



**DIGITAL
SICHER
NRW**

Kompetenzzentrum für
Cybersicherheit in der Wirtschaft

CYBERSICHERHEIT IN NRW 2025

Studie zur IT-Sicherheit in Unternehmen



In Zusammenarbeit mit



statista 

brand eins



GRUSSWORTE DER HERAUSGEBER

Digitale Sicherheit betrifft **jedes Unternehmen**. Um Cyberangriffen bestmöglich zu begegnen, helfen klare Leitplanken und Orientierung. Mit Vorgaben wie denen aus der **NIS-2-Richtlinie** wird deutlich: Die **Anforderungen an die IT-Sicherheit steigen**. Unternehmen stehen somit mehr denn je vor der Aufgabe, ihre Schutzmaßnahmen regelmäßig zu überprüfen und weiterzuentwickeln.

Die Ergebnisse der aktuellen Studie zeigen, wie unterschiedlich Unternehmen in NRW die derzeitige Lage im Hinblick auf Cybersicherheit wahrnehmen. Besonders ins Auge fällt die Diskrepanz zwischen der **objektiven Bedrohungslage** und der **subjektiven Risikoeinschätzung**. Das birgt die Gefahr, dass notwendige Sicherheitsmaßnahmen nicht die nötige Priorität erhalten.

Deshalb mein Appell: Bleiben Sie aufmerksam, handeln Sie vorbeugend und schaffen Sie in Ihrem Team ein Bewusstsein für digitale Sicherheit. Wer vorbereitet ist, kann Risiken entschärfen und Chancen nutzen. Unser **Kompetenzzentrum für Cybersicherheit** hilft Ihnen gern dabei!

Danke an alle, die an der Umfrage teilgenommen haben, an die **G DATA CyberDefense** für die erneute Bereitstellung der Daten und an alle Leserinnen und Leser, die sich mit den Ergebnissen befassen.



Sebastian Barchnicki,
Sprecher der Geschäftsführung
DIGITAL.SICHER.NRW

Ein Ende des **IT-Fachkräftemangels** ist leider nicht in Sicht, wie der Branchenverband Bitkom vor Kurzem errechnet hat. Bis zum Jahr 2040 werden mehr als **660.000 Stellen** unbesetzt sein. Dies hat unmittelbare Folgen, die auch die IT-Sicherheit von kleinen und mittelständischen Unternehmen betreffen.

Wie also können mittelständische Firmen ihre Netzwerke und Infrastruktur wirksam schützen, wenn sie im Kampf um Fachkräfte das Nachsehen haben? Wichtig ist, dass Unternehmen lernen, mit einem Notfall umzugehen. Auf dem Weg zu mehr Resilienz braucht es **Managed-Security-Lösungen** wie etwa **MXDR** (Managed Extended Detection and Response). Qualifizierte IT-Sicherheitsdienstleister verfügen über das Personal und die Expertise, um Firmen bei Notfallübungen oder dem Aufbau von **Security Awareness** zu unterstützen. Denn es geht nicht mehr nur um das Verhindern von Cyberangriffen, sondern um das **frühzeitige Erkennen und Handeln**.

Die vorliegenden Zahlen stammen aus einer repräsentativen Umfrage, die wir gemeinsam mit **Statista** und **brand eins** durchgeführt haben. Auch in diesem Jahr haben wir **DIGITAL.SICHER.NRW** die Ergebnisse für Nordrhein-Westfalen bereitgestellt, um zu zeigen, wie es um die IT-Sicherheit des Mittelstands in NRW bestellt ist.

Ich wünsche Ihnen eine aufschlussreiche Lektüre und hoffe, dass Sie die richtigen Schlüsse daraus ziehen.



Andreas Lüning,
Vorstand und Mitgründer
der G DATA CyberDefense AG

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.
-  Die Mehrheit der Unternehmen weiß nicht, ob sie von der **NIS-2-Richtlinie** betroffen ist.
-  Beschäftigte öffnen aus Neugier die Tür zu möglichen Sicherheitsrisiken: Auf potenzielles **Phishing** fallen sie am häufigsten herein.
-  Der Großteil der Angestellten traut ihrer **IT-Abteilung** zu, den aktuellen Anforderungen der IT-Sicherheit gewachsen zu sein. Das **Schutzgefühl** am Arbeitsplatz erreicht einen neuen Höchststand.
-  Trügerisch: **Kleine und mittlere Unternehmen* in Deutschland halten sich selbst für ein weniger attraktives Ziel** von Cyberangriffen als Großunternehmen – obwohl kein Betrieb zu klein oder zu unbedeutend ist, um angegriffen zu werden.



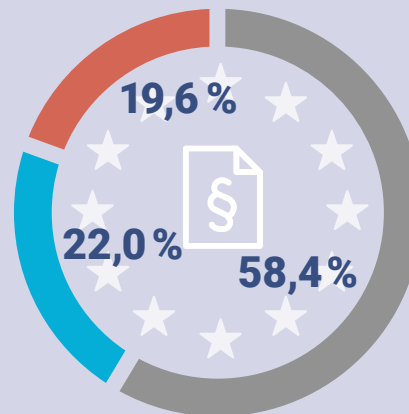
* **Kleine und mittlere Unternehmen (KMU)** sind Unternehmen mit weniger als 250 Beschäftigten. Großunternehmen sind Unternehmen mit mehr als 250 Beschäftigten.



EINSCHÄTZUNG ZUR BETROFFENHEIT VON DER NIS-2-RICHTLINIE

Die **NIS-2-Richtlinie** legt europaweit fest, welche Maßnahmen und Pflichten Unternehmen für ihre digitale Sicherheit erfüllen müssen.

Drei von fünf Unternehmen wissen jedoch nicht, ob sie davon betroffen sind.



Ist Ihr Unternehmen von der NIS-2-Richtlinie betroffen?

ja nein ich weiß es nicht



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

NIS-2-ANLAUFSTELLE FÜR KLEINE UND MITTLERE UNTERNEHMEN

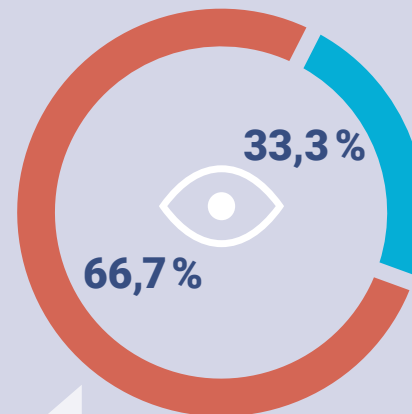


Der **eurobits e.V.** betreibt eine vom Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen geförderte Anlaufstelle, um KMU zum Thema NIS-2 vorzubereiten.

Unternehmen mit 50 bis 250 Mitarbeitenden erhalten eine **kostenlose Erstanalyse sowie Beratung**, bei der sie mit qualifizierten Expertinnen und Experten einen individuellen Maßnahmenplan erstellen.

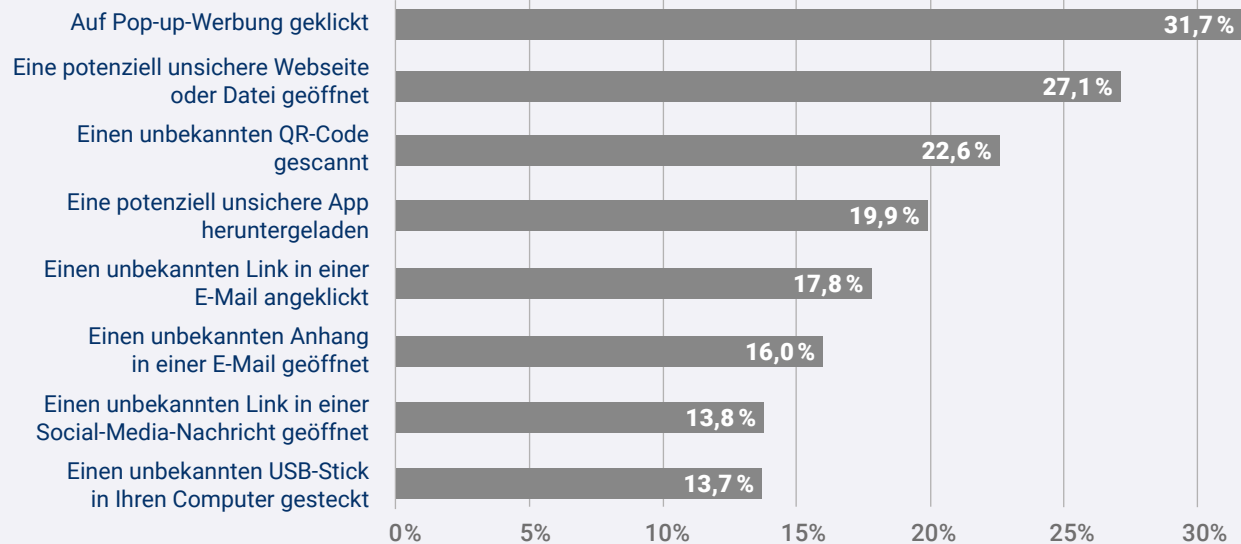
HANDLUNGEN ALS SICHERHEITSRISIKEN

Zwei Drittel der Befragten gehen aus Neugier mögliche **Sicherheitsrisiken** ein. Besonders anfällig sind sie für potenzielle **Phishing-Versuche**.



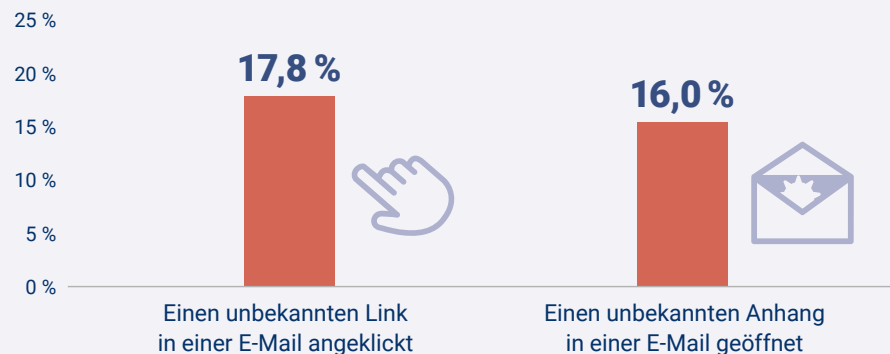
Haben Sie schon mal aus Neugierde folgende Dinge gemacht?
Mehrfachnennung möglich.

■ Neugierde ■ Keine der genannten *



E-MAIL-SICHERHEIT

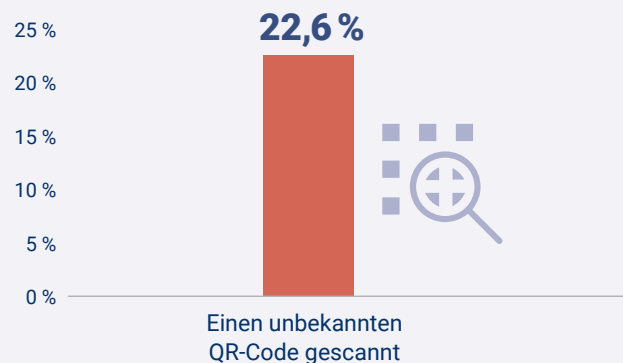
Sowohl **unbekannte Links** als auch **Anhänge** wurden in E-Mails geöffnet.



Haben Sie schon mal aus Neugierde folgende Dinge gemacht?
Mehrfachnennung möglich.

QR-CODES

Fast ein Viertel hat bereits einmal einen **unbekannten QR-Code** gescannt.



Haben Sie schon mal aus Neugierde folgende Dinge gemacht?
Mehrfachnennung möglich.



Ein unbekannter QR-Code kann auf eine **manipulierte Webseite** führen, die schädliche Dateien auf dem Gerät installiert oder eingegebene Daten abfängt.

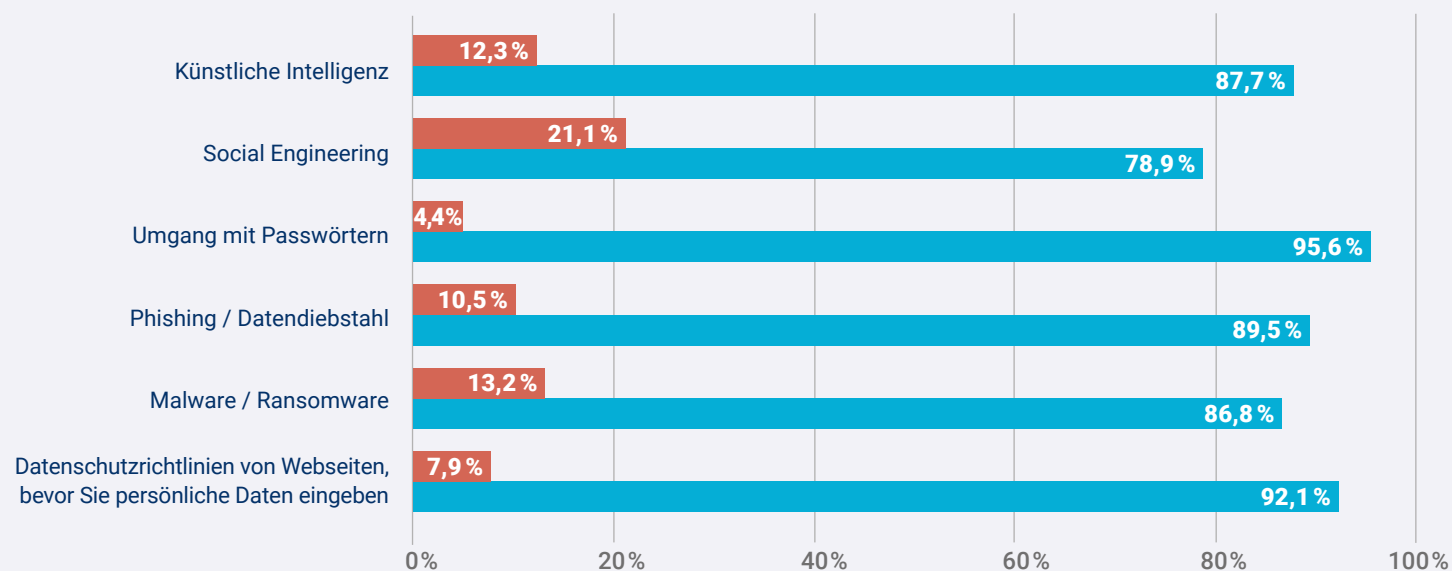
IT-SICHERHEITSTHEMEN

Im Schnitt informieren sich **fast 90 Prozent** der kleinen und mittleren Unternehmen in NRW zu Themen der IT-Sicherheit.



Wie oft informieren Sie sich über folgende Themen?
(n = 228)

Nie
Manchmal bis oft



Um das Bewusstsein für digitale Sicherheit zu stärken, bieten Aktionen wie [„Tür zu im Netz“](#) gezielt Informationen und praktische Hilfestellungen für Unternehmen.

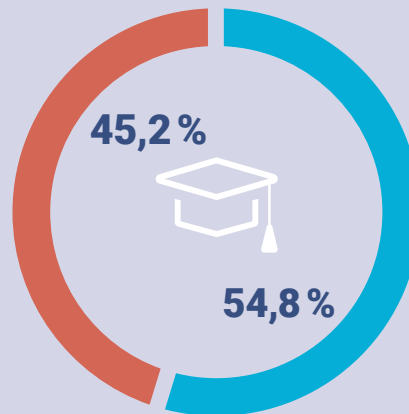
SCHULUNGSANGEBOTE

Im Vergleich zum Vorjahr bieten **mehr Unternehmen** Schulungen für Mitarbeiterinnen und Mitarbeiter an.

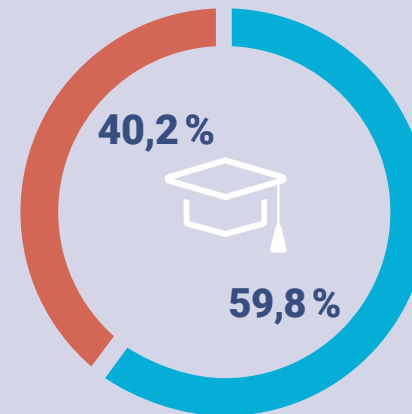
?

Bietet Ihr Unternehmen für alle Mitarbeiterinnen und Mitarbeiter (Online-)Schulungen/Veranstaltungen/Trainings rund um das Thema Cybersicherheit an?
(2023: n = 1101)

- Ja, für alle Mitarbeitende
- Nein, nicht für alle Mitarbeitende / noch nie von Schulungen etc. gehört



2023



2024

PERSÖNLICHE KOMPETENZ

Nur ein **Viertel** der Befragten aus NRW schätzt die eigene Kompetenz beim Thema IT-Sicherheit als **(sehr) gering** ein.

?

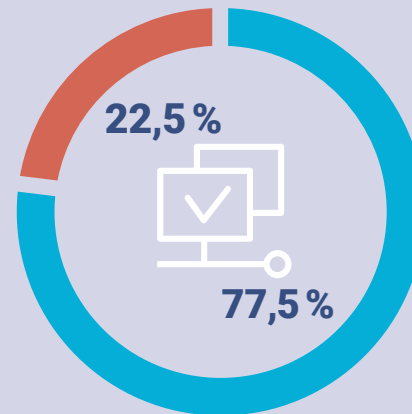
Wie schätzen Sie Ihre persönliche Kompetenz beim Thema IT-Sicherheit ein?



- (Sehr) geringe Kompetenz
- Mittlere bis sehr große Kompetenz

KOMPETENZ DER IT-ABTEILUNG

Mehr als drei Viertel der Angestellten halten ihre IT-Abteilung für **gut aufgestellt** in Sachen IT-Sicherheit.



?

Sind Sie der Ansicht, dass Ihre IT-Abteilung den aktuellen Anforderungen an eine effektive IT-Sicherheit gewachsen ist?

■ Ja ■ Nein

BERUFLICHES SCHUTZGEFÜHL

Nie zuvor fühlten sich Beschäftigte in NRW am Arbeitsplatz **so gut geschützt** wie jetzt.



?

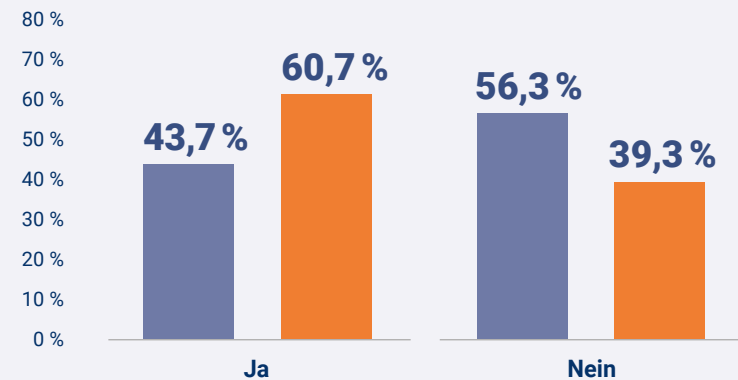
Wie gut fühlen Sie sich durch die angewendeten Sicherheits- und Schutzmaßnahmen in Ihrem beruflichen Umfeld geschützt?
(2021: n = 1102; 2022: n = 1120; 2023: n = 1101) Darstellung der Antwortoptionen: (sehr) gut

ANGRIFFSZIEL

Kleine und mittlere Unternehmen in Deutschland halten sich selbst für ein **weniger attraktives Ziel** von Cyberangriffen als Großunternehmen.



Alle Unternehmen – unabhängig von Größe, Alter oder Bekanntheit – sind von Cyberangriffen **betroffen**, da Angreifende oft breitflächig und automatisiert vorgehen.

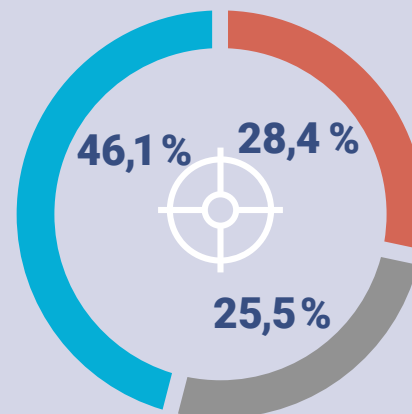


Ist Ihr Unternehmen aus Ihrer Sicht ein interessantes Angriffsziel für Cyberkriminelle?
(n = 1049, **3958**)

■ KMU ■ Großunternehmen

BERUFLICHE RISIKOEINSCHÄTZUNG

Das Risiko, selbst von Cyberkriminalität betroffen zu sein, schätzen Unternehmen in NRW am ehesten als **(sehr) gering** ein.



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

■ (Sehr) gering ■ (Sehr) hoch ■ Weder noch



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 2024 durchgeführt wurde. An der Online-Umfrage nahmen insgesamt 5.007 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 1.128 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



statista 

brandeins