**TÜV Rheinland: IT-Sicherheitslage in Deutschland verschärft sich weiter**

Umfrage anlässlich des Tages für Computersicherheit am 30. November / BSI bewertet Lage ebenfalls als angespannt / TÜV Rheinland mit Cybersecurity-Dienstleistungen und Unterstützung bei Umsetzung von EU-Regulierungen / [www.tuv.com/cybersecurity](http://www.tuv.com/cybersecurity)

**Köln, 28. November 2024.** Die IT-Sicherheitslage in Deutschland verschärft sich weiter. Das zeigt eine Umfrage unter Fachleuten für Cybersecurity, die TÜV Rheinland anlässlich des internationalen Tages für Computersicherheit am 30. November in Auftrag gegeben hat. In der von Civey im Oktober 2024 durchgeführten Online-Umfrage geben neun von zehn Befragten (90,2%) an, dass die Gefahr von Cyber-Angriffen für Unternehmen und Institutionen in Deutschland in den vergangenen zwölf Monaten zugenommen hat. Befragt wurden deutschlandweit rund 1.000 Personen, die im Bereich Cybersicherheit tätig sind. „Unsere Befragung zeigt: Unternehmen sind mehr denn je mit Cyberangriffen konfrontiert – und müssen entsprechend in ihre Cybersecurity investieren“, sagt Daniel Hanke, Experte für Cybersecurity bei TÜV Rheinland.

Das bestätigt der Bericht zur Lage der IT-Sicherheit in Deutschland, den das Bundesamt für Sicherheit in der Informationstechnik (BSI) Mitte November veröffentlicht hat: Das BSI schätzt die Situation als „angespannt“ ein, auch wenn es eine Verbesserung in der Resilienz gegenüber Cyberangriffen sieht. „Anders gesagt: Es stellt sich längst nicht mehr die Frage, ob ein Unternehmen Opfer eines Cyberangriffs wird, sondern wann und wie sich mögliche Schäden durch Cyberangriffe durch vorbeugende Maßnahmen verringern lassen“, so Cybersecurity-Experte Hanke.

**Veraltete Infrastruktur und mangelnde Vorbereitung als Herausforderungen**

TÜV Rheinland ließ ebenfalls danach fragen, welches die größten Herausforderungen für die Gewährleistung von Cybersicherheit in Unternehmen und Institutionen sind. Dabei sticht ein Aspekt hervor: Die ausgemachten Herausforderungen lassen sich nicht auf wenige, einzelne reduzieren. Die „Steigende Zahl von Angriffen“ (39,2%), „Veraltete IT-Infrastruktur“ (38,9%) und „Mangelnde Vorbereitung gegen Cyberangriffe“ (36,3%) werden von den Befragten am häufigsten genannt. Ähnlich herausfordernd werden die „Wachsende Komplexität von IT-Systemen“ (35,3%), der „Fachkräftemangel im IT-Bereich“ (34,7%) und „KI-unterstützte Hackerangriffe“ (32,3%) wahrgenommen. Mangelnde Budgets sind hingegen nur für jeden Fünften (21,9%) eine Herausforderung. „Einerseits haben die meisten Verantwortlichen offenbar erkannt, dass man an Cybersecurity nicht sparen sollte – andererseits ist es besorgniserregend, dass jeder Dritte die Unternehmen schlecht vorbereitet auf Cyberangriffe sieht“, kommentiert TÜV Rheinland-Experte Daniel Hanke.

**Handlungsdruck durch neue Regulierungen**

Zur Bedrohungslage kommen Veränderungen auf Ebene der Reglierung hinzu. So führt die „Network and Information Security Directive 2“ (NIS-2-Richtlinie) der Europäischen Union strengere Vorschriften zur Cybersicherheit für mehr Sektoren und Unternehmen ein. Ab März 2025 müssen damit Unternehmen ab 50 Mitarbeitenden und mit mehr als 10 Millionen Euro Umsatz in 18 Sektoren verstärkte Cybersecurity-Maßnahmen umsetzen. Das Ziel: der Schutz von essentiellen, wichtigen Sektoren und (kritischen) Infrastrukturen sowie eine höhere Widerstandsfähigkeit gegenüber Cyberangriffen. Ebenfalls auf der Regulierungsebene setzt der Cyber Resilience Act an. Hiermit führt die Europäische Union verbindliche Cybersicherheitsanforderungen für „Produkte mit digitalen Elementen“ ein. Das Ziel auch hier: die Widerstandsfähigkeit gegen Cyberangriffe zu erhöhen und verlässliche digitale Dienste zu gewährleisten.

„Insgesamt führen die steigenden Risiken durch Cyberangriffe verbunden mit den neuen regulatorischen Anforderungen dazu, dass der Handlungsdruck in den Unternehmen steigt“, sagt Daniel Hanke. „Die weltweit mehr als 250 Cybersecurity-Fachleute von TÜV Rheinland unterstützen dabei umfassend sowohl mit klassischen Cybersecurity-Dienstleistungen wie dem Pentesting wie auch bei der regelkonformen Umsetzung der Regulierungen.“

Weitere Informationen unter [www.tuv.com/cybersecurity](http://www.tuv.com/cybersecurity) 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 22.000 Mitarbeiterinnen und Mitarbeiter in über 50 Ländern und erzielt einen Jahresumsatz von mehr als 2,4 Milliarden Euro. Die hoch qualifizierten Expertinnen und Experten von TÜV Rheinland prüfen rund um*

*den Globus technische Anlagen und Produkte, begleiten Innovationen 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).