



CYBERSICHER LAGEBILD

Die aktuelle Bedrohungslage für kleine und
mittlere Unternehmen in Deutschland
Oktober 2026



Vorwort

Das neue Lagebild zeigt: Cyberangriffe auf kleine und mittlere Unternehmen erreichen eine neue Qualität. Künstliche Intelligenz verändert die Bedrohungslandschaft grundlegend und klassische Erkennungsmerkmale von Betrugsversuchen verlieren zunehmend an Aussagekraft. Was früher tiefes technisches Fachwissen erforderte, gelingt heute auch weniger versierten Tätern: KI-Modelle formulieren überzeugende Phishing-Mails und steuern in Teilen bereits eigenständig komplexe Angriffsabläufe. Gleichzeitig öffnet der eigene Einsatz von KI in Unternehmen neue Angriffsflächen, die viele Betriebe erst noch verstehen und absichern müssen.

Wie konkret Cyberkriminelle dabei vorgehen, zeigt die Auswertung unseres Transferstellen-Honeypots. Die gesammelten Daten geben einen seltenen Einblick in die Methodik der Angreifenden – von automatisierten Scans bis hin zu gezielten Zugriffsversuchen – und machen deutlich, wie unmittelbar die Gefahr für jedes vernetzte System ist, unabhängig von dessen vermeintlicher Unauffälligkeit.

Auch die etablierten Bedrohungen bleiben virulent: Ransomware-Angriffe haben weiter zugenommen, ihre Auswirkungen für betroffene Unternehmen werden gravierender. Verschärft wird die Lage durch globale Konflikte, deren digitale Kollateralschäden zunehmend auch kleine und mittlere Unternehmen in Deutschland treffen.

Ein weiterer wunder Punkt ist die digitale Souveränität: 66 % der deutschen KMU fühlen sich stark von nicht-europäischen Softwareanbietern abhängig. Hier besteht erheblicher Nachholbedarf, um technologische Abhängigkeiten zu verringern und im digitalen Raum eigenständig handlungsfähig zu bleiben.

Die Auswertung der Lagebild-Daten zeigt aber auch, dass der Mittelstand reagiert. Schutzmaßnahmen werden zunehmend nicht nur geplant, sondern tatsächlich umgesetzt. Cybersicherheit im Mittelstand wird zunehmend als das verstanden, was sie ist – ein strategisches Thema, das entsprechende Priorität verdient.

Genau hier setzt unsere Transferstelle Cybersicherheit im Mittelstand an. Mit kostenfreien und anbieterneutralen Angeboten, dank der Förderung des Bundesministeriums für Wirtschaft und Energie, begleiten wir kleine und mittlere Unternehmen, Handwerksbetriebe und Start-ups auf dem Weg zu mehr digitaler Resilienz. Denn eines steht fest: In einer Bedrohungslage, die sich durch KI, geopolitische Spannungen und technologische Abhängigkeiten stetig wandelt, ist Cybersicherheit kein Zustand, den man einmal erreicht, sondern eine Daueraufgabe, der sich jedes Unternehmen aktiv stellen muss.

Marc Dönges und Dirk Achenbach, Projektleitung Transferstelle Cybersicherheit im Mittelstand



Dirk Achenbach



Marc Dönges

KI: Neue Dimension der Phishing-Angriffe

Phishing ist und bleibt eine der häufigsten Angriffsformen.
In Zeiten von KI und Deepfakes gewinnen die Attacken an Qualität und klassische Erkennungsmerkmale verlieren an Aussagekraft.

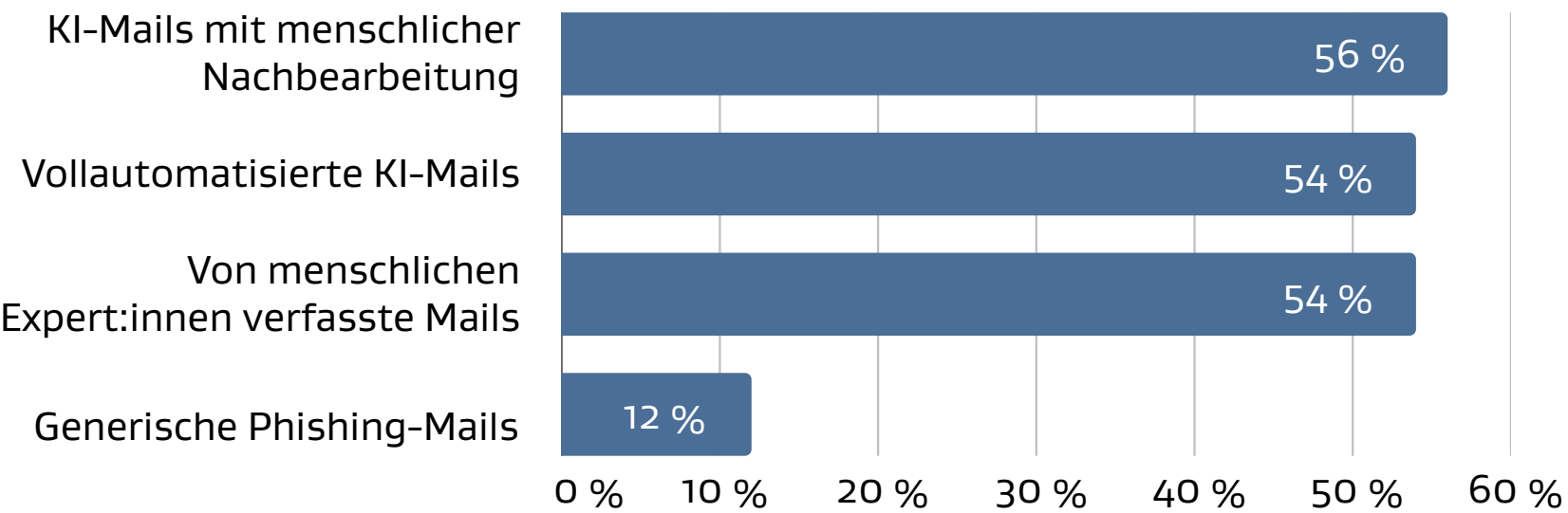
-  Cyberkriminelle nutzen KI, um betrügerische Phishing-Mails überzeugender wirken zu lassen.
-  Auf von KI automatisch generierte Spearphishingmails klicken fast drei- bis fünfmal so viele Nutzer:innen wie auf generische Phishingmails.
-  Das BSI weist ausdrücklich darauf hin, dass Cyberkriminelle hochwertige Phishingnachrichten erstellen können. Rechtschreibfehler und ungewöhnliche Formulierungen sind kein Merkmal für Phishing mehr.



Spearphishing

Spearphishingmails sind personalisierte Mails, die Personen in exponierten Positionen (z.B. Geschäftsführung, Abteilungsleitung, Empfang, Buchhaltung) zum Ziel haben.

Klickraten bei Spearphishing-Mails



 **66 %**
erkennen nicht, dass Deep-Fake-Audioaufnahmen gefälscht sind

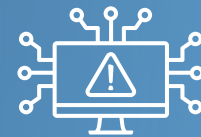
 **58 %**
der geklonten Stimmen werden als menschlich eingeordnet

 **43 %**
erkennen gefälschte Videos nicht

Skalierung von Cyberattacken durch KI-Automatisierung

Durch den Einsatz von KI werden automatisierte Angriffe und Schwachstellenscans häufiger und besser. **Das Finden und Ausnutzen von Schwachstellen wird zudem einfacher. Fachkenntnisse sind kaum mehr nötig, um komplexe Angriffe zu starten.**

Mit Hilfe von KI ist die Hürde für Angriffe niedriger. Cyberkriminelle benötigen immer weniger Fachwissen für ihre Angriffe.



Angreifende setzen KI ein, um automatisiert verwundbare Systeme zu finden und anschließend zu infizieren.



KI deckt (aktuell) neue Schwachstellen schneller auf, als öffentliche Datenbanken sie dokumentieren können.



CYBERSicher-Tipp

Grundlegende Sicherheitsmaßnahmen, wie Backups, regelmäßige Updates und starke Passwörter, sind und bleiben für kleine und mittlere Unternehmen der beste Schutz gegen Cyberangriffe – auch in Zeiten von KI.

**Juni
2025**

Cyberkriminelle setzen Schadsoftware ein, die KI-Komponenten enthält, um auf infizierten Rechnern automatisiert passende Malware schreiben zu lassen.



Angreifende setzen Schadsoftware ein, die KI-Komponenten enthält, um ihren eigenen Code zu verschleiern und eine Erkennung zu erschweren.

**Juni
2025**



**April
2026**

Anthropic präsentiert Claude Mythos als besonders leistungsfähiges Hacking-Modell und hält es vorerst aufgrund der Risiken unter Verschluss.

**Juli
2026**

Das Open AI-Modell namens GPT-5.6.-Sol führt unbeabsichtigt und selbstständig einen erfolgreichen Angriff auf Hugging Face durch.



Neue Sicherheitslücken durch KI

20 % der deutschen KMU setzen KI ein. Dadurch bauen sie sich häufig freiwillig und unwissentlich Hintertüren in ihr Unternehmensnetzwerk ein, die von Cyberkriminellen ausgenutzt werden können.



5–10 % der LLM-Anwendungen, wie z.B Chatbots auf Unternehmenswebseiten, geben private Dokumente, Adressen oder Firmengeheimnisse preis.



70 % der Softwareentwickler:innen in Deutschland setzen mehrfach pro Woche KI zum Erstellen von Programmcode ein.



KI als Blackbox

KI kann zur Blackbox werden, wenn Unternehmen nicht wissen, welche Daten verarbeitet werden und welche Risiken im Hintergrund entstehen.



Vibe-Coding

Vibe-Coding ist die Erstellung von Anwendungen (z.B. Apps) mit Hilfe von KI-Agenten. Anwender:innen beschreiben der KI ihre Anwendung, die KI setzt diese dann in Code um.

bis zu
20 x

mehr Sicherheitslücken in durch Vibe-Coding erstellten Anwendungen als in konventionell entwickelten Anwendungen



vs.



Honeypots: Angreifende beobachten & Attacken nachvollziehen

Ein „Honeypot“ wirkt nach außen wie ein echtes Computersystem und soll Angreifende dazu verleiten, den Honeypot anstatt echter Systeme anzugreifen. Dadurch werden diese geschützt und das Verhalten der Angreifenden kann beobachtet werden. Die Transferstelle Cybersicherheit betreibt einen Honeypot, um mögliche Angriffe zu beobachten.

Hintergrundwissen

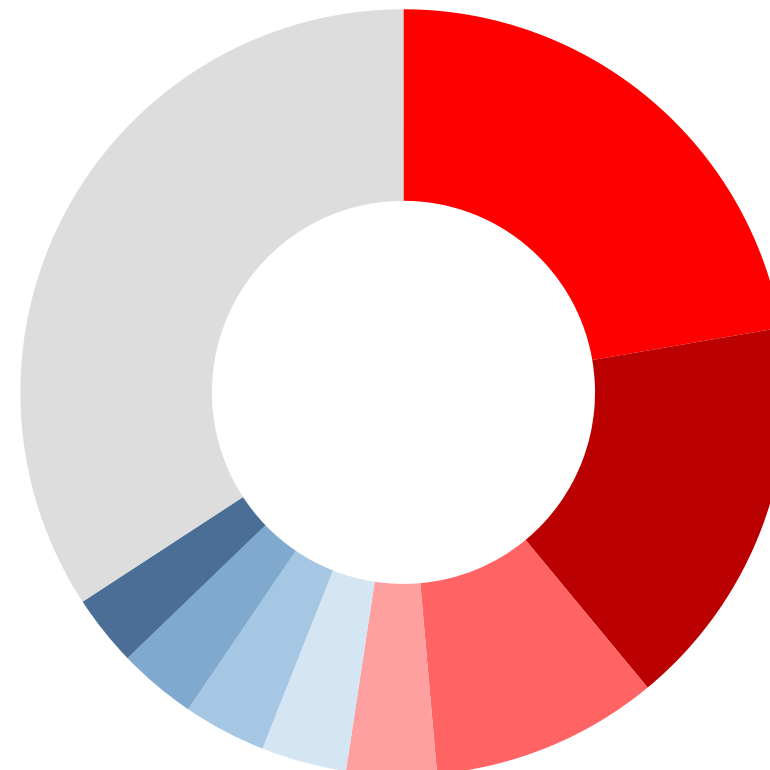
Für den Honeypot wurden auf einem Server der Transferstelle verschiedene Ports geöffnet – das angegriffene System ist in diesem Fall die CYBERSicher Notfallhilfe, deren IP-Adresse öffentlich bekannt ist.

Ein Netzwerk-Port ist eine logische Adresse, die Datenpakete an den richtigen Dienst auf einem Computer weiterleitet, vergleichbar mit einem Haus (IP-Adresse) und den verschiedenen Wohnungs- oder Zimmernummern darin (Ports).

Angreifende nutzen Dienste, um offene Ports zu finden, und probieren gezielt alle möglichen Ports unserer IP aus, um Angriffe zu starten. Dabei konzentrieren sie sich auf jene Ports, bei denen sie die höchsten Erfolgsaussichten erwarten, da jeder Port für einen Dienst steht, über den ein Angriff versucht werden kann. So können wir beobachten, wie sich die Angreifenden verhalten, wenn sie erfolgreich einzubrechen versuchen.

Angegriffene Dienste (Ports)

n = 8.123 Angreifende



Telnet	22,3 %	MySQL	3,6 %
SSH	16,7 %	SMB	3,5 %
RDP	9,6 %	FTP	3,3 %
SIP	3,8 %	MongoDB	3,0 %
		Sonstige	34,2 %

Am häufigsten getestete Nutzernamen

root deploy
user admin ubuntu
transferstelle cybersicherheit
transferstelle notfallhilfe
cybersicherheit
test



CYBERSicher-Tipp

Bei einem Angriff werden neben üblichen Zugangsdaten (wie z.B. root oder admin) auch auf das Unternehmen zugeschnittene Passwörter und Nutzernamen getestet. Deswegen sind auch komplexere, persönliche Passwörter oft nicht so sicher, wie Nutzer:innen annehmen. Hier kann ein Passwortmanager Abhilfe schaffen, der lange und zufällige Passwörter generiert und verwaltet.

Honeypot in der Praxis: Wie ein echter Cyberangriff aussieht

Auf dem Honeypot der Transferstelle kann nachvollzogen werden, wie Angreifende versuchen, den Server zu kompromittieren. **Angreifende haben mehrfach versucht, Schadsoftware (Malware) auf dem Honeypot zu installieren.**



Die Ziele der Schadsoftware

- Das Netzwerk analysieren und weitere angreifbare Dienste und Systeme finden
- Die Firewall-Regeln analysieren und darauf reagieren
- Sicherstellen, dass die Schadsoftware auch nach einem Neustart weiter funktioniert
- Das System vollständig kontrollieren und für ein Botnetz nutzbar machen



Bei jedem zweiten Angriff wurde versucht „Cryptojacking“-Malware zu installieren.



Bekannte Verschlüsselungstrojaner wurden nur selten entdeckt, da Angreifende zunächst vermutlich unauffällige Schadsoftware einschleusen und nur lukrative Ziele verschlüsseln.



Cryptojacking

Beim Cryptojacking werden infizierte Geräte zum Schürfen von Kryptowährungen missbraucht. Erkennbar ist dies oftmals an hoher Systemauslastung, erhöhtem Stromverbrauch und überhitzter Hardware, was zugleich den wesentlichen Schäden für das gehackte Unternehmen entspricht.



Malware

Eine Malware (Schadsoftware) installiert sich auf einem System wie ein normaler Dienst. Durch Zero-Trust-Policies, bei denen nur erlaubte Prozesse ausgeführt werden können, und durch Netzwerküberwachung lassen sich Angriffe frühzeitig verhindern.



Botnetz

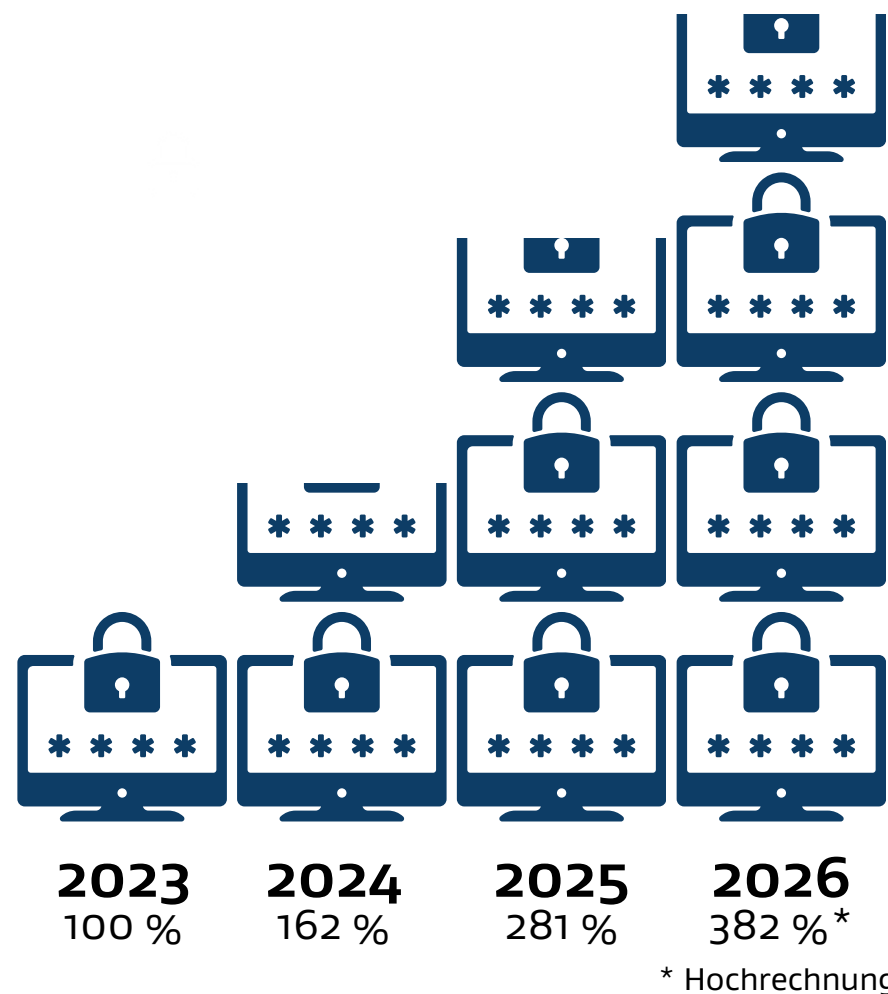
Ein Botnetz besteht aus mehreren infizierten Geräten, welche von einem Angreifenden ferngesteuert werden. Es besteht neben Servern oftmals auch aus Routern, Druckern und smarten Geräten ohne Wissen der Besitzer:innen, da die Geräte weiterhin normal funktionieren. Ein Botnetz wird für den Versand von Spam, zur Verschleierung der Identität des Angreifenden und für koordinierte Angriffe wie DDoS-Attacken, bei denen Server oder Netzwerke durch gezielte, massenhafte Anfragen überlastet werden, genutzt.

Verschlüsselungen nehmen weiter zu

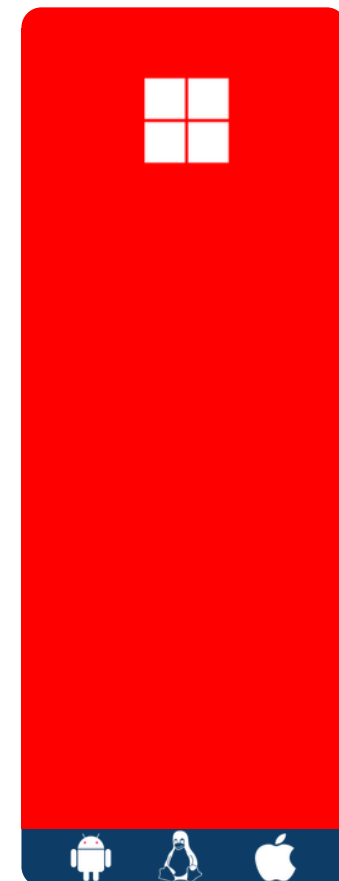
Bei einer Ransomware-Attacke machen Verschlüsselungstrojaner wichtige Daten unlesbar. Hacker fordern danach ein Lösegeld, um die Daten wieder zu entschlüsseln. Auch im Jahr 2026 nimmt die Häufigkeit von Ransomware-Angriffen weiter zu.

Bekanntgewordene Ransomware-Angriffe auf deutsche KMU

Wachstumsrate in %, Zunahmen im Vergleich zum Referenzjahr 2023 · Stand: 24.09.2026



Verteilung der beobachteten Malware nach Betriebssystemen



	Windows	849.257
	Android	25.691
	Linux	4.403
	MacOS	241

Zeitraum: 13.07.26 - 27.07.26



Cybercrime als Geschäftsmodell

Ransomware-as-a-Service (RaaS) bezeichnet ein Geschäftsmodell, bei dem Cyberkriminelle im Darknet fertige Ransomware zur Verfügung stellen. Über entsprechende RaaS-Plattformen und die zugehörige Infrastruktur können auch technisch weniger versierte Dritte die Schadprogramme mit geringem Aufwand einsetzen. Wie bei klassischer Ransomware verfolgen die Angreifenden dabei ein Ziel: die Erpressung von Lösegeld.



CYBERSicher-Tipp

Zum Schutz der eigenen Daten sind Backups über alle Betriebssysteme hinweg unabdingbar. Zu beachten ist die 3-2-1-Regel, die besagt, dass insgesamt drei Gesamtkopien der Daten auf zwei Speichermedien und einem externen Speicherort angelegt werden sollten. Außerdem müssen Backups regelmäßig auf Vollständigkeit geprüft und das Einspielen getestet werden.

Wie globale Konflikte die Cybersicherheit gefährden

Parallel zu globalen Konflikten spitzt sich auch die Lage in der Cybersicherheit zu.

Kleine und mittlere Unternehmen werden zunehmend Opfer von Kollateralschäden im Rahmen von Konflikten.



Cyberattacken während globaler Konflikte haben zum Ziel, Aufmerksamkeit zu erzeugen und gesellschaftliche Verunsicherung zu schaffen.



DDoS-Angriffe auf deutsche Ziele nehmen im Kontext mit geopolitischen Entwicklungen zu.



In Krisengebieten und unbeteiligten Ländern werden vornehmlich kleine und mittlere Unternehmen angegriffen.



Kritische Infrastruktur wird ebenfalls zum Ziel: Angriffe in jüngsten Konflikten fokussierten überwiegend die Bereiche Telekommunikation, Finanzen, Metallindustrie, Energie und Lieferketten.



Kleine und mittlere Unternehmen werden zum Ziel, wenn sie leicht angreifbar sind, zum Beispiel durch schlecht geschützte Fernzugänge und veraltete Software.



DDoS-Attacken (Distributed Denial of Service)

DDoS-Attacken (Distributed Denial of Service) sind Cyberangriffe, bei denen mehrere kompromittierte Systeme, oft Teil eines Botnetzes, gleichzeitig eine Zielressource wie eine Website oder einen Server mit einer Flut von Anfragen überlasten. Das Ziel ist es, die Verfügbarkeit der Ressource zu stören oder vollständig lahmzulegen, sodass legitime Benutzer:innen keinen Zugriff mehr darauf haben.

Sandworm

Gruppe, die mutmaßlich die Schadsoftware „NotPetya“ in Umlauf gebracht hat und ursprünglich vor allem die Ukraine zum Ziel hatte.

WhisperGate und HermeticWiper

Schadprogramme, die im Rahmen des Krieges gegen die Ukraine eingesetzt wurden und Daten und Systeme zerstören sollten.



Wie digital souverän ist der deutsche Mittelstand?

Bisher haben deutsche KMU Schwierigkeiten bei der Umsetzung von digitaler Souveränität.

Die Nutzung von europäischen Alternativen ist möglich. Das kann aber zu Mehraufwand bei der Integration und zu Kompatibilitätsproblemen führen.



Digitale Souveränität

Digitale Souveränität bedeutet, IT-Systeme und digitale Prozesse selbstbestimmt kontrollieren zu können, ohne unangemessen von einzelnen (oft nicht-europäischen) Anbietern abhängig zu sein.

Zentral ist die Fähigkeit, kritische Software und Cloud-Dienste bewusst und informiert auszuwählen, etwa mit Blick auf Rechts- und Ausfallsicherheit.

66 %

der deutschen KMU fühlen sich stark von nicht-europäischen Softwareanbietern abhängig



50 %

der deutschen KMU setzen kostenpflichtige Clouddienste ein



50 %

der deutschen KMU setzen von deutschen KMU entwickelte ERP-Systeme ein



Tool-Tipp

Über ein kostenfreies Tool des Förderschwerpunkts Mittelstand-Digital können Sie selbst prüfen, wie digital souverän Ihr Unternehmen aufgestellt ist. Auf der Website finden Sie zudem weiterführende Informationen, die die Themen des Tests mit Inhalten der Mittelstand-Digital Zentren verbinden.

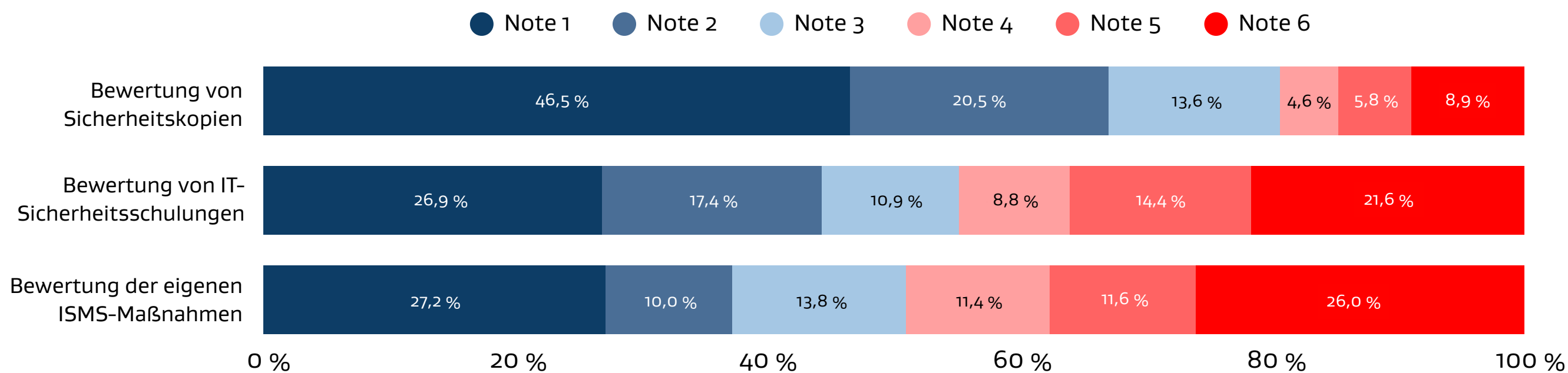


So schützt sich der Mittelstand vor Cyberangriffen

Die kleinen und mittleren Unternehmen in Deutschland nehmen das Thema Cybersicherheit ernst **und setzen konkrete Schutzmaßnahmen gezielt um.**

Selbsteinschätzung von KMU in den jeweiligen Bereichen (n = 1.190 Unternehmen)

Anteile in Prozent: Note 1 = beste Bewertung, Note 6 = schlechteste



CYBERsicher Tipp

In der kostenfreien ISMS-Werkstatt der Transferstelle Cybersicherheit erlernen Teilnehmer:innen praxisnah und gemeinsam mit anderen Unternehmen, wie sie ein maßgeschneidertes ISMS für ihr Unternehmen entwickeln und nachhaltig umsetzen.



Bewertung von Sicherheitskopien

81 % der Befragten bewerteten das Management von Sicherheitskopien in ihrem Unternehmen positiv (Note 3 oder besser). Ein gutes Sicherheitskonzept umfasst, dass Sicherheitskopien regelmäßig auf Vollständigkeit geprüft werden und das Einspielen geübt wird.



Bewertung von IT-Sicherheitsschulungen

Der Faktor Mensch ist eine der größten Schwachstellen in der Cybersicherheit und die Sensibilisierung der Mitarbeitenden ein wichtiger Faktor, um Cyberangriffe zu erkennen und abzuwehren. Im CYBERsicher Check bewerteten lediglich 55 % der Befragten die Schulungsmaßnahmen ihres Unternehmens als zufriedenstellend (Note 3 oder besser).



Bewertung der eigenen ISMS-Maßnahmen

Bei ISMS-Maßnahmen gibt es ein gemischtes Bild. In einer Studie geben 85 % der Befragten an, laufend ihre IT-Sicherheitsmaßnahmen zu aktualisieren, 74 % führen monatliche Schwachstellenchecks durch. Ein Informationssicherheitsmanagementsystem (ISMS) hilft Unternehmen dabei, das Thema Cybersicherheit strukturiert und umfassend anzugehen.

Gesetzliche Pflichten als Chance für KMU

Gesetzliche Pflichten und Regulierungen werden von der Mehrheit der deutschen kleinen und mittleren Unternehmen positiv aufgenommen **und wirken als zusätzlicher Umsetzungsanstoß für IT-Sicherheitsvorkehrungen.**

56 % der befragten Unternehmen befürworten gesetzliche Pflichten zu angemessenen Cybersecurity-Maßnahmen, wie z.B. NIS2



NIS2

Seit dem 06.12.2025 ist NIS2 in Deutschland geltendes Recht. NIS2 steht für „zweite Netzwerk- und Informationssicherheitsrichtlinie“. Die Richtlinie wurde im Jahr 2022 durch das Europäische Parlament verabschiedet und hat zum Ziel, die Cyberresilienz in der EU zu stärken. In Deutschland sind rund 29.500 Unternehmen unmittelbar betroffen, darunter Sektoren wie Logistik, Lebensmittelproduktion und Abfallwirtschaft. Für die Unternehmensleitung bedeutet das: Informationssicherheit ist ab sofort eine Führungsaufgabe mit rechtlichen Konsequenzen.



Cyber Resilience Act (CRA)

Der Cyber Resilience Act (CRA) soll digitale Produkte in der EU vor Cyberangriffen schützen. Er verlangt, dass Geräte und Programme so entworfen, entwickelt und aktualisiert werden, damit deren Nutzer:innen (Privatpersonen und Unternehmen) geschützt werden. So sollen u.a. zeitnah Sicherheitsupdates für Produkte bereitstehen, wenn Sicherheitslücken bekannt werden. Der CRA ist eine Ergänzung der DSGVO und der NIS2-Richtlinie und wird für neue Produkte ab dem 11. Dezember 2027 verbindlich.



Tool-Tipp

Der FitNIS2-Navigator ist ein speziell entwickeltes Online-Tool, das KMU unterstützt, die Anforderungen des NIS2-Gesetzes zu verstehen und umzusetzen. Das Fokusprojekt unterstützt bei der Betroffenheitsprüfung und gibt konkrete Handlungsempfehlungen.



Tool-Tipp

Das Fokusprojekt EASY.CRA unterstützt kleine und mittlere Unternehmen dabei, die Anforderungen des Cyber Resilience Act (CRA) verständlich und praxisnah umzusetzen.

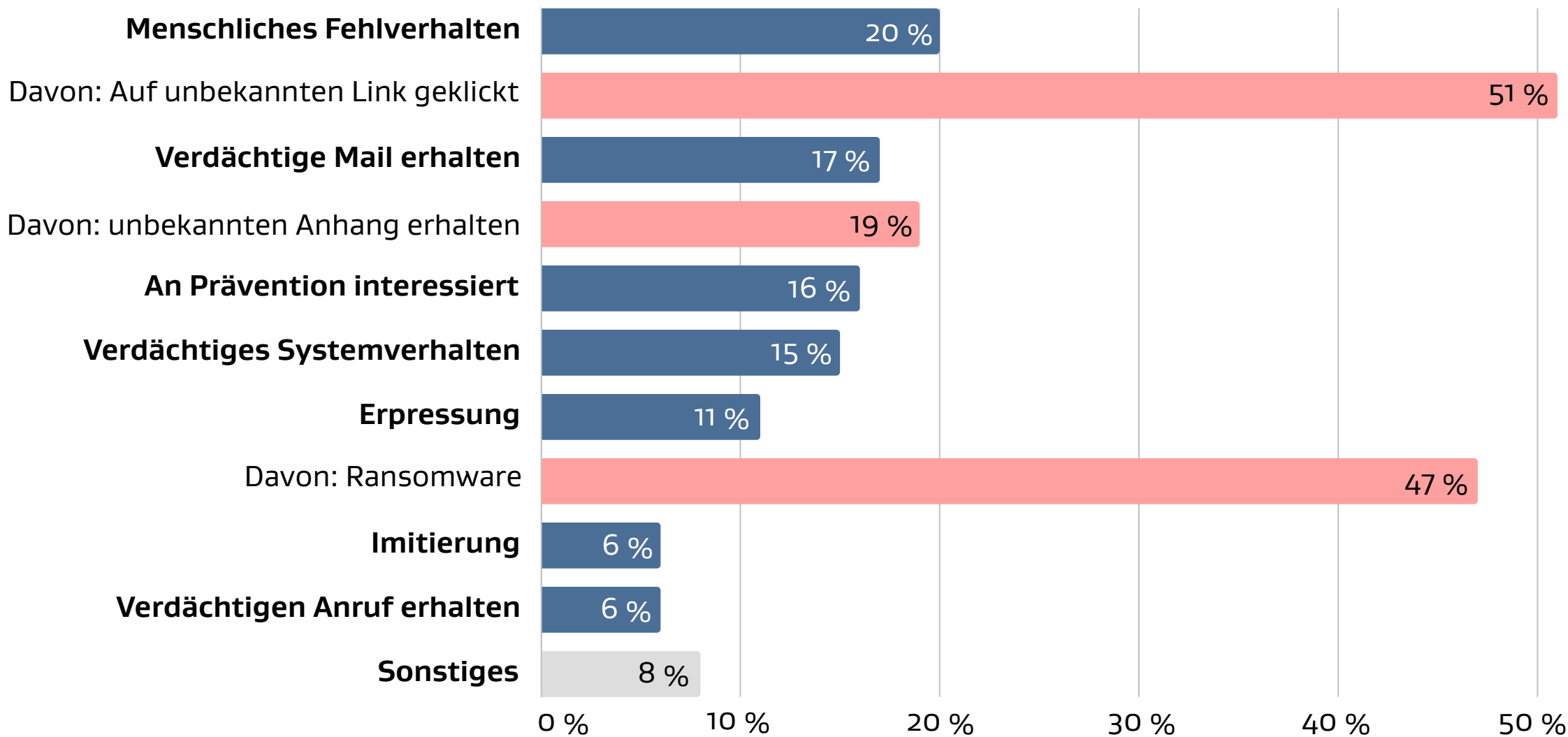


Beide Fokusprojekte sind Teil der Initiative IT-Sicherheit in der Wirtschaft. Mit dieser Förderinitiative unterstützt das Bundesministerium für Wirtschaft und Energie Unternehmen darin, ihre IT-Sicherheit zu verbessern.

Externe Unterstützung im Ernstfall

Der Selbstcheck der CYBERSicher Notfallhilfe zeigt, dass KMU am häufigsten aufgrund von menschlichem Fehlverhalten und verdächtigen E-Mails externe Hilfe aufsuchen. **Fast jedes sechste Unternehmen (16 %) ist proaktiv auf der Suche nach präventiven Maßnahmen.**

Häufigste Anfragen an den Selbstcheck der CYBERSicher Notfallhilfe (n = 831 Nutzer:innen*)



* Zeitraum: Juli 2025 bis Juli 2026



Tool-Tipp

Die CYBERSicher Notfallhilfe unterstützt im Ernstfall schnell und unkompliziert. Innerhalb weniger Minuten erhalten Nutzer:innen konkrete Rückmeldungen aus einem großen Netzwerk von Dienstleistern – anonym, unverbindlich und mit einer transparenten Übersicht zu Leistungen, Aufwand und Kosten.



Wir machen den Mittelstand CYBERsicher!

Die **Transferstelle Cybersicherheit** im Mittelstand unterstützt kleine und mittlere Unternehmen, Handwerksbetriebe und Start-ups kostenfrei und anbieterneutral.

Unsere Angebote:

CYBERsicher Notfallhilfe: Schnelle und unkomplizierte Unterstützung im Fall eines Cyberangriffs.



CYBERDialoge: Erstgespräche zur Bewertung der Cybersicherheit & Identifikation von Maßnahmen.



CYBERsicher Check: Einfache Ermittlung des Cybersicherheitsniveaus.



Workshops & Webimpulse: Vermittlung von praxisnahem Wissen, das direkt angewendet werden kann.



Materialienplattform: Checklisten, Lernspiele und Broschüren – alles an einem Ort.



ISMS-Werkstatt: Informationssicherheit strukturiert angehen und mithilfe von mehreren Workshops verbessern.



Besuchen Sie uns auf unserer Webseite
www.transferstelle-cybersicherheit.de

Gefördert durch:



Bundesministerium
für Wirtschaft
und Energie

Mittelstand-
Digital 

aufgrund eines Beschlusses
des Deutschen Bundestages

Die Transferstelle Cybersicherheit im Mittelstand gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung und IT-Sicherheit in kleinen und mittleren Unternehmen.

CYBERsicher 

Quellen & Methodik

Methodik

Die Transferstelle Cybersicherheit im Mittelstand hat die Daten von „ransomware.live“ analysiert und mittels einer speziell dafür aufgesetzten KI zusätzlich ausgewertet. Durch diese Auswertung konnten exakte Kategorisierungen sowie Firmenzuordnungen bestimmt werden. Anschließend wurden diese Informationen mit den Daten der Plattform NorthData abgeglichen, um die Daten auf deutsche KMU zu reduzieren. Als Honeytrap wurde der „T-Pot“ der Deutschen Telekom Security GmbH auf dem Server, auf welchem ebenfalls die CYBERSicher Notfallhilfe betrieben wird, installiert und ausgewertet.

Quellen I

- [1] Kemp, M., Kalutarage, H., & Al-Kadri, M. O. (03.02.2025). AI-powered spearphishing cyber attacks: Fact or fiction? (arXiv:2502.00961). arXiv. <https://doi.org/10.48550/arXiv.2502.00961>
- [2] Czybik, S., Kouam, A. J., Heubl, P., Nold, J. M., & Rieck, K. (2026). A large-scale study of personalized phishing using large language models. In Proceedings of the 35th USENIX Security Symposium.
- [3] Heiding, F., Lermen, S., Kao, A., Verdun, C. M., Schneier, B., & Vishwanath, A. (2026). Evaluating large language models' ability to automate spear phishing. Expert Systems with Applications, 314, 131546.
- [4] Lavan, N., Irvine, M., Rosi, V., & McGettigan, C. (2025). Voice clones sound realistic but not (yet) hyperrealistic. PLOS ONE, 20(9), e0332692. <https://doi.org/10.1371/journal.pone.0332692>
- [5] Bundesamt für Sicherheit in der Informationstechnik. (o. D.). BSI-Untersuchung: Wie KI die Cyberbedrohungslandschaft verändert. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/240430_Paper_Einfluss_KI_Cyberbedrohungslage.html
- [6] Google Threat Intelligence Group. (05.11.2025). GTIG AI threat tracker: Advances in threat actor usage of AI tools. Google Cloud Blog. <https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools>
- [7] Google Threat Intelligence Group. (11.05.2026). Adversaries leverage AI for vulnerability exploitation, augmented operations, and initial access. Google Cloud Blog. <https://cloud.google.com/blog/topics/threat-intelligence/ai-vulnerability-exploitation-initial-access/>
- [8] National Cyber Security Centre. (24.01.2024). The near-term impact of AI on the cyber threat. <https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat>
- [9] AI Security Institute. (30.04.2026). Our evaluation of OpenAI's GPT-5.5 cyber capabilities. AISI Work. <https://www.aisi.gov.uk/blog/our-evaluation-of-openais-gpt-5-5-cyber-capabilities>
- [10] Secure. (19.05.2026). AI didn't just find more bugs. It broke the system for tracking them. Secure Blog. <https://www.secure.com/blog/cybersecurity/ai-didnt-just-find-more-bugs-it-broke-the-system-for-tracking-them>
- [11] OpenAI. (21.07.2026). OpenAI und Hugging Face reagieren gemeinsam auf Sicherheitsvorfall bei Modellevaluation. <https://openai.com/de-DE/index/hugging-face-model-evaluation-security-incident/>
- [12] KfW Research. (11.02.2026). Künstliche Intelligenz kommt im Mittelstand immer häufiger zum Einsatz. KfW. https://www.kfw.de/%C3%9Cber-die-KfW/Newsroom/Aktuelles/Pressemitteilungen-Details_880896.html
- [13] Felder, L., Eisenreich, T., Fischer, M., Wagner, S., & Chen, C. (2026). Adoption of generative artificial intelligence in the German software engineering industry: An empirical study. In FSE Companion 2026: Proceedings of the 34th ACM International Conference on the Foundations of Software Engineering. ACM.
- [14] Deng, J., Fan, Z., & Meng, R. (2026). Understanding the (in)security of vibe-coded applications (arXiv:2606.23130). arXiv.

Quellen & Methodik

Quellen II

- [15] Yang, Y., Fu, C., Zhang, T., Zeng, R., Li, Q., Du, T., & Chen, W. (2026). Understanding and mitigating prompt leaking attacks in real-world LLM-based applications (arXiv:2606.18673). arXiv.
- [16] Telekom Security. (o. D.). T-Pot: The all-in-one multi-honeypot platform. GitHub. <https://github.com/telekom-security/tpotce>
- [17] AV-ATLAS. (o.D.). <https://portal.av-atlas.org/malware>
- [18] Ransomware.live. (o. D.). Ransomware.live. <https://ransomware.live/>
- [19] Bundeskriminalamt. (2025). Bundeslagebild Cybercrime 2024. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2024/CC_2024.html
- [20] Bundesamt für Sicherheit in der Informationstechnik. (2025). Zusammenfassung und Bewertung. BSI-Lagebericht 2025. <https://medien.bsi.bund.de/lagebericht/de/zusammenfassung-und-bewertung/>
- [21] Bundeskriminalamt. (03.06.2025). Bundeslagebild Cybercrime 2024: Zahlreiche Ermittlungserfolge bei anhaltend hoher Bedrohungslage. https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2025/Presse2025/250603_PM_BLB_Cybercrime.html
- [22] TLP:CLEAR. (2025). 2024 Cybercrime Activity Report: Trends, Insights & Predictions. https://www.gov.il/BlobFolder/reports/alert_1863/en/ALERT-CERT-IL-W-1863.pdf
- [23] AP News. (18.12.2023). A suspected cyberattack paralyzes the majority of gas stations across Iran. <https://apnews.com/article/iran-gas-stations-cyberattack-a9ae33c352812e40ca3d255a2533fea9>
- [24] Greenberg, A. (18.06.2025). Israel-tied Predatory Sparrow hackers are waging cyberwar on Iran's financial system. WIRED. <https://www.wired.com/story/israels-predatory-sparrow-hackers-are-waging-cyberwar-on-irans-financial-system/>
- [25] Check Point Software Technologies. (2026). The use of DDoS attacks in the Israel-Iran war. <https://checkpoint.cyberint.com/hubfs/The%20Use%20of%20DDoS%20Attacks%20in%20the%20Israel-Iran%20War.pdf>
- [26] Google Threat Analysis Group, Mandiant, & Google Trust & Safety. (2023). Fog of war: How the Ukraine conflict transformed the cyber threat landscape. Google. https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
- [27] CyberPeace Institute. (2023). Cyber dimensions of the armed conflict in Ukraine: Quarterly analysis report Q4 October to December 2022.
- [28] Del Fierro, C., & Dwyer, J. (24.02.2022). New destructive malware used in cyber attacks on Ukraine. IBM Security X-Force. <https://www.ibm.com/de-de/think/x-force/new-destructive-malware-cyber-attacks-ukraine>

Quellen & Methodik

Quellen III

- [29] **safeREACH. (13.03.2025). Bedrohung durch APT44/Sandworm für Unternehmen weltweit. safeREACH.** <https://safereach.com/de/wissen/apt44-sandworm-bedrohung-unternehmen/>
- [30] **Cybersecurity and Infrastructure Security Agency. (18.12.2025). Pro-Russia hackers conduct opportunistic attacks against US and global critical infrastructure. CISA.** <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-343a>
- [31] **Lang, T., Ramboll Management Consulting GmbH, Institut der deutschen Wirtschaft Köln e. V., Institut der deutschen Wirtschaft Köln Consult GmbH, Lübbers, T., Zetzsche, I., & Demary, V. (2026). Aktuelle Studienübersicht: Begleitforschung Mittelstand-Digital.** <https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/aktuelle-studien%C3%BCbersicht-digitalisierung-kmu.pdf>
- [32] **ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung. (o. D.). Digitale Souveränität: Unternehmen sehen Abhängigkeit bei KI und Software.** <https://www.zew.de/das-zew/aktuelles/digitale-souveraenitaet-unternehmen-sehen-abhaengigkeit-bei-ki-und-software>
- [33] **Lang, T., Scheufen, M., Engels, B., Institut der deutschen Wirtschaft Köln e. V., Institut der deutschen Wirtschaft Köln Consult GmbH, & Ramboll Management Consulting GmbH. (2026). Digitale Souveränität von KMU. Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie.** <https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/digitale-souveraenitaet.pdf>
- [34] **Gronau, N. (2026). Wie stark trägt der IT-Mittelstand den deutschen Mittelstand? Bundesverband IT-Mittelstand e. V.** <https://bitmi.de/wp-content/uploads/BITMI-Mittelstandsstudie.pdf>
- [35] **Deutsche Industrie- und Handelskammer, Siefert, A., & Sobania, K. (2026). Künstliche Intelligenz, Souveränität und Resilienz: DIHK-Digitalisierungsumfrage 2026.** <https://www.dihk.de/resource/blob/163540/486d8384c94a630d9aa0eaa978f0a786/dihk-digitalisierungsumfrage-2026-data.pdf>
- [36] **Transferstelle Cybersicherheit im Mittelstand. (o. D.). Cybersicher-Check.** <https://transferstelle-cybersicherheit.de/cybersicher-check/>
- [37] **Bundesamt für Sicherheit in der Informationstechnik. (o. D.). Cyber Resilience Act: Cybersicherheit EU-weit gedacht.** https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html
- [38] **Bundesamt für Sicherheit in der Informationstechnik. (o. D.). TÜV-Studie zur Cybersicherheit der deutschen Wirtschaft: Bedrohungslage steigt, Unternehmen wiegen sich in trügerischer Sicherheit.** https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/250611_TUEV-Studie_Cybersicherheit_Wirtschaft.html
- [39] **Transferstelle Cybersicherheit im Mittelstand. (o. D.). Neue Regeln für den Mittelstand durch NIS2 /** <https://transferstelle-cybersicherheit.de/schlaglichtthema-nis-2-richtlinie/>
- [40] **EASY.CRA. (o. D.).** <https://easycra.net/>
- [41] **FitNIS2 (o.D.).** <https://fitnis2.de/>
- [42] **Transferstelle Cybersicherheit im Mittelstand. (o. D.). Notfallhilfe.** <https://notfallhilfe.transferstelle-cybersicherheit.de/>

Sie haben Fragen zum Thema Cybersicherheit im Mittelstand?

Bitte wenden Sie sich an:
info@transferstelle-cybersicherheit.de

Sie möchten zum Thema
Cybersicherheit auf dem Laufenden
bleiben? Melden Sie sich jetzt für
unseren monatlichen Newsletter an.



Sie möchten mehr über die Initiative IT-Sicherheit in der Wirtschaft erfahren?

