Auf Selbstüberschätzung folgt Realismus: Deutsche Unternehmen erkennen ihr mangelndes Cyber-Know-how

Hiscox_Robert Dietrich © HISCOX

Cyber-Risiko wächst / 61% der deutschen Unternehmen erlebten im letzten Jahr mindestens eine Cyber-Attacke / Durchschnittliche Schadenhöhe steigt international im Vergleich zum Vorjahr um 61% / Cyber-Kriminelle finden neue Einfallstore wie die vernetzte Lieferkette / 70% der deutschen Unternehmen sind Cyber-Anfänger / Unternehmen zeigen sich mit Blick auf Cyber-Kompetenz weniger selbstbewusst / Realistische Selbsteinschätzung bietet Verbesserungspotenzial für Prävention

Die Ergebnisse des Cyber Readiness Reports aus den vergangenen Jahren legen eine Vermutung nahe: Trotz zunehmender Digitalisierung und Vernetzung, zunehmender Aufklärung vor Cyber-Gefahren und zahlreicher medienwirksamer Hacker-Angriffe vernachlässigen viele Unternehmen ihr Cyber-Risikomanagement. Dies verdeutlicht unter anderem die konstant hohe Anzahl an schlecht vorbereiteten „Cyber-Anfängern“, die die Studie jährlich ermittelt. (Cyber-Anfänger in Deutschland laut Report 2019: 70%; 2018: 77%) Die Daten basieren auf einer Umfrage unter 5.392 Unternehmen aus Deutschland, den USA, Großbritannien, Frankreich, Spanien, Belgien und den Niederlanden. Im Auftrag des Spezialversicherers Hiscox befragte das Marktforschungsinstitut Forrester Consulting Führungskräfte, Abteilungsleiter, IT-Manager und Verantwortliche für Cyber-Sicherheit zu ihren Erfahrungen sowie ihrem Umgang mit Cyber-Attacken.

Mangelndes Cyber-Know-how auf Unternehmensseite
Gemessen an den Kriterien Strategie, Ressourcen, Technologie und Prozesse zählt nach wie vor die überwiegende Mehrheit (70%) der befragten deutschen Unternehmen zu den sogenannten Cyber-Anfängern. Auf den Fall eines Cyber-Angriffs sind sie nur unzureichend vorbereitet. 19%

gelten als Fortgeschrittene und nur 11% als Cyber-Experten (Report 2018: 77% Anfänger; 14% Fortgeschrittene; 10% Experten).

Cyber-Selbstbewusstsein der Unternehmen sinkt

Während sich die Cyber-Abwehrbereitschaft der Unternehmen nur leicht verbessert hat, wächst zumindest das Bewusstsein für den mangelnden Schutz: Seit 2017 sinken die Zustimmungswerte in Bezug darauf, wie selbstbewusst Unternehmen ihrer Cyber-Strategie gegenüberstehen. So gaben beispielsweise im Report 2019 nur noch 59% der international Befragten an, dass ihre Geschäftsleitung eine klare Vorstellung davon hat, wie Cyber-Sicherheit gemanagt werden muss. Im Report 2018 stimmten dieser Aussage noch 61% zu und 2017 sogar 75%. Diese Entwicklung spricht dafür, dass sich der Kenntnisstand der Unternehmen rund um Cyber-Risiken gebessert hat und sie ihre Abwehrkompetenzen im Vergleich zu den Vorjahren nicht mehr überschätzen.

Erste Verbesserungen im Umgang mit digitalen Risiken

Obwohl die überwiegende Mehrheit der Befragten keine Cyber-Experten sind, zeigen sich dennoch Verbesserungen im Umgang mit digitalen Gefahren. Immer mehr Unternehmen in Deutschland verfügen über einen Mitarbeiter, der dezidiert für Cyber-Risiken zuständig ist (Report 2019: 85%; 2018: 69%). Außerdem reagieren mehr Firmen mit konkreten Gegenmaßnahmen, wenn sie Opfer eines Cyber-Angriffs wurden. Nur noch 32% der betroffenen deutschen Unternehmen gaben an, dass sich nach einer Attacke nichts geändert hat (Report 2018: 45%). Im Zuge regulatorischer Maßnahmen wie der Einführung der DSGVO haben 21% der deutschen Firmen 2018 verstärkt in Mitarbeitertrainings investiert. Zudem planen deutsche Firmen 11% ihres gesamten IT-Budgets 2019 in Cyber-Sicherheitsmaßnahmen zu investieren, womit die Investitionsbereitschaft 2 Prozentpunkte über der aller in der Studie befragten Unternehmen liegt (9% gemessen am IT-Budget).

Mehr Unternehmen setzen auf Cyber-Versicherungen

Zur Absicherung ihrer Risiken haben international bereits 41% der Studienteilnehmer eine Cyber-Versicherung abgeschlossen (Report 2018: 33%), 30% planen einen Abschluss innerhalb der nächsten 12 Monate (Report 2018: 25%). In Deutschland gaben 34% an, durch eine Cyber-Versicherung vor den Folgen eines Cyber-Schadens geschützt zu sein.

„In der vernetzten Business-Welt werden digitale Gefahren schnell zum Geschäftshemmnis. Um Cyber-Risiken kalkulierbar machen zu können, muss jedes Unternehmen die individuellen Schwachstellen kennen und und richtig absichern. Standard-Gewerbeversicherungen schützen jedoch nicht ausreichend vor Schäden durch Cyber-Angriffe, auch wenn sich dieser Irrglaube hartnäckig hält“, kommentiert Robert Dietrich, Managing Director Germany der Hiscox SA. „Eine gute Cyber-Versicherung unterstützt Unternehmen präventiv, um Risiken von vornherein zu reduzieren, hilft schnell und unbürokratisch im Schadenfall und danach, um die Angriffsfläche für die Zukunft zu minimieren.“

Anzahl der Cyber-Attacken und Schadenhöhen steigen drastisch

Die Ergebnisse der Studie verdeutlichen, dass Cyber-Risikokomanagement auf der Agenda jeder Firmenleitung stehen sollte: Die Frequenz von Cyber-Einschlägen steigt weiter und die Folgen der Angriffe für die Unternehmen werden immer teurer. 61% der befragten deutschen Firmen waren in den vergangenen 12 Monaten von mindestens einer Cyber-Attacke betroffen (Report 2018: 48%). Mit einem Anteil von 30% erlebten in den befragten Ländern zudem mehr Unternehmen vier oder sogar mehr Angriffe, während laut dem Report 2018 noch 20% so oft attackiert wurden. Eine Erklärung für den Anstieg könnte die 2018 in Kraft getretene Europäische Datenschutz-Grundverordnung sein, da seitdem 84% aller befragten europäischen Firmen im Panel verstärkt

in Maßnahmen zur Detektion und Meldung von Cyber-Vorfällen investiert haben. Die durchschnittlichen Kosten aus allen erlittenen Cyber-Zwischenfällen pro Unternehmen stiegen international von 229.000 US-Dollar (Report 2018) auf 369.000 US-Dollar, was einem Zuwachs von 61% entspricht. Aufgrund einzelner besonders hoher Schadenfälle vermeldeten betroffene deutsche Unternehmen eine durchschnittliche Schadenhöhe von besonders hohen 906.000 US-Dollar.

Cyber-Angriffe treffen häufiger auch den Mittelstand
Die steigenden Angriffszahlen bekommen vor allem kleine und mittlere Unternehmen verstärkt zu spüren. In allen untersuchten Ländern wurden 47% der kleinen und 63% der mittelgroßen Firmen Opfer von Cyber-Attacken (2018: kleine Firmen: 33%; mittlere Firmen: 36%). 23% der Unternehmen mit bis zu 999 Mitarbeitern fielen dabei Schadsoftware wie Viren oder Würmern zum Opfer, 20% mussten mit Datenschutzverletzungen und dem Verlust von Mitarbeiter- und Kundendaten umgehen und 15% erlitten eine Ransomware-Attacke.

„Der Anstieg von Schadenfällen und -summen verwundert uns nicht und deckt sich mit unserer Schadenpraxis. Die wenigsten Firmen beschäftigen sich aktiv mit Cyber-Krisenmanagement und das Niveau von Schutz- und Präventionsmaßnahmen ist in vielen Unternehmen nach wie vor bedenklich. Diesen Vorteil können Cyber-Kriminelle leicht für sich nutzen. Entscheider müssen realisieren, dass Cyber-Kriminalität ein reales Geschäftsrisiko der digitalisierten Welt ist, und nicht nur eine Modeerscheinung“, erläutert Robert Dietrich.

Der „Hiscox Cyber Readiness Report 2019“ und weitere Informationen zur Studie sind unter www.hiscox.de/cyber-readiness-report-2019 verfügbar.

Für weitere Informationen stehen wir Ihnen gerne zur Verfügung:

Hiscox
Yvonne Kautzner
+49 (0) 89 54 58 01 566
yvonne.kautzner@hiscox.de

Franziska Schaefer
Arnulfstraße 31
80636 München

LoeschHundLiepold Kommunikation
Sabina Howacker
+49 (0) 89 72 01 87 18
hiscox@lhlk.de