

Immer häufiger auch in Österreich auftretende Cyberangriffe sowie eine rasant fortschreitende Digitalisierung aufgrund der Covid-19-Pandemie haben die IT-Sicherheit im letzten Jahr so stark wie nie zuvor in den Fokus der heimischen Wirtschaft gerückt. Rund sieben von zehn österreichischen Unternehmen (73%) planen daher für das Jahr 2022 einen wesentlichen Anstieg ihrer Investitionen im Bereich Cybersecurity; die Hälfte der Unternehmen (50%) kalkuliert dabei sogar eine Erhöhung der Budgets von mehr als zehn Prozent zum Vorjahr ein und liegt damit weit über dem globalen Durchschnitt (26%).

Das zeigen die für Österreich geltenden Ergebnisse der „Global Digital Trust Insights Survey 2022“ von PwC, für die weltweit mehr als 3.600 CEOs und Führungskräfte qualitativ befragt wurden.

Diesem neuen Verständnis für die Bedeutung und Notwendigkeit von IT-Sicherheit steht in Österreich jedoch eine grobe Unwissenheit über die entscheidenden Schutzmaßnahmen sowie die größten Cyberrisiken gegenüber. Allen voran mögliche Bedrohungen durch Dritte, die zu häufig durch die Komplexität und Vernetzung von Partner- und Lieferantenbeziehungen verdeckt werden.

Blinder Fleck der Cyberrisiken

„Die Entwicklungen in den letzten Jahren haben die Bedeutung der IT-Sicherheit ins Rampenlicht gerückt. Doch man kann nicht schützen, was man nicht kennt. So haben viele österreichische Unternehmen enorme Schwierigkeiten dabei, ihre Risiken durch Dritte – wie Lieferanten – im eigenen Umfeld zu erkennen“, erklärt Georg Beham, Cybersecurity & Privacy Leader

bei PwC Österreich, und führt aus: „Gerade die Vorfälle der jüngeren Vergangenheit haben gezeigt, dass potenzielle Angreifer immer das schwächste Glied in der (Liefer-)Kette auswählen, um das Unternehmen lahmzulegen. Bei einer fehlenden Einbindung von Dienstleistern in die eigene Risikobetrachtung werden diese Risiken zumeist falsch oder gar nicht bewertet.“



© AP/WideWorld/Alamy

So gaben nur 35% der befragten heimischen Unternehmen an, dass sie das Risiko von Datenschutzverletzungen durch Dritte systematisch erheben und über ein gutes Verständnis der vorhandenen Risiken verfügen.

Bei Technologieanbietern oder IoT (Internet der Dinge)-Spezialisten haben lediglich 17% ein angemessenes Verständnis für diese Risiken – ein großer blinder Fleck, den Cyberkriminelle sehr wohl kennen und ausnutzen. Entgegen dem weltweiten Trend wird in Österreich immer noch zu sehr auf Lieferanten vertraut, ohne sich ein unabhängiges Bild zu machen. Die Durchführung von umfassenden Due-Diligence-Prüfungen

im Rahmen von Dienstleisterbeauftragungen wird von mehr als 80% der Befragten als nicht erforderlich betrachtet.

„Ich fürchte, dass wir besonders bei österreichischen KMU Aufholbedarf haben und in der Vergangenheit wenig gemacht bzw. zu viel gespart wurde. Wir sind keine Insel der Seligen, sondern Teil des globalen Cyberspace. Daher rate ich allen

Cyberangriffen. Den Weg in die Cloud sehen nur sieben Prozent der befragten Unternehmen als mögliche Strategie innerhalb der kommenden zwei Jahre.

Datenanalyse nicht vergessen

Ein bereits im Unternehmen vorhandener Erfolgsfaktor werde jedoch noch flächendeckend zu stark vernachlässigt: die Aufbereitung und Nutzung bestehender Daten. Während mehr als 80% der weltweiten Cybersecurity-Vorreiter beispielsweise Logdaten aus vergangenen Angriffen erfolgreich für ihre strategischen Entscheidungen nützen, greift in Österreich weniger als ein Drittel der befragten Unternehmen auf verfügbare Daten und Erkenntnisse zurück.

„Die wesentlichen Elemente zur Umsetzung einer datenbasierten Entscheidungsgrundlage sind in Österreich meist unzureichend vorhanden. Oft sind Cyberkriminelle bereits seit Monaten in das Unternehmensnetzwerk eingedrungen und haben ausreichend Zeit, sich überall auszubreiten. Das wäre fast so, als wenn man in einem Einfamilienhaus eine Alarmanlage montiert, aber vergisst, diese einzuschalten“, sagt Beham. Hier lohne es sich für heimische Unternehmen, einen Blick auf die weltweiten Vorreiter zu werfen, „denn Datenanalyse ist auch in der Verteidigung des eigenen Unternehmens eine entscheidende Macht“, betont Cybersecurityexperte Beham.

„Es gibt natürlich auch viele Fehlalarme, deren Klärung Ressourcen bindet. Die richtige Mischung aus Überwachung, Analyse und Akzeptanz zu finden, erfordert Gespür, das sich auch entwickeln muss. Hier das Optimum zu finden, ist nicht immer einfach, aber entscheidend“, ergänzt Jimmy Heschl.

Unternehmen – auf gut österreichisch – nicht jammern, sondern anpacken“, meint Jimmy Heschl, Head of Digital Security bei Red Bull, als einer der Befragten der Studie im Interview.

Strategie und Investition

Bei den wichtigsten Investitionsfeldern für IT-Sicherheit folge Österreich laut der Studie dem weltweiten Trend und erkenne vor allem Bedarf in der Integration und Harmonisierung von Prozessen und Maßnahmen über die gesamte Organisation hinweg (18%), den Abbau von veralteter Technologie (17%) sowie in der Erstellung von Checklisten und Workflows zur Unterstützung von Abläufen bei der Abwehr von