Hiscox Cyber Readiness Report 2024: Zahl der Angriffe wieder deutlich gestiegen – Cyber-Resilienz ist wichtiges Unternehmensziel

60 % der befragten Unternehmen wurden häufiger Opfer von Cyber-Angriffen / 46 % verloren aufgrund von Angriffen Kunden / Für ein Viertel entstanden Kosten von über 500.000 € / 79 % sehen Cyber-Resilienz als ein wichtiges bzw. sehr wichtiges Unternehmensziel / Ein Drittel brauchte nach Cyber-Attacke mehr als einen Monat bis zur vollständigen Wiederherstellung des regulären Betriebs

München (24. Oktober 2024) – Hiscox veröffentlicht die Ergebnisse des diesjährigen Cyber Readiness Reports. Die repräsentative und internationale Befragung wird seit 2016 jährlich durchgeführt. Der Report zeigt deutlich, dass sowohl die Gefahren durch Cyber-Angriffe als auch das Bewusstsein für Cyber-Risiken gestiegen sind: In Deutschland gaben 60 % der Befragten an, dass sie 2024 häufiger als im Vorjahr angegriffen wurden – diese Zahl ist gegenüber dem Vorjahr nochmal angestiegen (2023 gaben 58 % an, häufiger als im Jahr zuvor attackiert worden zu sein). Im Durchschnitt wurden deutsche Unternehmen binnen 12 Monaten 49-mal von Cyber-Kriminellen attackiert (erfolgreiche und abgewehrte Angriffe zusammengerechnet).

Reputationsschäden und Betriebsunterbrechungen durch Cyber-Angriffe können zu erheblichen Geschäftseinbußen führen

Reputationsschäden sind ein wichtiger Faktor im Zusammenhang mit Cyber-Angriffen: Die Hälfte der Befragten gab an, dass es für sie als Folge eines öffentlich bekannt gewordenen Angriffs schwieriger gewesen sei, neue Kundschaft zu gewinnen. Bei 46 % waren die Folgen schwerwiegender und sie verloren sogar Kundinnen bzw. Kunden.

Die Kosten der Angriffe variieren so stark wie die Arten der Angriffe selbst: Die Mehrheit (52 %) der angegriffenen Unternehmen verzeichnete Folgekosten von unter 100.000 Euro; gleichzeitig erlitt ein Viertel der Firmen Gesamtschäden von über 500.000 €. Neben finanziellen Schäden belastet die Unternehmen aber auch besonders die Dauer, bis der Zustand vor dem Angriff wieder hergestellt werden kann. Dies kann in vielen Fällen Wochen dauern: 26 % der Befragten gab an, dass sie Betriebsunterbrechungen von zwei bis vier Wochen verkraften mussten. Bei 30 % dauerte der Prozess sogar ein bis drei Monate, bei 7 % noch länger.

„Um eine langanhaltende Betriebsunterbrechung nach einer Cyber-Attacke zu vermeiden, ist es insbesondere für kleinere und mittelständische Firmen essenziell, neben Maßnahmen für eine angemessene Cyber-Resilienz auch eine Cyber-Versicherung abzuschließen. Neben der finanziellen Unterstützung im Schadenfall können versicherte Unternehmen über die in einer guten Cyber-Police enthaltenen Assistance-Leistungen auf rasche Unterstützung von Experten wie IT-Forensiker, Datenrechtsanwälte oder Krisen-PR-Berater zählen, um schnell wieder zum operativen Tagesgeschäft zurückkehren zu können“, sagt Gisa Kimmerle, Head of Cyber bei Hiscox.

Zahlungsumleitungsbetrug liegt wieder an erster Stelle

Die Schadenarten verteilen sich ähnlich wie in den vergangenen Jahren: Auf Platz 1 mit 55% lag wieder Zahlungsumleitungsbetrug (Payment Diversion Fraud), wobei Cyber-Kriminelle häufig vorgeblich geänderte Bankdaten von Dienstleistern verschicken und sich so Zahlungen erschleichen. 56 % der betroffenen Unternehmen erlitten auf diese Weise finanzielle Schäden. 47 % der betroffenen Unternehmen wurden von ‚Distributed denial of service‘ (DDoS)-Attacken getroffen, bei welchen ein Server gezielt mit so vielen Anfragen bombardiert wird, dass er die Menge nicht mehr bewältigen kann, den Dienst verweigert und im schlimmsten Fall zusammenbricht. 46 % berichten über einen Missbrauch

ihrer IT-Ressourcen, etwa wenn Hacker die Firmen-IT-Infrastruktur für ein Botnetz oder das Hosten von Malware verwenden.

Das häufigste Eintrittstor für Cyber-Angriffe war im vergangenen Jahr mit 55 % Unternehmens-Server in der Cloud. Angreifer dringen z.B. über Schwachstellen im Webserver oder die Kompromittierung von Zugangsdaten ein. Auch der Faktor Mensch spielt nach wie vor eine zentrale Rolle in der Cyber-Sicherheit, denn in 47 % der Fälle gelang Cyber-Kriminellen per Phishing bzw. Social Engineering über die Mitarbeitenden der Missbrauch von Unternehmensdaten. Ransomware ist auch weiterhin eine beliebte Methode von Cyber-Kriminalität. Häufige Methoden für erfolgreiche Angriffe waren neben Phishing-E-Mails auch die Entwendung von Zugangsdaten (49 %) und das Eindringen über ungepatchte Server (45 %).

Einige Unternehmen, die mit Ransomware angegriffen werden, neigen dazu, auf die Lösegeldforderung einzugehen, um langwierige Betriebsunterbrechungen zu vermeiden. Dass das meist keine gute Idee ist, zeigen die Ergebnisse der Befragung sehr klar: Nur 16 % gaben an, dass sie ihre Daten wieder vollständig zurückerhalten haben und 34 % konnten lediglich einen Teil ihrer Daten retten. In jeweils 22 % der Fälle funktionierte entweder der Wiederherstellungsschlüssel nicht oder die Erpresser forderten sogar noch mehr Geld. In 27 % der Fälle wurden die Daten trotz Zahlung dennoch geleakt.

Erhöhte Cyber-Kriminalität steigert Bewusstsein für Cyber-Resilienz – aber Absicherung de facto oft unzureichend

Die gute Nachricht: Diese gestiegene Aktivität von Cyber-Kriminellen sorgt bei Unternehmen für ein höheres Bewusstsein in Bezug auf Cyber-Sicherheit und -Resilienz. 79 % der befragten Firmen sehen in der eigenen Cyber-Resilienz ein wichtiges bzw. sehr wichtiges Unternehmensziel. Die Budgets für IT-Sicherheitsmaßnahmen reflektieren diese Aussage: 45 % der Befragten gaben an, dass ihr Unternehmen zwischen 6 % und 10 % den gesamten IT-Budgets für Cyber-Security ausgeben, 42 % sogar bis zu 15 % des IT-Budgets. Teil dieses Budgets entfällt auf dedizierte Personen bzw. Teams, die für Cyber-Security zuständig sind: 76 % der befragten Unternehmen haben diese klaren Zuständigkeiten bereits umgesetzt.

Stellt man jedoch gezielte Fragen zur Umsetzung dieses wichtigen Ziels in der Praxis, zeigt sich ein deutlich weniger positives Bild: Aufgrund der Antworten nach vorhandenen Maßnahmen zeigt sich, dass 8 % nur über eine minimale Resilienz verfügen und lediglich auf Cyber-Vorfälle reagieren. 28 % werden als „ad hoc“ eingestuft: Sie haben zwar einige formale Prozesse integriert, aber die Umsetzung von Cyber-Maßnahmen ist uneinheitlich und oft reaktiv. 33 % der Unternehmen können zumindest eine Basis-Resilienz vorweisen, welche dokumentierte und regelmäßige Prozesse umfasst, bei denen das Mitarbeiterwissen zum Thema Cyber-Sicherheit jedoch nur auf einem mittleren Niveau vorhanden ist. Nur bei 26% aller deutschen Unternehmen kann die Cyber-Resilienz tatsächlich als „fortgeschritten“ eingestuft werden, da sie integrierte Prozesse mit Metriken zur Nachverfolgung in der gesamten Organisation etabliert haben, eine proaktive Incident Response praktizieren und ein Hohes Maß von Mitarbeiter-Schulungen vorweisen können. An der Spitze stehen nur 4 %, die über eine vorbildliche Resilienz mit Best-in-Class-Praktiken verfügen, die vollständig in die Geschäftsstrategie integriert sind und kontinuierlich verbessert werden. Dazu kommt eine starke Zusammenarbeit mit externen Partnern und Stakeholdern.

Was sind die Hauptgründe, die einer höheren Cyber-Resilienz konkret entgegenstehen? Am häufigsten nannten die Befragten die sich rapide ändernden Cyber-Bedrohungen (43 %), gefolgt von limitierten Budgets für Cyber-Sicherheit (42 %) und zu wenig Verständnis bzw. Aufmerksamkeit für Cyber-Risiken bei Mitarbeitenden (38 %).

„Es ist besorgniserregend, wie viele Unternehmen in der Praxis noch immer zu wenige Maßnahmen zur Verbesserung ihrer Cyber-Sicherheit treffen. Zwar haben die meisten Unternehmen Cyber Readiness weit oben auf ihrer Agenda, die Realität sieht hingegen oft anders aus. Das Thema Digital Trust ist für viele Geschäftspartner aber auch für Kunden inzwischen ein wesentlicher Faktor für die Zusammenarbeit und entwickelt sich immer mehr zu einer Voraussetzung für Unternehmen, um wettbewerbsfähig zu bleiben. Robuste Sicherheitsmaßnahmen, Schutz von Daten, integrierte Prozesse für den Ernstfall und eine gute Cyber-Versicherung sind angesichts der Bedrohungslage die Grundlage vertrauensvoller Geschäftsbeziehungen“, betont Gisa Kimmerle.

Über die Studie:
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.

Weitere Informationen finden Sie online unter:
www.hiscox.de/research/hiscox-cyber-readiness-report

Für weitere Informationen stehen wir Ihnen gerne zur Verfügung:

Hiscox
Leo Molatore
Bernhard-Wicki-Str. 3
80636 München
+49 (0) 89 54 58 01 566
presse@hiscox.de

LHLK Agentur für Kommunikation
Eva-Maria Gose-Fehlisch
Tegernseer Platz 7
81541 München
+49 (0) 89 72 01 87 224
hiscox@lhlk.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. Weitere Informationen finden Sie unter: www.hiscox.de