NACHRICHTEN AG

04. Juni 2025

DAX-Unternehmen schätzen Risiken: Cyberangriffe und Bürokratie dominieren!

Die Universität Hohenheim analysiert DAX-Unternehmen 2025: steigende Risiken wie Cyber-Angriffe und Bürokratie im Fokus.

70599 Stuttgart, Deutschland - Die Universität Hohenheim und Crunchtime Communications haben in einer aktuellen Analyse die Geschäftsberichte von 134 DAX-Unternehmen sorgfältig unter die Lupe genommen. Die Ergebnisse dieser Analyse zeigen einen signifikanten Anstieg der gemeldeten Risiken: Börsennotierte Unternehmen in Deutschland berichten von rund 30 % mehr Risiken im Vergleich zu vor zwei Jahren. Unternehmenslenker sind sich der wachsenden Bedrohungen bewusst, doch die Kommunikation dieser Risiken in ihren Vorworten bleibt oft mangelhaft.

Die größten Risiken werden dabei von den Unternehmen selbst als regulatorische Belastungen (98 %) und Cyber-Angriffe (98 %) identifiziert, gefolgt von geopolitischen Entwicklungen und Finanzthemen (jeweils 86 %). Interessanterweise sprechen die Vorstandsvorsitzenden in nur 37 % der Vorworte über Risiken und erwähnen im Durchschnitt lediglich 1,2 Risiken; in 40 % der Vorworte fehlen jegliche Risikohinweise. Laut Prof. Dr. Frank Brettschneider ist die Wahrnehmung von Bürokratie und Cyber-Risiken als ernstes Geschäftsrisiko besonders ausgeprägt.

Wachsende Bedrohungen und Reaktionen

Cyber-Vorfälle weltweit nehmen zu, was durch die fortschreitende Digitalisierung und geopolitische Spannungen bedingt ist. Nach Einschätzung des Bundesamts für Sicherheit in der Informationstechnik (BSI) war die Bedrohung im Cyber-Raum im Frühjahr 2024 „so hoch wie nie zuvor“. Der Finanzsektor ist besonders betroffen: Fast 20 % aller globalen Cyber-Vorfälle in den letzten 20 Jahren richteten sich gegen diesen Sektor. Die finanziellen Schäden seit 2004 summieren sich auf fast 12 Milliarden US-Dollar, was die Anfälligkeit der Branche unterstreicht.

Die Unternehmen reagieren jedoch auf die steigenden Bedrohungen: 90 % der DAX-Unternehmen führen systematische quantitative Risikobewertungen durch, wobei auch 65 % der Unternehmen im Finanzsektor angesichts wachsender Herausforderungen bei Cyber-Angriffen existenzbedrohende Risiken befürchten. Im Jahr 2024 verzeichneten Zahlungsdienstleister bereits 258 Meldungen zu Zahlungsvorfällen, was einem Anstieg im Vergleich zu den Vorjahren entspricht.

Aktuelle Trends im Risikomanagement

Die Analyse zeigt außerdem einen Trend hin zur systematischeren Risikobewertung, die in den letzten zwei Jahren zugenommen hat. Externe Einflüsse wie Cyber-Angriffe

und regulatorische Herausforderungen werden als zentrale Bedrohungen wahrgenommen. Nur Vertrieb und Compliance wurden von über 80 % der Unternehmen genannt, was verdeutlicht, dass auch der Wettbewerb und ein Fachkräftemangel als bedeutende Risiken für den Geschäftserfolg gelten. Im Vergleich zu 2023 ist die Nennung von Pandemien, der Energiekrise und der Inflation als Risiken zurückgegangen.

Darüber hinaus haben 41 % der Organisationen weltweit im letzten Jahr drei oder mehr kritische Risikovorfälle erlebt. Die Besorgnis über Cyberkriminalität bleibt hoch, wobei 58 % der Risikomanager sie als eines der fünf größten Risiken für die nächsten drei Jahre betrachten. Dennoch glauben 63 % der Führungskräfte, dass ihre Risikomanagementprozesse keinen oder nur einen minimalen Wettbewerbsvorteil bieten.

Die BaFin plant, Maßnahmen zur Stärkung der Cyber-Sicherheit und zur Harmonisierung des Meldewesens für IKT-Vorfälle einzuführen. Ab Januar 2025 tritt der Digital Operational Resilience Act (DORA) in Kraft, der die Rahmenbedingungen für den Umgang mit Cyber-Risiken weiter definiert. Dies wird die allgemeine Sicherheitslage im Finanzsektor verbessern und die Resilienz gegen Cyber-Risiken erhöhen.

Insgesamt ist das Risikomanagement in deutschen Unternehmen stärker im Fokus denn je, und die Notwendigkeit, sich an die steigenden Bedrohungen anzupassen, wird unumstritten anerkannt. Unternehmen sind gefordert, ihre Strategien entsprechend zu überdenken und effizientere Maßnahmen zur Risikobewältigung einzuführen, um künftige Herausforderungen besser meistern zu können.

Die zunehmende Sensibilisierung in der Finanzbranche spiegelt sich auch in den Investitionen in die IT-Sicherheit wider, um potenzielle Angriffe abzuwehren und die geschäftliche Kontinuität zu sichern. Die Marktteilnehmer sind sich einig: Die Zeit für präventive und reaktive Maßnahmen ist gekommen.

Für weitere Informationen: **Universität Hohenheim**, **BaFin**, **Secureframe**.

Details	
Vorfall	Cyberkriminalität
Ursache	Digitalisierung, geopolitische Spannungen
Ort	70599 Stuttgart, Deutschland
Schaden in €	12000000000
Quellen	• **www.uni-hohenheim.de** • **www.bafin.de** • **secureframe.com**