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	