

Sicher leben in unsicheren Zeiten.

Januar 2025 | LBBW Research



- 01 Verteidigungsfähigkeit stärken.
[Seite 2 →](#)

- 02 Vor Cybersicherheitsrisiken schützen.
[Seite 6 →](#)

- 03 In „Sicherheit“ investieren.
[Seite 10 →](#)

Sicherheit ist ein zentrales Bedürfnis.

„Ohne Sicherheit ist keine Freiheit“ sagte schon Wilhelm von Humboldt 1792. Weise Worte, die auch mehr als 200 Jahre später noch Gültigkeit beanspruchen. Sicherheit ist eine unabdingbare Voraussetzung für alle Bereiche des öffentlichen Lebens und ein Grundbedürfnis des sozialen Zusammenlebens. Heute basiert Sicherheit auf der Fähigkeit zur Verteidigung, der Abwehr von Cyberkriminalität und dem Schutz kritischer Infrastrukturen.

Neben der physischen Verteidigung, die zu einer Renaissance der Rüstungsindustrie geführt hat, gewinnt die digitale Sicherheit zunehmend an Bedeutung. Be-

sonders wichtig ist dabei die Sicherung der kritischen Infrastruktur wie z. B. der Strom- und Wasserversorgung oder der Telekommunikationsnetze. Auch der Schutz von Unternehmen, ihrer Technologien sowie die persönliche Sicherheit im Eigenheim müssen gewährleistet sein, in der realen und in der digitalen Welt.

Angesichts technologischer Veränderungen und geopolitischer Spannungen bedarf es einer neuen Bewertung des Themas Sicherheit. Sicher ist dabei, dass Investitionen in Verteidigung, Cybersicherheit und kritische Infrastruktur von entscheidender Bedeutung sind.

Autoren:
Marcel Gaupp
 Head of Corporate Research
Sandro Pannagl
 Strategy/Macro Research
Stefan Maichl
Mirko Maier
Tobias Willems
Bettina Deuscher
 Corporate Research

Erstellt am: 08.01.2025, 10:00
 Erstmalige Weitergabe am:
 08.01.2025, 10:00

01 Verteidigungsfähigkeit stärken.

Der Angriff Russlands auf die Ukraine im Februar 2022 brachte eine Zeitenwende und machte klar: Europa braucht einen neuen Realismus in der Sicherheitspolitik. Dies umso mehr, da auch die internationale Ordnung mit dem Konflikt im Nahen Osten sowie der zunehmenden Rivalität zwischen den USA und China fragiler denn je erscheint.

Die Weltordnung befindet sich in einem strukturellen Wandel. Insbesondere Europa steht vor großen Herausforderungen. Es muss sich gegen das Erstarren autoritärer Staaten behaupten und im Kräfte-messen der Weltmächte bestehen.

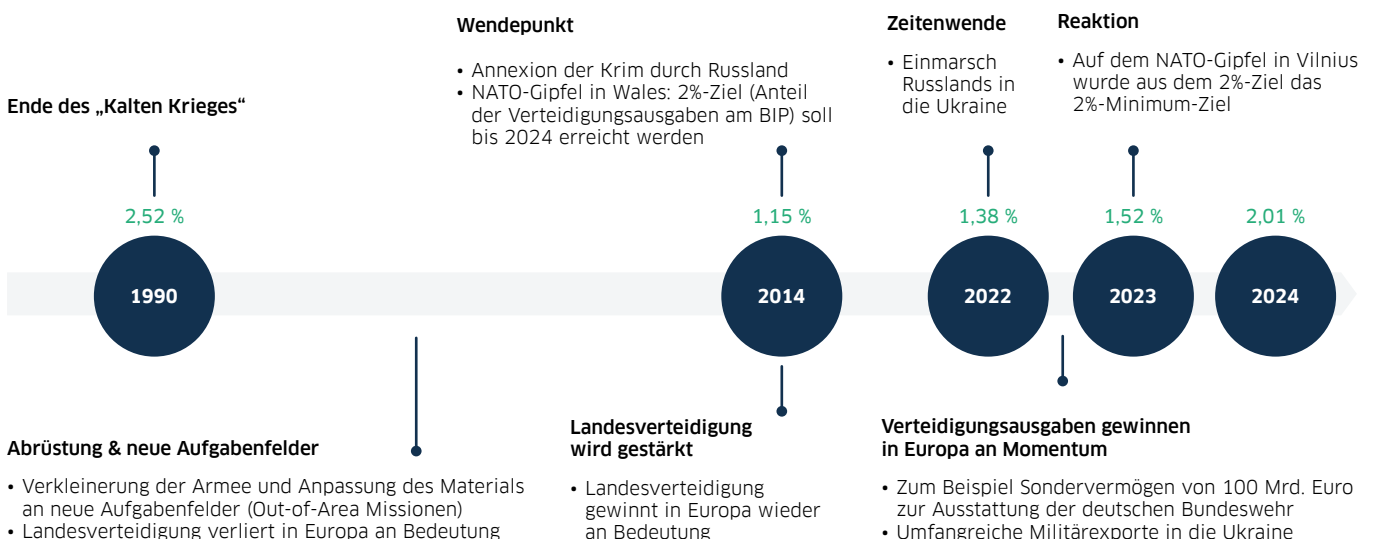
Doch die jahrelange Unterfinanzierung der militärischen Einheiten, Doppelstrukturen bei Verwaltung und Kommandos sowie mangelnde Interoperabilität der europäischen Systeme haben

die Verteidigungsfähigkeit der Union geschwächt.

Unter Donald Trump kann sich Europa nicht mehr ohne weiteres auf die USA als Schutzmacht verlassen. Die europäischen Staaten sind vielmehr gefordert, ihre Sicherheit selbst in die Hand zu nehmen. Um die Sicherheit dauerhaft aufrechtzuerhalten, wird Europa nicht um eine stärkere Koordination und höhere Verteidigungsausgaben herumkommen.

Die Sicherheitslage beeinflusst die Verteidigungsausgaben.

Anteil verteidigungsrelevanter Ausgaben am BIP in Deutschland in % (in grün)



Quellen: Statista, LBBW Research; Stand: 11.09.2024

Drei Säulen der Sicherheit.



Quelle: LBBW Research

Renaissance der Rüstungsindustrie.

Seit Beginn des Ukrainekriegs erlebt der europäische Rüstungssektor eine Renaissance. Ob Politik, Gesellschaft, Wirtschaft oder Kapitalmarkt, sie alle bewerten Rüstung positiver und differenzierter als zuvor. Hauptaspekte dieser Neubewertung sind:

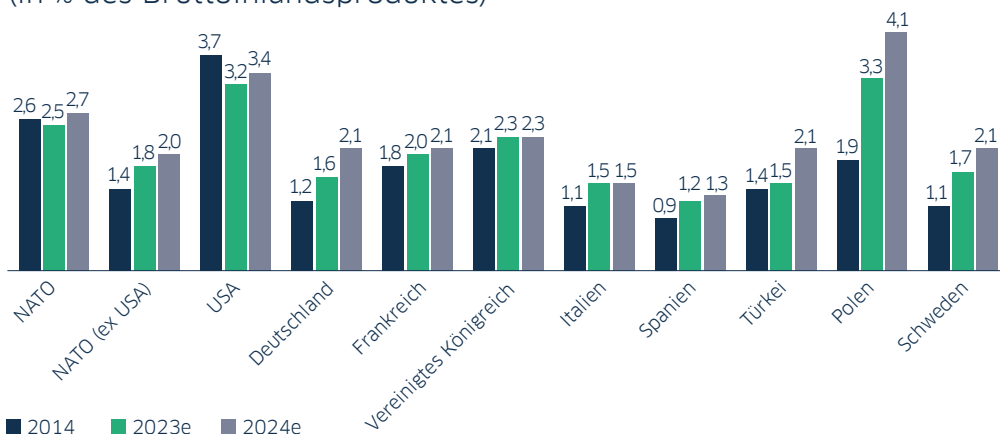
- **Gestiegenes Sicherheitsbedürfnis:** Die Bedrohung durch den Ukrainekrieg hat das Bewusstsein für die nationale Sicherheit in der Bevölkerung und der Politik geschärft.
- **Rollenwechsel:** Während Rüstung früher oft kritisch betrachtet wurde, wird diese nun zunehmend als notwendig angesehen, um Frieden und Stabilität zu sichern.
- **Öffentliche Diskussion:** In vielen Ländern gibt es eine verstärkte öffentliche Debatte darüber, welche Summen in Verteidigung

fließen sollen und welche Rolle die Rüstungsindustrie spielen sollte.

- **Investitionsbereitschaft:** Die Bereitschaft, in Verteidigung und Sicherheit zu investieren, ist deutlich angestiegen, was das Vertrauen der Investoren in eine nachhaltige Wachstumsperspektive der Rüstungsbranche gestärkt hat.

Schon nach der Krim-Annexion durch Russland im Jahr 2014 zeichnete sich eine Wende bei der Investitionsbereitschaft ab. In der NATO (ex USA) wuchsen die Verteidigungsausgaben seither im Durchschnitt real um rund 4 %. Ab 2022 beschleunigte sich der Trend. 2024 ist ein realer Anstieg von 18 % auf 430 Mrd. US-Dollar geplant. 2024 dürften 23 der 32 NATO-Staaten das Zwei-Prozent-Ziel erreicht oder übertroffen haben. Inzwischen werden höhere Ziele für die Verteidigungsausgaben diskutiert.

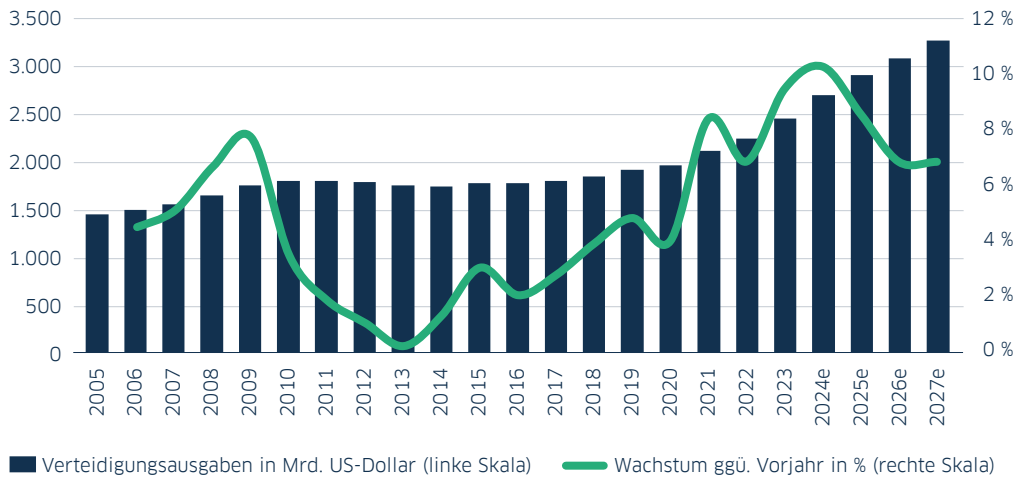
Verteidigungsausgaben ausgewählter NATO-Länder* (in % des Bruttoinlandsproduktes)



* konstante Preise und Wechselkurse 2015
Quelle: NATO, LBBW Research



Globale Verteidigungsausgaben in Mrd. US-Dollar.



Quelle: SIPRI, Statista, ab 2024 Simulation LBBW Research

Investitionsboom bei Verteidigung löst Superzyklus 2.0 aus.

Mit 2,44 Bio. US-Dollar haben die weltweiten Verteidigungsausgaben nach Schätzung des Friedensforschungsinstituts SIPRI im Jahr 2023 einen Höchstwert erreicht. Dies entspricht rund 2,3 % des globalen Bruttoinlandsprodukts (BIP). In den kommenden Jahren dürften die Ausgaben weiter steigen.

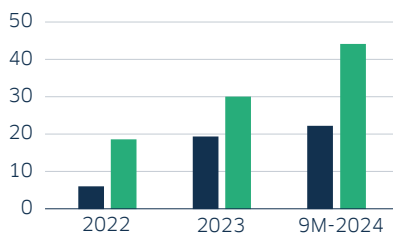
Verschiedene Prognoseinstitute erwarten im Zeitraum von 2023 bis 2027 ein durchschnittliches Wachstum der Verteidigungsausgaben zwischen 5 % und 7 % pro Jahr. Die gestiegene Nachfrage nach Rüstungsgütern hat bereits zu einer positiven Entwicklung bei den Aufträgen geführt, wie das Beispiel Rheinmetall zeigt. Ein überproportionales Wachstum erscheint insbesondere in Europa (Bedrohung durch Russland) und der Region Asien-Pazifik (Bedrohung durch China)

sowie im Hinblick auf die Teilstreitkräfte bei den Landstreitkräften und im maritimen Sektor wahrscheinlich.

Für die europäische Rüstungsindustrie dürfte dies der Beginn einer lang anhaltenden Wachstumsphase sein. Denn in vielen NATO-Staaten war die Ausrüstung der Streitkräfte lange Zeit quantitativ und qualitativ unterdimensioniert. Auf dem NATO-Gipfel im Juni 2025 könnte daher eine Anhebung des NATO-Budgetziels in Richtung 3 % beschlossen werden.

Der Rüstungskonzern Rheinmetall, der vor allem in der Ausrüstung von Landstreitkräften tätig ist, spricht angesichts steigender Budgets und Neubeschaffungen sogar vom Beginn eines langfristigen Superzyklus 2.0. Zudem erfordern die technologischen Fortschritte in den Bereichen Elektronik, Sensorik und Unterstützung durch KI die kontinuierliche Modernisierung der bestehenden Ausrüstung.

Nachfrageentwicklung Rheinmetall*.



■ Auftragseingang in Mrd. Euro
■ Auftragsbestand in Mrd. Euro

* inklusive Rahmenverträge

Quelle: Rheinmetall, LBBW Research

Automatisierungsgrad in der Militärtechnik nimmt weiter zu.

	Anteil Elektronikkomponenten		
	Früher	Aktuell	Zukünftig
Kampfpanzer	ca. 25 %	Leopard 2 A7 (ca. 45 %)	Erwartet ca. 55 %
Kampfflugzeug	ca. 25 %	Eurofighter (ca. 40 %)	Erwartet ca. 45 %
Fregatte	F122-Klasse (ca. 20 %)	F125-Klasse (ca. 35 %)	Erwartet ca. 40 %

Quelle: Renaissance Strategic Advisors, Hensoldt, LBBW Research; Stand: 26.08.2024

Umweltziele EU-Taxonomie.



Quelle: LBBW Research

Klassifizierung von Waffensystemen.



Geächtete Waffen sind gleichzeitig immer auch kontroverse Waffen, die aber zusätzlich durch internationale Abkommen verboten sind.

Quelle: LBBW Research



Neubewertung der Rüstungsindustrie.

Die Aussicht auf eine anhaltende Wachstumsphase und relativ stabile Einkommensströme machen die Rüstungsindustrie als wenig konjunktursensiblen Sektor für Investoren wieder attraktiv. Gleichwohl sind ethische und moralische Aspekte deshalb nicht verschwunden. Insbesondere in Europa wird diskutiert, ob Investitionen in Rüstungsunternehmen als notwendig für die nationale Sicherheit und Verteidigung angesehen werden können. In der EU-Taxonomie taucht die Rüstungsindustrie aufgrund der relativ geringen Umwelteffekte explizit nicht auf. Sie wird somit weder als ökologisch nachhaltig noch als nicht ökologisch nachhaltig klassifiziert.

Ein weiterer Punkt ist der Umgang mit kontroversen und geächteten Waffen. Da es keine allgemeingültige Definition gibt, werden unter kontroversen Waffen im Folgenden militärische Waffen verstanden, deren Verwendung entweder unverhältnismäßiges Leid bei Kampfteilnehmern bzw. Zivilisten auslöst oder zu Massenvernichtung führt.

Viele dieser Waffentypen sind darüber hinaus durch internationale Abkommen verboten und werden deshalb als geächtete Waffen klassifiziert. Die Herstellung und der Einsatz dieser Waffen sind in den an den Abkommen partizipierenden Ländern verboten. Auch für die meisten Anleger bleiben Investitionen in Hersteller von geächteten Waffen ein Tabu.

Top 10 der unternehmensbezogenen Ausschlusskriterien nachhaltiger Geldanlagen in Deutschland 2023 (in %).



Quelle: Forum Nachhaltige Geldanlagen, LBBW Research

Eine 2023 durchgeführte Markterhebung des Forums Nachhaltige Geldanlagen ergab, dass geächtete Waffen an vorderster Stelle bei den Ausschlusskriterien nachhaltiger Geldanlagen in Deutschland standen. Waffen an sich wurden hingegen weitaus weniger kritisch bewertet.

02 Vor Cybersicherheits- risiken schützen.

In einer digitalisierten Welt ist Cyberkriminalität ein weiteres Sicherheitsrisiko. Die Schäden durch Cyberangriffe sind schon jetzt beträchtlich und dürften durch den Missbrauch von KI weiter zunehmen. Umso wichtiger ist es, den Schutz gegen Cybersicherheitsrisiken zu intensivieren, insbesondere bei kritischen Infrastrukturen.

Cyberangriffe auf hohem Niveau.

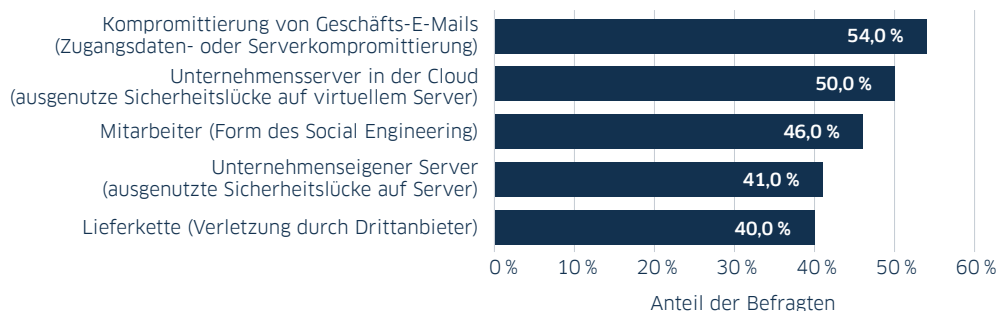
Sicherheit und Verteidigungsfähigkeit schließen in der heutigen Welt den Schutz vor und die Abwehr von Bedrohungen im digitalen Raum ein. Das gilt für Staaten, Unternehmen und Privatpersonen gleichermaßen.

So zeigt der Blick auf die Entwicklung der weltweiten Cyberangriffe einen besonders starken Anstieg in den Jahren 2020 und 2021. Zu dieser Zeit befanden sich aufgrund der Corona-Pandemie sehr viele Menschen im Homeoffice. Da längst nicht alle privaten Computer über hohe Sicherheitsstandards verfügen,

war das Risiko erfolgreicher Angriffe zu dieser Zeit besonders hoch. In den Jahren 2022 und 2023 ging die Zahl der Cyberangriffe zwar leicht zurück, lag aber immer noch rund 60 % über dem Vor-Corona-Niveau.

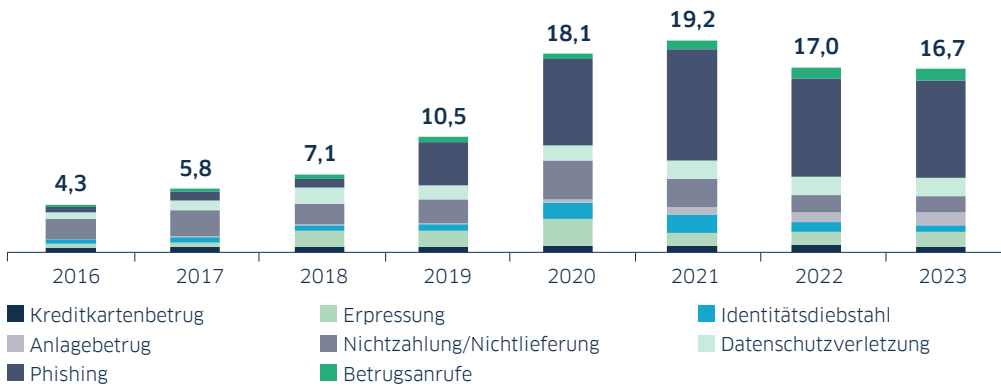
Mehr als die Hälfte der Cyberangriffe entfiel 2023 auf das Phishing. Hierbei versuchen Kriminelle z. B. mittels einer E-Mail die Empfänger dazu zu bringen, Links auf gefälschte Webseiten zu folgen und dort sensible Informationen wie Nutzernamen und Passwörter einzugeben. Dieses relativ einfache Vorgehen birgt für den Angreifer ein geringes Risiko bei einer gleichzeitig hohen Erfolgsrate.

Weltweit häufigste Einstiegspunkte für Cyberangriffe in den letzten 12 Monaten im Jahr 2024.



Quellen: Hiscox, Statista, LBBW Research; Stand: September 2024

Entwicklung der Cyberangriffe weltweit (in Mio.)



Quelle: Statista, LBBW Research

Ein Problem ist die kontinuierliche Weiterentwicklung der Art, wie Cyberangriffe durchgeführt werden. Neben den bekannten Bedrohungen erhöht die missbräuchliche Nutzung von künstlicher Intelligenz und maschinellem Lernen die Komplexität und die Qualität der Angriffe. In Deutschland hat das Bundeskriminalamt sowohl qualitativ als auch quantitativ eine steigende Tendenz bei Cyberkriminalität festgestellt.

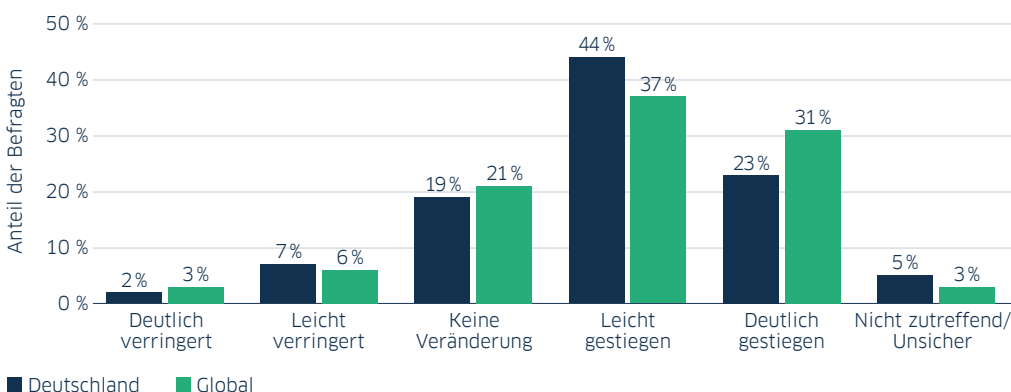
Große Schäden und weitreichende Folgen durch Cyberangriffe.

Die durch Cyberkriminalität verursachten Schäden können hohe Ausmaße annehmen. Angaben des Bundeskriminalamts zufolge lagen diese 2023 in Deutschland bei 148 Mrd. Euro. Ziel der Angreifer ist häufig der Diebstahl von Kundendaten, Zugangsdaten und Passwörtern sowie Patenten beziehungs-

weise Informationen aus den Bereichen Forschung und Entwicklung. Durch das Ausspionieren von Betriebsgeheimnissen und das Stehlen von geistigem Eigentum können Unternehmen Wettbewerbsvorteile verlieren.

Ein Weckruf für die deutsche Industrie war der Cyberangriff auf die Continental AG im Sommer 2022. Über mehrere Wochen konnten Angreifer 40 Terabyte Daten erbeuten, darunter auch sensible Daten. Diese Daten haben die Cyberkriminellen im Darknet für 50 Mio. US-Dollar angeboten, Continental verweigerte die Lösegeldzahlung. Im April 2023 führte ein Cyberangriff bei Evotec dazu, dass das Biotechnologieunternehmen seinen Geschäftsbericht nicht fristgerecht veröffentlichen konnte. Die Aktie musste aufgrund der Pflichtverletzung den MDAX verlassen, was mit deutlichen Kursverlusten einherging.

Der Einfluss von generativer KI auf die Cybersicherheit steigt.

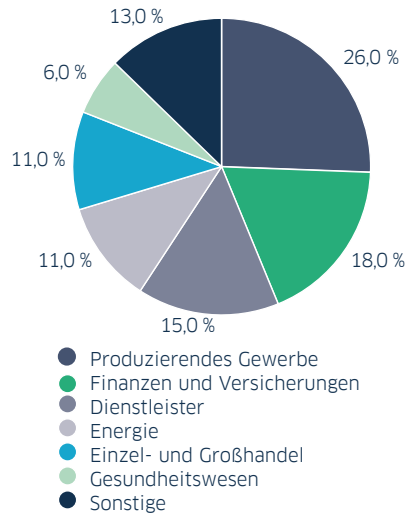


Quellen: PwC, Statista, LBBW Research; Stand: Juli 2024

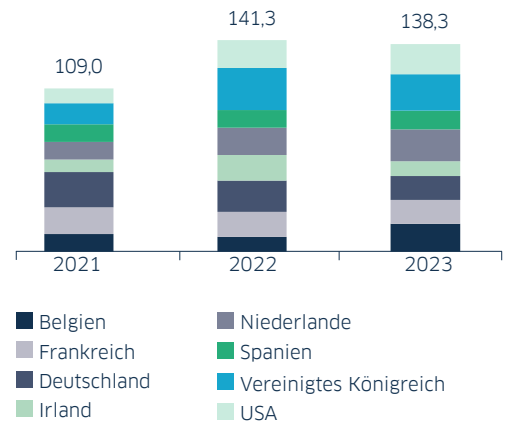
Umfrage: Inwieweit hat generative KI die Angriffsfläche für Cyberangriffe in Ihrer IT-Umgebung in den letzten 12 Monaten beeinflusst?



Verteilung von Cyberangriffen nach Branchen.



Durchschnittliche Schadenssumme je Cyberangriff in ausgewählten Ländern (in Tsd. US-Dollar).



Quelle: Statista, LBBW Research

Die Folgen von Cyberangriffen können noch gravierender sein, wenn sie zu längeren Produktionsausfällen führen oder sich gegen kritische Infrastrukturen wie die Energie- und Wasserversorgung, Krankenhäuser, den öffentlichen Verkehr oder Telekommunikationsnetze richten.

EU beschließt schärfere Präventionsmaßnahmen.

Die digitale Infrastruktur ist inzwischen zur gesellschaftlichen und wirtschaftlichen Lebensader geworden. Ländergrenzen verlieren dadurch an Bedeutung. Doch der signifikante Anstieg von Cyberangriffen hat zu einer deutlich veränderten Bedrohungslage geführt, insbesondere in Europa.

Die EU hat darauf reagiert und die rechtlichen Rahmenbedingungen verschärft. Klare Ziele sind, die Widerstandsfähigkeit gegen Cyberangriffe zu verbessern, die Reaktionszeiten zu verkürzen und die Störanfälligkeit der kritischen Infrastrukturen (KRITIS) durch unvorhergesehene Ereignisse mit Gefährdungspotenzial zu senken. Der Schwerpunkt liegt hierbei auf Netz- und Informationssystemen.

Die für alle Länder geltenden Mindeststandards umfassen insbesondere einheitliche Meldepflichten, Risikobewertungen und die Abschaffung von etwaigen Doppelregulierungen. Da die weit gefasste EU-Regulatorik den All-Gefahren-

Ansatz (sowohl von Naturkatastrophen als auch von Menschen verursachte Gefährdungen) verfolgt, gewährte die EU-Kommission den Mitgliedsländern eine mehrjährige Umsetzungsfrist, die am 17. Oktober 2024 endete.

Basierend auf dem EU-weiten Regelwerk NIS2 (Network and Information Security 2 Directive) wurden auch in Deutschland die bestehenden IT-Sicherheitsgesetze durch das neue NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz ergänzt.

Zudem soll das KRITIS-Dachgesetz (KRITIS-DachG) in Deutschland einen bundeseinheitlichen und sektorübergreifenden Rechtsrahmen für den physischen Schutz kritischer Infrastrukturen schaffen. Ziel ist es, die Widerstandsfähigkeit zu erhöhen und eine einheitliche Vorgehensweise bei Störfällen zu etablieren.

Anbieter von Cybersicherheitsdienstleistungen profitieren.

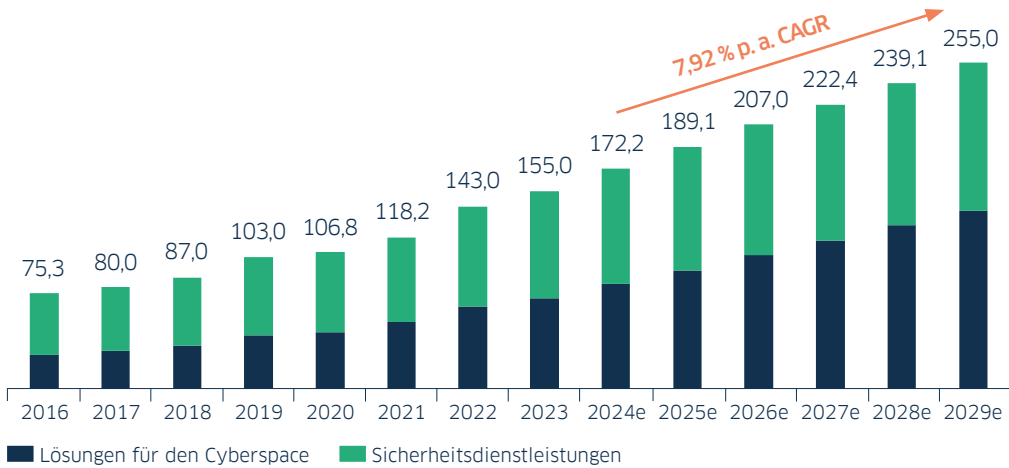
Die verschärften rechtlichen Rahmenbedingungen und die steigende Investitionsbereitschaft sind Wachstumstreiber für die Anbieter von IT-Sicherheitslösungen. Laut einer Umfrage des Branchenverbands der deutschen Informations- und Telekommunikationsbranche, Bitkom e.V., erhöhte sich der durchschnittliche Anteil des Budgets, den deutsche Unternehmen für IT-Sicherheit einplanen, 2024 im Vergleich zum Vorjahr um 21 %.

Unternehmen der kritischen Infrastruktur stammen laut dem Entwurf des KRITIS-DachG aus den folgenden Branchen:

1. Energie
2. Transport & Verkehr
3. Finanz- und Versicherungswesen
4. Gesundheit
5. Ernährung
6. Trinkwasser
7. Abwasser
8. Siedlungsabfallentsorgung
9. Informationstechnik
10. Telekommunikation
11. Weltraum

Quelle: Bundesministerium des Innern und für Heimat

Globaler Umsatz mit Cybersicherheit (in Mrd. Euro).



Quelle: Statista, LBBW Research

Der globale Markt für Cybersicherheit wächst kontinuierlich und soll 2024 einen Gesamtumsatz von 172 Mrd. Euro erreichen. Für die kommenden fünf Jahre wird eine durchschnittliche jährliche Wachstumsrate von 7,92 % (CAGR 2024 bis 2029) prognostiziert.

Wesentliche Treiber dieses Wachstums sind neben der weltweiten Verbreitung und Nutzung des Internets die voranschreitende Digitalisierung in den Unternehmen sowie die steigende Zahl von Cyberangriffen. Flexible Arbeitsmodelle wie Homeoffice erhöhen den Bedarf an Cybersicherheit zusätzlich. Von der steigenden Nachfrage profitieren die Anbieter von Lösungen und Dienstleistungen

zur Cybersicherheit. Hierzu zählen u. a. die Netzwerksicherheit, die unerlaubte Zugriffe und den Missbrauch von Netzwerken verhindert, die Datensicherheit, die Daten vor unbefugtem Zugriff und Datenverlust schützt, sowie die Anwendungs- und Endpunktsicherheit, die Sicherheitslücken in Softwareanwendungen und Endgeräten wie Computern und Smartphones schließt. Die gute Nachricht: Parallel zu den Cyberangriffen entwickeln sich auch die Schutzmaßnahmen ständig weiter.

Noch ist der Markt von vielen kleineren Unternehmen geprägt. Dennoch gibt es einige Anbieter, die den Markt dominieren. Für die Zukunft ist von einer Konsolidierung auszugehen.

Ausgewählte Anbieter im Bereich Cybersicherheit (Marktkapitalisierung und Wachstum).

Cybersicherheit

Lösungen für den Cyberspace

Palo Alto Networks

980 % Wachstum 10 Jahre

124 Mrd. US-Dollar Marktkapitalisierung

CrowdStrike

841 % Wachstum 10 Jahre

79 Mrd. US-Dollar Marktkapitalisierung

IBM

196 % Wachstum 10 Jahre

196 Mrd. US-Dollar Marktkapitalisierung

Sicherheitsdienstleistungen

Cisco Systems

231 Mrd. US-Dollar Marktkapitalisierung

129 % Wachstum 10 Jahre

Fortinet

63 Mrd. US-Dollar Marktkapitalisierung

1392 % Wachstum 10 Jahre

Capgemini

28 Mrd. US-Dollar Marktkapitalisierung

195 % Wachstum 10 Jahre

Quelle: Bloomberg, LBBW Research

03 In „Sicherheit“ investieren.

Die Weltordnung befindet sich in einem strukturellen Wandel. Für Unternehmen aus den Bereichen Rüstung und Cybersicherheit bietet das langfristige Wachstumschancen. Anleger können das Trendthema Sicherheit über einen Investmentfonds in ihren Depots abbilden.



Frieden und Freiheit sind wertvolle Errungenschaften. Doch es gibt sie nicht zum Nulltarif. Staaten wie Unternehmen sind fortlaufend Gefahren ausgesetzt – in physischer Form (Krieg, Sabotage) und zunehmend in virtueller Form (Hackerangriffe). Die Stärkung der Widerstandsfähigkeit und der Schutz kritischer Infrastrukturen gegen solch hybride Bedrohungen erfordern in den kommenden Jahren hohe Investitionen, besonders in Europa, das seine Verteidigungsfähigkeit lange vernachlässigt hat.

Russlands Angriff auf die Ukraine hat eine Zeitenwende in der europäischen Verteidigungspolitik eingeleitet. Allein Deutschland stellt für eine bessere Ausstattung der Bundeswehr ein Sondervermögen von 100 Mrd. Euro bereit. Andere Länder erhöhen ihre Etats ebenfalls deutlich.

Aussichtsreiche Perspektiven für Unternehmen und Investoren.

Für Firmen, die in den Bereichen Cybersicherheit und Verteidigung Produkte und Lösungen anbieten, lässt ein solches Umfeld steigende Aufträge erwarten. Das lockt die Privatwirtschaft. Unternehmen wie die Lufthansa oder der Motorenhersteller Deutz

planen den Ausbau bzw. Aufbau von Aktivitäten im Rüstungssektor.

Gleiches gilt für den Bereich Cybersicherheit, wo Netzwerksicherheit und Datenschutz weiterhin stark an Bedeutung gewinnen. Voraussetzung für eine sichere und effiziente Kommunikation ist eine leistungsstarke Infrastruktur, die von den Telekommunikationsunternehmen bereitgestellt wird. Start-ups mit hoher Expertise im Bereich künstliche Intelligenz können wiederum die Leistungsfähigkeit der Streitkräfte erhöhen.

Das langfristige Wachstumspotenzial sowie ein steigendes Angebot an Investitionsmöglichkeiten machen das Trendthema Sicherheit auch für private Anleger interessant. Hinzu kommt, dass die Unternehmen oft stabile Einkommensströme aufweisen, da die Ausgaben für Sicherheit und Verteidigung vor allem von Veränderungen in den Sicherheitslagen beeinflusst werden und weniger von Konjunkturzyklen. Ethische und moralische Aspekte sollten bei Investitionsentscheidungen weiterhin berücksichtigt werden. Dies gilt insbesondere für geächtete Waffen, die von Investitionen ausgeschlossen bleiben.



Impressum

Herausgeber:

LBBW Corporate Research
Bei Fragen wenden Sie sich bitte an Ihren Anlageberater.

Redaktion:

LBBW Research

Fotoquellen:

Getty Images, Landesbank Baden-Württemberg

Konzeption und Gestaltung:

Busch und Partner, Journalisten

Redaktionsschluss:

08.01.2025

Disclaimer

Diese Publikation richtet sich ausschließlich an Empfänger in der EU der Schweiz und in Liechtenstein.

Diese Publikation wird von der LBBW nicht an Personen in den USA vertrieben und die LBBW beabsichtigt nicht, Personen in den USA anzusprechen.

Aufsichtsbehörden der LBBW: Europäische Zentralbank (EZB), Sonnemannstraße 22, 60314 Frankfurt am Main, und Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Graurheindorfer Str. 108, 53117 Bonn / Marie-Curie-Str. 24-28, 60439 Frankfurt.

Diese Publikation beruht auf von uns nicht überprüfbaren, allgemein zugänglichen Quellen, die wir für zuverlässig halten, für deren Richtigkeit und Vollständigkeit wir jedoch keine Gewähr übernehmen können. Sie gibt unsere unverbindliche Auffassung über den Markt und die Produkte zum Zeitpunkt des Redaktionsschlusses wieder, ungeachtet etwaiger Eigenbestände in diesen Produkten. Diese Publikation ersetzt nicht die persönliche Beratung. Sie dient nur Informationszwecken und gilt nicht als Angebot oder Aufforderung zum Kauf oder Verkauf. Für weitere, zeitnähere Informationen über konkrete Anlagemöglichkeiten und zum Zwecke einer individuellen Anlageberatung wenden Sie sich bitte an Ihren Anlageberater.

Wir behalten uns vor, unsere hier geäußerte Meinung jederzeit und ohne Vorankündigung zu ändern. Wir behalten uns des Weiteren vor, ohne weitere Vorankündigung Aktualisie-

rungen dieser Information nicht vorzunehmen oder völlig einzustellen.

Die in dieser Ausarbeitung abgebildeten oder beschriebenen früheren Wertentwicklungen, Simulationen oder Prognosen stellen keinen verlässlichen Indikator für die künftige Wertentwicklung dar.

Die Entgegennahme von Research-Dienstleistungen durch ein Wertpapierdienstleistungsunternehmen kann aufsichtsrechtlich als Zuwendung qualifiziert werden. In diesen Fällen geht die LBBW davon aus, dass die Zuwendung dazu bestimmt ist, die Qualität der jeweiligen Dienstleistung für den Kunden des Zuwendungsempfängers zu verbessern.

Mitteilung zum Urheberrecht: © 2025, Moody's Analytics, Inc., Lizenzgeber und Konzerngesellschaften („Moody's“). Alle Rechte vorbehalten. Ratings und sonstige Informationen von Moody's („Moody's-Informationen“) sind Eigentum von Moody's und/oder dessen Lizenzgebern und urheberrechtlich oder durch sonstige geistige Eigentumsrechte geschützt. Der Vertriebshändler erhält die Moody's-Informationen von Moody's in Lizenz. Es ist niemandem gestattet, Moody's-Informationen ohne vorherige schriftliche Zustimmung von Moody's ganz oder teilweise, in welcher Form oder Weise oder mit welchen Methoden auch immer, zu kopieren oder anderweitig zu reproduzieren, neu zu verpacken, weiterzuleiten, zu übertragen, zu verbreiten, zu vertreiben oder weiterzuverkaufen oder zur späteren Nutzung für einen solchen Zweck zu speichern. Moody's® ist ein eingetragenes Warenzeichen.



LBBW auf LinkedIn
<https://de.linkedin.com/company/lbbw>



LBBW auf YouTube
<https://www.youtube.com/user/LBBWDirekt>



LBBW auf Instagram
<https://www.instagram.com/die.lbbw>



LBBW auf Facebook
<https://www.facebook.com/LBBW.Stuttgart>



LBBW auf Xing
<https://www.xing.com/company/lbbw>

Landesbank Baden-Württemberg

www.LBBW.de
kontakt@LBBW.de

Hauptsitze

Stuttgart

Am Hauptbahnhof 2
70173 Stuttgart
Telefon 0711 127-0

Karlsruhe

Ludwig-Erhard-Allee 4
76131 Karlsruhe
Telefon 0721 142-0

Mannheim

Augustaanlage 33
68165 Mannheim
Telefon 0621 428-0

Mainz

Rheinallee 86
55120 Mainz
Telefon 06131 64-0