

KI Sicherheit: welche Maßnahmen sollten heute umgesetzt werden?

Ausblick auf die PwC Webinar-Serie mit IT-Security Impulsen für die chemisch-pharmazeutische Industrie



Webinar Teil 1



„KI Security – welche Maßnahmen sollten heute umgesetzt werden, um KI-Bedrohungen zu antizipieren?“

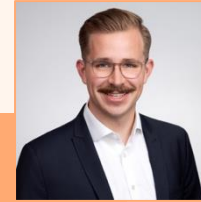


KI-Lösungen wie das Anthropic Modell „Mythos“ reduzieren die Zeit in den Schwachstellen ausgenutzt werden können von Tagen zu Stunden.

Gleichzeitig nimmt die Nutzung von KI in Unternehmen massiv zu, was neue Security-Herausforderungen erzeugt. Lernen Sie in unserem Webinar, was Sie heute angehen, sollten.

17.09.26: 10.00 – 11.00 Uhr

Webinar Teil 2



„Zero Trust: Wie sieht die Umsetzung in der chemisch-pharmazeutischen Industrie aus?“



Zero Trust ist mehr als ein Schlagwort, es beschreibt einen grundlegenden Paradigmenwechsel in der IT-Sicherheit.

Dieser Kurzvortrag erklärt die Funktionsweise der Zero Trust Architektur und ordnet sie in den Kontext der chemischen Industrie ein:

Welche spezifischen Herausforderungen gibt es, und wie gelingt eine praxisnahe Umsetzung?

22.10.26: 10.00 – 11.00 Uhr

Webinar Teil 3



„OT Security: Welche OT-Bedrohungen existieren für die chemisch-pharmazeutische Industrie?“



Industrielle Steuerungssysteme und Produktionsumgebungen stehen zunehmend im Fokus von Cyberangriffen.

Wir beleuchten die Besonderheiten der OT-Security, analysieren aktuelle Bedrohungsszenarien für die chemisch-pharmazeutische Industrie und stellen bewährte Ansätze zur technischen Absicherung vor.

19.11.26: 10.00 – 11.00 Uhr

Heute für Sie im Termin



Henning Kruse

Senior Manager
KI-Sicherheit



Düsseldorf



+49 151 52086063



henning.kruse@pwc.com

Agenda

1. Auswirkung von KI auf Cyberangriffe
2. Angriffe verhindern
3. Angriffe erkennen
4. Betrieb aufrechterhalten
5. Betrieb wiederherstellen
6. Umsetzungsplan
7. Q&A



Auswirkung von KI auf Cyberangriffe

KI erhöht die Geschwindigkeit von Angriffen und verändert dadurch die Cyber-Resilienz von Unternehmen

Leitfrage		Was KI verändert
1 Wie verhindern wir, dass ein Vorfall eintritt?	➔	KI skaliert Angriffe extrem: jedes Unternehmen wird zum Ziel; Angreifer gehen „in die Fläche“.
2 Wie erkennen wir einen Vorfall frühzeitig?	➔	Die Reaktions-Zeitfenster wird kürzer: klassische Cyber-Funktionen stoßen schneller an ihre Grenzen.
3 Wie erhalten wir kritische Prozesse aufrecht?	➔	Die Abhängigkeit von der IT steigt: KI wird noch tiefer in die Geschäftslogik integriert.
4 Wie kehren wir schnell und sicher zurück?	➔	Die Änderungsgeschwindigkeit steigt: Routinen veralten schneller und der Anpassungsbedarf steigt.
Resilienz wird zum Geschwindigkeitsproblem: Entscheidungen, Kontrollen und Wiederanlauf müssen mit der Geschwindigkeit der KI Schritt halten.		

Der Ablauf eines Cyberangriffs auf ein Unternehmen und der Einfluss von KI



KI erhöht das Angriffspotential, kann langfristig aber die Verteidigung skalieren

Kurzfristig

Risikobeschleunigung

Schnellere Angriffe



Schwerwiegendere Vorfälle



Versteckte Abhängigkeiten



Automatisierte Ausnutzung



Das Angriffspotential steigt

- 
- + Automatisierung
 - + Kontinuierliche Überwachung
 - + Menschliche Aufsicht

Langfristig

Vorteile für die Verteidigung

Kontinuierliche Transparenz



Bessere Erkennung



Automatisierte Reaktion



Reduzierter Erkundungsaufwand



Verteidiger skalieren mithilfe von KI

Unternehmen, die KI sicher integrieren, können die **Lücke zwischen der Geschwindigkeit von Angreifern und Verteidigern** verringern.

2

Angriffe verhindern

Prävention muss KI-Risiken frühzeitig einbeziehen



KI erweitert und verändert die Angriffsfläche



Das herkömmliche Risikomanagement berücksichtigt KI-spezifische Aspekte nicht



Einführung von KI-Komponenten durch Anbieter nach der Beschaffung



Cyber-Reife =

Verteidigungs-
maßnahmen
IT-Risiko

Führungskräfte
reagieren

Verteidigungsmaßnahmen
IT-Risiko + KI-Risiko

Wohin wir
gehen sollten

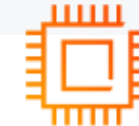
Verteidigungsmaßnahmen
Digitales Risiko

IT- und KI-Konvergenz

Anwendungen



Eingebettete KI



Allgegenwärtige
Funktionsfähigkeit



Da KI zunehmend in Unternehmensanwendungen integriert wird, wird KI-Sicherheit zur Unternehmenssicherheit



Ausblick: Künftige Cyberregulierung wird KI-Risiken voraussichtlich stärker berücksichtigen. KI-Sicherheit wird damit zum festen Bestandteil der Cybersicherheit.

Fünf Maßnahmen übersetzen den aktuellen Zeitvorteil in wirksame Prävention gegen KI-gestützte Angriffe

- 1 Angriffsfläche feststellen und bewerten** Erfassung der Schwachstellen und Exponiertheit über ein Assessment
- 2 Eigene Softwarelösungen prüfen** Anwendung von Frontier-KI zur Überprüfung der internen Lösungen und Angriffsflächen
- 3 Mitarbeitende schulen** Sichere KI-Nutzung verständlich und einfach umsetzbar erklären und sensibilisieren
- 4 Agile Steuerung** Dynamische Anpassung der Schutzmaßnahmen auf Basis von Bedrohung und IT
- 5 Verantwortlichkeiten klären** Klare Festlegung von KI-Verantwortung, Rollen für Prävention u. Reaktion

3

Angriffe erkennen

Früherkennung entsteht aus der aktiven Suche nach Bedrohungen in den Systemen, klaren Kontakten und einem beschleunigten SOC

1

Kompromittierungsanalysen

Threat Hunting statt reinem Alert-Fokus

- Hinweise auf Kompromittierung aktiv suchen
- Angriffspfade und Schwachstellen verkettet analysieren
- Neue KI-gestützte Taktiken kontinuierlich validieren

2

Security Operations und Service Provider beschleunigen

Mensch und KI gemeinsam messen

- KI-Wirkung auf Detektion und Analyse messen
- Angriffspfade und zeitbasiertes Risiko transparent machen
- Manuelle Wartezeiten reduzieren und Risikoreduktion steuern

3

Kontakte & Eskalation

Keine Zeit mit Zuständigkeiten verlieren

- Interne Ansprechpartner kommunizieren
- Provider- und Vendor-Kontakte aktuell halten und aktualisieren
- Eskalations- und Containment-Wege vorab abstimmen

Dialog mit Security-Partnern

Wo werden Tool-Fähigkeiten durch menschliche Vorgänge gebremst?

Wie haben sich Detektion und Analyse durch KI-Funktionen verbessert?

Wie werden verkettete Angriffspfade erkannt und dargestellt?

Welche Zeitannahmen liegen dem Risikoscoring zugrunde?

Werden Exploitability Window und % Auto-Remediation ausgewiesen?

4

Betrieb
aufrechterhalten

Betriebsfähigkeit braucht klare Regelungen für Angriffsszenarien statt langer Entscheidungsketten

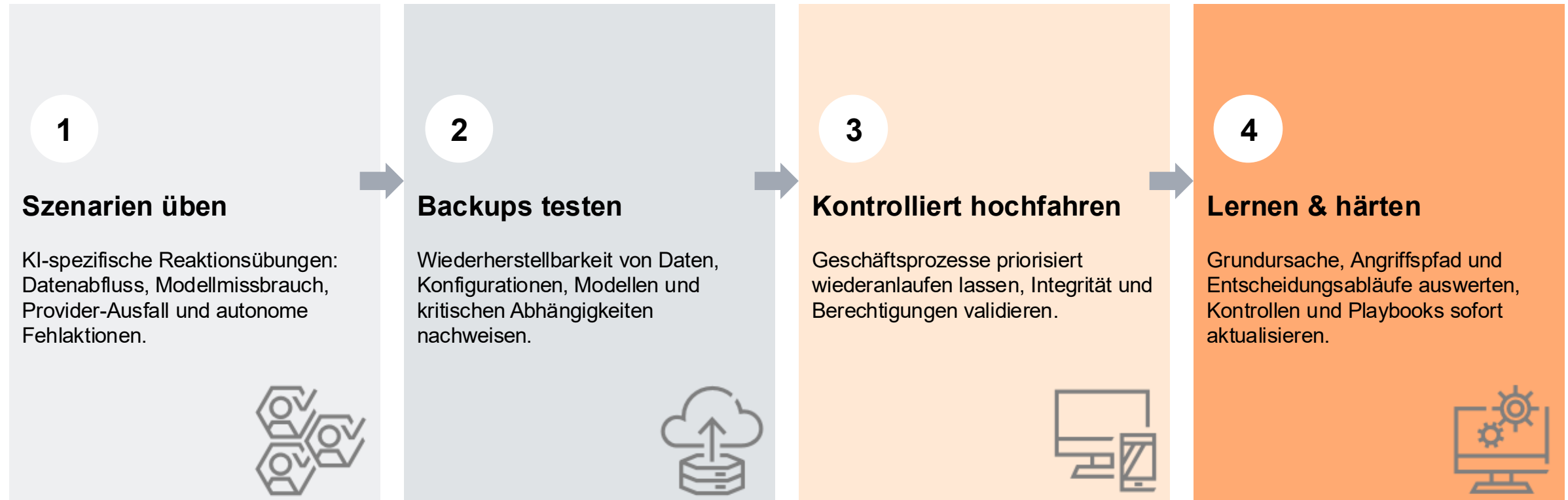


5

Betrieb
wiederherstellen

Wiederherstellung ist erst abgeschlossen, wenn Betrieb und Kontrollen verbessert sind

Wiederherstellen verbindet **technische Wiederanläufe** mit **geübten Entscheidungen** und **messbarer Risikoreduktion**.



6

Umsetzungsplan

KI-Sicherheit muss strategisch gesteuert und domänenübergreifend umgesetzt werden

Steuerung der Sicherheitsdomänen (ISMS)



KI-gestützte Cyberbedrohungen

KI-gestütztes Phishing, Deepfake-Betrug und automatisierte Angriffe

Angreifer nutzen adversarielle KI, um Schutzmaßnahmen zu umgehen

KI-Nutzung absichern

Sicherheitsgovernance sowie technische und organisatorische Maßnahmen auf KI anwenden

KI-Chancen für eine höhere Sicherheit nutzen

Domänenübergreifende Integration



Compliance & Regulatorik

Neue Vorgaben wie EU AI Act, NIST AI RMF und ISO 42001

Risikobasierte Klassifizierung von KI-Systemen und Compliance-Anforderungen

Recht, Datenschutz, & ethische Auswirkungen

Umgang mit personenbezogenen Daten in KI-Modellen (z. B. DSGVO)

Fragen zu Bias, Fairness, Transparenz und Verantwortlichkeit von KI

Strategische Überlegungen



Transformation der KI-Sicherheit

Belegschaft für KI befähigen und Einführung unterstützen
Sicheres KI-Engineering und Lifecycle-Management für die Entwicklung von KI-Anwendungsfällen

KI-Sicherheitsgovernance bereitstellen

Governance-Funktion für sichere KI-Implementierung und -Nutzung durch Richtlinien und Aufsicht

KI zur Stärkung von Zero Trust nutzen

KI-gestützte Zugriffskontrollen, Verhaltensanalysen und adaptive Sicherheit

KI-Sicherheit umsetzen

KI-gestützte Bedrohungen wie Deepfakes durch stärkeres Sicherheitsbewusstsein und interne Kontrollen adressieren

Schwerpunkte einer KI Sicherheits-Taskforce

01	Angriffsfläche steuern	Identifizieren und reduzieren Sie kontinuierlich Sicherheitslücken in Bezug auf Assets, Identitäten, APIs und KI-Agenten, bevor diese ausgenutzt werden können.	• Gefährdete Ressourcen • Schatten-KI / Agenten • Angriffswege über Identitäten
02	Intrusion Prevention	Setzen Sie Echtzeit-Kontrollen für Endgeräte, Netzwerke, die Cloud und Identitäten durch, um Bedrohungen direkt am Ort des Geschehens einzudämmen.	• Durchsetzung von Netzwerk- und Endpunkt-Richtlinien • Identitäts- und Zugriffskontrollen • Reduzierung des Schadensumfangs
03	Kompromittierung erkennen	Erkennen Sie proaktiv neue Angriffsmuster und verkettete Angriffspfade, die über statische Erkennungssysteme hinausgehen.	• Erkennung von verketteten Angriffen • KI-gestützte Erkennung von Bedrohungen • Kontinuierliche Validierung
04	Datensicherheit	Kontrollieren Sie den Zugriff auf Daten, deren Bewegung und Offenlegung sensibler Daten über KI-Workflows, Agenten und Systeme hinweg.	• Datenkennzeichnung und –klassifizierung • Datenzugriffskontrolle • KI-Datenflüsse • Verschleierung • Verhinderung von Datenlecks
05	Agile Steuerung	Ermöglichen Sie eine schnelle Entscheidungsfindung und die Umsetzung von Maßnahmen durch vorab genehmigte Eindämmungsmaßnahmen und KI-fähige Betriebsmodelle.	• Vorab genehmigte Eindämmungsmaßnahmen • Schnellere Entscheidungszyklen • Risikoorientierte Steuerung

Fünf Schritte schaffen die Grundlage für eine sichere und wirksame KI-Nutzung





Diskussion



Wir laden Sie
ein zum Dialog!

Q&A

Ausblick auf die PwC Webinar-Serie mit IT-Security Impulsen für die chemisch-pharmazeutische Industrie



Webinar Teil 1



„KI Security – welche Maßnahmen sollten heute umgesetzt werden, um KI-Bedrohungen zu antizipieren?“

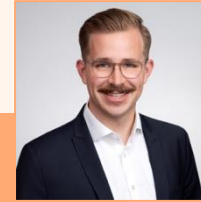


KI-Lösungen wie das Anthropic Modell „Mythos“ reduzieren die Zeit in den Schwachstellen ausgenutzt werden können von Tagen zu Stunden.

Gleichzeitig nimmt die Nutzung von KI in Unternehmen massiv zu, was neue Security-Herausforderungen erzeugt. Lernen Sie in unserem Webinar, was Sie heute angehen, sollten.

17.09.26: 10.00 – 11.00 Uhr

Webinar Teil 2



„Zero Trust: Wie sieht die Umsetzung in der chemisch-pharmazeutischen Industrie aus?“



Zero Trust ist mehr als ein Schlagwort, es beschreibt einen grundlegenden Paradigmenwechsel in der IT-Sicherheit.

Dieser Kurzvortrag erklärt die Funktionsweise der Zero Trust Architektur und ordnet sie in den Kontext der chemischen Industrie ein:

Welche spezifischen Herausforderungen gibt es, und wie gelingt eine praxisnahe Umsetzung?

22.10.26: 10.00 – 11.00 Uhr

Webinar Teil 3



„OT Security: Welche OT-Bedrohungen existieren für die chemisch-pharmazeutische Industrie?“



Industrielle Steuerungssysteme und Produktionsumgebungen stehen zunehmend im Fokus von Cyberangriffen.

Wir beleuchten die Besonderheiten der OT-Security, analysieren aktuelle Bedrohungsszenarien für die chemisch-pharmazeutische Industrie und stellen bewährte Ansätze zur technischen Absicherung vor.

19.11.26: 10.00 – 11.00 Uhr

Vielen Dank für Ihre Aufmerksamkeit.