Cybersecurity lohnt sich

Cyber-Bedrohungslage setzt Österreichs Unternehmen zunehmend unter Druck

Die Cyber-Bedrohungslage hat sich in den vergangenen Monaten zugespitzt. Wie eine aktuelle Deloitte Studie zeigt, ist nicht nur die Zahl der Attacken stark angestiegen, die Angreifenden agieren auch immer professioneller. Dennoch schätzt ein Großteil der Betriebe seine Daten und IT-Systeme als sicher ein – auch weil in der Vergangenheit viel in Cyber Security investiert wurde. Doch Unternehmen müssen aufpassen, sich angesichts der steigenden Anforderungen nicht in falscher Sicherheit zu wiegen. Das könnte nämlich fatale Folgen haben.

Deloitte erhebt jährlich mit dem Forschungsinstitut Foresight den Status quo österreichischer Betriebe zum Thema Cyber Security. Für den aktuellen Report wurden kürzlich rund 350 Mittel- und Großunternehmen im ganzen Land befragt. Die Umfrage zeigt, dass Österreichs Wirtschaft in den vergangenen Jahren viel in Cyber Security investiert hat. Doch die Gefahren sind – auch aufgrund aktueller globaler und technischer Entwicklungen – alles andere als gebannt.

„Wir führen mittels persönlicher telefonischer Interviews mit Führungskräften die größte repräsentative Umfrage zu Cyber-Sicherheit in Österreich durch. Dadurch bekommen wir ein aussagekräftiges Bild über die Lage im Land. Das beunruhigende Ergebnis macht deutlich, dass sich die Bedrohungslage in jüngster Zeit spürbar verschärft hat“, hält Christoph Hofinger, Geschäftsführer von Foresight, fest.

In konkreten Zahlen bedeutet das: Nahezu ein Drittel (28 %) der österreichischen Unternehmen berichtet aktuell von beinahe täglichen Ransomware-Angriffen. Das sind doppelt so viele wie noch 2024. „Zwei Drittel (66 %) können zudem nicht ausschließen, dass es aufgrund eines Cyber-Angriffes zu einem totalen Stillstand ihres Betriebes kommt. Das gefährdet nicht nur die finanzielle Stabilität des Unternehmens, sondern auch Arbeitsplätze. Und die Sicherheit von Kundinnen und Kunden steht dabei ebenfalls auf dem Spiel“, betont Karin Mair, Managing Partnerin für die Bereiche Technology & Transformation sowie Strategy, Risk & Transactions bei Deloitte Österreich. „Um die Gefahren zu minimieren, ist ein funktionierendes Business Continuity Management (BCM) mit durchdachten Notfallplänen, klar definierten Verantwortlichkeiten sowie regelmäßigen Übungen unabdingbar.“

Christoph Hofinger, Geschäftsführer von Foresight.
Bild: Mat Stefanic/Studio-matphoto

SICHERHEITSBUDGETS STAGNIEREN

Ein funktionierendes BCM gewinnt auch deshalb an Bedeutung, weil die Angreifenden immer professioneller agieren. Zwar können mittlerweile 80 % der Unternehmen Attacken mittels technischer Infrastrukturmaßnahmen eindämmen, doch das Wiederherstellen mittels Backups (40 %) sowie die Entschlüsselung der Daten (23 %) bei erfolgreichem Angriff gelingen immer seltener. Obwohl diese Entwicklung Unternehmen zunehmend in Alarmbereitschaft versetzen sollte, hält die Mehrheit an ihren bereits gesetzten Sicherheitsbudgets fest.

„60 % der Befragten wollen ihre Ausgaben für Technik und Prozesse in der Cyber Security auf dem Niveau des letzten Jahres halten. Über zwei Drittel (69 %) planen die Personalaufwendungen am Stand von 2025 zu belassen“, weiß Karin Mair. „Denn eines ist klar: Wer auch morgen gut aufgestellt bleiben will, muss Budgets entsprechend anpassen. Investitionen in Cyber Security sind ein Muss.“

Die Zurückhaltung bei der Ressourcenaufstockung liegt auch daran, dass die Unternehmen der Sicherheit ihrer Daten und IT-Systeme zu stark vertrauen. 86 % schätzen diese als sehr oder ziemlich sicher ein, 13 % bewerten sie sogar als absolut sicher.

UMSETZUNG ZENTRALER RICHTLINIEN GILT NICHT ALS OBERSTE PRIORITÄT

Investitionen sind auch notwendig, um die anstehenden Fristen bei zentralen Vorgaben wie der NIS II oder dem EU AI Act einzuhalten. Derzeit herrscht allerdings unter den Unternehmen noch große Unsicherheit, ob und in welchem Umfang die neuen europäischen Regulierungen die eigene Organisation überhaupt betreffen. Hinsichtlich NIS II, die am 1. Oktober 2026 in Kraft tritt, haben erst 23 % der Betroffenen ihre Vorbereitungen abgeschlossen. 16 % planen die Umsetzung in naher Zukunft und 9 % haben noch keine konkreten Pläne dazu.

„Unsere Erfahrung aus der Beratung zeigt: Die Umsetzung solcher Richtlinien dauert nicht Monate, sondern Jahre. Mit Blick auf die nahenden Verpflichtungen bleibt Unternehmen also kaum noch Zeit zu handeln“, warnt Georg Schwondra. „Doch nicht nur die Wirtschaft steht in der Verantwortung – auch der Gesetzgeber muss Tempo machen. Es braucht klare Rahmenbedingungen und gezielte Aufklärung, damit Unternehmen endlich die Planungssicherheit erhalten, die sie benötigen.“

www.deloitte.com