CYBERSCHUTZ – MASSNAHMENPROTOKOLL

ÜBERTRAGEN SIE JEMANDEM DIE VERANTWORTUNG FÜR DIE CYBER-SICHERHEIT

Nur wenige kleine Unternehmen haben einen Beauftragten für Cyber-Sicherheit. Dadurch wird die Identifikation, Nachverfolgung und Dokumentierung von Cyber-Angriffen erschwert, weil sich niemand verantwortlich fühlt. Außerdem werden die Möglichkeiten einer langfristigen Strategieplanung in diesem Bereich eingeschränkt.

zuständig: _____

erledigt am: _____

FÜHREN SIE PROZESSE EIN

Kleine Unternehmen hinken nicht notwendigerweise hinter großen Wirtschaftsunternehmen hinterher, wenn es um die Installation von Anti-Virus-, Anti-Spyware- und Anti-Malware-Technologien geht. Sie sind allerdings nicht so konsequent bei der Einführung zuverlässiger Prozesse, wie zum Beispiel bei der Erhebung von Daten in Bezug auf die Cyber-Sicherheit, bei der Integration von Cyber-Sicherheit in Planung, Vertrieb und interne Audits sowie bei der Überwachung und Dokumentation.

zuständig: _____

erledigt am: _____

FÜHREN SIE MEHR MITARBEITERSCHULUNGEN DURCH

Weniger als die Hälfte der kleinen Unternehmen (43 %) stimmten im Rahmen der Befragung zum Cyber Readiness Report 2019 zu, dass die Aussage „Die Organisation integriert Sicherheitsschulungen und die Sensibilisierung der gesamten Belegschaft“ ungefähr oder ganz genau ihren Ansatz beschreibt. Lediglich 29 % der kleinen Unternehmen erklärten, sie beabsichtigten im kommenden Jahr eine Erhöhung ihrer Ausgaben für Schulungen zur Sensibilisierung ihrer Mitarbeiter um mindestens 5 %. Alarmierend ist, dass ein Drittel der kleinen Unternehmen (33 %) im nächsten Jahr sogar ihr Budget für Cyber-Sicherheitsschulungen kürzen möchte.

zuständig: _____

erledigt am: _____

REAGIEREN SIE AUF DATENPANNEN MIT EFFEKTIVEN MASSNAHMEN

Nahezu die Hälfte der kleinen Unternehmen (45 %) ließen verlauten, sie hätten nach einem bzw. nach mehreren Cyber-Vorkommnissen nichts verändert. Obgleich dies eine Verringerung gegenüber den 58 % des Vorjahres darstellt, ist offensichtlich, dass kleine Unternehmen mehr unternehmen müssen, um aus Cyber-Angriffen in der Vergangenheit zu lernen und dafür zu sorgen, dass sie nicht erneut Opfer eines ähnlichen Cyber-Hacks werden.

zuständig: _____

erledigt am: _____

ERKENNEN SIE DIE HERAUSFORDERUNGEN IN DER LIEFERKETTE

Kleine Unternehmen werden sich nur langsam der Gefahr von Sicherheitsproblemen innerhalb ihrer Lieferketten bewusst. Während viele (60 %) erklären, sie hätten Vertrauen in die Maßnahmen ihrer Lieferanten zum Datenschutz, sagen knapp über die Hälfte (51 %), sie hätten bereits einen Vorfall in Zusammenhang mit ihrer Lieferkette erlebt. Doch nur eine Minderheit nimmt Kennzahlen zur Cyber-Sicherheit regelmäßig in die Verträge mit Lieferanten auf und lässt diese wiederkehrend dazu Bericht erstatten (jeweils 39 %). Für große Wirtschaftsunternehmen lauten die entsprechenden Zahlen 65 % bzw. 61 %.

Dies ist vielleicht noch verständlich: Bei der Festlegung der Einkaufskonditionen fehlt kleinen Unternehmen das Durchsetzungsvermögen der großen. Jedoch beziehen nur relativ wenige ihren Einkauf in die Entwicklung einer Cyber-Strategie ein (9 % gegenüber 14 % in größeren Unternehmen).

zuständig: _____

erledigt am: _____

SIMULIEREN SIE EINE CYBER-ATTACKE ODER FÜHREN SIE BETRIEBSINTERN PHISHING-EXPERIMENTE DURCH

Gerade einmal 26 % der kleinen Unternehmen gaben an, dass die Simulation einer Cyber-Attacke für sie im kommenden Jahr hohe oder oberste Priorität hat. Nur 35 % der kleinen Unternehmen berichteten, sie hätten ihre eigenen Phishing-Experimente durchgeführt, um das Verhalten der Angestellten nachvollziehen zu können und zu wissen, wie gut diese auf Angriffe vorbereitet sind.

zuständig: _____

erledigt am: _____

SCHLIESSEN SIE EINE CYBER-VERSICHERUNG AB

Der Abschluss einer Cyber-Versicherung ist dringend angeraten. Wir stellen diese Absicherung auf die gleiche Stufe, wie die Feuer- und Einbruchdiebstahlversicherung. Denn trotz bestem Brandschutz, stabiler Fenster und Eingangstüren ist der Abschuss einer Feuer- und Einbruchdiebstahlversicherung für fast alle Unternehmer selbstverständlich. Eine erfolgreiche Cyberattacke lässt sich auch bei dem umfangreichsten Vorsichtsmaßnahmen nicht ausschließen.

zuständig: _____

erledigt am: _____

Stand: 07/2021 · www.vfm.de