

Cybersicherheit: Die größten Bedrohungen in der Versicherungsbranche

Versicherungsbote, 23.10.2024

Die zunehmende Digitalisierung in der Versicherungsbranche bringt nicht nur viele Vorteile mit sich, sondern stellt Unternehmen auch vor erhebliche Herausforderungen im Bereich der Cybersicherheit und des Datenschutzes. Im Gastbeitrag beleuchtet Thomas Köhler (V-Quiz) die größten Bedrohungen.

Versicherungen sammeln und verarbeiten täglich eine Fülle von sensiblen Kundendaten, darunter persönliche Informationen, medizinische Daten und finanzielle Details. Diese Informationen machen Versicherungsunternehmen zu einem attraktiven Ziel für Cyberkriminelle.

Die größten Cybersecurity-Bedrohungen in der Versicherungsbranche

- 1. Phishing-Angriffe:** Phishing ist nach wie vor eine der häufigsten Bedrohungen für Versicherungen. Dabei versuchen Angreifer, über gefälschte E-Mails oder Websites an vertrauliche Informationen zu gelangen. Laut einer Studie von Statista verzeichnete allein Deutschland im Jahr 2022 über 300.000 Phishing-Angriffe. Versicherer müssen daher ihre Mitarbeiter schulen, um solche Angriffe frühzeitig zu erkennen.
- 2. Ransomware:** Ransomware-Angriffe sind eine der gefährlichsten Formen von Cyberangriffen. Hierbei

verschlüsseln Hacker die Daten eines Unternehmens und verlangen ein Lösegeld, um sie wieder freizugeben. Eine Analyse von Cybersecurity Ventures prognostiziert, dass die durch Ransomware verursachten Schäden weltweit bis 2025 auf 10,5 Billionen US-Dollar ansteigen könnten.

- 3. Datenlecks:** Ein weiteres großes Problem sind Datenlecks, die durch unzureichende Sicherheitsmaßnahmen entstehen können. Laut dem IBM Cost of a Data Breach Report 2022 kostet ein durchschnittliches Datenleck in der Finanzbranche etwa 5,97 Millionen US-Dollar.

Regulatorische Anforderungen und deren Auswirkungen

Neben den Bedrohungen durch Cyberkriminalität haben sich auch die regulatorischen Anforderungen an den Datenschutz in den letzten Jahren verschärft. Die Datenschutz-Grundverordnung (DSGVO) in Europa schreibt strenge Regeln für den Umgang mit personenbezogenen Daten vor. Versicherungsunternehmen müssen sicherstellen, dass sie diese Anforderungen erfüllen, um hohe Geldstrafen und Reputationsschäden zu vermeiden.

Zusätzlich zu den nationalen Vorschriften gibt es branchenspezifische Richtlinien wie die IDD (Insurance Distribution Directive), die Versicherungsunternehmen dazu verpflichtet, ihre Mitarbeiter regelmäßig zu schulen und fortzubilden.

Best Practices zur Verbesserung der Cybersicherheit

- **Verschlüsselung von Daten:** Eine der wichtigsten Maßnahmen, um sensible Informationen zu schützen, ist die Verschlüsselung von Daten. Versicherer sollten sicherstellen, dass alle gespeicherten und übertragenen Daten verschlüsselt sind. Moderne Verschlüsselungstechnologien stellen sicher, dass Daten selbst dann geschützt sind, wenn sie von Cyberkriminellen abgefangen werden.
- **Zwei-Faktor-Authentifizierung (2FA):** Die Einführung einer Zwei-Faktor-Authentifizierung erhöht die Sicherheit von Kundenkonten erheblich. Laut dem Verizon Data Breach Investigations Report 2021 können bis zu 80 % der Phishing-Angriffe durch den Einsatz von 2FA verhindert werden.
- **Mitarbeiterschulungen:** Oft sind die eigenen Mitarbeiter das schwächste Glied in der Sicherheitskette. Regelmäßige Schulungen und Sensibilisierungsprogramme sind entscheidend, um das Bewusstsein für Sicherheitsrisiken zu schärfen und sicherzustellen, dass Mitarbeiter im Umgang mit Cyberbedrohungen geschult sind.
- **Penetrationstests und Sicherheitsüberprüfungen:** Versicherungsunternehmen sollten regelmäßig Penetrationstests durchführen lassen, um Schwachstellen in ihren IT-Systemen zu identifizieren und zu beheben, bevor Angreifer diese ausnutzen können.

Cyber-Versicherungen: Ein wachsender Markt

Mit der zunehmenden Bedrohung durch Cyberangriffe wächst auch der Markt für Cyber-Versicherungen. Immer mehr Unternehmen erkennen die Notwendigkeit, sich gegen die finanziellen Folgen eines Cyberangriffs abzusichern. Cyber-

Versicherungen decken in der Regel Kosten für Datenverluste, Systemausfälle und rechtliche Streitigkeiten ab. Versicherer, die selbst solche Produkte anbieten, müssen besonders wachsam sein, um ihre eigenen Systeme zu schützen.

V-Quiz: Ein Tool zur Schulung der Mitarbeiter

Angesichts der steigenden Bedrohungen und der wachsenden regulatorischen Anforderungen ist es essenziell, dass Versicherungsmitarbeiter regelmäßig im Bereich Cybersecurity geschult werden. V-Quiz, eine App zur Weiterbildung in der Versicherungsbranche, bietet hier eine innovative Lösung. Mit gamifizierten Schulungsmodulen zu Themen wie Datenschutz, Cybersicherheit und regulatorischen Anforderungen hilft V-Quiz Versicherungsunternehmen, ihre Mitarbeiter auf spielerische Weise zu schulen und dabei gleichzeitig die gesetzlichen Vorgaben zu erfüllen.