DIGITAL SICHER NRW

Kompetenzzentrum für Cybersicherheit in der Wirtschaft

CYBERSICHERHEIT IN NRW 2026

Studie zur IT-Sicherheit in Unternehmen

In Zusammenarbeit mit G DATA CyberDefense, statista, brand eins

DIGITAL SICHER NRW

GRUSSWORTE DER HERAUSGEBER

Geopolitische Spannungen, Künstliche Intelligenz (KI) und eine professionalisierte Angriffsindustrie: Die **Bedrohungslage für Unternehmen** hat sich in den vergangenen Jahren spürbar verschärft. Umso wichtiger ist es, IT-Sicherheit strategisch anzugehen. Die seit Dezember 2025 geltende **NIS-2-Richtlinie** bietet dafür eine Chance, indem sie Orientierung gibt und verbindliche Standards schafft.

Doch wie sieht die **Realität in Unternehmen** aus? Wie schnell reagieren sie auf Sicherheitsvorfälle? Wie weit ist die Umsetzung der NIS-2-Richtlinie fortgeschritten? Und welche Rolle spielt KI in der Risikowahrnehmung? Die Ergebnisse zeigen ein **differenziertes Bild**: ermutigende Entwicklungen, aber auch einen klaren Handlungsbedarf.

Digitale Selbstverteidigung muss nicht kompliziert sein – und der Anfang nicht schwer. Als **Kompetenzzentrum für Cybersicherheit** in der Wirtschaft unterstützen wir insbesondere kleine und mittlere Unternehmen in Nordrhein-Westfalen mit unserem **kostenlosen Angebot** aus persönlicher Beratung und praxisnahem Wissen. Scheuen Sie sich nicht, uns anzusprechen!

Auch in diesem Jahr danken wir der **G DATA CyberDefense AG** für die Bereitstellung der Daten, auf denen diese Studie basiert. Und Ihnen, liebe Leserinnen und Leser, wünschen wir wertvolle Erkenntnisse und den Mut, sie umzusetzen.

Sebastian Barchnicki,
Sprecher der Geschäftsführung
DIGITAL.SICHER.NRW

Deutsche Unternehmen haben ihre IT-Sicherheit in den vergangenen Jahren **spürbar verbessert** – und das trotz Fachkräftemangels. Gleichzeitig nimmt mit der fortschreitenden Digitalisierung die Abhängigkeit von funktionierender und sicherer IT weiter zu. Wo mehr Prozesse digital stattfinden, wächst auch die **Verantwortung**, diese zuverlässig zu schützen.

Technologie allein reicht dafür jedoch nicht aus. Wir sehen immer deutlicher, dass **nachhaltige IT-Sicherheit** nur dort entsteht, wo technische Maßnahmen mit klaren Prozessen, Verantwortlichkeiten und einem geschärften Bewusstsein für Risiken im gesamten Unternehmen verbunden werden. IT-Sicherheit ist kein abgeschlossenes Projekt, sondern eine **dauerhafte Aufgabe**.

Aus meiner Sicht ist es deshalb entscheidend, IT-Sicherheit **strategisch** im Unternehmen zu verankern und als gemeinsame Verantwortung zu verstehen. Wenn Technologie, Organisation und Sicherheitsbewusstsein zusammenwirken, entsteht eine **resiliente digitale Infrastruktur**.

Die vorliegende Studie haben wir gemeinsam mit **Statista** und **brand eins** erhoben. Auch in diesem Jahr stellen wir **DIGITAL.SICHER.NRW** die Ergebnisse für Nordrhein-Westfalen bereit, um einen Einblick in den Stand der IT-Sicherheit des Mittelstands zu geben.

Ich wünsche Ihnen eine aufschlussreiche Lektüre.

Andreas Lüning,
Vorstand und Mitgründer
der G DATA CyberDefense AG

DIGITAL SICHER NRW

DIE WICHTIGSTEN PUNKTE IM ÜBERBLICK

Die vorliegende **repräsentative Studie** zeigt, wie Führungskräfte und Mitarbeitende in NRW ihre Fähigkeiten, ihr Verhalten und die Risiken beim Thema **Cybersicherheit** einschätzen.

Nur eines von zehn betroffenen Unternehmen in NRW hat die **NIS-2-Richtlinie** vollständig umgesetzt, obwohl diese seit Dezember 2025 in Kraft ist.

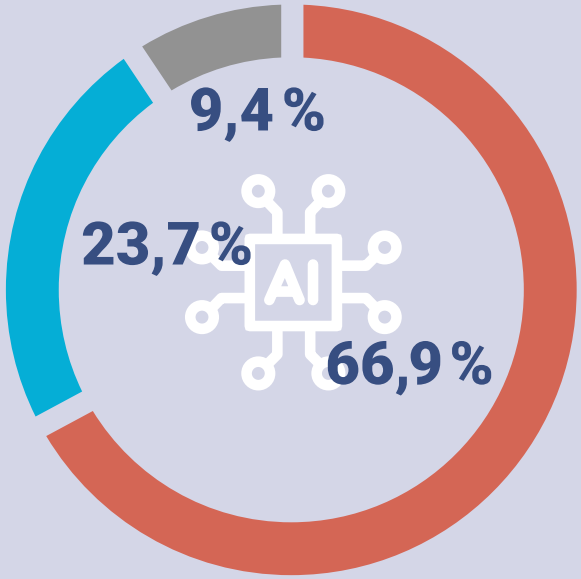
Künstliche Intelligenz verändert nicht nur Geschäftsprozesse, sondern auch die Bedrohungslage: Zwei Drittel der Unternehmen in NRW sehen KI als **wachsendes Sicherheitsrisiko**.

Bei **Cyberangriffen** zählt jede Minute – und wenn es darauf ankommt, **handeln Unternehmen in NRW schnell**: Im Bundesvergleich dämmen sie IT-Sicherheitsvorfälle am zügigsten ein.

Alle dargestellten Ergebnisse beziehen sich auf **Unternehmen in NRW**, sofern nicht explizit anders ausgewiesen. Als **kleine und mittlere Unternehmen (KMU)** gelten dabei Betriebe mit bis zu 249 Beschäftigten, als Großunternehmen solche mit 250 oder mehr.

KÜNSTLICHE INTELLIGENZ

Zwei Drittel der Unternehmen erwarten, dass **Cyberbedrohungen** durch den Einsatz von Künstlicher Intelligenz **zunehmen**.



Erwarten Sie, dass Bedrohungen für die IT-Sicherheit durch den verstärkten Einsatz von Künstlicher Intelligenz (KI) zunehmen?

- Ja, deutlich oder nur in bestimmten Bereichen
- Nein, das Risiko bleibt in etwa gleich oder nimmt ab
- Kann ich nicht beurteilen

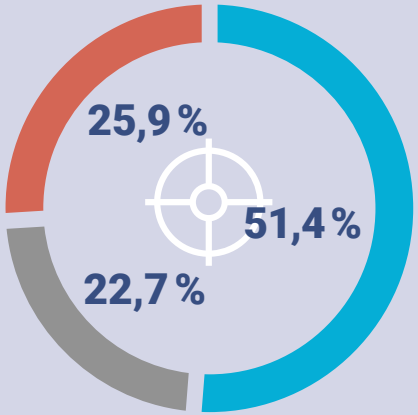
Mit dem zunehmenden Einsatz von KI wachsen auch die Möglichkeiten für **Cyberangriffe**. Betrügerische E-Mails (Phishing), manipulierte Videoaufnahmen (Deep Fakes) oder gefälschte Stimmen (Voice Cloning) lassen sich mithilfe von KI leichter umsetzen und sind schwerer zu durchschauen.

Risiken entstehen jedoch nicht nur durch gezielte Angriffe: **Falsch eingerichtete KI-Systeme** sowie die **(unautorisierte) Nutzung von KI-Tools** können dazu führen, dass sensible Informationen unkontrolliert nach außen gelangen.

BERUFLICHE RISIKOEINSCHÄTZUNG

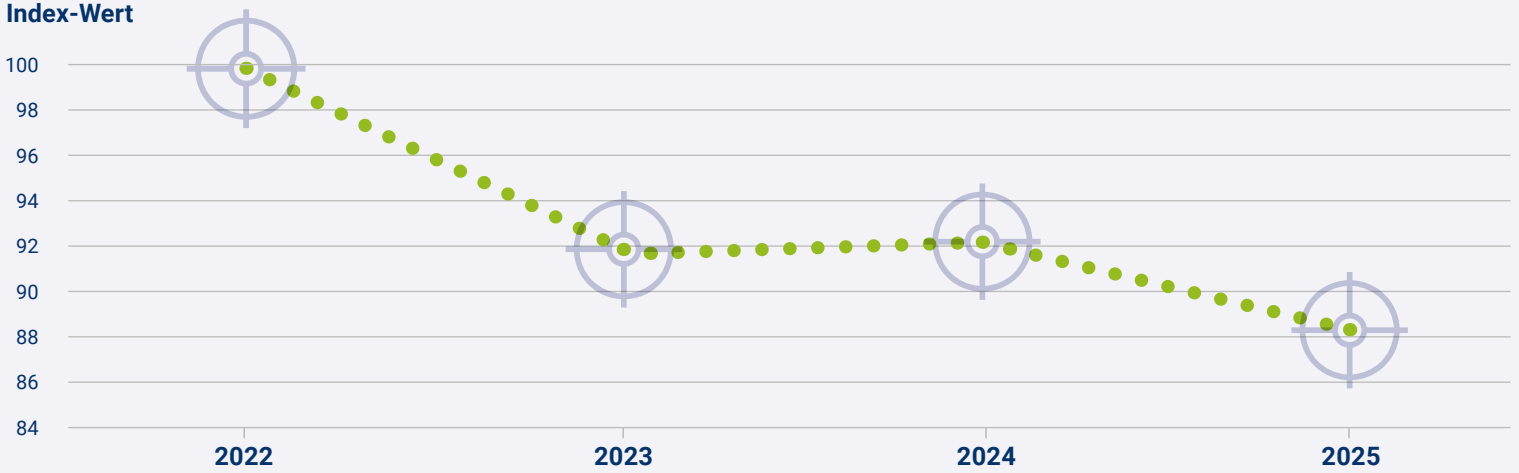
Rund die Hälfte der Unternehmen schätzt das Risiko, von Cyberkriminalität betroffen zu sein, als **(sehr) gering** ein.

Dieser Anteil ist in den letzten Jahren sogar gestiegen.



Wie hoch schätzen Sie das Risiko im beruflichen Umfeld ein, dass Sie Opfer von Cyberkriminalität oder Datenklau werden?

(sehr) gering | (sehr) hoch | weder noch



(n im Jahr 2022 = **1120**; in 2023 = **1101**; in 2024 = **1128**; in 2025 = **1133**)

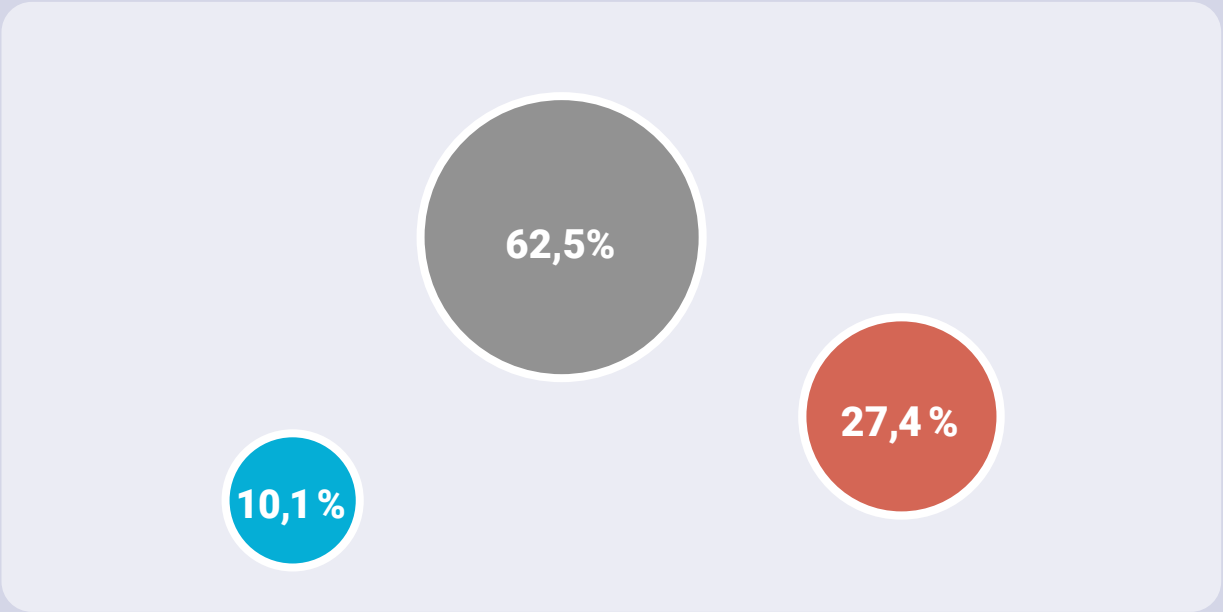
DIGITAL SICHER NRW

UMSETZUNG DER NIS-2-RICHTLINIE

Eines von zehn Unternehmen, die von NIS-2 betroffen sind, hat die Richtlinie **vollständig umgesetzt**.

Um die 30 Prozent haben noch **gar keine Maßnahmen** ergriffen.

Wie weit ist Ihr Unternehmen mit der Umsetzung der Anforderungen der NIS2-Richtlinie?
(n = **160**)



Filter: Befragte, die IT-Admin in der IT-Security oder IT/EDV sind oder die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT/EDV arbeiten oder Geschäftsführung/Vorstand sind

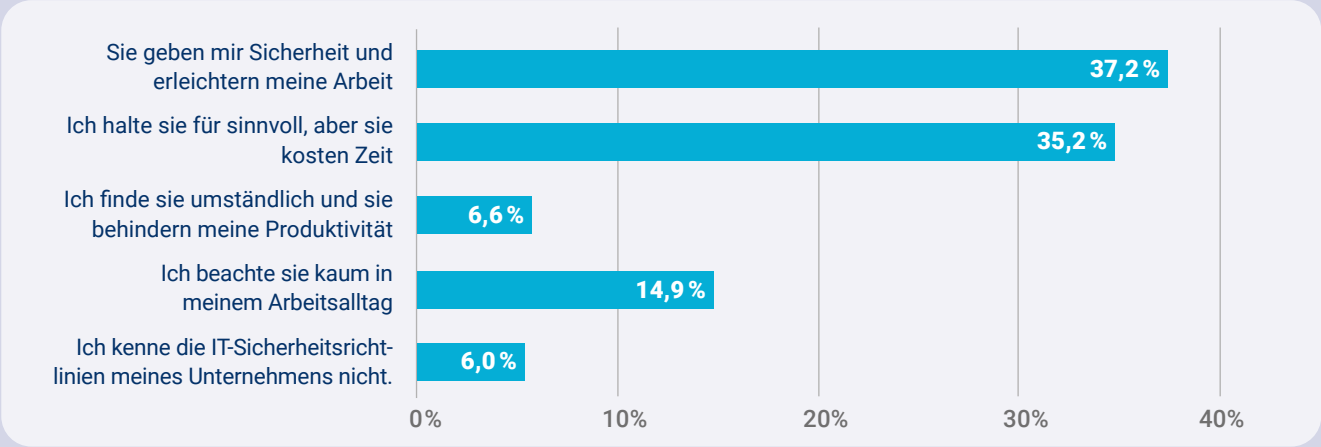
Die NIS-2-Richtlinie verpflichtet Unternehmen u.a. dazu, ihre **Sicherheitsstandards zu verbessern**, **Mitarbeitende zu schulen** und **Cybervorfälle zu melden**.

DIGITAL SICHER NRW

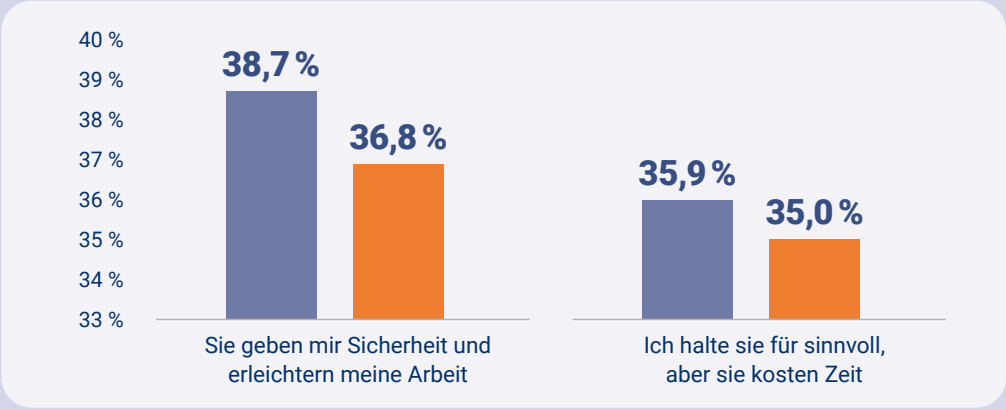
IT-SICHERHEITSRICHTLINIEN IM UNTERNEHMEN

Mitarbeitende bewerten IT-Sicherheitsrichtlinien **überwiegend positiv**: Sie vermitteln ihnen ein Gefühl von Sicherheit, werden als sinnvoll erachtet und erleichtern nach eigener Einschätzung die tägliche Arbeit – trotz des damit verbundenen Zeitaufwands.

Inwiefern beeinflussen IT-Sicherheitsrichtlinien Ihre tägliche Arbeit?

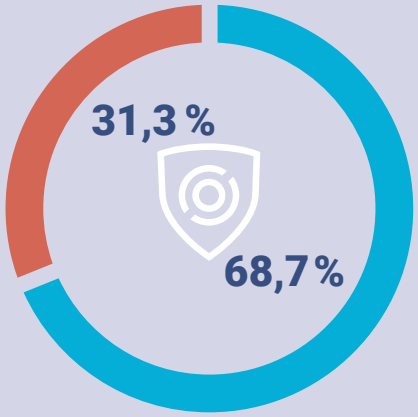


Diese positive Wahrnehmung ist in **KMU** noch etwas **stärker** als in Großunternehmen.



VERANTWORTUNG

Ein Großteil der Angestellten fühlt sich **persönlich** für die IT-Sicherheit im eigenen Unternehmen **verantwortlich**.

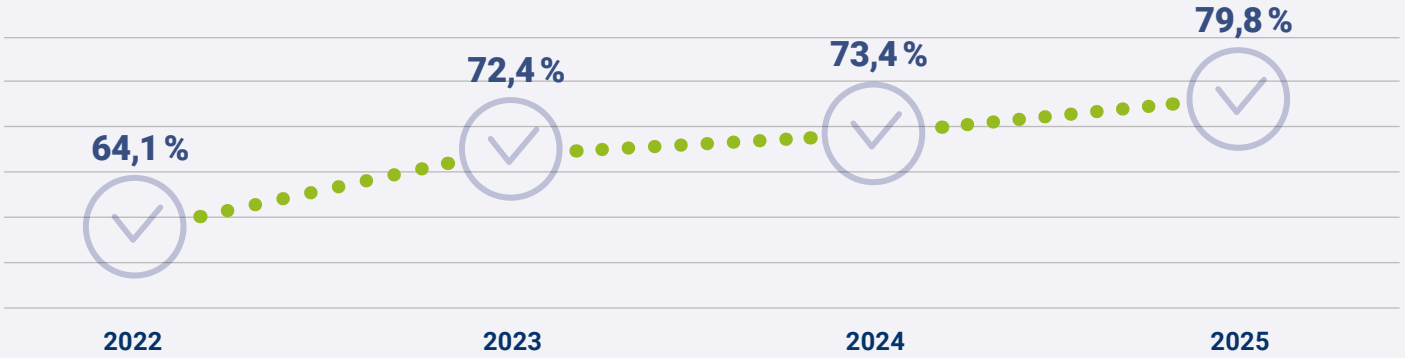


Wie stark fühlen Sie sich persönlich verantwortlich für die IT-Sicherheit in Ihrem Unternehmen?

- sehr / eher stark / teils, teils
- eher gering / gar nicht

KOMPETENZEINSCHÄTZUNG

Beim Thema IT-Sicherheit fühlen sich Angestellte **kompetenter** denn je.

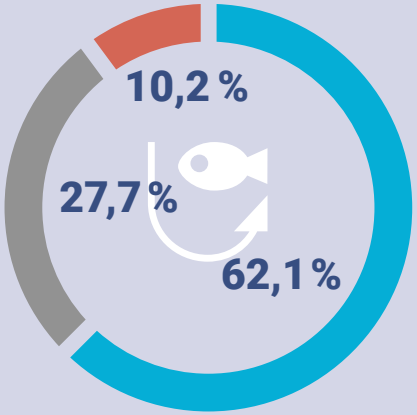


Wie schätzen Sie Ihre persönliche Kompetenz beim Thema IT-Sicherheit ein?

(n im Jahr 2022 = **1120**; in 2023 = **1101**; in 2024 = **1128**; in 2025 = **1133**)
Filter: Antwortoptionen „mittlere“ bis „sehr große Kompetenz“

PHISHING-E-MAILS

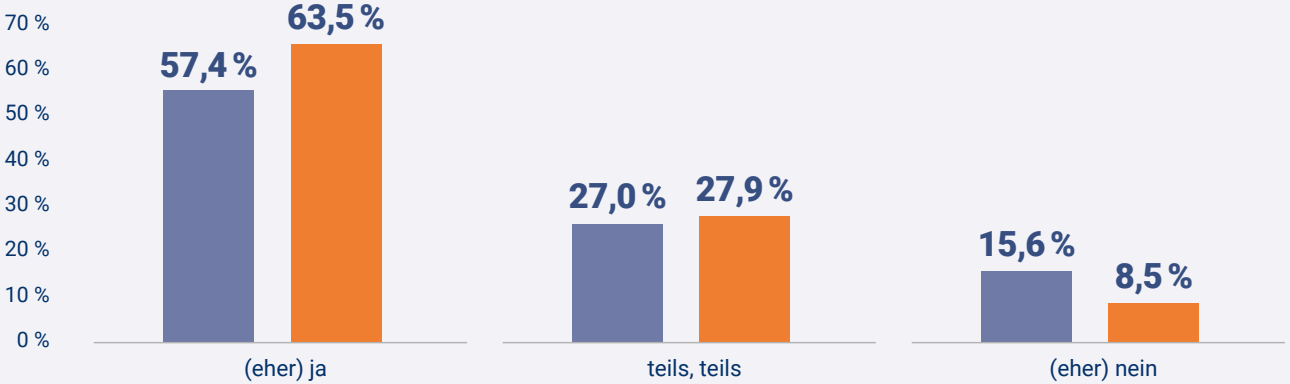
Die Mehrheit der Angestellten ist überzeugt, betrügerische E-Mails zu **erkennen**.



Glauben Sie, dass Sie betrügerische oder gefährliche E-Mails selbst erkennen können?

(eher) ja | teils, teils | (eher) nein

In **KMU** ist dieses Vertrauen in die eigenen Fähigkeiten jedoch **geringer ausgeprägt** als in Großunternehmen.

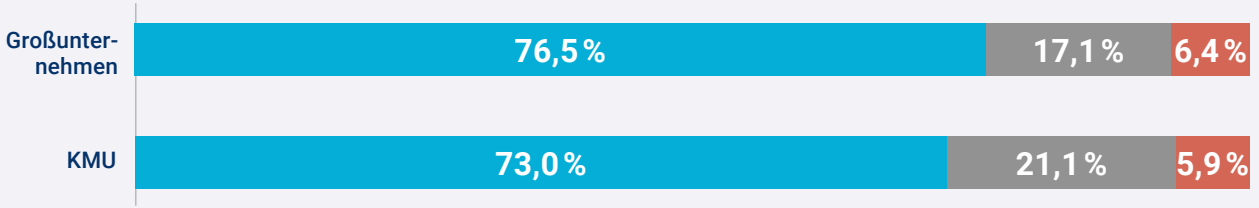


KMU | Großunternehmen

(n = 256 / 877)

SICHERHEITSKULTUR

Großunternehmen stufen ihre Sicherheitskultur als **stärker ausgeprägt** ein als KMU.

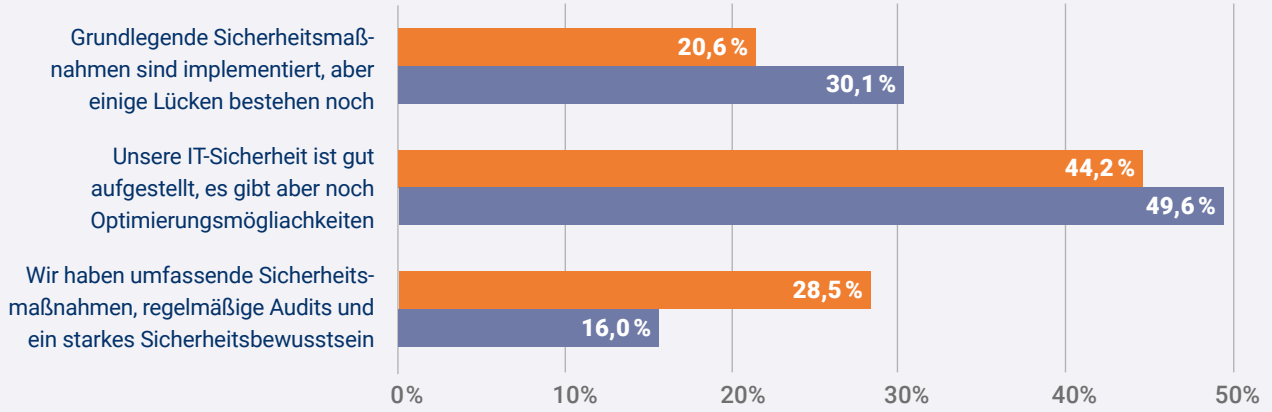


Wie würden Sie die Sicherheits-kultur in Ihrem Unternehmen einschätzen?
(n = 256 / 877)

- sehr ausgeprägt / gut entwickelt
- mittel
- eher schwach / nicht vorhanden

REIFEGRAD DER IT-SICHERHEIT

KMU bewerten ihre IT-Sicherheit als **weniger ausgereift** als Großunternehmen.

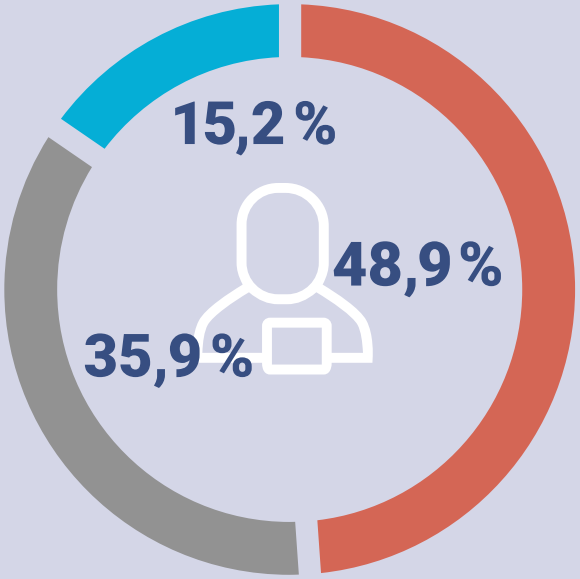


Wie schätzen Sie den Reifegrad der IT-Sicherheit in Ihrem Unter-nehmen ein?
(n = 256 / 877)

- Großunternehmen
- KMU

FACHKRÄFTEMANGEL

Knapp die Hälfte der Unternehmen schätzt den Fachkräftemangel im Bereich IT-Sicherheit als **(sehr) hoch** ein.



Wie schätzen Sie den Fachkräftemangel im Bereich IT-Sicherheit in Ihrem Unternehmen ein?
(n = **131**)

- (sehr) hoch
- durchschnittlich
- (sehr) niedrig

Filter: Befragte, die IT-Admin in der IT-Security oder IT/EDV sind oder die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT/EDV arbeiten

In die IT-Sicherheit führen viele Wege: über ein Studium, eine Ausbildung zur Fachinformatikerin oder zum Fachinformatiker mit anschließender Spezialisierung oder anerkannte Zertifizierungen wie den BSI-Grundschutz-Praktiker.

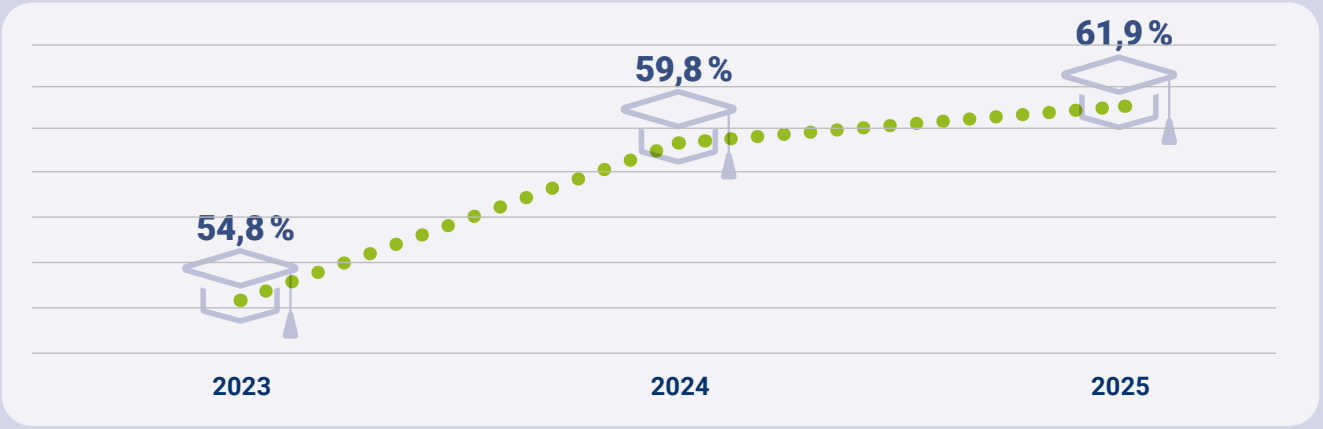
Da ein eigener **Ausbildungsberuf für IT-Sicherheit** bislang fehlt, setzt sich DIGITAL.SICHER.NRW gemeinsam mit dem eurobits e.V. und dem CISO Alliance e.V. für die Etablierung des Lehrberufs mit dieser Fachrichtung ein.

SCHULUNGEN

Unternehmen haben ihr Schulungsangebot in den **vergangenen Jahren ausgebaut**.

Bietet Ihr Unternehmen für alle Mitarbeiterinnen und Mitarbeiter (Online-) Schulungen/Veranstaltungen/Trainings rund um das Thema Cybersicherheit an?
(n im Jahr 2022 = **1120**; in 2023 = **1101**; in 2024 = **1128**; in 2025 = **1133**)

Filter: Antwortoptionen „Ja, regelmäßig“ und „Ja, aber eher unregelmäßig“

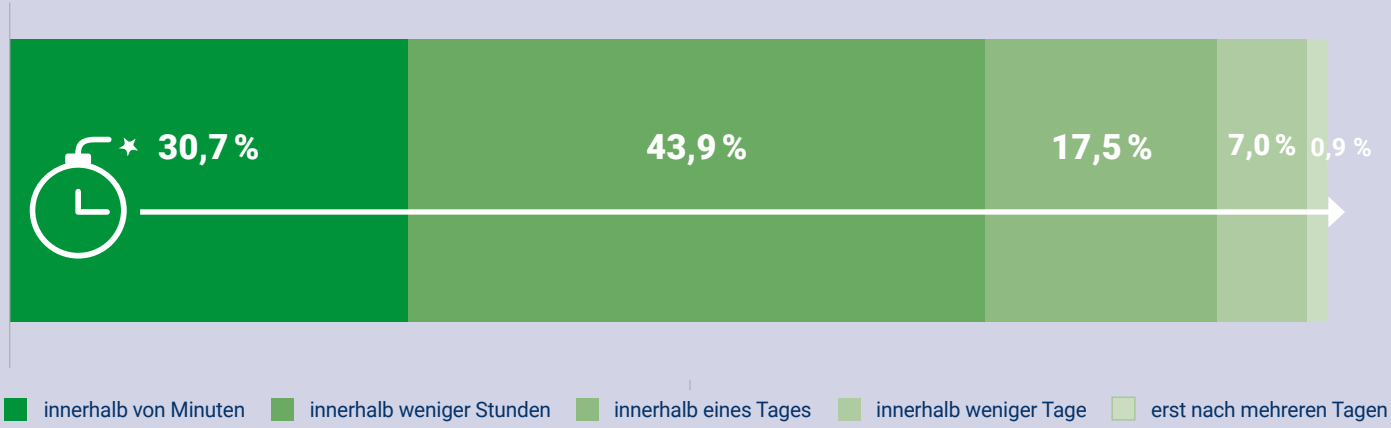


REAKTIONSZEIT

Bei IT-Sicherheitsvorfällen reagieren die meisten Unternehmen **spätestens innerhalb weniger Stunden**.

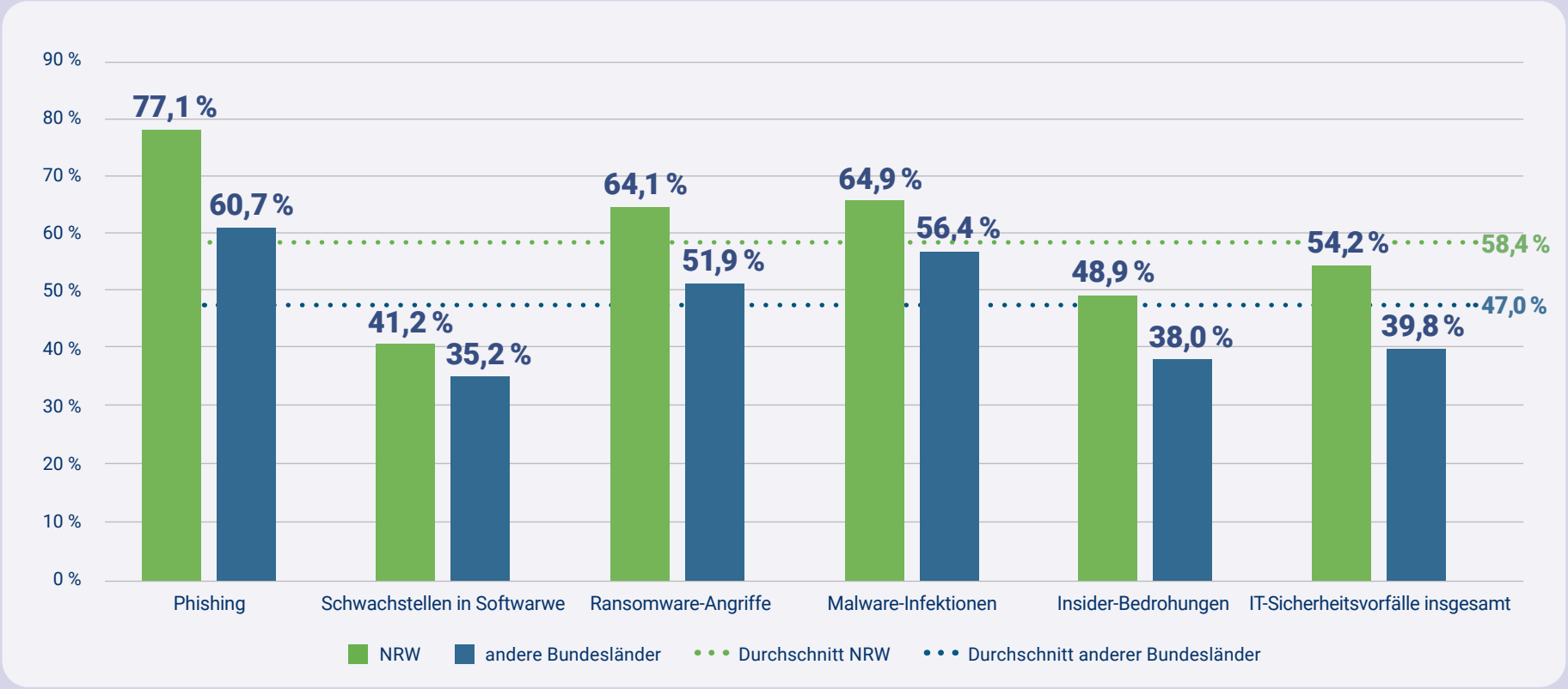
Wie schnell reagiert Ihr Unternehmen in der Regel auf einen IT-Sicherheitsvorfall?
(n = **114**)

Filter: Befragte, die IT-Admin in der IT-Security oder IT/EDV sind oder die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT/EDV arbeiten



EINDÄMMUNGSZEIT

Bei der Eindämmung von IT-Sicherheitsvorfällen liegen **NRW-Unternehmen im Bundesvergleich vorn** – den meisten gelingt sie innerhalb einer Woche.



Filter: Befragte, die IT-Admin in der IT-Security oder IT/EDV sind oder die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT/EDV arbeiten

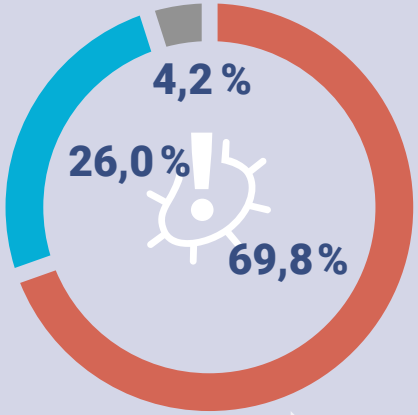
Filter 2: Antwortoption „bis zu einer Woche“

Wie lange dauert es Ihrer Einschätzung nach, bis ein IT-Sicherheitsvorfall entdeckt und eingedämmt wird?
(n = **131** / **356**)

ANGRIFFSAUSWIRKUNGEN

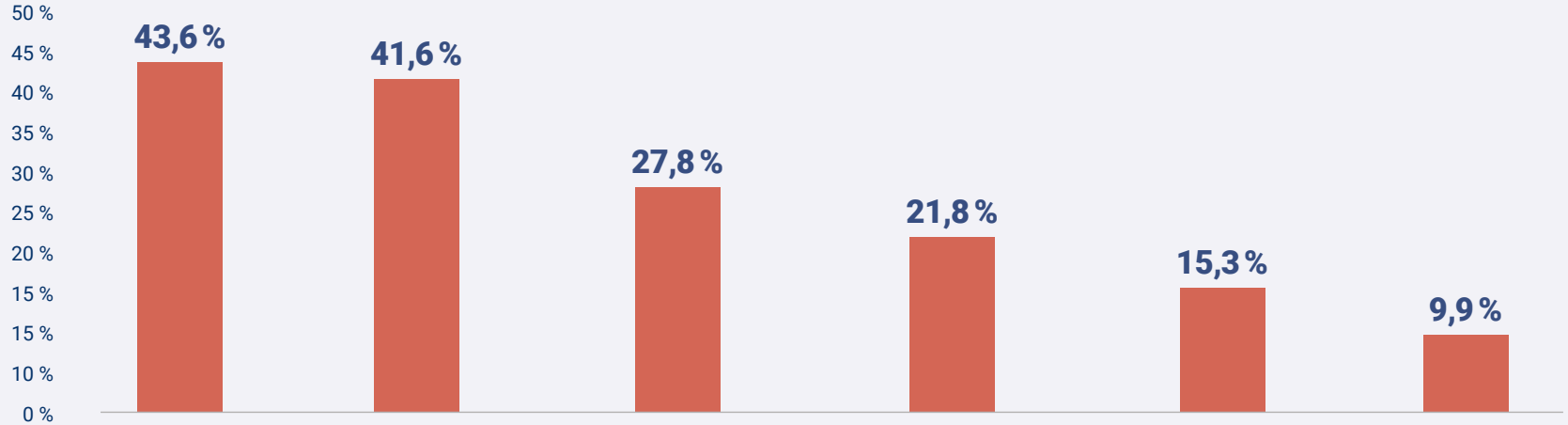
Fast drei Viertel der Befragten haben Auswirkungen eines Cyberangriffs wahrgenommen, darunter vor allem **Betriebsausfälle, Datenverluste** und **finanzielle Schäden**.

Filter: Befragte, die im letzten Jahr einen oder mehrere IT-Sicherheitsvorfälle oder Angriffe erlebt haben



Welche Folgen hatte der IT-Sicherheitsvorfall oder Angriff?
Mehrfachnennung möglich / * Exklusivoption
(n = **335**)

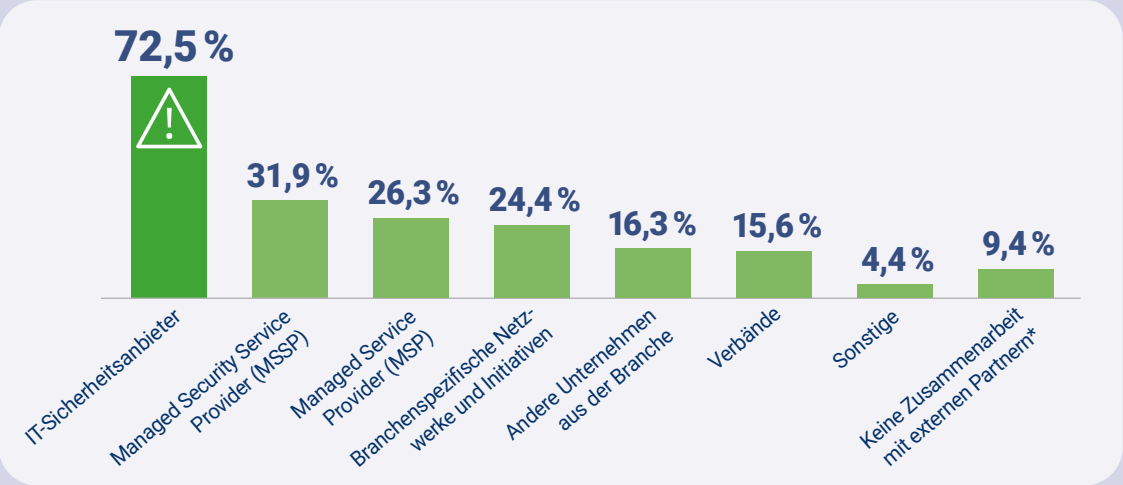
- Auswirkungen mitbekommen
- Keine spürbaren Auswirkungen*
- Weiß ich nicht*



(n = **234**) / Filter 2: Befragte, die Auswirkungen mitbekommen haben

ZUSAMMENARBEIT MIT IT-SICHERHEITSUNTERNEHMEN

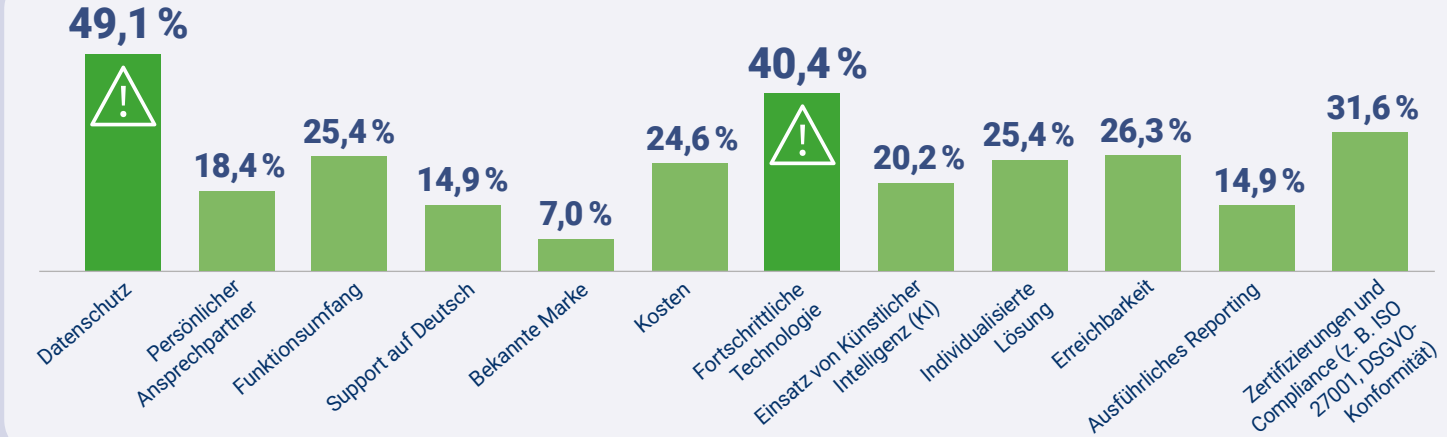
Etwa drei Viertel der Unternehmen arbeiten mit IT-Sicherheitsunternehmen zusammen. Bei der Auswahl ist der **Datenschutz** das wichtigste Kriterium, gefolgt von fortschrittlicher Technologie.



Mit welchen externen Partnern arbeitet Ihr Unternehmen im Bereich IT-Sicherheit zusammen?
Mehrfachnennung möglich / * Exklusivoption
(n = **160**)

Filter: Befragte, die IT-Admin in der IT-Security oder IT/EDV sind oder die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT/EDV arbeiten oder Geschäftsführung/Vorstand sind

Welche Kriterien sind Ihnen bei der Zusammenarbeit mit einem IT-Security-Dienstleister am wichtigsten (Top 3)?
(n = **114**)



Filter: Befragte, die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT/EDV arbeiten

DIGITAL SICHER NRW

Kompetenzzentrum für Cybersicherheit in der Wirtschaft

Zu Inhalt und Methodik:

Die vorliegenden Erkenntnisse basieren auf der Studie „**Cybersicherheit in Zahlen – Lernen. Wissen. Handeln.**“, die im Frühjahr 2025 durchgeführt wurde. An der Online-Umfrage nahmen insgesamt 5.000 Arbeitnehmerinnen und Arbeitnehmer in Deutschland teil, um Angaben zu ihren Erfahrungen, Einstellungen und ihrem Verhalten zum Thema Cybersicherheit zu machen. Es handelt sich um eine repräsentative Umfrage der deutschen Bevölkerung hinsichtlich der Merkmale Geschlecht, Alter, Region und Größe des Unternehmens. Die Stichprobengröße für NRW betrug 1.133 Personen.

Herausgeber:

CYBERSEC-NRW gGmbH (DIGITAL.SICHER.NRW)
Lise-Meitner-Allee 4
44801 Bochum
www.digital-sicher.nrw

G DATA CyberDefense AG
G DATA Campus
Königsallee 178 a
44799 Bochum
www.gdata.de

Verantwortlich:

Sebastian Barchnicki
barchnicki@digital-sicher.nrw

Vera Haake
vera.haake@gdata.de

Stefan Karpenstein
stefan.karpenstein@gdata.de

Redaktion:

Laura Schoner
schoner@digital-sicher.nrw

Alexander Wunderlich
wunderlich@digital-sicher.nrw

Lena Nienstedt
nienstedt@digital-sicher.nrw

In Zusammenarbeit mit

G DATA CyberDefense

statista

brand eins