Gefahr erkannt, **Gefahr gebannt**

Wie Immobilienverwaltungen sich gegen Risiken von Cyberangriffen schützen können.

Cybercrime gehört inzwischen zu den größten Geschäftsrisiken weltweit! Viele Unternehmen sehen sich zunehmend bedroht durch Cyberangriffe, die ihre Arbeitsfähigkeit erheblich beeinträchtigen können. Laut einer Umfrage sind 58 Prozent der befragten Unternehmen in Deutschland 2023 mindesten einmal Opfer einer Cyberattacke oder einer Netzwerkverletzung geworden (Statista). Insgesamt gab es einer Studie von Cybersecurity Ventures zufolge im Jahr 2023 alle 39 Sekunden einen Cyberangriff, das sind 2.200 Hackerangriffe pro Tag.

Auch die Wohn- und Immobilienwirtschaft bleibt von solchen Angriffen nicht verschont, denn durch die zunehmende Digitalisierung werden die Bedrohungsrisiken steigen. Noch betrachten auch Versicherer das Thema Cyber Risk moderat, aber es ist abzusehen, dass die Schäden und damit auch die Prämien für Cyber-Risk-Versicherungen in Zukunft steigen werden. Das Cyberrisiko hat sich durch Geopolitik, Künstliche Intelligenz (KI) und Remote Work weiter verschärft.

In den vergangenen Jahren haben auch die Unternehmen DOMUS, Pantaenius und INCON einen rasanten Anstieg der Cyberangriffe auf Immobilienverwaltungen registriert. Diese Angriffe führten zu mehrtägigen Arbeitsausfällen und erheblichen Kosten. Angesichts dieser wachsenden Bedrohung sollten Immobilienverwaltungen dringend Maßnahmen ergreifen, um sich vor diesen Risiken zu schützen.

Immobilienverwaltungen arbeiten mit zahlreichen sensiblen und kundenspezifischen Daten und sind auf verlässliche IT-Systeme angewiesen, um ihre Arbeitsfähigkeit zu gewährleisten. Ein wirksamer Schutz vor Cyberangriffen ist daher unerlässlich, um den Geschäftsbetrieb zu sichern und das Vertrauen der Kunden zu bewahren.

Phishing, Trojaner, Zoom-Bombing – Cyberkriminelle sind kreativ und lassen sich täglich etwas Neues einfallen, was sie inflationär oder aber auch ganz gezielt versenden. Die Wahrscheinlichkeit, dass es irgendwann auch einen selbst trifft, ist daher groß.

DIE AUTORINNEN

Sabine Leipziger
Geschäftsführerin INCON GmbH & Co. Assekuranz KG
www.incon-vm.de

Stephanie Kreuzpaintner
CEO DOMUS Software AG
www.domus-software.de

Christina Hesse
Geschäftsleitung Pantaenius Versicherungsmakler GmbH
www.pantaenius.eu/immo

Beispiele für Cyber-Risiken aus der Praxis

Verschlüsselung von Daten: Über schwache Passwörter gelangte Schadsoftware in das System einer Immobilienverwaltung und verschlüsselte sämtliche Dateien mit den Endungen .locked und .readme_txt. Die Mitarbeitenden konnten nicht mehr auf die Dateien zugreifen und waren somit stark in ihrer Arbeit eingeschränkt.

Hacking: Ein Mitarbeiter einer Immobilienverwaltung öffnete versehentlich einen E-Mail-Anhang, der einen Trojaner enthielt. Die Schadsoftware manipulierte den Server der Verwaltung und versandte über die IT-Infrastruktur Spam-E-Mails.

Verschlüsselung von Kundendaten: Ein Hacker nutzte eine Schwachstelle in der Verwaltungs-Software, um sich Zugang zum System einer Immobilienverwaltung zu verschaffen. Für die Entschlüsselung der Daten forderte er die Auszahlung von Bitcoins.

Laptop-Diebstahl: Einem Verwalter wurde sein Arbeitsrechner entwendet. Auf dem Laptop befanden sich Personendaten und Kontoverbindungen von mehreren Wohnungseigentümergemeinschaften und Dienstleistern.

Server lahmgelegt: Ein Mitarbeiter nutzte sein Firmen-Notebook für private Zwecke. Über eine vireninfizierte Bilddatei gelangte Schadsoftware in das Firmennetzwerk, wodurch der Server für mehrere Tage lahmgelegt wurde. Die Verwaltung war bis zur Wiederherstellung nicht arbeitsfähig und hatte keinen Zugriff auf ihr IT-System.

Vier Praxistipps für mehr Sicherheit

Unternehmen jeglicher Größe können sich widerstandsfähig aufstellen und sich durch die Umsetzung einiger Maßnahmen gut schützen.

1. Mitarbeitende sensibilisieren und schulen
   Der Mensch ist die häufigste „Schwachstelle" bzw. Ursache für Cyberschäden. Das Verhalten der Mitarbeitenden kann das Cyberrisiko nachhaltig minimieren. Die Sensibilisierung der Mitarbeitenden ist daher am wichtigsten. Regelmäßige Schulungen und die Stärkung der Medien- und Internetkompetenz jedes Einzelnen sind unerlässlich.

2. IT und Schnittstellen prüfen
   Welche Schnittstellen bieten Sicherheit und wo gibt es Nachbesserungsbedarf? Viele Verwaltungen arbeiten heute mit technischen Insellösungen. Dabei verfügen die wenigsten Dienstleister über zertifizierte Schnittstellen. Dies führt wiederum dazu, dass auch eigentlich sichere Infrastrukturen „Einfallstore nach außen" bieten. Das erhöht das Risiko für Fehler in den Arbeitsabläufen sowie digitale Angriffe erheblich. Zudem könnten Daten durch Dritte verändert werden. Das macht Haftungsansprüche gegenüber dem Software-Anbieter im Schadensfall nahezu unmöglich. Daher sollten Verwaltungen stets darauf achten, ausschließlich zertifizierte Schnittstellen für die Datenübertragung zu nutzen. Dies ist sowohl bei „kleineren" ERP-Programmen als auch bei umfangreichen CRM- und Cloud-Lösungen der Fall.

3. Cyberrisiken absichern, auch durch Versicherungsschutz
   Wenn der Fall dann doch eintritt, ist schnelle Hilfe wichtig. Spezielle Versicherungen bieten umfassenden Schutz vor den finanziellen Folgen von Cyberangriffen. Eine Cyber-Risk-Versicherung sollte inzwischen zur Standardabsicherung jedes Unternehmens gehören. Sie deckt verschiedene Arten von Schäden ab, die durch Cyberangriffe entstehen können, einschließlich Datenverlusten, Betriebsunterbrechungen, Reputationsschäden und Haftungsansprüchen. Diese Versicherung schützt umfassend und erlaubt es, im Ernstfall schnell und effektiv zu reagieren, um die Auswirkungen eines Angriffs zu minimieren und den Geschäftsbetrieb wiederherzustellen.

4. Notfallplan und -kommunikation
   Die Erarbeitung einiger Maßnahmen im Vorfeld, um nach einem Cyberangriff weiterhin arbeitsfähig zu bleiben, hat sich als wertvoll erwiesen. Was tun, wenn die IT lahmgelegt wurde? Gibt es Backups und wer ist verantwortlich? Cyber-Sicherheit ist nicht nur ein Thema für die IT-Abteilung oder den IT-Beauftragten. Alle Mitarbeitenden müssen im „Fall der Fälle" wissen, was zu tun ist und gegenüber den Eigentümern und Mietern eine entsprechende Kommunikationsstrategie kennen.

Zusammenfassend lässt sich sagen: Absolute Sicherheit gibt es leider nicht. Der bestmögliche Schutz vor Cyberangriffen wird durch eine Kombination aus gut geschulten und sensibilisierten Mitarbeitenden, sicherer und aktueller Software sowie einer umfassenden individuellen Versicherung erreicht.

Cyber-Risk-Versicherung im Detail

Eine Cyber-Risk-Versicherung deckt verschiedene Arten von Schäden ab, die durch Cyberangriffe entstehen können:

Eigenschäden
- z. B. Schäden an Hard- und Software infolge eines Hackerangriffs
- Kosten für die Wiederherstellung der Daten
- Kosten der Wiederherstellung der Funktionsfähigkeit der IT
- Betriebsunterbrechungsschaden der IT vor Ort oder Cloud
- Abwehrkosten bei behördlichen Verfahren wegen Datenrechtsverletzungen
- Kosten für IT-Forensiker, z. B. bei Erpressung

Drittschäden
- Vermögensschäden Dritter wegen Datenrechtsverletzung
- Vermögensschäden Dritter aufgrund Weiterleitung von Viren und Trojanern

Schadenermittlungskosten/Krisenkommunikation
- Kosten für IT-Spezialisten zur Schadenermittlung
- Kosten für Krisenkommunikation mit Geschädigten (Eigentümer, Mieter, Dienstleister und sonstige Vertragspartner)
- Kosten für anwaltliche Vertretung

Für eine optimale Absicherung sollte die Höhe der Versicherungssumme bedarfsgerecht mit einem Versicherungsexperten für Immobilienverwaltungen kalkuliert werden.