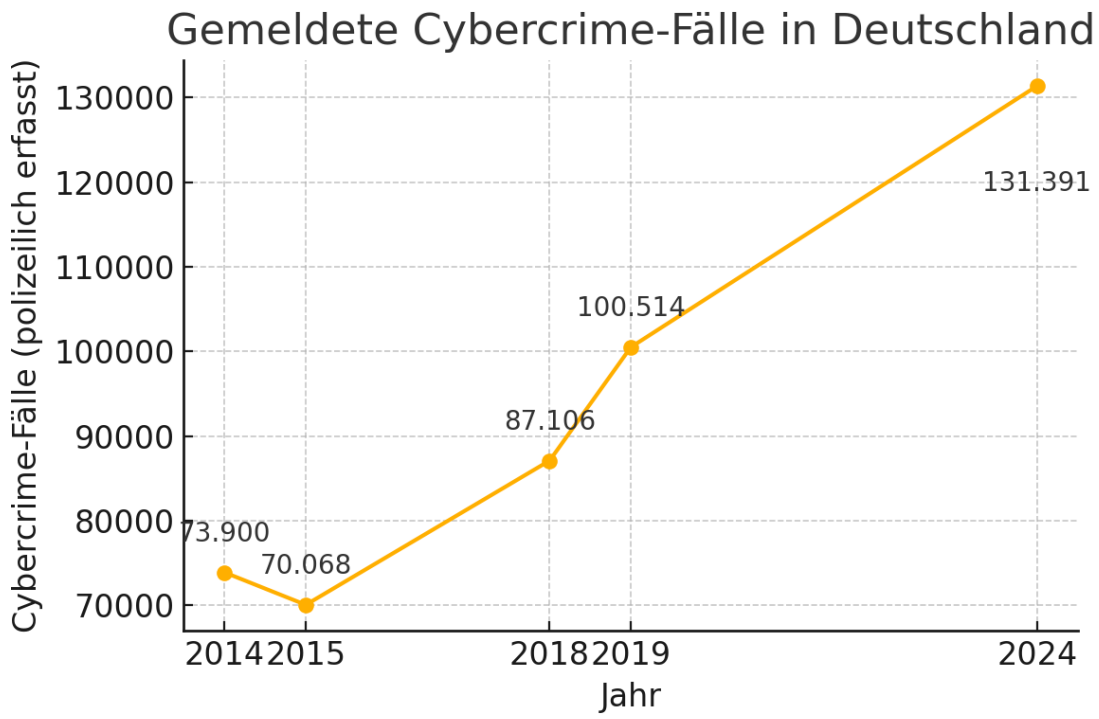
Statistiken zu Cyberangriffen im letzten Jahrzehnt (Fokus Deutschland)

Anstieg der Cyberangriffe seit 2015

In Deutschland ist die Anzahl der Cyberangriffe in den letzten 10 Jahren stark gestiegen. Laut polizeilicher Kriminalstatistik wurden 2014 rund 73.900 Fälle erfasst, 2015 etwa 70.000 Fälle[1]. Seitdem kletterten die Zahlen kontinuierlich: 2018 wurden 87.106 Fälle registriert, 2019 bereits 100.514 Fälle – ein Anstieg von über 15 % gegenüber 2018[2]. Aktuell erreicht die Cyberkriminalität neue Höchststände: Im Jahr 2024 verzeichnete die Polizei 131.391 Cybercrime-Fälle in Deutschland (Inland), **6,3 % mehr als im Vorjahr**[3]. Die tatsächlichen Vorfälle liegen vermutlich noch deutlich höher, da viele Unternehmen Vorfälle nicht melden (die Dunkelziffer gilt als *„überdurchschnittlich hoch“*[4]).



Gemeldete Cybercrime-Fälle in Deutschland. (Quellen: BKA/PKS[2][3])

Auch die **Betroffenheit von Unternehmen** hat drastisch zugenommen. Mitte der 2010er Jahre war etwa jedes zweite Unternehmen Opfer von Datendiebstahl, Spionage oder Sabotage; 2019 waren es schon **drei von vier Unternehmen**[5]. Neuere Studien zeigen einen weiteren Anstieg: 2024 meldeten **81 % der Unternehmen** einen erfolgreichen Angriff (plus weitere 10 % mit Verdacht)[6]. Im Jahr 2025 waren es sogar **87 % der Firmen** – nahezu neun von zehn Unternehmen[7]. Mit anderen Worten: **Cyberattacken sind für deutsche Unternehmen zur Regel geworden**, nicht mehr zur Ausnahme. Begleitet wird dieser Trend von steigenden Schadenssummen. Der geschätzte wirtschaftliche Schaden durch digitale Angriffe explodierte von rund **55 Mrd. €** im Jahr 2018 auf **102,9 Mrd. €** in 2019[8] und weiter

auf **223,5 Mrd. €** im Jahr 2021[9]. Nach einem leichten Rückgang 2022 (~205 Mrd. €) stieg der Schaden 2024 auf **266,6 Mrd. €** an und übertraf damit den bisherigen Rekord[9]. Zum Vergleich: Für 2025 wird ein weiterer Anstieg auf rund **289 Mrd. €** Schaden berichtet[10][7]. Dieser enorme finanzielle Schaden umfasst sowohl direkte Kosten (z.B. Betriebsunterbrechungen, Lösegeldzahlungen) als auch indirekte Verluste etwa durch Know-how-Abfluss und Plagiate[11][12].

Angriffsmethoden und genutzte Angriffswege

Welche Arten von Cyberangriffen stehen hinter diesen Vorfällen? In den letzten Jahren haben sich vor allem einige zentrale Bedrohungen herauskristallisiert:

- **Ransomware**: Erpressungs-Malware bleibt die größte Einzelbedrohung. 2024 wurden in Deutschland 950 Ransomware-Angriffe polizeilich gemeldet[13]. Bei solchen Angriffen verschlüsseln Kriminelle Firmendaten und verlangen Lösegeld für die Entschlüsselung – oft kombiniert mit Datendiebstahl (*Double Extortion*)[14]. Rund *72 %* der Ransomware-Fälle gehen mit Datenabzug einher[15]. Durchschnittlich flossen pro Vorfall fast 280.000 USD Lösegeld, wenn bezahlt wurde[15]. In Unternehmensumfragen gaben **31 %** der Firmen an, durch Ransomware **Schäden** erlitten zu haben[16] (z.B. Ausfall von IT-Systemen, Wiederherstellungskosten). Damit verursachte Ransomware 2024 in Deutschland den größten Anteil am Gesamtschaden (geschätzt **178,6 Mrd. €**, ca. 67 % der Schadenssumme)[17][16].

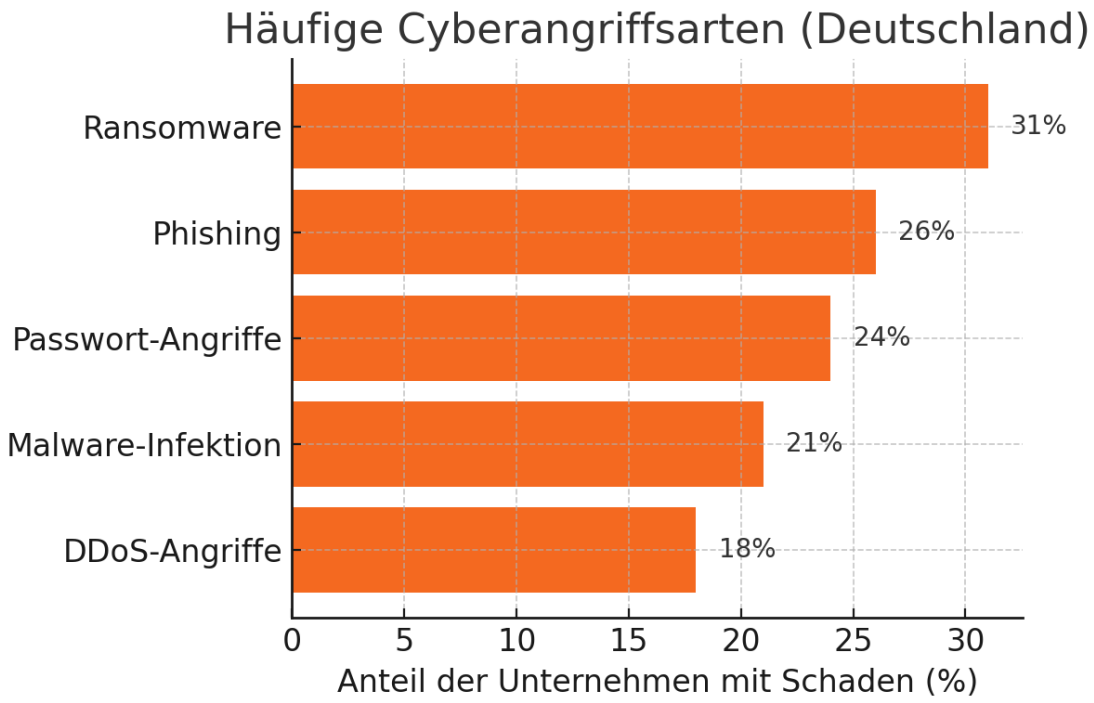
- **Phishing & Social Engineering**: Nach wie vor ist Phishing der häufigste *Angriffsvektor*, um erste Zugangsdaten abzugreifen. Laut EU-Agentur ENISA erfolgen die meisten ersten Kompromittierungen über **Phishing-Mails** oder ähnliche Täuschungsmanöver[18]. In Deutschland berichteten **26 %** der Unternehmen von Schäden durch Phishing-Attacken[16]. Darüber hinaus verzeichnete jedes zweite Unternehmen Social-Engineering-Versuche (z.B. Telefonanrufe oder gefälschte E-Mails, um Mitarbeiter zu manipulieren)[19]. Gerade **E-Mails** bleiben ein zentrales Einfallstor – 63 % der betroffenen Firmen nannten kompromittierte E-Mails bzw. Kommunikationsdaten als Folgeschaden[20].

- **Angriffe auf Zugangsdaten**: Die Kompromittierung von Passwörtern und Konten ist ein weiterer verbreiteter Angriffsweg. **Schwache oder gestohlene Passwörter** werden gezielt ausgenutzt. Etwa **24 %** der deutschen Unternehmen erlitten laut Umfrage Schäden durch Passwort-Angriffe (z.B. Kontoübernahmen)[16]. Häufig gelangen Angreifer via Phishing oder durch Leaks an die Zugangsdaten und verschaffen sich so Zugriff auf interne Systeme.

- **Schadsoftware (Malware)**: Klassische Malware-Infektionen – etwa durch verseuchte E-Mail-Anhänge oder Drive-by-Downloads – treten weiterhin oft auf. **21 %** der Firmen meldeten Schäden durch Malware-Infizierungen jenseits von Ransomware[16]. Hierzu zählen z.B. Trojaner, Spyware oder Crypto-Miner, die Daten stehlen oder Systeme beeinträchtigen. Die Zahl neuer Schwachstellen und Exploits

ist hoch – durchschnittlich werden rund 70 neue Sicherheitslücken pro Tag entdeckt (15 % davon kritisch)[21], die von Malware ausgenutzt werden können.

- **Denial-of-Service (DDoS)**: **Distributed Denial-of-Service**-Angriffe, die Server oder Netzwerke durch Überlastung lahmlegen, machen einen wachsenden Teil der Vorfälle aus. Rund **18 %** der Unternehmen in Deutschland berichten von DDoS-Schäden[16]. DDoS wird häufig von **Hacktivisten** in politischen Konflikten eingesetzt (z.B. pro-russische Gruppen gegen deutsche Webseiten)[22]. ENISA führt DDoS als **zweithäufigste** Cyberbedrohung in Europa an[23][18]. Die Angriffe werden volumetrisch immer größer und zielen vermehrt auch auf Cloud- und IoT-Infrastruktur.



Häufige Cyberangriffsarten in deutschen Unternehmen (Anteil der befragten Unternehmen, die dadurch Schaden erlitten).[16]

Neben diesen Hauptbedrohungen gibt es eine Vielzahl weiterer **Angriffsformen**. Darunter fallen z.B. **Supply-Chain-Angriffe**, bei denen Partner oder Dienstleister gehackt werden, um anschließend das eigentliche Zielunternehmen zu infiltrieren[24]. Auch neuere Methoden wie **Deepfakes** (KI-generierte Fake-Inhalte) oder **Voice Phishing (Vishing)** zeichnen sich ab – bislang führen sie jedoch eher selten zu Schäden (je ~3 % der Unternehmen)[25]. Klassische *analoge* Angriffe nehmen parallel ebenfalls zu: 50 % der Firmen berichten von **Diebstahl physischer Dokumente** und 30 % sogar von **Abhören von Besprechungen** vor Ort[26]. Die Grenzen zwischen digitaler und physischer Spionage verschwimmen, da Angreifer oft **mehrstufig** vorgehen (z.B. erst Hacking, dann Einschleusen von Personen vor Ort)[27]. Insgesamt steigt **Professionalität und Diversität** der Angriffe: Täter passen ihre Methoden laufend an neue Technologien und Gelegenheiten

an[28]. Unternehmen sehen sich daher einer immer breiteren Palette an Bedrohungen gegenüber.

Wandel von internen zu globalen Bedrohungen

Vor rund 20 Jahren galt oft der Grundsatz, die größten Risiken lauerten **im eigenen Hause** – viele Vorfälle gingen auf Mitarbeiter (Insider) oder interne Fahrlässigkeit zurück. Heute hat sich dieses Bild deutlich gewandelt: Die **meisten Angriffe erfolgen von außen** und häufig aus dem Ausland. Studien zeigen, dass Angriffe aus Deutschland im Verhältnis abgenommen haben. So konnten 2024 nur noch 20 % der betroffenen Firmen mindestens einen Angreifer in Deutschland verorten (2023: 29 %)[6]. Dagegen stammen zunehmend Attacken aus **anderen Ländern**: China (45 % der Unternehmen betroffen) und Russland (39 %) zählten 2024 zu den häufigsten Ursprungsländern für Attacken auf deutsche Firmen[6]. Im Jahr 2025 lagen China und Russland mit je 46 % Nennungen gleichauf als Hauptquellen für Cyberangriffe[12]. Auch osteuropäische Nicht-EU-Staaten, die USA oder andere EU-Länder tauchen oft als Ursprungsort auf[12]. Diese *Globalisierung der Bedrohung* bedeutet, dass Angreifer nicht mehr lokal gebunden sind – im Internet können ausländische Hackergruppen gezielt deutsche Unternehmen angreifen, sei es aus finanziellen Motiven oder im staatlichen Auftrag.

Die Folge: **Organisierte Cyberkriminalität** agiert heute überwiegend international. Das Bundeskriminalamt (BKA) betont, dass Cyberkriminelle „international vernetzt und arbeitsteilig“ vorgehen[29]. Viele Gruppen operieren aus Osteuropa oder Asien und greifen via Internet weltweit Ziele an. Insider-Vorfälle im Unternehmen (etwa Datendiebstahl durch Beschäftigte) bleiben zwar eine Gefahr – laut einer Umfrage erlebten 53 % der Firmen in einem Jahr einen solchen Insider-Zwischenfall[30] – doch **Insider sind nicht mehr der dominierende Angreifertyp**. Stattdessen sehen sich Unternehmen vor allem mit externen, hochspezialisierten Tätern konfrontiert.

Bemerkenswert ist der Anstieg **staatlich gesteuerter Angriffe** und *Hacktivismus*. Sicherheitsbehörden berichten, dass ausländische Nachrichtendienste verstärkt die deutsche Wirtschaft ins Visier nehmen[31]. 2024 konnten 20 % der betroffenen Firmen mindestens eine Attacke einem ausländischen Geheimdienst zuordnen – 2025 waren es schon 28 %[31]. Parallel dazu verübten politisch motivierte Gruppen (etwa pro-russische „Hacktivisten“) zahlreiche DDoS-Angriffe auf Behörden und Unternehmen, etwa im Kontext des Ukraine-Kriegs oder Nahost-Konflikts[32]. Insgesamt hat sich die Bedrohungslandschaft also **von der internen zur globalen Arena** verlagert: Angreifer agieren grenzüberschreitend, hochprofessionell und oft im Verborgenen.

Ziele und Motive der Angreifer

Welche Ziele verfolgen Cyberkriminelle? Im Wesentlichen lassen sich drei Motivfelder ausmachen:

- **Finanzielle Motivation (Cybercrime)** – Der größte Teil der Angriffe dient heute monetären Zwecken. Professionelle Banden wollen **Geld erbeuten**, sei es durch Erpressung (Ransomware), Betrug oder den Verkauf gestohlener Daten. Laut

Bitkom-Umfrage ordneten 2024 rund **70 %** der betroffenen Unternehmen die Täter der organisierten Kriminalität zu[33]. Diese kriminellen Gruppen agieren wie Unternehmen: Sie suchen maximalen Profit. Beliebte Ziele sind daher *wirtschaftlich lukrative Firmen* und kritische Infrastrukturen, wo die Zahlungsbereitschaft hoch ist[34]. Ransomware-Erpresser etwa wählen zunehmend lohnende Opfer (Industrie, Versorger), bei denen Ausfallzeiten teuer sind[35]. Auch Online-Betrug (z.B. CEO-Fraud, Online-Banking-Betrug) zielt auf direkte Einnahmen. Kurz gesagt: **„Geld verdienen" ist ein Hauptmotiv** – Cybercrime hat sich zu einem lukrativen Geschäftsmodell entwickelt.

- **Industriespionage & Informationsdiebstahl** – Ein zweites großes Motiv ist **Spionage**. Staatlich gesteuerte Hacker oder Konkurrenten versuchen, *geistiges Eigentum*, Forschungsergebnisse, Geschäftsgeheimnisse oder personenbezogene Daten zu stehlen. Dies dient der **Wirtschaftsspionage** (Wissensvorsprung, Kopieren von Technologien) oder klassischen Nachrichtendienst-Interessen. Der Verfassungsschutz beobachtet eine zunehmende Verzahnung von Cyberspionage und Cybercrime[27] – oft stecken hinter Attacken sowohl finanzielle als auch strategische Interessen. 2024 gaben 20 % der deutschen Unternehmen an, Angriffe ausländischen Geheimdiensten zugeordnet zu haben (zum Vergleich: 2023 erst 7 %)[33]. Ziele solcher Spionageangriffe sind vor allem **High-Tech-Branchen**, Mittelständler mit innovativen Produkten und staatliche Stellen. Die gestohlenen Daten reichen von Kundendaten (bei 62 % der betroffenen Firmen) über Zugangsdaten (35 %) bis hin zu *Patenten und F&E-Informationen* (26 %)[20]. Spionage-Motive überschneiden sich mit Sabotage, wenn z.B. staatliche Akteure kritische Infrastruktur auskundschaften oder stören.

- **Sabotage, Rache & „weil man es kann"** – Einige Angriffe erfolgen auch aus **ideologischen oder destruktiven Motiven**. Hierunter fallen etwa Hacktivisten, die Websites lahmlegen, um politische Botschaften zu senden, oder Insider, die aus Unzufriedenheit Schaden anrichten. In den letzten Jahren haben insbesondere politische Konflikte **Sabotageakte** im Cyberraum begünstigt. Beispielsweise wurden 2023 vermehrt *anti-israelische und pro-russische* DDoS-Kampagnen gegen deutsche Ziele registriert[22]. Solche Angriffe erfolgen nicht primär wegen Geld, sondern aus ideologischer Motivation („weil sie es können" oder um Aufmerksamkeit zu erzeugen). Auch Fälle von reiner Zerstörlust (Vandalismus) und Testen der eigenen Fähigkeiten gehören in diese Kategorie, sind allerdings schwer zu beziffern. Für Unternehmen sind diese Angriffe genauso gefährlich, da sie Betriebsabläufe stören können, ohne dass ein rationales finanzielles Motiv dahintersteht.

In der Praxis verschwimmen die Grenzen oft. **Kriminelle Banden und staatliche Gruppen kooperieren** teilweise oder nutzen ähnliche Tools, was die Attribution erschwert[36][37]. Fest steht aber: *Organisierte Cybercrime-Gruppen stellen derzeit die Hauptbedrohung*, gefolgt von staatlich gelenkten Akteuren[38]. Hacktivisten und Insider sind im Vergleich zwar weniger häufig, können aber in Einzelfällen gravierende Schäden anrichten. Unabhängig vom Motiv zielen die Angriffe häufig auf **Maximalschaden**: Sei es durch

Diebstahl sensibler Daten, großflächige Systemausfälle (z.B. durch Ransomware oder wiper-Malware) oder Kombinationen davon, um die Opfer maximal unter Druck zu setzen[17][16].

Wahrscheinlichkeit von Angriffen – Fokus KMU

Wie wahrscheinlich ist ein Cyberangriff? Für **kleine und mittlere Unternehmen (KMU)** ist diese Frage von besonderer Bedeutung, da sie oft weniger Ressourcen für IT-Sicherheit haben. Die Statistik zeigt eindeutig: **Jedes Unternehmen kann zum Opfer werden.** Eine repräsentative Befragung ergab, dass in den Jahren 2020/2021 **88 % der deutschen Unternehmen** mindestens einen Cyberangriff erlitten[39]. 2024 lag die Quote – wie oben erwähnt – bei über 80 %[6], Tendenz steigend. KMU sind dabei keineswegs ausgenommen. Im Gegenteil: Laut BKA entfielen rund **80 % der Ransomware-Betroffenen auf KMU**[40] – gerade mittelständische Betriebe werden also überproportional häufig von Verschlüsselungstrojanern getroffen. Der Branchenverband Bitkom formuliert es drastisch: *„Wird mein Unternehmen Opfer von Cybercrime? – Das ist keine Frage des Ob, es geht lediglich um das Wann und Wie."*[41]. Ähnlich warnt Bitkom-Präsident Ralf Wintergerst 2025: *„Die Frage ist nicht, ob Unternehmen angegriffen werden, sondern wann – und ob sie diese Angriffe erfolgreich abwehren können."*[42].

Für KMU bedeutet dies, dass die **Angriffswahrscheinlichkeit nahe bei 100 %** liegt, sobald man einen genügend langen Zeitraum betrachtet. Studien legen nahe, dass ein durchschnittliches Unternehmen mittlerweile *mehrere Angriffsversuche pro Tag* auf seine IT verzeichnet – viele davon automatisiert durch Bots, die rund um die Uhr nach Schwachstellen suchen. In Deutschland registriert das BSI z.B. täglich über 200.000 neue Varianten von Schadprogrammen[43] (Stand: BSI-Lagebericht 2024). Zwar führen nicht all diese Versuche zum Erfolg, doch allein die Wahrscheinlichkeit, Ziel von Angriffsbemühungen zu sein, ist extrem hoch. Besonders perfide: Viele Angriffe treffen **unspezifisch** jede erreichbare Firma (z.B. Massenphishing, Zufallsransomware), sodass *auch kleinste Betriebe ins Visier geraten*, selbst wenn sie kein prominentes Profil haben. Gleichzeitig gibt es gezielte Kampagnen gegen bestimmte Branchen: 2024 waren etwa Unternehmen aus Handel, Gesundheitswesen und verarbeitendem Gewerbe besonders oft Ziel von Attacken[44].

Statistiken zur **Eintrittswahrscheinlichkeit** eines erfolgreichen Hacks bei KMU lassen sich aus den genannten Betroffenheitsraten ableiten: So liegt die Chance, dass ein KMU innerhalb eines Jahres einen Cybervorfall erleidet, derzeit bei rund 80–90 %. Viele Sicherheitsexperten argumentieren daher, dass Unternehmen Vorsorge für den *Ernstfall* treffen müssen anstatt darauf zu hoffen, verschont zu bleiben[45]. Die hohe Bedrohungslage spiegelt sich auch in der Wahrnehmung der Firmen wider: Zwei Drittel der Unternehmen (65 %) sehen ihre **Existenz durch Cyberangriffe bedroht**[46]. Vor zwei Jahren lag dieser Wert noch unter 10 %[47] – ein drastischer Wandel, der zeigt, wie real die Gefahr mittlerweile eingeschätzt wird. Für KMU heißt das: **Cyberrisiken gehören heute zu den größten Geschäftsrisiken**, vergleichbar mit Brand oder Diebstahl. Dementsprechend raten Behörden und Verbände dringend, IT-Sicherheitsmaßnahmen zu erhöhen und Notfallpläne parat zu haben[48][49].

Deutschland/EU vs. USA: Regulierung und Einfluss auf Cyberkriminalität

Im internationalen Vergleich unterscheidet sich der Umgang mit Cyberangriffen und deren Meldepflichten teils deutlich. Die Europäische Union und Deutschland haben in den letzten Jahren umfangreiche **gesetzliche Vorgaben** eingeführt, die auf höhere Cyber-Sicherheit abzielen. Beispiele sind die Datenschutz-Grundverordnung (**DSGVO**, seit 2018), die EU-Richtlinie zur Netz- und Informationssicherheit (**NIS** 2018 und verschärft **NIS2** ab 2024) sowie sektorspezifische Regeln wie der Digital Operational Resilience Act (**DORA**, 2022) für die Finanzbranche. Diese Regulierungen haben **indirekte Auswirkungen** auf die Cyberkriminalität:

- **Erhöhte Transparenz und Meldepflichten**: Die DSGVO schreibt Unternehmen vor, *IT-Sicherheitsvorfälle mit personenbezogenen Daten binnen 72 Stunden* an die Aufsichtsbehörden zu melden[50]. Dadurch ist die Zahl der bekannt gewordenen Datenlecks sprunghaft gestiegen – viele Vorfälle, die früher vertuscht worden wären, erscheinen nun in der Statistik. Ähnliches gilt für NIS/NIS2, die Betreiber kritischer Infrastrukturen und essenzieller Dienste verpflichten, erhebliche Cybervorfälle zu melden und Sicherheitsmaßnahmen einzuhalten. In der EU wurden zwischen Juli 2022 und Juni 2023 insgesamt ca. **2.580 bedeutende Cyber-Zwischenfälle** erfasst, darunter 220 grenzüberschreitende Angriffe auf mehrere EU-Staaten[51]. Diese Zunahme an Meldungen bedeutet aber nicht unbedingt, dass es *durch die Gesetze* mehr Angriffe gibt – vielmehr kommen sie nun ans Licht. Auch in den USA gibt es neuerdings Meldepflichten (z.B. SEC-Regel 2023 für börsennotierte Firmen), jedoch ist das System fragmentierter, da kein einheitliches Bundesdatenschutzgesetz wie die DSGVO existiert.

- **Höhere Sicherheitsstandards**: EU-Vorgaben zwingen Unternehmen, **präventiv in IT-Sicherheit zu investieren**. Die DSGVO droht bei Verstößen Strafen bis zu 4 % des weltweiten Umsatzes an – ein starker Anreiz, Datenschutz und IT-Sicherheit zu verbessern[52]. NIS2 verlangt von deutlich mehr Unternehmen (u.a. Mittelständlern in wichtigen Sektoren) die Einführung von Mindeststandards, Risikoanalysen und Incident Response Plänen. DORA schreibt Finanzinstituten robuste Resilienzstrategien und regelmäßige Penetrationstests vor. Diese **Compliance-Maßnahmen** erhöhen tendenziell die Widerstandsfähigkeit gegen Angriffe. So ist in Deutschland der Anteil des IT-Sicherheitsbudgets an den IT-Ausgaben zuletzt deutlich gestiegen (im Schnitt 17 % des IT-Budgets 2024, vs. 9 % in 2022)[53]. Regulierungen wie IT-SiG 2.0 (Deutschland) gehen in eine ähnliche Richtung, indem sie branchenspezifische Sicherheitsstandards festlegen. Langfristig könnten solche Maßnahmen das *Cyberrisiko reduzieren*, indem „low-hanging fruits“ für Angreifer weniger werden.

- **Abschreckung der Täter**: Ob strengere Gesetze direkt zu weniger Cybercrime führen, ist unklar. Cyberkriminelle selbst werden von Datenschutzgesetzen kaum abgeschreckt – sie operieren oft in Rechtsräumen, wo ihnen keine Konsequenzen drohen, und die Strafverfolgung hapert angesichts internationaler Hürden. Allerdings **nutzen Täter EU-Vorschriften teils sogar aus**: Ransomware-Gruppen

drohen z.B., gestohlene Daten zu veröffentlichen, was für das Opfer DSGVO-Bußgelder und Imageschäden bedeuten könnte – dieser zusätzliche Druck soll die Lösegeldzahlung erzwingen. Insofern hat die DSGVO einen *unbeabsichtigten Effekt*: Die Angst vor Strafen bei Datenlecks erhöht die Verhandlungsmasse der Erpresser. Auch das Verbot, Lösegeld steuerlich abzusetzen (z.B. in Deutschland seit 2021), soll Kriminelle treffen, könnte aber Unternehmen in eine schwierige Lage bringen, da sie den Schaden voll tragen müssen. Auf der **Täterseite** ist eher eine Professionalisierung als Resignation zu beobachten – z.B. verkaufen Cybercrime-as-a-Service-Anbieter Exploits und Zugangsdaten und umgehen Gesetze durch Offshore-Standorte.

Vergleicht man die **Zahlen in EU und USA**, so zeigen sich auf beiden Seiten alarmierende Trends. In den USA registrierte das FBI 2024 knapp **859.000 Beschwerden über Internetkriminalität** (via IC3-Meldestelle) mit gemeldeten Schäden von **über 16 Mrd. US$** – ein Anstieg der Verluste um 33 % gegenüber 2023[54]. Die häufigsten Delikte in den USA waren Phishing, Erpressung und Datendiebstahl, während finanziell der größte Schaden durch Anlagebetrug (v.a. Krypto-Scams) entstand[55]. Die absoluten Fallzahlen sind in den USA höher als in Deutschland, was teils an der größeren Bevölkerung und wirtschaftlichen Bedeutung liegt. Pro Kopf oder pro Unternehmen gesehen jedoch unterscheiden sich die Bedrohungsraten nicht grundlegend – sowohl Europa als auch Nordamerika sehen einen **rasanten Anstieg** an Cybervorfällen. So wird der *globale* Schaden durch Cybercrime für 2020 auf knapp **1 Billion US-Dollar** geschätzt, über 50 % mehr als 2018[56]. Dieser Trend setzt sich unvermindert fort, unabhängig von regionalen Regulierungen.

Fazit: Strenge gesetzliche Vorgaben in Deutschland und der EU (DSGVO, NIS2, DORA usw.) haben dazu beigetragen, dass Unternehmen Cyberangriffe ernster nehmen, mehr investieren und Vorfälle transparenter gemacht werden. Sie zwingen Unternehmen zu besserer Hygiene – was langfristig die Gesamtresilienz erhöht. Dennoch bleibt die **Cyberkriminalität auf hohem Niveau**, da Angreifer sich schnell anpassen und global agieren. Kein Gesetz in Europa oder den USA kann allein die Flut an Angriffen stoppen. Daher fordert z.B. der deutsche Innenminister zusätzliche Maßnahmen, etwa verpflichtende Sicherheitsstandards für alle Unternehmen und engere Zusammenarbeit mit Behörden[48]. Gleichzeitig betonen Experten, dass **internationale Kooperation** nötig ist, um Täter grenzüberschreitend zu verfolgen. Unterm Strich ist die Lage sowohl in Deutschland/EU wie auch in den USA angespannt: Die Zahl der Angriffe wächst, die Methoden werden komplexer – und Unternehmen jeder Größe müssen damit rechnen, ins Visier zu geraten. Die *„hybride Kriegsführung“* im Cyberraum, wie Bitkom sie nennt, spielt sich täglich hundertfach ab[57]. Entsprechend lautet die Kernbotschaft an KMU wie Großunternehmen gleichermaßen: **Prävention, Detektion und Reaktion auf Cyberangriffe müssen Chefsache sein**, um der Bedrohungslage gerecht zu werden[58][49].

Quellen: Bundeskriminalamt (BKA) – Lagebilder Cybercrime; Bitkom-Studien *Wirtschaftsschutz 2019–2025*; Bundesamt für Sicherheit in der Informationstechnik (BSI) – Lageberichte; ENISA Threat Landscape 2023; FBI IC3 Report 2024; Pressemitteilungen und Fachartikel[2][3][6][16][7][18][40][42][50][54].

[1] Polizeiliche Kriminalstatistik: Immer weniger Online-Kriminalität, immer bessere Aufklärung

https://netzpolitik.org/2016/polizeiliche-kriminalstatistik-immer-weniger-online-kriminalitaet-immer-bessere-aufklaerung/

[2] [14] [29] Aktuelles | Kriminalistik - Nachrichten aus der Redaktion

https://kriminalistik.de/65370.htm

[3] [13] [22] [32] Cybercrime in Deutschland erreicht 2024 neuen Höchststand | DataAgenda

https://dataagenda.de/cybercrime-in-deutschland-erreicht-2024-neuen-hoechststand/

[4] [5] [8] [24] [28] [34] Cyberkriminalität in Deutschland – Ein aktueller Überblick | BASYS Brinova

https://basys-brinova.de/cyberkriminalitaet-in-deutschland-ein-aktueller-ueberblick/

[6] [9] [16] [17] [20] [25] [26] [27] [33] [41] [45] [46] [47] [53] [58] Angriffe auf die deutsche Wirtschaft nehmen zu | Presseinformation | Bitkom e. V.

https://www.bitkom.org/Presse/Presseinformation/Angriffe-auf-die-deutsche-Wirtschaft-nehmen-zu

[7] [10] [11] [12] [31] [38] [42] [57] Russland und China nehmen deutsche Wirtschaft ins Visier | Presseinformation | Bitkom e. V.

https://www.bitkom.org/Presse/Presseinformation/Russland-China-deutsche-Wirtschaft-Visier

[15] [40] [44] [48] [49] Bundeslagebild Cybercrime: größte Bedrohung Ransomware

https://www.orbit.de/news-bundeslagebild-cybercrime-deutschland/

[18] [23] [35] ENISA 2023 Key Findings and Recommendations

https://cpl.thalesgroup.com/blog/identity-data-protection/enisa-2023-key-findings-and-recommendations

[19] [36] [37] Bitkom-Studie: Milliarden Schäden - PSW GROUP Blog

https://www.psw-group.de/blog/bitkom-studie-2022/?srsltid=AfmBOorkGipJMyEcMcrlp_QGUyrAXBkhYWsQstK1mVw7zZYg2Fkru5mp

[21] [PDF] Die Lage der IT-Sicherheit in Deutschland 2023 - BSI - Bund.de

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=8

[30] Die unterschätzte Gefahr: Innentäter-Angriffe - Allgeier secion

https://www.secion.de/de/blog/blog-details/die-unterschaetzte-gefahr-innentaeter-und-wie-sich-ihr-unternehmen-vor-innentaeter-angriffen-schuetzen

[39] 9 von 10 Unternehmen Opfer von Cyberkriminalität - DGQ

https://www.dgq.de/aktuelles/9-von-10-unternehmen-opfer-von-cyberkriminalitaet/

[43] Die Lage der IT-Sicherheit in Deutschland - BSI

https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

[50] [PDF] Cybersecurity and The EU General Data Protection Regulation

https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/MMC-Marsh%20Beshar%20GDPR%20and%20WannaCry%20Insights%20062017.pdf

[51] ECCC -

https://ec.europa.eu/newsroom/ECCC/items/806536/

[52] GDPR: Studying the World's Strictest Security Law 6 Years On

https://cybermagazine.com/articles/gdpr-studying-the-worlds-strictest-security-law-6-years-on

[54] [55] FBI Releases Annual Internet Crime Report — FBI

https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

[56] Cyber risk and cybersecurity: a systematic review of data availability

https://pmc.ncbi.nlm.nih.gov/articles/PMC8853293/