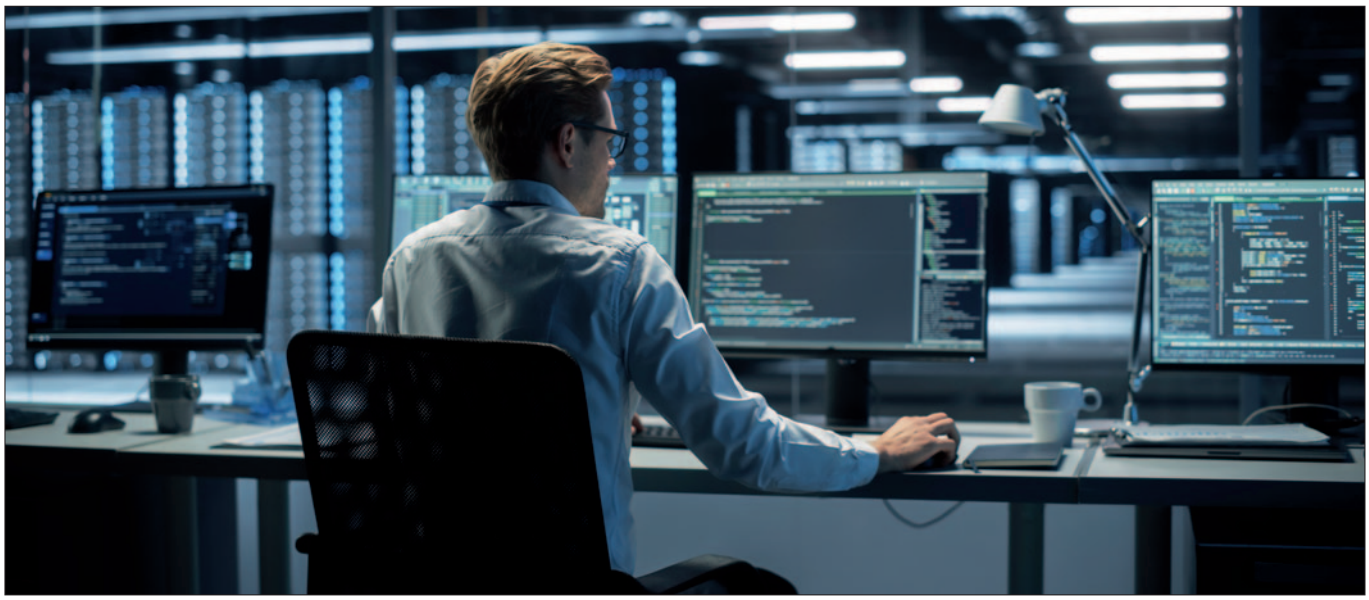

Die Schaffung eines sicheren und stabilen Cyber-Raumes ist essenziell für die Resilienz Österreichs und der Europäischen Union.

# Einheitliche EU-Vorgaben

**Computer-Kriminalität ist im Steigen. Staat, Wirtschaft und Gesellschaft sind immer stärker vom Funktionieren der IKT-Infrastruktur abhängig. Dies bringt große Herausforderungen mit sich und führt zu immer stärkerer Regulierung der Cyber-Sicherheit auf europäischer Ebene, die national umgesetzt werden muss.**

Computerkriminalität nimmt stetig zu. Die kritische Infrastruktur ist immer stärker mit dem Internet verknüpft. Staat, Wirtschaft und Gesellschaft bringen sich in eine immer größere Abhängigkeit zu einer funktionierenden IKT-Infrastruktur. Cyber-Sicherheit ist längst eine sicherheitspolitische Herausforderung mit gesamtgesellschaftlicher Dimension. Dieser Herausforderung müssen Staat und Wirtschaft mit umfassenden Maßnahmen zur Erhöhung der Resilienz begegnen.

**Die Europäische Union** reagiert auf diese neue Herausforderung, indem sie regulierend tätig wird. In den letzten Jahren verabschiedete sie mehrere Vorgaben, die, effektiv umgesetzt, einen wichtigen Beitrag zu mehr Cyber-Sicherheit und Widerstandsfähigkeit bringen werden. Österreich hat bereits seit mehreren Jahren die Netz- und Informationssystemsicherheit (NIS) Richtlinie durch eine strategische und eine operative NIS-Behörde im BMI umgesetzt. Nun steht Österreich vor der anspruchsvollen Aufgabe, mehrere Vorgaben der Europäischen Union zeitnah umsetzen zu müssen, und zwar die Schaffung einer nationalen Cyber-Zertifizierungsbehörde, eines nationalen Cyber-Koordinierungszentrums und die Umsetzung der Cyber-Sicherheit im Bereich der Luftfahrt. Mit Ziel Mitte 2024 wird Österreich auch die Umsetzung der NIS-2 Richtlinie und der Richtlinie über die Resilienz kritischer Einrichtungen umsetzen müssen. Erwartet wird für Herbst 2022, dass die Europäische Kommission ein Gesetzesvorhaben zu Cyber-Resilienz präsentieren wird, das ebenso in den kommenden Jahren umzusetzen sein wird.

**Mehr staatliche Unterstützung.** Derzeit sind die Cyber-Sicherheitslandschaft und die Zuständigkeiten in einigen EU-Mitgliedsstaaten zersplittert. Auch in Österreich sind die staatlichen Kompetenzen, die für die Sicherstellung umfassender Cyber-Sicherheit erforderlich sind, fragmentiert. Laut einer aktuellen Studie von KPMG zur Cyber-Sicherheit in Österreich gaben 78 Prozent der befragten Unternehmen an, in der Cyber-Sicherheit stärker vom Staat unterstützt werden zu wollen. Auch die Europäische Kommission und der Rechnungshof drängen darauf, das vorhandene Know-how zu bündeln und so Effektivität und Effizienz in diesem Bereich nachhaltig zu erhöhen, auch mit Blick auf die physische Resilienz der kritischen Infrastruktur. In ihrer Präsentation des EU Cyber-Sicherheitspakets 2020 forderte die Europäische Kommission, dass digitale und physische Sicherheit in Zukunft gemeinsam gedacht werden.

**Resilienter Cyber-Raum.** Die Schaffung eines sicheren und stabilen Cyber-Raumes ist essenziell für die Resilienz Österreichs und der Europäischen Union. Nur so kann die Digitalisierung in einem geschützten Raum wachsen und gelingen. Wenn es uns gelingt, den Cyber-Raum sicher zu gestalten, dann werden wir es schaffen ein lebendiges digitales Ökosystem zu haben und die Attraktivität des Wirtschaftsstandorts zu wahren.

Um dieses Ziel zu erreichen, ist es erforderlich, im Bereich der Cyber-Sicherheit leistungsfähig und flexibel agieren zu können. Österreich muss seine kritische Infrastruktur schützen, ein lebendiges Cyber-Ökosystem schaffen und im Cyber-Krisenfall bestmöglich vorbereitet und international vernetzt sein. Die Regulierung auf europäischer Ebene soll als Chance verstanden werden und rasch und effizient umgesetzt werden.

*Caroline Schmidt*

FOTO: GORODENKOFF/STOCK.ADOBE.COM