Bild: Stock

Zwischen Risiko und Resilienz: KI in der ERP-Sicherheit

Nadine Rahman

Künstliche Intelligenz (KI) verändert die Spielregeln in der Cybersecurity – auch für ERP-Systeme. Dabei geht es weniger um völlig neue Entwicklungen als um eine deutliche Beschleunigung bestehender Mechanismen: Angriffe werden für bösartige Akteure skalierbarer, zielgerichteter und schneller anpassbar. Gleichzeitig entstehen auf der Verteidigerseite neue Möglichkeiten, Sicherheitsvorfälle mit KI frühzeitig zu erkennen, diese fundierter zu bewerten und entsprechend zu reagieren. Für Unternehmen ergibt sich daraus ein Spannungsfeld, das höchste strategische Relevanz hat.

ERP-Systeme stehen dabei im besonderen Fokus. Sie sind nicht nur technische Plattformen, sondern das Rückgrat zentraler Geschäftsprozesse. Entsprechend wirken sich Sicherheitsvorfälle hier unmittelbar auf operative Abläufe, finanzielle Stabilität und regulatorische Anforderungen aus – von möglichen reputativen Auswirkungen ganz zu schweigen. Die Frage, wie KI diese Systeme beeinflusst, ist daher keine rein technologische, sondern eine unternehmerische.

Angreifer setzen KI vor allem dort ein, wo sich bestehende Methoden effizienter skalieren lassen. Dazu zählen automatisierte Phishing-Kampagnen, die Erstellung realistischer Fake-Infrastrukturen oder die systematische Analyse potenzieller Schwachstellen.

Ein typisches Szenario: Mithilfe KI-gestützter Tools werden öffentlich verfügbare Informationen über ein Unternehmen aggregiert und strukturiert – etwa zu Organisationsstrukturen, Lieferketten oder eingesetzten Technologien. Auf dieser Basis lassen sich zielgerichtete Angriffskampagnen entwickeln, die deutlich präziser sind als klassische, opportunistische Massenangriffe. Gleichzeitig können KI-Systeme unterschiedliche Varianten solcher Angriffe automatisiert generieren und testen, um die Erfolgsquote kontinuierlich zu erhöhen.

Auch die Identifikation technischer Schwachstellen lässt sich beschleunigen. Bekannte Sicherheitslücken können automatisiert mit spezifischen Systemkonfigurationen abgeglichen werden. In Kombination mit öffentlich verfügbaren Exploit-Informationen entsteht so ein effizienter Mechanismus zur Priorisierung potenzieller Angriffspunkte.

Lesen Sie:

- inwiefern KI für ERP-Systeme zugleich Risiko und Chance darstellt
- wie Unternehmen ihre ERP-Sicherheit strategisch weiterentwickeln können

Entscheidend ist dabei weniger die Neuartigkeit einzelner Angriffe als deren Geschwindigkeit, Skalierbarkeit und Anpassungsfähigkeit. Diese Faktoren erhöhen insbesondere für komplexe Systemlandschaften wie ERP-Systeme die Angriffsintensität erheblich.

ERP als strukturell verwundbares Zielsystem

ERP-Systeme vereinen eine Vielzahl geschäftskritischer Funktionen – von Finanzprozessen über Logistik bis hin zur Produktionssteuerung. Gleichzeitig sind sie häufig über Jahre hinweg gewachsen und entsprechend komplex aufgebaut. Diese Kombination aus hoher Kritikalität und struktureller Komplexität macht sie besonders anfällig für Sicherheitsrisiken.

Mehrere typische Schwachstellen lassen sich dabei immer wieder beobachten:

- **Patch-Management vs. betriebliche Prozesse**
  Sicherheitsupdates stehen oft in direktem Konflikt

https://doi.org/10.58678/erp-information_26-2_33-36

mit Anforderungen an Stabilität und Verfügbarkeit. Gerade in produktionsnahen Umgebungen werden Patches daher teils verzögert eingespielt oder nur selektiv umgesetzt. Diese Praxis schafft länger bestehende Angriffsflächen, die bekannt und somit vermeidbar wären.

- **Unzureichend abgesicherter Custom Code**
  Individuelle Anpassungen des ERP-Systems sind für viele Unternehmen unverzichtbar, bringen jedoch zusätzliche Risiken mit sich. Häufig fehlt eine durchgängige Sicherheitsprüfung im Entwicklungsprozess, sodass Schwachstellen unentdeckt bleiben. Zudem erschwert mangelnde Transparenz über bestehende Anpassungen eine systematische Absicherung.

- **Fragmentierte Systemlandschaften und Schnittstellen**
  ERP-Systeme sind selten isoliert, sondern in eine Vielzahl von weiteren Anwendungen und Plattformen eingebunden. Jede Schnittstelle erweitert die potenzielle Angriffsfläche – insbesondere dann, wenn Sicherheitsstandards nicht konsequent umgesetzt werden.

- **Überkomplexe Berechtigungsstrukturen**
  Historisch gewachsene Rollenmodelle führen häufig zu übermäßigen oder schwer nachvollziehbaren Zugriffsrechten. Angreifer können solche Strukturen ausnutzen, um sich nach einem initialen Zugriff lateral im System zu bewegen.

Das Credo der Sicherheitsexperten: Reale Angriffsszenarien basieren selten auf einer einzelnen Schwachstelle. Vielmehr handelt es sich um Kombinationen mehrerer Faktoren, die zusammen ein ausnutzbares Risiko ergeben. So zeigte sich beispielsweise im Kontext kritischer Schwachstellen in ERP-nahen Plattformen – etwa bei der breit diskutierten Sicherheitslücke in SAP NetWeaver –, dass erfolgreiche Angriffe häufig nicht nur auf der initialen Schwachstelle basieren, sondern durch nachgelagerte Faktoren wie unzureichendes Patch-Management, unnötig weitreichende Berechtigungen oder zusätzliche unsichere Komponenten erst ihre volle Wirkung entfalten.

KI als Katalysator bestehender Risiken

Vor diesem Hintergrund fungiert KI primär als Verstärker bereits vorhandener Schwächen. Organisationen mit unzureichend integrierten Sicherheitsprozessen oder mangelnder Transparenz geraten stärker unter Druck, da bestehende Lücken schneller identifiziert und ausgenutzt werden können.

Gleichzeitig entsteht eine stärkere Differenzierung zwischen Unternehmen. Während einige Organisationen Schwierigkeiten haben, mit der Geschwindigkeit neuer Bedrohungen Schritt zu halten, können andere ihre Sicherheitsarchitektur gezielt weiterentwickeln und KI aktiv einsetzen.

Entscheidend ist dabei, dass KI nicht isoliert betrachtet wird. Sie entfaltet ihre Wirkung immer im Zusammenspiel mit bestehenden Prozessen, Technologien und organisatorischen Rahmenbedingungen. Organisationen, die auf spezialisierte Sicherheitslösungen setzen und ihre Systeme kontinuierlich überwachen, reduzieren diese Angriffsfläche jedoch deutlich.

Neue Angriffsflächen durch Digitalisierung und Lieferketten

Neben klassischen Angriffsszenarien rücken zunehmend auch indirekte Angriffsvektoren in den Fokus. ERP-Systeme sind eng mit digitalen Lieferketten verbunden – etwa über Entwicklungsplattformen, Cloud-Services oder externe Dienstleister. Ein denkbares Szenario ist die Kompromittierung von Softwarekomponenten innerhalb einer Entwicklungsumgebung. Werden solche Komponenten in ERP-nahe Anwendungen integriert, kann Schadcode unbemerkt in produktive Systeme gelangen. Gerade in modernen, stark vernetzten IT-Landschaften ist diese Art von Angriffen schwer zu erkennen, da sie nicht direkt auf das Zielsystem abzielen.

KI kann solche Angriffe sowohl erleichtern als auch verschleiern, etwa durch automatisierte Anpassung von Schadcode oder die gezielte Auswahl besonders wirkungsvoller Angriffspunkte. Für Unternehmen bedeutet das, dass Sicherheitsstrategien über das eigene ERP-System hinausgedacht werden müssen. Ein aktuelles Beispiel sind die Angriffe auf Entwicklungs- und Supply-Chain-Prozesse, bei denen kompromittierte Softwarepakete in Entwicklungsframeworks eingeschleust wurden. Angreifer versuchen gezielt, über Build-Pipelines oder abhängige Softwarekomponenten Zugriff auf sensible Systeme zu erlangen. Untersuchungen solcher Angriffsmuster durch Forschungsteams verdeutlichen, wie gefährlich diese indirekten Angriffspfade sind.

KI – nicht nur Gefahr, sondern auch Unterstützung

Trotz der steigenden Risiken bietet KI auf der anderen Seite auch erhebliche Potenziale für die Verbesserung der Sicherheitslage – insbesondere in ERP-Umgebungen, in denen technische und geschäftliche Zusammenhänge eng miteinander verknüpft sind.

Ein zentraler Anwendungsbereich ist das Schwachstellen- und Patch-Management. In vielen Unternehmen besteht nicht das Problem, dass Sicherheitsupdates nicht verfügbar sind, sondern dass ihre Umsetzung im Spannungsfeld zwischen Sicherheit und Systemverfügbarkeit verzögert wird. KI kann hier unterstützen, indem

sie Schwachstellen nicht nur nach technischen Kriterien bewertet, sondern in den jeweiligen Geschäftskontext einordnet. So kann sie beispielsweise priorisieren, welche Systeme oder Prozesse besonders kritisch sind, wo ein zeitnahes Patchen den größten Effekt hat und dies gegebenenfalls automatisiert umsetzen.

Darüber hinaus kann KI helfen, Risiken im Custom Code frühzeitig zu identifizieren. Durch automatisierte Analysen von Eigenentwicklungen und Erweiterungen lassen sich potenzielle Schwachstellen bereits im Entwicklungsprozess erkennen. Das reduziert nicht nur das Risiko im laufenden Betrieb, sondern verlagert Sicherheitsmaßnahmen stärker in Richtung „Security by Design".

Auch die kontinuierliche Überwachung von Veränderungen im System kann ein Einsatzbereich für KI sein. Gerade in ERP-Systemen führen Anpassungen und Updates regelmäßig zu neuen Risiken. KI-gestützte Analysen können dabei unterstützen, Auffälligkeiten zu erkennen und Veränderungen im Kontext bestehender Sicherheitsrichtlinien zu bewerten.

Schließlich gewinnen automatisierte, kontextbasierte Reports an Bedeutung. Sie ermöglichen es, technische Sicherheitsinformationen so aufzubereiten, dass sie auch für nicht-technische Stakeholder verständlich und entscheidungsrelevant sind. Für das Management entsteht dadurch eine kontinuierliche Transparenz über den Sicherheitsstatus und die Risikoentwicklung.

Grundlegend bleibt aber immer die Einordnung und Supervision dieser Punkte als zentrale Aufgabe erfahrener ERP- und Sicherheitsverantwortlicher. Künstliche Intelligenz ersetzt keine Sicherheitsstrategie, sondern unterstützt deren Umsetzung. Ihr Mehrwert liegt vor allem darin, Komplexität zu reduzieren und fundierte Entscheidungen zu ermöglichen – insbesondere in Umgebungen, in denen manuelle Prozesse an ihre Grenzen stoßen. Die abschließende Kontrolle kritischer Prozesse erfordert jedoch weiterhin menschliche Expertise.

Integration als zentrale Voraussetzung

Damit diese Potenziale in der Praxis wirksam werden, ist ihre Einbettung in bestehende Sicherheitsarchitekturen entscheidend. Im ERP-Umfeld zeigt sich dabei, dass isolierte KI-Anwendungen oder punktuelle Automatisierung selten ausreichen, um die Sicherheitslage nachhaltig zu verbessern.

Vielmehr kommt es auf den Einsatz spezialisierter Sicherheitslösungen an, die auf die Besonderheiten von ERP-Systemen ausgerichtet sind und KI gezielt dort einsetzen, wo sie den größten Mehrwert bietet – etwa bei der Analyse komplexer Systemlandschaften, der Bewertung von Schwachstellen


Bild: Stock

im Geschäftskontext oder der Überwachung von Änderungen und Zugriffen.

Diese Lösungen verbinden technische Analyse mit prozessualem und geschäftlichem Kontext. Sie ermöglichen eine konsolidierte Sicht auf Systeme, Schnittstellen und Benutzeraktivitäten und schaffen damit die Grundlage für fundierte Entscheidungen. Gleichzeitig unterstützen sie dabei, Sicherheitsmaßnahmen nicht nur reaktiv umzusetzen, sondern kontinuierlich zu priorisieren und weiterzuentwickeln.

Entscheidend ist dabei das Zusammenspiel mehrerer Ebenen:

- Technologie: Transparenz über Systeme, Datenflüsse und Abhängigkeiten
- Prozesse: klare Abläufe für Patching, Schwachstellenmanagement und Incident Response
- Organisation: definierte Verantwortlichkeiten und Governance-Strukturen

ERP-Sicherheit als strategische Managementaufgabe

Vor dem Hintergrund steigender Komplexität und neuer Bedrohungsszenarien entwickelt sich die Absicherung von ERP-Systemen zunehmend zu einer Managementaufgabe. Neben technischen Maßnahmen rücken dabei vor allem Transparenz, Priorisierung und die kontinuierliche Bewertung von Risiken in den Mittelpunkt – insbesondere in Umgebungen mit umfangreichem Custom Code, komplexen Berechtigungsstrukturen und einer Vielzahl an Systemänderungen.

Unternehmen stehen vor der Herausforderung, Sicherheitsrisiken nicht isoliert zu betrachten, sondern im Kontext geschäftskritischer Prozesse zu bewerten. Die zentrale Frage ist nicht nur, welche Schwachstellen existieren, sondern welche davon tatsächlich ein relevantes Risiko für den Geschäftsbetrieb darstellen und

https://doi.org/10.58678/erp-information_26-2_33-36

wie schnell darauf reagiert werden muss. Gerade im ERP-Umfeld erfordert diese Einordnung eine konsolidierte Sicht auf Systeme, Abhängigkeiten und laufende Veränderungen.

Hier zeigt sich, dass punktuelle Sicherheitsmaßnahmen oder generische Tools häufig nicht ausreichen. Vielmehr braucht es spezialisierte Ansätze, die technische Analyse mit geschäftlichem Kontext verbinden und eine kontinuierliche Bewertung ermöglichen – von der Identifikation über die Priorisierung bis hin zur Nachverfolgung der Durchführung von Maßnahmen.

KI kann in diesem Zusammenhang einen entscheidenden Beitrag leisten, indem sie große Datenmengen strukturiert auswertet, Zusammenhänge sichtbar macht und die Priorisierung unterstützt – etwa bei der Bewertung von Patches, der Analyse von Custom Code oder der Einordnung von Systemänderungen. Sie ersetzt jedoch nicht die Notwendigkeit klarer strategischer Leitlinien, sondern ermöglicht es, diese konsequenter umzusetzen.

Fazit: KI zwingt zu klaren Prioritäten

Künstliche Intelligenz verstärkt bestehende Stärken und Schwächen gleichermaßen. Für die ERP-Sicherheit bedeutet das: Nicht die Technologie allein entscheidet über das Risikoniveau, sondern der Reifegrad der zugrunde liegenden Prozesse und Strukturen.

Unternehmen, die weiterhin mit verzögerten Patch-Zyklen, intransparentem Custom Code und fragmentierten Sicherheitsansätzen arbeiten, erhöhen mit zunehmendem KI-Einsatz auf Angreiferseite ihr Risiko zusätzlich. Organisationen hingegen, die ihre ERP-Sicherheitsarchitektur konsequent weiterentwickeln, spezialisierte Security-Lösungen einsetzen und KI gezielt zur Analyse, Priorisierung und Entscheidungsunterstützung nutzen, können ihre Resilienz nachhaltig stärken.

Für das Management ergibt sich daraus eine klare Aufgabe: ERP-Sicherheit muss als integraler Bestandteil der Unternehmensstrategie verstanden und aktiv gesteuert werden. KI ist dabei weder Risiko noch Lösung per se – sondern ein Verstärker dessen, was bereits vorhanden ist. Wer diese Dynamik frühzeitig adressiert, verschafft sich einen entscheidenden Vorteil.

Nadine Rahman verantwortet als Head of International Go-To-Market (GTM) den internationalen Field Sales, die globale Go-to-Market-Strategie sowie den Ausbau des Partner- und SAP-Ökosystems. Sie verfügt über mehr als 20 Jahre internationale Führungserfahrung in über 30 Ländern, darunter CXO-Positionen in den Bereichen industrielle Automatisierung, SAP und im SAP-Ökosystem sowie eine fundierte technische Expertise als SAP-Projektberaterin und ABAP-Entwicklerin.

Onapsis
Nadine Rahman
Salomon-Calvi-Straße 1-3, 69124 Heidelberg
E-Mail: info@onapsis.com

Stichwörter:
KI, ERP-Sicherheit, SAP-Sicherheit, Cybersecurity, Resilienz