

# Schutz vor KI-verstärkten Cyberangriffen

Was Inhaberinnen und Inhaber kleiner Betriebe jetzt wissen und tun sollten.

---



ANGRIFFSSZENARIO: KI-GESTÜTZTE PHISHING UND DEEFAKE-KOMBINATION (CHEF-BETRUG)

## Dienstag, 09:32 Uhr

Eine Mitarbeiterin der Buchhaltung öffnet eine E-Mail, die aussieht wie die Rechnung eines bekannten Lieferanten. Der Anhang installiert im Hintergrund ein Schadprogramm, mit dem sich die Angreifer Zugriff auf das E-Mail-Postfach verschaffen. Unbemerkt lesen sie mehrere Tage mit: die Kommunikation mit Kunden, den Tonfall der Chefin – und den Kalendereintrag, dass sie freitag-nachmittags beim Sporttraining ihres Kindes ist.

## Freitag, 15:47 Uhr

Die Buchhaltung bekommt einen Anruf. Die Stimme: eindeutig die Chefin. Gestresst verlangt sie, sofort 18.500 Euro zu überweisen. Die Mitarbeiterin kennt diese Stimme seit Jahren und überweist. Die echte Chefin sitzt beim Sporttraining, ihr Handy ist aus. Wenige Sekunden aus einem alten Firmenvideo reichten, um ihre Stimme nachzubilden – in Deepfake. Die Angreifer wussten durch den Hackerangriff, wann sie zuschlagen mussten.

# KI-verstärkte Angriffe betreffen alle Unternehmen

Künstliche Intelligenz (KI) macht nicht nur die eigene Arbeit leichter – sie verbessert auch die Werkzeuge von Cyberkriminellen. Gefälschte Stimmen und Videos (Deepfakes), täuschend echte Phishing-Mails und automatisierte Angriffe werden dadurch häufiger und schwerer zu erkennen. Das betrifft nicht nur große Unternehmen: Kleine Betriebe sind oft sogar ein leichteres Ziel, da Schutzmaßnahmen und Sensibilisierung dort seltener vorhanden sind.

## Cybersicherheit: Das ist Chefinnen- und Chefsache!

KI- und Cyberrisiken gehören ins unternehmerische Risikomanagement. Oberste Priorität hat, einen Angriff gar nicht erst erfolgreich werden zu lassen – erst danach geht es um Schadensbehebung. Diese drei Schritte gehören dazu:



### Risikovorsorge

Schutzmaßnahmen, bevor etwas passiert ergreifen



### Notfallmanagement

Im Ernstfall, Abläufe kennen und klar kommunizieren



### Wiederherstellung

Maßnahmen kennen, um rasch wieder handlungsfähig zu sein

Gut vorbereitet lässt sich der Schaden gering halten, aber absolute Sicherheit gibt es nicht. Gleichzeitig ist KI auch eine Chance: Richtig eingesetzt hilft sie, Angriffe früher zu erkennen.

## Selbsttest: drei Leitfragen

JA NEIN

Wissen Sie, welche KI-Tools in Ihrem Betrieb genutzt werden und welche Daten dabei eingegeben werden?

☐ ☐

Würde Ihr Team eine gefälschte Chef-Stimme am Telefon erkennen?

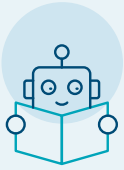
☐ ☐

Könnte Ihr Betrieb nach einem erfolgreichen Cyberangriff innerhalb eines vertretbaren Zeitraums wieder arbeiten?

☐ ☐

→ Haben Sie hauptsächlich „nein“ angekreuzt? Wir helfen Ihnen mit passenden Sofortmaßnahmen auf dieser und der nächsten Seite weiter.

# Jetzt handeln – drei Sofortmaßnahmen:



## 1. KI-Nutzung im Betrieb regeln

Viele Mitarbeitende nutzen bereits KI-Tools wie ChatGPT – oft ohne klare Absprache.

- ☐ Mitarbeitende über Chancen und Risiken aufklären und den Austausch im Team dazu fördern, zum Beispiel durch Schulungen.
- ☐ Festlegen, welche KI-Tools genutzt werden dürfen.
- ☐ Regeln für den Umgang mit Kunden-, Mitarbeiter- und Firmendaten sowie für die Bearbeitung von Inhalten mit KI-Tools definieren.
- ☐ Je nach Unternehmensgröße eine verantwortliche Person für das Thema benennen.

**Wichtig:** Auch ohne eigene KI-Nutzung sind Betriebe vor KI-gestützten Cyberangriffen nicht sicher – die übrigen Maßnahmen gelten unabhängig davon.



## 2. Schutz vor Deepfakes und KI-Phishing

Cyberkriminelle nutzen KI für überzeugende Chef-Anrufe (Deepfakes) und personalisierte Phishing-Mails, so schützen Sie Ihr Unternehmen:

- ☐ Offene Fehlerkultur: Vorfälle im Betrieb offen ansprechen und gemeinsam daraus lernen, statt Schuldzuweisungen zu machen.
- ☐ Bei ungewöhnlichen, dringenden Anfragen: Selbst Rückruf initiieren über einen anderen, bekannten und sicheren Kanal – nicht über die Nummer oder Adresse aus der verdächtigen Nachricht. Idealerweise geheimes „Signalwort“ mit Geschäftsführung zur Identifikation vereinbaren.
- ☐ Mitarbeitende anhand von Beispiel-Mails regelmäßig für Phishing sensibilisieren – eine einmalige Schulung reicht nicht.
- ☐ Vier-Augen-Prinzip bei Überweisungen und sensiblen Daten verbindlich einführen.



## Technische Basics umsetzen

Die meisten Angriffe nutzen keine hochentwickelten Methoden, sondern bekannte Sicherheitslücken. Die drei wichtigsten technischen Basics sind:

1

### Patchen, patchen, patchen

Sicherheitsupdates für Kassensystem, Buchhaltungssoftware, Router & Co. sofort einspielen, sobald sie verfügbar sind – das schließt bereits die meisten Einfallstore.

2

### Multi-Faktor-Authentifizierung

Zusätzlichen Anmeldecode per App oder SMS für E-Mail, Online-Banking und wichtige Programme aktivieren. Für alle Mitarbeitenden pflichtmäßig einführen.

3

### Sicherheitskontakt einrichten ([security.txt](#))

Eine kleine Textdatei auf der eigenen Webseite, über die Sicherheitsforschende Schwachstellen melden können. Gilt für jede Firmenwebsite – der Aufwand ist gering. Wird die Website extern betreut, sollte der Kontakt des Dienstleisters hinterlegt werden, nicht der eigene. Details im [Flyer zur security.txt](#) der Allianz für Cyber-Sicherheit.

- ☐ Beim Kauf von Hard- und Software auf Sicherheitssiegel (z. B. IT-Sicherheitskennzeichen des BSI) und DSGVO-Konformität achten, ebenso beim Sicherheitsniveau externer Dienstleister (IT-Betreuer, Cloud-Anbieter).
- ☐ Backups regelmäßig testen, Notfallplan und Ansprechpartner festlegen – dafür eignet sich die IT-Notfallkarte der Allianz für Cybersicherheit.

## WEITERFÜHRENDE INFORMATIONEN:

[BSI-CyberRisikoCheck](#)  
für KMU durch qualifizierte  
IT-Dienstleister.

[Management von Cyber-Risiken](#)  
Handbuch für die Chefetage der  
ACS.

[BSI-IT-Notfallkarte](#)  
„Verhalten bei IT-Notfällen“  
Aushang für den Betrieb.

[BSI-Cybersicherheit für KMU](#)  
Grundlagen der IT-Sicherheit in  
14 FAQs.

[BSI- Weg in die Basis-Absicherung](#)  
Kostenlose Checklisten zur Selbst-  
prüfung.

Diese Publikation entstand in Zusammenarbeit mit:

