Die Mehrheit der deutschen Unternehmen ist schlecht auf Cyber-Attacken vorbereitet

Hiscox_Robert Dietrich © HISCOX

Internationale Studie von Hiscox und Forrester zeigt: Deutsche Unternehmen haben Nachholbedarf in Sachen Cyber-Sicherheit / Im Ländervergleich liegen deutsche Unternehmen bei Cyber-Risk-Management deutlich hinter den USA und Großbritannien / Fokus auf Investitionen in IT-Infrastruktur, umfassende Cyber-Risk-Strategie wird vernachlässigt / Aufklärungsbedarf bei Cyber-Versicherungen

Der „Cyber Readiness Report 2017“ des Spezialversicherers Hiscox zeigt, wie gut oder schlecht deutsche, britische und US-amerikanische Unternehmen auf Cyber-Attacken vorbereitet sind. Das Marktforschungsinstitut Forrester Consulting hat dazu im Auftrag von Hiscox die „Cyber-Readiness“ von je rund 1.000 Unternehmen in den drei Ländern anhand der Kriterien Strategie, Ressourcen, Technologie sowie Prozesse ermittelt. Schlechte Noten erhalten vor allem die deutschen Unternehmen: Mit 62 Prozent weist Deutschland im Ländervergleich (USA: 40%; GB: 57%) den höchsten Anteil an Unternehmen auf, die als sogenannte „Cyber-Anfänger“ gelten, also unzureichend auf Cyber-Attacken vorbereitet sind. Der Anteil der „Cyber-Experten“ liegt in Deutschland bei lediglich 20 Prozent, wohingegen 44 Prozent der befragten US-Unternehmen gut gegen Cyber-Attacken gerüstet sind (GB: 26%). 18 Prozent der deutschen Befragten zählen zu den „Cyber-Fortgeschrittenen“, die zumindest teilweise mit den Folgen einer Cyber-Attacke klarkommen können (USA: 16%; GB 17%).

Nur eine umfassende Strategie hilft, Cyber-Attacken zu bewältigen

„Die Anzahl der schlecht gegen Cyber-Attacken gerüsteten Unternehmen in Deutschland ist erschreckend hoch. Bei gut vorbereiteten Unternehmen ist IT-Security ein Top-Management-Thema und es existiert eine klare Strategie. Der Fokus muss dabei auf zeitgemäßen Prozessen und Richtlinien, laufenden Investitionen in die technische IT-Security, Sensibilisierung und

Schulung der Mitarbeiter und auf spezifischem Cyber-Versicherungsschutz liegen. Wer eines dieser Handlungsfelder vernachlässigt, läuft Gefahr, durch Cyber-Attacken nachhaltig geschädigt zu werden. Kein Unternehmen kann sich absolut vor Cyber-Attacken schützen, aber es kann die Schäden klein halten“, erläutert Robert Dietrich, Hauptbevollmächtigter bei Hiscox Deutschland.

Gezielte Cyber-Attacken auf wichtige Branchen der deutschen Wirtschaft

Dass Attacken zum Alltag gehören, zeigt auch die Studie: 56 Prozent der befragten deutschen Unternehmen haben im vergangenen Jahr mindestens einen Angriff auf ihre Netzwerke und Daten festgestellt (USA: 63%; GB: 51%). Besonders stark betroffen waren hierzulande die Fertigungsindustrie und die Medien-, Kommunikations- und Technologiebranche, in denen jeweils 65 Prozent der befragten Unternehmen mindestens eine Cyber-Attacke feststellten – gefolgt von der Finanzdienstleistungs-branche (64%).

Cyber-Strategie muss Chefsache sein

Die Diskrepanz zwischen „Cyber-Anfängern“ und „Cyber-Experten“ manifestiert sich beispielsweise in der Rolle des Top-Managements. Während in den deutschen Unternehmen mit „Experten-Status“ insgesamt 88 Prozent der Befragten der Aussage „Cyber-Sicherheit muss Chefsache sein“ zustimmen (USA: 93%; GB: 91%), sind es bei den Anfängern nur 58 Prozent (USA: 70%; GB: 62%).

Risikofaktor Mitarbeiter: Potential von Cyber-Schulungen bislang verkannt

Zwar nehmen externe Cyber-Attacken den ersten Platz auf der Liste der folgenschwersten Cyber-Angriffe bei deutschen Unternehmen ein (DE: 38%; USA: 25%; GB: 34%). Auf Platz zwei und drei folgen aber schon die Cyber-Zwischenfälle durch Mitarbeiter: Bei jedem fünften deutschen Unternehmen (20%) konnten die Verantwortlichen innerhalb der Organisation ausgemacht werden (USA: 22%; GB: 16%), 14 Prozent der Befragten berichteten von verlorengegangenen bzw. gestohlenen mobilen Geräten, wie Firmenhandys oder -tablets (USA: 17%; GB: 18%).

Trotz dieser alarmierenden Ergebnisse vernachlässigen die deutschen Befragten das Thema Sensibilisierung und Schulung von Mitarbeitern bislang. So verpflichtet gegenwärtig nur jedes vierte Unternehmen in Deutschland (24%) seine Mitarbeiter zur Teilnahme an speziellen Cyber-Trainings (USA: 34%; GB: 25%). Jedoch wollen sich die deutschen Unternehmen für die Zukunft wappnen: 57 Prozent der deutschen Befragten planen, in den kommenden zwölf Monaten die Investitionen für Mitarbeiterschulungen um mehr als fünf Prozent zu erhöhen (USA: 64%; GB: 57%). Einen größeren Stellenwert nehmen hierzulande aber weiterhin Investitionen in neue IT-Sicherheitstechnologien ein: 68 Prozent der Befragten haben vor, das Budget dafür im kommenden Jahr um mehr als fünf Prozent zu steigern (USA: 71%; GB: 67%).

„Investitionen in die IT sind sinnvoll und notwendig, doch sie gaukeln eine trügerische Sicherheit vor, die den in der Realität immer komplexer werdenden Risiken aus dem Netz nicht gerecht werden. Der Faktor Mensch wird bei Investitionsentscheidungen immer noch hintenangestellt, obwohl ein Großteil der Cyber-Attacken durch Mitarbeiter verursacht wird. Dabei bieten gezielte Mitarbeitertrainings das größte Präventionspotential zur Vermeidung von Cyber-Zwischenfällen oder zumindest zur Minimierung ihres Ausmaßes. Sie lassen sich mit relativ überschaubarem Budget umsetzen und ermöglichen insbesondere kleinen und mittleren Unternehmen, ihre ‚Cyber-Readiness‘ zu verbessern“, verdeutlicht Robert Dietrich.

Deutsche Unternehmen zeigen sich skeptisch gegenüber Cyber-Versicherungen

Auch der Abschluss einer Cyber-Police als zentrales Strategie-Element wird noch von vielen deutschen Unternehmen vernachlässigt. Hierzulande liegt der Anteil der versicherten Unternehmen mit 30 Prozent merklich hinter den USA (55%) und Großbritannien (36%). Jedoch

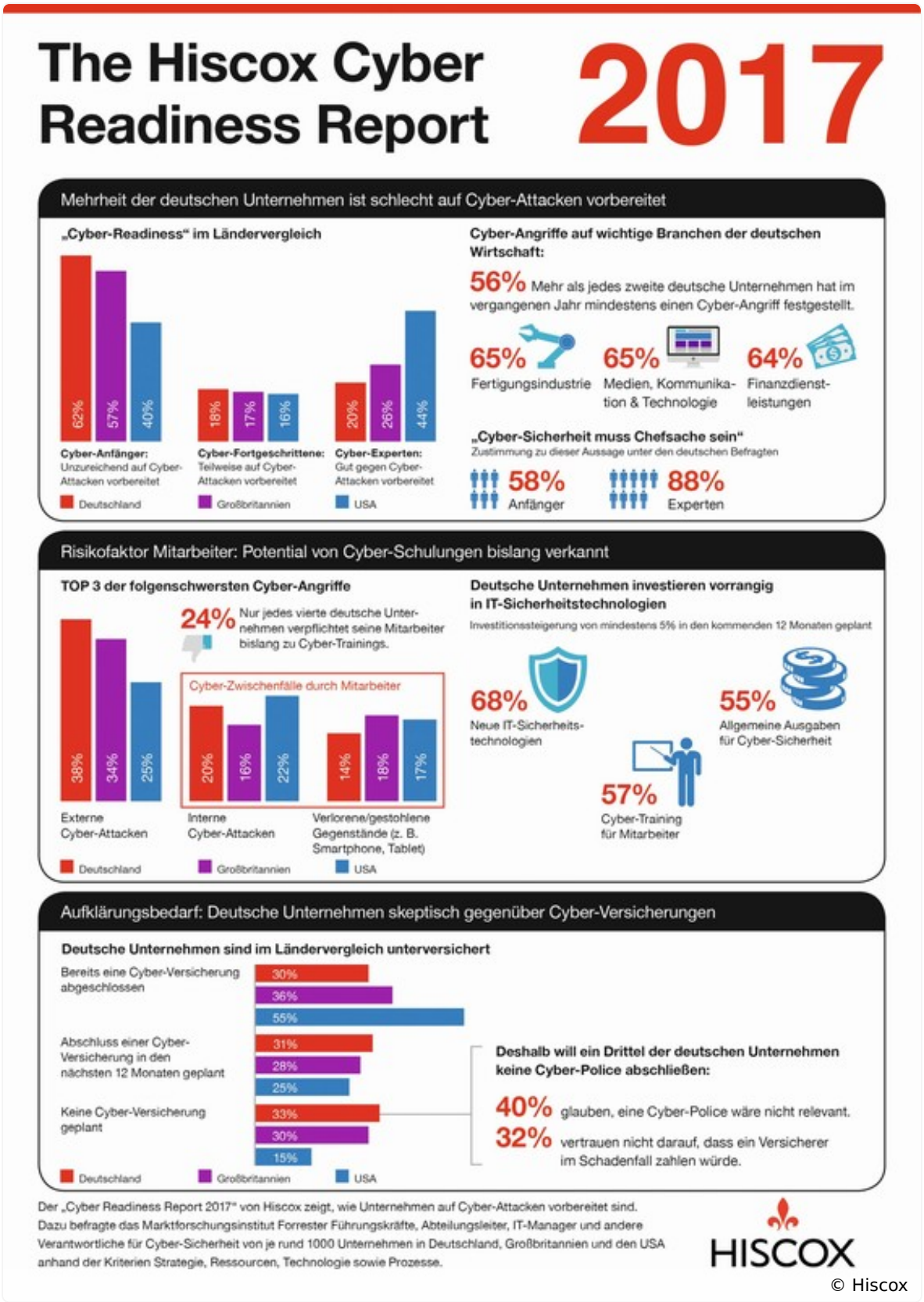
plant nahezu jedes dritte deutsche Unternehmen (31%), das noch keine Cyber-Police abgeschlossen hat, dies innerhalb der nächsten zwölf Monate nachzuholen. Ihnen gegenüber steht aber immer noch ein Drittel (33%), das kein Interesse an einer Cyber-Police hat. 40 Prozent von ihnen glauben, eine Cyber-Versicherung wäre für sie nicht relevant und 32 Prozent vertrauen nicht darauf, dass ein Versicherer im Schadenfall überhaupt zahlen würde.

„Diesem hohen Anteil an Unternehmen, die keine Cyber-Police abschließen möchten, ist der Nutzen einer zusätzlichen Absicherung noch immer nicht klar. Hier fehlt es an Aufklärung, vor allem zu den Risiken und den damit verbundenen Kosten, aber auch zu den Leistungen einer Cyber-Versicherung. Denn nach wie vor gehen Unternehmen davon aus, dass Cyber-Schäden von ihrer Gewerbeversicherung gedeckt sind. Wir als Versicherer sind also gefragt, das öffentliche Bewusstsein für Cyber-Gefahren zu schärfen und transparente Produkte zu schaffen, um das Vertrauen der Wirtschaft zu gewinnen“, so Robert Dietrich.

Im Ernstfall: Krisenmanagement aus einer Hand

Besonders die zusätzlichen Leistungen im Rahmen von Cyber-Policen stoßen bei Unternehmen auf reges Interesse. Von den deutschen Unternehmen, die bereits eine Cyber-Versicherung haben oder planen, in den nächsten zwölf Monaten eine abzuschließen, gaben 44 Prozent an, sie würden die Beratungsleistungen ihres Versicherers in Anspruch nehmen. 41 Prozent würden Angebote des Versicherers zu präventiver Hard- oder Software nutzen und 40 Prozent interessieren sich für Mitarbeitertrainings.

Der vollständige „Hiscox Cyber Readiness Report 2017“ und weitere Informationen zur Studie sind unter www.hiscox.de/hiscox-cyber-readiness-report-2017 verfügbar.



Pressekontakt:

Yvonne Kautzner
Telefon: +49 (0) 89 54 58 01 566
E-Mail: yvonne.kautzner@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.

Pressekontakt:

Eva Weis
Telefon: +49 (0) 89 72 01 87 23
E-Mail: e.weis@lhlk.de

Unternehmen

LoeschHundLiepold Kommunikation
Tegernseer Platz 7
81541 München

Internet: www.lhlk.de