MYRA

CYBERSECURITY REPORT H1 2025

Mit Resilienz und Souveränität der KI-Offensive begegnen

Vorwort

Das erste Halbjahr 2025 markiert einen neuen Wendepunkt in der Entwicklung der Cyberbedrohungslandschaft in Deutschland. Die zunehmende Intensität von DDoS-Angriffen verdeutlicht, wie sehr sich die Gefahrenlage im digitalen Raum weiter verschärft. Parallel hierzu führen anhaltende geopolitische Konflikte und die Rückkehr von Donald Trump ins Präsidentenamt der USA zu einer zusätzlichen Verunsicherung – insbesondere im Hinblick auf die digitale Souveränität Europas.

Diese Entwicklungen verdeutlichen nachdrücklich: Klassische Verteidigungsmethoden reichen nicht mehr aus. Die fortschreitende Nutzung Künstlicher Intelligenz durch Angreifer erhöht das Risiko für Unternehmen und Institutionen erheblich. Attacken werden infolgedessen gezielter, intensiver und technisch immer ausgefeilter. Besonders betroffen sind Banken, kritische Infrastrukturen und der öffentliche Sektor, wobei Angreifer vermehrt globale Cloud-Infrastrukturen missbrauchen, um Attacken zu verschleiern und zu verstärken.

Vor diesem Hintergrund zeigt sich die Dringlichkeit, technologische Abhängigkeiten zu reduzieren und die eigene Handlungsfähigkeit im digitalen Raum zu stärken. Digitale Souveränität und resiliente IT-Architekturen sind die Grundvoraussetzung, um Cyberrisiken zu minimieren und die Einhaltung strenger Regulatorik- und Compliance-Vorgaben zu gewährleisten. Mit Investitionen in europäische Lösungen und einem kontinuierlichen Aufbau eigener Kompetenzen ist es möglich, die deutsche Wirtschaft und Verwaltung auch künftig sicher und handlungsfähig zu halten – sofern die Bereitschaft der Entscheidungsträger gegeben ist.

Zusammenfassend gilt: Cyberresilienz und Digitale Souveränität sind keine Nischenthemen mehr, sondern ein gesellschaftlicher Imperativ, dessen Bedeutung durch die aktuelle Bedrohungslage weiter gestiegen ist. Der vorliegende Cybersecuirty Report von Myra beleuchtet die relevantesten Entwicklungen und zeigt auf, wie Unternehmen und öffentliche Einrichtungen mit gezielten Maßnahmen ihre Resilienz stärken können, um aktuellen und zukünftigen Gefahren wirksam entgegenzutreten.

Christof Klaus
Director Global Network Defense
bei Myra Security

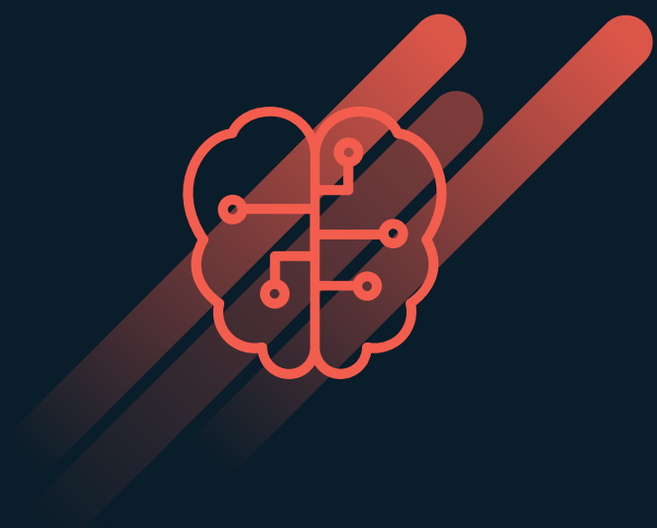
Inhalt

Executive Summary

Auch im Jahr 2025 bleibt die Cybersicherheitslage in Deutschland angespannt und hochdynamisch. Zwar ist die Zahl der durch Myra dokumentierten und abgewehrten Angriffe im ersten Halbjahr rückläufig (**-18,5 Prozent** im Vergleich zum Vorjahr), doch nehmen Intensität, Zielgerichtetheit und technische Raffinesse der Attacken weiter zu. Besonders betroffen sind hochregulierte Branchen wie die Finanzindustrie, kritische Infrastrukturen und der öffentliche Sektor: **40 Prozent aller Attacken zielen auf Banken** und andere Finanzdienstleister ab. Die Angreifer missbrauchen zudem gezielt globale Cloud-Infrastrukturen, um ihre Attacken zu verschleiern und deren Schlagkraft zu erhöhen. Die **stärksten Angriffe** verzeichneten die Abwehrsysteme für die **Technologiebranche,** während sich die längsten Attacken über einen **Zeitraum von fast zwei Tagen erstreckten.**

Eskalation von Cyberrisiken durch Offensive AI

Die breite Verfügbarkeit und sukzessive Integration von Künstlicher Intelligenz (KI) in Angriffswerkzeugen verschärft die Cyberbedrohungslage erheblich: Angreifer können schneller, präziser und kostengünstiger Schwachstellen identifizieren und automatisierte, adaptive Angriffskampagnen orchestrieren, die klassische Schutzmaßnahmen zunehmend umgehen. Besonders im Bereich von DDoS-Attacken ermöglichen KI-optimierte Techniken eine **dynamische Anpassung der Angriffsvektoren** und ein effektives Management von Botnetzen, wodurch die Effizienz und Schlagkraft solcher Angriffe deutlich steigt. Auch **KI-basierte Bots und Crawler** verursachen durch massenhafte automatisierte Anfragen eine erhebliche Serverlast auf Webseiten und können dadurch Ausfälle provozieren.
Die überwiegende Mehrheit der Unternehmen erkennt die wachsende Gefahr: 82 Prozent sehen eine gezieltere Ausnutzung von Schwachstellen durch KI, während 89 Prozent davon ausgehen, dass der Einsatz von KI Cyberkriminellen effizientere und präzisere Angriffe ermöglicht.



Hybride Bedrohungslage und geopolitische Dimension

Indessen verschwimmen die Grenzen zwischen finanziell und politisch motivierten Angriffen zusehends. Hacktivistische Gruppen und staatlich unterstützte Akteure nutzen **Cyberangriffe als Mittel hybrider Kriegsführung**, um Verunsicherung zu stiften und gesellschaftliche Spaltung zu fördern. **Deutschland ist** laut Informationen der Bundeswehr und des Bundesamtes für Sicherheit in der Informationstechnik (BSI) täglich **Ziel solcher hybriden Angriffe,** die neben IT-Systemen auch die Stabilität der öffentlichen Ordnung insgesamt ins Visier nehmen.[1] Dieser Bedrohungslage kann nur eine hochresiliente IT-Infrastruktur standhalten – die in Deutschland momentan nur bedingt zur Verfügung steht. So mahnte jüngst der Bundesrechnungshof vor gravierenden Sicherheitslücken in den Rechenzentren des Bundes: *„Die IT des Bundes ist nicht auf die aktuellen Bedrohungen vorbereitet."* [2] In deutschen Behörden sowie in der Wirtschaft mangelt es oftmals an erforderlichen Redundanzen, Krisenresilienz und Souveränität.

Souveränität ist das Fundament für Cyberresilienz

Digitale Souveränität beschreibt die Fähigkeit von Unternehmen, Organisationen und Staaten, die Kontrolle über ihre Daten, digitalen Infrastrukturen und Schlüsseltechnologien zu behalten und Abhängigkeiten von außereuropäischen Anbietern zu minimieren. Diese digitale Unabhängigkeit ist insbesondere vor dem Hintergrund unzuverlässiger Partnerschaften außerhalb Europas essenziell. Nur durch souveräne IT-Architekturen, den gezielten Einsatz europäischer Lösungen und die Einhaltung strenger Datenschutz- und Compliance-Standards lässt sich die **Widerstandsfähigkeit gegenüber Cyberbedrohungen** nachhaltig stärken. Zwar haben sowohl Politik als auch Wirtschaft die Bedeutung digitaler Souveränität erkannt, doch äußert sich dies noch unzureichend in Investitionen in europäische Cloud-, KI- und Sicherheitslösungen. Oftmals mangelt es an der Kenntnis leistungsfähiger Alternativen. Regulatorische Initiativen wie die **NIS-2**-Richtlinie, die **DORA**-Verordnung oder der **Cyber Resilience Act** weisen derweil die Richtung zu holistischer Cyberresilienz entlang der gesamten digitalen Wertschöpfungskette.

Resilient in die Zukunft

Die **Stärkung der digitalen Souveränität** ist daher keine abstrakte Zukunftsvision, sondern eine akute Notwendigkeit für die Sicherheit und Wettbewerbsfähigkeit Deutschlands. Sie ist Voraussetzung für effektiven Datenschutz, rechtssichere Compliance und die Resilienz kritischer Infrastrukturen. Unternehmen und Behörden müssen ihre Abhängigkeit von nicht-europäischen Technologien systematisch reduzieren, eigene Kompetenzen und Lösungen ausbauen und strategische Partnerschaften innerhalb Europas stärken. Nur so lässt sich die digitale Zukunft nachhaltig, sicher und selbstbestimmt gestalten.

Im Hauptteil des vorliegenden Cybersecurity Reports erwarten Sie detaillierte Analysen, Interviews und praxisnahe Empfehlungen zu den aufgezeigten Themen. Die aggregierten Zahlen aus dem Security Operations Center (SOC) von Myra liefern einen umfassenden Überblick über Trends und Angriffsmethoden aus zentraleuropäischer beziehungsweise DACH-Perspektive – mit besonderem Fokus auf hochregulierte Sektoren und den KRITIS-Bereich.

Schäden und Risiko auf Rekordniveau

Wie hoch der Bedarf an besseren Schutzsystemen ausfällt, veranschaulichen die einschlägigen Schadenstatistiken, die neue Rekordwerte erreichen. So beläuft sich der durch Cyberkriminalität hervorgerufene **Schaden für die deutsche Wirtschaft auf 178,6 Milliarden Euro** – ein Anstieg um mehr als 20 Prozent gegenüber dem Vorjahr. 8 von 10 Unternehmen sind von Datendiebstahl, Spionage oder Sabotage betroffen.[3] 47 Prozent der deutschen Unternehmen sehen **Cybervorfälle als größtes Geschäftsrisiko**, noch vor Betriebsunterbrechungen und Naturkatastrophen.[4] Rund 3 von 4 Führungskräften sind sich sicher, dass das Gefährdungsrisiko für das eigene Unternehmen in den vergangenen zwei Jahren gestiegen ist, und mehr als die Hälfte geht von einer massiven Verschärfung der Lage in der Zukunft aus.[5]

Mitigationstrends und Angriffsmuster

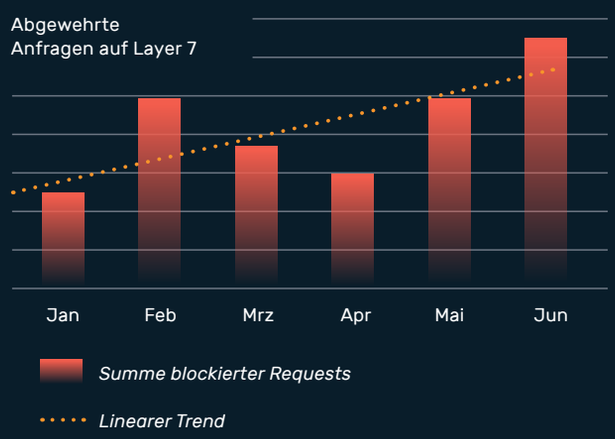
Im ersten Halbjahr 2025 zeigte sich die Bedrohungslage im Bereich schädlicher Traffic-Ströme weiterhin äußerst dynamisch. Zwar ist ein leichter Rückgang der Gesamtzahl an Angriffen zu beobachten, doch einzelne massive Angriffswellen und immer ausgefeiltere Methoden verdeutlichen, dass die Qualität und Zielgerichtetheit der Attacken zunimmt. Besonders Unternehmen aus hochregulierten Branchen stehen im Fokus der Angreifer und sehen sich zunehmend komplexen und langanhaltenden Angriffen ausgesetzt. Cyberkriminelle missbrauchen globale Cloud-Infrastrukturen und nutzen moderne Verschleierungstechniken, was eine zuverlässige Zuordnung und die Abwehr der Attacken erheblich erschwert.

Konkret lässt sich festhalten, dass sich die Anzahl schädlicher Anfragen auf Webanwendungen, Onlineportale und APIs im Betrachtungszeitraum auf einem konstant hohen Niveau einpendelt. Obwohl die Gesamtzahl der Angriffe im Vergleich zum Vorjahreszeitraum um 18,5 Prozent zurückging, signalisieren aktuelle Entwicklungen und der Langzeittrend eine qualitative Verschärfung der Bedrohungslage.

Massive Angriffswellen in einzelnen Monaten untermauern diesen Trend:

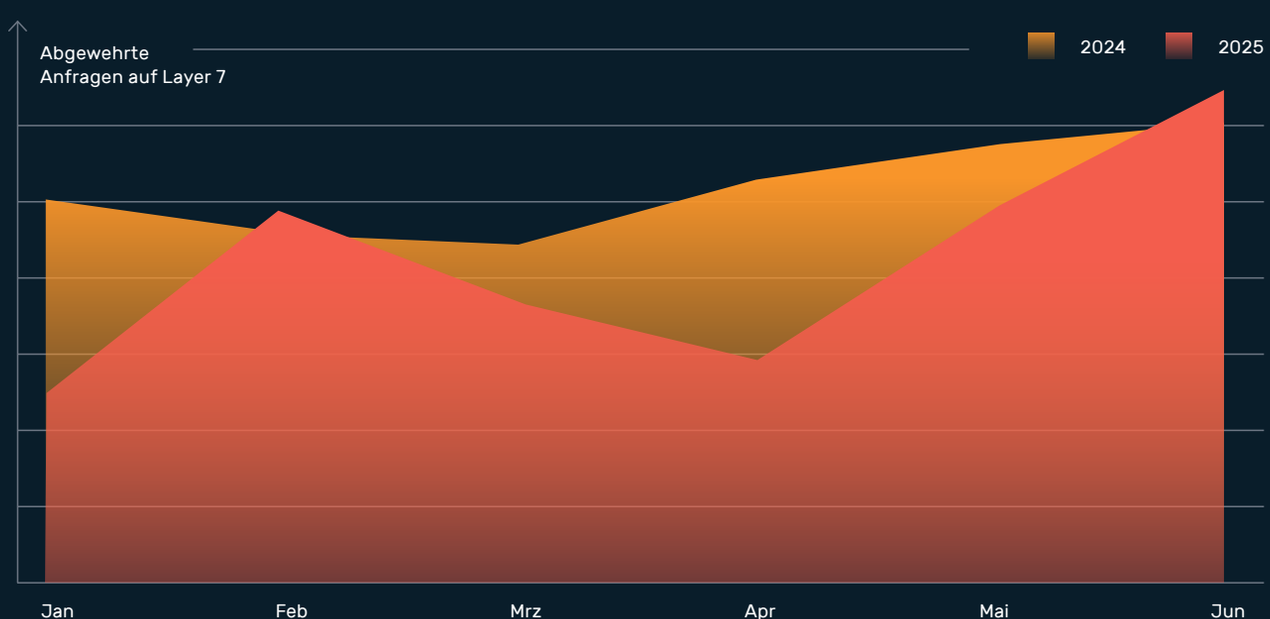
- **Februar 2025:** Bereits im Frühjahr wurde ein Zuwachs schädlicher Requests von 6 Prozent registriert, der maßgeblich auf eine gezielte Angriffskampagne gegen bayerische Behörden zurückzuführen ist.
- **Juni 2025:** Ein signifikanter Anstieg um 6,6 Prozent gegenüber dem Vorjahresmonat deutet auch hier auf eine erhöhte Angriffsaktivität zum Ende des Halbjahres hin.

Angriffsaktivität H1 2025



Diese Daten zeigen, dass trotz eines statistischen Gesamtrückgangs die Intensität und Zielgerichtetheit von Angriffen zunehmen.

Angriffsaktivität im Jahresvergleich



Im Vergleich zum Vorjahreszeitraum gab es im ersten Halbjahr 2025 insgesamt 18,5 Prozent weniger schädliche Requests zu verzeichnen. Dennoch traten im Februar (+6 Prozent) und Juni (+6,6 Prozent) deutliche Spitzen auf, die sogar das bereits hohe Mitigationsniveau des Vorjahres übertrafen.

Herkunftsanalyse und Limitationen in der Attribution

Die Analyse der von Myra verarbeiteten Angriffsdaten ermöglicht Erkenntnisse bezüglich der globalen Traffic-Quellen, wobei eine differenzierte Interpretation erforderlich ist.

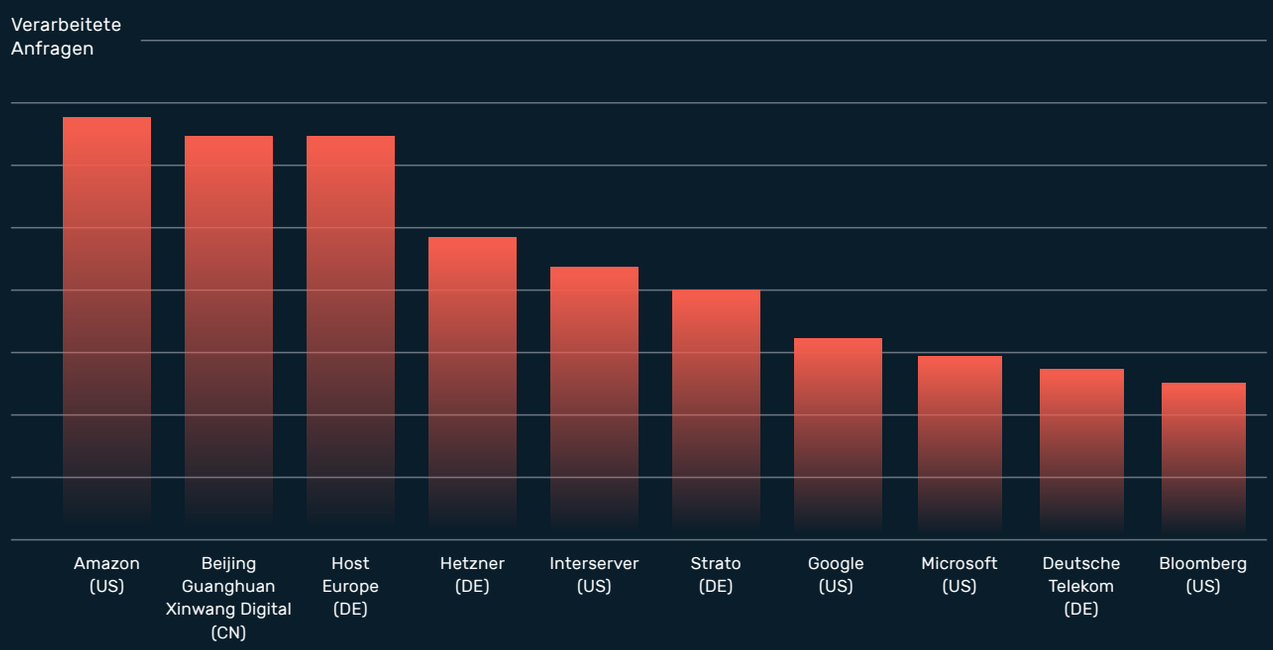
Geografische Verteilung der Anfragen:
Der Großteil der schädlichen Anfragen stammte aus den USA. Bei Betrachtung der zehn Request-stärksten Ursprungsländer entfallen 42 Prozent auf die Vereinigten Staaten. Mit deutlichem Abstand folgen Deutschland mit 19 Prozent und China mit 12 Prozent. Russland rangiert mit lediglich 3 Prozent auf dem siebten Platz.

Top 10 Origin Countries

Die Analyse zeigt, dass Cyberkriminelle ihre Angriffskampagnen meist über Länder mit leistungsfähiger technischer Infrastruktur und schneller Internetanbindung leiten. Das deutet auf eine gezielte Nutzung globaler Ressourcen und mögliche Verschleierungstaktiken hin.

Verteilung nach Autonomen Systemen (AS): Eine Aufschlüsselung der schädlichen Anfragen nach Netzwerkinfrastruktur zeigt eine hohe Konzentration auf wenige große Cloud-Anbieter und Hoster. Die meisten schädlichen Anfragen stammten aus den Netzen des US-Hyperscalers Amazon, dicht gefolgt von Beijing Guanghuan Xinwang Digital aus China und Host Europe aus Deutschland. Dies unterstreicht die Bedeutung großer, global agierender Infrastruktur-Anbieter als Plattformen für Angreifer, die gezielt Ressourcen der Provider für ihre Zwecke missbrauchen.

Top 10 Origin AS



Die Analyse der Ursprungs-AS im Top-10-Ranking zeigt, dass ein großer Teil der Angriffe aus den Netzen von US-Hyperscalern stammt. Daneben nutzen Cyberakteure auch regionale Netze mit hoher Glaubwürdigkeit, wie etwa Hetzner, Host Europe oder die Deutsche Telekom. Dadurch verlieren klassische Herkunftsfilter zunehmend an Wirksamkeit.

Hinweise zur Attribution: Die Informationen über Herkunftsländer oder verwendete AS erlauben keine belastbaren Rückschlüsse auf den tatsächlichen Standort oder die Identität der Angreifer. Cyberkriminelle setzen gezielt auf Techniken wie IP-Spoofing, Reflection-Angriffe und den Einsatz global verteilter Botnetze, um ihre wahre Herkunft zu verschleiern. Darüber hinaus werden häufig kompromittierte Server oder Cloud-Ressourcen als Sprungbrett genutzt, sodass die Angriffe scheinbar aus ganz anderen Regionen stammen (mehr hierzu erfahren Sie in der Infobox auf Seite 8).

Die Auswertung der Top-Origin-AS oder -Länder dient daher in erster Linie der Einordnung und Analyse von Traffic-Strömen. Sie kann helfen, Muster zu erkennen und Schutzmaßnahmen gezielt auszurichten.

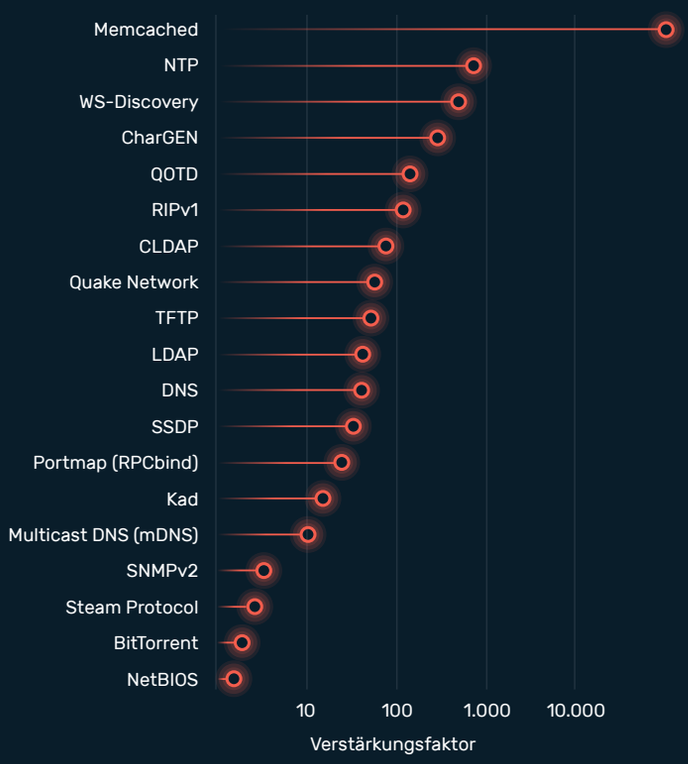
Für die Identifikation konkreter Angreifer oder deren Standorte ist sie jedoch ungeeignet. Die Attribution im Cyberraum bleibt eine der größten Herausforderungen der Branche und erfordert stets eine kritische und mehrschichtige Analyse.

Diese Branchen stehen im Fokus der Angreifer

Im ersten Halbjahr 2025 registrierten die Abwehrsysteme von Myra eine signifikante Fokussierung von Angriffen auf Unternehmen aus der Finanzbranche, die mit einem Anteil von 40 Prozent am häufigsten ins Visier der Angreifer gerieten. Dicht dahinter folgten Technologiefirmen, auf die 38 Prozent aller mitigierten Attacken entfielen. Mit deutlichem Abstand folgten Versicherungsunternehmen (7 Prozent) sowie Organisationen aus der Öffentlichen Verwaltung (4 Prozent).

Auffällig ist, dass die massivsten Angriffe im Technologiebereich auftraten – gefolgt von der Telekommunikation und der Öffentlichen Verwaltung. Besonders bemerkenswert war zudem die Dauer einzelner Angriffe: Der längste dokumentierte Angriff erstreckte sich über einen Zeitraum von nahezu zwei Tagen (46,08 Stunden) und verdeutlicht die ansteigende Ausdauer und Hartnäckigkeit moderner Angreifer.

UDP-basierte Verstärkungsangriffe



Viele DDoS-Attacken erfolgen über hoch verstärkende Reflektoren wie DNS-Dienste, welche die kurzen Anfragen der Angreifer mit großen Datenpaketen beantworten. Auf diese Weise steigern solche Reflection-Attacken die Schlagkraft der Angriffe um ein Vielfaches.[6]

So verschleiern Angreifer Ihre Attacken

IP-Spoofing: Angreifer manipulieren die Quell-IP-Adresse in Paket-Headern, um ihre Identität zu verschleiern. Dabei werden gefälschte IP-Pakete erzeugt, deren Absenderadresse bewusst verfälscht ist, um eine Rückverfolgung zu verhindern und Sicherheitssysteme zu umgehen. Diese Technik wird besonders bei DDoS-Angriffen eingesetzt, wobei zufällig generierte Quell-IPs die Filterung erschweren.

Reflection-Angriffe: Hier missbrauchen Angreifer öffentliche Dienste wie DNS, NTP oder SNMP. Sie senden Anfragen mit gefälschter Absenderadresse (Opfer-IP) an diese Dienste. Die daraufhin generierten Antworten werden an das Opfer geleitet – oft mit erheblicher Verstärkung (Amplification), da Antwortpakete größer als Anfragen sein können. Diese Methode erfordert keine Kontrolle über die genutzten Server.

Global verteilte Botnetze: Angreifer steuern kompromittierte Geräte („Bots“) weltweit, die über Command-and-Control-Server koordiniert werden. Diese Botnetze generieren Angriffstraffic aus tausenden Quellen, wodurch geografische oder AS-basierte Zuordnungen wertlos werden.

Wer sind die Angreifer? Ein Überblick über moderne Cyberakteure

Hinter den Angriffen auf Webseiten, APIs und Infrastrukturen stecken verschiedene Gruppen mit unterschiedlichen Motiven und Vorgehensweisen. Wobei festzuhalten bleibt, dass 9 von 10 Angreifern monetäre Ziele verfolgen und bei rund einem Fünftel der Angriffe Spionage eine zentrale Rolle spielt.[7]

Staatlich unterstützte Akteure: Staatlich unterstützte Cyberakteure setzen Angriffe vor allem zur Spionage ein. Sie planen langfristig und nutzen ein breites Spektrum an Angriffswerkzeugen – von DDoS-Attacken bis zu fortschrittlicher Schadsoftware. Ihre Ziele sind nicht nur andere Staaten, sondern auch Unternehmen und Organisationen, um an sensible Informationen oder finanzielle Ressourcen zu gelangen.

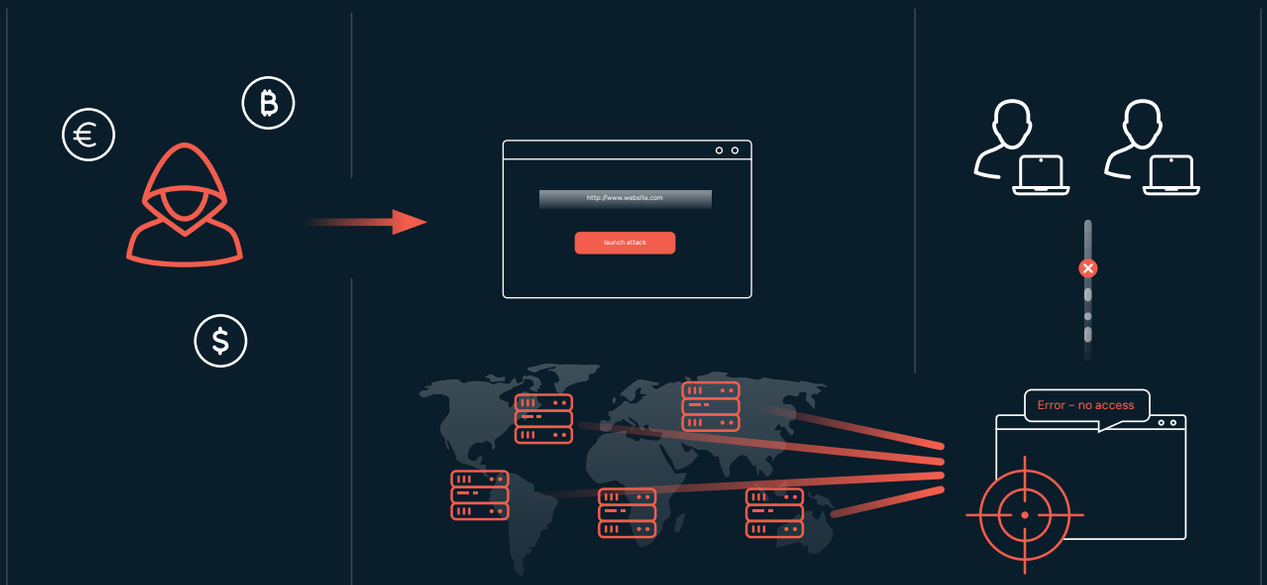
Script Kiddies: Ein Script Kiddie ist ein unerfahrener Cyberakteur, der vorgefertigte Hacking-Tools, Skripte und Services nutzt, ohne deren Funktionsweise wirklich zu verstehen. Typisch ist der Einsatz öffentlich verfügbarer Software, um Schwachstellen auszunutzen oder Systeme zu stören. Trotz ihres geringen Fachwissens können Script Kiddies durch automatisierte Angriffe erheblichen Schaden anrichten.

Cyberkriminelle: Cyberkriminelle sind für den Großteil aller Angriffe verantwortlich. Sie agieren meist opportunistisch und setzen auf breit angelegte Attacken, um gezielt Daten oder kritische Infrastrukturen zu kompromittieren. Ihr Ziel ist es, maximalen Schaden anzurichten – sei es durch direkten Diebstahl digitaler Werte, Erpressung der Opfer oder den gewinnbringenden Verkauf gestohlener Informationen.

Insider Threats: Auch interne Akteure stellen ein erhebliches Risiko dar – unabhängig davon, ob ihre Handlungen vorsätzlich oder unbeabsichtigt erfolgen. In der Praxis sind viele Sicherheitsvorfälle auf menschliche Fehler, Fehlkonfigurationen oder unzureichende Sicherheitsrichtlinien zurückzuführen. Unternehmen sollten daher nicht nur externe Bedrohungen, sondern auch potenzielle Risiken durch Insider in ihre Sicherheitsstrategie einbeziehen.

Hacktivisten: Hacktivistische Gruppen setzen Cyberangriffe ein, um politische oder gesellschaftliche Ziele zu verfolgen. Ihr Hauptanliegen ist es, Aufmerksamkeit zu erzeugen, Störungen im öffentlichen Leben zu verursachen und Unsicherheit zu schüren. Die technischen Fähigkeiten und Angriffsmethoden dieser Gruppen variieren stark. Zudem werden Hacktivisten gelegentlich von staatlichen Akteuren instrumentalisiert, etwa für gezielte Desinformationskampagnen oder zur Beeinflussung öffentlicher Meinungen.

Ablauf einer DDoS-Attacke mittels DDoS as a Service



1.
Kriminelle mieten im Internet einen DDoS-Angriffsdienst und geben die Ziel-IP-Adresse an. Die Bezahlung erfolgt meist in Kryptowährungen.

2.
Der Booter-Dienst startet die DDoS-Attacke über seine Angriffsinfrastruktur.

3.
Der DDoS-Angriff überlastet die Server des Ziels, wodurch sie für reguläre Nutzende nicht mehr erreichbar sind.

Günstige Attacken mit enormer Schlagkraft: DDoS as a Service

Zur Verschärfung der Bedrohungslage tragen im besonderen Maße DDoS-as-a-Service-Angebote bei, die von Cyberkriminellen im Darknet oder auf Plattformen wie Telegram zur Verfügung gestellt werden. Dort vermieten Akteure die Schlagkraft ihrer Botnetze – und das bereits für wenige US-Dollar pro Tag. Bereits kostengünstige Angriffe reichen oftmals aus, um ungeschützte Webprozesse für die gebuchte Dauer lahmzulegen.

Die Effektivität solcher DDoS-as-a-Service-Angebote wurde zuletzt bei der Attacke auf den Blog des Cybersicherheitsexperten Brian Krebs (KrebsOnSecurity) deutlich: Am 12. Mai 2025 erreichte die Attacke mit dem Aisuru-Botnetz eine Spitzenlast von 6,3 TBit/s. In öffentlichen Telegram-Chatkanälen haben die Hintermänner von Aisuru das Botnet in Abonnement-Stufen von 150 US-Dollar pro Tag bis 600 US-Dollar pro Woche zur Miete angeboten, wobei Angriffe mit bis zu 2 TBit/s beworben wurden.[8]

Insgesamt präsentiert sich die Preisstruktur für diese Dienste erschreckend niedrig – die Preise rangieren zwischen einem niedrigen zweistelligen Betrag und mehreren hundert US-Dollar – abhängig von Dauer und Stärke der durchgeführten Angriffe. Die Bezahlung erfolgt in aller Regel anonym in Form von Kryptowährungen wie Bitcoin.

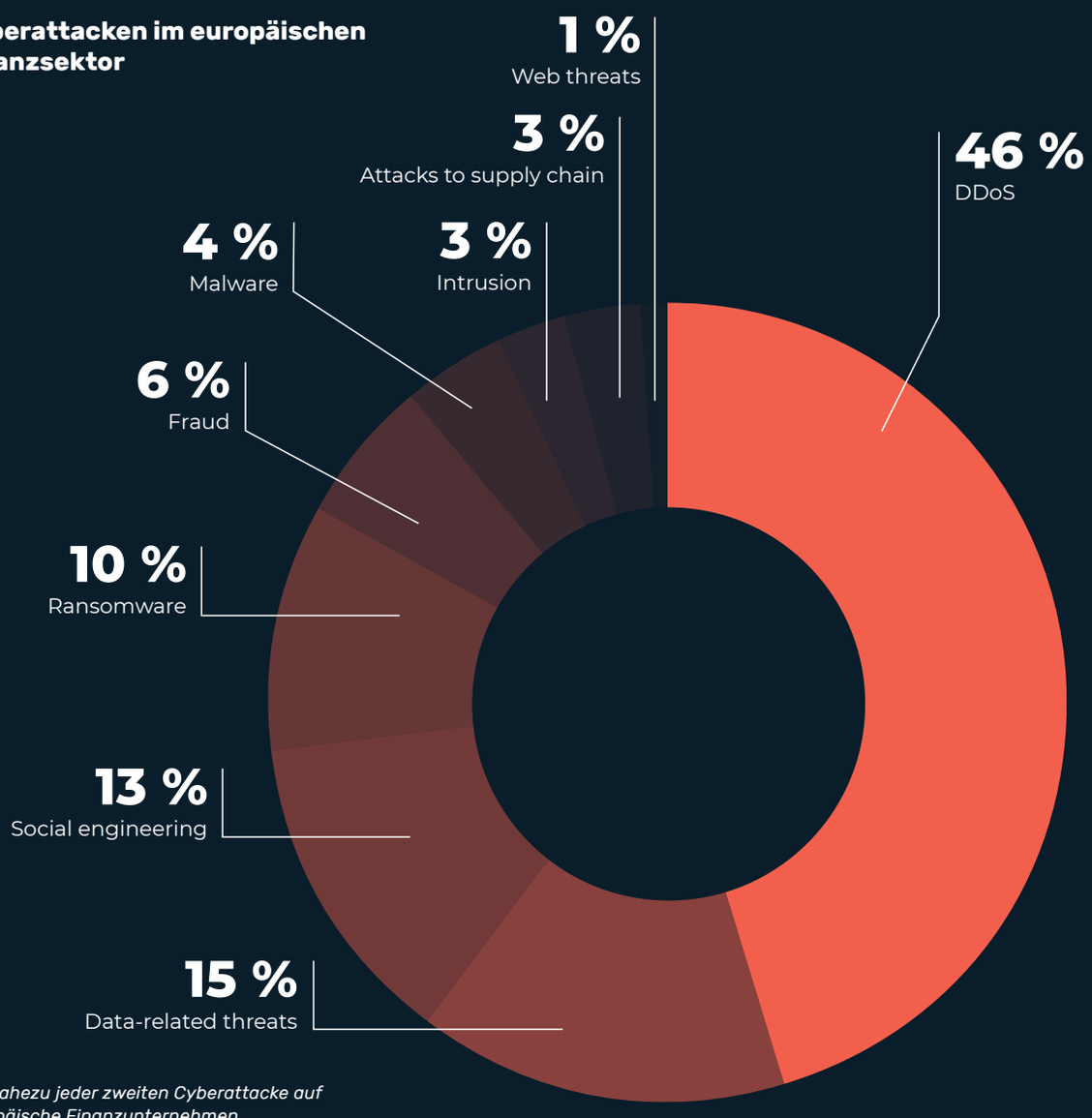
Finanzsektor im Fokus von Cyberkriminalität

Die Finanzbranche zählt seit Jahren zu den bevorzugten Zielen von Cyberkriminellen – ein Umstand, der sich durch die hohe Konzentration sensibler Daten und erheblicher Vermögenswerte in diesem Sektor erklärt. Wo große Werte verwaltet und Transaktionen in Echtzeit abgewickelt werden, ist das Interesse potenzieller Angreifer besonders ausgeprägt. Cybervorfälle stellen daher das zentrale Risiko für Finanzinstitute dar.[9]

DDoS-Angriffe sind in den meisten Fällen das Mittel der Wahl, wenn Cyberkriminelle Banken und Finanzdienstleister angehen: In Europa entfallen 46 Prozent aller Attacken auf den Finanzsektor auf diesen Angriffsvektor.[10] Solche Angriffe zielen darauf ab, die Verfügbarkeit von Online-Banking, Zahlungsdienstleistungen und Börsenplattformen zu stören, was nicht nur finanzielle Schäden verursacht, sondern auch das Vertrauen der Kunden nachhaltig schädigt. Das Myra SOC registrierte im vergangenen Halbjahr die höchste Anzahl an Attacken im Finanzbereich, was die besondere Gefährdungslage unterstreicht.

Vor diesem Hintergrund hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) die Stärkung der operativen Resilienz zu einem ihrer vorrangigen strategischen Aufgaben für die kommenden Jahre erklärt. Ziel sei es, die Widerstandsfähigkeit der Branche gegenüber Cyberbedrohungen zu erhöhen, Ausfallzeiten zu minimieren und das Vertrauen in die Stabilität des Finanzsystems zu sichern.[11]

Cyberattacken im europäischen Finanzsektor

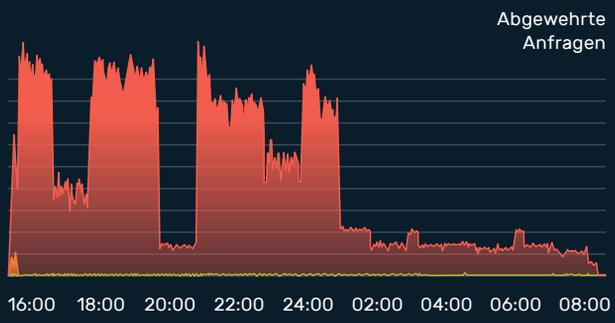


Bei nahezu jeder zweiten Cyberattacke auf europäische Finanzunternehmen handelt es sich um einen DDoS-Angriff. [12]

Abgewehrte DDoS-Angriffskampagne im ersten Halbjahr 2025

Nachdem Ende April zahlreiche Verwaltungsportale deutscher Städte von einer koordinierten DDoS-Angriffskampagne betroffen waren, schwenkten Cyberkriminelle im Mai ihre Attacken auf deutsche Banken und Finanzdienstleister um – auch mehrere Kunden von Myra Security waren von der Angriffswelle betroffen.

Über einen Zeitraum von mehr als 16 Stunden attackierten Cyberakteure die Systeme der Finanzinstitute in mehreren Wellen. Die Angreifer setzten dabei auf verschiedene Methoden und Vektoren – unter anderem Slowloris – und griffen gezielt auf unterschiedlichen Netzwerklayern an. Die Schutzsysteme von Myra blockierten in diesem Zeitraum mehr als 240 Millionen Requests und verhinderten so eine Überlastung der kritischen Infrastrukturen.



Die koordinierte Cyberattacke auf deutsche Finanzinstitute erfolgte in mehreren Wellen über einen Zeitraum von mehr als 16 Stunden.

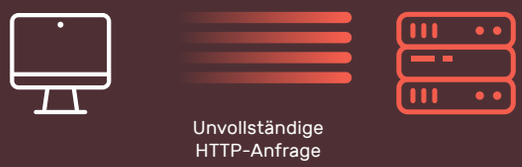
Dank der zertifizierten Sicherheitstechnologie und der Expertise des Myra SOC konnten alle betroffenen Finanzdienste durchgehend verfügbar und leistungsfähig gehalten werden. Die Angriffe wurden auf sämtlichen relevanten Netzwerkschichten erkannt und abgewehrt. Automatisierte Prozesse ermöglichten eine unmittelbare Reaktion auf die wechselnden Angriffsmuster.

> *Unsere Abwehrsysteme sind vollautomatisch gegen die Angreifer vorgegangen und haben ihre Attacken auf allen relevanten Netzwerkschichten abgeblockt.*
>
> *Auffällig war insbesondere die Vielschichtigkeit der Angriffe: Unter anderem nutzten die Akteure Slowloris als Angriffsvektor. Hierbei werden zahlreiche Verbindungen zu einem Webserver geöffnet und diese so lange wie möglich offen gehalten. Dadurch werden die Serverressourcen schleichend erschöpft, ohne dass der Angriff durch ungewöhnlich hohe Bandbreite auffällt – legitimer Traffic wird so effektiv blockiert, während der Angriff für klassische Schutzmechanismen schwer zu erkennen bleibt.*
>
> *Unsere mehrschichtigen Verteidigungsmechanismen identifizieren auch diese Low-and-Slow-Angriffe frühzeitig und leiten eine Mitigation ein, bevor die Verfügbarkeit der anvisierten Dienste gefährdet ist.*

Christof Klaus
Director Global Network Defense
bei Myra Security

Gewöhnliche HTTP-Anfrage – Response Connection

DDoS-Angriff durch Slowloris



Slowloris: Unscheinbare Attacke mit großer Wirkung

Bei der Slowloris-Attacke, einer speziellen Form des Denial-of-Service-Angriffs, öffnet ein Angreifer zahlreiche Verbindungen zu einem Webserver und hält diese mit unvollständigen HTTP-Anfragen so lange wie möglich offen. Dadurch werden die verfügbaren Verbindungen des Servers blockiert, sodass legitime Nutzende keine Verbindung mehr aufbauen können, obwohl der Server technisch weiterhin freie Kapazitäten besitzt. Im Gegensatz zu klassischen DDoS-Angriffen benötigt Slowloris nur wenig Bandbreite und bleibt oft unbemerkt, da der Angriff wie normaler, jedoch äußerst langsamer Traffic aussieht.

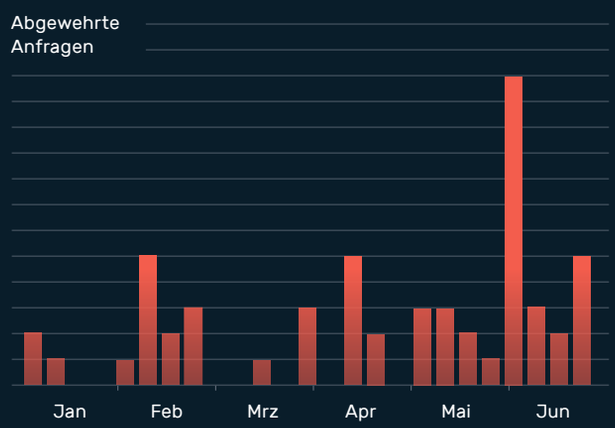
Behörden, Städte und Kommunen unter Dauerbeschuss

Im vergangenen Jahr wurden laut Angaben der Bundesregierung insgesamt 80 IT-Sicherheitsvorfälle bei Bundesbehörden registriert – 17 davon konnten nicht erfolgreich abgewehrt werden.[13]
Neben Bundeseinrichtungen standen aber auch Behörden von Ländern und Kommunen im Visier schwerwiegender Cyberangriffe. Die Abwehrsysteme von Myra verzeichnen mit die meisten Angriffe auf Kunden aus dem öffentlichen Sektor. Weltweit rangieren Cybervorfälle im Bereich von Public Services & Government auf Rang zwei der größten Risiken.[14]

Besonders auffällig war eine Angriffswelle mit geopolitischem Hintergrund, die im April 2025 zahlreiche deutsche Behörden und Städte traf. So wurde etwa das Hauptstadtportal berlin.de durch massive DDoS-Attacken lahmgelegt.

Bereits im Februar waren auch bayerische Behörden, der Bundesfinanzhof und die Polizei von Cyberattacken betroffen und mussten zeitweise Einschränkungen im Online-Betrieb hinnehmen.

Cyberbedrohungslage Public Sector



Diese Angriffe führten dazu, dass digitale Verwaltungsdienste für Bürgerinnen und Bürger teilweise nicht erreichbar waren und interne Abläufe erheblich gestört wurden. Die Angreifer nutzten dabei gezielt politische Spannungen, um Unsicherheit zu schüren und das Vertrauen in staatliche Strukturen zu schwächen.

Die Angriffe verdeutlichen: Der öffentliche Sektor bleibt ein attraktives Ziel für Cyberkriminelle und politisch motivierte Angreifer. Die Angriffe sind real, die Folgen spürbar – und der Handlungsbedarf bleibt hoch.

Deutschlandweit sorgen Cyberattacken für Ausfälle und Performance-Probleme bei Digitalprozessen von Bund, Ländern und Kommunen.[15]

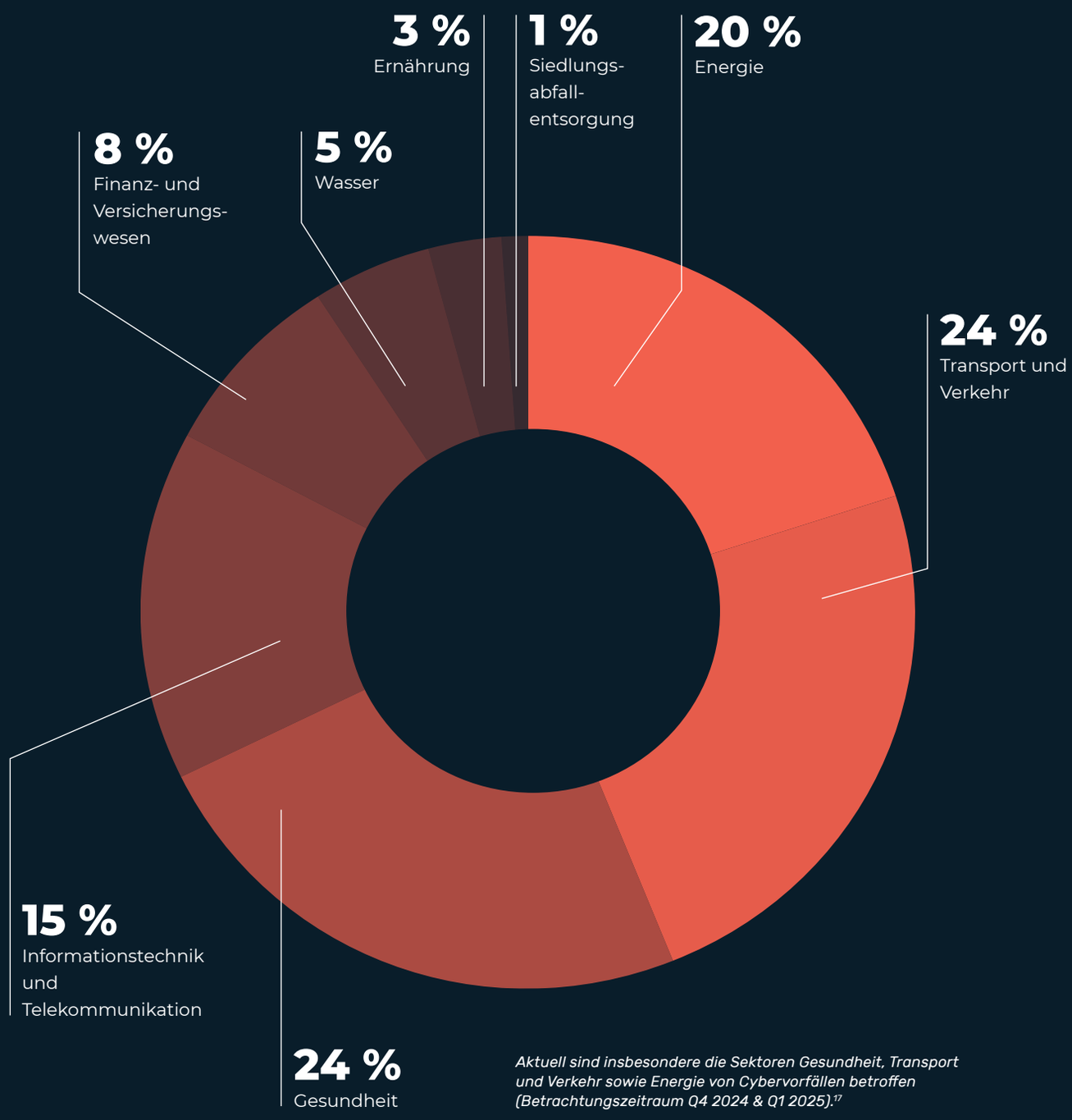
Cybervorfälle im Öffentlichen Sektor

KRITIS: Wachsende Bedrohung trifft auf schleppende NIS-2-Umsetzung

Während sich die Wartezeit auf die NIS-2-Umsetzung in Deutschland weiter in die Länge zieht, verschärft sich die Bedrohungslage für Organisationen der Kritischen Infrastrukturen (KRITIS) spürbar. Gemäß offizieller Statistiken wurden dem BSI im vergangenen Jahr insgesamt 769 Vorfälle gemeldet – was einer Steigerung von 43 Prozent im Vergleich zum Vorjahr entspricht.[16] Diese Zahlen machen deutlich: Cyberangriffe auf die kritische Infrastruktur Deutschlands sind keine abstrakte Gefahr, sondern eine akute Bedrohung für die Funktionsfähigkeit und Sicherheit unserer Gesellschaft.

Nur **4 EU-Staaten** haben **NIS-2** fristgerecht umgesetzt: **Belgien, Italien, Kroatien und Litauen**

KRITIS: Gemeldete Störungen



Aktuell sind insbesondere die Sektoren Gesundheit, Transport und Verkehr sowie Energie von Cybervorfällen betroffen (Betrachtungszeitraum Q4 2024 & Q1 2025).[17]

Besonders die Sektoren Energie, Transport und Verkehr, Gesundheit sowie IT und Telekommunikation stehen kontinuierlich im Fadenkreuz von Angreifern – mit teils gravierenden Folgen.

Unterdessen sieht das BSI speziell im Bereich der Energieversorgung eine „wachsende Angriffsfläche für Cyberkriminelle", wie BSI-Präsidentin Claudia Plattner im Mai mitteilte. Durch die dezentrale Struktur mit zahlreichen kleinen Kraftwerken, Windparks und Solaranlagen entstehen immer mehr Zugangspunkte für gezielte Infiltration, Sabotage und Manipulation. [18]

Auch vermeintlich weniger betroffene Sektoren wie Wasser, Ernährung oder Abfallentsorgung stellen im Fall einer erheblichen Störung ein großes Risiko für die Gesellschaft dar. Es ist festzuhalten, dass kein Bereich im KRITIS-Sektor vor Angriffen gefeit ist, wie auch exemplarisch die Attacke auf einen Staudamm im Südwesten Norwegens veranschaulicht (siehe folgende Seite).

Warnschuss aus Norwegen: Wie verwundbar sind Europas Infrastrukturen?

Ein aktueller Vorfall aus Norwegen verdeutlicht die realen Risiken für kritische Infrastrukturen: Im April 2025 gelang es unbekannten Angreifern, die Wasserdurchlass-Ventile eines Staudamms am Risevatnet-Stausee im Südwesten des Landes über mehrere Stunden hinweg unbemerkt zu öffnen. Die Cyberkriminellen hatten sich über ein schwaches Passwort Zugang zu den Kontrollsystemen verschafft, die über das Internet erreichbar waren. Nach erfolgreicher Authentifizierung konnten sie die Sicherheitskontrollen umgehen und direkten Zugriff auf die Operational-Technology-(OT)-Umgebung erlangen. Die Folge: Alle Ventile wurden vollständig geöffnet und der Wasserabfluss erhöhte sich um 497 Liter pro Sekunde über den vorgeschriebenen Mindestdurchfluss. Glücklicherweise entstand durch den Angriff kein weiterer Schaden. Der Vorfall gilt jedoch als Warnschuss und macht deutlich, wie angreifbar kritische Infrastrukturen durch unzureichende Schutzmaßnahmen sind.

Dass die ausgenutzte Schwachstelle am Risevatnet-Stausee kein Einzelfall darstellt, verrät schon ein Blick in die globale Suchmaschine Shodan, die zum Auffinden vernetzter Geräte dient: Tausende Gebäudeautomatisierungs- und Steuerungssysteme weltweit sind direkt aus dem Internet erreichbar – viele davon ohne ausreichende Sicherheitsvorkehrungen.

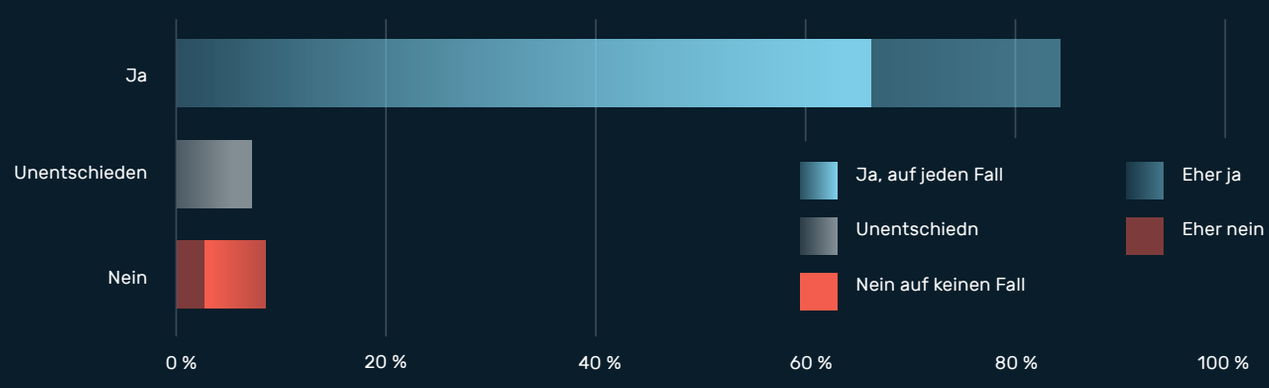
Forderungen nach digitaler Souveränität werden laut

Die angespannte Lage im Bereich der kritischen Infrastrukturen spiegelt sich auch im Meinungsbild der IT-Entscheidungsträger wider. Das geht aus einer aktuellen Civey-Studie im Auftrag von Myra hervor. Über vier Fünftel der Befragten fordern darin, dass kritische Infrastrukturen in Europa künftig ausschließlich oder vorrangig auf europäische Softwarelösungen setzen sollten. Damit zeigt sich ein klarer Konsens – insbesondere unter den Verantwortlichen für IT-Sicherheit.

Gleichzeitig zeigt die Umfrage aber auch: Zwischen Anspruch und Wirklichkeit klafft eine enorme Lücke. Die tatsächliche Abhängigkeit von internationalen Softwareanbietern ist nach wie vor groß, die Umsetzung digitaler Souveränität kommt nur schleppend voran.[19]

Die Implikation ist eindeutig: Während die Bedrohungslage zunimmt und die Forderung nach europäischer Unabhängigkeit lauter wird, bleibt die praktische Umsetzung hinter den Erwartungen zurück. Bekenntnisse allein machen keine Infrastruktur sicher. Was in den Köpfen der IT-Verantwortlichen längst entschieden ist, muss nun konsequent in Budgets, Vergaberichtlinien und Umsetzungspläne übersetzt werden.

Sollten Staaten und Betreiber kritischer Infrastruktur in Europa Ihrer Meinung nach eher europäische Anbieter für digitale Produkte nutzen, um unabhängig von außereuropäischen Anbietern zu sein?



Digitale Souveränität als Schlüssel zu nachhaltiger Digitalisierung und Compliance

Die Mitigationsdaten aus dem Myra SOC sprechen eine deutliche Sprache: die Cyberbedrohungslage in Deutschland ist angespannt wie selten zuvor. Unternehmen sehen sich aber nicht nur mit einer steigenden Zahl von Angriffen konfrontiert, sondern auch mit der Herausforderung, diese technisch und organisatorisch abzuwehren, ohne dabei gegen Datenschutz- und Compliance-Vorgaben zu verstoßen.

Gleichzeitig gilt es, kritische Abhängigkeiten und Risiken in der digitalen Lieferkette zu vermeiden. Insbesondere bei der Sicherung der eigenen Cyberresilienz achten Organisationen aus Deutschland und Europa zunehmend darauf, auf lokale Angebote zu setzen, um ihre digitale Souveränität zu stärken. Speziell vor dem Hintergrund geopolitischer Spannungen und Unsicherheiten gewinnt dieser Trend an Momentum. So sieht sich aufgrund der Politik der US-Regierung unter Präsident Donald Trump mittlerweile jedes zweite Unternehmen in Deutschland gezwungen, die eigene Cloud-Strategie zu überdenken.[20]

Im Gespräch mit Prof. Dr. Louisa Specht-Riemenschneider, Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), und Prof. Dr. Dennis-Kenji Kipker, Cybersicherheitsexperte und Mitglied des Myra Advisory Boards, beleuchten wir die komplexe Gemengelage zwischen digitaler Souveränität, Datenschutz und Cyberresilienz.

Herr Prof. Dr. Kipker, immer wieder führen uns Cyberangriffe vor Augen, wie verwundbar digitale Infrastrukturen in Deutschland immer noch sind. Was sind aus Ihrer Sicht die größten Herausforderungen bei der Abwehr von Cyberattacken – etwa DDoS?

Wir müssen beachten, dass die Abwehr von DDoS-Angriffen längst mehr als eine rein technische Frage ist – es geht um Lieferketten, es geht um Compliance, um Haftung und auch um digitale Souveränität. Denn zur Abwehr von Überlastungsangriffen – etwa durch Traffic-Analyse und Filterung – müssen Dienstleister tief in den Datenverkehr blicken und eingreifen. Das bringt nicht nur technische, sondern vor allem auch erhebliche Compliance-Risiken mit sich. Insbesondere, wenn personenbezogene oder geschäftskritische Daten betroffen sind.

Als Unternehmen muss ich hier sicherstellen, dass die eingesetzten Dienstleister vertrauenswürdig sind und alle regulatorischen Vorgaben einhalten, um Haftungsrisiken zu minimieren und die Verfügbarkeit von Systemen zu gewährleisten. Grundlage hierfür ist ein sauberes Risikomanagement, auf dessen Basis der Dienstleister über eine Due Diligence auf Herz und Nieren geprüft wird.

Die Zusammenarbeit mit internationalen – und besonders US-Dienstleistern wirft oft Fragen auf, da hier unterschiedliche Rechtsräume aufeinandertreffen. Welche Compliance-Risiken ergeben sich daraus?

In der Praxis birgt die Zusammenarbeit mit US-Anbietern große Risiken, da diese Unternehmen in erster Linie der US-amerikanischen Jurisdiktion unterliegen. Selbst wenn Server in der EU stehen, können US-Behörden auf Daten zugreifen, oder besser gesagt, den Zugriff anordnen – Stichwort CLOUD Act, FISA 702 oder Patriot Act. Die politische Entwicklung in den USA, die wir nun in der zweiten Amtszeit von Donald Trump verfolgen können, spitzt diese Problematik weiter zu.

Gleichzeitig ist die rechtliche Basis für DSGVO-konforme transatlantische Datenübertragungen äußerst fragil. Der bestehende Angemessenheitsbeschluss zwischen der EU und den USA baut lediglich auf einer Executive Order von Joe Biden auf, die jederzeit durch seinen Nachfolger widerrufen werden kann. Und Trump hat schon im Rahmen seiner Agenda 47, also seiner US-Präsidentschaftsagenda, bekannt gegeben, dass er alles, was Biden gemacht hat, im Wesentlichen rückgängig machen will.

Mit der Entlassung der demokratischen Mitglieder des Privacy Oversight Boards – einem zentralen Bestandteil des EU-US Data Privacy Frameworks, das als Grundlage für den aktuellen Angemessenheitsbeschluss dient, hat dieser Prozess bereits begonnen. Unternehmen, die sich auf US-Dienstleister verlassen, setzen sich daher einem erheblichen Compliance- und Haftungsrisiko aus.

Welchen strategischen Rat geben Sie Organisationen, um sich zukunftssicher aufzustellen?

Mein Rat ist klar: Unternehmen müssen ihre Abhängigkeit von außereuropäischen Anbietern reduzieren und konsequent auf originär europäische Lösungen setzen. Das betrifft nicht nur DDoS-Schutz, sondern die gesamte digitale Lieferkette. Die regulatorischen Anforderungen – etwa durch die NIS-2-Richtlinie oder den Cyber Resilience Act – werden weiter steigen. Wer jetzt frühzeitig auf europäische Anbieter umstellt, minimiert nicht nur Compliance-Risiken, sondern fördert auch die digitale Souveränität und Resilienz des eigenen Unternehmens. Das ist kein optionaler Schritt mehr, sondern eine Notwendigkeit.

Frau Prof. Dr. Specht-Riemenschneider, in den vergangenen Jahren sind die Abhängigkeiten Deutschlands in Bereichen wie Gesundheit, Energie und IT immer wieder deutlich hervorgetreten. Wie lassen sich diese Abhängigkeiten verringern und die Souveränität Deutschlands stärken?

Die Abhängigkeiten sind oft bekannt, werden aber zu spät oder nicht mit der nötigen Konsequenz adressiert. Ein wesentlicher Grund ist, dass wirtschaftliche Effizienz und kurzfristige Kostenersparnis lange Priorität hatten, während strategische Resilienz und digitale Souveränität erst in Krisenmomenten ins Zentrum rücken.

Für digitale und technische Souveränität braucht es eine vorausschauende Digital- und Industriepolitik, die gezielt europäische Technologien und Infrastrukturen stärkt. Das bedeutet Investitionen in Schlüsseltechnologien wie Cloud, KI und Halbleiter, die europäische Werte verwirklichen. Aber auch eine verstärkte europäische Zusammenarbeit, um Skaleneffekte zu nutzen und eigene Handlungsfähigkeit durch gebündelte Nachfrage zu stärken.

Zudem müssen regulatorische Rahmenbedingungen so gestaltet werden, dass sie grundrechtskonforme Innovation ermöglichen, ohne uns gleichzeitig in neue Abhängigkeiten zu begeben. Kurz gesagt: Wir brauchen weniger Reaktion und mehr strategische Weitsicht.

Wie können wir angesichts des bedrohten EU-US-Datenschutzrahmens unsere Abhängigkeit von nicht-europäischen Technologien verringern und die Kontrolle über Daten in der EU sichern?

Die Vorgänge in den USA sehe ich mit Sorge und hoffe, dass die EU kluge Entscheidungen treffen wird. Gleichzeitig würde ich mir wünschen, dass die europäischen Unternehmen ihren Wissensvorsprung in datenschutzfreundlicher Technologie endlich stärker als Wettbewerbsvorteil erkennen. Ich stehe mit meinem Haus bereit, dabei mit Information und Beratung zu unterstützen und Wege zu bereiten.

Technologie und Know-how sind Europa gegeben, aber an der Umsetzung souveräner IT-Lösungen hapert es. Wo sehen Sie Handlungsbedarf?

Für mich ist die entscheidende Frage: Was hält uns ab? Digitalpolitik muss eine Vision verfolgen, ein Ziel, an dem sich gesetzgeberisches Handeln ausrichten kann. Werteorientierte Digitalisierung könnte so ein Ziel sein. Aufsicht kann durch Information, Beratung, aktive Unterstützung wie Reallabore aktivierend sein. Ich biete das gerne an. Aber die passenden Regeln dafür, die Innovation ermöglichen und gleichzeitig Grundrechte schützen, muss der Gesetzgeber machen. Ich meine, wir brauchen zielgerichtete Investition in Lösungen, die unsere europäischen Werte in eine digitale Zukunft tragen.

Sie wollen mehr erfahren?
Über die QR-Codes gelangen Sie zu den vollständigen Interviews.

Im Gespräch mit Prof. Dr. Dennis-Kenji Kipker | Datenkontrolle und Verfügbarkeit sind Imperative, nicht nur Empfehlungen.

Im Gespräch mit Prof. Dr. Louisa Specht-Riemenschneider (BfDI) | Digitaler Aufbruch: Europas Weg zur Souveränität

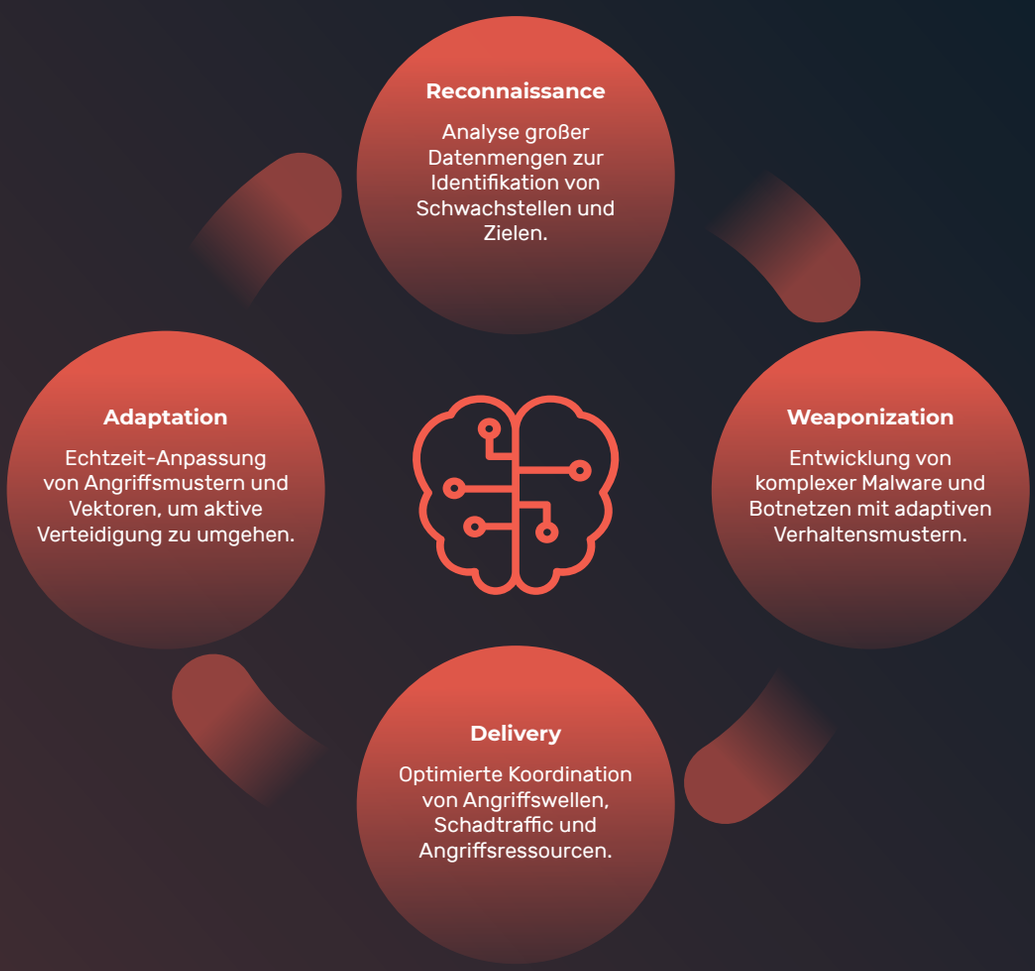
„Offensive AI“ eskaliert die Bedrohungslage

Schnell, präzise, günstig: Die breite Verfügbarkeit von KI revolutioniert die Angriffskampagnen von Cyberkriminellen weltweit. Durch die Integration von KI in Angriffswerkzeugen (Offensive AI) können Cyberakteure schneller und einfacher Lücken in der Abwehr von Unternehmen identifizieren und auf den Angriffsvektor zurückgreifen, der die höchste Erfolgsquote liefert.

Waren früher erfahrene Black Hat Hacker erforderlich, um über mehrere Tage hinweg zielgerichtet Sicherheitslecks für Angriffe wie beispielsweise XSS, SQLi oder ungeschützte Domains auszumachen, kann das heute ein Neuling mit einer gut trainierten KI in wenigen Stunden erledigen. KI ermöglicht es, adaptive und langanhaltende Angriffskampagnen zu orchestrieren, die gezielt ganze Branchen über Monate hinweg attackieren, ohne dass die Urheber identifizierbar sind. Hierdurch verschärft sich die Cyberbedrohungslage enorm, da Angriffe zahlreicher, präziser und schlagkräftiger werden. In der Praxis übernimmt die KI klassische Aufgaben wie Reconnaissance (Informationsbeschaffung), Bewertung von Angriffswegen, Impact-Analyse und die Auswahl der effektivsten Angriffspunkte.

Das nachfolgende Kapitel liefert einen qualitativen Überblick der gegenwärtig relevantesten KI-Cyberrisiken im Kontext schädlicher Datenströme. Die dargestellten Erkenntnisse stützen sich auf empirische Daten und Erfahrungswerte aus dem Myra SOC.

Künstliche Intelligenz verstärkt jede Angriffsphase



KI unterstützt Angriffskampagnen, indem sie klassische Aufgaben wie das Auskundschaften von Zielen, die Analyse möglicher Angriffswege und die Bewertung der erfolgversprechendsten Angriffspunkte automatisiert und optimiert. Dadurch können Attacken gezielter und schneller durchgeführt werden.

Die Rolle von KI in der Weiterentwicklung von DDoS-Attacken

Durch den Einsatz KI-gestützter Angriffswerkzeuge spitzt sich die DDoS-Bedrohungslage immens zu. Cyberkriminelle nutzen zunehmend KI-optimierte Verstärkungsangriffe (Intelligent Amplification Attacks), um sicherzustellen, dass Attacken mit minimalem Ressourceneinsatz eine maximale Wirkung entfalten – beispielsweise durch die dynamische Anpassung der Angriffsvektoren in Sekundenschnelle. Darüber hinaus profitieren Cyberakteure beim Einsatz KI-gestützter Lösungen durch eine weitgehend automatisierte und effizientere Orchestrierung von Angriffen, Botnetzen und Angriffsvektoren.

Intelligente Angriffssysteme sind zudem in der Lage, Abwehrmechanismen wie Rate Limiting und Firewalls gezielt zu umgehen. Sie erkennen Schwachstellen und passen ihre Angriffsmuster flexibel an, was die Entwicklung auto-evasiver Angriffstaktiken ermöglicht. Außerdem lassen sich besonders komplexe und schwer erkennbare Angriffe realisieren, die klassische Schutzmaßnahmen sukzessive aushebeln. Nicht zuletzt sorgt KI für ein autonomes und effektives Management von Botnetzen, wodurch deren Widerstandsfähigkeit und Angriffspotenzial signifikant gesteigert werden.

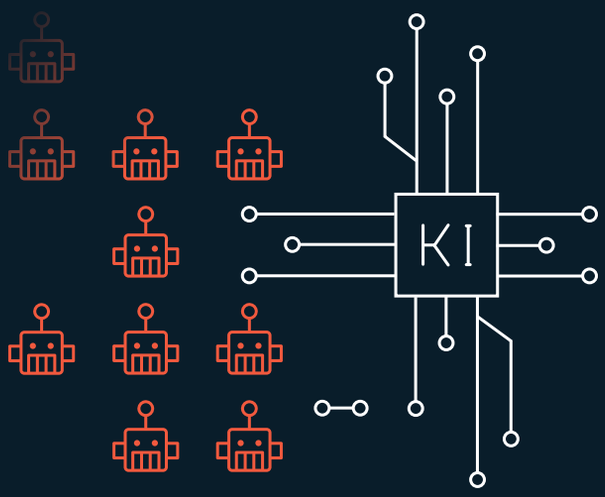
Wie KI das Gefahrenpotenzial schädlicher Requests steigert

Distributed-Denial-of-Service (DDoS):
Durch KI-gestützte Automatisierung werden groß angelegte DDoS-Angriffe einfacher und effizienter umsetzbar.

SQL Injection:
Künstliche Intelligenz beschleunigt die automatisierte Erkennung und Ausnutzung von SQL-Injection-Schwachstellen.

Zero-Day-Angriffe:
Zero-Day-Angriffe nutzen unbekannte Schwachstellen aus und sind besonders schwer abzuwehren.

Cross-Site Scripting (XSS):
Mit KI lassen sich XSS-Angriffe automatisieren und durch schwer erkennbare Payloads weiterentwickeln.

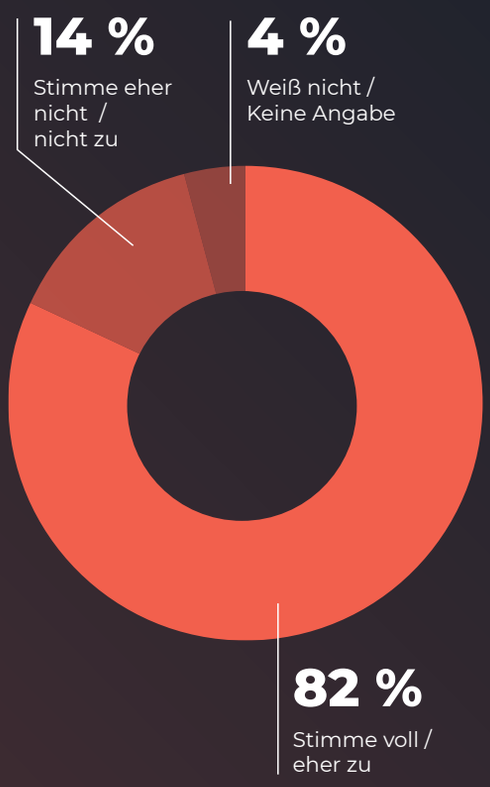


Risiken durch KI-Bots und Crawler

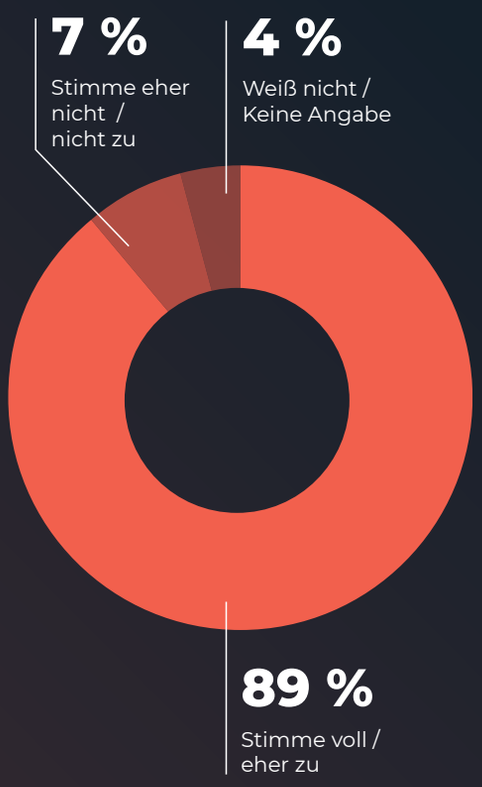
KI-basierte Bots und Crawler durchsuchen das Internet automatisiert und verursachen enorme Serverlast. Ein Beispiel aus veröffentlichten Daten des Cloud-Hosting-Dienstes Vercel zeigt das Ausmaß eindrucksvoll. Allein im Dezember 2024 generierten GPTBot 569 Millionen und ClaudeBot 370 Millionen Anfragen, was einem Anteil von etwa 20 % der Googlebot-Anfragen im gleichen Zeitraum entspricht. Solche immensen Aktivitäten können Webserver überlasten und zu Ausfällen führen, wie etwa ein Vorfall im Git-Hosting-Service SourceHut zeigt, bei dem aggressive LLM Crawler im März 2025 die Server des Unternehmens lahmlegten.

Inwiefern stimmen Sie diesen Aussagen zum Einsatz von KI bei Cyberangriffen zu.

Künstliche Intelligenz ermöglicht es Angreifern, gezielt Schwachstellen in unseren Systemen auszunutzen.



Künstliche Intelligenz trägt dazu bei, dass Cyberangriffe effizienter und zielgerichteter durchgeführt werden können.



Unternehmen sind sich einig: KI macht Angreifer deutlich schlagkräftiger. Mehr als vier Fünftel gehen davon aus, dass KI das gezielte Ausnutzen von IT-Schwachstellen erleichtert, während 9 von 10 Organisationen erwarten, dass Angriffe mittels KI sowohl effizienter als auch zielgerichteter werden.[21]

Quellenverzeichnis

1 https://www.security-insider.de/deutschland-ziel-cyberangriffe-drohnen-russland-a-ce7e9670547109240427f094798ebc58/
2 https://www.spiegel.de/politik/deutschland/cybersicherheit-rechnungshof-warnt-vor-mangelndem-schutz-der-bundes-it-a-6baacfe5-2e6b-4e8b-a64b-e10d9cf2585e
3 Bitkom Wirtschaftsschutz 2024
4 Allianz Risk Barometer 2025
5 EY Datenklaustudie 2025 | Forensic & Integrity Services
6 https://www.cisa.gov/news-events/alerts/2014/01/17/udp-based-amplification-attacks
7 Verizon: 2025 Data Breach Investigations Report
8 https://krebsonsecurity.com/2025/05/krebsonsecurity-hit-with-near-record-6-3-tbps-ddos/
9 Allianz Risk Barometer 2025
10 ENISA: Threat Landscape: Finance Sector 2025
11 BaFin: Strategische Ziele 2026-2029
12 ENISA: Threat Landscape: Finance Sector 2025
13 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Manuel Höferlin, Maximilian Funke-Kaiser, Konstantin Kuhle, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 20/14372
14 Allianz Risk Barometer 2025
15 https://kommunaler-notbetrieb.de
16 https://www.zeit.de/digital/2025-01/parlamentarische-anfrage-zahl-cybersicherheitsvorfaelle-kritische-infrastruktur-gestiegen
17 https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/KRITIS-in-Zahlen/kritis-in-zahlen_node.html
18 https://www.tagesschau.de/inland/innenpolitik/bsi-energie-cyberangriffe-100.html
19 Myra Security: State of Digital Sovereignty 2025
20 Bitkom Cloud Report 2025
21 TÜV Cybersecurity Studie 2025

Deshalb entscheiden sich CISOs für Myra

Security

Durch Cyberangriffe werden Daten gestohlen, Systemausfälle provoziert und Kommunikationskanäle gestört. Myra wehrt Angriffe auf Ihre digitalen Prozesse in Echtzeit ab.

Performance

Traffic-Peaks durch Sales-Kampagnen, Livestreaming oder unplanbare Ereignisse überfordern Web-Anwendungen. Myra liefert Ihren Content immer hochperformant aus.

Business Continuity

Myra gewährleistet den größtmöglichen Schutz für Ihr Unternehmen, indem es direkte und georedundante Verbindungen zu Ihrer Infrastruktur nutzt, ohne von externen Faktoren abhängig zu sein.

Compliance

Gesetzliche und unternehmensspezifische Vorgaben zu IT-Sicherheit und Datenschutz erfordern auditierte Prozesse. Myra ist Ihr Garant für strengste Anforderungen.

Cyberresilienz

Myra stärkt die Robustheit Ihrer Infrastruktur gegen Cyber-bedrohungen, sodass Angriffe die Geschäftsfähigkeit weder beeinträchtigen noch zum Stillstand bringen.

Digitale Souveränität

Mit Myra verwalten Sie Ihre digitale Wertschöpfungskette autark und behalten dabei durchgehend die Kontrolle über kritische Prozesse und Daten.

BSI-zertifizierte IT-Sicherheit

Die Myra-Technologie ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach dem Standard ISO 27001 auf Basis von IT-Grundschutz zertifiziert. Zudem erfüllen wir als einer der führenden Anbieter alle 37 Kriterien des BSI für qualifizierte KRITIS-Sicherheitsdienstleister. Damit setzen wir den Maßstab in der IT-Sicherheit.

ISO 27001 BSI zertifiziert auf der Basis von IT-Grundschutz Zertifikat Nr.: BSI-IGZ-0667-2024 | PCI DSS Certified | BSIG KRITIS-qualifiziert | BSI C5 Testat Typ 2 | Trusted Cloud Service | IDW PS 951 ISAE 3402 | KRITIS Nachweis gemäß § 8a. Abs. 3 BSIG | ISO 9001:2015

Zertifiziert vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf Basis von IT-Grundschutz | Zertifiziert nach Payment Card Industry Data Security Standard (PCI DSS) | KRITIS-qualifiziert nach §3 BSI-Gesetz | BSI-C5-Testat Typ 2 | Geprüfter Trusted Cloud Service | IDW PS 951 Typ 2 (ISAE 3402) geprüfter Dienstleister | KRITIS-Betreiber gemäß § 8a Abs. 3 BSIG | Qualitätsmanagement nach ISO 9001

Myra schützt, was zählt. In der digitalen Welt.

1&1 versatel | Barmenia Gothaer | Baden-Württemberg Staatsministerium | msc Munich Security Conference

Sparkasse | lb 1861 | flatex DEGIRO | Stadt Regensburg

Made in Germany

Myra schützt, was zählt.
In der digitalen Welt.

Sie wollen mehr darüber erfahren, wie Sie mit unseren Lösungen Ihren Umsatz steigern, Ihre Kosten minimieren und Ihre Anwendungen vor bösartigen Angriffen schützen? Unser Expertenteam berät Sie gerne individuell und erarbeitet eine maßgeschneiderte Lösung für Ihre Organisation. Vereinbaren Sie am besten noch heute ein unverbindliches Beratungsgespräch.

Cyberangriffe sind teuer,
ein unverbindliches Gespräch kostet nichts.

Myra Security GmbH

+49 89 414141 - 345
www.myrasecurity.com
info@myrasecurity.com