Ihre Fragen – unsere Antworten

Webinar „Cyber-Risiken für Immobilienverwaltungen – Prävention, Haftung und richtiges Vorgehen im Schadenfall“

Frage

Gibt es statistische Daten, die belegen, wie häufig Immobilienverwaltungen in ganz Deutschland in den Jahren 2024 oder 2025 angegriffen wurden? Gibt es weiterhin Angaben zur Höhe des entstandenen Schadens – sowohl zum jährlichen Gesamtschaden als auch zum durchschnittlichen Schaden pro Angriff bzw. Vorfall?

Antwort

Konkrete Branchenzahlen für Immobilienverwaltungen gibt es nicht. Der jährliche Gesamtschaden durch Cyberattacken in Deutschland beträgt laut Bitkom über 200 Milliarden Euro pro Jahr. Immobilienverwaltungen sind darin enthalten, lassen sich aber nicht isoliert ausweisen.

Begründung, warum es keine spezifischen Zahlen für Immobilienverwaltungen gibt:

1. **Keine eigene statistische Kategorie**
   Immobilienverwaltungen werden statistisch nicht als eigene Kategorie erfasst, sondern unter „Dienstleistungen“ oder „Immobilienwirtschaft“ eingeordnet.
2. **Hohe Dunkelziffer**
   Viele Vorfälle werden aus Angst vor Imageschäden oder Haftungsfolgen nicht gemeldet.
3. **Starke Heterogenität**

   Zwischen kleinen WEG-Verwaltern und großen Wohnungsunternehmen bestehen erhebliche Unterschiede in Angriffsfläche und Schadenpotenzial.

Fazit

Eine verlässliche Branchenquote, die belegt, wie viele Immobilienverwaltungen angegriffen wurden oder wie hoch der durchschnittliche Schaden pro Vorfall ist, existiert nicht.

Folgende Aussagen sind belastbar:

- „Jedes sechste Unternehmen wurde 2024 Opfer eines Cyberangriffs.“
- „Fast alle Unternehmen hatten in den letzten Jahren Kontakt mit Cyberangriffen.“
- „Schäden reichen häufig bis in den sechsstelligen Bereich.“
- „Immobilienunternehmen geraten zunehmend ins Visier.“

Folgende Aussagen können nicht seriös getroffen werden:

- „X % aller Immobilienverwaltungen sind betroffen.“
- „Der Durchschnittsschaden speziell für Verwalter beträgt …“

Fortsetzung siehe Seite 2

Typische Angriffsszenarien aus der Praxis

(basierend auf Marktbeobachtung und Schadenerfahrung, keine offizielle Statistik)

- **Phishing mit Zahlungsumleitung**
  Der mit Abstand häufigste Angriff. Betrüger geben sich per E-Mail als bekannte Geschäftspartner aus und leiten Zahlungen auf eigene Konten um.
- **Ransomware**
  Schadsoftware verschlüsselt sämtliche Daten und Systeme. Ohne Zahlung oder Backup besteht das Risiko einer vollständigen Betriebsstilllegung.
- **E-Mail-Kompromittierung**
  Beispielsweise übernehmen Angreifer bestehende E-Mail-Konten und versenden darüber gefälschte Rechnunge von Handwerkern oder Dienstleistern.

Frage

Woran merke ich eigentlich, dass eine Datenschutzverletzung stattgefunden hat? Erst, wenn das System steht?

Antwort

Eine Datenschutzverletzung im Sinne von Art. 4 Nr. 12 der Datenschutz-Grundverordnung (DSGVO) liegt vor, wenn personenbezogene Daten unbeabsichtigt oder unrechtmäßig

- offengelegt,
- verändert,
- verloren oder
- unzugänglich gemacht werden.

Herausforderung

Eine Datenschutzverletung kündigt sich selten eindeutig an – sie zeigt sich meist nur über indirekte Hinweise. Viele Angriffe bleiben zunächst unbemerkt, weil Angreifer bewusst unauffällig vorgehen, um möglichst lange im System aktiv zu bleiben und möglichst viele Informationen abzuschöpfen. Der Stillstand eines Systems ist daher oft nicht der Beginn, sondern bereits das Ende eines längeren Vorgangs.

Frage

Ist der Versicherungsschutz an Bedingungen geknüpft (gibt es Kürzungen, weil keine Vorsorge getroffen wurde?)

Antwort

Cyber-Risk-Versicherungen zahlen nicht automatisch, sondern der Schutz ist immer an konkrete Sicherheitsanforderungen geknüpft. Werden diese nicht eingehalten, kann es zu Leistunsgkürzungen oder sogar zur vollständigen Leistungsablehnung kommen.

Bitte beachten Sie vor allem die Antragsfragen und Obliegenheiten.

Fortsetzung siehe Seite 3

Frage

Gibt es seitens des Versicherers eine „due diligence“ vor dem Abschluss der Cyber-Risk-Versicherung?

Antwort

Versicherer prüfen vor Abschluss der Cyber-Risk-Versicherung das Risikoprofil, allerdings meist standardisiert und risikoorientiert, in Form der Antragsfragen:

- IT-Infrastruktur (Server, Cloud, externe Dienstleister)
- Sicherheitsmaßnahmen (Firewall, Updates, Backups)
- Zugriffskontrollen (Passwörter, MFA)
- frühere Sicherheitsvorfälle
- Umgang mit personenbezogenen Daten (relevant zur Datenschutz-Grundverordnung)

Frage

Wo finde ich den Link für die Checkliste zum richtigen Vorgehen im Ernstfall?

Den Link zu der Checkliste „Cyber-Risken: Das ist im Ernstfall zu tun“ finden Sie hier:

Zur Checkliste

Sind Sie unsicher, ob Sie umfassend und mit ausreichender Deckungssumme vor Cyber-Risiken abgesichert sind oder benötigen Sie eine individuelle Beratung?

Als Spezialist sind wir gerne für Sie da!

INCON
EINFACH.DIGITAL.PERSÖNLICH.

Kontakt

INCON GmbH & Co. Assekuranz KG
Telefon 089 330075-0 (München)
info@incon-vm.de