Digitale Bedrohung nimmt zu

Cyber-Angriffe werden schneller, gezielter und zunehmend durch künstliche Intelligenz unterstützt. Die Studie „Cybersecurity in Österreich 2026“ zeigt, vor welchen Herausforderungen Unternehmen, Behörden und kritische Infrastruktur stehen und welche Maßnahmen ihre Widerstandsfähigkeit stärken können.

Die Bedrohung durch Cyber-Angriffe wächst. Gleichzeitig verkürzt sich die Zeit zwischen dem Bekanntwerden einer Sicherheitslücke und ihrer Ausnutzung durch Angreifer. Welche Risiken sich daraus für Unternehmen, Behörden und kritische Infrastruktur ergeben, zeigte die Vorstellung der Studie „Cybersecurity in Österreich 2026“ durch das *Kompetenzzentrum Sicheres Österreich (KSÖ)* und *KPMG Österreich* am 20. Mai 2026 im Erste Campus in Wien.

„Cyber-Sicherheit ist längst keine Aufgabe mehr, die allein von IT-Abteilungen bewältigt werden kann“, betonte Helmut Leopold, Leiter des Centers for Digital Safety and Security am Austrian Institute of Technology (AIT). Angesichts der fortschreitenden Vernetzung seien gemeinsame Sicherheitsstrategien von Wirtschaft, Forschung, Verwaltung und Politik erforderlich.

Angriffe werden schneller und gezielter. Laut der „Zero Clock Study“ verkürzte sich die Zeitspanne zwischen dem Bekanntwerden einer Schwachstelle und ihrer Ausnutzung von durchschnittlich 23,2 Tagen auf rund zehn Stunden. Unternehmen und Behörden geraten dadurch zunehmend unter Druck, Sicherheitslücken rasch zu erkennen und zu schließen. Gleichzeitig professionalisieren sich Cyber-Kriminelle. Neben Ransomware-Angriffen gewinnen langfristig angelegte Spionage- und Informationsbeschaffungsoperationen an Bedeutung. Diese bleiben oft lange unentdeckt und können erheblichen Schaden verursachen.

Künstliche Intelligenz unterstützt nicht nur die Abwehr von Angriffen, sondern wird auch von Cyber-Kriminellen genutzt. Sie hilft dabei, Schwachstellen schneller aufzuspüren, Phishing-Nachrichten überzeugender zu formulieren und Angriffe effizienter vorzubereiten. Gefälschte E-Mails, Kurznachrichten oder Internetseiten wirken dadurch zunehmend authentisch und sind oft nur schwer als Täuschungsversuche zu erkennen.

Expertinnen und Experten aus Wirtschaft, Forschung und Verwaltung bei der Präsentation der Studie „Cybersecurity in Österreich 2026“ im Erste-Campus in Wien

Der Mensch bleibt die größte Schwachstelle. Trotz technischer Fortschritte zählt der Faktor Mensch weiterhin zu den größten Risiken. Phishing- und Spear-Phishing-Angriffe gehören nach wie vor zu den häufigsten Einfallstoren für Schadsoftware und Datendiebstahl.

Robert Lamprecht, Leiter des Bereichs Technology Consulting mit Schwerpunkt Cybersecurity bei *KPMG Österreich,* verwies auf die anhaltende Bedeutung von Social Engineering. Spam-Anrufe, täuschend echt wirkende Nachrichten und andere Manipulationsversuche seien weiterhin weit verbreitet. Zudem würden Cyber-Kriminelle verstärkt Lieferketten und externe Dienstleister als Einstiegspunkte in Unternehmensnetzwerke nutzen.

Kritische Infrastruktur schützen. Der Cyber-Sicherheit kritischer Infrastruktur kommt besondere Bedeutung zu. Angriffe auf Energieversorgung, Telekommunikation, Gesundheitswesen, Verkehr oder staatliche Einrichtungen können nicht nur wirtschaftliche Schäden verursachen, sondern auch die Versorgungssicherheit beeinträchtigen.

Sarah Case Lackner vom *Vienna Center for Disarmament and Non-Proliferation (VCDNP)* erläuterte die Rolle digitaler Sicherheitsmaßnahmen in der Nuklearsicherheit. Regelmäßige Sicherheitsüberprüfungen, technische Anpassungen und Notfallübungen seien entscheidend, um Risiken frühzeitig zu erkennen und wirksam zu beherrschen.

Die vorgestellten Beispiele machten deutlich, wie eng digitale Sicherheit und der Schutz kritischer Infrastruktur miteinander verknüpft sind. Cyber-Angriffe können längst nicht mehr nur einzelne Computersysteme beeinträchtigen, sondern auch Auswirkungen auf Versorgung, Kommunikation und öffentliche Dienstleistungen haben.

Cyber-Sicherheit als Führungsaufgabe. Laut Studienautoren sei Cyber-Sicherheit zunehmend eine strategische Führungsaufgabe. Investitionen in Technologie, qualifiziertes Personal sowie Aus- und Weiterbildung gelten ebenso als entscheidend wie die Zusammenarbeit von Staat, Wirtschaft und Forschung, um den wachsenden Bedrohungen im digitalen Raum wirksam zu begegnen. *Michael Ellenbogen*

FOTO: WWW.ANNARAUCHENBERGER.COM / ANNA RAUCHENBERGER