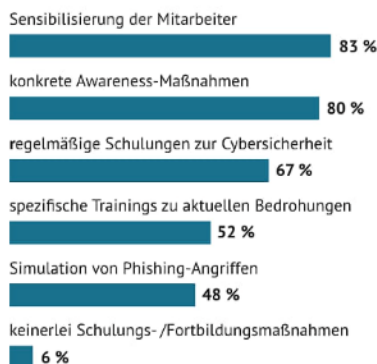




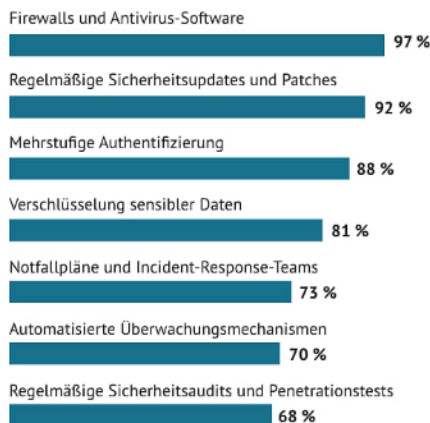
SOLARSEN/ISTOCKPHOTO

Schulungs- und Awareness-Maßnahmen



KURIER-Grafik: LG | Quelle: EY Cybersecurity Studie 2026

Schutzmaßnahmen gegen Cyberangriffe



KURIER-Grafik: LG | Quelle: EY Cybersecurity Studie 2026

Weil Cyberangriffe nicht nur die anderen treffen

Sicherheit. Cyberangriffe gehören für Unternehmen in Österreich längst zum Geschäftsalltag. Die Frage ist daher, wie gut Unternehmen auf einen solchen Angriff vorbereitet sind.

Von Herta Scheidinger

Österreichs Wirtschaft hat in den vergangenen Jahren deutlich in die IT-Sicherheit investiert. Auch das Sicherheitsbewusstsein in den Führungsetagen ist gestiegen – und das hat seinen Grund. Die Cyberangriffe nehmen zu und werden immer raffinierter. Darum muss Cybersecurity zunehmend als Teil des unternehmerischen Risikomanagements verstanden werden und nicht mehr ausschließlich als technische Aufgabe der IT-Abteilung. Aber es ist vor allem in den KMU noch viel zu tun, denn die Angriffe betreffen längst nicht mehr nur große Konzerne.

„Das Sicherheitsniveau ist hier sehr unterschiedlich und es ist vor allem der Finanzbereich wie Banken bzw. Versicherungen die stark investieren und besser aufgestellt sind. Dann noch die Börsennotierten Unternehmen die immer mehr gefordert durch ihre Aktionäre das Thema Cybersecurity immer ernst nehmen“, erklärt Robert Herscovici, CEO Trusted Cyber Security Solutions. Bei KMU sieht er die Lage durchwachsen, da ihnen sowohl Per-



„KI wirkt wie ein enormer Beschleuniger. Wir können unseren Augen und Ohren nicht mehr vertrauen.“

Nahed Hatahet
nahedahatahet.eu

STUDIO HEIDEGGER

sional als auch finanzielle Mittel bzw. Know-how fehlen.

Hohes Risiko

Doch wie schätzen die österreichischen Unternehmen das tatsächliche Risiko eines Angriffs ein? Darüber gibt die aktuelle EY-Cybersecurity-

ty-Studie 2026 Auskunft. So schätzen 38 Prozent das Risiko für sehr oder eher hoch – nach 47 Prozent im Vorjahr und 35 Prozent im Jahr 2024. Besonders gefährdet sehen sich der Pharma-, Chemie- und Gesundheitssektor, die Versicherungsbranche und Banken sowie die Technologie-, Medien- und Telekommunikationsbranche. Auch mit dem Umsatz steigt die Risikowahrnehmung: Bei Unternehmen ab 51 Millionen Euro Jahresumsatz sehen 24 Prozent ein sehr hohes Risiko.

Die Anzahl der tatsächlichen Angriffe steigt weiter leicht an. 64 Prozent der befragten Unternehmen hatten in den vergangenen fünf Jahren keine Hinweise auf Datenangriffe, 36 Prozent hingegen schon (17 Prozent einmal, 19 Prozent mehrfach) – ein Plus von vier Prozentpunkten gegenüber 2025. Mit dem Umsatz steigt die Wahrscheinlichkeit erneut: Bei Unternehmen ab 51 Millionen Euro Umsatz berichten 48 Prozent von mehrfachen Angriffen. Und ein Faktor lässt aufhorchen: Bei Unternehmen, die bereits KI-Technologien einsetzen, liegt der Anteil mit Angriffshinweisen bei 65 Pro-

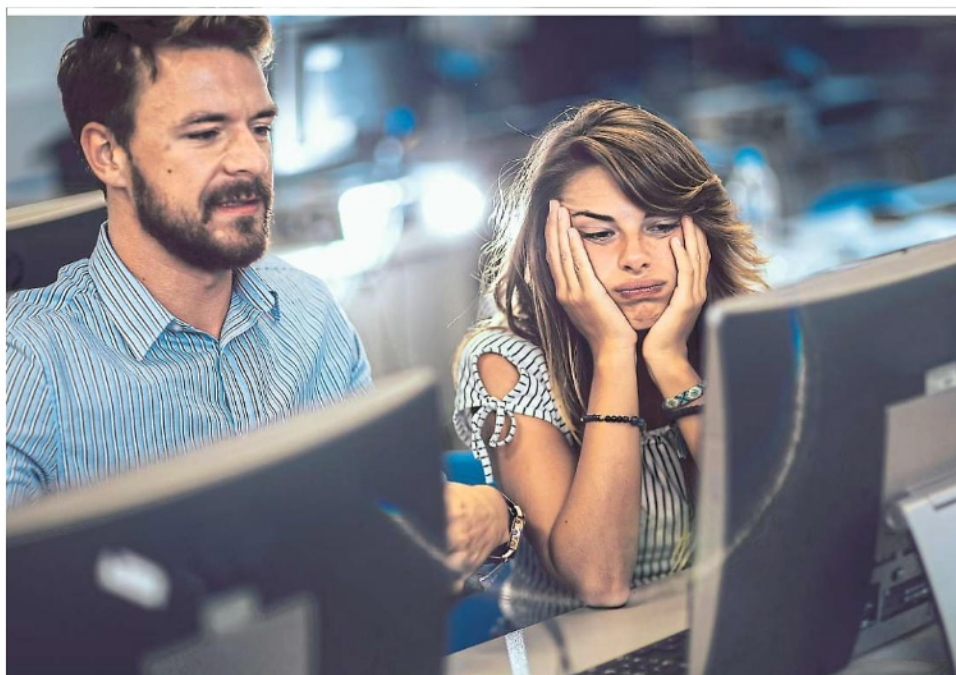
zent, ohne KI-Einsatz bei nur 29 Prozent. „Österreichs Unternehmen fühlen sich sicherer – und genau das kann trügerisch sein. Die Angriffszahlen steigen weiter, die Methoden werden professioneller. Wer sich zurücklehnt, verliert“, kommentiert Gottfried Tonweber, EY Partner, Cybersecurity Lead, Consulting, Österreich, das Ergebnis der Studie.

Auf Angriffe reagieren

Viele österreichische Unternehmen haben in den vergangenen Jahren massiv in Cybersecurity investiert. „Trotzdem dürfen wir Sicherheit nicht mit Resilienz verwechseln“, warnt Transformationsexperte Nahed Hatahet. „Aus meiner Sicht liegt gerade bei österreichischen Unternehmen eine der größten Herausforderungen darin, dass technische Sicherheit vielerorts bereits sehr ernst genommen wird, organisatorische Resilienz aber noch nicht überall denselben Stellenwert hat. Ein Unternehmen kann technisch sehr gut geschützt sein und trotzdem enorme Probleme bekommen, wenn ein erfolgreicher Angriff den Betrieb für Tage oder Wochen lahmlegt.“ Entscheidend sei deshalb nicht nur die Frage: Wie verhindere ich einen Angriff? Sondern auch: Wie schnell kann ich reagieren, Schäden begrenzen und wieder arbeitsfähig werden? „Dabei scheitert es oft gar nicht an den spektakulärsten Angriffsmethoden, sondern an grundlegenden Dingen: Systeme werden nicht rechtzeitig aktualisiert, Berechtigungen sind zu großzügig vergeben, Back-ups wurden nie unter realistischen Bedingungen getestet oder ein Dienstleister wird zum Einfallstor in die eigene Organisation.“

KI verschärft Situation

Die Bedrohungslage hat sich durch den Einsatz Künstlicher Intelligenz fundamental verändert. Cyberangriffe werden nicht nur professioneller, sondern vor allem schneller, glaubwürdiger und wesentlich einfacher skalierbar. „Künstliche Intelligenz wirkt dabei wie ein enormer Beschleuniger“, so Hatahet. Er vergleicht es mit der Kunstfertigkeit von Kunstfälschern. „Was früher außergewöhnliche Fähigkeiten, Wissen, Zeit und Aufwand benötigte, kann heute mit KI wesentlich einfacher erzeugt und potenziell millionenfach skaliert werden. Texte, Bilder, Stimmen, Videos und sogar ganze digitale Identitäten lassen sich miteinander kombinieren.“ Damit verändert sich auch die Bedeutung von Cybersecurity. Es geht längst nicht mehr ausschließlich da-



Cyberangriffe stellen eine große Gefahr für Unternehmen dar. Diese können für längere Zeit lahmgelegt werden.



„Regelmäßige, praxisnahe Schulungen und einfache Meldewege helfen, Angriffe früh zu erkennen.“

Robert Herscovici
TCSS

TRUSTED CYBER SECURITY SOLUTIONS

rum, Systeme und Daten technisch zu schützen. „Unternehmen müssen sich zunehmend damit beschäftigen, wie sie Vertrauen und Echtheit in einer digitalen Welt absichern, in der wir unseren eigenen Augen und Ohren nicht mehr selbstverständlich vertrauen können“, so Hatahet.

Die EY Cybersecurity Studie 2026 belegt auch einen Anstieg der KI-Angriffe. Deepfakes betreffen

mittlerweile bereits zehn Prozent der Befragten – im Jahr davor waren es noch drei Prozent – und auch bei den klassischen Phishing-Angriffen kommt zunehmend KI zum Einsatz.

Risiko-Faktor Mensch

Auch der Faktor Mensch bleibt entscheidend. Ein unbedachter Klick auf einen manipulierten Link oder eine gefälschte Rechnung kann technische Schutzmaßnahmen aushebeln. Dazu Tonweber: „Die stärkste Firewall nützt wenig, wenn ein Klick genügt, um sie zu umgehen. Der Mensch bleibt die entscheidende Schwachstelle – und gleichzeitig die stärkste Verteidigungslinie.“ Die Mitarbeiter müssen sich der Bedrohung also ebenso bewusst sein, wie der Unternehmer selbst. „Regelmäßige, praxisnahe Schulungen und einfache Meldewege helfen, Angriffe früh zu erkennen. Automatisierte Schulungsprogramme, die das Personal trainieren Phishing Mails zu erkennen wäre eine Basis-Notwendigkeit“, rät Herscovici. Sicherheitskultur muss im gesamten Unternehmen gelebt werden – vom Lehrling bis zur Geschäftsführung.

Hier gibt die EY Cybersecurity Studie 2026 Auskunft über die Praxis in den Unternehmen. Bei den Schulungs-



„Die Angriffszahlen steigen, die Methoden werden professioneller. Wer sich zurücklehnt, verliert.“

Gottfried Tonweber
EY

EY/CHRISTINA HÄUSLER

und Awareness-Maßnahmen zeigt sich ein klares Bild: 83 Prozent setzen auf die Sensibilisierung der Mitarbeiter, 80 Prozent auf konkrete Awareness-Maßnahmen, 67 Prozent auf regelmäßige Schulungen zur Cybersicherheit, 52 Prozent auf spezifische Trainings zu aktuellen Bedrohungen und 48 Prozent auf die Simulation von Phishing-Angriffen. Nur sechs Prozent geben an, keinerlei

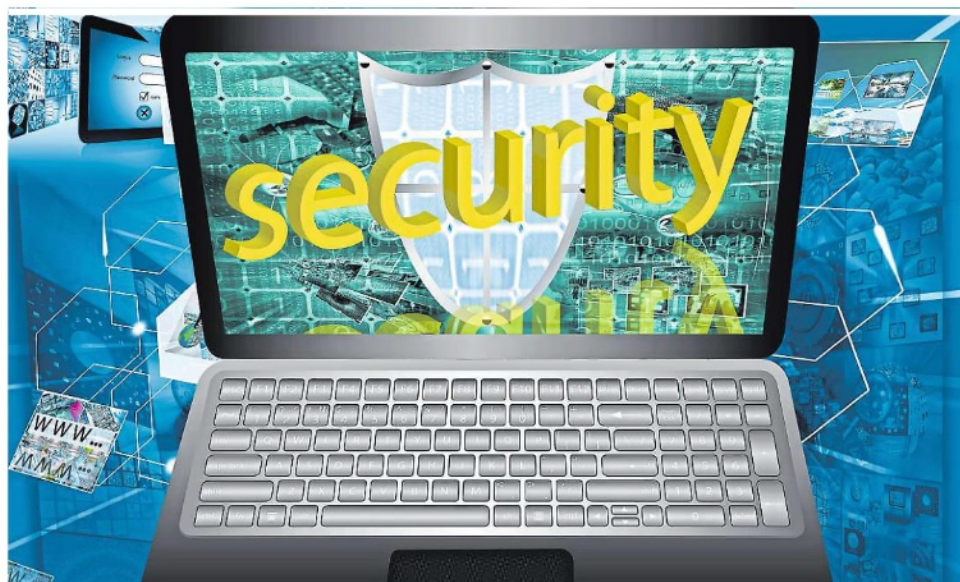
Schulungs- oder Fortbildungsmaßnahmen umzusetzen. Aktuelle Themen wie Deepfakes und KI-Bedrohungen sind bereits bei 48 Prozent Bestandteil der Schulungen, weitere 23 Prozent planen dies.

Sicherheit ernst nehmen

Österreichs Unternehmen sind damit auf einem Weg, der bereits deutlich weiter ist als noch vor einigen Jahren. Gleichzeitig gibt es insbesondere bei kleineren Betrieben und bei der Absicherung von Lieferketten noch Nachholbedarf. Entscheidend wird sein, ob Cybersecurity dauerhaft als strategische Aufgabe betrachtet wird – und ob Unternehmen bereit sind, nicht erst nach einem Angriff zu handeln, sondern vorher in ihre Widerstandsfähigkeit zu investieren. „Cybersecurity ist für mich deshalb kein Projekt, das irgendwann abgeschlossen ist. Es ist eine permanente Reise in einer digitalen Umwelt, die sich laufend verändert. Unternehmen brauchen technische Schutzmaßnahmen, belastbare Prozesse und gut vorbereitete Menschen. Denn am Ende zeigt sich die Qualität von Cybersecurity nicht nur daran, ob ein Angriff verhindert wurde, sondern vor allem daran, wie handlungsfähig ein Unternehmen bleibt, wenn doch etwas passiert“, ist Transformationsexperte Hatahet überzeugt.

Auch Robert Herscovici sieht auch in Zukunft dringenden Handlungsbedarf. „Angriff und Abwehr werden stärker automatisiert. Es ist wichtig jetzt dringend die Hausaufgaben zu erledigen und Mindeststandards für Cyber Security einzuhalten. Ansonsten werden die Unternehmen den AI-geführten Angriffen in Zukunft nicht standhalten können.“

Auch wenn Firewalls und Antivirus-Software, regelmäßige Sicherheitsupdates und Patches mittlerweile bei praktisch jedem Unternehmen Standard sind, ist der Blick in die Zukunft bei vielen Unternehmen eher pessimistisch, wenn es um Cybersecurity geht. Laut EY Studie rechnen 30 Prozent der Befragten mit einem sehr starken Anstieg von Cyberangriffen und Datenklau, weitere 52 Prozent rechnen mit einem moderaten Anstieg. Nur sechs Prozent gehen von einem Rückgang aus. Besonders skeptisch ist die Versicherungsbranche – 74 Prozent erwarten einen starken oder moderaten Anstieg. Mehrheitlich zunehmende Bedrohungen sieht man auch im Pharma- und Gesundheitsbereich sowie in der Industrie.



Cybersicherheit ist ein Langzeitprojekt, denn die Art der Angriffe verändert sich ständig.