TABLETOP EXERCISES

TESTEN UND STEIGERN SIE IHRE RESILIENZ

Zusammenarbeit.
Sicher.

AwareTec GmbH

INHALT

ZUSAMMENFASSUNG

Cybersicherheits-Tabletop-Übungen sind stärker als traditionelle, diskussionsbasierte Formate. Denn die heutige Bedrohungslage erfordert mehr als nur vorab festgelegte Gespräche. Sie verlangt stattdessen informationsgestützte Erfahrungen, die die Komplexität realer Vorfälle widerspiegeln.

Dieser Katalog präsentiert 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.

COO

Irina Nork

TTX-AUSWIRKUNG

Warum Tabletops wichtig sind: Unsicherheit in Cyber-Bereitschaft verwandeln

Strategische Auswirkungen

- 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 die 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)

TTX-FORMATE

Wir bieten folgende Formate von TTX-Übungen an

Diskussionsbasiert

Stärken Sie Ihre strategische Bereitschaft durch gezielte, wirkungsvolle Gespräche

Eine strukturierte, moderierte Diskussion, die Ihre Führungskräfte und Abteilungsleiter durch einen hypothetischen Cybervorfall führt.

Dieses Format zeigt, wie Ihr Unternehmen unter Druck denkt, wie Entscheidungen getroffen werden und ob kritische Lücken in den Rollen, Eskalationswegen oder im Verständnis der Vorschriften bestehen.

Ihr Vorteil:

Diskussionsbasierte Übungen sind ideal für Führungskräfte und Notfallbeauftragte und bieten eine leicht zugängliche und dennoch aufschlussreiche Einführung in das Krisenmanagement ohne technische Komplexität.

Praxisorientiert

Testen Sie die Echtzeitkoordination und Teamagilität in einer kontrollierten Umgebung

Eine interaktive Übung, mit der getestet wird, wie gut Ihre technischen und operativen Teams bei der Reaktion auf einen simulierten Cybervorfall zusammenarbeiten.

Oftmals können Kommunikationsprobleme verheerender sein als der Angriff selbst. In praktischen Übungen werden Schwachstellen identifiziert, bevor sie Sie Zeit, Geld oder Ihren guten Ruf kosten.

Ihr Vorteil:

Diese Übungen trainieren das Muskelgedächtnis und decken Verfahrenslücken auf – so reagieren Ihre Teams im Ernstfall nicht nur, sondern handeln zielgerichtet.

Szenariobasierte Tabletop-Übungen

Testen Sie Ihren vollständigen Reaktionsplan unter realistischen Bedingungen

Eine maßgeschneiderte, ereignisspezifische Simulation, bei der Ihr Team in Echtzeit auf eine Cyber-Bedrohung reagieren muss.

Dies ist die realistischste Simulation einer Cyber-Krise, ohne dass dabei ein tatsächliches Risiko besteht. Diese Übungen zeigen, ob Ihre Pläne, Tools und Mitarbeiter wirklich bereit sind.

Ihr Vorteil:

Diese hochpräzise Übung hilft Ihnen dabei, Schwachstellen in Ihren Tools und Richtlinien zu identifizieren und so Ihre Cyber-Resilienz messbar zu verbessern.

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

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 und 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

- **Individuell & realistische Szenarien:** Wir entwickeln Szenarien, die auf Ihre Branche, Bedrohungslage und Geschäftsprozesse zugeschnitten sind, sodass sie die in der Bewertung ermittelten tatsächlichen Risiken widerspiegeln.
- **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 – sämttliche Perspektiven sind entscheidend
- **Entscheidungsträger vs. operative Mitarbeiter**: Unsere Übungen bringen Entscheidungsträger und operative Teams in einen realitätsnahen Dialog.

Durchführungsstil, Engagement Und Logistik

- **Das passende Format:** Ob vor Ort, remote oder hybrid, wir gestalten die Übung so, wie es zu Ihrem Team und Ihren Zielen passt.
- **Motivierendes Erlebnis**: Gamification-Elemente und interaktive Moderation sorgen für hohe Aufmerksamkeit und starke Beteiligung.
- **Professionelle Umsetzung:** Mit Tools, Visuals und Impulsen strukturieren wir die Sitzung effizient für messbare Ergebnisse.

TTX-METHODIK

Wie wir TTX realisieren – methodisch, relevant, wirksam

Hack Your Plan

- **Ziel:** Aufdeckung von Schwachstellen in Ihrem bestehenden Incident-Response-Plan. Wo fehlen klare Verfahren? Wo kommt es zu Verzögerungen oder Missverständnissen? Wir spielen ein Szenario durch, das gezielt Ihre bekannten Schwachstellen ausnutzt
- **Empfohlenes Format:** szenariobasierte Übung
- **Teilnehmer:** IT-Sicherheit, Notfall-/Incident-Response-Team, Fachabteilungen
- **Intensität:** Hoch
- **Mehrwert:** Ihre IR-Strategie wird in Echtzeit getestet und Schwachstellen werden identifiziert, bevor ein Notfall eintritt

Real-World Threat Intelligence

- **Ziel:** Simulation auf Basis realer Angriffsvektoren und Bedrohungsinformationen. Diese Übung basiert auf realen, aktuellen Bedrohungsszenarien aus Ihrer Branche. Wir simulieren, wie sich diese auf Ihr Unternehmen auswirken würden – mit konkreten Konsequenzen
- **Empfohlenes Format:** Szenariobasierte Übung
- **Teilnehmer:** IT, OT, CISO-Team, externe Partner möglich
- **Intensität:** mittel bis hoch
- **Mehrwert:** realistische Analyse der aktuellen Bedrohungslage und Stärkung der Widerstandsfähigkeit gegenüber „echten“ Risiken

Strategische Übungen auf Führungsebene

- **Ziel:** Sie werden durch eine simulierte Cyberkrise geführt, deren Schwerpunkt auf Entscheidungsprozessen unter Unsicherheit, interner und externer Kommunikation, Eskalation und Verantwortlichkeiten auf Führungsebene liegt
- **Empfohlenes Format:** diskussionsbasiert
- **Teilnehmer:** Geschäftsleitung, Management, PR, Rechtsabteilung, Compliance
- **Intensität:** mittel
- **Mehrwert:** Fördert strategisches Denken, Kommunikationsfähigkeiten in Krisen und die Koordination zwischen Führungskräften und technischen Mitarbeitern

Red Team vs. Blue Team

- **Ziel:** Angriffssimulation mit direktem Gegner – Angriff gegen Verteidigung. Während das rote Team simulierte Angriffe ausübt, muss das blaue Team in Echtzeit reagieren. Diese Übung fördert die Kommunikation, Geschwindigkeit und Koordination innerhalb Ihrer Cyberabwehr
- **Empfohlenes Format:** praxisorientiert
- **Teilnehmer:** IT, SOC, Security Operations, Netzwerk- und Systemadministratoren
- **Intensität:** sehr hoch
- **Mehrwert:** Echtzeit-Stresstest für Ihre Verteidigungsprozesse und Teamkoordination unter Druck

TTX-PROZESS

Unser bewährter 5-Stufen-Prozess für Tabletops

Schritt 1- Planung

- Ziele und Vorgaben definieren
- Die Unternehmenskultur verstehen
- Wichtige Stakeholder identifizieren
- Das Szenario auswählen und strukturieren
- Logistik und Zeitplan koordinieren

Geschätzte Dauer: 1- 2 Wochen

Schritt 2 - Szenario-Entwurf

- Recherche und Szenarioentwurf
- Entwicklung von Leitfäden und Materialien
- Genehmigung des Szenarios durch die Stakeholder
- Entwurf von Injects (z. B. Social Media, visuelle Elemente)
- Finalisierung des Szenarios

Geschätzte Dauer: 2 - 5 Wochen

Schritt 3 - Vorbereitung

- Festlegung des Übungsplans
- Verteilung der Vorab-Unterlagen
- Überprüfung der Injects mit dem Durchführungsteam
- Koordination mit den Beteiligten
- Vorbereitung der Logistik (Imbiss und Verbrauchsmaterialien)

Geschätzte Dauer: 1 Woche

Schritt 4 - Umsetzung

- Vorbereitung des Veranstaltungsortes für die Sitzung
- Realisierung und Moderation der Übung
- Dokumentation der Ergebnisse

Geschätzte Dauer: 4 - 8 Stunden

Schritt 5 - Analyse & Report

- Analyse der Übungsergebnisse
- Identifizierung von Lücken und Optimierungsbereichen
- Erstellung und Präsentation eines After-Action-Reports (AAR)
- Anpassung der erforderlichen Änderungen am AAR
- Entwicklung eines Plans zur Behebung der Mängel

Geschätzte Dauer: 1 - 3 Wochen

TTX – Ablauf von Anfang bis Ende

1. Sie legen den Umfang und die Ziele fest
2. Wir analysieren und bewerten Ihr Unternehmen
3. Sie entscheiden über das Format und die Methode der TTX-Datei
4. Wir entwickeln das Szenario und Sie geben es frei
5. Wir empfehlen Ihnen eine Liste der Stakeholder, die Entscheidung liegt bei Ihnen
6. Wir realisieren und moderieren den TTX
7. Wir dokumentieren und analysieren die Ergebnisse
8. Wir erstellen einen Plan zur Risikominderung
9. Wir bieten einen Workshop nach dem TTX an

IHR WERT

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 führen 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.

WARUM MIT UNS ZUSAMMENARBEITEN?

Kompetenz

Weltweite Experten für defensive und offensive Cybersicherheit. Wir bringen unsere operative und strategische Expertise für Sie ein.

Maßgeschneidert für Tech-Teams und Führungskräfte

Unsere Formate beziehen alle Ebenen Ihres Unternehmens ein, vom IT-Personal bis zur Führungsetage, und gewährleisten so eine einheitliche Entscheidungsfindung, Kenntnis der regulatorischen Rahmenbedingungen und Kommunikation unter Druck.

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.

Get Started

Termin vereinbaren

Oder kontaktieren Sie uns: mail@awaretec.de