KPMG

11 AUSGABE CYBERSECURITY STUDIE

Cybersecurity in Österreich

Sicherheitsforum
Digitale Wirtschaft
Österreich

Mai 2026

kpmg.at/cyber

KPMG. Make the Difference.

Ein Jahr Patenschaft für die Europäischen Sumpfschildkröten – was bleibt

Seit 2022 begleitet uns die Schildkröte bereits sinnbildlich durch die Tiefen der Cyberwelt. Als Urgestein hat sie uns gelernt, was es heißt, weise, beständig und anpassungsfähig zu sein – trotz einer Welt im Wandel und zahlreicher neuer Bedrohungen, die täglich auf sie und auf uns zukommen.

Mit viel Ausdauer und Robustheit navigiert sie durch Wasser und Land. Genauso wie sich auch Unternehmen in Österreich durch die zahlreichen Cyberangriffe hindurchmanövrieren müssen.

2025, im Rahmen unserer zehnten Jubiläumsausgabe, haben wir beschlossen, unserem Dank und unserer Wertschätzung diesem Tier gegenüber Ausdruck zu verleihen. So hat KPMG die Patenschaft für die Europäischen Sumpfschildkröten im Tiergarten Schönbrunn übernommen.

Ein Jahr später haben wir die Schildkröten erneut besucht. Obwohl unsere Patenschaft hier endet, ist unsere Wertschätzung für diese besondere Tierart sowie die Wichtigkeit des Artenschutzes ungebrochen. Auch bleibt unsere Arbeit an der Seite der heimischen Unternehmen weiter bestehen. Gemeinsam meistern wir die rauen Gewässer der Cybersecurity. Gemeinsam machen wir den Unterschied. Die Resilienz der Schildkröte dabei stets vor Augen.

Robert Lamprecht, Marlene Zauner, Mariana Herrloss (v. l. n. r.)

„Als Urgestein in der Tierwelt hat uns die Schildkröte gelehrt, was es heißt, weise, beständig und anpassungsfähig zu sein – trotz einer Welt im Wandel und zahlreicher neuer Bedrohungen, die täglich auf sie und auf uns zukommen. Die perfekte Metapher auch für die Cyberwelt.“

Souveränität entscheidet

Die digitale Transformation eröffnet Unternehmen neue Chancen für Wachstum, Innovation und Effizienz. Und so taucht auch die Schildkröte, die dieses Jahr unser Cover ziert, sinnbildlich in die digitale Welt ein und nutzt Agenten für ihre Fortbewegung.

Gleichzeitig steigt auch die Angriffsfläche für Unternehmen: Cyberangriffe treffen heute nicht nur IT-Systeme, sondern Geschäftsprozesse, Lieferketten und unser Vertrauen. Künstliche Intelligenz wirkt dabei als Beschleuniger; sie ermöglicht neue Formen der Automatisierung, verändert aber ebenso die Dynamik zwischen Angriff und Verteidigung. Parallel rückt digitale Souveränität in den Fokus: Wer zentrale Daten, Plattformen und Abhängigkeiten nicht steuern kann, verliert im Ernstfall Handlungsoptionen.

Die 11. Ausgabe unserer KPMG & KSÖ Studie „Cybersecurity in Österreich“ 2026 bietet Ihnen einen kompakten Orientierungsrahmen, um diese drei Themenfelder – Digitalisierung, KI und digitale Souveränität – als Teil moderner Unternehmensführung einzuordnen.

Cybersecurity ist Führungsaufgabe

Für die heimischen Unternehmen bedeutet das vor allem eines: Cybersecurity muss in Entscheidungen, Prioritäten und Governance-Strukturen fest verankert sein. Cyberangriffe sind kein Ausnahmeereignis, sondern ein dauerhaftes Geschäftsrisiko, mit Auswirkungen auf Verfügbarkeit, Integrität und Vertraulichkeit. Der Einsatz von KI erhöht die Geschwindigkeit und Komplexität, mit der sich Risiken entwickeln, und stellt zugleich neue Anforderungen an die Governance. Digitale Souveränität ergänzt diese Perspektive um die Frage, wie abhängig wir von Technologien, Anbietern und Rechtsräumen sind und welche Alternativen im Krisenfall realistisch verfügbar sind. Das Ziel kann nicht Aktionismus sein, sondern klare Steuerbarkeit.

Orientierung statt Alarmismus

Die vorliegende Studie soll dazu beitragen, Entwicklungen einzuordnen und die richtigen Fragen für die Cybersecurity-Steuerung zu schärfen: Welche kritischen Prozesse müssen auch unter Druck funktionsfähig bleiben? Wo entstehen neue Risiken durch KI-gestützte Automatisierung und durch schwer prüfbare Informationen? Und wie lässt sich digitale Souveränität so gestalten, dass Wahlmöglichkeiten, Compliance und Resilienz nicht nur am Papier bestehen?

Sie finden in den folgenden Kapiteln keine Alarm-Rhetorik, sondern eine strukturierte Grundlage für strategische Diskussionen, Priorisierung und wirksame Umsetzung, mit dem Fokus auf Orientierung, Verantwortung und langfristige Widerstandsfähigkeit.

Ein großer Dank geht an dieser Stelle an die zahlreichen Teilnehmenden, die an unserer Umfrage mitgewirkt und auch in diesem Jahr unsere Fragen beantwortet haben, sowie an alle, die uns im Rahmen von Interviews unterstützt haben.

Nur mit Ihrer Hilfe ist es möglich, die Cybersecurity-Studie für Österreich im Jahr 2026 erneut in diesem Umfang und in dieser Qualität zu veröffentlichen!

Wir wünschen Ihnen eine anregende Lektüre sowie hilfreiche Impulse für die weitere strategische Ausrichtung Ihrer Organisation.

Robert Lamprecht
KPMG Partner

Andreas Tomek
KPMG Partner

Michael Schirmbrand
KPMG Partner

Daniel Kroiß
KPMG Partner

Unsere Kooperationspartner

Vielen Dank an unsere Kooperationspartner für die Zusammenarbeit bei der Studie:

Die Studie wurde in Kooperation mit dem Sicherheitsforum Digitale Wirtschaft des Kompetenzzentrum Sicheres Österreich (KSÖ) durchgeführt. Das Sicherheitsforum Digitale Wirtschaft Österreich ist die Arbeitsplattform, wo Wirtschaft, Forschung und Behörden gemeinsam Verantwortung übernehmen und ihren Beitrag zur sicheren Digitalisierung leisten.

KSÖ Kompetenzzentrum Sicheres Österreich

Sicherheitsforum Digitale Wirtschaft Österreich

Wir bedanken uns auch bei unseren Kooperationspartnern in den Bundesländern:

IV Industriellenvereinigung Kärnten

SILICONALPS

WKO Wirtschaftskammer Wien Information·Consulting

FHV Vorarlberg University of Applied Sciences

FH Salzburg

JOANNEUM RESEARCH

universität innsbruck
Netzwerk Banking, Accounting Auditing, Finance & IT (BAFIT)

Cybersicherheit braucht uns alle

Ein Blick auf die Ergebnisse der Studie „Cybersecurity in Österreich 2026“ zeigt, dass wir einen Mix aus alten und neuen, aus bereits bekannten und aus bis dato noch nicht als umfassende Bedrohungen wahrgenommene Herausforderungen beobachten müssen. Dieses Spektrum reicht von „klassischen“ Malware- und Phishing-Angriffen über Angriffe auf die Lieferkette bis zu KI-gestützten Angriffsvektoren wie beispielsweise Deep Fakes.

Auch im 11. Jahr ihrer Durchführung überraschen die Ergebnisse der Studie in Bezug auf Häufigkeit, Impact und „Erfolge“ der Cyberkriminellen nicht. Besonders interessant und aufschlussreich ist die Einbettung dieser Ergebnisse in regulatorische und politische Rahmenbedingungen. So haben Unternehmen eine hohe Sensibilität in Bezug auf die Abhängigkeit von digitalen Technologien. In diesem Zusammenhang möchte ich die Bedeutung der Bemühungen des österreichischen Digitalisierungsstaatssekretärs Alexander Pröll, der in Abstimmung mit der europäischen Ebene eine Charta der Digitalen Souveränität vorantreibt, unterstreichen. Wir brauchen nicht nur das Miteinander von Unternehmen, Behörden sowie Forschungs- und Technologieeinrichtungen auf nationaler Ebene: Vielmehr braucht es eine gemeinsame europäische Kraftanstrengung in einem geopolitisch volatilen Umfeld, um die digitale Sicherheit von Unternehmen zu unterstützen.

In diesem Prozess stehen eine Reihe europäischer regulatorischer Rahmen, von der Umsetzung der NIS-2-Richtlinie über Cyber Resilience oder KI-Regulatorien zur Verfügung. Für die Unternehmen ist dabei besonders wichtig, dass diese Regulatorien umsetzbar, auf dem Stand der Technik und in ihrer Anwendung berechenbar und transparent sind. Nur so können sie helfen, den Digitalisierungsstandort Europa zu sichern und nicht mit unnötiger Bürokratie zu belasten.

Im KSÖ haben wir uns aktuell eine Reihe von Aktivitäten vorgenommen, um an den genannten Themen und Herausforderungen mitzuarbeiten. Maßnahmen zur Cybercrime-Prävention ziehen sich durch eine Vielzahl unserer Bemühungen und werden insbesondere auch durch unsere Landesklubs vorangetrieben. In Partnerschaft mit einem renommierten Fachverlag wird Anfang 2027 die neue Publikation „SECURE Austria“ erscheinen, die u. a. Themen der Informations- und Cybersicherheit ebenso wie andere Sicherheitsherausforderungen aufgreift und an zentrale Stakeholder-Gruppen transportieren wird. Im ersten Halbjahr 2027 werden wir zu einem großen, nationalen Cybersicherheits-Planspiel einladen. Parallel dazu arbeiten wir mit Partnern aus der Wirtschaft an der Entwicklung des Projekts „CyberCampus Österreich“. All das möchten wir gemeinsam mit Ihnen vorantreiben. Weil Cybersicherheit braucht uns alle!

FOTO © EVA_KELETY

Mag.
Michael Höllerer
Präsident des KSÖ

Inhaltsverzeichnis

11. AUSGABE CYBERSECURITY STUDIE

Die Illusion der Ruhe

Ein Trend, der sich in den letzten Monaten abgezeichnet hat und sich vermutlich auch in Zukunft fortsetzen wird, ist die Veränderung der Art und Weise, wie Cyberangriffe durchgeführt werden und mit welchen Signalen sie auftauchen. Wurde es in der Vergangenheit noch relativ laut bei einem Angriff (z. B. Ransomware, die sehr schnell für einen Stillstand in der Organisation gesorgt hat), werden Cyberangriffe nun zunehmend leiser.

Aber leise ist kein Zeichen von Entspannung, sondern vielmehr ein eindeutiger Hinweis dafür, dass die Professionalisierung, die Intensität und die Komplexität der Cyberattacken weiter zunehmen. Leise Angriffe unterstreichen einmal mehr, dass wir es nicht mehr ausschließlich mit der klassischen organisierten Kriminalität zu tun haben. Wir erleben Phänomene, die miteinander in Kombination stehen, wie staatliche oder staatlich unterstützte Akteur:innen in Zusammenarbeit mit Nachrichten- oder Geheimdiensten. Täter:innen agieren heute strategisch durch Spionage und Informationsbeschaffung gegen Forschungs-, öffentliche und Industrieeinrichtungen, aber auch mit Desinformationskampagnen, die unser Vertrauen in Institutionen und Informationen unterminieren sollen.

Sie alle haben eines gemeinsam: Sie arbeiten leiser, geduldiger und langfristiger. Ihr Erfolg bemisst sich nicht vorrangig an einer schnellen Lösegeldzahlung, sondern am dauerhaften und persistenten Zugriff. Gerade wenn wir an exportorientierte Länder wie Österreich denken, die eine starke Industrie mit hoher Innovationsdichte und eng verflochtenen Lieferketten aufweisen, ist das keine abstrakte Bedrohung mehr. Es ist eine Bedrohung, die die Wettbewerbsfähigkeit betrifft, die Standortattraktivität herausfordert und im Kern die Frage stellt: Was bleibt noch verlässlich, wenn Systeme, Daten und Entscheidungen unter den Druck von Cyberangriffen geraten?

Effizienter, besser, schneller?

Die letzten 12 Monate haben uns gezeigt, dass kein Stein mehr auf dem anderen liegen geblieben ist, wenn es um Cybersicherheit und technologische Entwicklung geht. KI hat für eine rasante Veränderung gesorgt, die uns auf der einen Seite viel Freude bereitet hat, weil wir Aufgaben automatisieren und interaktiver bewerkstelligen können. Auf der anderen Seite hat sie uns aber auch gezeigt, wie schnell wir Angreifer:innen ausgeliefert sind. Langfristig mögen KI-Tools die Welt sicherer machen, doch kurzfristig bedingen die derzeit verfügbaren Modelle ein „Wild West"-Szenario. Die Zero Day Clock zeigt anschaulich jene Zeit, die es vom Erkennen einer Schwachstelle bis zur Ausnutzung benötigt. Waren es im Jahr 2025 noch 23,2 Tage, liegen wir im Mai 2026 bei 10 Stunden.

Dieser Faktor (ein Sechsundfünfzigstel) führt dazu, dass wir in einer neuen Realität angekommen sind. Eine Realität, die wir uns bewusst geschaffen haben, weil sie uns schneller, effizienter, leistungsfähiger macht. Doch genau diese Realität entlarvt schonungslos, dass unsere Grundlagen mit diesem Tempo nicht Schritt halten. Es ist, als würden wir ein Hochhaus bauen, das immer schneller in die Höhe wächst. Ein Stockwerk nach dem anderen schießt nach oben, die Fassade glänzt, die Architektur beeindruckt, alles wirkt modern, souverän, unter Kontrolle. Der Bau wird gefeiert, weil er zeigt, was möglich ist.

Nur: Das Fundament darunter ist noch nicht fertig. Es ist nicht ausgehärtet, nicht darauf ausgelegt, diese Last zu tragen. Und während wir oben weiterbauen, entstehen unten erste Risse. Kaum sichtbar zunächst, leicht zu ignorieren. Doch mit jedem zusätzlichen Stockwerk wächst der Druck, und damit die Wahrscheinlichkeit, dass das gesamte Gebäude nicht an seiner Höhe scheitert, sondern an dem, was es eigentlich tragen sollte.

Das Ruder aus der Hand geben

Darüber hinaus haben wir uns auch dazu entschieden, unsere Entscheidungskompetenz immer weiter abzugeben. Wir lassen die Maschine für uns bestimmen, inklusive aller damit einhergehenden Konsequenzen. So erleben wir, dass Halluzinationen weiterhin auf der Tagesordnung stehen und autonome Systeme für immer mehr Kopfzerbrechen sorgen, wenn sie unsere Daten und Informationen löschen. Aber zumindest bleiben sie höflich dabei und entschuldigen sich danach, es getan zu haben.

Genau das ist die Welt, die wir geschaffen haben. Eine Welt, in der wir den Angreifer:innen gezeigt haben, wie schnell wir heute verwundbar sind. Im Wettlauf gegen die Cyberkriminellen sind wir um viele Plätze zurückgefallen, und das Momentum liegt eindeutig auf der Seite der Angreifer:innen.

Was bleibt noch verlässlich, wenn Systeme, Daten und Entscheidungen unter Druck von Cyberangriffen geraten?

Automatismus mit Automatismus besiegen

Autonome Systeme können momentan bereits selbstständig und vollständig Angriffe durchführen. Ja, aktuell nur in Laborumgebungen. Und ja, Laborumgebungen stellen nicht die volle Realität eines Unternehmens in freier Wildbahn mit all ihren Abhängigkeiten, Eigenschaften und Besonderheiten dar. Nichtsdestotrotz zeigt es uns, dass die Möglichkeiten da sind. Wenn wir uns in 12 Monaten wieder treffen, werden wir das sicherlich schon in einer automatisierten Form erleben. Was heißt das für uns? Wir müssen Automatismen mit Automatismen begegnen und selbst in der Lage sein, Aufgaben, die wir noch manuell erledigen oder die Abstimmungsaufwand bedürfen, in Zukunft zu automatisieren. Geht das immer so leicht? Nein. Aber es braucht dieses Umdenken auf Seiten der Unternehmen. Vermeintlich uninteressante Dinge wie Hygienemaßnahmen in der Infrastruktur werden zum Rettungsanker. Die Handlungsfähigkeit der Unternehmen bei (möglichen) Cyberangriffen muss schneller werden – nicht nur wegen der regulatorischen Meldeverpflichtungen. Und auch bei der Reaktion auf Cyberangriffe sollten Automatismen zur Selbstverständlichkeit werden.

Zu spät, zu langsam, zu bequem?

Automatismen und KI sind nicht die Antworten auf alle Probleme, sondern sie sind Lösungen und Probleme zugleich. Dieses Umdenken muss nicht

Hier geht's zum Download