

Publiziert am: 07.06.2024



Der Schlüssel zur Cyber-Resilienz

CYBER RISK – Cyber-Vorfälle gehören seit Jahren zu den Top-Geschäftsrisiken und nehmen stetig zu – und Schweizer KMU bleiben von dieser Entwicklung nicht verschont. Eine solide IT-Infrastruktur ist für die Cyber-Sicherheit notwendig, und eine Cyber-Versicherung kann die Effekte eines Angriffs signifikant mindern. Auch Mitarbeitende spielen für die Cyber-Sicherheit eine immer wichtigere Rolle.



Das Risikoverhalten der Mitarbeiter im Cyberbereich beeinflusst auch die Versicherungsprämien der Unternehmen. Wichtig sind eine persönliche Ansprache und eine regelmässige Kommunikation. Bild: 123RF

Das Verhalten der Mitarbeitenden beeinflusst die Sicherheit des Unternehmens auf zwei Arten. Erstens bietet es einen Schutz gegen die Angriffe selbst. Die Mehrheit der Angriffe startet durch Phishing. Wenn die Mitarbeitenden nicht Opfer von Phishing-Versuchen werden, ist das Unternehmen besser geschützt. Zweitens können Mitarbeitende die negativen Folgen eines Cyber-Angriffs mindern, indem sie mithelfen, den Geschäftsbetrieb aufrechtzuerhalten. Besonders wichtig dabei ist es, die bei den Kunden aufgetretenen Probleme zu lösen. Schutz und Minderung sind zwei Kernkomponenten der Cyber-Resilienz.

Faktor Mensch im Vordergrund

Versicherungen beobachten die Entwicklung am Markt und passen ihre Deckungen und Prämien stetig an. In den letzten Jahren stand vor allem die IT-Infrastruktur im Fokus von neuen Underwriting-Richtlinien. Allerdings rückt der Faktor Mensch mehr in den Vordergrund, und die Prämie wird zunehmend durch eine Einschätzung des Risikoverhaltens der Mitarbeitenden

beeinflusst. Mit der Pflege eines angemessenen Risikoverhaltens können Unternehmen gleichzeitig ihre Cyber-Resilienz steigern, und der Entwicklung der Versicherungsprämie Einhalt gebieten.

Die Frage ist jedoch: Wie kann ein KMU seine Mitarbeitenden am wirksamsten für die Unternehmenssicherheit sensibilisieren? Zeit und finanzielle Ressourcen sind knapp, und Cyber-Risiken haben oft keinen direkten Bezug zum Tagesgeschäft. Welche Themen sind also besonders wichtig, und wie platzieren Führungskräfte diese am besten bei den Mitarbeitenden?

Die persönliche Einstellung zählt – und kann beeinflusst werden

Die Ergebnisse eines aktuellen Forschungsprojekts des Instituts für Finanzdienstleitungen Zug IFZ der Hochschule Luzern zeigen, dass bestimmte Einstellungen der Mitarbeitenden gegenüber Cyber-Risiken besonders relevant sind. Die drei wichtigsten, die von den Unternehmen, insbesondere KMU, gepflegt werden sollen, sind:

Ich (Mitarbeitender) besitze wichtige Informationen. Das sind z. B. Kundendaten oder Zugang zum Zahlungsverkehr. Diese Informationen und Prozesse sollen geschützt werden.

Ich (Mitarbeitender) habe eine Verantwortung, die Firma zu schützen. Hier geht es um die Einstellung, nicht um eine rechtliche Aussage.

Ich (Mitarbeitender) kann und soll etwas unternehmen. In einer Sondersituation möchten die Mitarbeitenden sich mehr und flexibel einsetzen und z. B. sicherstellen, dass die Kunden ihre letzte Bestellung trotz Systemausfall rechtzeitig erhalten.

Um diese Einstellungen zu beeinflussen, ist es essenziell, sie richtig anzusprechen. Dazu muss ein Bezug zu einzelnen Personen hergestellt und deren Einfluss auf die Cyber-Resilienz aufgezeigt werden. Dies geschieht am besten mit konkreten Beispielen: Alina kann Überweisungen freigeben, also soll sie sich absichern, bevor sie das tut, vor allem bei aussergewöhnlichen Anweisungen. Frank hält Kontakt zu einem Kundensegment. Wie kann er im Falle eines Systemabsturzes weiterhin mit den Kunden in Verbindung bleiben? Vielleicht muss er sein eigenes Smartphone und eine gedruckte Liste verwenden.

Regelmässig kommunizieren

Die drei genannten Punkte sind so zentral, dass auch eine Sensibilisierung mit relativ simplen Massnahmen zu mehr Sicherheit führen kann. Wichtig dabei ist die Regelmässigkeit der Kommunikation. Damit kann ein Unternehmen resilienter gestaltet und gleichzeitig die Versicherungsdeckung optimiert werden.

Carlo Pugnetti, Stefan Hunziker (Hochschule Luzern) und Carlos Casián (Kessler & Co AG)