KMU und Cybersicherheit: Es geht vorwärts, doch Lücken bleiben

Vor allem mit technischen Massnahmen schützen sich KMU vor Cyberattacken. Aber genau dort, wo Hacker am häufigsten angreifen, tut sich noch zu wenig. Zwei Studien zeigen Entwicklungen und Hintergründe dazu auf.

Von Martina Schäfer

Immer mehr Schweizer KMU werden von Cyberkriminellen angegriffen. Das merken auch Cyberversicherer wie die Mobiliar. Eine repräsentative Befragung von über 500 KMU bestätigt: 2021 wurde schon ein Drittel von ihnen mindestens einmal Opfer eines Cyberangriffs. Im Vorjahr war es erst ein Viertel. Die Studie «Homeoffice und Cybersicherheit in Schweizer KMU» erschien Ende November 2021.

Technische Massnahmen im Vordergrund

Die Studie zeigt: Cyberattacken werden häufiger, aber das Gefahrenbewusstsein der KMU nimmt im Vergleich nur leicht zu. Doch je besser die Befragten zum Thema Cyberrisiko informiert sind und je bewusster ihnen die Bedrohung ist, desto mehr setzen sie Schutzmassnahmen um. Technische Massnahmen werden besonders oft ergriffen, während organisatorische noch vernachlässigt werden. Gerade dort, wo Internetkriminelle am häufigsten angreifen – bei den Mitarbeitenden – harzt es mit der Planung und Umsetzung von Cyberschutzmassnahmen. Eine Verhaltensstudie, die von der Universität Bern und effex AG im Auftrag der Mobiliar durchgeführt wurde, untersuchte die Gründe dafür (mehr dazu im Interview mit Claude Messner auf der rechten Seite).

Ein vielfältiges, dynamisches Risiko

Viele KMU sind der Meinung, dass einmalige Cyberschutzmassnahmen genügen. Aber Cybersicherheit im Unternehmen ist eine permanente Aufgabe: Zum Beispiel tauchen neue Schwachstellen auf oder ehemalige Mitarbeitende haben noch Zugriff auf die Firmensysteme. Erst technische Massnahmen plus organisatorische Massnahmen plus sichere Prozesse ergeben ein gutes Cyberschutzkonzept. Was sind geeignete Massnahmen, um auch nicht-technische Cyberrisiken zu senken? Am wichtigsten ist die regelmässige Sensibilisierung der Mitarbeitenden. Es reicht eine unachtsame oder

FÜNF FRAGEN AN SIMON SEEBECK, EXPERTE FÜR CYBERSCHÄDEN BEI DER MOBILIAR

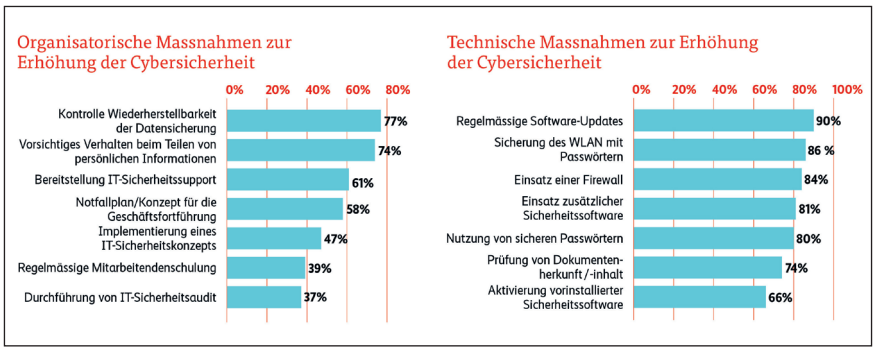
Wie lange dauert es, bis ein Betrieb nach einer Cyberattacke wieder arbeiten kann?
Gibt es ein vollständiges Backup, dauert es im Schnitt einen Tag bis zwei Tage. Danach kann es noch ein bis zwei Wochen Einschränkungen geben. Falls es kein Back-up gibt, geht für längere Zeit nichts mehr.

Lösegeld zahlen oder nicht?
Nicht zahlen. Denn nicht jeder Angreifer ist in der Lage, die Daten wiederherzustellen oder bereit, es nach der Zahlung überhaupt zu tun. Dann zahlt man ein zweites Mal. Ausserdem: Wer einmal erfolgreich erpresst wurde, wird in Zukunft erneut zum Opfer.

Was sollte ein Unternehmen bei einer Cyberattacke als Erstes tun?
Bei einem Angriff mit Erpressersoftware müssen sofort die Rechner vom Netz und das System heruntergefahren werden. Wenn man einem Online-Betrüger auf den Leim gegangen ist, sollte man die Bank kontaktieren und die Transaktionen stoppen. In jedem Fall ist es sinnvoll, mit dem IT-Dienstleister Kontakt aufzunehmen.

Wie werden die Betroffenen im Schadenfall von der Mobiliar unterstützt?
Wir kommen für die Kosten auf wie z.B. für die Wiederherstellung von Daten und Systemen. Ausserdem unterstützen unsere IT-Sicherheitspartner bei der Wiederinbetriebnahme der Systeme mit einer Zweitmeinung.

Soll ich einen Cyberangriff der Polizei melden?
Ja, wir empfehlen eine Meldung bei der Polizei und beim Nationalen Zentrum für Cybersicherheit.



Wie sich KMU vor Cyberattacken schützen – bei den organisatorischen Massnahmen besteht am meisten Handlungsbedarf.

«VERANTWORTLICH SIND IMMER DIE ANDEREN»

Claude Messner ist Professor für Consumer Behavior an der Universität Bern. Gemeinsam mit der Marketing- & Unternehmensberatung effex haben er und sein Team letztes Jahr untersucht, warum sich KMU nicht besser vor Cyberangriffen schützen.

Claude Messner, schon ein Drittel aller KMU wurde Opfer einer Cyberattacke. Sind sich die KMU der Gefahr nicht bewusst?
Die Entscheiderinnen und Entscheider, die wir interviewt haben, kennen das Problem durchaus. Bei den Mitarbeitenden hingegen sieht es anders aus. Die meisten wissen nicht, dass das Einfallstor bei 70 Prozent der Cyberattacken die Mitarbeitenden sind. Sie sehen den Cyberschutz vor allem als technisches Problem, das die IT-Verantwortlichen betrifft und wiegen sich selbst in Sicherheit, auch aufgrund falscher Vorstellungen wie Cyberattacken funktionieren. Zum Beispiel wird unterschätzt, wie täuschend echt Phishing-Mails sein können. Ausserdem ist die Meinung stark verbreitet, dass Cyberattacken nur die anderen treffen, weil man selber viel zu unwichtig sei. Was natürlich nicht stimmt.

Aber wenn die Vorgesetzten die Gefahr grundsätzlich kennen, warum werden dann nicht umfassendere Massnahmen ergriffen?
Das Hauptproblem ist Verantwortungsdiffusion, das hat die Studie erstaunlich deutlich gezeigt. Das bedeutet konkret, die KMU schieben das Thema Cyberschutz den IT-Verantwortlichen zu. Diese setzen dann technische Massnahmen um wie Firewalls, Back-ups oder Passwort-Mindestanforderungen. Sie wissen zwar, dass die Mitarbeitenden die grösste Sicherheitslücke sind, aber sehen dort die KMU-Führung in der Verantwortung. Dessen sind sich die KMU meist gar nicht bewusst. Was herauskommt ist, dass dort, wo das Angriffsrisiko für Cyberattacken am grössten ist – bei den Mitarbeitenden – nichts getan wird, weil sich keiner zuständig fühlt.

Wie können KMU dieses Problem lösen?
Zum einen sollte Cyberschutz Chefsache sein und im Unternehmen permanent auf dem Tisch bleiben. Zum anderen geht es um gute Beratung und externe Anbieter. Ein möglicher Weg ist es, sich zusätzlich zum IT-Dienstleister einen unabhängigen Partner zu suchen, der die Gesamtsicht auf das Thema Cyberschutz einnimmt, Sicherheitslücken und Lösungen aufzeigt und allenfalls auch die Sensibilisierung der Mitarbeitenden übernimmt. Oder der IT-Dienstleister nimmt das Thema ins Portefeuille auf und kümmert sich selbst darum.

Welche Möglichkeiten gibt es, Mitarbeitende zum richtigen Verhalten zu bewegen?
Es gibt Unternehmen, die verteilen gedruckte Richtlinien oder führen Schulungen durch. Attraktiver wird das Thema Cyberschutz, wenn es interaktiv wird, zum Beispiel mit simulierten Attacken. Oder wenn es sogar einen spielerischen Charakter bekommt wie in Cyber Escape Rooms, in denen man selbst in die Rolle eines Hackers schlüpft. Aber wir alle haben die Tendenz, Unangenehmes von uns weg zu schieben. Zum Beispiel sind lange Passwörter zwar sicher, aber ich kann sie mir nicht merken. Oder jedes Mal die Frage, ob ich nun auf einen Link im Mail klicken soll. All das ist mühsam und hindert mich am effizienten Arbeiten. Deshalb spielt auch die Unternehmenskultur eine grosse Rolle, die sicheres Verhalten unterstützen und fördern kann.

unwissende Person, die ihre Daten am falschen Ort eingibt, und das Unglück ist geschehen.

Bereit im Falle eines Angriffs

Eine weitere wichtige Massnahme ist ein vollständiges Inventar der IT-Infrastruktur. Oft wissen Unternehmen nicht, was ihre Hard- und Software alles umfasst und ob die ganze IT-Infrastruktur konsequent gewartet wird. Solche Inventare werden zum Beispiel vom Cyber Red-Box-Schwachstellen-Scan der Mobiliar automatisch erstellt. Besonders für den Fall eines Angriffs sind auch klare Zuständigkeiten und Abläufe elementar. Denn ist die Cyberattacke im Gang und sind die Systeme blockiert, ist es zu spät, um ein Notfallkonzept zu entwickeln. Es muss vorher definiert werden, wie im Krisenfall das Geschäft weitergeführt werden soll. Eine umfassende Vorbereitung hilft, schnell wieder handlungsfähig zu sein.

Unterstützung holen

Trotz aller Vorsicht: Weil sich Cyberrisiken schnell verändern, kann eine Attacke nie ganz ausgeschlossen werden. Dann steht einem Unternehmen der IT-Dienstleister bei. Und die Cyberversicherung: Zumindest der finanzielle Schaden wird damit in Grenzen gehalten.

Die inhaltliche Verantwortung für den Artikel liegt bei der Schweizerischen Mobiliar Versicherungsgesellschaft AG.

MEHR INFORMATIONEN

- «Homeoffice und Cybersicherheit in Schweizer KMU», durchgeführt von digitalswitzerland, der Fachhochschule Nordwestschweiz, der Schweizerischen Akademie der Technischen Wissenschaften, gfs-zürich und der Mobiliar, 2021
- Verhaltensstudie «Cyberrisiken durch das Verhalten von Mitarbeitenden in KMU langfristig minimieren», durchgeführt vom Institut für Marketing und Unternehmensführung der Universität Bern und effex AG, 2021

Zusammenfassungen der beiden Studien finden Sie auf www.mobiliar.ch/kmu