1012/A(E)
vom 23.09.2026 (XXVIII. GP)

ENTSCHLIESSUNGSANTRAG

der Abgeordneten Süleyman Zorba, Freundinnen und Freunde

betreffend eine nationale Sicherheits- und Aufklärungsoffensive gegen KI-gestützte Cyberkriminalität für kleine und mittlere Unternehmen und die Bevölkerung

BEGRÜNDUNG

Cyberkriminalität ist in Österreich seit Jahren auf einem konstant hohen Niveau. Der am 27. August 2026 präsentierte Cybercrime-Report 2025 des Bundeskriminalamts weist 63.459 angezeigte Delikte aus. Besonders im Fokus stehen Formen des Investitionsbetrugs mit einer Schadenssumme von rund 120 Millionen Euro. Das Bundeskriminalamt nennt als aktuelle Entwicklung ausdrücklich den Einsatz Künstlicher Intelligenz. KI wird unter anderem zur Erstellung betrügerischer Inhalte und von Deepfakes sowie zur Automatisierung und Professionalisierung komplexer Betrugsmodelle genutzt.[1]

Auch Unternehmen spüren diese Verschiebung. In der KPMG-Studie „Cybersecurity in Österreich 2026" berichten 47 Prozent der 1.396 befragten Unternehmen, dass KI verstärkt bei Angriffen eingesetzt wird, 50 Prozent sehen KI-gestützte Angriffe als größte Herausforderung. Jeder achte Angriff war erfolgreich, die häufigsten Einfallstore bleiben Schadsoftware per E-Mail (78 Prozent) und Phishing über Links (69 Prozent). Der Anteil der Unternehmen, die über kompromittierte Dienstleister oder Lieferanten angegriffen wurden, hat sich binnen eines Jahres auf 22 Prozent verdoppelt.[2] Nach Zählung im Cyber Security Report von Check Point Software Technologies waren österreichische Organisationen 2025 im Schnitt 1.665 Angriffen pro Woche ausgesetzt, um zwölf Prozent mehr als im Jahr davor.[3]

Künstliche Intelligenz verändert die Bedrohungslage auf zwei Ebenen. Die erste Ebene ist der Mensch als Ziel. Phishing-Nachrichten sind heute fehlerfrei, personalisiert und in perfektem Deutsch verfasst. Stimmen von Geschäftsführer:innen, Angehörigen oder Behördenmitarbeiter:innen lassen sich aus wenigen Sekunden Tonmaterial klonen, Videoanrufe mit gefälschten Gesichtern sind mit frei verfügbaren Werkzeugen möglich. Der klassische „Chef-Betrug" und der „Enkeltrick" erhalten

---

[1] https://www.bundeskriminalamt.at/newsb0e5.html?id=42307473384354634638 6f3d
[2] KPMG Austria, Cybersecurity in Österreich 2026, https://kpmg.com/at/de/media/publications/cybersecurity-studie.html
[3] Check Point Software Technologies, Cyber Security Report 2026 (14. Ausgabe), 30.1.2026, Österreich-Zahlen zitiert nach itwelt.at, https://itwelt.at/news/cyber-security-report-12-prozent-mehr-cyberangriffe-in-oesterreich-im-jahr-2025/

damit eine Qualität, gegen die die bisherigen Erkennungsregeln (Rechtschreibfehler, unpersönliche Anrede, fremde Absender) nicht mehr helfen. Betroffen sind Buchhaltungen von Kleinbetrieben ebenso wie ältere Menschen, die per Telefon oder Messenger kontaktiert werden.

Die zweite Ebene ist die Technik als Ziel. Das deutsche Bundesamt für Sicherheit in der Informationstechnik warnte in einem Bericht des Handelsblatts am 3. August 2026, dass aktuelle KI-Modelle erhebliches Potenzial beim Auffinden von Sicherheitslücken zeigen, diese eigenständig ausnutzen und mehrere Angriffsschritte zu einer durchgehenden automatisierten Operation verketten können. Die Folge ist eine höhere Skalierbarkeit von Angriffen bei sinkenden Einstiegshürden.[4] Für einen Betrieb bedeutet das, dass die Zeit zwischen dem Bekanntwerden einer Sicherheitslücke und ihrer massenhaften Ausnutzung von Wochen auf Stunden schrumpft, dass Schadsoftware ohne Fachwissen erzeugt und laufend verändert werden kann und dass automatisierte Suchläufe jeden schlecht gewarteten Router, jede offene Fernwartung und jeden Webshop finden. Ein Kleinbetrieb, der bisher schlicht zu klein war, um als Ziel interessant zu sein, ist heute ein automatisiert auffindbares Ziel. Hinzu kommt eine neue Angriffsfläche in den Unternehmen selbst, wenn KI-Assistenten und Chatbots eingesetzt werden, deren Eingaben manipuliert werden oder über die vertrauliche Daten abfließen können.

Auf diese Lage ist die bestehende Struktur nicht ausgelegt. Die NIS-2-Richtlinie und ihre nationale Umsetzung erfassen grundsätzlich erst mittlere und große Unternehmen in bestimmten Sektoren.[5] Die große Mehrheit der österreichischen Betriebe, die Ein-Personen-Unternehmen und Kleinstunternehmen, unterliegt keinerlei verbindlicher Sicherheitsstruktur und hat in der Regel weder IT-Personal noch Budget für externe Beratung. Die Bevölkerung wiederum ist auf ein Nebeneinander von Informationsangeboten und Meldestellen angewiesen, die für die Betroffenen kaum unterscheidbar sind. Die vorhandenen Initiativen, etwa KMU.DIGITAL, die Cyber-Security-Hotline der Wirtschaftskammer, Watchlist Internet oder Saferinternet.at, leisten wertvolle Arbeit, sind aber überwiegend auf das bisherige Bedrohungsbild ausgerichtet.

Gegen KI-gestützte Angriffe hilft in erster Linie Wissen. Wer weiß, dass eine Stimme gefälscht sein kann, ruft zurück. Wer weiß, dass Sicherheitsupdates binnen Stunden eingespielt werden müssen, tut es. Aufklärung, Schulung und ein niederschwelliger technischer Grundschutz sind daher die wirksamste und zugleich kostengünstigste Maßnahme, um Schäden in Millionenhöhe zu verhindern. Sie sind eine gesamt-

---

[4] https://www.handelsblatt.com/politik/deutschland/kuenstliche-intelligenz-sicherheitsbehoerden-warnen-vor-welle-ki-gestuetzter-cyberattacken/100243667.html; Zusammenfassung u.a. https://www.it-boltwise.de/bsi-warnt-ki-kann-cyberangriffe-skalieren-und-sicherheitsluecken-automatisiert-ausnutzen.html

[5] Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie); nationale Umsetzung durch das Netz- und Informationssystemsicherheitsgesetz (NISG).

staatliche Aufgabe und es darf nicht dem Zufall überlassen bleiben, ob ein Betrieb oder eine Person auf das richtige Angebot stößt.

Die unterfertigenden Abgeordneten stellen daher folgenden

ENTSCHLIESSUNGSANTRAG

Der Nationalrat wolle beschließen:

„Die Bundesregierung, wird aufgefordert, eine nationale Sicherheits- und Aufklärungsoffensive gegen KI-gestützte Cyberkriminalität umzusetzen, die insbesondere folgende Maßnahmen umfasst:

1. Ein kostenloses, flächendeckendes Schulungs- und Beratungsangebot für Ein-Personen-Unternehmen sowie kleine und mittlere Unternehmen mit ausdrücklichem Schwerpunkt auf KI-gestützte Angriffe, in Zusammenarbeit mit den Wirtschaftskammern, dem Kuratorium Sicheres Österreich und CERT.at, etwa durch Erweiterung von KMU.DIGITAL um ein Cybersicherheitsmodul mit Beratungsgutscheinen und um praxisnahe Übungsformate wie simulierte Deepfake-Anrufe und Phishing-Tests.
2. Ein öffentlich zugängliches Frühwarnsystem, das aktuelle KI-gestützte Betrugsmaschen und aktiv ausgenutzte Sicherheitslücken zeitnah und in allgemein verständlicher Sprache an Unternehmen und Bevölkerung meldet, aufbauend auf den bestehenden Strukturen von CERT.at und Watchlist Internet.
3. Eine bundesweite Informationskampagne für die Bevölkerung, auch mit besonderem Augenmerk auf ältere Menschen, zu Stimm- und Videofälschungen, Deepfake-Erpressung, Sextortion und automatisiertem Anlagebetrug, verbunden mit einer einzigen, leicht merkbaren Anlaufstelle für Betroffene, die Meldung, Erstberatung und Weiterleitung an die zuständigen Stellen bündelt.
4. Die Verankerung der Erkennung KI-gestützter Betrugs- und Angriffsformen in der Digitalen Grundbildung an den Schulen sowie in der Erwachsenenbildung, insbesondere in den Volkshochschulen und in den Schulungsangeboten des Arbeitsmarktservice.
5. Eine jährliche Berichterstattung an den Nationalrat über Umfang und Entwicklung KI-gestützter Cyberangriffe in Österreich, über die Inanspruchnahme der genannten Angebote und über deren Wirkung, erstmals bis 30. Juni 2027."

In formeller Hinsicht wird die Zuweisung an den Ausschuss für Wissenschaft, Forschung und Digitalisierung vorgeschlagen.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2026-09-23T17:20:37+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	