

28.01.2021 - 11:00 Uhr

Studie ZHAW und Allianz Suisse / Cybersicherheit in KMU: Mitarbeitende sind der entscheidende Schlüssel zum Erfolg

Wallisellen (ots) -

Mitarbeitende in Schweizer KMU unterschätzen die Gefahr von Cyberattacken für das eigene Unternehmen. Um Risiken zu senken, braucht es Sensibilisierungsmassnahmen und die Vorbereitung von Notfallszenarien. Das zeigt eine aktuelle Studie der ZHAW und von Allianz Suisse.

Die Einstellung ihrer Mitarbeitenden gegenüber Cyberattacken macht kleine und mittlere Unternehmen in der Schweiz verwundbar: Zwar sind sie sich der allgemeinen Risiken von Cyberkriminalität und des grossen Schadenpotenzials eines Angriffs bewusst. Allerdings schätzen sie ihr eigenes Unternehmen und sich selbst nicht als wichtig genug ein, um ein lohnendes Ziel darzustellen. Diese Haltung kann Mitarbeitende dazu verleiten, nicht genügend wachsam zu sein. Zu diesen Resultaten kommt eine Studie der ZHAW School of Management and Law in Zusammenarbeit mit Allianz Suisse. Die Forschenden haben dafür vertiefte Interviews mit Mitarbeitenden aus ausgewählten KMU geführt, um ihre Haltungen und die Treiber von Entscheidungen zu verstehen, die hinsichtlich Cyberrisiken getroffen werden.

Aktuell verbreitetes Homeoffice verstärkt Risiken

"Cyberkriminelle zielen in der Regel auf Menschen und versuchen über sie eine Schadsoftware in das Unternehmenssystem einzuschleusen oder an Passwörter zu gelangen. Die Einstellung und das Verhalten der Mitarbeitenden sind daher entscheidend für die Abwehr von Angriffen", erklärt Carlos Casián, Co-Autor der Studie und Underwriter Sach / Cyber Risk bei Allianz Suisse. "Gerade in der heutigen Zeit, in der viele Mitarbeitende von zu Hause aus arbeiten, steigen die Risiken: Einerseits spielen technische Aspekte wie externe Zugriffe auf das Unternehmensnetzwerk eine Rolle. Andererseits ist der Ad-hoc-Austausch mit Kolleginnen und Kollegen über verdächtige E-Mails schwieriger, was Mitarbeitende anfälliger für Manipulationsversuche macht." Gemäss der Studie assoziieren KMU-Mitarbeitende Cyberattacken primär mit geopolitischen Konfrontationen, Terrorismus oder dem organisierten Verbrechen. Die Schweiz hingegen sehen sie als Sphäre, die im Vergleich deutlich sicherer sei. "Das ist jedoch ein Trugschluss. Auch hierzulande waren rund ein Drittel der KMU schon Angriffen ausgesetzt", sagt Studienleiter Carlo Pugnetti, Dozent an der ZHAW School of Management and Law.

Cyberattacken nur als Problem für Spezialistinnen und Spezialisten wahrgenommen

Bei der Erkennung einer konkreten Attacke auf das eigene Unternehmen und der Reaktion darauf fühlen sich die befragten KMU-Mitarbeitenden relativ hilflos. Sie gehen in einem solchen Fall jedoch davon aus, dass Spezialistinnen und Spezialisten helfen würden. Diese Annahme kann eine gewisse Passivität fördern und Mitarbeitende dazu verleiten, die eigene Rolle bei der Minimierung von Cyberrisiken zu unterschätzen. Gleichzeitig zeigen die Studienresultate, dass KMU über eine Unternehmenskultur mit stark ausgeprägter Lösungsorientierung verfügen. Die Mitarbeitenden agieren entsprechend meist proaktiv und würden in einem konkreten Schadensfall bei dessen Bewältigung mithelfen wollen.

Um die Risiken und Auswirkung einer Cyberattacke zu reduzieren, geben die Autoren der Untersuchung eine Reihe von Empfehlungen: Diese umfassen unter anderem Informationsmassnahmen innerhalb der KMU, die Mitarbeitende für die objektive Bedrohung sensibilisieren und ihnen aufzeigen, wie sie zu deren Abwehr beitragen können. Weiter sollten die Unternehmen Strategien erarbeiten, um allfällige Attacken und damit verbundene Ausfälle von IT-Systemen zu bewältigen und diese Szenarien trainieren. Bei der Entwicklung entsprechender Lösungsstrategien sollten die Firmen ihre Mitarbeitenden aktiv einbeziehen und deren engagierte Arbeitshaltung nutzen.

Spezielle Methodik

Die Studie "Cyberrisiken und Schweizer KMU - Eine Untersuchung der Einstellungen von Mitarbeitenden und verhaltensbedingter Anfälligkeiten" durchgeführt hat das Institut für Risk & Insurance der ZHAW School of Management and Law in Zusammenarbeit mit Allianz Suisse und mit Unterstützung von verschiedenen Partnern. Die Forschenden führten in drei ausgewählten KMU aus der Wärme- und Fertigungsbranche vertiefte Interviews mit 17 Mitarbeitenden verschiedener Funktionen. Dafür nutzten sie die sogenannte "Tiefen-Metapher-Interviewtechnik", bei der die Befragten Bilder auswählten, die ihre Vorstellungen und Haltungen gegenüber verschiedenen Aspekten der Cyberkriminalität zum Ausdruck bringen. "Dank dieser Methodik konnten wir auch persönliche Einstellungsmuster identifizieren, die den befragten Personen selbst nicht unmittelbar bewusst sind", erklärt Carlo Pugnetti. "Der Fokus lag entsprechend darauf, verborgene Erkenntnisse an die Oberfläche zu bringen und dadurch wirkungsvollere Massnahmen zu entwickeln." Die Gespräche fanden im September 2020 statt.

Pressekontakt:

Carlo Pugnetti, ZHAW School of Management and Law, Institut für Risk & Insurance
Telefon 058 934 66 41, E-Mail: carlo.pugnetti@zhaw.ch

Carlos Casián, Allianz Suisse, Telefon 058 358 77 51, E-Mail: carlos.casian@allianz-suisse.ch

Bernd de Wall, Allianz Suisse, Telefon 058 358 84 14; E-Mail: bernd.dewall@allianz.ch

Diese Meldung kann unter <https://www.presseportal.ch/de/pm/100008591/100864121> abgerufen werden.