G DATA academy

Case Study

Mit Phishing Simulationen von G DATA Kunden zeigen, wo der IT-Sicherheitsschuh drückt

Herausforderung

- Awareness Schulungen als Ergänzung des Portfolios, um Mitarbeiter für Cybergefahren zu sensibilisieren
- Möglichkeit, Firmen den Handlungsbedarf im Bereich Awareness aufzuzeigen

Lösung

- G DATA Phishing Simulation
- G DATA Security Awareness Trainings

Vorteile

- Phishing Simulation hilft, aktuelles Bewusstsein für Cybergefahren zu prüfen
- Management Report der Phishing-Simulation zeigt den Handlungsbedarf bei Mitarbeitenden
- Awareness Schulungen helfen Angestellten, ihr Security-Wissen auszubauen

smartSEC

Branche:
Krisenmanagement und -prävention bei Cyberattacken

Standort:
Wernau, Deutschland

Immer mehr Unternehmen setzen auf Awareness Trainings, um das Bewusstsein der Mitarbeiter für Cyberrisiken zu verbessern. Zur Vorbereitung auf Cyberattacken setzt smartSEC auf Awareness Trainings von G DATA CyberDefense. Zusätzlich nutzt das StartUp Phishing Simulationen des Cyber-Defense-Unternehmens, um Kunden aufzuzeigen, wie es um die IT-Sicherheit im Unternehmen steht.

Mit Cyberangriffen kennt sich smartSEC aus: Das 2020 gegründete StartUp ist Spezialist für das Krisenmanagement bei Cyberattacken. Der Fokus liegt bei managementorientierten Fragestellungen im betroffenen Unternehmen und der Koordination vor Ort. Dabei fungieren die Fachleute unter anderem auch als „Übersetzer“ zwischen nicht-technischer Geschäftsführung und technischen Forensikern. Aus dieser Arbeit hat sich ein zweiter inhaltlicher Schwerpunkt für das junge Unternehmen ergeben: Die Vorbereitung von Unternehmen auf IT-Notfälle. Mit ihren Kunden aus dem Mittelstand entwickeln die Spezialisten ein individuelles IT-Notfallhandbuch und führen realitätsnahe Krisensimulationen durch.

„Früher oder später wird jedes Unternehmen Opfer einer Cyberattacke“, sagt Oliver Filipzik, verantwortlich für das Marketing bei smartSEC. „Wir helfen dem Mittelstand, sich auf den Worst Case vorzubereiten, damit im Ernstfall der Schaden so gering wie möglich ausfällt. Daher haben wir auch die Awareness Trainings von G DATA in unser Portfolio aufgenommen, weil der Mensch eine Schlüsselrolle in der Abwehr von Cyberangriffen einnimmt.“

Nach wie vor ist der Mensch mit seinem Verhalten ein zentraler Angriffsvektor bei Cyberattacken. Es braucht Schulungen, um das Bewusstsein der Mitarbeiter für neue Bedrohungen zu schärfen, damit sie ihr Verhalten anpassen. IT-Notfallhandbücher alleine reichen dafür nicht aus. Es braucht praxisnahe Übungen, damit Angestellte ihr

Wir hatten vom Start weg ein gutes Gefühl bei der Auswahl. Ein weiterer Pluspunkt ist, dass G DATA ein deutscher Anbieter ist. Ebenfalls überzeugt hat uns die Phishing Simulation. Diese nutzen wir, um den Status Quo bei unseren Kunden zu prüfen – in Kombination mit einem Schwachstellenscan zeigen wir, wie verwundbar Firmen sind.

Oliver Filipzik
Verantwortlich für das Marketing bei smartSEC

MIT PHISHING SIMULATIONEN MACHEN SIE DAS BEWUSSTSEIN FÜR IT-SICHERHEIT MESSBAR.

Verhalten anpassen. Auch die Kunden haben den Bedarf erkannt und fragen bei smartSEC nach, wie sie das Bewusstsein für Cybergefahren auf Seiten der Belegschaft verbessen können.

Bewusstsein schaffen mit Online-Trainings

Schnell entschieden sich die Verantwortlichen, Security Awareness Trainings als externe Lösung ins Angebot aufzunehmen. Nach einer eingehenden Marktanalyse aktueller Angebote fiel die Entscheidung auf G DATA. Für die Lernplattform sprachen die übersichtliche Benutzeroberfläche, die gute Struktur des Lernplans und der inhaltliche Aufbau.

Gerade kleinere Unternehmen sind häufig immer noch davon überzeugt, dass sie kein attraktives Ziel für Cyberkriminelle sind. Aber dem ist nicht so: Während ein Schwachstellenscan unter anderem offene Ports und damit einen möglichen Angriffsvektor zeigt, macht die Phishing Simulation deutlich, wie leicht manche Angestellten auf eine gefälschte E-Mail hereinfallen. Hinzu kommt: Viele Phishing-Attacken sind sehr gut gemacht und werden immer besser. Angreifer investieren viel, um erfolgreich zu sein. Der abschließende Management-Report zeigt, wie groß der Handlungsbedarf ist. Das Feedback der Kunden fällt durchweg positiv aus.

Die Cyberattacke ist nur einen Klick entfernt

„Die Phishing Simulation liefert gute Argumente für Verantwortliche, mit dem sie den aktuellen Stand des Unternehmens bestimmen können," sagt Oliver Filipzik. „Wenn auch nur ein Mitarbeiter auf einen Link klickt oder einen Anhang öffnet, ist es eigentlich schon 5 nach 12 und die Ransomware im Netzwerk. Zusätzlich profitieren wir von der Partnerschaft mit G DATA CyberDefense. Denn der Name hat bei vielen Kunden Gewicht als vertrauenswürdiger Partner."

Während der Phishing Simulation erhalten die Kunden über einen Zeitraum von vier Wochen unterschiedliche Phishing-Mails. Die Erfahrungen zeigen, dass Öffnungsraten zwischen einzelnen Szenarien zwar unterschiedlich hoch sind, es jedoch fast immer mehrere Mitarbeiter gibt, die den Angreifern ins Netz gegangen wären. Während Corona haben insbesondere Mails mit Homeoffice-Bezug gut funktioniert. Aber auch persönliche Themen wie Umstellung der Firmenparkplätze oder Essenänderungen in der Firmenkantine verleiten viele Angestellte zum Öffnen einer Mail bis hin zum Anklicken eines falschen Links oder gar zur Preisgabe sensibler Daten.

„Die Zusammenarbeit mit G DATA läuft sehr angenehm", sagt Oliver Filipzik. „Sonderwünsche von Kunden hat der Support schnell und lösungsorientiert gelöst. Auch die direkte Kommunikation zwischen unseren Kunden und G DATA lief immer reibungslos. Wir fühlen uns gut aufgehoben."

Neugierig, wie auch Sie Ihr Unternehmen mit G DATA absichern können?
Hier erfahren Sie mehr:

gdata.de/business vertrieb@gdata.de 0234 / 9762-170

G DATA academy