IT-Sicherheit

Wie sich KMU vor Cybergefahren schützen können

Cybergefahren gehören heute zu den grössten Risiken für ein KMU und die Folgen können verheerend sein. Massnahmen wie Mitarbeitersensibilisierung, Schutz der IT-Systeme und Versicherungen können diese Risiken reduzieren. Der Beitrag beleuchtet die häufigsten Gefahren und Schutzmassnahmen.

› Luca Orsini, Bernhard Fässler, Armin Burri

«Es gibt zwei Arten von Unternehmen: Die einen sind gehackt worden. Die anderen wissen es nur noch nicht.» Dies ist ein Zitat des früheren FBI-Direktors James Comey aus dem Jahr 2014 und könnte heute nicht aktueller sein. Zahlen des Bundesamts für Cybersicherheit (BACS) zeigen, dass bereits jedes dritte KMU in der Schweiz Opfer eines Cyberangriffs wurde. Trotzdem wird das Ausmass des Risikos, das ein solcher Angriff darstellt, häufig immer noch unterschätzt.

Kriminelle Motivation

Cyberangriffe zielen darauf ab, sich unbefugt Zugang zu Netzwerken, Computersystemen oder digitalen Geräten zu verschaffen, um sensible Daten zu stehlen, offenzulegen, zu manipulieren, zu deaktivieren oder zu zerstören. Kriminelle Motivation spielt hierbei eine zentrale Rolle: Angreifer handeln oft aus finanziellen Gründen, indem sie Gelder entwenden, Daten verkaufen oder Unternehmen durch Lösegeldforderungen erpressen.

Mit der zunehmenden Integration von künstlicher Intelligenz (KI) haben sich Cyberangriffe deutlich weiterentwickelt. KI erleichtert die Durchführung solcher Angriffe, indem sie diese schneller und professioneller gestaltet. Dies führt zu einer zunehmenden Bedrohungslage für KMU durch unterschiedliche Arten von Cybergefahren.

kurz & bündig

- Mit der zunehmenden Integration von künstlicher Intelligenz (KI) haben sich Cyberangriffe deutlich weiterentwickelt. KI erleichtert die Durchführung solcher Angriffe, indem sie diese schneller und professioneller gestaltet.
- Die Frage ist nicht ob, sondern wann ein Unternehmen von einem Cyberangriff betroffen sein wird. Präventive Massnahmen sind entscheidend, um Schäden zu minimieren und schnell wieder handlungsfähig zu sein.
- Ein gut durchdachter Notfallplan, regelmässige Mitarbeiterschulungen und technische Schutzmassnahmen sind der Schlüssel, um die Widerstandsfähigkeit eines Unternehmens zu stärken.

Häufigste Cybergefahren

Ransomware
Diese Schadsoftware blockiert den Zugriff auf Daten oder Systeme, bis ein Lösegeld gezahlt wird. Die Auswirkungen auf den Betriebsablauf können gravierend sein und hohe Kosten verursachen.

Datenabfluss und Spionage
Unbefugter Zugriff auf vertrauliche Daten kann zu erheblichen finanziellen Verlusten und einem Vertrauensverlust bei Kunden führen. Die Sicherung sensibler Daten hat daher oberste Priorität.

Phishing
Phishing-Angriffe zielen darauf ab, Benutzer zu täuschen und sie zur Preisgabe sensibler Informationen wie Passwörter oder Kreditkartendaten zu bringen. Diese Angriffe erfolgen meist über gefälschte E-Mails oder Websites.

Zero-Day-Lücken
Sicherheitslücken in Software, die den Entwicklern noch nicht bekannt sind, werden von Cyberkriminellen ausgenutzt, um unbemerkt in Systeme einzudringen.

Häufigste Ursachen

Mit der fortschreitenden Digitalisierung und dem Einsatz neuer Technologien entstehen immer neue Schwachstellen. In den letzten Jahren haben Grossunternehmen erheblich in ihre IT-Sicherheit investiert und ihre Sicherheitsmassnahmen verbessert.

Dadurch haben sich Cyberkriminelle zunehmend auf kleinere und mittlere Unternehmen (KMU) konzentriert, da diese oft nicht über die gleichen Ressourcen verfügen, um umfassende Sicherheitsvorkehrungen zu treffen.

Vor diesem Hintergrund ist es wichtig, die häufigsten Ursachen für Cybergefahren in KMU genauer zu betrachten.

Verlagerung der Arbeit ins Homeoffice
Die durch die Pandemie ausgelöste Verlagerung der Arbeit ins Homeoffice hat neue Herausforderungen und Risiken mit sich gebracht. Heimnetzwerke sind häufig weniger gut geschützt als Unternehmensnetzwerke, was zusätzliche Angriffsflächen bietet.

Cloud-Computing und zunehmende Virtualisierung
Die Nutzung von Cloud-Services birgt Risiken, insbesondere dann, wenn die gespeicherten Daten nicht ausreichend geschützt werden.

Stärkere Vernetzung mit dem Internet
Die zunehmende Vernetzung von Geräten, vor allem im industriellen Umfeld, erhöht das Risiko von Cyberangriffen. Viele industrielle Systeme sind nicht ausreichend abgesichert.

Technologische Innovationen
Neue Technologien, insbesondere im Bereich IoT, bringen neue Schwachstellen mit sich, die von Cyberkriminellen ausgenutzt werden.

Menschliches Verhalten
Viele Cyberrisiken entstehen durch menschliches Fehlverhalten. Phishing-Angriffe – die durch den Einsatz von KI zunehmend professioneller und schwerer zu erkennen sind – sowie unzureichende Schulungen führen oft dazu, dass Mitarbeitende unwissentlich zur Zielscheibe von Angriffen werden.

Schutzmassnahmen

Um sich wirksam gegen die zunehmenden Cybergefahren zu schützen, können KMU verschiedene präventive Massnahmen ergreifen. Die folgenden Ansätze bieten eine solide Grundlage, um Sicherheitslücken zu schliessen und die Resilienz gegenüber Angriffen zu stärken.

Inventare erstellen und regelmässige Back-ups durchführen
Die Erstellung eines vollständigen Inventars aller verwendeten Geräte und Software ist der erste Schritt, um das Unternehmen gegen Cybergefahren abzusichern. Nur wenn bekannt ist, welche Systeme und Daten geschützt werden müssen, können die richtigen Massnahmen ergriffen werden. Dieses Inventar sollte mindestens einmal jährlich überprüft und aktualisiert werden.

Zusätzlich ist ein systematisches Back-up-Management unerlässlich. Die 3-2-1-Back-up-Regel, wonach mindestens drei Kopien wichtiger Daten auf zwei unterschiedlichen Speichermedien abgelegt und eine Kopie extern gespeichert werden sollte, stellt eine solide Grundlage dar. Um die Funktionsfähigkeit der Back-ups sicherzustellen, sind regelmässige Wiederherstellungstests durchzuführen. Dies minimiert das Risiko, durch Ransomware oder ähnliche Angriffe kritische Daten zu verlieren.

Mitarbeitersensibilisierung
Mitarbeitende sind eine zentrale Verteidigungslinie gegen Cyberangriffe. Regelmässige Schulungen helfen, die Sensibilität für mögliche Bedrohungen zu schärfen und das Risiko menschlicher Fehler zu reduzieren.

Phishing-Angriffe, schwache Passwörter oder unachtsames Verhalten im Umgang mit Unternehmensdaten können durch gezielte Schulungen und Übungen deutlich verringert werden. Mitarbeitende sollten darin geschult werden, verdächtige E-Mails zu erkennen und sicherheitsbewusste Verhaltensweisen zu entwickeln.

Sichere Passwörter und Zwei-Faktor-Authentifizierung
Ein effektives Passwortmanagement ist entscheidend für die Sicherheit von IT-Systemen. Sichere Passwörter sollten mindestens zwölf Zeichen umfassen und Sonderzeichen, Zahlen sowie Gross- und Kleinbuchstaben enthalten. Mitarbeitende sollten zudem darauf hingewiesen werden, unterschiedliche Passwörter für verschiedene Systeme zu verwenden. Die Implementierung einer Zwei-Faktor-Authentifizierung (2FA) verstärkt den Schutz zusätzlich, indem eine zweite Verifizierungsebene hinzugefügt wird, zum Beispiel ein Code per SMS oder eine App-basierte Bestätigung.

Technische Sicherheitsmassnahmen umsetzen
Firewalls und Antivirenprogramme sind unerlässlich, um das Netzwerk und Endgeräte vor Malware und Angriffen zu schützen. Diese Systeme müssen regelmässig aktualisiert werden, um neue Bedrohungen abzuwehren. Unternehmen sollten sicherstellen, dass diese Sicherheitslösungen auf allen Endgeräten installiert und korrekt konfiguriert sind, um ein hohes Schutzniveau zu gewährleisten.

E-Mail-Sicherheit stärken
E-Mails bleiben eine der grössten Schwachstellen für Unternehmen. Durch regelmässige Sensibilisierung der Mitarbeitenden können Phishing-Angriffe und betrügerische Nachrichten frühzeitig erkannt werden.

Zusätzlich bieten Anti-Phishing-Software und strenge Filtermechanismen Schutz vor gefährlichen E-Mails, die darauf abzielen, Schadsoftware zu verbreiten oder vertrauliche Informationen zu stehlen.

Cyberversicherung abschliessen
Cyberversicherungen bieten zusätzlichen Schutz für Unternehmen, insbesondere im Falle von Cyberangriffen, die trotz technischer und organisatorischer Massnahmen erfolgreich sind.

Eine Cyberversicherung kann dabei helfen, finanzielle Verluste zu decken, die durch Angriffe entstehen, sowie die Kosten für die Wiederherstellung und Reaktion auf Vorfälle zu übernehmen. Ein besonders wichtiger Aspekt der Cyberversicherung ist die Entschädigung des Betriebsunterbruchs nach einer vertraglich definierten Karenzfrist. Diese Kostenkomponente stellt oft den grössten Anteil bei einem Cyber-Schaden dar und kann erhebliche finanzielle Belastungen für ein Unternehmen bedeuten.

Darüber hinaus vermitteln sie spezialisierte Partner für rechtliche Beratung, Forensik, Krisen- und Kommunikationsmanagement, um Vorfälle rasch und professionell zu bewältigen.

Sicherheitsverfahren auslagern
Viele KMU verfügen nicht über die internen Ressourcen, um umfassende Sicherheitslösungen zu implementieren und zu verwalten. In solchen Fällen kann es sinnvoll sein, Sicherheitsverfahren an spezialisierte Dienstleister auszulagern. Bei der Auswahl solcher Dienstleister sollten Unternehmen darauf achten, dass diese die erforderlichen Standards im Bereich Datenschutz und Sicherheit einhalten. Labels wie Cyber Seal, die speziell für KMU entwickelt wurden, bieten Orientierung. Dank solcher Labels oder Zertifizierungen kann man sich verge-

wissern, dass der ausgewählte Dienstleister die anerkannten Standards in den Bereichen Datenschutz und Sicherheit einhält und über das erforderliche Know-how verfügt.

Der Notfallplan für alle Fälle

Selbst bei der besten Vorbereitung auf Cyberangriffe ist es entscheidend, auf den Ernstfall vorbereitet zu sein. Wenn ein Cyberangriff im Gange ist, darf keine Zeit verloren werden – alle Beteiligten müssen genau wissen, welche Schritte zu unternehmen sind. Ein gut durchdachter Notfallplan ist hier unverzichtbar.

Dieser Plan sollte eine detaillierte Checkliste mit den wichtigsten Sofortmassnahmen, Zuständigkeiten und Kontaktdaten der relevanten IT-Verantwortlichen sowie externer Partner wie Versicherungen enthalten. Regelmässige Trainings und Simulationen stellen sicher, dass der Plan in der Praxis funktioniert und Schwachstellen frühzeitig erkannt werden.

Neben der technischen Seite sollten auch klare Kommunikationsstrategien definiert sein, um Mitarbeitende und Kunden rasch und transparent über den Vorfall und die ergriffenen Massnahmen zu informieren. Der Plan muss flexibel genug sein, um auf verschiedene Bedrohungsszenarien reagieren zu können, sei es ein Ransomware-Angriff, ein Hardware-Ausfall oder eine Datenschutzverletzung.

Die Frage ist nicht ob, sondern wann ein Unternehmen von einem Cyberangriff betroffen sein wird. Präventive Massnahmen sind entscheidend, um Schäden zu minimieren und schnell wieder handlungsfähig zu sein. Ein gut durchdachter Notfallplan, regelmässige Mitarbeiterschulungen und technische Schutzmassnahmen sind der Schlüssel, um die Widerstandsfähigkeit eines Unternehmens zu stärken. Nur wer vorbereitet ist, kann im Ernstfall schnell reagieren und die Auswirkungen eines Angriffs begrenzen. «

Quellenhinweis

- Masterarbeit «Cyber-Risk-Marktstrategie im Business Continuity und Incident Response Management für die Mobiliar» von Christoph Clavadetscher
- Expertengespräch mit Christoph Clavadetscher, Betriebswirtschafter Cyber-Risk bei der Mobiliar
- Bundesamt für Cybersicherheit (BACS)
- Marktstudie «Cyber Risk Management in grösseren Schweizer Unternehmen» von der Hochschule Luzern in Zusammenarbeit mit «die Mobiliar» und Economiesuisse.

Porträt

Luca Orsini
Leiter Verkauf,
die Mobiliar Generalagentur Willisau-Entlebuch

Armin Burri
Managing Director, Orgatent AG

Bernhard Fässler
CEO Esprit Netzwerk AG

Die Autoren sind Teilnehmer des Executive MBA der Hochschule Luzern – Wirtschaft.

Kontakt

luca.orsini@mobiliar.ch, www.mobiliar.ch
a.burri@orgatent.ch, www.orgatent.ch
bernhard.faessler@esprit-netzwerk.ch, www.esprit-netzwerk.ch