# 2023 Cyber-Vorfälle in Zahlen

Berichtszeitraum: 01. Januar - 31. Dezember 2023

Datum des Berichts: 5. Februar 2024

SWISS IT SECURITY GROUP

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

# Im Fokus –
## AV-TEST Europe Cyber Incident Analysis für 2023.

Seit 2023 sammelt und analysiert unser Team Daten zu Cybervorfällen in ganz Europa, mit besonderem Schwerpunkt auf Deutschland. Der diesjährige Jahresrückblick beleuchtet die sich entwickelnde Landschaft der Cyber-Bedrohungen, wobei der Schwerpunkt auf Distributed Denial of Service (DDoS) und Ransomware-Angriffen liegt, da diese erhebliche Auswirkungen haben und sehr sichtbar sind. Diese Arten von Cyber-Vorfällen sind nicht nur häufiger, sondern auch raffinierter geworden, was die Cybersicherheitsabwehr vor große Herausforderungen stellt und ein tieferes Verständnis ihrer Mechanismen und Auswirkungen erfordert.
Die von AV-TEST gemeldeten Cyber-Vorfälle stammen aus Überwachungsaktivitäten in öffentlichen und Deep-Web-Quellen. Es ist wichtig zu beachten, dass diese Ergebnisse möglicherweise nicht die gesamte Landschaft der aufgetretenen Vorfälle repräsentieren.

### Europa

**Die 20 meist angegriffenen Länder im Jahr 2023.**

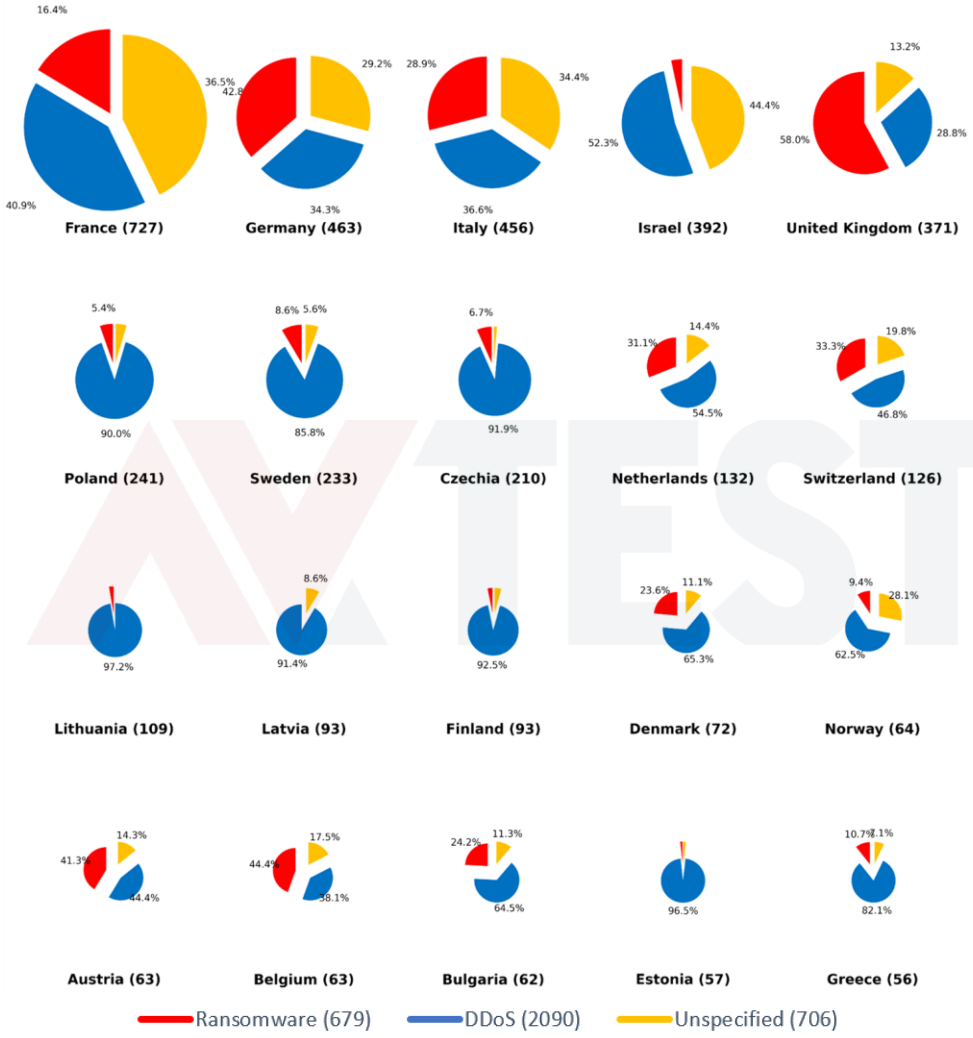


*Abbildung 1: veranschaulicht die Verteilung von Cyberangriffen auf die 20 am stärksten angegriffenen europäischen Länder im Jahr 2023, mit einer Aufschlüsselung der Angriffsarten - Ransomware, DDoS und nicht spezifizierte Angriffe - in Kreisdiagrammen für jedes Land. Die Gesamtzahl der Angriffe ist neben den Ländernamen angegeben.*

Im Jahr 2023 beobachtete AV-TEST insgesamt 4.618 Cyberangriffe in Europa, wobei Distributed Denial of Service (DDoS) und Ransomware den Großteil dieser bösartigen Aktivitäten ausmachten. Konkret gab es 2.525 DDoS-Vorfälle und 1.066 Ransomware-Angriffe sowie 1.027 nicht spezifizierte Ereignisse, die eine Reihe anderer bösartiger Aktivitäten wie Datendiebstahl für Hacktivismus oder Spionage umfassen. Diese Zahlen unterstreichen die anhaltende Bedrohung durch bekannte Angriffsvektoren sowie die Prävalenz von verdeckten Operationen.

| Land | Ransomware | DDoS | nicht spezifiziert | Gesamtzahl der Angriffe |
|---|---|---|---|---|
| Frankreich | 119 | 297 | 311 | 727 |
| Deutschland | 169 | 159 | 135 | 463 |
| Italien | 132 | 167 | 157 | 456 |
| Israel | 13 | 205 | 174 | 392 |
| Vereinigtes Königreich | 215 | 107 | 49 | 371 |
| Polen | 13 | 217 | 11 | 241 |
| Schweden | 20 | 200 | 13 | 233 |
| Tschechien | 14 | 193 | 3 | 210 |
| Niederlande | 41 | 72 | 19 | 132 |
| Schweiz | 42 | 59 | 25 | 126 |
| Litauen | 3 | 106 | 0 | 109 |
| Lettland | 0 | 85 | 8 | 93 |
| Finnland | 3 | 86 | 4 | 93 |
| Dänemark | 17 | 47 | 8 | 72 |
| Norwegen | 6 | 40 | 18 | 64 |
| Österreich | 26 | 28 | 9 | 63 |
| Belgien | 28 | 24 | 11 | 63 |
| Bulgarien | 15 | 40 | 7 | 62 |
| Estland | 1 | 55 | 1 | 57 |
| Griechenland | 6 | 46 | 4 | 56 |

*Tabelle 1: enthält eine tabellarische Zusammenfassung der Cyberangriffe in 20 europäischen Ländern für das Jahr 2023, aufgeschlüsselt nach Typ: Ransomware, DDoS, nicht spezifiziert, und die Gesamtzahl der Angriffe für jedes Land.*

## Untersuchung der Dynamik von Cyber-Bedrohungen:
DDoS, Ransomware und andere aufkommende Angriffe in der zweiten Hälfte des Jahres 2023*.

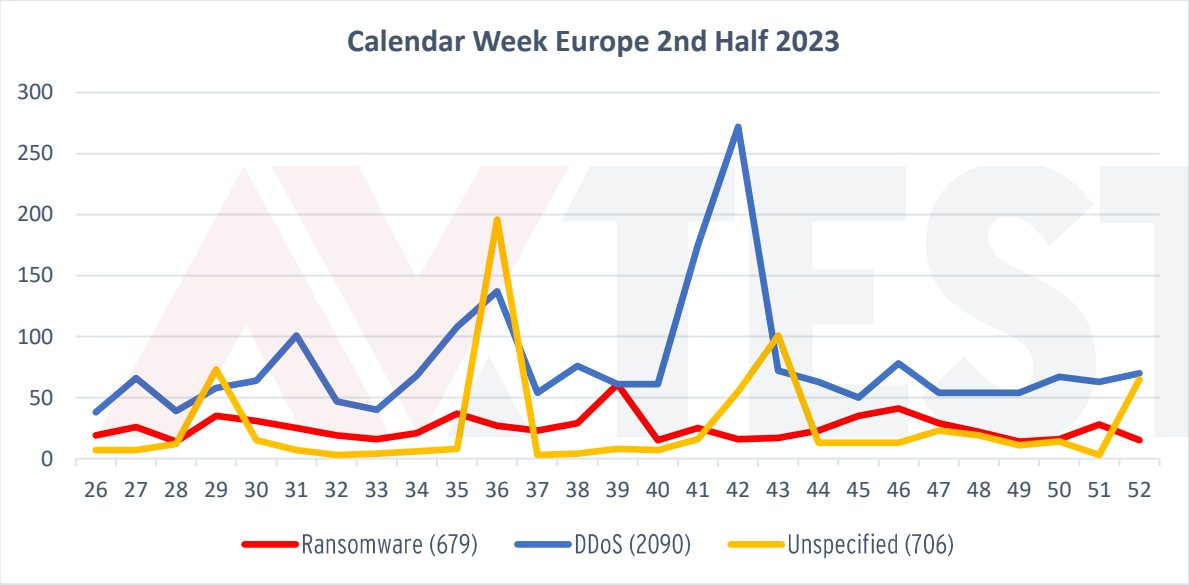


*Abbildung 2: zeigt ein Liniendiagramm, das die wöchentliche Häufigkeit von drei Arten von Cyber-Bedrohungen - DDoS, Ransomware und nicht spezifizierte Angriffe - in den europäischen Ländern in der zweiten Jahreshälfte 2023 darstellt. Jede Linie steht für eine Bedrohungsart, wobei die Legende die Gesamtzahl der Vorkommnisse für das Halbjahr angibt.*

Frankreich, Deutschland, Italien, Israel und das Vereinigte Königreich waren die Länder in Europa, die am meisten angegriffen wurden, mit 727, 463, 456, 392 und 371 Angriffen.
DDoS-Angriffe waren in den letzten sechs Monaten des Jahres die häufigste Form, was wahrscheinlich auf verstärkte Hacktivismus-Aktivitäten hinweist. Diese Vorfälle zeichnen sich durch ihre Schwankungen aus, wobei bemerkenswerte Spitzenwerte mit bestimmten Hacktivistenkampagnen zusammenfallen. Im Gegensatz dazu traten Ransomware-Angriffe ziemlich regelmäßig mit kurzen Ausbrüchen auf, was darauf hindeutet, dass Unternehmen während dieser Zeit immer noch bedroht waren.

Unspezifische Angriffe sind ebenfalls eine Konstante in der Landschaft, wenn auch im Allgemeinen weniger häufig als die anderen Arten. Es gibt jedoch Fälle von extremen Spitzen, die möglicherweise auf vielschichtige Kampagnen oder zu wenig gemeldete Vorfälle zurückzuführen sind, die erst nach eingehender Untersuchung ans Licht kamen.

Zwei bedeutende Ausbrüche sind hervorzuheben. In der Kalenderwoche 36 kam es in Frankreich zu einem konzertierten Angriff der Hacktivistengruppe "Mysterious Team Bangladesh", die behauptete, 188 Unternehmen angegriffen zu haben. Die Gruppe gab die angewandten Methoden nicht bekannt, so dass die Art dieser Vorfälle weitgehend unbekannt war. Der zweite bemerkenswerte Anstieg ereignete sich in Woche 42, in der Frankreich erneut in den Mittelpunkt der Angriffe rückte. Diesmal wurde die Aggression von "AnonGhost Indonesia" und "Anonymous Indonesia" angeführt, die sich zu DDoS-Angriffen gegen 173 französische Unternehmen bekannten.

*Die hier vorgestellten Daten beziehen sich nur auf die zweite Hälfte des Jahres 2023, da die Quellen und Methoden zur Erhebung von Informationen über Cybervorfälle erheblich geändert wurden. Diese Anpassungen haben zu Unstimmigkeiten in den historischen Daten geführt, was es schwierig macht, einen Trend über einen längeren Zeitraum genau darzustellen. Um die Integrität und Genauigkeit unserer Analyse zu wahren, haben wir uns daher auf den Zeitraum nach diesen Änderungen beschränkt, um sicherzustellen, dass die Daten die aktuellsten und konsistentesten Meldepraktiken widerspiegeln.

Cyber-Attacken in Europa 2023 nach Bevölkerung Top 20 angegriffene Länder.

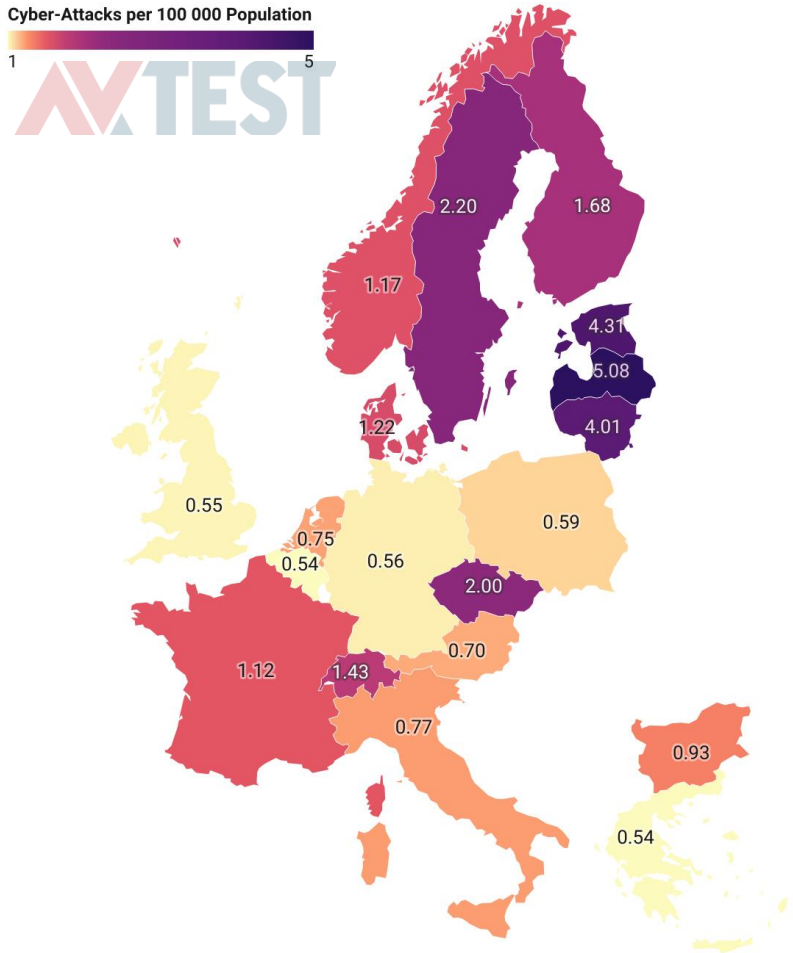


*Abbildung 3: zeigt eine farbkodierte Karte von Europa, die die Häufigkeit von Cyberangriffen pro 100.000 Einwohner in verschiedenen Ländern im Jahr 2023 angibt. Höhere Häufigkeiten sind in dunkleren Farbtönen dargestellt, wobei bestimmte Werte auf der Karte vermerkt sind.*

| Länder | Angriffe pro 100 000 Einwohner |
|---|---|
| Lettland | 5,08 |
| Estland | 4,31 |
| Israel | 4,19 |
| Litauen | 4,01 |
| Schweden | 2,20 |
| Tschechien | 2,00 |
| Finnland | 1,68 |
| Schweiz | 1,43 |
| Dänemark | 1,22 |
| Norwegen | 1,17 |
| Frankreich | 1,12 |
| Bulgarien | 0,93 |
| Italien | 0,77 |
| Niederlande | 0,75 |
| Österreich | 0,70 |
| Polen | 0,59 |
| Deutschland | 0,56 |
| Vereinigtes Königreich | 0,55 |
| Griechenland | 0,54 |
| Belgien | 0,54 |

*Tabelle 2: ergänzt die Karte durch eine Auflistung der europäischen Länder mit der genauen Anzahl von Cyberangriffen pro 100.000 Einwohner, wobei Lettland die höchste und Belgien die niedrigste Rate aufweist.*

Betrachtet man die Dichte der Angriffe pro Kopf der Bevölkerung, ergibt sich ein anderes Bild. Kleinere Länder wie Lettland, Estland, Israel, Litauen und Schweden verzeichneten mit 5,08, 4,31, 4,19, 4,01 bzw. 2,20 Vorfällen pro 100.000 Einwohner die höchsten Raten von Cyberangriffen im Verhältnis zu ihrer Bevölkerungsgröße. Dies deutet darauf hin, dass die Auswirkungen von Cyber-Bedrohungen nicht nur von der Größe einer Nation abhängen, sondern auch von ihrer Cyber-Resilienz und ihrem potenziellen Wert als Ziel.

Es sind nicht nur historische Faktoren, die Länder wie Lettland, Estland, Litauen und in gewissem Maße auch Schweden zu häufigen Zielen für russisch motivierten Hacktivismus machen, sondern auch ihre Haltung zum anhaltenden Konflikt zwischen der Ukraine und Russland. Diese Länder haben sich mit der Ukraine solidarisiert und kritisieren das russische Vorgehen lautstark, was ihr Profil als Ziel für Cyberoperationen erhöht, die der Einschüchterung oder Vergeltung politischer Positionen dienen.

Für Schweden kommt erschwerend hinzu, dass es vor kurzem einen Antrag auf NATO-Mitgliedschaft gestellt hat. Dieser Schritt stellt eine erhebliche Veränderung der regionalen Sicherheitsdynamik dar und wird von Russland als ungünstig angesehen. Infolgedessen ist Schweden möglicherweise zu einem stärkeren Ziel für Cyberangriffe geworden, die darauf abzielen, den NATO-Beitritt des Landes zu untergraben, oder einfach nur ein Mittel sind, um geopolitischen Dissens zum Ausdruck zu bringen.

Die Cyber-Domäne bietet ein relativ risikoarmes, aber wirkungsvolles Mittel zur Einflussnahme, zum Sammeln von Informationen und zur potenziellen Destabilisierung von Gegnern oder als Bedrohung empfundenen Personen. Für russische Hacktivistengruppen, seien es staatlich geförderte oder nationalistische Sympathisanten, können Angriffe auf diese Länder als eine Erweiterung der umfassenderen strategischen Ziele Russlands angesehen werden. Cyberangriffe können kritische Infrastrukturen stören, Verwirrung stiften und als Warnung für andere Nationen dienen, die ähnliche außenpolitische Haltungen oder Bündnisse in Erwägung ziehen könnten.

Im Falle der baltischen Staaten könnte man ihre Cyber-Infrastruktur sowohl als Testfeld für russische Cyber-Fähigkeiten als auch als Frontlinie der digitalen Konfrontation betrachten. Diese Länder haben nicht nur mit dem historischen Erbe von Cyber-Bedrohungen zu kämpfen, sondern sind auch aktiv in einen aktuellen Kontext eingebunden, in dem Cyber-Operationen ein ständiges Anliegen sind, das mit aktuellen internationalen Spannungen verbunden ist.

## Deutschland

Die folgenden umfassenden Karten zeigen die geografische Verteilung von Cybervorfällen in Deutschland im Jahr 2023. Für das Verständnis der lokalen Auswirkungen von zwei vorherrschenden Arten von Cyberbedrohungen sind diese Visualisierungen unerlässlich.

Innerhalb Deutschlands zeigt die Verteilung der Cyberangriffe die Schwerpunkte der bösartigen Aktivitäten. Nordrhein-Westfalen, Baden-Württemberg, Bayern, Berlin und Hessen waren mit 94, 81, 80, 48 bzw. 40 Angriffen die am stärksten betroffenen Regionen.

**Alle beobachteten Cyber-Attacken Deutschland 2023.**

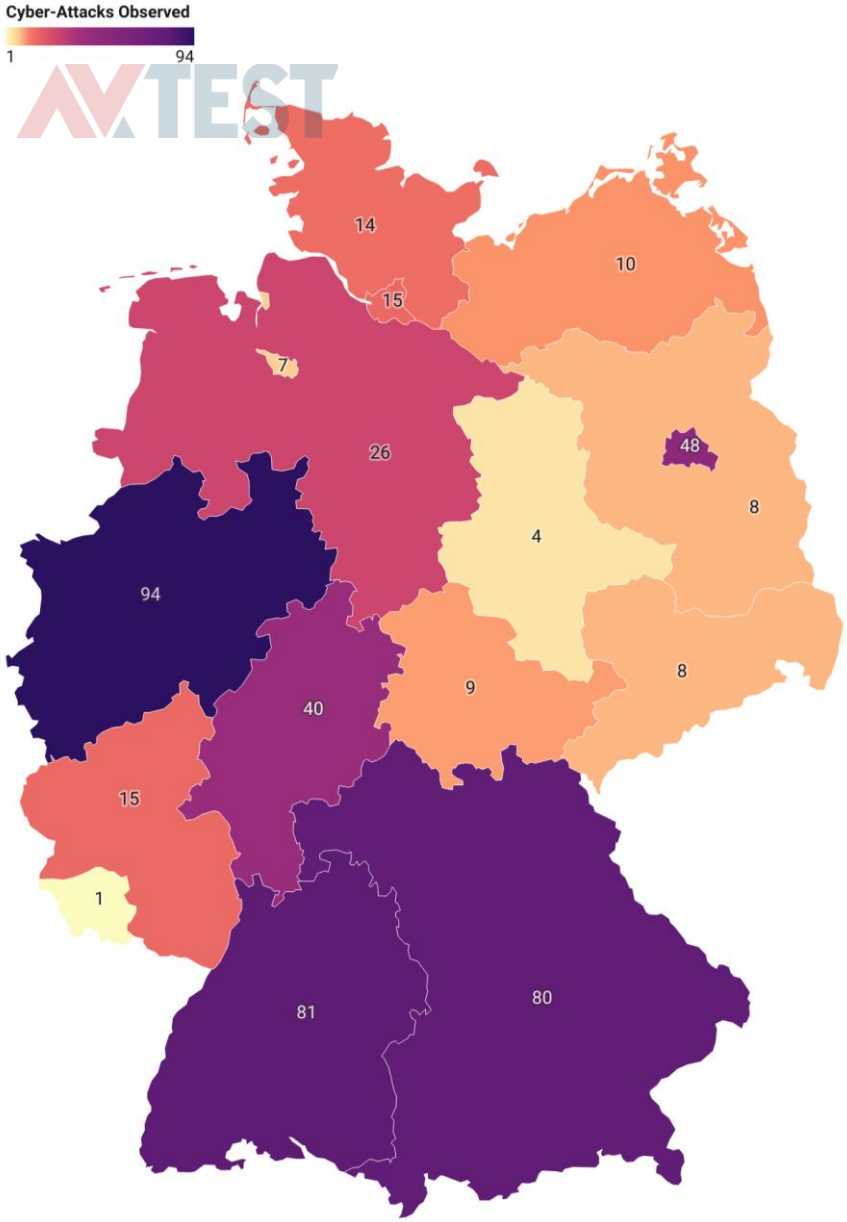


*Abbildung 4: zeigt eine Karte mit Farbverlauf für Deutschland, auf der die Gesamtzahl der im Jahr 2023 in den einzelnen Bundesländern beobachteten Cyberangriffe dargestellt ist. Dunklere Schattierungen weisen auf eine höhere Anzahl von Angriffen hin, wobei für bestimmte Regionen spezifische Zahlen auf der Karte vermerkt sind.*

## Ransomware vs DDoS.

Für Ransomware- und DDoS-Angriffe bieten die folgenden Karten einen detaillierten Einblick in die Häufigkeit dieser Vorfälle und geben Aufschluss über regionale Schwachstellen und die Widerstandsfähigkeit von Cybersicherheitsmaßnahmen in verschiedenen Bereichen.

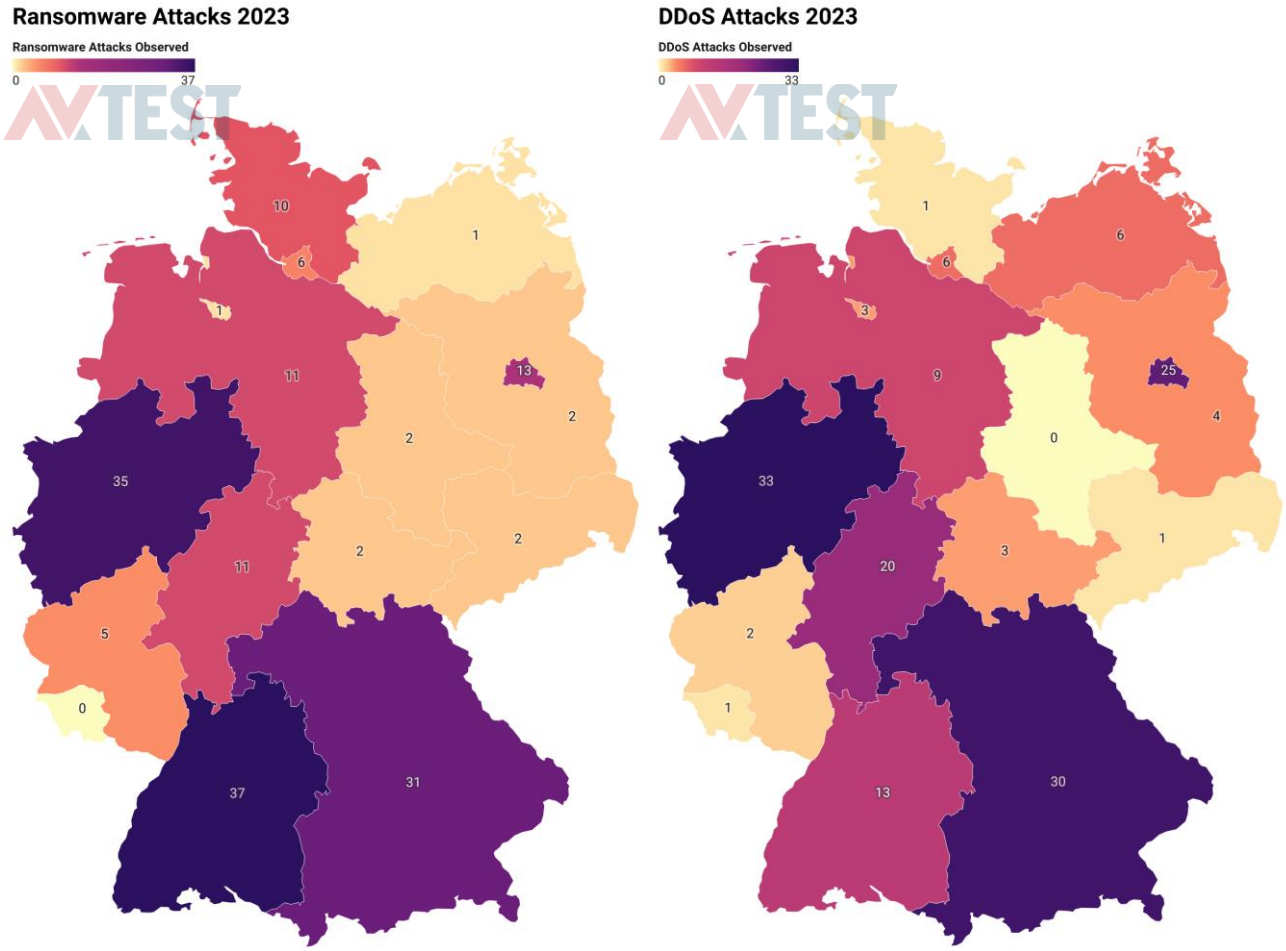


*Abbildung 5: zeigt zwei separate Karten mit Farbverlauf für Deutschland, die jeweils die regionale Verteilung von zwei verschiedenen Arten von Cyberangriffen im Jahr 2023 veranschaulichen. Die linke Karte zeigt die Häufigkeit von Ransomware-Angriffen, während die rechte Karte die Häufigkeit von DDoS-Angriffen darstellt. Dunklere Farben stehen für eine höhere Anzahl von Angriffen in den jeweiligen Bundesländern, wobei für jede Region spezifische Zahlen angegeben sind.*

Die erste Karte befasst sich mit Ransomware-Angriffen, einer Form von Malware, die die Daten eines Unternehmens verschlüsselt und eine Zahlung für deren Freigabe verlangt. Diese Karte zeigt das Ausmaß, in dem jedes deutsche Bundesland von diesen störenden Bedrohungen betroffen war, was die Verbreitung dieser speziellen Cyberkriminalität in verschiedenen Regionen widerspiegelt.

Die zweite Karte konzentriert sich auf DDoS-Angriffe, bei denen Dienste mit übermäßigem Internetverkehr überflutet werden, um ihre normale Funktion zu stören. Die Visualisierung zeigt die Intensität dieser Angriffe in den einzelnen Bundesländern und weist auf die Gebiete hin, in denen diese Taktiken am häufigsten eingesetzt wurden.

Zusammengenommen dienen diese Karten nicht nur als Aufzeichnung der Cybergefahren, mit denen man im Jahr 2023 konfrontiert sein wird, sondern auch als Instrument für die strategische Planung und Ressourcenzuweisung für die künftige Cybersicherheitsverteidigung in Deutschland.

### Cyber-Attacken nach Bevölkerungsgruppen.

In Berlin, Bremen, Hamburg, Baden-Württemberg und Hessen wurden die höchsten Anfallsraten pro 100.000 Einwohner mit 1,28, 1,02, 0,79, 0,72 und 0,63 festgestellt, wenn die Bevölkerungsgröße berücksichtigt wird.

Cyber-Attacken Deutschland 2023 nach Einwohnerzahl

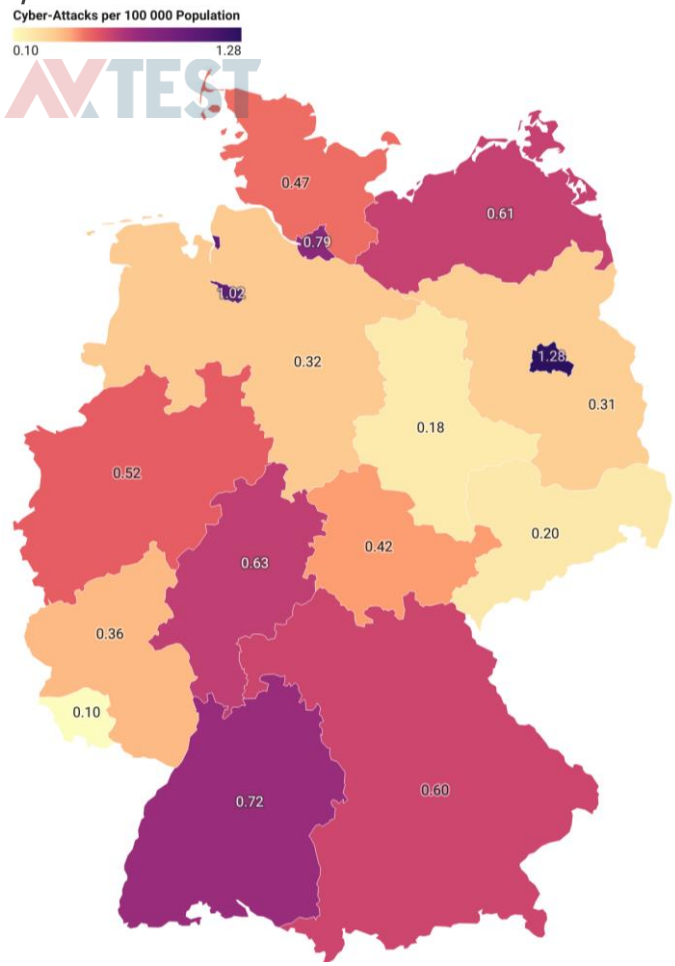


*Abbildung 6: zeigt eine Karte mit Farbverlauf für Deutschland, die Cyberangriffe pro 100.000 Einwohner in den Bundesländern im Jahr 2023 darstellt. Die Intensität der Farbe zeigt die Häufigkeit der Angriffe an, wobei die Werte auf der Karte markiert sind.*

| Bundesländer | Angriffe pro 100 000 Einwohner |
|---|---|
| **Berlin** | 1,28 |
| Bremen | 1,02 |
| Hamburg | 0,79 |
| Baden-Würtenberg | 0,72 |
| Hessen | 0,63 |
| Mecklenburg-Vorpommern | 0,61 |
| Bayern | 0,60 |
| Nordrhein-Westfalen | 0,52 |
| Schleswig-Holstein | 0,47 |
| Thüringen | 0,42 |
| Rheinland-Pfalz | 0,36 |
| Niedersachsen | 0,32 |
| Brandenburg | 0,31 |
| Sachsen | 0,20 |
| Sachsen-Anhalt | 0,18 |
| Saarland | 0,10 |

*Tabelle 3: listet die deutschen Bundesländer zusammen mit der Anzahl der Cyberangriffe pro 100.000 Einwohner auf, wobei die spezifische Angriffsdichte in Berlin am höchsten ist.*

Die vorgelegten Daten weisen auf eine überproportionale Konzentration von Cyberangriffen in den deutschen Stadtstaaten hin, wenn man sie um die Bevölkerungsgröße bereinigt. Die Stadtstaaten Berlin, Bremen und Hamburg weisen die höchsten Raten von Cyberangriffen pro 100.000 Einwohner auf, was darauf hindeutet, dass diese dicht besiedelten städtischen Gebiete besonders attraktive Ziele für Cyberkriminelle sind.

Mehrere Faktoren tragen wahrscheinlich zu diesem Trend bei:

1. **Hohe Konnektivität:** In den Stadtstaaten gibt es eine hohe Konzentration von Unternehmen und Einzelpersonen, die in hohem Maße mit digitalen Netzen verbunden sind, was eine größere Angriffsfläche für Cyberkriminelle bietet.
2. **Konzentration von Behörden in Berlin:** Als Hauptstadt Deutschlands weist Berlin eine hohe Konzentration von Bundesbehörden und Regierungsstellen auf. Diese Einrichtungen sind häufig das Ziel von DDoS-Angriffen, die darauf abzielen, Dienste und den Zugang zu Informationen zu stören, indem sie die Systeme mit einer Flut von Internetverkehr überschwemmen. Solche Angriffe können politisch motiviert sein oder versuchen, Störungen als eine Form des Protests oder der Stellungnahme zu verursachen.
3. **Wirtschaftliche Bedeutung:** Diese Stadtstaaten sind wirtschaftliche Kraftzentren mit bedeutenden Handelsaktivitäten. Cyberangriffe, insbesondere Ransomware und DDoS, zielen in der Regel auf Regionen mit florierenden Wirtschaftszweigen ab, um den Betrieb zu stören und aufgrund des höheren Einsatzes höhere Lösegelder zu fordern.
4. **Sichtbarkeit und Auswirkungen:** Angriffe auf prominente Städte erregen oft mehr Aufmerksamkeit in den Medien, was für Hacktivisten, die für eine Sache werben wollen, oder für Cyberkriminelle, die ihre Fähigkeiten demonstrieren wollen, attraktiv sein kann.
5. **Ressourcenallokation:** Die Konzentration von Wohlstand und Ressourcen in Stadtstaaten kann zu einer besseren Cybersicherheitsinfrastruktur führen. Dies bedeutet jedoch auch, dass erfolgreiche Angriffe wertvollere Daten liefern oder mehr Störungen verursachen könnten, was einen Anreiz für hartnäckigere und ausgefeiltere Angriffe darstellt.
6. **Herausforderungen für die Cybersicherheit:** Die komplexe Infrastruktur und die Vielfalt der Organisationen in den Stadtstaaten können einzigartige Herausforderungen in Bezug auf die Koordinierung und Reaktion im Bereich der Cybersicherheit mit sich bringen, die möglicherweise zu Schwachstellen führen, die ausgenutzt werden können.

Unterrepräsentation im Osten: Die Daten zeigen, dass östliche Bundesländer wie Sachsen, Sachsen-Anhalt und Brandenburg eine der niedrigsten Raten von Cyberangriffen pro Kopf aufweisen. Dies könnte auf mehrere Faktoren zurückzuführen sein:

1. **Weniger hochrangige Ziele:** In diesen Gebieten gibt es möglicherweise weniger große Unternehmen oder hochwertige Infrastrukturen, die in der Regel anspruchsvollere Cyber-Bedrohungen anziehen.
2. **Wirtschaftliche Faktoren:** Das wirtschaftliche Profil dieser Regionen ist möglicherweise für bestimmte Arten von wirtschaftlich motivierter Cyberkriminalität nicht so attraktiv.
3. **Sichtbarkeit und Berichterstattung:** Es könnte auch Unterschiede bei der Sichtbarkeit und Meldung von Cybervorfällen geben. Wenn die Cybersicherheitsmaßnahmen oder das Bewusstsein dafür weniger entwickelt sind, werden einige Angriffe möglicherweise nicht gemeldet.

Die beobachteten Daten spiegeln das erhöhte Risiko wider, dem urbane Zentren in der Cyberdomäne ausgesetzt sind. Während bevölkerungsreichere Länder wie Nordrhein-Westfalen, Baden-Württemberg und Bayern in absoluten Zahlen eine höhere Anzahl von Angriffen verzeichneten, lässt die Pro-Kopf-Rate in den Stadtstaaten auf ein gezieltes Muster von Cybervorfällen schließen. Dies deutet darauf hin, dass Cyberkriminelle strategische Entscheidungen treffen, um sich auf Ziele zu konzentrieren, bei denen die potenziellen Gewinne maximiert werden oder bei denen die Verteidigung trotz der Ressourcenkonzentration ungleichmäßig ist.

Das Verständnis der Motive und Methoden, die hinter diesen gezielten Angriffen stehen, ist entscheidend für die Entwicklung wirksamer Cybersicherheitsstrategien, die diese kritischen städtischen Zentren schützen können, die eine wichtige Rolle für die Wirtschaft und die gesellschaftlichen Funktionen in Deutschland spielen.

*Gesammelt und kuratiert von*
*David Walkiewicz, Director Test Research, AV-TEST GmbH*
*Jens Lichtenstein, Testing Engineer, AV-TEST GmbH*
*Maik Morgenstern, CTO, AV-TEST GmbH*


Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

# Über die **AV-TEST**

Die AV-TEST GmbH ist ein unabhängiger Anbieter von Dienstleistungen in den Bereichen IT-Security und Antivirenforschung. Der Schwerpunkt liegt dabei auf der Erkennung und Analyse aktueller Schadsoftware und deren Nutzung für umfassende vergleichende Tests von Sicherheitsprodukten.

Durch die Aktualität der Testdaten kann Schadsoftware sofort analysiert und kategorisiert werden, Trends in der Virenentwicklung können frühzeitig erkannt und IT-Sicherheitslösungen getestet und zertifiziert werden. Die Ergebnisse des AV-TEST-Instituts stellen eine exklusive Informationsbasis dar, die Herstellern bei der Optimierung ihrer Produkte, Fachzeitschriften bei der Veröffentlichung von Forschungsdaten und Endanwendern bei der Produktauswahl hilft.

AV-TEST ist seit 2004 in Magdeburg (Deutschland) ansässig und beschäftigt mehr als 30 Mitarbeiter, die über umfangreiche praktische Erfahrungen verfügen.

In den AV-TEST-Laboratorien werden auf 300 Client- und Serversystemen mehr als 2.500 Terabyte unabhängig gesammelter Testdaten, die sowohl bösartige als auch harmlose Musterinformationen enthalten, gespeichert und verarbeitet.

Für weitere Informationen besuchen Sie bitte unsere Website unter https://www.av-test.org .


Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org