TABLETOP EXERCISES

TESTEN UND OPTIMIEREN SIE IHRE RESILIENZ

AwareTec GmbH

Inhalt

Zusammenfassung

Angesichts der sich ständig weiterentwickelnden Landschaft der Cybersicherheitsbedrohungen müssen Unternehmen ihre Bereitschaft kontinuierlich verbessern, um effektiv auf potenzielle Sicherheitsverletzungen und Angriffe reagieren zu können. Tabletop-Exercises gehen über vorab festgelegte Gespräche hinaus und bieten einen realistischen Ansatz, der die Komplexität realer Vorfälle widerspiegelt.

Diese Broschüre präsentiert stattdessen einen modernen Ansatz für ein Cyber-Krisentraining: eine Kombination aus realistischen Simulationen, szenariobasierten Rollenspielen und spielerischen Elementen, um sowohl technische Teams als auch Entscheidungsträger aus dem Unternehmen vollständig einzubinden.

Die Übungen basieren auf aktuellen Bedrohungen und sich weiterentwickelnden Vorschriften wie NIS2 und DSGVO, sodass Unternehmen nicht nur ihre technischen Abwehrmaßnahmen, sondern auch die Reaktionsfähigkeit ihrer Führungskräfte und ihre Compliance-Bereitschaft testen können.

Durch die Integration von Live-Simulationen in Cyber-Range-Umgebungen und die Nutzung von Analysen nach Vorfällen, erhalten Unternehmen ein umfassendes Verständnis ihrer Stärken und Schwachstellen – zusammen mit praktischen, priorisierten Schritten zur Verbesserung.

CTO
Irina Nork

Tabletop Exercises

(TTX)

Ihr Unternehmen wird Opfer eines Cyberangriffs. Cyberkriminelle hacken sich in Server, verschlüsseln Daten und veröffentlichen sensible Daten im Darknet. Der Vorfall wird publik. Kunden erwarten Erklärungen. Der Angreifer fordert Lösegeld.

Funktionieren Ihre Notfallpläne? Haben Sie Ihren Notfallplan unter realistischen Bedingungen getestet?

Was sind Tabletop-Exercises (TTX)?

- **Maßgeschneiderte, interaktive Simulationen von Cybervorfällen** – Ihr Team wird in realistische Cyberangriffsszenarien versetzt und dabei angeleitet und moderiert, um die Entscheidungsfindung unter Druck zu trainieren.
- **Sichere Umgebung, realistische** Stress-Situationen – Wir testen Ihre Notfallpläne und die Teamkoordination in einer kontrollierten, aber äußerst realistischen Umgebung, ähnlich einer militärischen Simulation für das digitale Schlachtfeld.
- **Klarheit und Widerstandsfähigkeit –** Wir decken Stärken auf, legen Schwachstellen offen und schärfen Ihre Verteidigungsstrategie, damit Ihr Unternehmen wirklich auf die nächste Cyberkrise vorbereitet ist.

Warum AwareTec?

- **Kompetenz** – Worldclass-Experten mit operativer und strategischer Erfahrung im Schutz kritischer Infrastrukturen
- **Maßgeschneidert für Tech-Teams und Führungskräfte** – Unsere TTXs beziehen alle Ebenen ein, von IT-/OT-Teams bis hin zum Management, um koordinierte Entscheidungen, regulatorische Klarheit und effektive Kommunikation auch unter Druck zu gewährleisten
- **Klare, umsetzbare Ergebnisse** – Wir unterstützen Sie bei der Umsetzung unserer priorisierten Empfehlungen und einer Roadmap zur Verbesserung von Mitarbeitern, Prozessen und Vorbereitungen, nicht nur mit einer passiven Zusammenfassung.

Vom Cybervorfall zur Krise

Warum ist Vorbereitung für die Eskalation eines Angriffs entscheidend?

Ein Cyberangriff kann schnell eskalieren – von einem einzigen Klick zu einer ausgewachsenen Krise mit Datenlecks, Ausfallzeiten und Reputationsschäden.

Dies verdeutlicht, warum Vorbereitung und koordinierte Reaktion auf allen Ebenen von entscheidender Bedeutung sind

Tabletop Exercises im Einsatz

Warum Tabletops wichtig sind: Unsicherheit in Cyber-Bereitschaft verwandeln

Strategische Ergebnisse

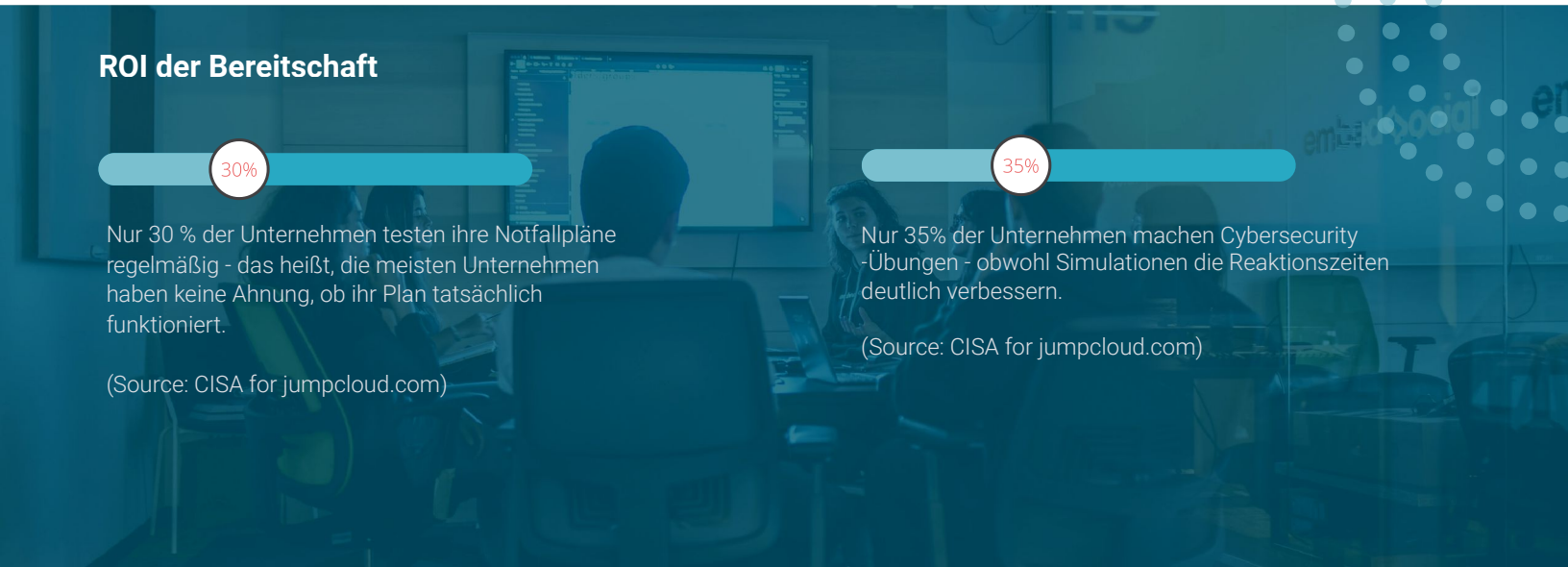
- Sensibilisierung der Führungskräfte für Cyberrisiken und entsprechende Reaktionsmaßnahmen
- Testen und Verfeinern von Entscheidungsprozessen unter simuliertem Krisendruck
- Abstimmung der Cybersicherheit auf übergeordnete Strategien zur Stärkung der Widerstandsfähigkeit des Unternehmens

Reaktionsfähigkeit

- Verbessern Sie die Kommunikation und Zusammenarbeit zwischen IT, OT und Führungskräften
- Identifizieren Sie Schwachstellen, Lücken und Eskalationsverzögerungen in einer sicheren Umgebung
- Sammeln Sie praktische Erfahrungen mit Vorfallszenarien

Messbare Verbesserung

- Validieren Sie Ihre Krisenreaktions- und Wiederherstellungspläne
- Generieren Sie umsetzbare Erkenntnisse und Reports
- Verbessern Sie Teamabstimmung, Geschwindigkeit und Klarheit in Stress-Situationen



ROI der Bereitschaft

30%

Nur 30 % der Unternehmen testen ihre Notfallpläne regelmäßig - das heißt, die meisten Unternehmen haben keine Ahnung, ob ihr Plan tatsächlich funktioniert.

(Source: CISA for jumpcloud.com)

35%

Nur 35% der Unternehmen machen Cybersecurity -Übungen - obwohl Simulationen die Reaktionszeiten deutlich verbessern.

(Source: CISA for jumpcloud.com)

Umsetzung von Tabletop Exercises

Unsere Übungen sind für IT- und OT-Umgebungen konzipiert.

Wir bieten folgende Formate von TTX an:

Diskussionsbasiert

Stimmt Teams hinsichtlich Entscheidungen und Verantwortlichkeiten ab und sorgt so für eine schnellere, koordinierte Krisenreaktion

Viele Unternehmen haben Notfallpläne, aber oft wissen die Mitarbeiter nicht genau, welche Aufgaben sie in einer Krisensituation haben. Missverständnisse können zu kostspieligen Verzögerungen führen.

Ihr Mehrwert:
Eine moderierte Diskussion sorgt dafür, dass sich alle über ihre Verantwortlichkeiten, Entscheidungsprozesse und Eskalationswege einig sind, und schafft so Klarheit, bevor eine echte Krise eintritt.

Szenariobasierte Übung

Schafft Vertrauen durch praktische Übungen zum Umgang mit hochriskanten Angriffsszenarien

Cyberbedrohungen wie Ransomware und Datenverletzungen sind komplex, und Teams bekommen selten die Gelegenheit, zu sehen, wie sie sich von Anfang bis Ende entwickeln

Ihr Mehrwert:
Durch die Simulation eines realistischen Angriffs erkennen die Teilnehmer die potenziellen Auswirkungen auf das Unternehmen, üben koordinierte Maßnahmen und gewinnen Vertrauen im Umgang mit hochriskanten Situationen.

Praktische Reaktionsübung (funktional + technisch)

Funktionsübergreifende Teams simulieren aktiv die Erkennung, Eindämmung, Kommunikation und Wiederherstellung während eines Live-Cyber-Events

Bei einem Angriff arbeiten IT-/OT-Teams, Security Team, und das Management oft getrennt voneinander, was zu Verzögerungen und Fehlern führen kann. Technische Mitarbeiter könnten zu spät bemerken, dass Prozesse nicht wie geplant ablaufen.

Ihr Mehrwert:
Es entsteht echte Teamarbeit unter Druck, Prozesse werden abteilungsübergreifend validiert und die technische Grundlage Ihrer Incident Response wird gestärkt.

Schritte zu erfolgreichen Tabletop-Exercises

Von der Zielsetzung bis zur Bewertung – ein strukturierter Fahrplan für realistische und effektive Cyber-Incident-Simulationen

Ziel festlegen

- Entscheiden Sie über Umfang und Teilnehmer
- Legen Sie eine Eskalationsstufe fest
- Legen Sie Ziele fest unter Berücksichtigung von:
  - Angriffsfläche
  - Organisatorische Prioritäten
  - Bestehende Prozesse
  - Sicherheitsmaßnahmen

Szenariotyp und Methode

- Identifizieren Sie den Szenariotyp basierend auf:
  - Notfallplan
  - Spezifische Cyberangriff
- Entscheiden Sie sich für eine Liefermethode
  - Diskussionsbasiert
  - Szenariobasiert
  - Funktional + technisch

Entwurf einer Tabletop-Übung

- Recherche:
  - Basierend auf der Angriffsfläche
  - Basierend auf der Risikomatrix des Unternehmens
- Erstellen Sie eine Storyline für die Tabletop-Übung
- Erstellen Sie Spielerhandbücher (Video oder Präsentation)

Injektionen

- Entwurf und Herstellung von Injektionen
- Bereitstellung neuer Updates während der Übung:
  - Einbeziehung relevanter Informationen
  - Bereitstellung realistischer Erfahrungen

TTX-Ausführung

- Einrichtung des Veranstaltungsortes für die Sitzung
- Moderation der Übung
- Eskalation
- Dokumentation der Ergebnisse

Bewertung und Verbesserung

- Analyse der Wirksamkeit der Tabletop-Übung:
  - Technologie
  - Personen
  - Prozesse
- Identifizierung von Verbesserungsmöglichkeiten
- Entwicklung des Entwurfs für den Nachbericht (After Action Report, AAR)

Tabletop Exercises

Strategische Überlegungen

Damit eine Tabletop-Übung nicht nur nicht nur Mittel zum Zweck ist, sondern auch ihre Wirkung zeigt, müssen einige entscheidende Faktoren berücksichtigt werden. Ziel ist es, praxisnahe Erkenntnisse zu gewinnen, Handlungssicherheit zu stärken und kritische Schwachstellen frühzeitig zu identifizieren.

Ziele & Umfang – Fokus schafft Wirkung

- **Klare Zielsetzung:** Was möchten Sie erreichen? Zum Beispiel: Notfallprozesse testen, Entscheidungssicherheit unter Druck analysieren oder Kommunikationsabläufe prüfen.
- **Realistischer Umfang:** Der Umfang muss zu Ihrer Organisation passen in Bezug auf Zeit, Teilnehmerzahl und Reifegrad.

Szenariodesign – Relevanz statt Theorie

- **Individuelle & realistische Szenarien:** Wir entwickeln Szenarien auf der Grundlage Ihrer Bedrohungslage und Ihrer Geschäftsprozesse, um Bewertungsrisiken aufzuzeigen.
- **Komplexität:** Sie bestimmen die Intensität, von der ersten IT-Störung bis zur konzernweiten Krise.

Stakeholder einbinden – Teams stärken

- **Alle relevanten Bereiche am Tisch:** IT/Security, Geschäftsleitung, Kommunikation, Recht, HR und Fachbereiche – sämtliche Perspektiven sind entscheidend
- **Entscheidungsträger vs. operative Mitarbeiter:** Unsere Übungen bringen Entscheidungsträger und operative Teams in einen realitätsnahen Dialog.

Umsetzung, Engagement & Logistik

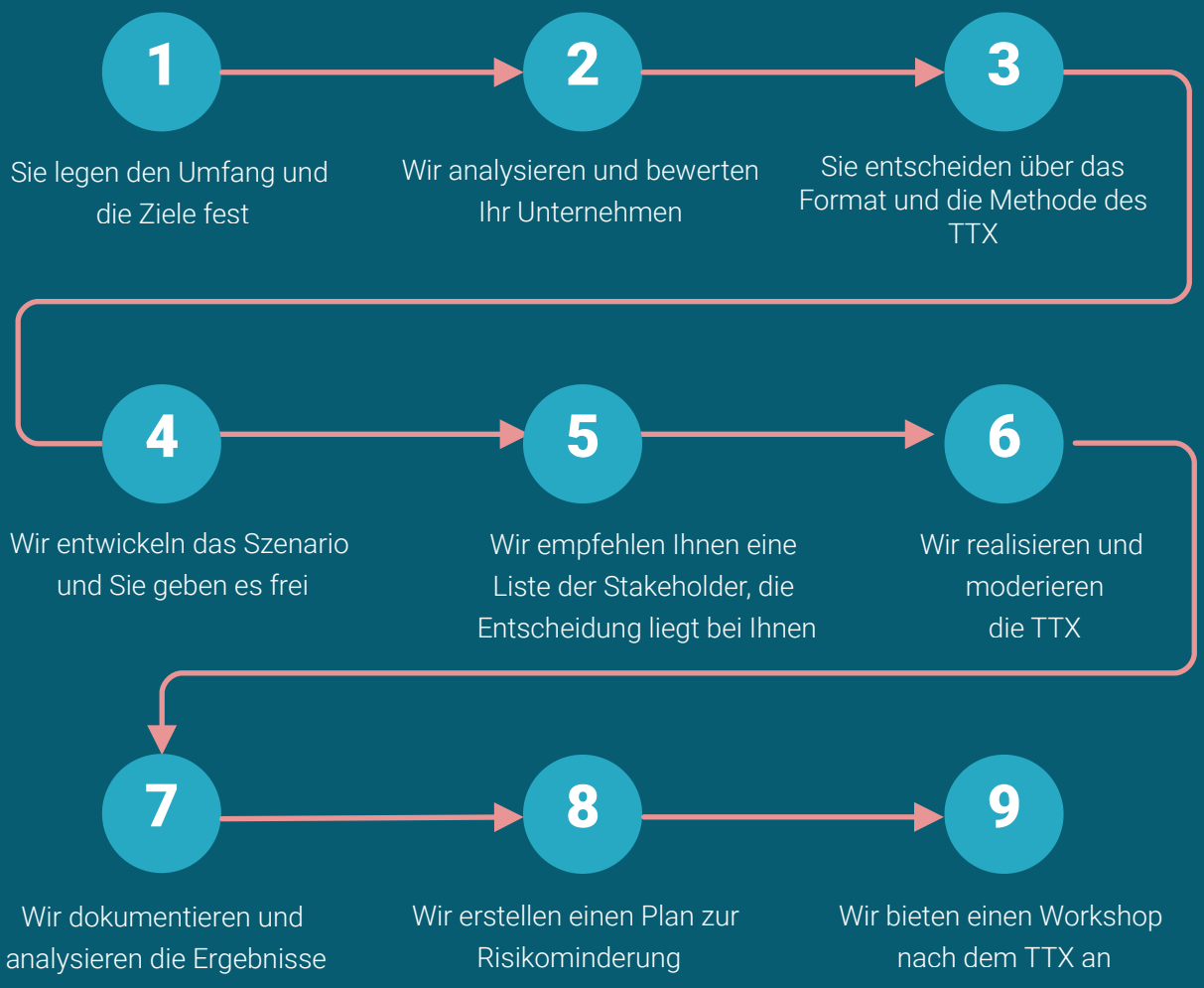
- **Das Format:** Wir passen die Übungen an Ihr Team und Ihre Ziele an, egal ob vor Ort, remote oder hybrid.
- **Motivierende Erfahrung:** Interaktive Moderation steigert die Aufmerksamkeit und das Engagement.
- **Professionelle Umsetzung:** Wir strukturieren die Sitzungen mit Tools, Visualisierungen und Triggern für nachweisbare Ergebnisse.

Tabletop-Exercises

der Prozess

Die meisten Unternehmen halten herkömmliche Tabletop-Excercises zu Recht für sehr arbeitsintensiv. Bei AwareTec ist das Gegenteil der Fall: Hier übernehmen wir den Großteil der Arbeit: Wir analysieren, entwickeln das Szenario, moderieren die Übung und liefern schließlich klare Ergebnisse und Empfehlungen. Für Sie bedeutet dies einen minimalen Zeitaufwand bei maximalem Nutzen. Ihre Teams investieren nur wenige Stunden, doch Sie bekommen realistische Erkenntnisse, klare Empfehlungen und - mehr Sicherhei.

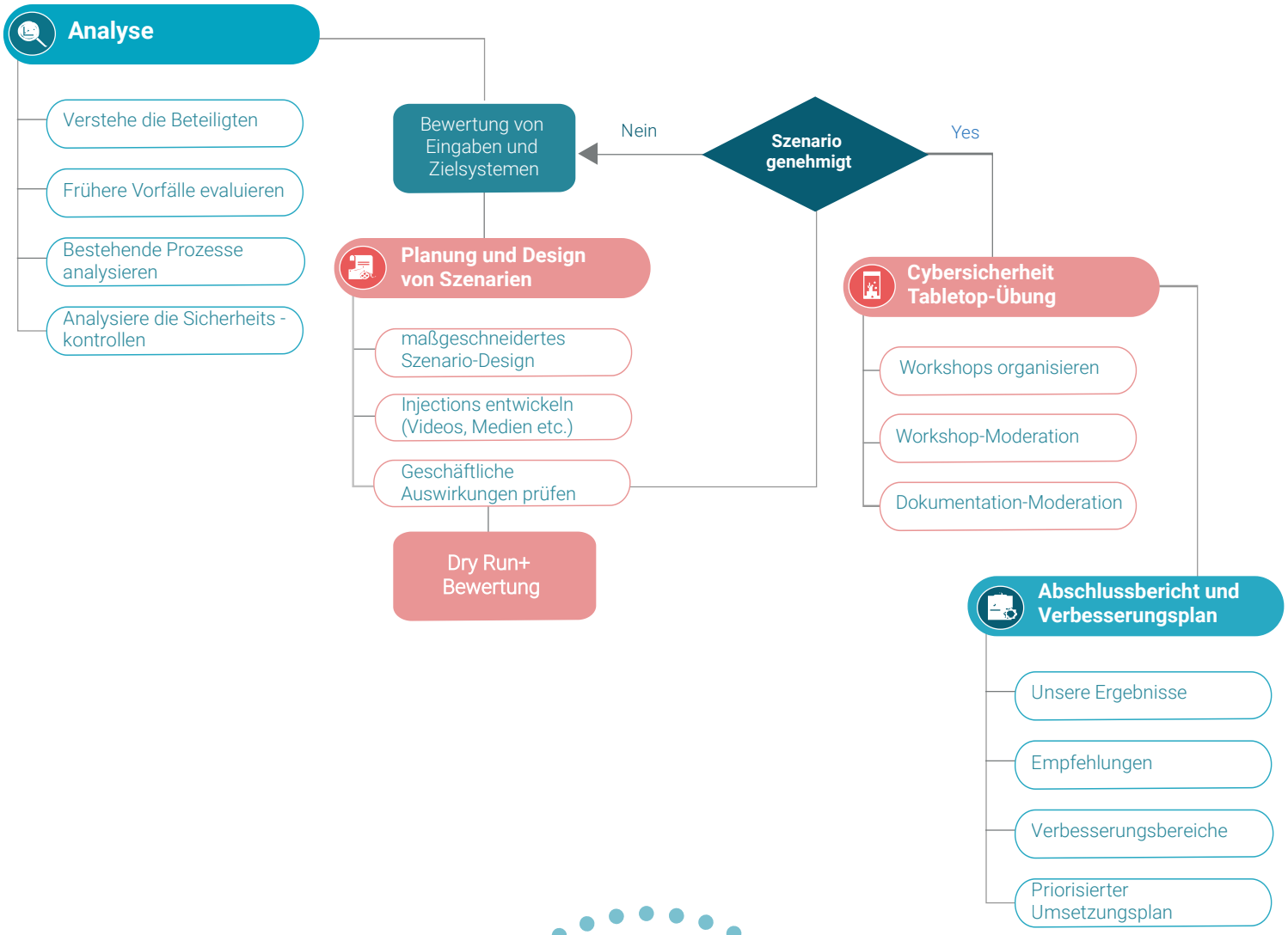
Ein klarer Fahrplan – von der Zieldefinition bis zur Umsetzung und Verbesserung



Tabletop-Exercises

Szenario-Design

Jede Tabletop-Übung basiert auf einem maßgeschneiderten Szenario. Um sicherzustellen, dass es realistisch, relevant und effektiv ist, folgen wir einem klaren Prozess. Wir bieten Ihnen eine genau auf Ihr Unternehmen zugeschnittene Übung, die Ihnen echtes Vertrauen in Ihre Fähigkeiten vermittelt, effektiv zu reagieren.



Tabletop-Exercise

Ihr Nutzen

Was Sie während eines TTX-Einsatzes erwartet

Strategische Planung und Ausrichtung

Wir beginnen damit, die wichtigsten Ressourcen Ihres Unternehmens und die Prozesse, die diese unterstützen, zu verstehen. Wir überprüfen Ihre wichtigsten Dokumente wie Backup-, Kontinuitäts- und Reaktionspläne. Auf diese Weise können wir Szenarien entwerfen, die relevant, realistisch und auf Ihre individuelle Umgebung zugeschnitten sind.

Maßgeschneiderte Szenarien, die Ihre Risikolandschaft widerspiegeln

Wir entwickeln Cyber-Incident-Szenarien, die Ihr Risikoprofil widerspiegeln. Diese Szenarien sind so konzipiert, dass sie zunehmend komplexer werden und Ihre Teams unter Druck reagieren müssen. Jedes Szenario dient dazu, Ihre Bereitschaft und Reaktion im Einklang mit Ihrem Notfallplan und Ihre Sicherheitsleitfäden zu testen.

Moderation durch Experten und Real-Time Feedback

Unsere erfahrenen Moderatoren leiten die Teilnehmer Schritt für Schritt durch die Übung und liefern relevante Kontextinformationen und Live-Feedback, während sich die Ereignisse entwickeln. Dies gewährleistet eine strukturierte und ansprechende Erfahrung, die zu sinnvollen Diskussionen und realistischen Entscheidungen führt.

Umsetzbare Erkenntnisse und umfassender Ergebnisbericht

Wir liefern einen detaillierten Bericht, der die Leistung Ihres Teams anhand Ihrer internen Pläne und Best Practices bewertet. Die Ergebnisse zeigen operative Stärken auf, identifizieren Lücken und enthalten Expertenempfehlungen zur Verbesserung Ihrer Incident-Response-Fähigkeiten.

Tabletop Exercises

Arbeitspaket

Unsere Cyber-Tabletop-Exercises (TTX) sollen die Widerstandsfähigkeit von Organisationen stärken, die Entscheidungsfindung verbessern und Teams darauf vorbereiten, Cybervorfälle effektiv zu bewältigen.

Das Arbeitspaket umfasst Folgendes:

- Tabletop-Exercises / Simulierte Cyberkrise
- Realistisches Szenario, zugeschnitten auf Ihr Unternehmen
- Expertenmoderation & geleitete Diskussion
- Detaillierter Bericht zur Bewertung der Bereitschaft
- Fahrplan zur Optimierung, priorisiert und risikobasiert

Optionale Erweiterungen:

- Cyber Threat Intelligence - Analyse Ihrer externen Angriffsfläche und Simulation auf Basis realer Angriffsvektoren und Bedrohungsinformationen
- Technische Übung - Praktische Simulationen für IT /OT-, SOC- und Incident Response Team
- Hack your Plan - Lückenanalyse und umsetzbare Verbesserungen, ein Szenario, das speziell Ihre bekannten Schwachstellen ausnutzt
- AR-Erlebnis - Krisenmanagement-Gamification mit AR-Brillen

Get In Touch

E-Mail: mail@awaretec.de
Website: www.awaretec.de

Oder

Termin vereinbaren