

Digitale Angriffe können weitreichende wirtschaftliche Folgen haben.

Cyberkriminellen einen Schritt voraus

Text **Tobias Ellenberger**
Bilder **Shutterstock**

Cyberangriffe auf KMU nehmen weiter zu. Wer grundlegende Sicherheitsmassnahmen konsequent umsetzt, Mitarbeitende sensibilisiert und neue Risiken wie KI frühzeitig berücksichtigt, stärkt seine Widerstandsfähigkeit entscheidend und kann im Ernstfall schneller reagieren.

Autor Tobias Ellenberger ist CEO und Vice Chairman der Oneconsult AG sowie Vizepräsident von Swiss Cyber Experts.

KMU sind heute nicht mehr bloss gelegentliche Nebenopfer digitaler Kriminalität, sondern ein festes Ziel professionell organisierter Angreifer. Wer unvorbereitet in einen Vorfall gerät, riskiert Betriebsunterbrüche, finanzielle Schäden, Reputationsverlust und im schlimmsten Fall eine längerfristige Handlungsunfähigkeit bis hin zum Konkurs.

Bezüglich Cyberattacken gibt es also keine Entspannung. Im Gegenteil: Die Situation hat sich und wird sich –

auch aufgrund des technologischen Fortschritts – verschärfen. Dabei gilt besonders für KMU: Es ist nicht notwendig, mit Grosskonzernen gleichzuziehen, sondern es ist erforderlich,die wichtigsten Risiken zu kennen, Prioritäten richtig zu setzen und dort gezielt zu investieren, wo die Wirkung am grössten ist.

Die Lage heute

Cyberangriffe auf grosse Unternehmen, aber auch auf KMU sind fast täglich in den Schlagzeilen. Insbesondere als Opfer von Betrugsversuchen oder sogenannter Ransomware sind viele KMU weiter in den Fokus von Angreifern gerückt, weil sie oft über wertvolle Daten und Zahlungsfähigkeit verfügen, gleichzeitig aber nur begrenzte personelle Ressourcen haben. Vielen KMU ist zudem nicht bewusst, wie wichtig sie für die Lieferketten grosser Unternehmen sind und dass daher ein erfolgreicher Angriff erheblichen Schaden weit über das eigene Unternehmen hinaus verursachen kann.

Die Bedrohungslage ist heute breiter und dynamischer. Laut der Studie «KMU Cybersicherheit 2025» von der Fachhochschule Nordwestschweiz sowie Firmen aus Wirtschaft, Forschung und Cybersicherheit sieht die grosse Mehrheit der Schweizer KMU Cyberkriminalität als ernst zu nehmendes Problem. Gleichzeitig fühlt sich nur noch ein kleiner Teil der Unternehmen ausreichend auf einen Angriff vorbereitet.

Zu den häufigsten Angriffsmethoden zählen weiterhin Schadsoftware, betrügerische E-Mails (Phishing) und der Missbrauch von Zugangsdaten. Besonders verbreitet sind sogenannte Ransomware-Angriffe. Dabei verschlüsseln Kriminelle nicht nur Daten, sondern kopieren diese zuvor auch. Anschliessend drohen sie mit einer Veröffentlichung der Informationen, um ihre Forderungen durchzusetzen.

Neue Qualität von Täuschung
Hinzu kommt eine neue Qualität von Täuschung: Mithilfe generativer KI lassen sich E-Mails sprachlich sauber formulieren, Stimmen imitieren und Nachrichten täuschend echt personalisieren. Gerade in KMU mit kurzen Wegen und pragmatischen Prozessen steigt dadurch das Risiko, dass gefälschte Zahlungsanweisungen, Support-Anfragen oder vermeintliche Nachrichten der Geschäftsleitung nicht rechtzeitig erkannt werden.

Ein Cybervorfall trifft kleine Unternehmen häufig besonders hart. Wenn die zentrale Software zur Steuerung und Verwaltung aller Geschäftsprozesse eines Unternehmens ausfallen oder Kundendaten nicht mehr verfügbar sind, gerät der Betrieb rasch ins Stocken oder kommt im schlimmsten Fall vorübergehend zum Stillstand.

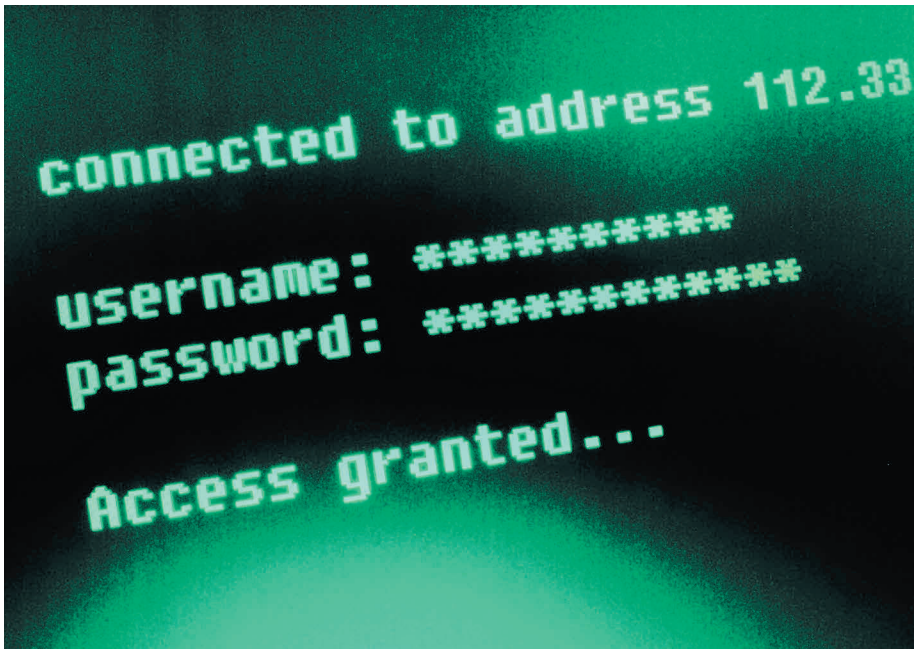
Gleichzeitig entstehen zusätzliche Kosten, etwa für die Wiederherstellung der Systeme, die Unterstützung durch externe Spezialisten, die Information von Kunden oder notwendige rechtliche Abklärungen.

Warum Vorbereitung entscheidet
Viele Cyberangriffe sind nicht nur wegen technischer Schwächen erfolgreich, sondern vor allem auch, weil Unternehmen nicht ausreichend darauf vorbereitet sind. Fehlen klare Zuständigkeiten, Informationen zu kritischen Systemen, Notfallpläne oder wichtige externe Ansprechpartner, geht im Ernstfall wertvolle Zeit verloren.

Deshalb ist Prävention nach wie vor die wirksamste Form der Absicherung. Sie bedeutet allerdings nicht, einmalig Massnahmen umzusetzen und das Thema anschliessend abzu-

Cybersicherheit-Services

Die Oneconsult Unternehmensgruppe mit Hauptsitz in Zürich und Niederlassungen in Bern, München (D) und Auckland (NZ) bietet verschiedene Dienstleistungen im Bereich Cybersicherheit an, darunter Beratungsservices und simulierte Hackerangriffe als Tests. Die Firma begleitet regelmässig Unternehmen bei der Bewältigung von Ransomware und vergleichbaren Angriffen.



haken. Sicherheit ist vielmehr ein laufender Prozess aus Aktualisieren, Überprüfen, Schulen, Verbessern und Üben.

Die meisten KMU arbeiten heute mit IT-Dienstleistern, Cloud-Plattformen und spezialisierten Software-Anbietern zusammen. Das ist sinnvoll, entbindet die Geschäftsleitung jedoch nicht von der Verantwortung. Wer Leistungen auslagert, lagert das Angriffsrisiko nicht automatisch mit aus.

KMU sollten deshalb mit ihren Dienstleistern regelmässig besprechen,

- welche Schutzmassnahmen umgesetzt sind,
- welche Systeme besonders kritisch sind,
- wie rasch Sicherheitsupdates eingespielt werden können,
- was im Notfall konkret geschieht.

Bereits bei der Auswahl von Cloud- und SaaS-Lösungen sowie während der laufenden Nutzung müssen Fragen zu Sicherheit, Datenspeicherung, Zugriffsrechten, Protokollierung und Wiederherstellung zwingend berücksichtigt und regelmässig mit dem Anbieter besprochen werden.

Cybersicherheit ist heute ein unverzichtbarer Teil solider Unternehmensführung.

Neue Risiken durch KI

Künstliche Intelligenz ist für KMU gleichzeitig Chance und Risiko. Sie kann Prozesse beschleunigen, Texte verfassen, den Support verbessern oder Analysen erleichtern. Dieselben Werkzeuge helfen jedoch auch Angreifern, glaubwürdige Phishing-Kampagnen zu automatisieren, Informationen über Zielpersonen zusammenzutragen und Angriffe präziser auf das Zielunternehmen zuzuschneiden.

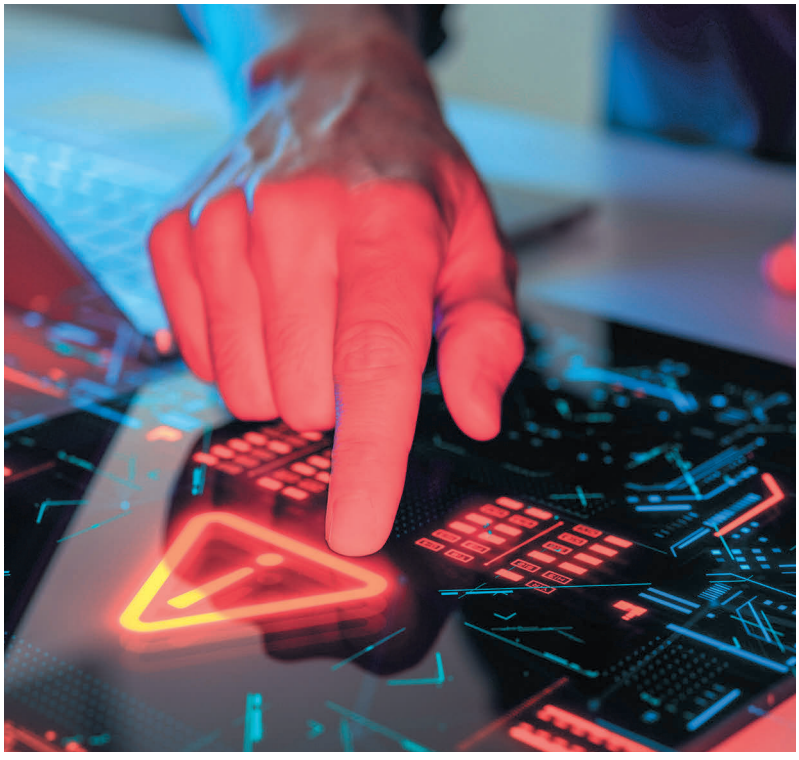
Zusätzlich entsteht ein internes Risiko: Mitarbeitende geben unter Umständen vertrauliche Informationen in öffentliche KI-Dienste ein, ohne sich der Folgen bewusst zu sein. Werden Angebote, Verträge, Kundendaten, Quellcode oder interne Strategiepapiere unkontrolliert in externe Werkzeuge kopiert, können Datenschutz- und Geheimhaltungsprobleme sowie Verstösse gegen gesetzliche und interne Vorgaben entstehen.

KMU brauchen deshalb keine komplizierte KI-Strategie, wohl aber klare Spielregeln. Dazu gehören Vorgaben, welche Daten in KI-Tools eingegeben werden dürfen, welche Anwendungen freigegeben sind, wie Ergebnisse geprüft werden und wann eine menschliche Freigabe zwingend erforderlich ist. KI sollte produktiver machen, nicht neue Einfallstore für Cyberkriminalität schaffen.

Sicherheit mit Augenmass

Nicht jedes KMU kann ein eigenes Security-Team aufbauen, und nicht jede Massnahme muss sofort perfekt umgesetzt werden. Entscheidend ist, das verfügbare Budget dort einzusetzen, wo es das Risiko am stärksten senkt: beim Aktualisieren von Systemen und Geräten, beim Absichern von Identitäten, bei Back-ups, Berechtigungen und klaren Abläufen.

Ebenso wichtig ist eine realistische Einschätzung der eigenen Widerstandsfähigkeit. Absolute Sicherheit gibt es nicht. Wer aber die wahrscheinlichsten Angriffswege schliesst, Mitarbeitende einbindet, Dienstleister kritisch prüft und neue KI-Risiken berücksichtigt, reduziert die Eintrittswahrscheinlichkeit eines Cyberangriffs deutlich und kann im Ernstfall schneller handeln. Vereinfacht gesagt: Wer nicht zu den am schlechtesten geschützten KMU gehört, wird selten zum ersten Ziel.



KMU stehen zunehmend im Fokus professioneller Cyberkriminalität.

Das Fazit

Cybersicherheit gehört heute zu einer soliden Unternehmensführung. KMU sollten sich daher frühzeitig mit dem Thema befassen und bei Bedarf fachkundige Unterstützung beiziehen. /