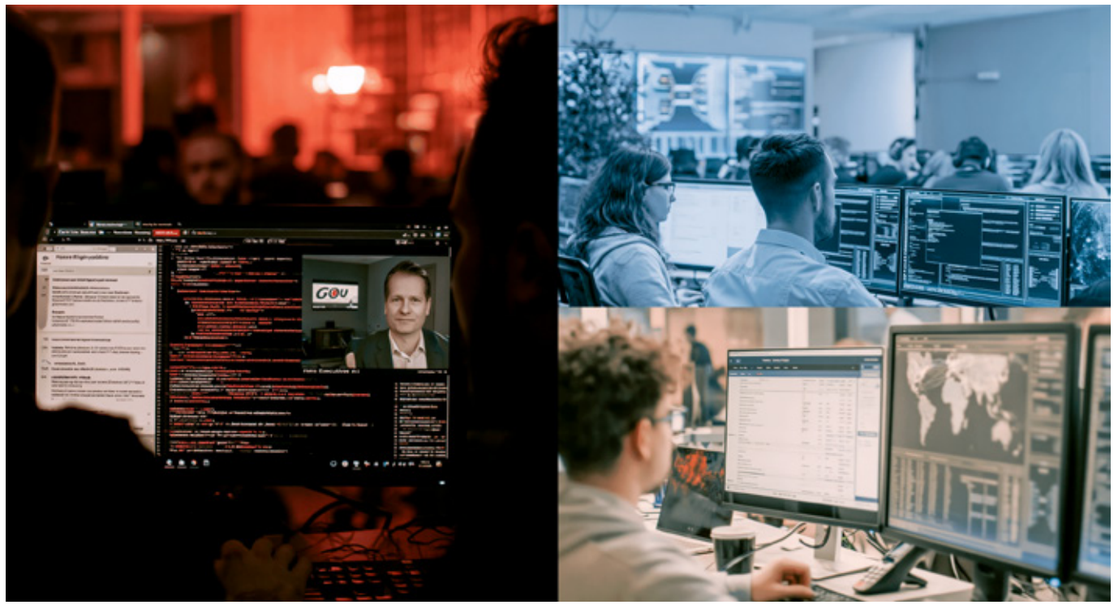

KI in der IT Sicherheit *Bild: RedCastle*

Wenn beide Seiten aufrüsten

Künstliche Intelligenz in der IT-Sicherheit: Heubacher RedCastle eG gibt Einblicke

Künstliche Intelligenz hat die IT-Sicherheit binnen weniger Monate verändert, und zwar für Angreifer wie für Verteidiger gleichermaßen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) spricht von einer „dualen" Wirkung. Dieselbe Technologie, die Unternehmen schützt, senkt zugleich die Einstiegshürden für Cyberkriminelle.

Was sich bei den Angriffen ändert

Am deutlichsten zeigt sich das heute beim Social Engineering. Phishing-Mails lassen sich nicht mehr an Rechtschreibfehlern erkennen. KI formuliert sie fehlerfrei, personalisiert und in jeder Sprache, in Sekunden und in großer Zahl. Dazu kommen Deepfakes. Gefälschte Stimmen oder Videos von Geschäftsführern werden bereits genutzt, um Mitarbeitende zu eiligen Überweisungen zu verleiten (CEO-Fraud).

Auch bei Schadsoftware hilft KI den Tätern. Große Sprachmodelle schreiben einfachen Schadcode und können Malware automatisiert so verändern, dass klassische Virenscanner sie schwerer erkennen. Vollautomatische KI-Angriffe, die ganz allein in Netzwerke eindringen, gibt es laut BSI allerdings noch nicht. Die nächste Stufe sind sogenannte KI-Agenten, die Aufgaben in mehreren Schritten selbstständig abarbeiten. Noch sind sie keine eigenständigen Angreifer, doch die Grenze verschiebt sich. Was sich heute schon massiv erhöht, sind Tempo, Menge und Qualität der Angriffe. Der BSI-Lagebericht 2025 mahnt zudem, dass Deutschland digital verwundbar bleibt, weil viele Organisationen schon einfache Angriffe zu wenig abwehren. Kleine und mittlere Unternehmen sind dabei ein beliebtes Ziel.

Was die Verteidigung gewinnt

KI hilft aber auch beim Schutz. Ein Security Operations Center (SOC), ein Leitstand für die IT-Sicherheit, wertet riesige Mengen an Log-Daten in Echtzeit aus, erkennt ungewöhnliches Verhalten und filtert Fehlalarme. So bleiben den Analysten die wirklich kritischen Vorfälle. Das ist gerade für kleine und mittlere Unternehmen wertvoll, die kein eigenes Team rund um die Uhr stellen können. Denn die meisten gezielten Angriffe erfolgen außerhalb der Geschäftszeiten.

Felix Wanner, SOC Operations Lead bei der RedCastle eG in Heubach.
Bild: RedCastle eG

Worauf Unternehmen jetzt achten sollten

Menschen schulen. Sensibilisieren Sie Ihr Team für KI-Phishing und Deepfakes. Eine einfache Regel hilft: Bei Zahlungs- oder Datenanforderungen immer über einen zweiten, bekannten Kanal rückversichern.

Schneller und proaktiv handeln. Sicherheitsupdates zeitnah einspielen und Systeme härten. Zudem aktiv nach Schwachstellen und Bedrohungen scannen. Wer langsam patcht, seine Systeme nicht überwacht und laufend prüft, bietet (automatisierten) Angriffen leichte Ziele.

Schatten-KI vermeiden. Mitarbeitende nutzen KI-Werkzeuge oft eigenmächtig. Geraten dabei Kunden- oder Geschäftsdaten in öffentliche Modelle, können sie ungewollt abfließen. Legen Sie fest, welche Tools erlaubt sind und welche Daten tabu bleiben.

Angriffe früh erkennen. Auf kontinuierliche Überwachung setzen, etwa Managed Detection and Response oder ein SOC, idealerweise rund um die Uhr.

Grundschutz sicherstellen. Mehr-Faktor-Authentifizierung überall, getestete und offline gespeicherte Backups sowie ein geübter Notfallplan.

KI selbst sicher nutzen. Wer KI im Unternehmen einsetzt, sollte vorab eine Risiko- und Datenschutzanalyse machen. Das BSI stellt dafür konkrete Kriterienkataloge bereit.

Fazit

KI ist kein Allheilmittel, aber auch keine reine Bedrohung. Worauf es ankommt, ist das Tempo. Angreifer werden schneller, also müssen Erkennung und Reaktion mithalten. Unternehmen, die ihre Mitarbeitenden schulen, den Grundschutz konsequent umsetzen und Angriffe frühzeitig erkennen, sind den neuen Methoden gewachsen. Die BSI-Präsidentin fasst es so zusammen: Es geht darum, mit den Angreifenden Schritt zu halten.

Die Genossenschaft bietet Managed Security Operations, IT-Forensik und Incident Response für den Mittelstand.

Autor: Felix Wanner

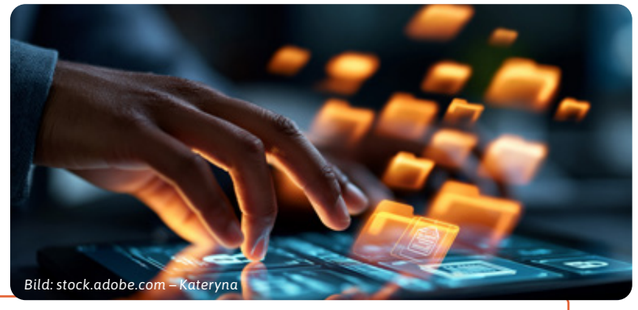

Bild: stock.adobe.com – Kateryna

Hürden auf dem Weg zu mehr Digitalisierung – eine Übersicht

- 61 % (2025): Fehlende Zeit als größtes Hemmnis
- 55 % (2025): Hohe Komplexität der Digitalisierung
- 42 % (2025): Finanzierungsprobleme

Strukturelle Hürden:

- 18 % (2025): Mangelhafte Infrastruktur bzw. unzureichende Internetanbindung
- 72 % (2025): Unternehmen haben grundsätzlich Zugang zu schnellem Internet

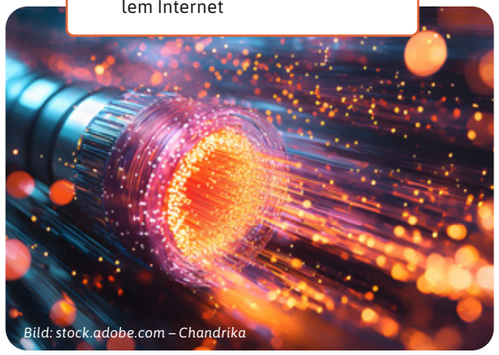

Bild: stock.adobe.com – Chandrika