Wie Sie zum Best-Practice-Unternehmen in Sachen Cyber-Sicherheit werden

Kelkheim, 14. März 2017

Flickr: elhombredenegro CC Lizenz

Nach dem „Hiscox Cyber Readiness Report 2017“ sind nur 20 Prozent der deutschen Unternehmen gut auf eine Cyber-Attacke vorbereitet. Sie werden als so genannte „Cyber-Experten“ bewertet. Doch was unterscheidet diese 20 Prozent von den 62 Prozent der Unternehmen, die so ungenügend auf Cyber-Attacken vorbereitet sind, dass sie als „Cyber-Anfänger“ kategorisiert werden bzw. den 18 Prozent, die immerhin schon „Cyber-Fortgeschrittene“ sind?

Es gibt noch viel zu tun

Den deutschen Unternehmen ist mehrheitlich bewusst, dass sie noch viel zu tun haben, wenn es um den Bereich IT-Sicherheit geht. Deshalb plant die Mehrheit von ihnen für die kommenden 12 Monate auch mindestens 5 Prozent mehr Budget für Investitionen in die Sicherheit ihrer IT ein, dabei liegt der Fokus auf neuen Sicherheitstechnologien. 61 Prozent wollen gezielt ihre Schwachstellen angehen. Aber was kann man ihnen empfehlen? Ein Blick auf die 20 Prozent Best-Practice-Unternehmen zeigt, was diese besser machen.

Die meisten der befragten Unternehmen sind, wenn es um die Sicherheitstechnologien geht bereits gut aufgestellt. Hier gibt es den geringsten Nachholbedarf; nur im Bereich Nachrichtenverschlüsselung könnte es noch besser werden.

Was machen Cyber-Security-Experten besser?

Der größte Unterschied zwischen Cyber-Anfängern und -Experten liegt in den Bereichen Strategie und Prozesse. Während in den Best-Practice- Unternehmen rund 88 Prozent der Befragten Cyber-Sicherheit als Chefsache ansehen, sind es bei den als Anfänger eingestuften Unternehmen nur 58 Prozent.

Bei den Experten wird also das Top-Management in die Cyber-Strategie miteinbezogen und ist wesentlich an der Entwicklung eines formalisierten Cyber-Sicherheitsstrategie beteiligt. Es sind klar definierte Strukturen und Prozesse entwickelt worden, die allen bekannt sind.

Zudem gibt es Cyber-Security-Guidelines für Mitarbeiter, Partner und Externe. Alle werden regelmäßig geschult und getestet, um zu gewährleisten, dass die Richtlinien eingehalten werden. Die Schulung der Mitarbeiter ist dabei insgesamt ein wesentlicher Teil des Cyber-Sicherheitskonzepts. Denn nur sensibilisierte und gut trainierte Mitarbeiter können mithelfen, Attacken zu vermeiden. Die Personalabteilung ist mit eingebunden und sorgt für die Weiterbildung der Mitarbeiter.

Der letzte Baustein eines umfassenden Cyber-Risk-Managements ist eine Cyber-Versicherung. Fast zwei Drittel der „Cyber-Experten“ verfügen über eine Cyber-Police. Ein Großteil der Experten plant zudem, den Cyber-Schutz in den nächsten 12 Monaten weiter auszubauen. Denn den Experten ist bewusst: Ganz gleich, wie viel sie in IT-Sicherheitstechnologien und in die Schulung der Mitarbeiter investieren, die Gefahr eines Cyber-Angriffes kann man zwar reduzieren, aber nie ganz eliminieren. Daher schützen sie sich durch eine Cyber-Versicherung vor den Restrisiken.

Über die gb.online gmbh

Die gb.online gmbh hat sich auf die berufliche Absicherung von Freelancern spezialisiert und bietet mit www.easy-insure.eu das umfangreichste Online-Versicherungsportal für freie und beratende Berufe in Deutschland. Seit 2011 können Selbstständige und Unternehmen bis 1 Million Euro Umsatz pro Jahr hier ihre beruflichen Risiken versichern.

Steigt der Umsatz, und wird eine individuelle Lösung benötigt, so steht mit dem Schwesterunternehmen groot bramel versicherungsmakler gmbh ein verlässlicher Partner zur Seite, der seit über 25 Jahren Gewerbetreibende und industriellen Unternehmen in Versicherungsfragen vertritt. Die groot bramel versicherungsmakler gmbh ist in 18 Ländern vertreten und begleitet sie, wohin auch immer sich ihr Geschäftsfeld entwickelt.

Kontaktdaten

gb.online gmbh
Frankfurter Straße 93
65779 Kelkheim

Ansprechpartner: Lutz-Hendrik Groot Bramel, Geschäftsführer

Folgen Sie uns auch auf	

Hiscox Cyber Readiness Report 2017 – Mehrheit deutscher Unternehmen als „Cyber-

Anfänger“ einzustufen

Kelkheim, 03. März 2017

Der „Hiscox Cyber Readiness Report 2017“ ist erschienen – und bringt teilweise erschreckende Erkenntnisse zu Tage. Fast 40 Prozent der deutschen Unternehmen hinken im internationalen Vergleich deutlich hinterher, wenn es um Cyber-Sicherheit geht.

Flickr: elhombredenegro CC Lizenz

Für den „Hiscox Cyber Readiness Report 2017“ wurden über 3000 Führungskräfte, Abteilungsleiter, IT-Manager und andere für die Cyber-Sicherheit verantwortliche Mitarbeiter von Unternehmen befragt; je rund 1000 in Deutschland, Großbritannien und USA. Die Befragten sollten eine Selbsteinschätzung zu ihrer Cyber-Security-Strategie, ihren Ressourcen, ihren Prozessen und ihrer Technologie abgeben. Auf Basis dieser Einschätzung wurden die Unternehmen in die Kategorien „Cyber-Anfänger“, „Cyber-Fortgeschrittene“ und „Cyber-Experten“ eingeteilt. Als Anfänger zählt, wer nur unzureichend auf

Cyber-Attacken vorbereitet ist, Cyber-Fortgeschrittene sind zumindest teilweise für einen Angriff gewappnet. Nur wer gut geschützt auf einen Cyber-Angriff reagieren kann, gilt als Cyber-Experte.

Deutschland ist Nachzügler bei IT-Sicherheit

Das Bild, das sich abzeichnete, ist eindeutig: Deutschland ist Nachzügler, was das Thema IT-Sicherheit angeht. Während in den USA 40 Prozent der Unternehmen als „Cyber-Anfänger", also als unzureichend gegen Cyber-Attacken geschützt, einzustufen sind, sind es in Deutschland ganze 62 Prozent. Großbritannien liegt mit 57 Prozent in der Mitte.

Als gut geschützt können in Deutschland lediglich 20 Prozent der Unternehmen angesehen werden. Im Vergleich: 44 Prozent, also mehr als doppelt so viele, der befragten US-Unternehmen sind gut gegen Cyber-Attacken gerüstet, in Großbritannien sind es 26 Prozent.

Mehr als die Hälfte der deutschen Unternehmen wurde schon einmal attackiert

Dieses schlechte Abschneiden der deutschen Unternehmen ist umso erstaunlicher, wenn man sich dazu die Zahlen der Cyber-Attacken im vergangenen Jahr anschaut: 56 Prozent der befragten deutschen Unternehmen haben 2016 einen Angriff auf ihre Netzwerke und Daten verzeichnet.

Besonders oft werden hierzulande Unternehmen aus der Fertigungsindustrie, den Medien sowie den Branchen Kommunikation und Technologie Ziel von Cyber-Attacken. Hier haben jeweils 65 Prozent der befragten Unternehmen mindestens einen Cyber-Angriff entdeckt; knapp dahinter liegt die Finanzdienstleistungsbranche mit 64 Prozent.

Unterschätztes Risiko Mitarbeiter

Den Cyber-Angriff, den Unternehmen befürchten, ist die typische Hacker-Attacke von außen. Tatsächlich verursachen externe Angriffe mit 38 Prozent auch die meisten Cyber-Zwischenfälle. Auf Platz 2 und 3 folgen aber schon Zwischenfälle, die durch die eigenen Mitarbeiter hervorgerufen wurden: absichtlich oder unabsichtlich. Rund 20 Prozent der von Cyber-Attacken betroffenen Unternehmen stellten fest, dass der Verantwortliche innerhalb der eigenen Organisation

auszumachen war; weitere 14 Prozent berichteten von verlorenen oder gestohlenen mobilen Devices, wie Firmenhandys oder -tablets, als Ursache.

Obwohl ein Fünftel der Cyber-Attacken intern verschuldet werden, vernachlässigen deutsche Unternehmen das Thema Mitarbeiterschulung bzw. -sensibilisierung. Nur ein Viertel der Unternehmen führen verpflichtende Cyber-Trainings durch. Allerdings hat der Report hier auch etwas Positives zu berichten: Mehr als die Hälfte (57 Prozent) der befragten deutschen Unternehmen planen in den kommenden 12 Monaten mehr in die Cyber-Security-Schulung der Mitarbeiter zu investieren.

Cyber-Experten verfügen über eine Cyber-Versicherung

Dass Deutschland beim Thema Cyber-Security noch einiges aufzuholen hat, zeigt auch ein Blick auf die Anzahl der abgeschlossenen Cyber-Versicherungen. Während in den USA 55 Prozent der Unternehmen eine Cyber-Police besitzen, sind es in Deutschland nur 30 Prozent. Immerhin wollen etwa ein Drittel der deutschen Unternehmen, die noch über keine Cyber-Versicherung verfügen, dies in den kommenden 12 Monaten nachholen. Doch rund 40 Prozent glauben, sie bräuchten keine Versicherung: entweder weil sie überzeugt sind, gut genug abgesichert zu sein, nicht darauf vertrauen, dass der Versicherer im Schadenfall auch zahlen würde oder nicht wissen, dass es ein spezielles Versicherungsprodukt gibt, das Cyber-Risiken abdeckt.

Was kann Deutschland tun, um international den Anschluss zu bekommen?

Wie der Report zeigt, gibt es auch einige deutsche Unternehmen, die zu den Cyber-Experten gehören. Was können die Unternehmen aus den Kategorien Anfänger und Fortgeschrittene von den Experten lernen? Was die Experten besser machen erfahren Sie in unseren nächsten Artikel.

Über die gb.online gmbh

Die gb.online gmbh hat sich auf die berufliche Absicherung von Freelancern spezialisiert und bietet mit www.easy-insure.eu das umfangreichste Online-Versicherungsportal für freie und beratende Berufe in Deutschland. Seit 2011 können Selbstständige und Unternehmen bis 1 Million Euro Umsatz pro Jahr hier ihre beruflichen Risiken versichern.

Steigt der Umsatz, und wird eine individuelle Lösung benötigt, so steht mit dem Schwesterunternehmen groot bramel versicherungsmakler gmbh ein verlässlicher Partner zur Seite, der seit über 25 Jahren Gewerbetreibende und industriellen Unternehmen in Versicherungsfragen vertritt. Die groot bramel versicherungsmakler gmbh ist in 18 Ländern vertreten und begleitet sie, wohin auch immer sich ihr Geschäftsfeld entwickelt.

Kontaktdaten

gb.online gmbh
Frankfurter Straße 93
65779 Kelkheim

Ansprechpartner: Lutz-Hendrik Groot Bramel, Geschäftsführer

Folgen Sie uns auch auf	