Hiscox Cyber Readiness Report 2023: Angriffszahlen zum dritten Mal in Folge gestiegen

Gisa Kimmerle © Hiscox

53 % der befragten Unternehmen wurden Opfer eines Cyberangriffs / Angriff für jedes fünfte Unternehmen existenzbedrohend / In Deutschland werden Cyberangriffe als größtes Geschäftsrisiko angesehen (43 %) / Durchschnittliche Ausgaben für Cybersicherheit stiegen innerhalb von drei Jahren um 39 % / 71 % der Entscheider erwarten Reputationsschaden nach Cyberangriff

Pünktlich zum Cyber-Security-Monat veröffentlicht Hiscox die Zahlen des diesjährigen Cyber Readiness Reports. Die repräsentative und internationale Studie, die bereits seit 2017 jährlich durch das Marktforschungsunternehmen Forrester erhoben wird, zeigt deutlich, dass das Bewusstsein für Cyber-Risiken bei Entscheidern gestiegen ist. In Deutschland werden Cyberangriffe erneut als größtes Geschäftsrisiko angesehen (43 %). International ist ein leichter Stimmungsumschwung zu beobachten: Nur noch fünf von acht Ländern nennen Cyberrisiken als wichtigstes Risiko für Unternehmen. Doch die Fallzahlen bleiben konstant hoch: Mehr als jedes zweite Unternehmen (53%) war auch im vergangenen Jahr wieder Opfer einer Attacke. Deshalb stellt Hiscox die Betrachtung der Studienergebnisse in den größeren Rahmen und hinterfragt, was sie über „Digital Trust“ aussagen.

In einer zunehmend digitalen Welt ist Vertrauen ein entscheidender Faktor, der viele Aspekte von Online-Aktivitäten, wie z. B. den elektronischen Handel, die gemeinsame Nutzung von Daten und die Online-Kommunikation, erst ermöglicht. Nach der Definition des World Economic Forum bedeutet Digital Trust, dass Menschen tagtäglich darauf vertrauen, dass digitale Technologien und die Organisationen, die sie nutzen, ihre Interessen wahren und Erwartungen erfüllen.

Mangelnde Cyber-Sicherheit als größtes Hindernis für Digital Trust

Doch die internationalen Daten sind alles andere als vertrauenerweckend: Die Zahl der angegriffenen Unternehmen ist im dritten Jahr in Folge gestiegen (53 % 2023; 48 % 2022; 43 % 2021). Auch in Deutschland werden Cyberangriffen häufiger. Die Ergebnisse zeigen sogar einen

zweistelligen Anstieg von 46 % im Jahr 2022 auf 58 % im Jahr 2023. Auch die Zahl der Cyber-Attacken hat in Deutschland pro Unternehmen deutlich zugenommen: Im letzten Jahr lag der Median bei 6, in diesem Jahr bei 10 Angriffen, was Deutschland nach Irland zum zweithäufigsten angegriffenen Land macht.

Rasche technologische Entwicklungen und langsame Anpassung der rechtlichen Rahmenbedingungen sind Herausforderungen, die Vertrauen in digitale Prozesse behindern. Doch die größte Hürde bleibt mangelnde Cybersicherheit. Besonders bei großen Unternehmen gehören Cyberangriffe zur Tagesordnung: So verzeichnen Firmen mit mehr als 1.000 Beschäftigten den größten Anstieg von 62 % auf 70 % mit mindestens einem Angriff. Jedes fünfte Unternehmen (21 %), das angegriffen wurde, gab an, dass die Auswirkungen so groß waren, dass sie ihre wirtschaftliche Existenz hätten bedrohen können.

Diese Risikolage bleibt nicht ohne Konsequenzen für die Stimmung in Unternehmen. Der Anteil derjenigen, die sich als Cyber-Experten bezeichnen, also darauf vertrauen, dass sie gut gerüstet sind und sich beim Thema Cyber-Security auskennen, ist erneut gesunken: von 4,5 % im Jahr 2021 auf 3,4 % im Jahr 2022. Dementsprechend ist der Anteil der selbstdefinierten Cyber-Neulinge in diesem Jahr um 0,8 Prozentpunkte auf 28,3% gestiegen.

Diese immer größere Unsicherheit materialisiert sich am stärksten bei den kleineren Firmen: Nur drei von fünf Unternehmen (61 %) mit weniger als 250 Beschäftigten sind zuversichtlich, dass sie auf dem Gebiet der Cybersicherheit gut gewappnet sind. Bei den größeren Unternehmen sind es 71 %. Die Befragten kleinerer Unternehmen sind auch weniger sicher, dass ihre Geschäftsleitung der Cybersicherheit Priorität einräumt, und bezweifeln eher, dass ihre IT-Ausstattung dieser Aufgabe gewachsen ist.

„Uns führt das zu der Frage: Wenn Unternehmen nicht einmal selbst in ihre Cyber Readiness vertrauen, wie sollen es dann ihre Kunden oder Auftraggeber tun? Die Studienergebnisse zeigen deutlich, wo die Stolpersteine auf dem Weg zu einer Gesellschaft liegen, die dauerhaft souverän mit den Risiken umgeht, die eine digitale und vernetzte Welt mit sich bringt. Dabei geht es nicht nur darum, dass Hackerangriffe sich teilweise schneller entwickeln als die Abwehr von Unternehmen. Unser Ziel als Versicherer ist es, ein Bewusstsein dafür zu schaffen, dass diese digitalen Risiken nicht mehr verschwinden und es nicht möglich ist, einen Status quo ohne Investitionen zu halten. Priorisierung von Datenschutzmaßnahmen, kontinuierliche Weiterbildung von Mitarbeitenden und Investitionen in CyberSecurity sollten schon lange keine Sonderprojekt mehr im Unternehmen sein. In den Studiendaten sehen wir zwar einen positiven Trend, aber die Entwicklung ist aus unserer Sicht noch sehr langsam“, sagt Gisa Kimmerle, Head of Cyber bei Hiscox.

Mehr Cyber-Resilienz bedeutet mehr Digital Trust

Hiscox-Experten sind sich einig, dass ein so hoher Anteil gehackter Unternehmen und die jahrelang wachsende Verunsicherung bei Entscheidern kein Dauerzustand sein dürfen. Denn Digital Trust ist ein gesellschaftliches Ziel, und gleichzeitig businessrelevant: Nur Unternehmen, die digital vertrauenswürdig sind, können in Zukunft erfolgreich Geschäfte machen. Über kurz oder lang wird ein Ökosystem aus cybersicheren Unternehmen entstehen, das Nachzügler zunehmend aus dem Geschäftsverkehr ausschließen wird. Anderenfalls könnte der dauerhafte Mangel an digitalem Vertrauen dem Gesellschafts- und Wirtschaftssystem nachhaltigen Schaden zufügen.

Und das Bewusstsein für die Konsequenzen von beschädigtem Vertrauen ist weit verbreitet: 71 % der Befragten stimmen zu, dass die Marke des Unternehmens Schaden nimmt, wenn die Daten von Kunden und Partnern nicht sicher gehandhabt werden. Im Ernstfall ist der Schutz von Kundendaten sogar der Hauptgrund (46 %) für die Zahlung von Lösegeld infolge von

Ransomware-Attacken. Bei deutschen Unternehmen sind die Erwartungen ihrer Geschäftspartner bereits der größte Antrieb (28%), ihre CyberResilienz zu erhöhen.

Die wichtigsten Maßnahmen für mehr digitales Vertrauen und Cyber-Resilienz

„Ein Schlüssel zum Erfolg ist aus Hiscox-Sicht die Akzeptanz, dass es sich bei Cyber-Risiken nicht um eine temporäre oder außergewöhnliche Bedrohung handelt. Wer dies in vollem Umfang akzeptiert, kann automatisch die passenden Maßnahmen ableiten. Beispielsweise haben absichtliches oder unabsichtliches Fehlverhalten von Mitarbeitenden völlig andere Konsequenzen, sobald sensible Daten involviert sind. Darüber hinaus ist die Einführung und Aktualisierung von Notfallplänen, der sogenannten Incident Response Plans, eine sinnvolle Konsequenz auch für kleinere Unternehmen“, ergänzt Gisa Kimmerle.

Ein Beispiel für den genannten positiven Trend sind die höheren Investitionen in IT-Sicherheit: Die durchschnittlichen Ausgaben stiegen innerhalb von drei Jahren um 39 % auf 142.600 Euro. Bei Unternehmen mit weniger als zehn Mitarbeitern vervierfachten sie sich innerhalb von zwei Jahren. Deutschland ist Vorreiter: Unternehmen in der Bundesrepublik gaben am meisten für IT-Sicherheit aus bei einem Median von 195.040 Euro im Vergleich zu 142.600 Euro international.

Auch eine höhere Abdeckung durch passende Cyber-Versicherungen ist ein Schritt zu mehr digitalem Vertrauen. Der Anteil der Cyber-Versicherungsnehmer unter den Befragten ist dabei im internationalen Vergleich in Deutschland am höchsten (67 %). Versicherungen spielen eine wichtige Rolle bei der Abmilderung der Auswirkungen von Cybervorfällen, Schutz vor monetären Schäden und der Förderung bewährter Praktiken im Bereich der Cybersicherheit.

„Ziel muss es sein, in einer Welt zu leben, in der man sich generell wieder vertrauen kann und in welcher der Umgang mit Daten den Grundsätzen der Informationssicherheit entspricht: Integrität, Vertraulichkeit und Verfügbarkeit. Der Zero-Trust-Ansatz, der zum Aufsetzen eines resilienten IT-Systems sinnvoll erscheinen mag, sollte nicht unseren gesellschaftlichen Alltag beherrschen. Der erste Schritt dahin ist klar: Deutsche Unternehmen müssen bei der IT-Sicherheit aufholen, ihre Hausaufgaben hinsichtlich der Aufstellung einer resilienten Organisation machen und so in einem großen Ausmaß ‘versicherbar‘ werden“, ergänzt Gisa Kimmerle.

Über die Studie:

Der siebte internationale Hiscox Cyber Readiness Report, der jährlich von Forrester erstellt wird, liefert 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 Umfrage unter insgesamt 5.005 Führungskräften, Abteilungsleitern, IT-Managern und anderen wichtigen Fachleuten. Es handelt sich dabei um eine repräsentative Auswahl von Unternehmen verschiedenster Größen und Branchen aus acht Ländern (Belgien, Frankreich, Deutschland, die Niederlande, Spanien, Großbritannien, Irland und die USA), was diesen Report zu einem der umfassendsten und meistbeachteten seiner Art macht. Weiter Informationen finden Sie online unter: https://www.hiscox.de/cyber-readiness-report-2023/

Pressekontakt:

Leo Molatore
Telefon: +49 (0) 89 54 58 01 566
E-Mail: presse@hiscox.de

Unternehmen

HISCOX
Arnulfstraße 31
80636 München

Internet: www.hiscox.de

Über HISCOX

Hiscox ist ein internationaler Spezialversicherer mit einem auf die Absicherung beruflicher Risiken, privater Vermögenswerte und Spezialrisiken fokussierten Versicherungsportfolio. Gegründet vor über 100 Jahren ist das Unternehmen an der London Stock Exchange notiert (LSE:HSX) und hat Büros in vierzehn Ländern. Kunden mit hochwertigem Privatbesitz bietet Hiscox Versicherungen mit einer umfassenden Allgefahrendeckung, insbesondere für Kunst, wertvollen Hausrat, Ferienhäuser und Oldtimer sowie Lösegeldversicherungen. Für Kunstsammlungen und Kunstausstellungen bietet Hiscox spezielle Konzepte an. Für Geschäftskunden bietet Hiscox branchenspezifische Vermögensschadenhaftpflicht-, D&O- und Cyberversicherungen, die auf mittelständische Dienstleistungsunternehmen zugeschnitten sind. Hier konzentriert sich Hiscox auf die IT-, Medien, Telekommunikations- sowie Unternehmensberatungsbranche.