Einfache und kosteneffiziente Wege zur Schulung Ihres Teams zum Thema Cybersicherheit

Angesichts des zunehmenden Risikos von Cyberangriffen und Datenschutzverletzungen müssen UnternehmerInnen sich Zeit für den Schutz ihres Unternehmens nehmen. Ein wichtiger Startpunkt sind dabei Ihre MitarbeiterInnen, denn Sie bieten die größte Angriffsfläche.

Viele GeschäftsinhaberInnen versäumen die Vermittlung grundlegender Kenntnisse im Bereich Cybersicherheit an ihre MitarbeiterInnen, weil sie zu beschäftigt sind.

Dies wird für das Unternehmen jedoch möglicherweise später teuer. Eine kürzlich im Vereinigten Königreich durchgeführte Studie hat ergeben, dass bei Verstößen gegen die Cybersicherheit durchschnittliche jährliche Kosten von 15.300 GBP pro betroffener Person entstehen. Rund 95 % aller Probleme mit der Cybersicherheit lassen sich auf menschliches Versagen, also Ihre MitarbeiterInnen, zurückführen.

Möchten Sie Ihr Team bei der Erkennung von Risiken unterstützen und verhindern, dass Ihr Unternehmen Opfer von Cyberangriffen wird? Im Folgenden finden Sie einige einfache und kosteneffiziente Möglichkeiten, Ihr Team zu schulen.

Bereitstellung der richtigen Ressourcen

Eine gute Gelegenheit zur Schulung Ihres Teams in Sachen Cybersicherheitspraktiken ist der Onboardingprozess für neue MitarbeiterInnen. Auf diese Weise kommunizieren Sie Ihre Erwartungen gleich zu Beginn und Ihr Unternehmen ist weniger anfällig, wenn Sie neue MitarbeiterInnen einstellen oder digitale Systeme die BesitzerInnen wechseln.

Sie müssen Ihrem Team außerdem einen einfachen Zugriff auf Schulungsmaterial und Ressourcen zum Thema Cybersicherheit ermöglichen. Solange alle MitarbeiterInnen die Schulung abschließen, können sie den Lernprozess an ihren eigenen Zeitplan anpassen.

Bei der Suche nach Schulungsressourcen informieren Sie sich zunächst auf der Website Ihrer Regierung oder prüfen Sie, ob es in Ihrem Land eine nationale Behörde für Cybersicherheit gibt. Andernfalls finden Sie im Folgenden einige nützliche Ressourcen für kostenfreie Schulungen zum Thema Cybersicherheit.

Kurse

- Das National Cyber Security Centre (NCSC): Das NCSC ist Teil des GCHQ (Government Communications Headquarters), der Behörde für Nachrichten-, Sicherheits- und Cyberdienste des Vereinigten Königreichs. Das Onlineschulungspaket ist kostenfrei, einfach in der Verwendung und nimmt weniger als 30 Minuten in Anspruch. Es richtet sich in erster Linie an kleine Unternehmen und den ehrenamtlichen Sektor.

- Hub für Schulungen zum Thema Cybersicherheit von Dell: Unsere Website enthält kostenfreie Informationen und Ressourcen zu Themen wie Datenschutzverletzungen, Ransomware sowie Anwendungs- und Infrastruktursicherheit. Hier erfahren Sie mehr.
- QA: QA verfügt über ein breites Angebot an Cybersicherheitskursen zu Themen wie Cloud-Sicherheit, Datenschutz und Sicherheit neuer Technologien.

Podcasts

- Security Now: Die Experten Steve Gibson und Leo Laporte sprechen in ihrem wöchentlichen Podcast über Cybersicherheit und die neuesten Cybernachrichten.
- CyberWireDaily: Dieser Podcast erscheint täglich von Montag bis Freitag und bietet Nachrichten und Analysen zum Thema Cybersicherheit.
- Malicious Life: Malicious Life von Cybereason erzählt den unbekannten Teil der Geschichte von Cybersicherheit – mit Anmerkungen und Beobachtungen von echten HackerInnen, SicherheitsexpertInnen, JournalistInnen und PolitikerInnen.

Weitere Ressourcen

- Cybersicherheitsressourcen für kleine Unternehmen der CISA: Die CISA (Cybersecurity and Infrastructure Security Agency) bietet Services zur Förderung von Sicherheit und Resilienz in den Vereinigten Staaten an. Der Hub mit nützlichen Ressourcen enthält vielfältiges Lehrmaterial, das die Cybersicherheit in Ihrem Unternehmen unterstützt.
- Cyber and Fraud Centre in Schottland: Das Cyber and Fraud Centre hat seinen Sitz in Schottland, stellt aber Leitfäden und andere Ressourcen frei zugänglich bereit.
- TECH TALK: AI for business: How to leverage the power of AI with Microsoft
- TECH TALK: Cyber security: Protect your business from hackers
- https://dwen.com/en-us/blog-how-to-avoid-cyber-attacks-coode-larson/
- https://dwen.com/en-us/blog-dr-amit-elazari-cybersecurity-for-small-business/

Abgesehen von Schulungen müssen Sie Ihr Team dazu ermutigen, vorsichtig zu sein und jede potenzielle Bedrohung zu melden. Selbst wenn sich später herausstellt, dass keine Bedrohung vorlag, verbringen Sie lieber Zeit damit, eine falsche Bedrohung zu überprüfen, als sich mit einer echten Bedrohung zu befassen, die früher hätte erkannt werden können.

Überblick über alle potenziellen Lernmöglichkeiten

Da die Cybersicherheitsrisiken sich ständig ändern, müssen Sie sich regelmäßig über die neuesten Entwicklungen informieren. Derzeit nutzen AngreiferInnen beispielsweise KI für ausgereiftere Cyberangriffe.

Damit Ihr Unternehmen auch weiterhin geschützt ist, müssen Sie Ihre Pläne zur Cybersicherheit regelmäßig überprüfen. Außerdem sind neuere Systeme sicherer, denn die häufigsten Ziele von Cyberangriffen sind veraltete Systeme.

Eine Möglichkeit, sich über potenzielle Cyberrisiken für Ihr Unternehmen zu informieren, besteht darin, die Cybersicherheit zu testen. Mithilfe des Tools Exercise in a Box des

National Cyber Security Centre können Sie die Resilienz Ihres Unternehmens bei Cyberangriffen testen. Probieren Sie das Tool hier aus.

Verwendung von Phishing-Sicherheitstests

Bei einem Phishing-Sicherheitstest senden ArbeitgeberInnen eine Nachahmung einer echten Phishing-E-Mail an ihre MitarbeiterInnen. Dies ist eine beliebte Methode, um das Onlineverhalten der MitarbeiterInnen zu testen und ihr Bewusstsein für Phishing-Angriffe zu bewerten.

Bedenken Sie, dass diese Tests zwar die Wachsamkeit der MitarbeiterInnen erhöhen, aber auch Stress für Ihr Team bedeuten können. Wenn Sie diese Tests verwenden möchten, ist der richtige Ansatz wichtig. MitarbeiterInnen, die den Test nicht bestehen, dürfen nicht bestraft oder bloßgestellt werden. Versuchen Sie, die Situation spielerisch in eine positive Erfahrung zu verwandeln.

Geeignete Tools und Praktiken

Der Einsatz der richtigen Tools, Software und Praktiken trägt dazu bei, das Risiko und die negativen Auswirkungen eines Cyberangriffs zu verringern.

Ihre MitarbeiterInnen folgen in der Regel Ihrem Beispiel. Wichtig ist also, dass die richtigen Prozesse vorhanden sind und Sie diesen ebenfalls folgen. Dazu gehören auch sichere und eindeutige Kennwörter sowie die Aktualisierung Ihrer Sicherheitssysteme.

Zusätzlich müssen all Ihre Geräte über einen geeigneten Cyberschutz verfügen, mit dem sich Bedrohungen erkennen und abwehren lassen. Sie sind nicht sicher, welche Tools Sie nutzen möchten? Hier finden Sie die von Dell zur Verfügung gestellten Sicherheitsservices.