BXC SECURITY

CIRT360 TABLETOP EXERCISE

Simulieren Sie einen Cybervorfall und prüfen Sie die Reaktionsfähigkeit Ihres Teams, bevor der Ernstfall sie prüft.

FOR **IMPACTING** BUSINESS **SOLUTIONS**

LEISTUNG: TABLETOP EXERCISE

BxC Security bewertet mit Ihnen, wie wirksam Ihr Cyber Incident Response Team (CIRT) in einem Krisen-szenario agiert.
In einer kontrollierten, realistischen Simulation prüfen wir, wie Ihre Organisation einen Cybervorfall unter Druck bewältigt.

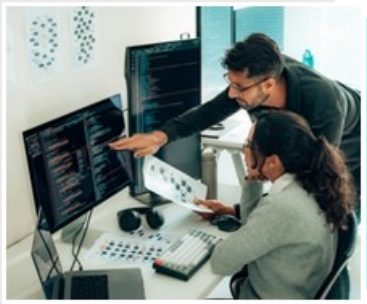
Unser Ziel bei BxC Security: hochwertige Cybersecurity-Leistungen, die die Resilienz von Wirtschaft und Gesellschaft stärken.
Wir setzen auf pragmatische Lösungen mit messbarem Nutzen.

Vorbereitung

- Sie wählen ein vordefiniertes Vorfallszenario auf Basis gängiger Bedrohungslagen
- Gemeinsam stimmen wir den Übungsumfang auf Ihre Organisationsstruktur ab
- Darauf aufbauend definieren wir Ablauf und zentrale Diskussionspunkte

Durchführung

- Wir moderieren eine strukturierte Tabletop-Übung (4–6 Stunden) mit realistischem Vorfallszenario
- Ihr CIRT arbeitet zentrale Entscheidungspunkte zu Eskalation, Kommunikation und Reaktion durch
- Wir beobachten, wie Ihr Team unter Druck handelt



Auswertung

- Wir bewerten Ihr Team anhand der beobachteten Entscheidungen und Maßnahmen
- Wir identifizieren Lücken in Kommunikation, Eskalation und Rollenklarheit
- Wir liefern eine kompakte Zusammenfassung mit Maßnahmen und nächsten Schritten

Ihre Vorteile auf einen Blick!

- Schnelle Validierung Ihrer Incident-Response-Fähigkeit
- Klare Sicht auf Lücken in Koordination und Entscheidungen
- Praxisnahe, umsetzbare Empfehlungen
- Unterstützt Compliance (NIS2, ISO 27001, IEC 62443) und liefert auditfähige Nachweise

SIE MÖCHTEN MEHR ERFAHREN?
BESUCHEN SIE UNS AUF:
https://www.bxc-security.com/

FALLSTUDIE

Um seine Incident-Response-Fähigkeit zu validieren, hat ein Produktionsunternehmen mit integrierten IT- und OT-Umgebungen BxC Security mit einer strukturierten Tabletop-Übung beauftragt.

Ein Cyber Incident Response Team (CIRT) und dokumentierte Prozesse waren vorhanden. Zu prüfen war, ob sie im realen Vorfall wirksam greifen – unter Zeitdruck und bereichsübergreifender Koordination. Zudem benötigte das Unternehmen dokumentierte Nachweise nach NIS2 und ISO 27001 sowie den Beleg, dass diese Fähigkeit in der Praxis getestet wurde.

ERGEBNISSE

10+ Stakeholder eingebunden	**7+** Entscheidungen unter Zeitdruck
1 Tag Aufwand beim Kunden	**4** Lücken vor dem Ernstfall

Unser Beitrag

Vorbereitung der Übung

- Ein Szenario aus unserer Bibliothek wurde auf die Bedrohungslage und Fertigungsarchitektur des Kunden zugeschnitten
- Der Übungsumfang wurde gemeinsam mit dem Kunden und anhand der Organisationsstruktur festgelegt
- Darauf aufbauend wurde ein Übungsablauf mit zentralen Diskussions- und Entscheidungspunkten definiert, der eine fokussierte Bewertung der Incident-Response-Fähigkeit ermöglichte

Durchführung der Übung

- Die Tabletop-Übung wurde als interaktive Session durchgeführt und führte die Teilnehmenden durch ein realistisches Cybervorfallszenario in IT- und Betriebsumgebungen
- Im Verlauf wurden neue Informationen und Entwicklungen eingespielt, um die sich verändernde Lage abzubilden und die Komplexität zu erhöhen
- Besonderes Augenmerk lag auf teamübergreifender Koordination, zeitnahen Entscheidungen und der Einbindung relevanter Stakeholder unter Druck

Auswertung & Empfehlungen

- Die Reaktionsfähigkeit wurde in Governance, Kommunikation und Koordination analysiert
- Zentrale Lücken wurden bei Eskalation, IT/OT-Abstimmung und regulatorischer Handhabung identifiziert
- Die Ergebnisse wurden als Managementbericht mit priorisierten Maßnahmen und auditfähigem Übungsnachweis dokumentiert

UNSER ANGEBOT

***Preis für Vor-Ort-Durchführung auf Anfrage**

Wir bieten Ihnen eine strukturierte und pragmatische Leistung, mit der Sie Ihre Incident-Response-Fähigkeit unter realistischen Bedingungen validieren.

Ziel ist es zu zeigen, wie Ihr Cyber Incident Response Team in der Praxis agiert, und konkrete Verbesserungsfelder zu identifizieren – mit minimalem Aufwand für Sie.

CIRT TABLETOP EXERCISE

Unsere strukturierte Tabletop-Übung ist ein schneller und effizienter Weg, Ihr Cyber Incident Response Team in einem realistischen Szenario zu testen.

In einer fokussierten Session arbeitet Ihr Team einen vordefinierten Vorfall durch – so validieren Sie Entscheidungsfindung, Koordination und Kommunikation unter Druck.

Wir bringen Szenario, Moderation und Bewertungsmethodik mit – Sie bringen Ihr Team und Ihren Organisationskontext ein.

Preis: 10.000 Euro

Was wir benötigen

- Liste der relevanten Stakeholder (z. B. IT, Security, Operations, Management)
- Grundlegender Überblick über Ihr Incident-Response-Setup
- Verfügbarkeit für eine Session von 4–6 Stunden
- Übergeordnete Informationen zu Ihrer IT/OT-Umgebung

Was Sie erhalten

- Moderierte Tabletop-Übung
- Realistisches, vordefiniertes Vorfallszenario
- Strukturierte Bewertung der Reaktionsfähigkeit
- Identifikation zentraler Lücken und Schwachstellen
- Kompakter Bericht mit Empfehlungen und nächsten Schritten

BXC SECURITY

info@bxc-security.com

+49 811 128 807 43

Foehrenweg 1
85399 Hallbergmoos
Deutschland

FOR IMPACTING BUSINESS SOLUTIONS