# Cybersecurity-Trends 2024: TÜV Rheinland zeigt Wege zur effektiven Cybersicherheit auf

# Zunahme von Cyberangriffen macht Cybersecurity zur strategischen Priorität für Unternehmen aller Größen / TÜV Rheinland bietet Einblicke in die Herausforderungen und Lösungen / [www.tuv.com/cs-trends](http://www.tuv.com/cs-trends)

**Köln, 27. November 2023**. Die Cybersecurity-Trends 2024 von TÜV Rheinland zeigen auf, wie sich Unternehmen in einer zunehmend digitalisierten und vernetzten Welt vor Cyberangriffen schützen können. Die Angriffsflächen haben sich erheblich vergrößert, insbesondere für kleine und mittlere Unternehmen, die ihre Gefährdung oft unterschätzen. Aber auch große Unternehmen mit hohen Sicherheitsstandards sind nicht immun gegen die fortgeschrittenen Techniken professioneller Hackerorganisationen.

Top-Risiken: Phishing, schnellere Ransomware-Angriffe, KI-Einsatz

Top-Risiken wie Phishing und schnellere Ransomware-Angriffe dominieren weiterhin die Bedrohungslandschaft, so die Fachleute von TÜV Rheinland. Die steigende Anzahl vernetzter Geräte verschärft die Gefahren durch immer mehr Schwachstellen. Mit dem Einsatz von KI wird die Fähigkeit, diese Schwachstellen auszunutzen, auf ein neues Level gehoben. Neue Technologien machen Cyberangriffe effektiver, zugleich bilden geopolitische Krisen ein Umfeld, das die Risiken erhöht. „Die alarmierende Zunahme von Cyberangriffen in den letzten Jahren hat unterstrichen: Unternehmen und Institutionen jeder Größe sollten Cybersecurity als strategische Priorität betrachten“, sagt Petr Láhner, Leiter des Geschäftsbereichs Industrie Service & Cybersecurity bei TÜV Rheinland.

Zehn wichtige Trends für 2024

Die Cybersecurity-Trends 2024 von TÜV Rheinland bieten einen Überblick über zehn wichtige Trends, auf die sich Unternehmen einstellen müssen. Dazu gehören strengere Cybersecurity-Richtlinien, die Bildung von Allianzen für Cybersecurity, die Bedrohung der wirtschaftlichen Existenz durch Cyberangriffe, der Einsatz von KI in Cyberangriffen, organisierte Cyberkriminalität, schnellere Ransomware-Angriffe, ein Anstieg der Sicherheitslücken, massenhafte Konnektivität und Automotive Hacking. TÜV Rheinland bietet Unternehmen Lösungen und Empfehlungen, um sich auf diese Herausforderungen vorzubereiten und ihre Cyberabwehrfähigkeit zu erhöhen.

Ausführliche Informationen zu den zehn Cybersecurity-Trends 2024 finden Sie unter [www.tuv.com/cs-trends](http://www.tuv.com/cs-trends) bei TÜV Rheinland.

*Sicherheit und Qualität in fast allen Wirtschafts- und Lebensbereichen: Dafür steht TÜV Rheinland. Das Unternehmen ist seit mehr als 150 Jahren tätig und zählt zu den weltweit führenden Prüfdienstleistern. TÜV Rheinland hat mehr als 20.000 Mitarbeiterinnen und Mitarbeiter in über 50 Ländern und erzielt einen Jahresumsatz von rund 2,3 Milliarden Euro. Die hoch qualifizierten Expertinnen und Experten von TÜV Rheinland prüfen rund um den Globus technische Anlagen und Produkte, begleiten Innnovationen in Technik und Wirtschaft, trainieren Menschen in zahlreichen Berufen und zertifizieren Managementsysteme nach internationalen Standards. Damit sorgen die unabhängigen Fachleute für Vertrauen entlang globaler Warenströme und Wertschöpfungsketten. Seit 2006 ist TÜV Rheinland Mitglied im Global Compact der Vereinten Nationen für mehr Nachhaltigkeit und gegen Korruption. Website:* [*www.tuv.com*](http://www.tuv.com)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

Ihr Ansprechpartner für redaktionelle Fragen:

Pressestelle TÜV Rheinland, Tel.: +49 2 21/8 06-21 48

Die aktuellen Presseinformationen sowie themenbezogene Fotos und Videos erhalten Sie auch per E-Mail über contact@press.tuv.com sowie im Internet: [www.tuv.com/presse](http://www.tuv.com/presse) und [www.twitter.com/tuvcom\_presse](http://www.twitter.com/tuvcom_presse)