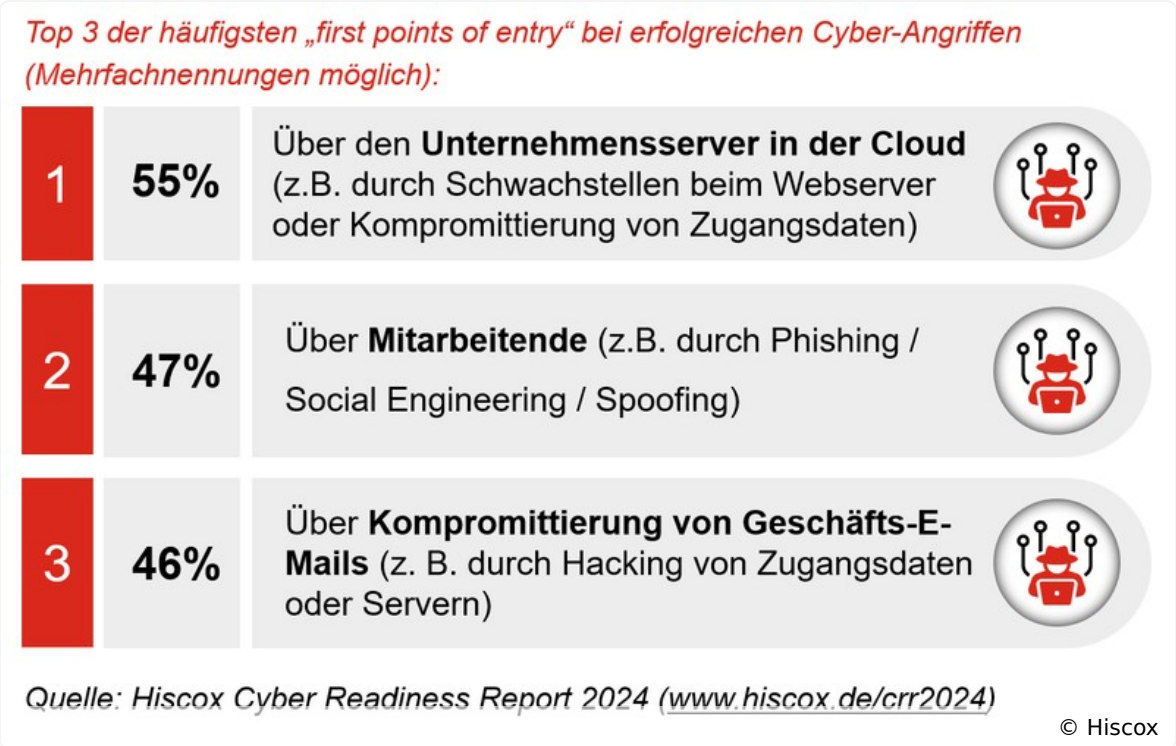
Cybersicherheitsrisiko Mitarbeitende – Angriffspunkt bei 47 % der deutschen Unternehmen



Mitarbeitende gehören zu den häufigsten Cybersicherheitsrisiken für Unternehmen. Laut dem aktuellen Cyber Readiness Report des Spezialversicherers Hiscox berichteten 47 % der deutschen Unternehmen (global 46 %), die im vergangenen Jahr Ziel eines Cyberangriffs wurden, dass Mitarbeitende der erste Einstiegspunkt in mindestens einen dieser Angriffe waren.

Somit sind Mitarbeitende (47 %) gleich nach Cloud-Sicherheitslücken auf Unternehmensservern (55 %) das größte Risiko für Cyberangriffe in Deutschland. Insbesondere manipulative Social-Engineering-Techniken, wie beispielsweise Phishing, missbrauchen das Vertrauen von Mitarbeitenden und gefährden dadurch die Cybersicherheit von Unternehmen.

Viele Mitarbeitende arbeiten hybrid im Homeoffice und oftmals auch mit eigenen technischen Geräten (Bring Your Own Device, BYOD). Dadurch ist nicht nur das Cyberangriffsrisiko erhöht, sie erhalten zudem auch nicht immer die neuesten Informationen und Aufklärungen zu Cybersicherheitsrichtlinien und Best Practices. Außerdem sind sie anfälliger für Fehler oder Sicherheitsverletzungen, die unbeachtet bleiben. Die Hälfte aller Führungskräfte in Deutschland (49 %) sieht einen Anstieg des Cyberrisikos in der Remote-Arbeit. Immerhin geben zwei Drittel der Führungskräfte (65 %) an, dass ihr Unternehmen zusätzliche Schulungsmaßnahmen zur Cybersicherheit für remote arbeitende Mitarbeitende getroffen hat, um das Risiko von Cyberangriffen zu verringern.


Gisa Kimmerle © Hiscox

„Cybersicherheitsrichtlinien sind nur dann wirksam, wenn alle Mitarbeitenden ihre Bedeutung verstehen und aktiv Schutzmaßnahmen ergreifen. Cybersicheres Verhalten muss Teil jeder Unternehmenskultur sein. Proaktive Schulungen von Mitarbeitenden, Tests und Richtlinien – vor allem bei eigenen technischen Geräten – sind entscheidende Maßnahmen, um die Cyberresilienz des Unternehmens zu erhöhen. Nur mit einem gut informierten Team, das sich der Gefahren bewusst ist, können Unternehmen ihre sensiblen Daten ausreichend schützen und so gegen die immer besser getarnten Angriffe im digitalen Raum vorbereitet sein. Für die Absicherung des Restrisikos ist eine Cyber-Versicherung sehr ratsam”, erklärt Gisa Kimmerle, Head of Cyber bei Hiscox.

Über die Umfrage:
Der internationale Hiscox Cyber Readiness Report liefert jährlich seit 2016 ein aktuelles Bild der Cyber-Bereitschaft von Organisationen und bietet eine Blaupause für Best Practices im Kampf gegen eine sich ständig weiterentwickelnde Bedrohung. Er basiert auf einer internationalen Befragung von 2150 Expertinnen und Experten, die für die Cybersicherheitsstrategie ihres Unternehmens verantwortlich sind. Befragt wurden Führungskräfte wie Geschäftsführer, Abteilungsleiter, IT-Manager und andere wichtige Fachleute, aber auch Selbstständige. Es handelt sich dabei um eine repräsentative Auswahl von Unternehmen verschiedener Größen und Branchen. Die Teilnehmenden stammen aus den folgenden Ländern: Deutschland, den USA, dem Vereinigten Königreich, der Republik Irland, Frankreich, Spanien, Belgien und den Niederlanden, was diesen Report zu einem der umfassendsten und meistbeachteten seiner Art macht. Die Befragungen für den CRR2024 wurden zwischen dem 12. August und dem 2. September 2024 durchgeführt.