IT-Sicherheit im KMU

Bedrohungslage 2025/26 · KI im Social Engineering · Schutzmaßnahmen

Stand: Juli 2026

Es ist klug und weise an allem zu zweifeln. Voltaire

ITSR
die hammer agentur

ÜBERBLICK

Agenda

ITSR
die hammer agentur

01 **Bedrohungslage 2025/26 in Zahlen**
Schäden, Betroffenheit, Trends

02 **KMU im Fadenkreuz**
Warum gerade kleine und mittlere Unternehmen?

03 **Phishing im KI-Zeitalter**
KI-Mails, Quishing, Messenger, gefährliche Anhänge

04 **KI im Social Engineering**
Deepfakes, Voice Cloning, CEO-Fraud

05 **Fallbeispiele aus der Praxis**
Arup, Fasana, ZEGO – reale Folgen

06 **Schutzmaßnahmen & Fazit**
Technik, Prozesse, Verhalten

Bedrohungslage 2025/26 in Zahlen

289,2 Mrd. €

Gesamtschaden für die deutsche Wirtschaft 2025 – Rekordwert, +8 % zum Vorjahr (Bitkom)

87 %

der deutschen Unternehmen waren von Datendiebstahl, Spionage oder Sabotage betroffen

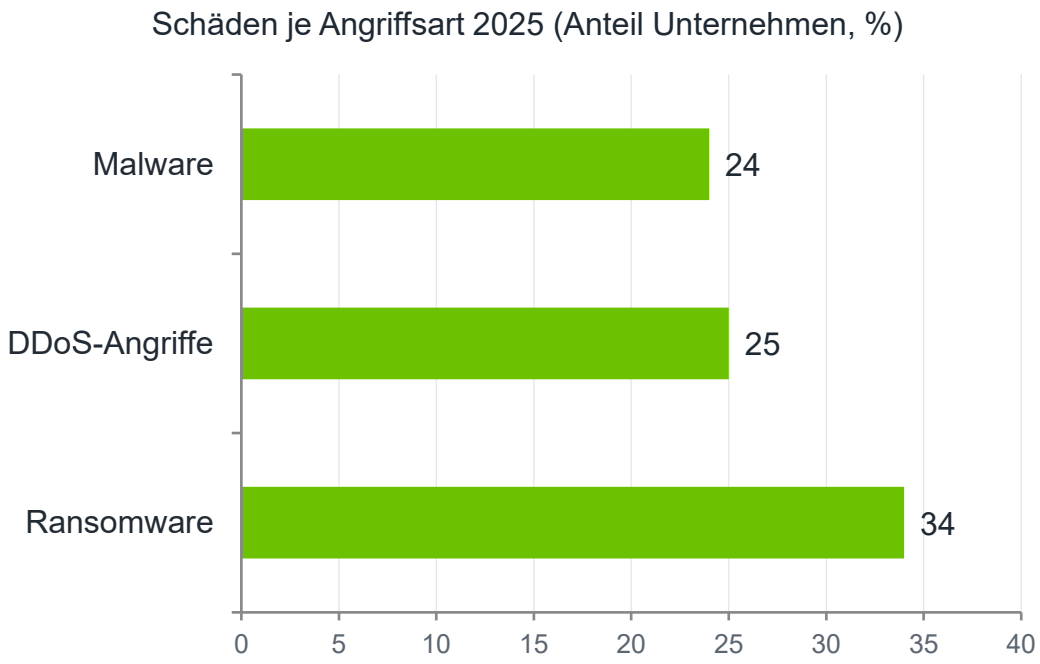
119 / Tag

neu bekannt gewordene Schwachstellen – +24 % gegenüber dem Vorjahr (BSI-Lagebericht 2025)

Cyberangriffe allein: 202,4 Mrd. € Schaden (70 % des Gesamtschadens). 46 % der Angriffe werden jeweils Russland und China zugeordnet.

WARUM GERADE WIR?

KMU im Fadenkreuz



Quelle: Bitkom Wirtschaftsschutz 2025

80 % der Ransomware-Angriffe — treffen kleine und mittlere Unternehmen (BSI / BKA)

+91 % Cyber-Erpressung — in Deutschland binnen eines Jahres – KMU bis 250 Mitarbeitende sind die Hauptopfer

Kein eigenes Security-Team — flache Hierarchien und kurze Wege werden bei CEO-Fraud zur Schwachstelle

15 % zahlten bereits Lösegeld — typisch 100.000–500.000 € pro Fall – hohe Dunkelziffer

DIE REGELN HABEN SICH GEÄNDERT

Phishing im KI-Zeitalter

Diese Warnsignale verschwinden

- **Rechtschreib- und Grammatikfehler**
KI schreibt fehlerfrei – in jeder Sprache und im Stil des Absenders.
- **Unpersönliche Massen-Mails**
KI personalisiert automatisiert aus LinkedIn, Website & Social Media.
- **Plumpe, unglaubwürdige Geschichten**
Vorwände passen zu echten Projekten, Kollegen und Terminen.

Darauf kommt es jetzt an

- **Absender-Domain exakt prüfen**
Zeichendreher, fremde Domains, abweichendes Reply-To.
- **Druck & Dringlichkeit hinterfragen**
„Streng vertraulich, sofort, nur Sie“ bleibt das stärkste Warnsignal.
- **Zweitkanal-Verifikation als Standard**
Zahlungen & Datenfreigaben nie allein aufgrund einer Mail auslösen.

Analysten registrierten Ende 2025 einen Sprung KI-unterstützter Phishing-Angriffe von 4 % auf 56 % – binnen eines Monats.

SO SIEHT DAS HEUTE AUS

Beispiel: KI-generierte Phishing-Mail

ITSR
die hammer agentur

Neue Nachricht

Von: Sandra Weber <s.weber@itsr-gmbh.de>
An: buchhaltung@ihre-firma.de
Betreff: AW: Projekt Hallenbau – geänderte Bankverbindung Schlussrechnung

Hallo Frau Maier,

wie eben mit Herrn Schuster telefonisch besprochen: Für die Schlussrechnung im Projekt Hallenbau hat sich unsere Bankverbindung geändert (Umstellung auf unser neues Geschäftskonto). Bitte überweisen Sie den offenen Betrag von 48.350,00 € bis Freitag auf die unten stehende IBAN, damit die Skontofrist gewahrt bleibt.

Vielen Dank für die schnelle Abwicklung – und viele Grüße auch an das Team!

Sandra Weber · Leitung Rechnungswesen

Warum diese Mail so gefährlich ist

Fehlerfrei & persönlich
korrekte Namen, echtes Projekt, passender Ton – aus öffentlichen Quellen per KI zusammengesetzt

Nahezu echte Domain
itsr-gmbh.de statt der echten Firmendomain – nur ein Detail weicht ab

Plausibler Vorwand
„geänderte Bankverbindung“ ist die häufigste Betrugsmasche im Rechnungswesen

Zeitdruck mit Begründung
Skontofrist statt plumper Drohung – Dringlichkeit wirkt geschäftlich normal

Einzig sicherer Check: Rückruf unter der bekannten Nummer – nie unter der Nummer aus der Mail.

Angriffe jenseits der E-Mail

QR-Code-Phishing (Quishing)

QR-Codes in Mails, auf Briefen, Plakaten oder als Aufkleber (z. B. an Parkautomaten) führen auf gefälschte Login-Seiten – der Link steckt im Bild und umgeht viele E-Mail-Filter.

Schutz: QR-Codes aus Mails nie scannen; nach dem Scan die URL prüfen, bevor Daten eingegeben werden.

WhatsApp- & Teams-Phishing

„Hallo, neue Nummer"-Maschen, gefälschte Chef-Nachrichten und externe Teams-Anfragen vom angeblichen „IT-Support" – Messenger umgehen den geschützten Mail-Kanal.

Schutz: Externe Absender prüfen; Codes, Passwörter und Zahlungen niemals per Chat – Rückruf über bekannte Nummer.

USB-Stick-Angriffe (Baiting)

„Verlorene" Sticks auf Parkplatz oder per Post, beschriftet mit „Gehälter" o. Ä. – BadUSB-Sticks tippen beim Einstecken unsichtbar Befehle wie eine Tastatur.

Schutz: Fremde USB-Geräte nie anschließen – immer bei der IT abgeben; USB-Ports technisch einschränken.

Fake-Microsoft-Support

Anruf oder Browser-Popup: „Ihr PC ist infiziert!" – dann Fernwartung (z. B. AnyDesk), Zugriff auf Daten und Konten. Microsoft ruft nie unaufgefordert an.

Schutz: Auflegen bzw. Popup schließen (nicht anrufen!), nichts installieren, sofort die IT informieren.

Gefährliche Anhänge: PDF, HTML & OneNote

ITSR
die hammer agentur

PDF-Anhänge

Gefälschte Rechnungen oder Bewerbungen mit eingebettetem JavaScript, Phishing-Links oder QR-Codes im Dokument selbst.

Schutz: Unerwartete Anhänge nicht öffnen; Links/QR-Codes im PDF nie anklicken oder scannen; PDF-Reader aktuell halten.

HTML-Anhänge (HTML-Smuggling)

Der Schadcode wird erst lokal im Browser zusammengebaut oder eine gefälschte Microsoft-365-Login-Seite direkt im Anhang angezeigt – so umgehen die Angriffe viele Mail-Filter.

Schutz: HTML/HTM-Anhänge grundsätzlich nicht öffnen und am Mail-Gateway blockieren; nie Login-Daten in einer aus einem Anhang geöffneten Seite eingeben.

OneNote-Dateien (.one)

Seit Office-Makros aus dem Internet blockiert werden, weichen Angreifer auf OneNote aus: Skripte verstecken sich hinter „Doppelklick zum Öffnen“-Schaltflächen.

Schutz: „.one“-Anhänge von extern blockieren; eingebettete Dateien in Dokumenten nie per Doppelklick starten – im Zweifel an die IT.

Der Dateityp ist austauschbar – unerwarteter Anhang plus Aufforderung zum Klicken heißt immer: erst verifizieren.

NEUE BEDROHUNG

KI im Social Engineering

ITSR
die hammer agentur

Voice Cloning

Drei Sekunden Audiomaterial genügen, um eine Stimme täuschend echt zu klonen – Quellen: Mailbox-Ansagen, Videos, Podcasts, LinkedIn.

+442 %

Vishing-Angriffe (Voice-Phishing) in einem Jahr

Deepfake-Videocalls

KI-generierte Gesichter in Echtzeit: Ganze Videokonferenzen inklusive „Chef“ und „Kollegen“ können gefälscht sein.

+1.600 %

Deepfake-Vishing allein in Q1 2025

KI-gestützter CEO-Fraud

KI imitiert Schreibstil und Tonfall von Vorgesetzten und kombiniert E-Mail, Anruf und Video zu einer glaubwürdigen Kette.

+53 %

Deepfake-Betrugsversuche gegen deutsche Unternehmen 2025

BKA: KI-gestützte Betrugsdelikte seit 2023 um über 300 % gestiegen – Voice Cloning wird 2025 erstmals als eigenständiges Tatmittel geführt.

Fallbeispiel: Der 25-Millionen-Dollar-Videocall

1. **Phishing-Mail**
   Ein Finanzmitarbeiter des Ingenieurbüros Arup erhält eine Mail des vermeintlichen CFO – er schöpft zunächst Verdacht.

2. **Deepfake-Videokonferenz**
   Zur „Bestätigung“ folgt ein Videocall mit CFO und mehreren Kollegen. Alle Teilnehmer sind KI-generierte Deepfakes.

3. **15 Überweisungen**
   Überzeugt von Gesichtern und Stimmen führt der Mitarbeiter Transaktionen über insgesamt 25,6 Mio. US-Dollar aus.

4. **Zu späte Entdeckung**
   Der Betrug fällt erst bei einer manuellen Rückfrage in der Konzernzentrale auf – das Geld ist weg.

Die Lehre daraus

- **Ein Videocall ist kein Identitätsnachweis mehr.**
- Sehen und Hören reichen nicht – nur definierte Prozesse schützen.
- Rückruf über bekannte Nummer und Vier-Augen-Prinzip hätten den Schaden verhindert.

REALE FOLGEN

Wenn es KMU trifft: Fälle aus Deutschland

Mai 2025

Fasana GmbH, Euskirchen

Ransomware verschlüsselt Netzwerke, Server und Rechner des Serviettenherstellers. Weder Auftragsbearbeitung noch Rechnungen oder Löhne laufen. Rund 2 Mio. € Umsatzverlust in zwei Wochen – Insolvenz.

März 2026

ZEGO Textilveredelung, Aschaffenburg

Cyberangriff legt die Produktion wochenlang lahm. Die finanziellen Belastungen sind so hoch, dass das Unternehmen nach 37 Jahren im Juli 2026 Insolvenz beantragt.

Laufend

Der Mittelstand insgesamt

Rund 950 registrierte Ransomware-Angriffe im BSI-Berichtszeitraum – 80 % davon gegen KMU. Ein Viertel des Mittelstands hat bereits Vorfälle mit erheblichen Betriebsunterbrechungen erlebt.

Ein erfolgreicher Angriff ist für KMU keine IT-Störung – er ist ein Existenzrisiko.

Ransomware heute: Erpressung als Geschäftsmodell

ITSR
die hammer agentur

Crime-as-a-Service
Ransomware wird als fertiger Baukasten vermietet; Zugänge zu Firmennetzen werden von „Initial Access Brokern“ verkauft. KI steigert Reichweite und Tempo der Kampagnen.

Double & Triple Extortion
Daten werden nicht nur verschlüsselt, sondern vorher gestohlen. Gedroht wird mit Veröffentlichung, DDoS und der Information von Kunden und Partnern.

Haupteinfallstore
Phishing & gestohlene Zugangsdaten, Fernzugänge (VPN/RDP) ohne Mehr-Faktor-Authentifizierung und ungepatchte Schwachstellen – bei 119 neuen Lücken pro Tag.

Lösegeld lohnt sich nicht
Zahlung garantiert weder Entschlüsselung noch Löschung der Daten – und finanziert die nächste Angriffswelle. BSI und Bitkom raten klar von Zahlungen ab.

Schutzmaßnahmen: Technik

Mehr-Faktor-Authentifizierung (MFA) — verpflichtend für alle Konten – vor allem E-Mail, VPN/Fernzugriff und Admin-Zugänge; phishing-resistente Verfahren bevorzugen

Backups nach 3-2-1-Regel — drei Kopien, zwei Medien, eine Kopie offline/unveränderlich – und die Wiederherstellung regelmäßig testen

Endpoint-Schutz & Erkennung — aktuelle Schutzsoftware plus Angriffserkennung (EDR); Firewall und Netzwerksegmentierung begrenzen die Ausbreitung

Updates & Patch-Management — Betriebssysteme und Software automatisch aktualisieren; ungenutzte Programme und Dienste konsequent entfernen

E-Mail-Absicherung — SPF, DKIM und DMARC gegen Spoofing; moderne Filter erkennen zunehmend auch KI-generierte Phishing-Muster

Minimale Rechte — Arbeit ohne Admin-Rechte im Alltag, separate Konten für Administration, Zugriffe nach dem Need-to-know-Prinzip

ITSR
die hammer agentur

Schutzmaßnahmen: Prozesse & Menschen

Rückruf-Verifikation — Zahlungs- und Kontoänderungen sowie ungewöhnliche Chef-Anweisungen immer über die bekannte Nummer zurückrufen – nie über Nummern aus Mail oder Anruf

Vier-Augen-Prinzip — keine Überweisung über einem festen Limit ohne Freigabe durch eine zweite autorisierte Person – ohne Ausnahme, auch nicht „für den Chef“

Codewort für Notfälle — vereinbartes Codewort für sensible telefonische Anweisungen – ein einfacher, wirksamer Schutz gegen geklonte Stimmen

Schulung & Simulation — regelmäßige Awareness-Trainings und Phishing-Simulationen – inklusive der neuen KI-Maschen (Deepfake, Voice Cloning)

Notfallplan — Wer wird informiert, wer trennt Systeme, wo liegen Backups und Notfallkontakte offline? Im Ernstfall zählt jede Minute

Meldekultur ohne Schuldzuweisung — verdächtige Mails und Beinahe-Fehler sofort melden – wer meldet, schützt das Unternehmen und wird nicht sanktioniert

Prozessuale Zweitprüfung stoppt die große Mehrheit der Deepfake-Angriffe – unabhängig davon, wie perfekt die Fälschung ist.

FAZIT

Fünf Sätze, die hängen bleiben sollen

1. KMU sind Hauptziel, nicht Beifang: 80 % der Ransomware-Angriffe treffen den Mittelstand.
   Ein erfolgreicher Angriff ist für KMU keine IT-Störung – er ist ein Existenzrisiko.

2. KI hat Phishing perfektioniert: Fehlerfreie, persönliche Nachrichten sind der Normalfall – alte Erkennungsregeln reichen nicht mehr.
   Es ist klug und weise an allem zu zweifeln. Voltaire

3. Stimme und Video beweisen nichts mehr: Deepfakes und Voice Cloning machen Rückruf-Verifikation und Vier-Augen-Prinzip zur Pflicht.
   Es ist klug und weise an allem zu zweifeln. Voltaire

4. Die Basis bleibt: MFA überall, Updates, getestete Offline-Backups und minimale Rechte schließen die häufigsten Einfallstore.

5. Sicherheit ist Kultur: Melden statt vertuschen, verifizieren statt vertrauen – jede*r Einzelne ist Teil der Verteidigung.

ITSR
die hammer agentur

Quellen & Datenstand

- **Bitkom Wirtschaftsschutz-Studie 2025**
Gesamtschaden 289,2 Mrd. €, 202,4 Mrd. € durch Cyberangriffe, 87 % betroffene Unternehmen, Angriffsarten, Lösegeldzahlungen, Täterherkunft.

- **BSI – Die Lage der IT-Sicherheit in Deutschland 2025**
119 neue Schwachstellen pro Tag (+24 %), rund 950 Ransomware-Angriffe, 80 % der Angriffe gegen KMU, Handlungsempfehlungen.

- **BKA / Verbraucherzentrale / CrowdStrike Global Threat Report**
KI-Betrugsdelikte +300 % seit 2023, Vishing +442 %, Deepfake-Vishing +1.600 % (Q1 2025), Deepfake-Versuche gegen deutsche Unternehmen +53 %.

- **Orange Cyberdefense Security Navigator 2026**
Cyber-Erpressung in Deutschland +91 %, KMU bis 250 Mitarbeitende als Hauptbetroffene.

- **Fallberichte**
Arup-Deepfake-Betrug (25,6 Mio. USD, 2024); Fasana GmbH Insolvenz nach Ransomware (Mai 2025); ZEGO Textilveredelung Insolvenz nach Cyberangriff (2026); Presse- und Fachberichte.