



KI im Arbeitsalltag: Wo Datenschutz und Datensicherheit kippen – und was Unternehmen jetzt tun müssen

Whitepaper, Oktober 2026

Inhalt

Executive Summary	3
Ausgangslage: KI-Euphorie und Wildwuchs	4
KI-gestützte Bedrohungen	5
Datenschutz-Fallstricke im Arbeitsalltag	7
Regulatorischer Rahmen	8
Was Unternehmen jetzt tun müssen — Checkliste	9
Fazit.....	10

Executive Summary

Künstliche Intelligenz hat in Unternehmen jeder Größe längst Einzug gehalten – oft schneller, als Regeln und Kontrollen mitwachsen können. Drei Risikofelder verschränken sich dabei: neue, KI-gestützte Angriffsvektoren, Datenschutzverstöße im ganz normalen Arbeitsalltag und neue gesetzliche Pflichten, die Unternehmen jetzt erfüllen müssen. Was alle drei Felder verbindet, ist der Faktor Mensch: Er entscheidet am Ende, ob der KI-Einsatz im Unternehmen sicher gelingt oder zum Einfallstor wird.

Dieses Whitepaper zeigt, wo die größten Risiken liegen – und was Unternehmen konkret tun können, um vorbereitet zu sein.

Ich wünsche Ihnen eine interessante Lektüre und stehe für Kommentare und Rückfragen gerne zur Verfügung.



Werner Grohmann

Geschäftsführer SecaSkill GmbH
(wg@secaskill.de)

Ausgangslage: KI-Euphorie und Wildwuchs

In den meisten Unternehmen nutzen Mitarbeitende KI-Tools längst im Alltag – oft, bevor die Geschäftsführung überhaupt Regeln dafür aufgestellt hat. Diese Lücke zwischen Praxis und Vorgabe ist kein Randphänomen, sondern mittlerweile der Normalfall.



Wir nennen dieses Phänomen Schatten-KI: den unkontrollierten, aber meist gut gemeinten Einsatz von KI-Tools ohne Freigabe oder Aufsicht. Schatten-KI entsteht dabei selten aus böser Absicht. Sie entsteht aus Effizienzdruck und fehlender Orientierung – Mitarbeitende wollen schneller arbeiten und greifen zu den Werkzeugen, die ihnen dabei helfen, unabhängig davon, ob diese Werkzeuge freigegeben sind.

Wir kennen dieses Spannungsfeld auch aus eigener Erfahrung – wenn auch mit anderer Ursache. 2019 wurden wir selbst Opfer eines Ransomware-Angriffs: Die Kosten beliefen sich auf rund 30.000 Euro, der Betrieb stand zwei Wochen still. Diese Erfahrung hat unseren Blick auf IT-Sicherheit grundlegend verändert – und ist der Grund, warum wir heute nicht nur aus der Theorie sprechen, sondern aus eigener Betroffenheit wissen, wie schnell ein einzelner Vorfall ein Unternehmen ins Wanken bringen kann. Die Bedrohungslage 2026 hat sich verschärft, aber das Grundproblem bleibt dasselbe: Sicherheit scheitert selten an der Technik allein, sondern an fehlender Vorbereitung der Menschen, die täglich mit dieser Technik arbeiten.

KI-gestützte Cybersecurity-Bedrohungen

Die Bedrohungslage hat sich 2026 grundlegend verändert – nicht graduell, sondern grundsätzlich. KI senkt die Einstiegshürde für Angreifer und erhöht gleichzeitig deren Erfolgsquote, und das lässt sich mittlerweile in Zahlen belegen.

So sind beispielsweise Voice-Phishing-Angriffe laut CrowdStrike Global Threat Report 2025 zwischen der ersten und zweiten Jahreshälfte 2024 um über 400 Prozent gestiegen. Der Grund: Eine geklonte Stimme lässt sich heute mit wenigen Sekunden Audiomaterial erzeugen – ein kurzer Videocall oder ein öffentlich zugängliches Podcast-Interview reichen bereits als Ausgangsmaterial.

Wie funktioniert Voice Cloning in der Praxis?

Moderne KI-Systeme können eine menschliche Stimme aus wenigen Sekunden Audiomaterial nachbilden – oft reicht ein kurzer Videoanruf, eine Sprachnachricht oder ein öffentlich zugängliches Interview als Ausgangsbasis. Die Software analysiert dabei charakteristische Merkmale wie Tonhöhe, Sprechrhythmus und Klangfarbe und erzeugt daraus ein digitales Stimmmodell, mit dem sich beliebige neue Sätze in der geklonten Stimme „sprechen“ lassen.

Für Angreifer ist das attraktiv, weil die Hürde denkbar niedrig ist: Es braucht weder technisches Spezialwissen noch teure Ausrüstung, sondern lediglich öffentlich verfügbares Audiomaterial – etwa von Firmenwebseiten, Social-Media-Videos, Podcasts oder Webinar-Aufzeichnungen. Genau das macht Führungskräfte, die öffentlich auftreten, besonders exponiert.

Für Unternehmen bedeutet das: Der Schutz kann nicht darauf beruhen, eine geklonte Stimme am Telefon zu erkennen – das gelingt selbst Fachleuten zunehmend schwer. Wirksam ist stattdessen ein organisatorischer Prozess, der unabhängig von der Stimme greift: eine zweite Bestätigung über einen separaten Kanal, etwa ein Rückruf auf einer bekannten, hinterlegten Nummer, bevor eine sensible Anweisung ausgeführt wird.

Auch beim klassischen Phishing verschiebt sich die Bedrohung. KI-generierte Phishing-Mails sind nicht nur häufiger, sie sind vor allem wirksamer: Sie erzielen eine Klickrate von 54 Prozent, gegenüber nur 12 Prozent bei manuell verfassten Nachrichten. Klassische Erkennungsmerkmale wie Grammatikfehler oder holprige Formulierungen, auf die Mitarbeitende bislang trainiert wurden, fallen als Warnsignal zunehmend weg.

Deutschland ist von dieser Entwicklung nicht ausgenommen: Deepfake-Betrugsversuche gegen deutsche Unternehmen haben laut Sumsb Identity Fraud Report (November 2025) im Jahresvergleich um 53 Prozent zugenommen.

Wie real dieses Risiko bereits ist, zeigt ein aktueller Fall aus Italien: Im Februar 2026 erhielt Paolo Molesini, frühere Führungskraft der Privatbank Fideuram (einer Tochtergesellschaft von Intesa Sanpaolo), eine WhatsApp-Nachricht, die angeblich vom Konzernchef stammte. Ein anschließender Anruf eines vermeintlichen Kanzleipartners – dessen Stimme per KI geklont worden war – veranlasste ihn zu mehreren Auslandsüberweisungen. Insgesamt wurden rund 95 Millionen Euro transferiert, 36 Millionen Euro blieben dauerhaft verschwunden. Unter anderem [DER SPIEGEL berichtete über den Fall](#).

Trotz dieser Entwicklung sind die meisten Unternehmen kaum vorbereitet: Laut einer Umfrage von Attestiv haben weniger als 30 Prozent bereits konkrete Schutzmaßnahmen gegen Deepfake-Betrug ergriffen, 46 Prozent sind komplett unvorbereitet. Genau hier setzt die Frage an, die uns zu den notwendigen Handlungsschritten führt: Was können Unternehmen konkret tun, um nicht zum nächsten Fall zu werden?

+400%

Anstieg Voice-Phishing
(CrowdStrike GTR 2025)

54% vs. 12%

Klickrate KI-Phishing vs.
handgeschrieben (Mimecast)

+53%

Deepfake-Betrug gg. deutsche
Unternehmen (Sumsub, Nov. 2025)

<30%

Unternehmen mit Schutzmaßnahmen
gg. Deepfake-Betrug (Attestiv)

Sind Sie im Ernstfall vorbereitet?

Ob Deepfake-Betrug oder klassischer Cyberangriff: Entscheidend ist, wie schnell und strukturiert ein Unternehmen reagiert. **Sie haben keinen (aktuellen) IT-Notfallplan?**

Wir helfen gerne – und erstellen für Sie Ihren individuellen IT-Notfallplan – kostenlos und sofort einsatzbereit. Damit Sie und Ihr Team im Ernstfall sofort wissen, was zu tun ist.

Jetzt kostenlosen IT-Notfallplan anfordern: security-awareness-toolbox.de/it-notfallplan-anfordern

Quellen: CrowdStrike Global Threat Report 2025; Mimecast-Klickratenstudie; Sumsub Identity Fraud Report (Nov. 2025); Attestiv-Umfrage; SPIEGEL-Berichterstattung zum Fideuram-Fall

Datenschutz-Fallstricke im Arbeitsalltag

Während Kapitel 2 zeigt, wie Angreifer KI gegen Unternehmen einsetzen, entsteht das zweite große Risikofeld im Inneren: durch den ganz alltäglichen, meist gut gemeinten Umgang der eigenen Mitarbeitenden mit KI-Tools.

Das typische Muster sieht so aus: Mitarbeitende kopieren Kunden- oder Personaldaten in öffentlich zugängliche KI-Tools, um sich Arbeit zu erleichtern – ohne sich der datenschutzrechtlichen Tragweite bewusst zu sein. Was als praktische Abkürzung gedacht ist, wird damit unbemerkt zum Datenschutzverstoß.

Drei Situationen, die sich in dieser oder ähnlicher Form in vielen Unternehmen abspielen:

Situation 1:

Eine Mitarbeitende im Kundenservice erhält eine komplexe Kundenanfrage und fügt die komplette E-Mail – inklusive Namen, Vertragsdaten und Anliegen – in ein öffentliches KI-Tool ein, um sich eine Antwort formulieren zu lassen. Die Kundendaten verlassen damit unkontrolliert das Unternehmen.

Situation 2:

Ein Mitarbeitender in der Personalabteilung lädt eingehende Bewerbungsunterlagen in ein KI-Tool hoch, um sie schneller vorzusortieren. Lebensläufe enthalten dabei regelmäßig besonders schützenswerte Daten – von Gesundheitsangaben bis zu Angaben zur Staatsangehörigkeit.

Situation 3:

Ein Vertriebsmitarbeitender lässt sich einen Vertragsentwurf mit vollständigen Kundendaten von einer KI zusammenfassen, um schneller in ein Kundengespräch zu gehen – ohne zu wissen, ob und wie diese Daten beim Anbieter des Tools weiterverarbeitet werden.

In keinem dieser Fälle handelt es sich um Vorsatz. Es handelt sich um die Lücke zwischen Praxis und Policy: Was Mitarbeitende im Arbeitsalltag tatsächlich tun, deckt sich nicht mit dem, was im Unternehmen offiziell erlaubt ist – häufig, weil es dazu noch gar keine klare Regelung gibt. Schatten-KI bedeutet damit nicht nur einen Kontrollverlust über Prozesse, sondern vor allem einen Kontrollverlust über Daten.

Genau diese Lücke zu schließen – durch klare Vorgaben und durch Regulatorik, die inzwischen ausdrücklich dazu verpflichtet – ist Thema des nächsten Kapitels.

Regulatorischer Rahmen

Die beiden vorangegangenen Kapitel zeigen, warum Unternehmen handeln sollten. Der Gesetzgeber lässt inzwischen wenig Spielraum, ob sie das auch tun: Seit 2025 gilt mit Artikel 4 des EU AI Act eine Schulungspflicht für Unternehmen, die KI-Systeme einsetzen. Aus einem „kann“ ist damit ein „muss“ geworden – Mitarbeitende, die mit KI-Systemen arbeiten, müssen über ein Kompetenzniveau verfügen, das den sicheren und verantwortungsvollen Umgang mit diesen Systemen ermöglicht.

Diese Pflicht steht nicht isoliert. Auch NIS2 und das deutsche Umsetzungsgesetz BSIG verlangen von Unternehmen regelmäßige Sensibilisierungsmaßnahmen – und binden die Verantwortung dafür ausdrücklich an die Geschäftsführung. Nach § 38 BSIG ist diese Verantwortung nicht delegierbar: Die Geschäftsführung kann die Umsetzung an Mitarbeitende oder externe Dienstleister übertragen, die Verantwortung dafür bleibt aber bei ihr.

Beide Regelwerke eint eine zentrale Anforderung: Eine einmalige Schulung reicht nicht aus. Verlangt wird ein wiederkehrender Prozess mit nachvollziehbarem Nachweis – wer geschult wurde, wann und mit welchem Ergebnis.

Für Unternehmen bedeutet das eine Verschiebung der Perspektive: Security Awareness ist kein IT-Thema mehr, das sich delegieren lässt, sondern eine Führungsaufgabe mit Dokumentationspflicht. Wer diesen Rahmen heute schafft, ist nicht nur regelkonform, sondern auch strukturell besser vorbereitet auf die Bedrohungen aus Kapitel 2 und die Datenschutzrisiken aus Kapitel 3 – ein Aspekt, der auch beim EU AI Act mitschwingt: die Betonung des Faktors Mensch als entscheidende Stellschraube für den sicheren KI-Einsatz.

Was folgt daraus für die tägliche Praxis? Das nächste Kapitel fasst das in konkrete Handlungsschritte.

Was Unternehmen jetzt tun müssen — Checkliste

Aus den vorangegangenen Kapiteln lassen sich vier konkrete Handlungsfelder ableiten:

1. Klare, schriftliche Vorgaben zur KI-Nutzung

Legen Sie mit einer KI-Richtlinie fest, welche KI-Tools im Unternehmen genutzt werden dürfen, welche Daten dabei niemals eingegeben werden dürfen, und wer im Zweifelsfall gefragt wird. Ohne diese Vorgabe bleibt Schatten-KI der Normalfall statt der Ausnahme.

Individuelle KI-Richtlinie für Ihr Unternehmen

Eine individuelle KI-Richtlinie schafft genau die schriftliche Grundlage, die hier gefordert wird – zugeschnitten auf Ihre Prozesse statt als generische Vorlage.

Jetzt individuelle KI-Richtlinie anfordern: security-awareness-toolbox.de/ki-richtlinie-anfordern

2. Regelmäßige, nachweisbare Schulung statt Einmalaktion

Sowohl der EU AI Act als auch NIS2/BSIG verlangen einen wiederkehrenden Prozess mit dokumentiertem Nachweis. Eine Kickoff-Schulung allein erfüllt diese Anforderung nicht.

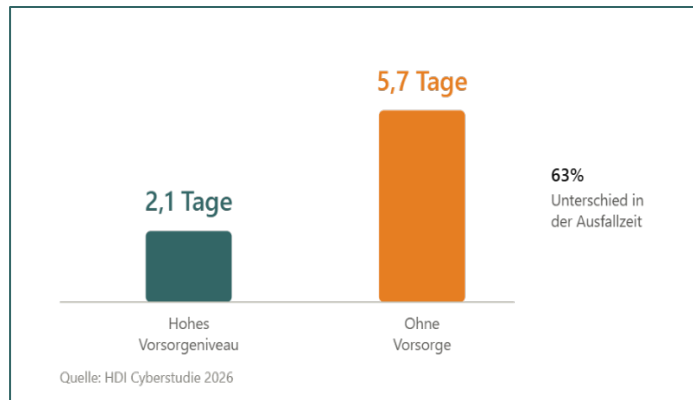
3. Sensibilisierung an echten Alltagssituationen ausrichten

Abstrakte Warnungen („Seien Sie vorsichtig mit KI“) verpuffen. Wirksam sind konkrete Situationen – wie die Beispiele aus Kapitel 3 – an denen Mitarbeitende ihr eigenes Verhalten erkennen. „KI und Datenschutz“ ist eines der zwölf Schulungsmodule der Security Awareness Toolbox.

4. Verifikationsprozesse für sensible Anweisungen etablieren

Wie in Kapitel 2 beschrieben, lässt sich ein Deepfake-Anruf nicht zuverlässig am Klang erkennen. Ein zweiter Bestätigungskanal – etwa ein Rückruf über eine bekannte, hinterlegte Nummer – wirkt unabhängig davon, wie überzeugend die Fälschung ist.

Dass sich Prävention auszahlt, belegen auch die Zahlen: Laut HDI-Cyberstudie 2026 kommen Unternehmen mit hohem Vorsorgeniveau nach einem Cyberangriff im Schnitt mit 2,1 Tagen Ausfallzeit aus – Unternehmen ohne entsprechende Vorsorge benötigen 5,7 Tage. Das ist ein Unterschied von 63 Prozent, und er entsteht nicht durch bessere Technik allein, sondern durch Menschen, die im Ernstfall wissen, wie sie reagieren müssen.



Was würde Sie ein Cyberangriff kosten?

Mit unserem kostenlosen Schadensrechner ermitteln Sie per Mausklick, welche Kosten ein Sicherheitsvorfall für Ihr Unternehmen konkret verursachen könnte – als erste Orientierung für Ihre Vorsorge.

Jetzt Schadensrechner nutzen: security-awareness-toolbox.de/schadensrechner

Fazit

Der Faktor Mensch bleibt entscheidend – auch und gerade im KI-Zeitalter. Die Bedrohungen werden raffinierter, die Datenschutzrisiken alltäglicher, und die gesetzlichen Anforderungen verbindlicher. Was sich nicht ändert, ist der Kern der Lösung: Mitarbeitende, die wissen, worauf sie achten müssen, und Prozesse, die auch dann greifen, wenn die Täuschung überzeugend ist.

Wer diesen Weg jetzt geht, ist nicht nur besser geschützt, sondern auch auf dem aktuellen Stand der regulatorischen Anforderungen.

Über den Autor:

Werner Grohmann ist Gründer und Geschäftsführer der [SecaSkill GmbH](https://www.seca-skill.de) in Freiburg im Breisgau. Mit über 20 Jahren IT-Erfahrung unterstützen er und sein Team kleine und mittlere Unternehmen dabei, die wachsenden Anforderungen im Bereich Mitarbeitersensibilisierung zu Datenschutz und Datensicherheit („Security Awareness“) zu meistern.