO).

Hacker auf Mietjagd

- Hackerangriff auf Immobilienunternehmen (Berlin, 2023): Ransomware-Angriff legte IT-Infrastruktur lahm und verschlüsselte Mieterdaten. Das Unternehmen zahlte Lösegeld in Kryptowährung. Schaden: mehrere Millionen Euro, Reputationsverlust und Datenschutzprobleme.
- Cyberangriff auf Facility-Management-Unternehmen (2022): Hacker manipulierten Überwachungssysteme und Türsteuerungen in Wohnanlagen, was zu Mietausfällen führte. Die Wiederherstellung dauerte Monate, Schaden: siebenstelliger Betrag.
- Datenleck bei deutschem Wohnungsbauunternehmen (2021): Fehlkonfiguration in der Cloud machte Tausende Mieterdaten öffentlich zugänglich. Folge: Hohe Kosten, DSGVO-Strafen, Reputationsschäden und Mieterfluktuation.
- Cyberangriff auf Smart Building-Systeme (2020): Hacker griffen über IoT-Geräte auf zentrale Steuerungen zu, schalteten Heizungen ab und verursachten teure Reparaturen. Mieter klagten wegen der Unannehmlichkeiten.

5 Best Practices zur Prävention von Cyberbedrohungen in der Wohnungswirtschaft

» Schulung von Mitarbeitern: Regelmäßige Cybersecurity-Trainings, speziell für Facility Manager und IT-Teams.

» Technische Maßnahmen: Nutzung von Firewalls, regelmäßige Software-Updates, Passwort-Management-Systeme.

» Risikobewertung: Identifikation und Absicherung der wichtigsten IT-Infrastrukturen, z.B. Zugang zu Smart-Building-Systemen.

Cyberrisiko Mensch: Phishing, veraltete Technik und schwache Passwörter

Schulung von Mitarbeitern:

» Gefahr durch Phishing: Facility Manager, die administrative Zugänge zu IT-Systemen haben, sind häufige Ziele von Phishing-Angriffen. Unzureichend geschulte Mitarbeiter öffnen versehentlich bösartige E-Mails oder laden infizierte Anhänge herunter.

» Lösung: Regelmäßige Schulungen zur Sensibilisierung für Cyberbedrohungen und zur Erkennung von Phishing-Attacken.

Technische Maßnahmen:

» Firewall- und Netzwerküberwachung: Eine starke Firewall und kontinuierliche Netzwerküberwachung können Anomalien erkennen und Angriffe abwehren, bevor Schaden entsteht.

» Regelmäßige Updates: Häufig ignorierte Updates können Schwachstellen in der Software schließen und Systeme sicherer machen.

» Passwort-Management-Systeme: Schwache Passwörter sind nach wie vor eine der häufigsten Ursachen für Cyberangriffe. Die Implementierung von Passwort-Management-Systemen und Zwei-Faktor-Authentifizierung ist entscheidend.

Risikobewertung:

» Gefahr durch veraltete Infrastruktur: In vielen Gebäuden der Wohnungswirtschaft werden noch immer ältere IT-Infrastrukturen verwendet, die nicht für moderne Cybersecurity-Anforderungen ausgelegt sind.

» Lösung: Eine regelmäßige Risikobewertung hilft dabei, Schwachstellen frühzeitig zu erkennen und Maßnahmen zur Absicherung zu ergreifen.

6 Zukünftige Herausforderungen und Trends in der Cybersecurity für die Wohnungswirtschaft

» Gesetzliche Anforderungen: Zunehmende Anforderungen durch NIS2-Richtlinien und die EU-Datenschutzverordnung.

» Trends: Künstliche Intelligenz in der Cybersicherheit, Zero-Trust-Architekturen, erhöhte Integration von IoT-Sicherheit.

» Zukunftssichere Cybersecurity: Strategien zur Implementierung von Cybersicherheitslösungen, die auch künftige Bedrohungen adressieren.

Ausblick: Neue Vorgaben erzwingen Umdenken

Gesetzliche Anforderungen:

» NIS2-Richtlinien: Diese werden für kritische Infrastruktur zunehmend relevant. Unternehmen der Wohnungswirtschaft könnten unter diese Regelungen fallen, wenn sie größere Netzwerke oder cloudbasierte Systeme betreiben.

Trends:

» Zero-Trust-Architektur: Dieser Ansatz basiert darauf, jedem Benutzer und Gerät standardmäßig zu misstrauen, bis ihre Identität und Berechtigungen eindeutig geprüft wurden. Dieser Trend könnte für die Wohnungswirtschaft besonders wichtig werden, um den Zugang zu kritischen Systemen zu schützen.

» Künstliche Intelligenz in der Cybersicherheit: KI wird zunehmend eingesetzt, um verdächtiges Verhalten in Netzwerken zu erkennen und potenzielle Angriffe proaktiv zu verhindern.

» Zukunftssichere Cybersecurity: Wohnungsbauunternehmen sollten in Technologien und Strategien investieren, die nicht nur gegen aktuelle Bedrohungen, sondern auch gegen zukünftige Herausforderungen robust sind. Dazu gehören erweiterte Netzwerküberwachung, verstärkte Zugangskontrollen und die Implementierung von Verschlüsselungstechnologien.

FAZiT

Diese detaillierte Ausführung gibt Ihnen einen Einblick in die spezifischen Gefahren und Herausforderungen, die für Unternehmen der Wohnungswirtschaft in Bezug auf Cybersecurity bestehen.

Unternehmen stehen vor erheblichen Haftungsrisiken, wenn sie Cybersecurity vernachlässigen, da Angriffe nicht nur zu Datenlecks und Imageverlust führen, sondern auch hohe finanzielle Schäden verursachen können. Es ist daher unerlässlich, die Cybersecurity-Strategien regelmäßig zu überprüfen und auf dem neuesten Stand zu halten.

Zusätzlich bietet sich die Möglichkeit, durch Security-Checks oder Beratungen als Serviceleistung proaktiv das Risiko zu minimieren und potenziellen Haftungsfällen vorzubeugen.

ANGRiFF

„Erfolgreiche Cyberangriffe sind keine Frage des Ob, sondern des Wann. Jeden kann es treffen – seid vorbereitet.“

Dr. Dirk Häger
Bundesamt für Sicherheit in der Informationstechnik (BSI)

WiR

24/7 High Performance Cybersecurity

360° Cybersecurity	Eigens entwickelte Tools im Einsatz
Heterogene Kundenstruktur	Zertifiziert ISO 27001

Alle Experten mit tiefgreifender Cybersecurity-Erfahrung.
Spezialisten aus Team Red (Pentester) & Team Blue (Verteidigung)

DGC AG – Ihr Partner für maßgeschneiderte Cybersecurity-Lösungen

Die DGC AG zählt zu den führenden Anbietern in der Cybersicherheit. Wir bieten maßgeschneiderte Lösungen, die für Unternehmen unverzichtbar sind. Unser Leistungsspektrum reicht von Penetrationstests (simulierte Hackerangriffe) über Security Awareness Trainings und Sicherheitsberatung bis hin zu Notfalldiensten. Damit bieten wir flexible, anpassbare Services, die individuell auf die Anforderungen unserer Kunden aus verschiedenen Branchen zugeschnitten sind.

Unser USP: das eigens entwickelte Cybersecurity-Portal cyberscan.io®

Das von unseren IT-Sicherheitsexperten entwickelte Cybersecurity-Portal cyberscan.io® bietet Ihnen 24/7 aktuelle Informationen zu Sicherheitslücken, um Ihre Systeme proaktiv zu überwachen und effektiv zu schützen. Mit unserem umfassenden Fachwissen und modernster Technologie sorgen wir dafür, dass Bedrohungen frühzeitig erkannt und gezielt abgewehrt werden. Setzen Sie auf unsere Erfahrung und zukunftssichere, maßgeschneiderte Lösungen für maximalen Schutz.

MERCi

BLEIBEN SIE SICHER!