CYBERsicher

IT-Sicherheit
IN DER WIRTSCHAFT

CYBERSICHER LAGEBILD

Die aktuelle Bedrohungslage für kleine und mittlere Unternehmen in Deutschland

Oktober 2025

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

Mittelstand-
Digital

aufgrund eines Beschlusses
des Deutschen Bundestages

Vorwort

Das vorliegende **Lagebild** zeigt eine besorgniserregende **Entwicklung** auf: Hackerangriffe auf deutsche Unternehmen, die auf Leakseiten veröffentlicht wurden, haben sich zwischen 2021 und 2024 mehr als vervierfacht. Diese Zahlen sind nicht nur Statistik. Sie spiegeln eine **Realität** wider, mit der sich täglich Tausende von Unternehmen konfrontiert sehen.

Besonders alarmierend ist die Erkenntnis, dass der Mensch nach wie vor das bevorzugte Einfallstor für Cyberkriminelle darstellt. **Phishing-Attacken**, bei denen sich Angreifer als vertrauenswürdige Personen oder Institutionen ausgeben, bleiben die **häufigste Angriffsform**. Dabei nutzen die Täter geschickt menschliche **Schwächen** aus, um sensible Daten abzugreifen.

Durch die zunehmende Professionalisierung von **Ransomware-Gruppen** (cyberkriminelle Erpresser, die Daten mithilfe von Schadsoftware verschlüsseln und nur durch Zahlung von Lösegeld wieder freigeben) erreicht das Phänomen Ransomware eine weitere Dimension. **Verschlüsselungstrojaner** bedrohen nicht nur die Verfügbarkeit wichtiger Unternehmensdaten, sondern entwickeln sich zunehmend zu komplexeren Angriffen mit sogenannter **„Double Extortion"** – der gleichzeitigen Verschlüsselung und Veröffentlichung gestohlener Daten.

Doch bei aller Dramatik der Lage zeigt unsere Analyse auch **positive Entwicklungen**. Viele mittelständische Unternehmen haben bereits erkannt, dass **Cybersicherheit** fest im **Unternehmen verankert** werden muss. Die über **1.000 Nutzer:innen** des Selbstchecks unserer **CYBERsicher Notfallhilfe** und die Ergebnisse des **CYBERsicher Checks** belegen ein wachsendes Bewusstsein für die Bedeutung präventiver Maßnahmen.

Und genau hier kommt unsere **Transferstelle Cybersicherheit im Mittelstand** ins Spiel. Wir stehen **kleinen** und **mittleren Unternehmen**, **Handwerksbetrieben** und **Start-ups** als kompetenter Partner zur Seite. Mit kostenfreien und anbieterneutralen **Angeboten**, dank der Förderung durch das Bundesministerium für Wirtschaft und Energie.

Von der **CYBERsicher Notfallhilfe** bis hin zu strukturierten **ISMS-Workshops**, unterstützen wir Unternehmen dabei, ihre digitale Resilienz zu stärken. Denn eines ist sicher: **Cybersicherheit** ist keine Option, sondern eine **Notwendigkeit** für alle, die im digitalen Zeitalter erfolgreich wirtschaften möchten.

Marc Dönges und Dirk Achenbach, Projektleitung
Transferstelle Cybersicherheit im Mittelstand

Dirk Achenbach

Marc Dönges

CYBERsicher

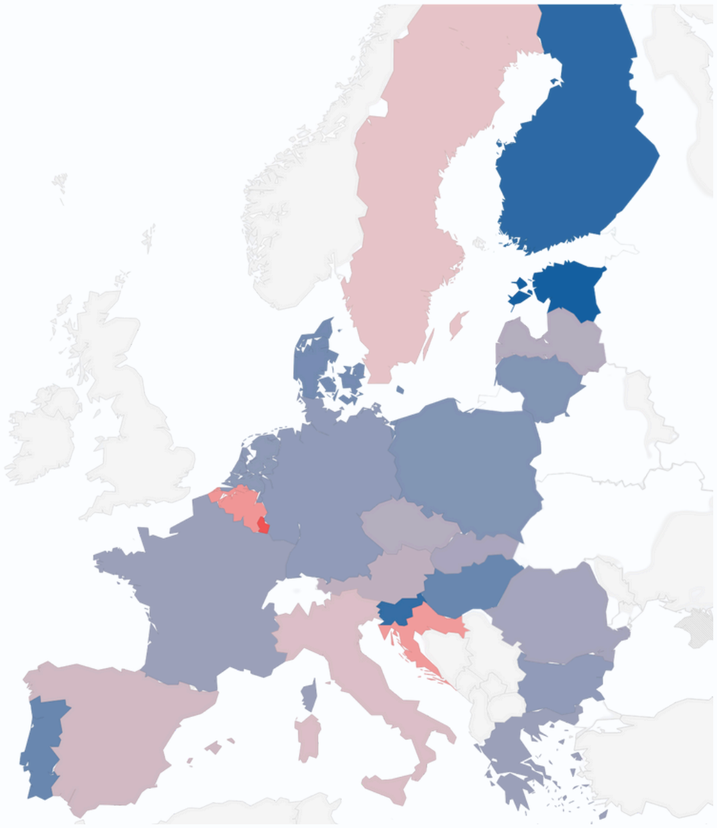
Cyberattacken: Deutschland im internationalen Vergleich

Die Bedrohungslage für Unternehmen in Europa spitzt sich zu und die Anzahl der Cyberangriffe steigt kontinuierlich. Hackerangriffe auf deutsche Unternehmen, die auf Leakseiten veröffentlicht wurden, haben sich zwischen 2021 und 2024 mehr als vervierfacht.

Im europaweiten Vergleich steht **Deutschland** an **sechzehnter Stelle** der meisten **Cyberangriffe** (in Bezug auf das Bruttoinlandsprodukt).

Die Anzahl der **Cyberangriffe auf KMU** in **Deutschland** hat sich in den letzten Jahren **ähnlich entwickelt** wie bei anderen europäischen Ländern.

2024 berichtete das **BKA**, dass mehr als **80 %** der **950 Ransomware-Angriffe** kleine und mittlere Unternehmen betroffen haben. In **251 Fällen** konnte über **ransomware.live** ein Datenabfluss nachgewiesen werden.

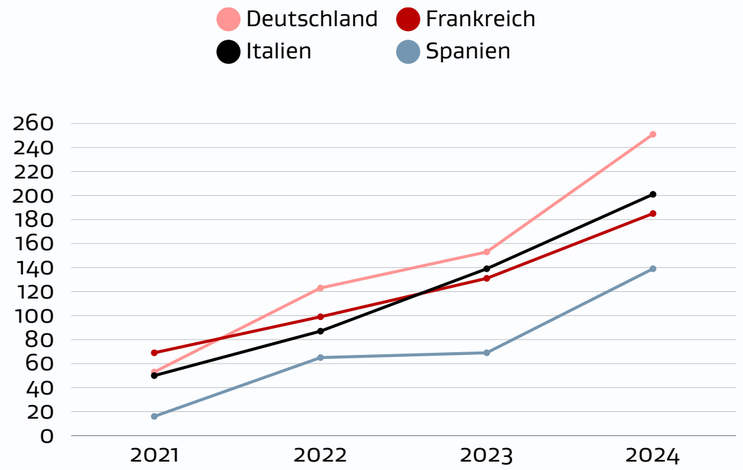


Angriffsdichte nach BIP

0 — 0,206

Entwicklung Anzahl Cyberangriffe auf Unternehmen

basierend auf Daten von ransomware.live



> *„Spätestens jetzt sollten mittelständische Unternehmen die Lage ernst nehmen und entsprechende Maßnahmen zur Absicherung ihrer Betriebe konsequent umsetzen.“*
> **Dirk Achenbach, Projektleiter der Transferstelle Cybersicherheit**

[1], [3], [21]

CYBERsicher

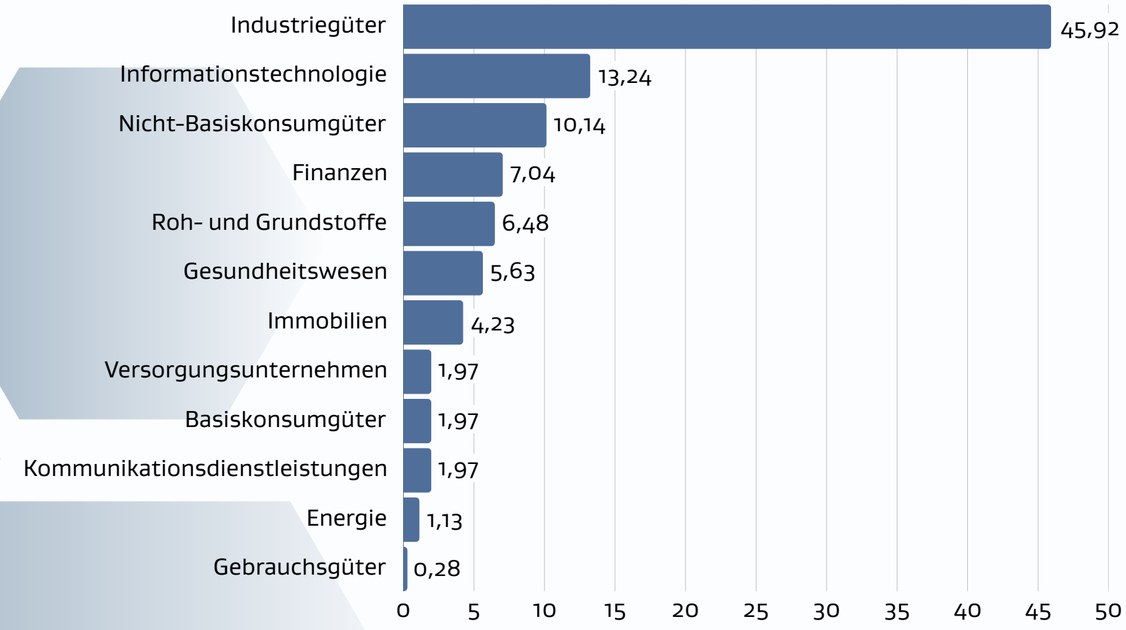
Deutsche Unternehmen im Visier der Hacker

Meist angegriffene Branchen

Die deutsche Industrie ist besonders häufig von Hackerattacken betroffen. Cyberangriffe haben dort weitreichende Folgen und wirken sich negativ auf die Produktion, Auslieferung und Kundenbeziehungen aus.

Aber auch die Branchen Informationstechnologie, Nicht-Basiskonsumgüter (z.B. Automobile, Elektronik oder Luxusgüter) und Finanzen sind attraktive Ziele für Cyberkriminelle.

Meist angegriffene Branchen in %



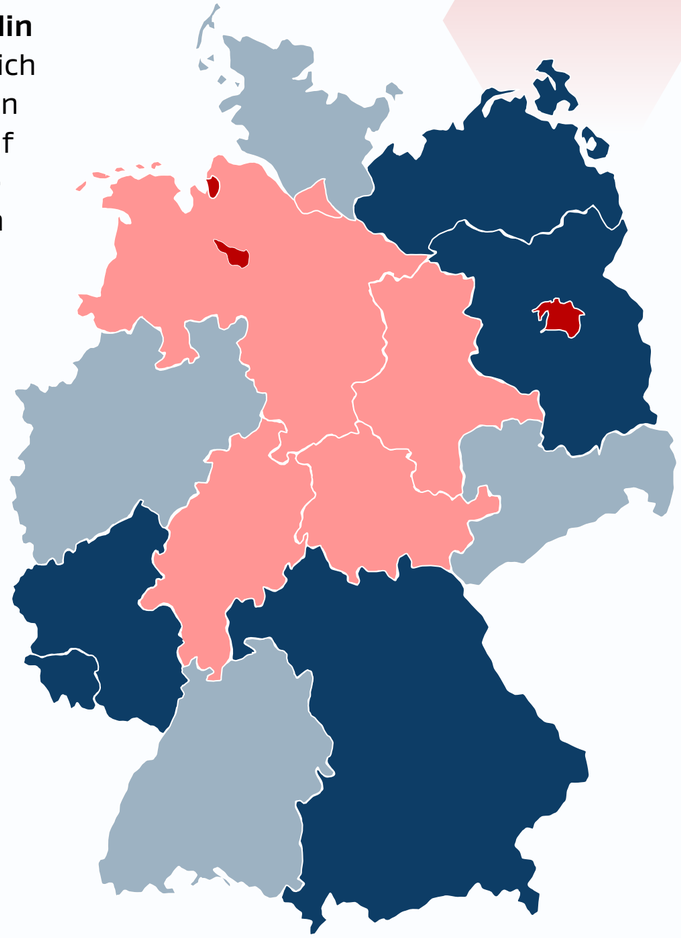
[3], [4], [5]

Angriffsverteilung pro KMU je Bundesland

Während die Bundesländer **Berlin** und **Bremen** überdurchschnittlich oft von Cyberangriffen betroffen sind, halten sich die Angriffe auf Unternehmen in **Mecklenburg-Vorpommern**, **Bayern** und dem **Saarland** in Maßen.

Angriffe pro KMU in 2024

1. **Bremen** – 0,175
2. **Berlin** – 0,108
3. **Sachsen-Anhalt** – 0,084



CYBERsicher

Eine Cybergefahr mit vielen Gesichtern

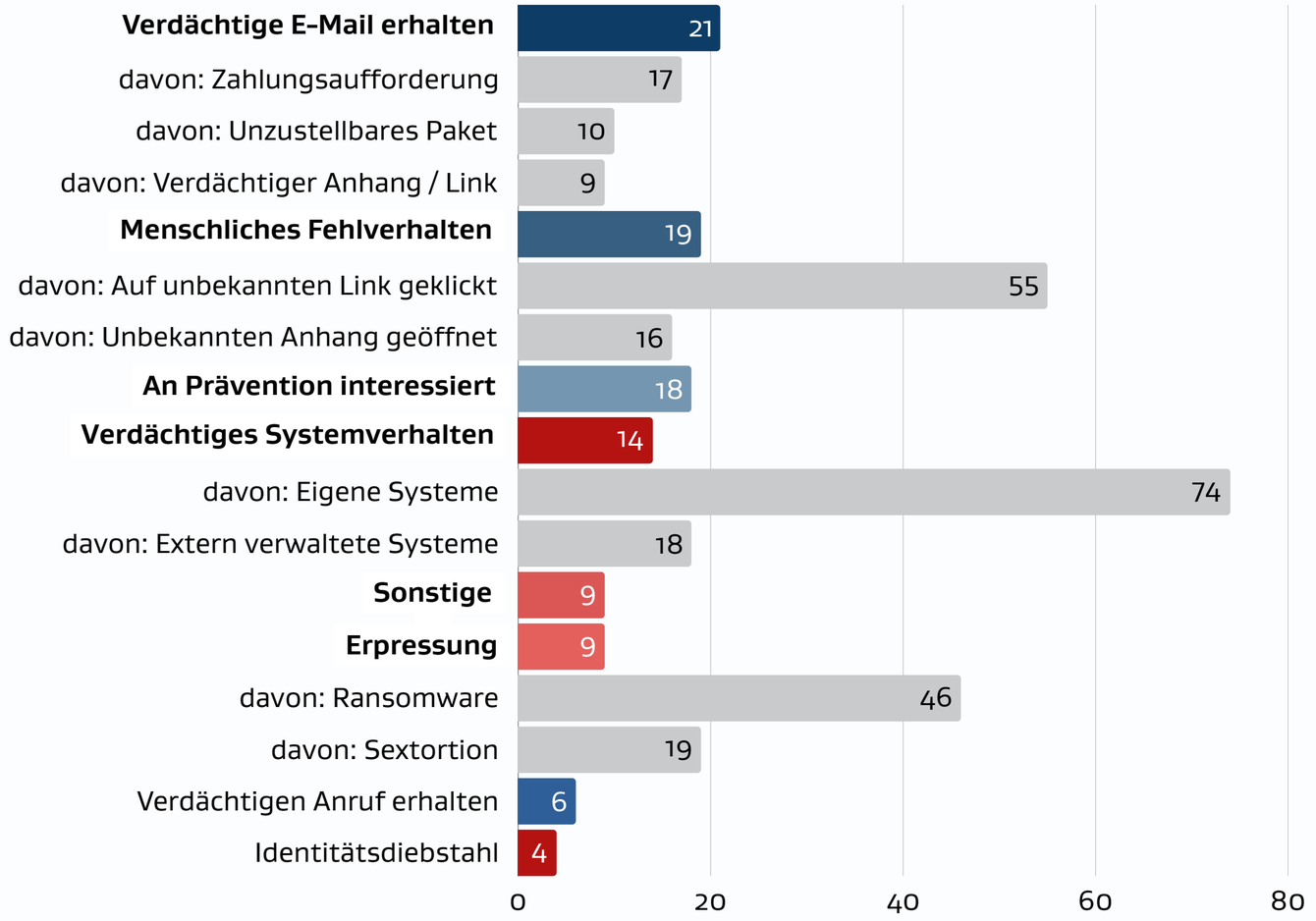
Was sind die Angriffsformen, die kleine und mittlere Unternehmen besonders betreffen?

Auf welche Bereiche der IT-Sicherheit sollten kleine und mittlere Unternehmen ihre Ressourcen fokussieren?

Bereits über **1.000 Personen** haben den **Selbstcheck** der **CYBERsicher Notfallhilfe** genutzt, um eine Einschätzung zu einem (möglichen) Angriff zu erhalten. Die Ergebnisse zeigen, dass sich die meisten Nutzer:innen aufgrund verdächtiger Mails an die Plattform wenden.

Der **Selbstcheck** der **CYBERsicher Notfallhilfe** gibt eine erste **Einschätzung**, ob ein Angriff vorliegt. Zusätzlich erhalten die Nutzer:innen eine Liste von **Handlungsempfehlungen**, um das **Schadensausmaß** zu begrenzen.

Häufigste Anfragen an den Selbstcheck in %



CYBERsicher

Der Faktor Mensch in der Cybersicherheit

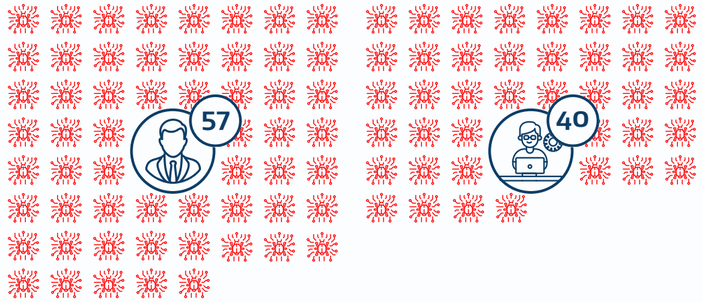
Neben technischen Schwachstellen sind die Mitarbeitenden von kleinen und mittleren Unternehmen ein beliebtes Angriffsziel.

Phishing-Attacken: Angreifer:innen geben sich per **E-Mail**, **SMS**, oder durch einen anderen **Kanal** als z. B. Geschäftsführer:innen, Administrator:innen, Geschäftskund:innen oder Paketzusteller:innen aus, um das Opfer zu einer unüberlegten Handlung zu verleiten.

Generell gilt: Ruhe bewahren und ein grundlegendes Misstrauen gegenüber ungewöhnlichen Prozessen.

Auf unserer **Materialienplattform** können Sie sich umfassend zu Cybersicherheitsthemen informieren.

Gezielte Angriffe pro Jahr



CEOs und **IT-Verantwortliche** sind häufig das Ziel von **Hackern**. **Geschäftsführende (CEOs)** erhalten durchschnittlich **57 gezielte Cyberangriffe** pro Jahr und **IT-Verantwortliche 40**.

Von Kaspersky-Lösungen blockierte Phishing-Versuche im Jahr 2024

Phishing-Versuche in Deutschland **37.5 Mio.**

Schädliche E-Mail-Anhänge **2.6 Mio.**

17 % der Bundesbürger:innen in Deutschland haben Phishingangriffe nicht als Phishing erkannt.

13 % der Betroffenen haben nach einem Phishingangriff ihre Zugangsdaten nicht geändert.

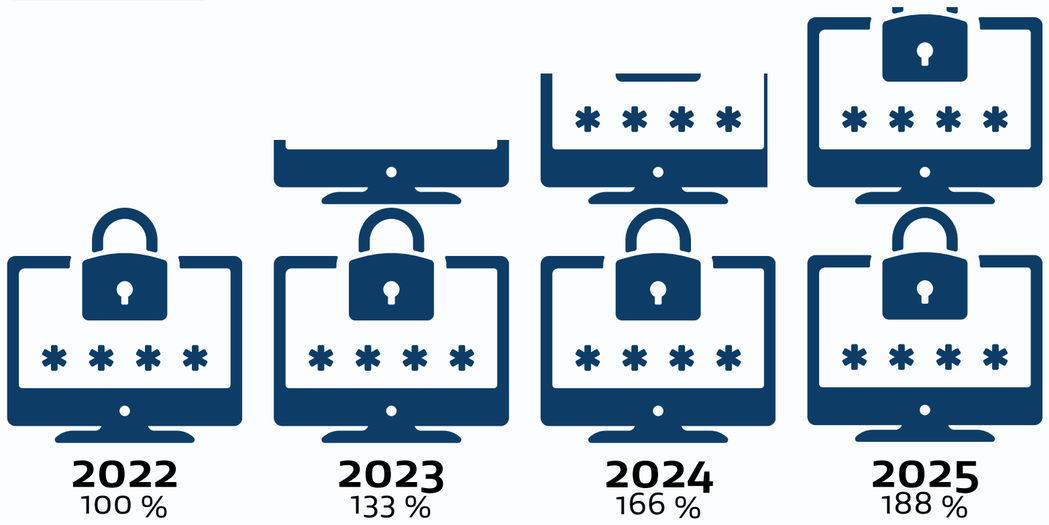
[7], [8]

CYBERsicher

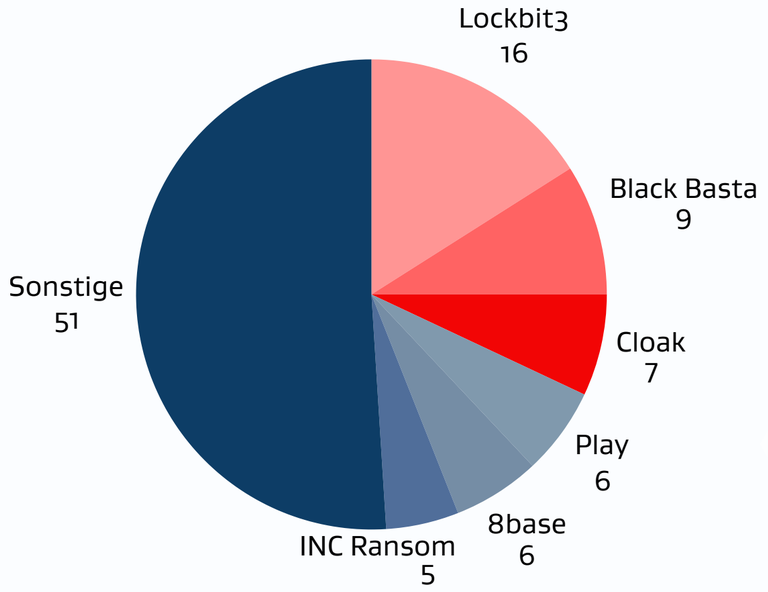
Das Phänomen Ransomware

Was ist Ransomware? Die **Verschlüsselungstrojaner** machen wichtige Daten unlesbar und die Hacker fordern ein Lösegeld, um die Daten wieder zu entschlüsseln. **Ransomware** ist ein weit verbreitetes und **ernstzunehmendes Phänomen**.

Aktuelle Entwicklungen: Bei einer Ransomware-Attacke muss in den meisten Fällen mit **Double Extortion** gerechnet werden. Dabei handelt es sich um **doppelte Erpressung** in Bezug auf zunächst die **Verschlüsselung** und dann die **Veröffentlichung** der **gestohlenen Daten**. Außerdem ist Phishing das mit Abstand größte Risiko für Unternehmen.



Wachstumsrate: Anzahl der bekanntgewordenen Ransomware-Angriffe auf deutsche KMU in % (Stand: 30.06.2025)
Zunahmen im Vergleich zum Referenzjahr 2022

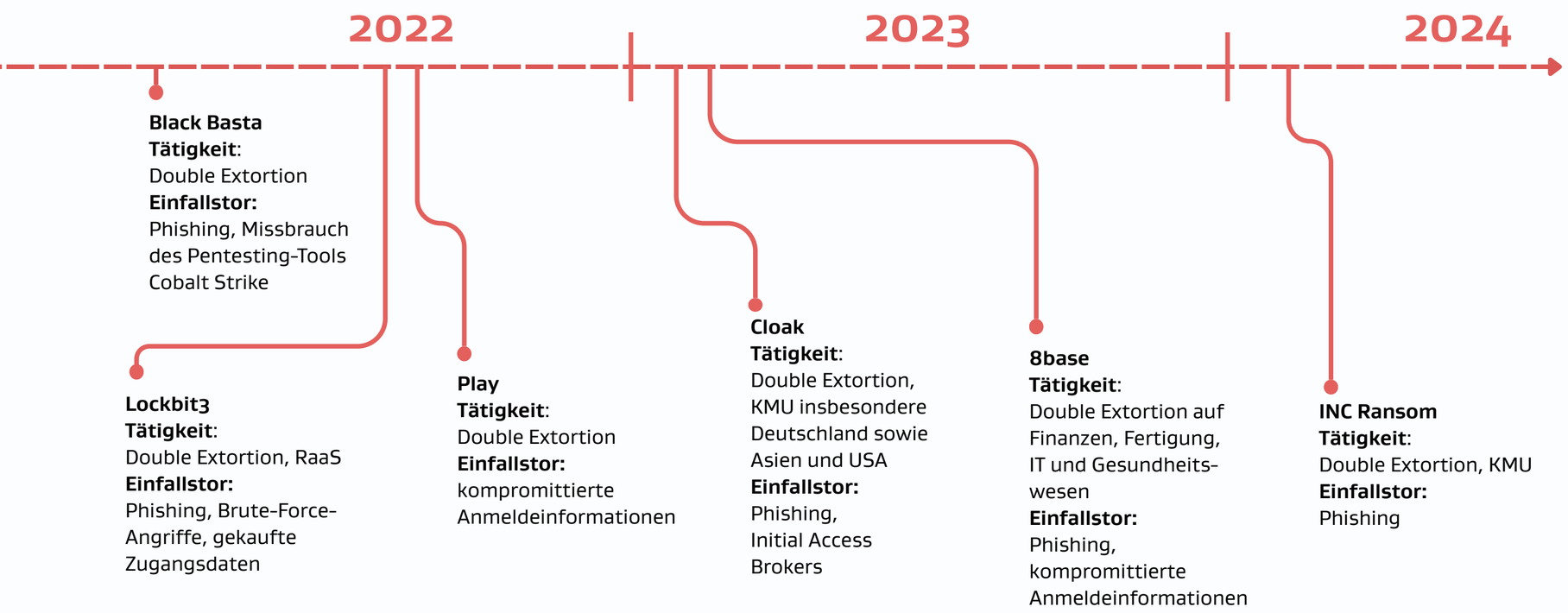


Aktivste Ransomware-Gruppen mit der Zielgruppe deutsche KMU 2024 in %

[3], [9], [10], [11], [12], [13], [14]

CYBERsicher

Das Phänomen Ransomware



Ransomware as a Service (RaaS):
Ransomware-Entwickler verkaufen ihre Schadsoftware an andere Hacker.

Brute-Force-Angriffe:
Systematisches Ausprobieren von Passwörtern, Login-Daten und gekaufte Zugangsdaten.

Initial Access Broker:
Hacker dringen in Netzwerke und Systeme von Unternehmen ein, etablieren dort Zugangsrechte und verkaufen diese dann im Darknet an andere Cyberkriminelle weiter.

[9], [10], [11], [12], [13], [14]

CYBERsicher

Datenschutz mitdenken, Bußgeld vermeiden

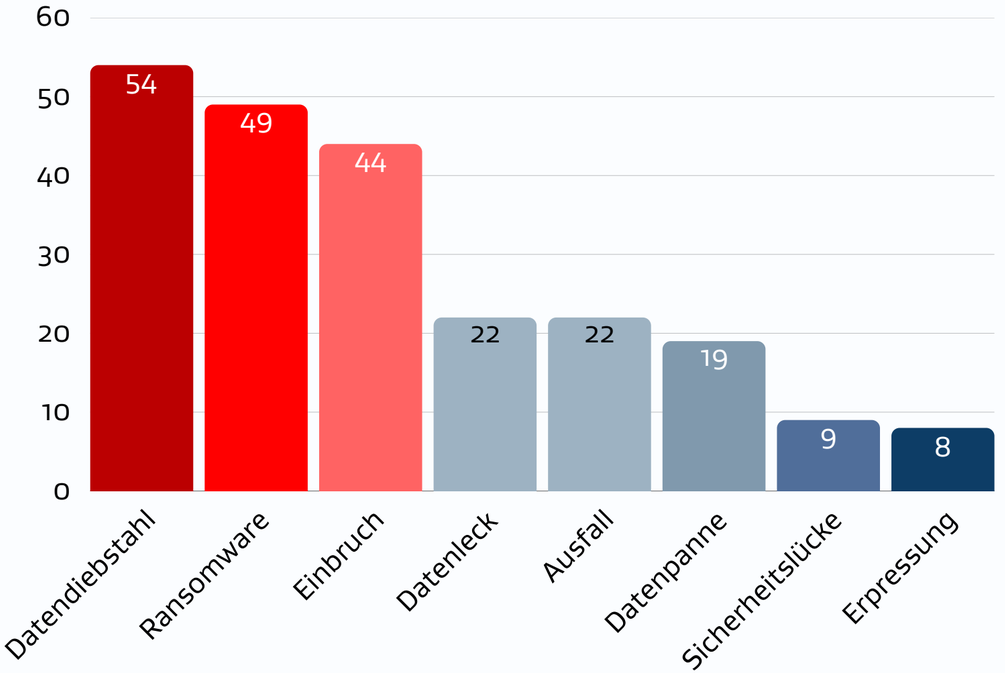
Art. 33 der Datenschutzgrundverordnung (DSGVO) verlangt bei einer Verletzung des Schutzes personenbezogener Daten eine unverzügliche Meldung des Vorfalls an die zuständige Aufsichtsbehörde.

Ein **Bußgeld** für **DSGVO-Verstöße** wird fällig, wenn u.a. die Regeln für die **Verarbeitung personenbezogener** Daten **missachtet** werden, beispielsweise durch das **Fehlen** einer **Datenschutzerklärung** oder die unverschlüsselte Übertragung von Daten.

In **87 %** der Fälle wird ein **Bußgeld** verhängt, das sehr gravierend ausfallen kann. Der **Durchschnitt** des **Bußgeldes** liegt bei über **350.000 €** mit einem **Median** von rund **7.000 €.**

[15]

Häufigste gemeldete Schlagwörter im Zusammenhang mit Cybersicherheit im DSGVO-Portal in %



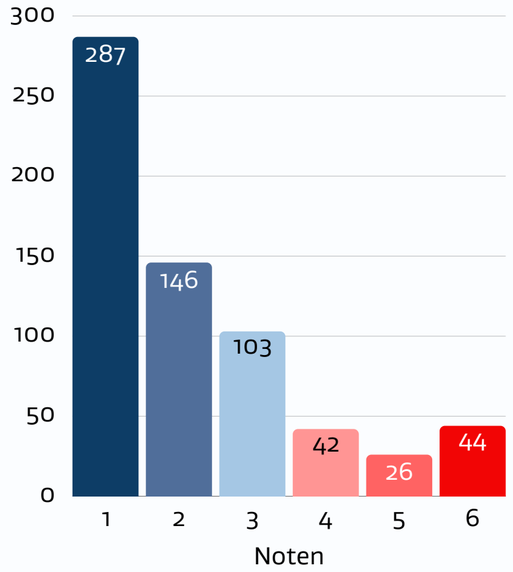
Mit **Datendiebstahl** und **Ransomware** gehören cyberkriminelle Tätigkeiten zu den **häufigsten** Ursachen für Meldungen im **DSGVO-Portal** im Zusammenhang mit Cybersicherheit. Das DSGVO-Portal ist eine Website, die eine Übersicht über DSGVO-Verstöße und - Verletzungen sowie Informationen rund um die Datenschutzgrundverordnung bietet.

CYBERsicher

So schützt sich der Mittelstand vor Cyberangriffen

Selbsteinschätzung von KMU in den jeweiligen Bereichen

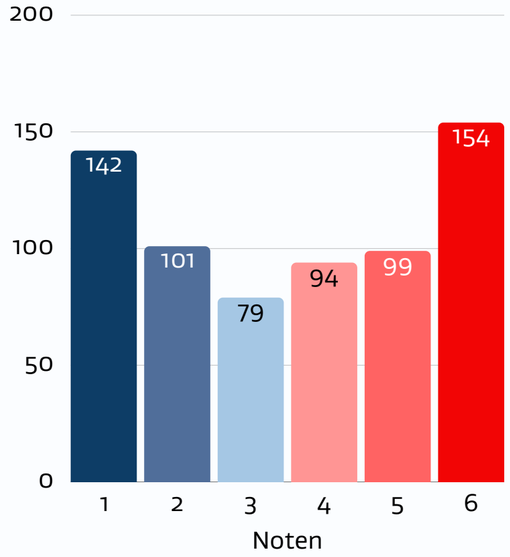
Bewertung von Sicherheitskopien (n = 669)



Die meisten Unternehmen besitzen ein gutes Konzept für **Sicherheitskopien**.

Wichtig ist, regelmäßig die Wiederherstellung der Daten zu üben.

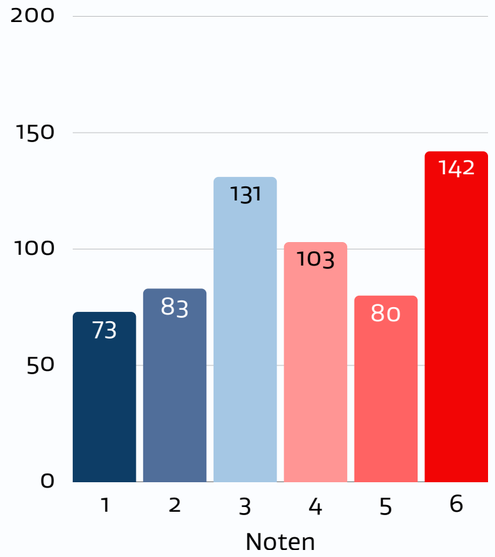
Bewertung von IT-Sicherheitsschulungen (n = 648)



Bei Schulungen gibt es ein gemischtes Bild, dabei ist der **Mensch** eine der größten Schwachstellen im Unternehmen.

Um diese Schwachstelle zu schließen, sind Schulungen das Mittel der Wahl.

Bewertung von Schutzbedarfsanalysen (n = 612)



Schutzbedarfsanalysen haben keinen hohen Stellenwert.

Organisatorische Maßnahmen sind stets die Grundlage für darauf aufbauende, technische Maßnahmen und sollten nicht vernachlässigt werden.

CYBERsicher

Wie KI die Cyberlandschaft verändert

Künstliche Intelligenz erleichtert nicht nur unseren Alltag, sondern auch den von Cyberkriminellen. **KI-generierte Phishing-Mails** sind mittlerweile hochprofessionell, sodass mehr als die Hälfte der Empfänger:innen darauf reinfallen. Auch Deepfake-Angriffe, bei denen gefälschte Medieninhalte zum Einsatz kommen, wachsen stark.

40% aller Phishing E-Mails sind KI generiert

40 %
erkennen diese
als Phishing

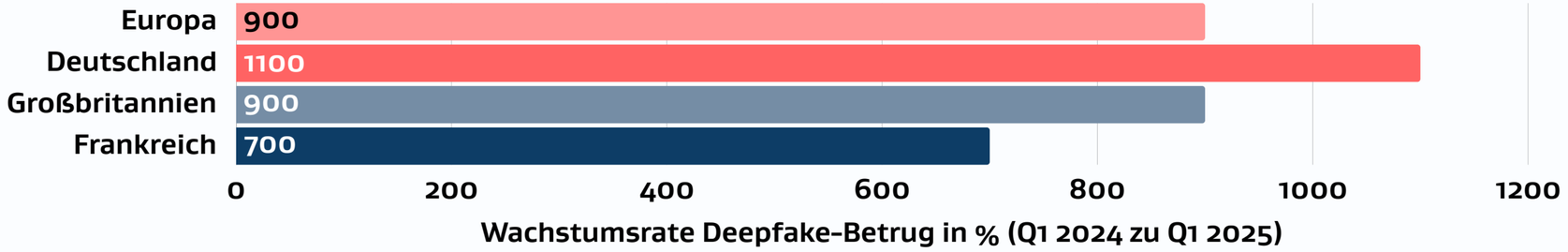
60 %
erkennen diese
nicht als Phishing

Die effektivsten Maßnahmen gegen Cyberangriffe – egal, ob durch Menschen oder KI – bleiben:

- Schulung der Mitarbeitenden hinsichtlich der Gefahren durch Phishing und KI
- Etablierung und Einhaltung starker Passwortrichtlinien
- Förderung und Sicherstellung einer konsequenten Cyberhygiene

Wachstumsrate Deepfake-Betrug (Q1 2025)

200 Millionen US-Dollar betragen die Kosten für Deepfake gestützten Betrug weltweit (Q1 2025)



[16], [17], [18], [19]

CYBERsicher

Schnelle Unterstützung im Ernstfall

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

11 Minuten dauert im Durchschnitt das Ausfüllen des **Onlineformulars** der **CYBERsicher Notfallhilfe** zur Dienstleistersuche.[1]

Zwischen einer **Anfrage** des Betroffenen und der ersten **Rückmeldung** durch einen Dienstleister vergehen im Durchschnitt **8 Minuten.**[2]

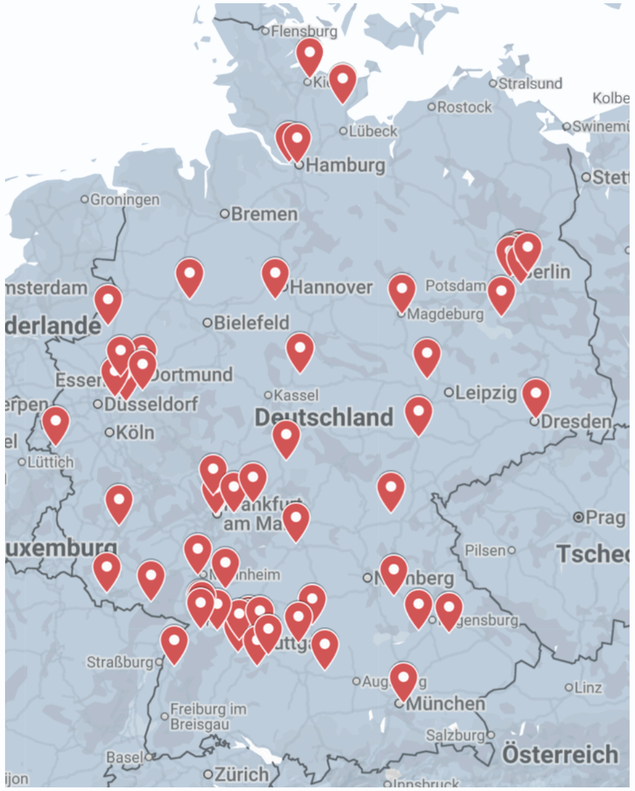
Dienstleister können in der Regel in unter **5 Stunden** nach erfolgter Anfrage mit ihrer **Unterstützung** beginnen.[3]

[1] n = 15, Durchschnitt (Plattformdaten und interne Auswertung)
[2] n = 12, Median
[3] n = 98, Median

Selbst betroffen?

Im Notfall professionelle Unterstützung finden.

Standorte der registrierten IT-Dienstleister der CYBERsicher Notfallhilfe



[6], [20]

CYBERsicher

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 KMU zu reduzieren.

[1] Destatis – Bruttoinlandsprodukt (BIP) Europa https://www.destatis.de/Europa/DE/Thema/Basistabelle/Uebersicht.html
[2] IfM Bonn – Anzahl KMU in der EU 2013–2023 https://www.ifm-bonn.org/.../Unternehmen_EU-27_ZR_2013-2023Sch.pdf
[3] Ransomware.live – Übersicht über Angriffe weltweit https://ransomware.live
[4] BKA – Polizeiliche Kriminalstatistik, Fälle nach Bundesland (2024) https://www.bka.de/.../LA-F-01-T01-Laender-Faelle_xls.xlsx
[5] IfM Bonn – KMU-Dichte Deutschland (2022) https://www.ifm-bonn.org/.../Unt_2022_D_BL_KMU-Dichte.pdf
[6] CYBERsicher Notfallhilfe – Selbstcheck (interne Quelle)
[7] Kaspersky – Phishing in Deutschland (2024) https://www.kaspersky.de/about/press-releases/kaspersky-report-rund-16-prozent-mehr-phishing-in-deutschland
[8] Aware7 – Statistik Social Engineering (700 Attacken pro Jahr) https://aware7.com/de/blog/social-engineering-statistik-700-attacken-pro-jahr
[9] Lockbit 3.0 – Joint Technical Advisory https://isomer-user-content.by.gov.sg/.../joint-technical-advisory-on-lockbit-3-0.pdf
[10] SentinelOne – BlackBasta Anthology https://www.sentinelone.com/anthology/black-basta/
[11] OwnSecurity – Cloak Ransomware Analyse https://www.own.security/.../click-clock-analyse-des-ttps-du-ransomware-cloak
[12] Vectra – Threat Actor „PLAY“ https://www.vectra.ai/modern-attack/threat-actors/play
[13] Checkpoint – 8base Ransomware Group https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/8base-ransomware-group/
[14] ReliaQuest – Inc.Ransom Analyse https://reliaquest.com/blog/inc-ransom-attack-analysis-extortion-methodologies/
[15] DSGVO-Portal – Schlagworte & Bußgelder https://www.dsgvo-portal.de
[16] VPNRanks – Statistiken zu KI-Cyberangriffen https://www.vpnranks.com/de-de/ressourcen/statistiken-zu-ki-cyberangriffen
[17] Resemble AI – Deepfake Threat Report Q1 2025 https://www.resemble.ai/.../ResembleAI-Q1-Deepfake-Threats.pdf
[18] IT-Daily – Bericht zu KI-Betrug (2025) https://www.it-daily.net/it-sicherheit/cybercrime/ki-betrug-explodiert
[19] AP News – KI-Impersonation Marco Rubio https://apnews.com/article/rubio-artificial-intelligence-impersonation-1b3cc78464404b54e63f4eba9dd4f5a9
[20] CYBERsicher Notfallhilfe – Interne Auswertungen (FZI, PLZ-Daten, Reaktionszeiten) (interne Quelle)
[21] Cybercrime Bundeslagebild, Bundeslagebild 2024, Seite 20 https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2024/CC_2024.html
[22] CYBERsicher Check https://transferstelle-cybersicherheit.de/cybersicher-check/

CYBERsicher

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.

Impressum: Impressum Der Mittelstand, BVMW e.V. | Potsdamer Straße 7 | 10785 Berlin |Vereinsregister Berlin Charlottenburg Nr. 19361 Nz | Ust.-ID-Nr. DE 230883382 Fachliche Erarbeitung: Dr. Dirk Achenbach (FZI Forschungszentrum Informatik), Sergio Marschall (FZI Forschungszentrum Informatik), Marc Nemes (FZI Forschungszentrum Informatik) - Text & Redaktion: Tamara Bayreuther (Der Mittelstand, BVMW e.V.), Johanna Baldus (Der Mittelstand, BVMW e.V.), Marc Dönges (Der Mittelstand, BVMW e.V.) | Verantwortlicher i.S.v. § 5 TMG: Lutz Kordges, Pressesprecher des BVMW | Vereinsregister Berlin Charlottenburg Nr. 19361 Nz | USt.-ID-Nr. DE 230883382 | Vertreten durch den Vorsitzenden der Bundesgeschäftsführung i.S.v. §26 BGB: Senator a. D. Christoph Ahlhaus | Design: Agentur Emilian | Stand: Oktober 2025

CYBERsicher