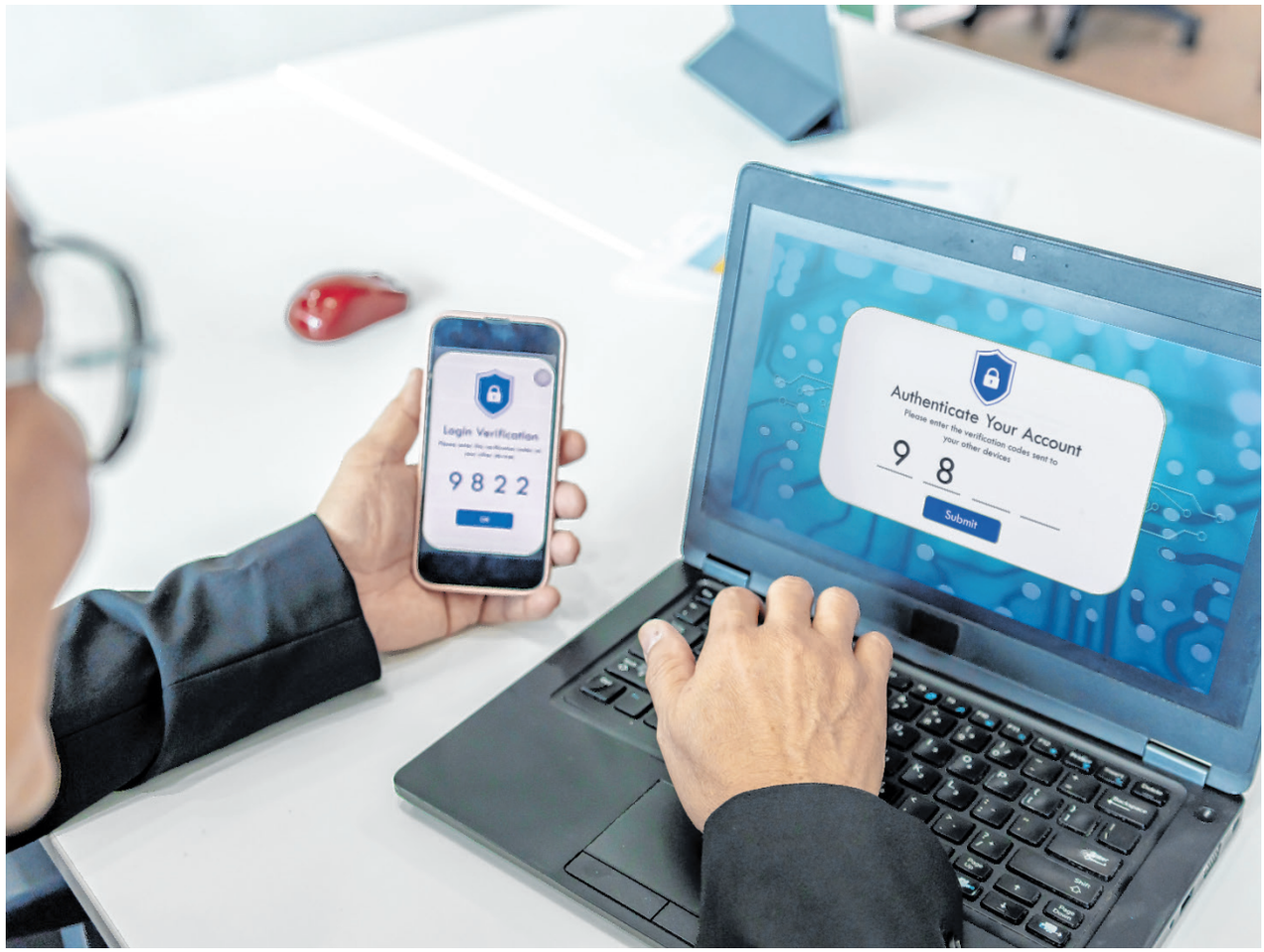
Wie sich Unternehmen gegen kriminelle KI schützen können

Moderne Cyberkriminelle nutzen KI auf vielfältige Weise, um Unternehmen zu schaden. Um sich dagegen zu schützen, braucht es einen mehrschichtigen Ansatz.

Oft setzen Cyberkriminelle hyperrealistische Phishing-Kampagnen ein, bei denen täuschend echte E-Mails im Namen von Vorgesetzten verschickt werden (CEO-Fraud). So gelingt es ihnen, Beschäftigte zur Freigabe von Zahlungen oder sensiblen Daten zu bewegen. Deepfake-Technologie ermöglicht es zusätzlich, gefälschte Video- oder Audioanrufe zu generieren – etwa um als vermeintliche Geschäftsführer Anweisungen zu erteilen. Im Finanzsektor gab es bereits Fälle, in denen Täter mit geklonten Stimmen Überweisungen in Millionenhöhe bewirkten.

Doch die Bedrohung geht weiter: KI kann Schadsoftware („Malware") erschaffen, die ständig ihren Code ändert, sodass sie schwer von Antiviren-Programmen erkannt wird. Ebenso automatisieren Kriminelle mit KI die Suche nach Schwachstellen in IT-Systemen. Bekannte Zielsysteme sind z. B. KI-Server, die mit Standardkomponenten und mangelhaften Konfigurationen oft leicht angreifbar sind. Auch das gezielte Manipulieren von Eingabedaten (Adversarial Attacks) oder das Umgehen von Sicherheitsmechanismen mit KI-optimierten Angriffen nehmen zu.



Kein Nutzer oder Gerät darf ohne Kontrolle Zugriff auf kritische Daten erhalten. Die Mehrfaktor-Authentifizierung setzt dafür einen modernen Sicherheitsstandard.

Foto: iStock/gahsoon

„Eine starke Verbindung der künstlichen und menschlichen Intelligenz ist in der digitalen Welt unerlässlich!"

Christoph Hofmann, stv. Datenschutzbeauftragter der Wirtschaftskammer Tirol

Konkrete Schutzmaßnahmen

Um sich gegen kriminelle KI zu wappnen, braucht es einen mehrschichtigen Ansatz. Technologisch empfiehlt sich der Einsatz von KI-gestützten Sicherheitssystemen: Sie erkennen verdächtige Anomalien und neue Angriffsmuster schneller als herkömmliche Tools. Die Einführung eines Zero-Trust-Modells sorgt dafür, dass kein Nutzer oder Gerät ohne zusätzliche Kontrolle Zugriff auf kritische Daten erhält. Mehrfaktor-Authentifizierung setzt hierfür einen modernen Sicherheitsstandard um.

Proaktiver Schutz ist Pflicht

Organisatorisch ist es unerlässlich, Mitarbeitende regelmäßig zu aktuellen Betrugsmaschen, Deepfakes und Social-Engineering-Methoden zu schulen. Simulierte Phishing-Tests und Notfallpläne mit klaren Eskalationsprotokollen bereiten auf echte Angriffe vor. Vor allem sollten Unternehmen den Zugriff auf sensible Informationen massiv einschränken – das Prinzip der Datensparsamkeit macht es Angreifern schwerer, personalisierte Angriffe vorzubereiten. Ergänzend bieten regelmäßige Sicherheits-Audits sowie die Bildung eines Incident-Response-Teams effektiven Schutz.

Die kriminelle Nutzung von KI bringt eine neue Qualität der Bedrohungslage mit sich. Unternehmen können sich dennoch effektiv schützen – durch technische Innovation, organisatorische Wachsamkeit und eine lückenlose Sensibilisierung aller Mitarbeitenden. Entscheidend ist ein ganzheitliches Sicherheitskonzept, das stets den technologischen Wandel im Blick behält und so kriminelle KI ausbremst, bevor sie größeren Schaden anrichten kann.