# AI & Cybersecurity

Eine Anleitung für optimierte Sicherheit im Mittelstand durch den Einsatz von AI Solutions

# Executive Summary

Die Bedrohung durch Cyberangriffe ist real – 74 % der Unternehmen in Deutschland waren bereits betroffen. Insbesondere mittelständische Unternehmen sehen sich überfordert, da Ressourcen, Know-how und strukturierte Verteidigungsstrategien fehlen.

Gleichzeitig fehlen vielen Unternehmen Zeit, Fachkräfte und Budgets, um traditionelle Sicherheitsarchitekturen auf Enterprise-Niveau zu bringen.

Künstliche Intelligenz bietet hier einen echten Ausweg: Sie erkennt Bedrohungen frühzeitig, priorisiert automatisch nach Relevanz, unterstützt bei der Reaktion – und übersetzt komplexe Sicherheitslage in verständliche Maßnahmen.

Dieses Whitepaper zeigt, wie mittelständische Unternehmen mit Hilfe von Microsoft-Technologie und AI-gestützten Tools ihre Cybersicherheit deutlich steigern können – ohne unnötige Komplexität, aber mit klarer Struktur und messbarem Mehrwert.

Es erklärt:

- Wo AI im Bereich IT-Sicherheit konkret hilft – von Phishing-Erkennung bis Incident Reporting
- Welche Tools im Microsoft-Ökosystem bereitstehen (Defender, Sentinel, Copilot & Co.)
- Wie Data Governance als Sicherheitsbasis funktioniert
- Wie Unternehmen Schritt für Schritt in ein AI-gestütztes Security-Modell einsteigen können

Fazit: AI macht IT-Sicherheit nicht nur stärker – sondern auch smarter. Der Einstieg lohnt sich – besonders jetzt.

# Die Bedrohungslage im Mittelstand

Der deutsche Mittelstand steht zunehmend im Fokus von Cyberkriminellen. Angriffe wie Ransomware, CEO-Fraud, Phishing-Kampagnen und Social Engineering betreffen nicht mehr nur Großkonzerne, sondern immer häufiger auch kleine und mittlere Unternehmen (KMU). Der Grund: Viele KMU verfügen trotz wertvoller Datenbestände nicht über adäquate Sicherheitsstrukturen.

## Aktuelle Zahlen und Fakten aus 2024

### 81% betroffene Unternehmen

81 % der Unternehmen in Deutschland waren in den letzten zwölf Monaten von Datendiebstahl, Spionage oder Sabotage betroffen. Weitere 10 % vermuten dies.

### 266,6 Milliarden Euro Schaden

Der wirtschaftliche Schaden durch Cyberangriffe erreichte einen neuen Rekordwert von 266,6 Milliarden Euro, was einem Anstieg von etwa 29 % gegenüber dem Vorjahr entspricht.

### Existenzbedrohung

Zwei Drittel der Unternehmen fühlen sich durch Cyberangriffe in ihrer Existenz bedroht.

### 309.000 neue Schadprogramme täglich

Täglich werden durchschnittlich 309.000 neue Schadprogramm-Varianten registriert, was einen Anstieg von 26 % gegenüber dem Vorjahr bedeutet.

## Ursachen und Herausforderungen

Cyberkriminelle professionalisieren ihre Vorgehensweise kontinuierlich. Sie nutzen fortschrittliche Technologien und agieren aggressiv. Die Angriffe erfolgen häufig automatisiert und breit gestreut, sodass auch Unternehmen ohne spezifische Zielausrichtung betroffen sind.

Viele KMU haben Schwierigkeiten, mit der rasanten Entwicklung Schritt zu halten. Es fehlt oft an spezialisierten Ressourcen, um den wachsenden Herausforderungen der Cybersicherheit gerecht zu werden.

# Der wirtschaftliche Impact

Die finanziellen Auswirkungen von Cyberangriffen sind erheblich:

### Direkte Kosten

- Produktionsausfälle
- Lösegeldzahlungen
- Systemwiederherstellungen

### Indirekte Kosten

- Reputationsverlust
- Kundenabwanderung
- Rechtliche Konsequenzen

Diese Faktoren führen zu einer erheblichen Belastung für betroffene Unternehmen und können im schlimmsten Fall deren Existenz gefährden.

> Die Bedrohungslage im Mittelstand ist real und nimmt weiter zu. Es ist entscheidend, dass KMU proaktiv handeln, um ihre Sicherheitsstrukturen zu verbessern. Der Einsatz von Künstlicher Intelligenz kann dabei helfen, Bedrohungen frühzeitig zu erkennen und angemessen zu reagieren.

In den folgenden Kapiteln werden wir aufzeigen, wie der gezielte Einsatz von AI-Lösungen die Cybersicherheit im Mittelstand stärken kann.

# Was AI im Security-Kontext leisten kann

Künstliche Intelligenz ist in der Cybersicherheit längst mehr als ein Buzzword. Sie übernimmt heute zentrale Aufgaben in der Erkennung, Bewertung und Abwehr von Bedrohungen – schneller, präziser und ressourcenschonender als es klassische Security-Ansätze allein leisten können. KI ermöglicht signifikante Effizienzsteigerungen in der IT-Sicherheit durch automatische Bedrohungserkennung, Anomaliedetektion und automatisierte Incident Response.

Gerade für den Mittelstand, der unter Fachkräftemangel und begrenztem IT-Budget leidet, bietet AI-basierte Cybersicherheit eine reale Chance, das Schutzniveau deutlich zu erhöhen.

## Wo AI den Unterschied macht

| Einsatzbereich | AI-Funktion | Nutzen für den Mittelstand |
|---|---|---|
| Bedrohungserkennung | Verhaltensanalyse, Mustererkennung, Anomalie-Erkennung | Frühzeitige Erkennung von Angriffen, auch bei Zero-Day-Exploits |
| Risikobewertung | Priorisierung nach Risiko, Kontextanalyse | Entlastung der IT durch Fokus auf wirklich kritische Vorfälle |
| Automatisierte Reaktion | Isolation von Endpunkten, Blockieren verdächtiger Aktivitäten | Schnellere Eindämmung bei Vorfällen ohne manuelles Eingreifen |
| Phishing-Analyse | Echtzeitbewertung von E-Mails und Links | Schutz vor Social Engineering und CEO-Fraud |
| Security Copilot-Assistenz | Generative AI liefert Erklärungen, Empfehlungen und Reports | Verständliche Aufbereitung komplexer Security-Lagen |

# Vom Alarm zur Entscheidung – mit AI in Sekunden statt Stunden

Ein klassisches Security Operations Center (SOC) arbeitet oft mit hunderten Alerts pro Tag. Ohne Priorisierung führt das zu Überlastung und Blindstellen. AI schafft hier Klarheit:

### Kritische Vorfälle identifizieren

Welche Vorfälle sind wirklich kritisch?

### Sofortmaßnahmen erkennen

Wo muss sofort gehandelt werden?

### Automatisierung nutzen

Was kann automatisiert gelöst werden?

Durch diese intelligente Filterung und Automatisierung gewinnen IT-Teams wieder Kontrolle – und Zeit.

## Der Gamechanger: Generative AI trifft auf Security

Mit Tools wie dem Microsoft Security Copilot beginnt eine neue Phase:

- Analysten erhalten kontextbezogene Antworten in natürlicher Sprache
- Die AI kann selbstständig Playbooks entwerfen, Erklärungen liefern und Berichte generieren
- Bedrohungen werden nicht nur erkannt, sondern verständlich aufbereitet

Das macht Security nicht nur schneller, sondern auch zugänglicher – insbesondere für IT-Teams ohne dedizierte Security-Spezialisierung.

# Die wichtigsten Microsoft AI Security Tools im Überblick

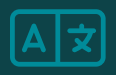
Microsoft hat in den letzten Jahren eine der leistungsfähigsten integrierten Sicherheitsplattformen weltweit aufgebaut – und verbindet klassische Cyberabwehr mit modernen AI-gestützten Funktionen. Das ist besonders relevant für mittelständische Unternehmen, die bereits Microsoft 365 einsetzen und nun ihr Sicherheitsniveau einfach und kosteneffizient steigern möchten.

## Überblick: Die Microsoft Security & AI Toolchain

| Tool / Plattform | Funktion und AI-Nutzen |
| --- | --- |
| Microsoft Defender XDR | Erkennung & Abwehr von Bedrohungen über E-Mail, Endpoints, Cloud, Identities hinweg – mit AI-gestützter Korrelation |
| Microsoft Sentinel (SIEM) | Zentrale Sicherheitsplattform mit Machine-Learning-Modulen zur Anomalie-Erkennung und automatisierten Reaktion |
| Microsoft Security Copilot | Generative AI unterstützt bei Analyse, Einschätzung und Dokumentation von Vorfällen (aktuell in Preview) |
| Entra ID (ehem. Azure AD) | Zugriffskontrolle mit AI-gestützter Risikobewertung von Login-Vorgängen und Identitäten |
| Intune + Defender for Endpoint | Gerätemanagement & Endpoint Protection mit AI-gestützter Bedrohungserkennung |
| Microsoft Purview | Klassifikation & Schutz sensibler Daten mit AI-gestützter Erkennung und Automatisierung von Richtlinien |

# Besonderheit: Microsoft Security Copilot

Der Security Copilot hebt IT-Sicherheit auf ein neues Niveau:



### Natürliche Sprache

Analysten können Fragen stellen wie „Was war die Ursache des letzten Angriffs?"

### Automatisierte Reports

Die AI generiert vollständige Incident-Reports inkl. Maßnahmenempfehlung

### Playbook-Integration

Standardisierte Reaktionswege werden auf konkrete Fälle angewendet – automatisch und reproduzierbar

Mit dem Microsoft Security Copilot lassen sich Sicherheitsvorfälle deutlich schneller analysieren und dokumentieren. Teams können über Spracheingabe Sicherheitsprobleme beschreiben und erhalten in Echtzeit Analysen und Handlungsvorschläge.

Das Ergebnis: Weniger Aufwand, mehr Wirkung – selbst in kleinen IT-Teams.

# Warum gerade Microsoft?

- Hohe Integration in bestehende M365- und Azure-Umgebungen
- Einheitliches Lizenzmodell (Microsoft Security kommt meist mit bestehenden Plänen)
- Skalierbar für KMU bis Enterprise
- Datenspeicherung in der EU (je nach Tenant-Region)
- Starke KI-Forschung durch Partnerschaft mit OpenAI

Microsoft bietet mittelständischen Unternehmen damit ein komplettes Sicherheits-Ökosystem – mit AI-Kompetenz, Integrationsfähigkeit und sofortigem Mehrwert im täglichen Betrieb.

# AI-basiertes Sicherheitskonzept in der Praxis

Ein gutes Sicherheitskonzept erkennt man nicht an der Anzahl der Tools – sondern an seiner Wirksamkeit. Für den Mittelstand heißt das: Effizienz vor Komplexität, Klarheit vor Perfektion. Die Kombination aus Künstlicher Intelligenz, Automatisierung und klaren Sicherheitsprinzipien bietet dabei einen enormen Hebel.

Dieses Kapitel zeigt, wie mittelständische Unternehmen mit überschaubarem Aufwand ein AI-basiertes Sicherheitskonzept umsetzen können – integriert in ihre bestehende Microsoft-Infrastruktur.

## Prinzip: Zero Trust + AI = Adaptiver Schutz

### Zero Trust

Vertraue niemandem – überprüfe alles.

### AI

Erkenne Muster – und reagiere schneller.

Gemeinsam ermöglichen beide Ansätze ein dynamisches Sicherheitsmodell, das sich ständig an neue Bedrohungen, Nutzerverhalten und Systemzustände anpasst.

## Schlüsselkomponenten eines AI-basierten Security-Konzepts

| Komponente | Umsetzung mit Microsoft AI Tools |
|---|---|
| Identität absichern | Entra ID + risikobasierte MFA + AI-Anomalieerkennung |
| Endgeräte schützen | Intune + Defender for Endpoint mit KI-gestützter Bedrohungserkennung |
| Daten klassifizieren & sichern | Microsoft Purview + DLP + Sensitivity Labels |
| Angriffe erkennen & reagieren | Microsoft Sentinel + Security Copilot |
| User sensibilisieren | AI-gestützte Phishing-Simulationen & Awareness-Kampagnen |

# Praxisbeispiele für den Mittelstand

### Automatische Phishing-Erkennung

AI erkennt verdächtige Mails anhand von Inhalt, Absender, Sprache und Metadaten. Verdächtige Nachrichten werden automatisch markiert oder blockiert – ohne manuellen Eingriff.

### Risikobasiertes Login-Management

Entra ID erkennt, wenn sich ein Nutzer von einem ungewöhnlichen Ort, Gerät oder unter Zeitdruck einloggt – und fordert z. B. eine zusätzliche Verifizierung oder blockiert den Zugriff.

### KI-gestützte Incident Reports

Der Security Copilot schreibt bei einem Angriff automatisch einen verständlichen Bericht: Was ist passiert? Was wurde blockiert? Was ist noch zu tun?

### Compliance Alerts in Echtzeit

Purview erkennt, wenn z. B. personenbezogene Daten in eine unsichere Umgebung verschoben werden – und blockiert oder protokolliert diesen Vorgang sofort.

### Security Awareness mit Chatbot-Assistenz

Ein unternehmensinterner AI-Chatbot kann Mitarbeitende schulen, Fragen beantworten („Was tun bei verdächtigen E-Mails?") und gezielt auf Risiken hinweisen.

Ein modernes Sicherheitskonzept ist kein zusätzliches Projekt – es ist die Weiterentwicklung bestehender Systeme mit Hilfe von AI. Gerade für den Mittelstand gilt: Wer jetzt beginnt, schützt sich nicht nur besser – sondern arbeitet auch effizienter.

# Data Governance als Voraussetzung für sichere AI

Die beste Security-Technologie nützt wenig, wenn die zugrunde liegenden Daten nicht kontrolliert, nicht klassifiziert oder ungeschützt sind. Data Governance wird zum Enabler von KI – denn nur klar klassifizierte, vertrauenswürdige und auditierbare Daten dürfen Grundlage automatisierter Entscheidungen sein. Gerade bei AI-gestützten Lösungen ist das Risiko hoch, dass sensible Daten ungewollt verarbeitet, gespeichert oder gar extern weitergegeben werden – z. B. durch Schatten-AI, schlecht konfigurierte Systeme oder fehlende Rollenmodelle.

Data Governance ist deshalb kein Widerspruch zu AI – sondern ihre Voraussetzung.

## Was bedeutet Data Governance im Security-Kontext?

- Wer darf was sehen, bearbeiten, löschen oder exportieren?
- Welche Daten gelten als besonders schützenswert – und warum?
- Welche AI-Systeme greifen auf welche Daten zu – und auf welcher Grundlage?
- Wie wird dokumentiert, überwacht und auditiert?

Die Antworten auf diese Fragen entscheiden, ob AI sicher und compliant eingesetzt werden kann – oder ob sie zum Risiko wird.

## Typische Probleme ohne Data Governance

| Schwäche | Risiko |
| --- | --- |
| Unklare Datenklassifikation | AI verarbeitet z. B. HR- oder Kundendaten ohne Schutzmaßnahmen |
| Fehlende Zugriffskontrollen | Ehemalige Mitarbeitende oder Gäste haben weiterhin Zugriff |
| Schatten-AI | Mitarbeitende nutzen externe Tools (z. B. ChatGPT) mit Firmendaten |
| Kein Logging & Monitoring | Es ist nicht nachvollziehbar, wer wann auf welche Daten zugegriffen hat |
| Keine Sensibilisierung der Nutzer | Fehlverhalten oder Missbrauch geschehen oft unbewusst |

# Die richtigen Tools für Data Governance im Microsoft-Ökosystem

### Microsoft Purview

Klassifizierung, Sensitivity Labels, DLP, Datenflusserkennung

### Simplify 365 Cleaner

Analyse & Bereinigung von Microsoft Teams: ungenutzte Kanäle, externe Zugriffe, Eigentümerkontrolle

### Entra ID

Zentrale Verwaltung von Identitäten, Rollen und Zugriffsrechten

### Microsoft Defender

Erkennung von ungewöhnlichem Datenverhalten und internen Risiken

## Governance ist kein „Projekt" – sondern ein Prozess

Wichtige Grundsätze:

- Klein starten, kontinuierlich verbessern
- Business & IT gemeinsam einbinden
- Governance in Tools & Prozesse „mitdenken" – nicht obendrauf setzen
- Auditierbarkeit sicherstellen – für AI Act, DSGVO & Co.

> Sichere AI ist nur auf der Basis sauberer Governance möglich. Wer den Schutz und die Kontrolle über seine Daten nicht beherrscht, gibt auch die Kontrolle über seine AI-Nutzung auf. Deshalb beginnt Cybersecurity nicht mit der Firewall – sondern mit der Datenstrategie.

# Einstieg, Skalierung und Kontrolle

Der Einsatz von AI in der Cybersicherheit muss nicht mit einem Big-Bang beginnen. Für mittelständische Unternehmen ist ein gestufter, kontrollierter Einstieg der nachhaltigste Weg: schnell erste Sicherheitsvorteile erzielen, Erfahrung aufbauen, dann gezielt skalieren. Dabei gilt: Transparenz, Schulung und Governance sind genauso wichtig wie die Technologie selbst.

## Drei Phasen zur erfolgreichen Einführung von AI-basierter Security

### Phase 1: Einstieg – Transparenz schaffen

- Status-Check: Welche Sicherheits-Tools sind vorhanden? Was ist aktiviert?
- Quick Audit mit Tools wie Simplify 365 Cleaner, Defender, Entra ID
- Klärung: Gibt es Schatten-AI? Welche Daten sind besonders kritisch?
- Erste Maßnahmen: Aktivierung KI-gestützter Schutzfunktionen (z. B. Phishing-Erkennung, risikobasierte Logins)

### Phase 2: Ausbau – Strukturen schaffen

- Einführung von Sensitivity Labels und DLP-Richtlinien mit Purview
- Start von Awareness-Kampagnen & Schulungen (z. B. über Microsoft Learn oder eigene AI-Chatbots)
- Integration von Microsoft Sentinel und ggf. Security Copilot in die Sicherheitsprozesse
- Klare Rollenverteilung: Wer verantwortet welche Sicherheitsbereiche?

### Phase 3: Kontrolle & Skalierung

- Automatisierte Reaktionen und Playbooks ausrollen
- Regelmäßige Reports und Audits zur Governance und Policy-Einhaltung
- Nutzung von AI zur Analyse interner Vorfälle („Was können wir daraus lernen?")
- Integration von Security-Kennzahlen in das Unternehmensreporting

## Wichtige Erfolgsfaktoren für den Mittelstand

| Faktor | Warum er entscheidend ist |
| --- | --- |
| Einheitliche Policies | Klare Regeln für alle – besonders bei wachsender Tool-Vielfalt |
| Benutzerfreundliche Tools | Akzeptanz steigt, wenn AI verständlich und integrierbar ist |
| Fortlaufende Schulung | Nur informierte Mitarbeitende können aktiv zur Sicherheit beitragen |
| Governance by Design | Sicherheit ist Teil des Prozesses – nicht „obendrauf" |
| Messbarkeit & Reporting | Fortschritt sichtbar machen und dokumentieren |

# Fazit & Empfehlungen

Der Mittelstand steht vor einer doppelten Herausforderung: steigende Cyberbedrohungen bei gleichzeitig begrenzten personellen und technischen Ressourcen. Klassische Schutzkonzepte stoßen dabei an ihre Grenzen – zu träge, zu unflexibel, zu reaktiv.

Mit dem gezielten Einsatz von Künstlicher Intelligenz können Unternehmen diesen Spieß umdrehen: von der passiven Verteidigung zur proaktiven, intelligenten Sicherheitsarchitektur – die schneller reagiert, besser priorisiert und Ressourcen schont.

## Was bleibt festzuhalten:

1 **AI schafft echten Mehrwert**

Nicht nur Automatisierung, sondern Kontext und Geschwindigkeit.

2 **Microsoft bietet ausgereifte Toolchain**

Mit Copilot, Defender, Sentinel & Co., die im Mittelstand sofort einsetzbar ist.

3 **Data Governance ist Voraussetzung**

Ohne klare Datenkontrolle keine sichere AI-Nutzung.

4 **Schatten-AI und unstrukturierte IT sind reale Risiken**

Transparenz ist der erste Schritt zur Besserung.

5 **Schrittweiser Einstieg bringt Erfolg**

Konkrete Use Cases bringen Sicherheit, Erfahrung und Akzeptanz.

## Unsere Empfehlungen für den Mittelstand

### Transparenz schaffen

IT- und Datenlage analysieren, Schatten-AI aufdecken, Tools aktivieren

### Grundlagen stärken

Data Governance etablieren, Zugriffskontrolle strukturieren

### Quick Wins nutzen

KI-gestützte Funktionen aktivieren (Phishing-Erkennung, Risikologins etc.)

### Mitarbeitende befähigen

Awareness fördern, Chatbots & Schulung integrieren

### Sicherheit messbar machen

KPIs definieren, Audits regelmäßig durchführen

Cybersicherheit ist kein Zustand, sondern ein Prozess – und AI ist der wichtigste Beschleuniger dieses Prozesses. Wer heute investiert, schützt nicht nur sein Unternehmen – sondern gewinnt Souveränität, Vertrauen und Zukunftsfähigkeit.

Die Bedrohung durch Cyberkriminalität ist real – aber sie ist beherrschbar. Mit einem strukturierten Ansatz, intelligenter Technologie und einem Partner, der den Mittelstand versteht, können Sie Ihre digitale Sicherheit auf ein neues Niveau heben.

Schreiben Sie uns an hero@365heroes.de und vereinbaren Sie ein unverbindliches Erstgespräch.

Sicherheit ist kein Zustand – sondern ein Prozess. Der richtige Zeitpunkt zum Handeln ist jetzt.