DEFENDERBOX
EINFACH.SCHNELL.CYBERSICHER.

Referenzbericht
Connecting Media GmbH

Resultat
Solide Grundlage vorhanden!

Als IT-Dienstleister und Security-Service-Provider steht Connecting Media selbst im besonderen Fokus: Wer Kunden bei Firewall- und Applikationsüberwachung, IT-Sicherheit und Datenschutz unterstützt, muss die eigene Angriffsfläche mindestens genauso konsequent im Blick behalten. Öffentliche Systeme, interne Infrastruktur und die eigene Reputation im Darknet sind dabei zentrale Prüfpunkte.

> „Die DEFENDERBOX gibt uns als Security-Service-Provider genau das transparente, priorisierte Lagebild, das wir auch unseren eigenen Kunden empfehlen – angewendet auf unsere eigene Infrastruktur."
>
> Andreas Kunz, Geschäftsführer, Connecting Media GmbH

Zielsetzung & Umsetzung

Mit NIS-2, AI Act und ISO 27001 reicht es nicht mehr, ein Sicherheitskonzept zu haben. Unternehmen müssen nachweisen, dass ihre Maßnahmen auch im Alltag wirksam sind.

Ein Audit einmal im Jahr liefert dafür jedoch nur eine Momentaufnahme. Die entscheidende Frage bleibt: Was passiert an den übrigen 364 Tagen?

Deswegen war Connecting Media auf der Such nach einer Lösung, die die gesamte Angriffsfläche kontinuierlich betrachtet: Öffentliche Systeme, interne Infrastruktur und kompromittierte Zugangsdaten bzw. Informationen im Darknet. Schwachstellen sollen dabei nicht nur gefunden, sondern zu konkreten Angriffspfaden zusammengeführt werden.

Nur so entsteht ein belastbares und priorisiertes Lagebild, das zeigt, wo das tatsächliche Risiko liegt – und welche Sicherheitslücke zuerst geschlossen werden sollten. Damit lässt sich der Aufwand speziell dort einsetzen, wo er die größte Wirkung erzielt.

Ergebnisse & Maßnahmen

Die erste Sicherheitsüberprüfung mit der **DEFENDERBOX** bestätigte eine solide Ausgangsbasis – und lieferte zugleich den dokumentierten, risikobasierten Nachweis, den ISO 27001 und BSI-IT-Grundschutz fordern:

Externer Pentest:
Schwachstellen ausschließlich mit geringem Schweregrad – u. a. unterbrochene bzw. selbstsignierte Zertifikatskette, anstehender Zertifikatsablauf, fehlendes HSTS sowie eine ICMPTimestamp-Antwort mit Rückschluss auf die Systemzeit.

Interner Pentest:
Ohne Domain-Anmeldung durchgeführt, vereinzelte Lücken mit geringem Schweregrad. Kritische oder hohe Risiken: keine. Darknet-Recherche: eine bereits durchgesickerte EMail-Adresse aus einem bekannten Datenleck identifiziert – relevant für die nach NIS-2 geforderte Melde- und Reaktionsfähigkeit.

Alle Lücken wurden priorisiert geschlossen.

Referenzbericht

Connecting Media GmbH

Für Connecting Media war das Ergebnis mehr als eine bestandene Prüfung. Statt einer einmaligen Momentaufnahme liefern die wöchentlichen, automatisierten Überprüfungen mit der DEFENDERBOX den durchgehenden Nachweis, den Auditoren, Kunden und der eigene Anspruch an NIS-2- und ISO-27001-Konformität verlangen: Sicherheit wird nicht einmal im Jahr besprochen, sondern an 365 Tagen aktiv gelebt – transparent, priorisiert und belegbar. Genau dieses Modell bietet Connecting Media nun auch seinen eigenen Kunden als Compliance-as-a-Service an.

„Die wöchentlichen, automatisierten Sicherheitsüberprüfungen zeigen uns zuverlässig, wo wir als Erstes ansetzen müssen. Das gibt nicht nur uns, sondern auch unseren eigenen Kunden zusätzliche Sicherheit."

Andreas Kunz, Geschäftsführer, Connecting Media GmbH, Ettlingen

IT

Mitarbeiter DE: 11

Einsatz: wöchentl. DEFENDERBOX Sicherheitsüberprüfung

Connecting Media

Wir helfen gerne!
Kontaktieren Sie uns unter
vertrieb@defenderbox.de