TABLETOP EXERCISES

TESTEN UND OPTIMIEREN SIE IHRE RESILIENZ

Inhalt

Zusammenfassung

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

Diese Broschüre stellt einen modernen Ansatz für Cyber-Krisentraining vor: eine Kombination aus realistischen Simulationen, szenariobasierten Rollenspielen und spielerischen Elementen, um sowohl technische Teams als auch Entscheidungsträger in Unternehmen voll einzubeziehen.

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

Durch die Integration von Tabletop-Übungen in Ihre Cyber-Strategie nutzen Sie die Analyse nach einem Vorfall und erhalten einen detaillierten Einblick in Ihre Stärken und Schwächen – 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)?

- **Individuelle und interaktive Cyber-Angriffssimulationen** – Ihr Team erlebt realistische Cybervorfälle und wird dabei von erfahrenen Experten begleitet. In geführten Szenarien trainieren die Teilnehmenden Entscheidungsfähigkeit, Kommunikation und Handlungsstärke unter Druck.
- **Sichere Umgebung mit realistischem Stressfaktor –** wir testen Notfallpläne, Verantwortlichkeiten und die Zusammenarbeit der Teams in einer kontrollierten, aber hochrealistischen Umgebung – vergleichbar mit einer militärischen Übung für das digitale Schlachtfeld.
- **Mehr Klarheit, mehr Widerstandsfähigkeit –** wir decken Stärken auf, was gut funktioniert, wo Lücken bestehen und wie sich Ihre Verteidigungsstrategie gezielt verbessern lässt. So wird Ihr Unternehmen tatsächlich krisenfest und bereit für den nächsten Cyberangriff.

Warum AwareTec?

- **Kompetenz** – internationale Experten durchgeführt, die über operative und strategische Erfahrung im Schutz kritischer Infrastrukturen verfügen. Sie bringen Praxiswissen aus realen Cybervorfällen mit – kein Lehrbuchwissen, sondern echte Erfahrung.
- **Maßgeschneidert für Tech-Teams und Führungskräfte** – unsere TTXs beziehen alle Ebenen ein, von IT-/OT-Teams bis hin zu Geschäftsführung und Management. So entstehen abgestimmte Entscheidungen, klare Verantwortlichkeiten und sichere Kommunikation – auch unter hohem Zeit- und Entscheidungsdruck.
- **Klare, umsetzbare Ergebnisse** – nach der Übung erhalten Sie keine passive Zusammenfassung, sondern klare Prioritäten, konkrete Handlungsempfehlungen und einen realistischen Fahrplan zur Verbesserung von Mitarbeitern, Prozessen und Reaktionsfähigkeit.

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

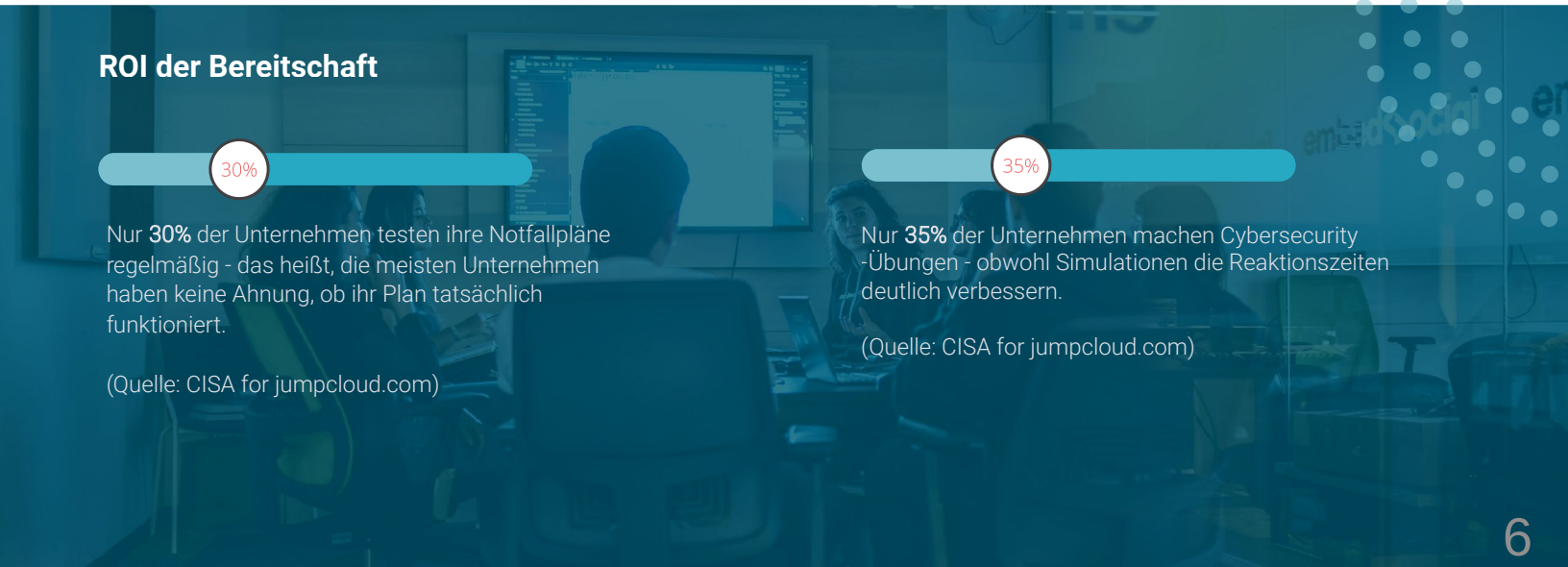
- Sensibilisierung von Führungskräften für Cyberrisiken und wirksame Reaktionsmaßnahmen.
- Testen und Verfeinern von Entscheidungsprozessen unter realitätsnaher Krisendynamik.
- Abstimmung der Cybersicherheitsmaßnahmen mit der Unternehmensstrategie, um die Gesamtresilienz zu stärken.

Reaktionsfähigkeit

- Verbesserung der Zusammenarbeit und Kommunikation zwischen IT, OT und Management.
- Aufdeckung von Schwachstellen, Verzögerungen und Lücken in einem sicheren Trainingsumfeld.
- Praktische Erfahrung im Umgang mit realitätsnahen Vorfallsszenarien.

Messbare Fortschritte

- Überprüfung und Optimierung von Notfall- und Wiederherstellungsplänen
- Erstellung konkreter, umsetzbarer Erkenntnisse und strukturierter Berichte
- Verbesserung von Teamkoordination, Reaktionsgeschwindigkeit und Entscheidungsqualität unter Stress



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.

(Quelle: CISA for jumpcloud.com)

35%

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

(Quelle: CISA for jumpcloud.com)

Umsetzung von Tabletop Exercises

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

Wir bieten folgende Formate von TTX an:

Diskussionsbasierte Übung

Bringt Klarheit, bevor es ernst wird.

Viele Unternehmen verfügen über Notfallpläne, doch oft ist unklar, wer im Ernstfall welche Rolle übernimmt. Unstimmigkeiten führen zu Verzögerungen und Fehlentscheidungen.

Ihr Mehrwert:
In einer moderierten Diskussion werden Verantwortlichkeiten, Entscheidungswege und Eskalationsprozesse gemeinsam definiert. So entsteht ein gemeinsames Verständnis und eine koordinierte Basis für den Ernstfall.

Szenariobasierte Übung

Stärkt Sicherheit im Umgang mit kritischen Angriffen

Angriffe wie Ransomware oder Data-Breaches entwickeln sich dynamisch und komplex. Teams erleben selten den gesamten Ablauf von der ersten Auffälligkeit bis zur Eskalation.

Ihr Mehrwert:
Durch die Simulation eines realistischen Angriffs erkennen die Teilnehmenden die potenziellen Auswirkungen auf das Unternehmen, üben abgestimmte Maßnahmen und gewinnen Sicherheit im Umgang mit Hochrisikosituationen.

Praktische Reaktionsübung (funktional und technisch)

Trainiert den Ernstfall unter realen Bedingungen

In vielen Fällen arbeiten technische Teams und das Management isoliert voneinander, was zu Fehlern und Verzögerungen führt. Technische Teams erkennen oft zu spät, dass Prozesse nicht wie erwartet funktionieren.

Ihr Mehrwert:
Es simuliert einen realen Cybervorfall, bei dem Teams gemeinsam erkennen, eindämmen, kommunizieren und wiederherstellen müssen. Sie stärkt die abteilungsübergreifende Zusammenarbeit, validiert Prozesse und festigt die technischen Grundlagen Ihrer Vorfallreaktion.

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

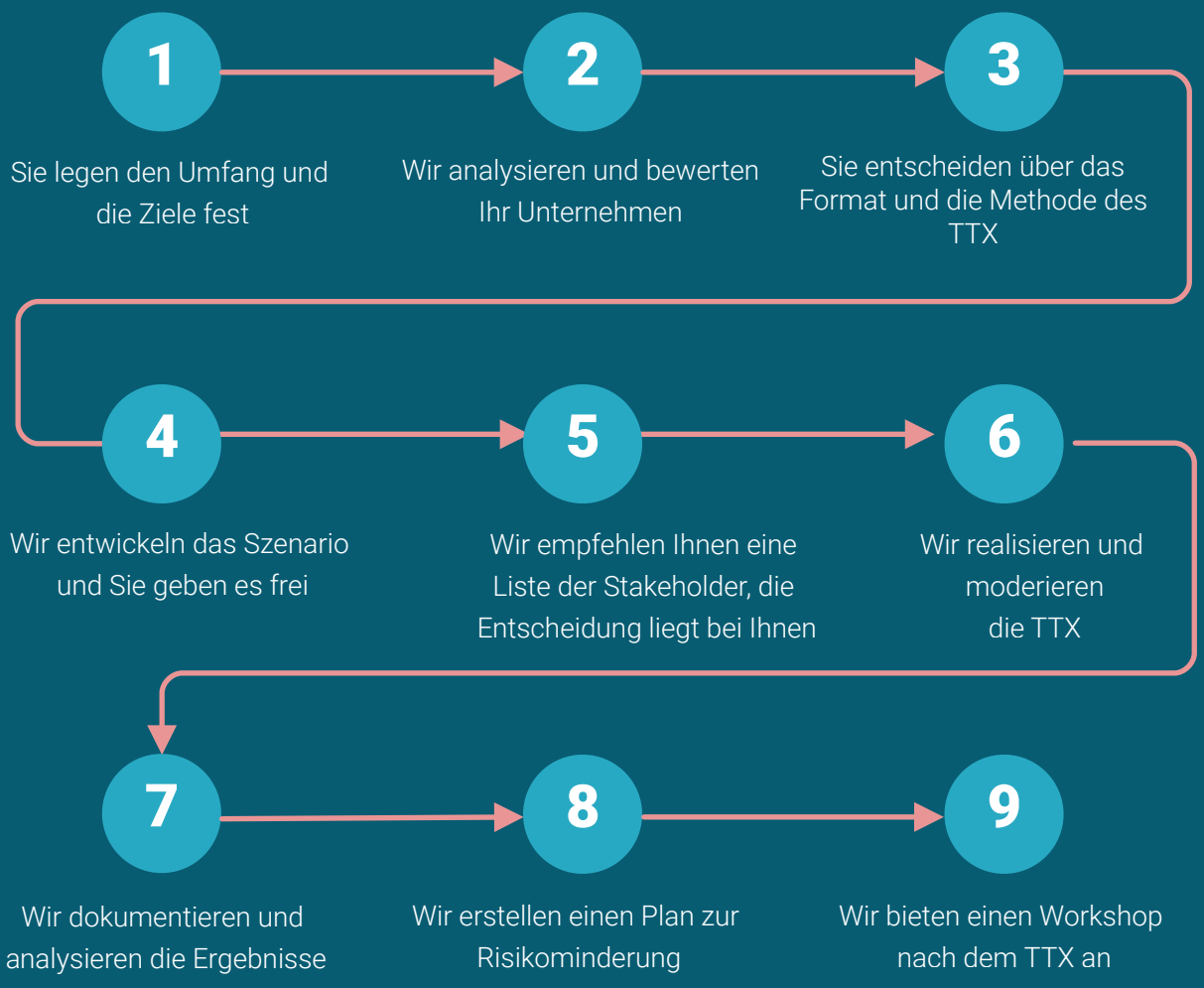
- **Das Format:** Wir passen die Übungen an Ihr Team und Ihre Ziele an, egal ob vor Ort, remote oder hybrid.
- **Motivierende Erfahrung:** Interaktive Moderation steigert die Aufmerksamkeit und das Engagement.
- **Professionelle Umsetzung:** Wir strukturieren die Sitzungen mit Tools, Visualisierungen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

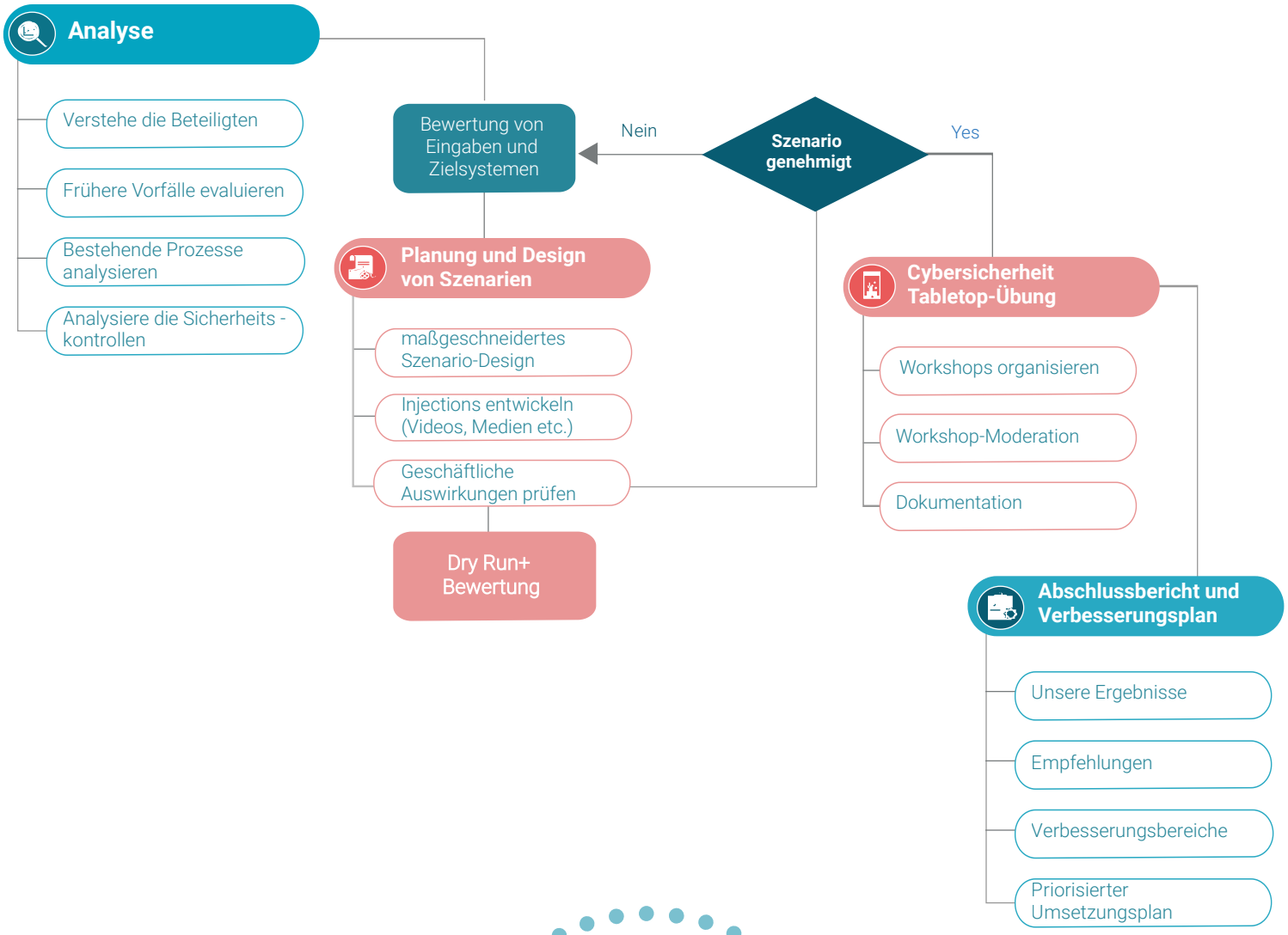
Ein klarer Fahrplan – von der Zieldefinition bis zur Umsetzung und Verbesserung



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, zu verstehen, **was für Ihr Unternehmen am wichtigsten ist**. Dazu gehören Ihre kritischen Vermögenswerte, wichtige Geschäftsprozesse und vorhandene Dokumentationen wie Backup-, Geschäftskontinuitäts- und Notfallpläne. Auf dieser Grundlage entwickeln wir Übungen, **die realistisch, relevant und vollständig auf Ihre Umgebung abgestimmt sind**.

Maßgeschneiderte Szenarien, die Ihre Risikolandschaft widerspiegeln

Wir entwickeln unsere Cyber-Incident-Szenarien **auf Grundlage Ihres spezifischen Bedrohungsprofils.** Diese können schrittweise an Komplexität zunehmen, um Ihre Teams herauszufordern und ihre Entscheidungsfähigkeit unter Druck zu testen. **Jedes Szenario bewertet, wie gut Ihr Unternehmen gemäß Ihren Notfallverfahren und Sicherheitsrichtlinienreagieren kann**.

Moderation durch Experten und Real-Time Feedback

Unsere Spezialisten leiten Ihr Team in **einem strukturierten und ansprechenden Format** durch die Übung. Die Teilnehmer erhalten während des Szenarios kontextbezogene Updates, realistische Entwicklungen und direktes Feedback. **Dieser Ansatz fördert sinnvolle Diskussionen und realistische Entscheidungsfindungen**.

Umsetzbare Erkenntnisse und umfassender Ergebnisbericht

Nach Abschluss der Exercise erhalten Sie einen **übersichtlichen und detaillierten Bericht**. Darin wird Ihre Leistung anhand interner Standards und bewährter Branchenpraktiken bewertet. Der Bericht hebt Stärken hervor, zeigt Schwächen auf und enthält **priorisierte Empfehlungen zur Verbesserung Ihrer Fähigkeiten im Umgang mit Vorfällen.**

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