SOPHOS

So gestalten Sie Tabletop-Übungen für Ihre Cybersecurity

Best Practices für Tabletop-Übungen zur Vorbereitung Ihres Unternehmens auf Cyberangriffe

Sophos-Whitepaper. Juli 2024

Einführung

Im Rahmen von Tabletop-Übungen werden Szenarien simuliert und geplante Reaktionsmaßnahmen durchgespielt. So können Sie die Handlungsfähigkeit Ihrer Teams und die Effektivität Ihrer Prozesse in der Praxis prüfen. Diese Übungen haben sich als wertvolles Instrument zur Vorbereitung auf schwierige Situationen bestens bewährt. So erprobt etwa das Militär verschiedene Strategien in Konfliktsituationen mit Hilfe von Tabletop-Übungen. Regierungen wiederum führen diese Übungen durch, um ihr Krisenmanagement zu verbessern. Unternehmen und Organisationen können sich mit Tabletop-Übungen effektiv auf mögliche Cyberangriffe vorbereiten.

In diesem Guide erfahren Sie mehr über Tabletop-Übungen für die Cybersecurity und ihren Ablauf. Der Guide basiert auf unserem eigenen Ansatz, mit dem unser Cybersecurity-Team unser Unternehmen auf Angriffe vorbereitet.

Transparenz zählt zu den Kernwerten unserer Unternehmensphilosophie und wir freuen uns, unsere Strategien und Ressourcen mit Ihnen teilen zu können. Weitere Einblicke und Ressourcen finden Sie in unserem Trust Center.

Was sind Tabletop-Übungen in der Cybersecurity?

Eine Tabletop-Übung spielt einen Cyberangriff durch und analysiert mögliche Schäden. So erkennen Sie, in wie weit Ihr Unternehmen in der Lage ist, auf einen Angriff zu reagieren. Zudem erhalten Sie wichtige Einblicke in Ihre Cybersecurity, mit denen Sie Ihre Strategie optimieren können.

Warum sind diese Übungen wichtig?

Erkennen blinder Flecken: Mit Tabletop-Übungen ermitteln Sie Schwachstellen in Ihrer Cyberabwehr, bevor Cyberkriminelle diese finden und ausnutzen können.

Sicherheitsstatusanalyse: Die Übungen ermöglichen Ihnen, Ihren Sicherheitsstatus zu bewerten und zu optimieren.

Kommunikationsanalyse: Tabletop-Übungen können Kommunikationsprobleme zwischen Abteilungen aufzeigen, die die Reaktion auf Cyberangriffe beeinträchtigen können.

Compliance: In vielen stark reglementierten Branchen müssen Tabletop-Übungen in der Cybersecurity im Rahmen von Sicherheitsprogrammen zur Vorbereitung auf Vorfälle sogar durchgeführt und dokumentiert werden.

Reaktionsfähigkeit: Indem die Reaktion auf einen simulierten Vorfall durchgespielt wird, üben die Teilnehmer, welche Maßnahmen sie bei einem echten Angriff ergreifen müssen. So können sie diese im Ernstfall schneller umsetzen.

Unterschiedliche Tabletop-Übungen für die Cybersecurity

Es gibt verschiedene Arten von Tabletop-Übungen, die jeweils unterschiedlich lange dauern und unterschiedliche Vorteile bieten.

Rapid-Fire-Szenarien

Laut ISACA sind Rapid-Fire-Szenarien „sehr allgemein gehalten und sollen einfach und schnell verstanden und besprochen werden können". Hierfür sind keine oder nur wenige Vorbereitungen nötig und der Zeitaufwand beträgt 10 bis 30 Minuten.

An Rapid-Fire-Szenarien können Mitarbeiter in nicht leitender, mittlerer und leitender Funktion aus unterschiedlichen Abteilungen teilnehmen. Dabei spielen die Teilnehmer unterschiedliche Sicherheitsszenarien durch und schlüpfen jeweils in die Rolle eines Incident-Responders.

Rein technische Szenarien

Rein technische Szenarien dauern in der Regel ein bis zwei Stunden. Bei diesen Szenarien liegt der Schwerpunkt auf den technischen Aspekten, die ausführlich diskutiert werden. Diese Szenarien müssen minutiös geplant werden, sodass die Teams die entsprechenden Einflussfaktoren eines Sicherheitsvorfalls analysieren können.

In der Regel gehen rein technische Szenarien von einem „Kern"-Ereignis aus. Im Verlauf der Übung können Sie weitere Details hinzufügen. Mit diesen Übungen können sich Teams auf komplexe Cyberangriffe vorbereiten.

Szenarien mit allen Stakeholdern

Szenarien mit allen Stakeholdern gehen über rein technische Szenarien hinaus. Sie konzentrieren sich auf technische und nicht technische sowie logistische Fragestellungen.

Ein Szenario mit allen Stakeholdern nimmt in der Regel zwei bis vier Stunden in Anspruch. Daran können technische Teams sowie Vertreter der Rechts-, Marketing- und Personalabteilung teilnehmen.

Szenarien mit allen Stakeholdern bieten sich insbesondere für Unternehmen und Organisationen an, die die abteilungsübergreifende Kommunikation verbessern möchten. Dabei kann es von Vorteil sein, sowohl technisches als auch nicht technisches Personal in Tabletop-Übungen mit allen Stakeholdern einzubeziehen. Auf diese Weise können Mitarbeiter aus unterschiedlichen Teams oder Abteilungen zusammen an der Behebung eines Sicherheitsproblems arbeiten.

Manche Unternehmen bitten bestimmte Teams oder Abteilungen, sich zu unterschiedlichen Zeitpunkten während des Szenarios einzubringen. So würde die Vorgehensweise auch für die jeweiligen Teams bzw. Abteilungen bei einem realen Sicherheitsvorfall aussehen.

Wer führt Tabletop-Übungen in der Cybersecurity durch?

Tabletop-Übungen können von internen oder externen Teams durchgeführt werden. Beide Optionen bieten jeweils unterschiedliche Vorteile.

Extern

Externe Tabletop-Serviceanbieter im Bereich Cybersecurity stellen Szenarien bereit, verwalten diese und leiten Diskussionen an. Der Aufwand für die Vorbereitung und Durchführung der Übungen ist für Sie dabei minimal.

Der externe Anbieter passt die Tabletop-Übung in der Regel an Ihr Unternehmen und Ihre Umgebung an. Dazu informiert sich der Anbieter über Ihr Unternehmen und Ihre potenziellen Sicherheitsgefährdungen und arbeitet ein speziell auf Ihr Unternehmen abgestimmtes Szenario aus.

Intern

Sie können Ihre eigenen Sicherheitsübungen konzipieren. Zwar geht dies häufig mit einem hohen zeitlichen und finanziellen Aufwand einher, doch können Sie so sicherstellen, dass Ihre Cybersecurity-Übungen ganz auf Ihr Unternehmen und Ihre Umgebung zugeschnitten sind. Ein Beispiel: Wenn Sie Systeme einbeziehen, die Ihre Mitarbeiter täglich nutzen, wirkt das Szenario praxisnaher und die Teilnehmer arbeiten engagierter mit.

Zudem können Mitarbeiter bei unternehmensinternen Tabletop-Übungen gemeinsam Probleme ermitteln und erörtern, die sich auf das Unternehmen, die Belegschaft und seine Kunden auswirken.

Der Ansatz von Sophos

Bei Sophos erstellen wir individuelle Tabletop-Cybersecurity-Übungen für bestimmte Teams bzw. Abteilungen. Dabei gehen wir in der Regel von einem kleinen Sicherheitsproblem aus. Dabei haben die Teilnehmer die Gelegenheit, ihre Strategien und Ideen auszutauschen. Anhand der Erkenntnisse beleuchten wir dann den Schweregrad des Problems.

Im Folgenden finden Sie einige Beispiele für von uns durchgeführte Szenarien. Sie können diese als Vorlage für Ihre eigenen Tabletop-Übungen nutzen.

ABTEILUNG	SZENARIO
Sophos X-Ops	Interne Bedrohung
HR	Ransomware und Verlust personenbezogener Daten durch einen Mitarbeiter
Technischer Support	Gezielter Angriff durch eine Person, die sich als Kunde ausgibt
Marketing	Manipulation (Defacement) der Unternehmenswebsite und sozialen Medien durch über einen Mitarbeiter kompromittierte Ressourcen
Rechtsabteilung	Böswilliger Bug-Bounty-Researcher
Sophos X-Ops	Kompromittiertes Analystensystem, Angriff auf die Lieferkette
Engineering	Kompromittierte Sophos-Binärdateien, Angriff auf die Lieferkette
Engineering	Von Phishing betroffener Mitarbeiter
IT	Schwerwiegender Ransomware-Vorfall
Engineering	Zero-Day-Schwachstelle in Anwendung führt zu Kompromittierung von Kundendaten

Best Practices zur Entwicklung einer Cybersecurity-Tabletop-Übung

Die folgenden Best Practices unterstützen Sie bei der Ausarbeitung effektiver Tabletop-Übungen für die Cybersecurity:

1. Bestimmen Sie Ihre Zielgruppe

Bestimmen Sie zunächst Ihre Zielgruppe und entwickeln Sie dann Ihr Cybersecurity-Szenario. Komplexe Szenarien eignen sich sehr gut, wenn Sie Übungen für Ihr Cybersecurity-Team konzipieren. Wählen Sie für Ihre IT oder DevOps ein Problem, das die Teilnehmer verstehen und dem sie sich entsprechend konzentriert widmen.

2. Wählen Sie die richtigen Teilnehmer aus

Überlegen Sie, ob Sie einzelne oder mehrere Teams oder Abteilungen in das Security-Szenario einbeziehen möchten. In Szenarien mit einem einzelnen Team lässt sich feststellen, wie bestimmte Teilnehmer auf einen Cyberangriff reagieren. Wenn Sie dagegen mehrere Teams oder Abteilungen beteiligen, können Stakeholder aus unterschiedlichen Geschäftsbereichen an der Behebung eines Sicherheitsvorfalls arbeiten.

3. Bestimmen Sie, wann Beteiligte eingebunden werden sollen

Überlegen Sie sich, wann Sie die jeweiligen Teams oder Abteilungen in Ihr Cybersecurity-Szenario einbeziehen möchten. Sind etwa personenbezogene Daten kompromittiert, müssen Sie eventuell Mitarbeiter aus Ihrer Rechtsabteilung einbeziehen, um die Einhaltung der DSGVO und anderer Datenschutzbestimmungen zu gewährleisten.

Dabei empfiehlt sich, dass sich mindestens ein Mitarbeiter aus allen Teams oder Abteilungen Ihres Unternehmens an einem Security-Szenario beteiligt. Auf diese Weise fördern Sie die abteilungsübergreifende Kommunikation und Zusammenarbeit.

4. Legen Sie die Teilnehmeranzahl fest

Stellen Sie sicher, dass Ihr Szenario Teilnehmer umfasst, die aufeinander eingehen und zusammenarbeiten können, um gemeinsame Ziele zu erreichen. Wir beziehen häufig bis zu 25 Mitarbeiter aus unterschiedlichen Ebenen eines Teams oder einer Abteilung oder mehrerer Teams oder Abteilungen in unsere Szenarien ein. Berücksichtigen Sie bei der Festlegung der Teilnehmeranzahl die Größe Ihrer Organisation bzw. Ihres Unternehmens sowie die Struktur Ihrer Teams und Abteilungen.

5. Erstellen Sie einen Zeitplan für Ihre Übung

Geben Sie den Teilnehmern ausreichend Zeit für die Tabletop-Übung. Bei Sophos versuchen wir jedoch, langwierige Tabletop-Übungen zu vermeiden. Denn es ist nicht immer einfach, einen Termin zu finden, an dem alle Teilnehmer für mehrere Stunden verfügbar sind.

6. Bereiten Sie Ihre Materialien vor

Präsentieren Sie Ihr Szenario mit PowerPoint oder anderen Materialien. Bei Sophos arbeiten wir in der Regel mit PowerPoint-Präsentationen. Jede Folie zeigt dabei den Verlauf der Ereignisse und umfasst Fragen, die die Teilnehmer berücksichtigen sollen. Meist beschränken sich die PowerPoint-Präsentationen für diese Übungen auf maximal 20 Folien.

7. Erarbeiten Sie Ihre Tabletop-Story

Entwickeln Sie das theoretische Gerüst, die Story, und reichern Sie sie mit individuell darauf zugeschnittenen Informationen an. Mit tagesaktuellen Nachrichten wecken Sie die Aufmerksamkeit der Teilnehmer. Bei ausführlichen Stories können Sie Hinweise in Systeme und Protokolle einfügen, die die Teilnehmer finden und nachverfolgen können.

8. Passen Sie Ihre Tabletop-Übung an Ihre Teilnehmer an

Passen Sie Ihre Cybersecurity-Tabletop-Übung an das Know-how Ihrer Teilnehmer in puncto Cybersicherheit an. So eignen sich besonders ausführliche Stories vor allem für Teilnehmer mit umfangreicher Fachkenntnis im Bereich Cybersecurity. In anderen Situationen sind allgemeiner gehaltene Szenarien meist sinnvoller.

Falls Sie umfangreiche Szenarien konzipieren, achten Sie darauf, dass diese realitätsbasiert sind. Wenn Sie etwa eine bestimmte Zielgruppe in Ihrem Unternehmen oder Netzwerk ansprechen möchten, informieren Sie sich zunächst bei einem Spezialisten über diesen Bereich. So können Sie ein Szenario entwickeln, das Ihre Zielgruppe anspricht.

9. Holen Sie Feedback von den Teilnehmern ein

Bitten Sie die Teilnehmer ihre Ideen, die Sie in Ihre Übung einfließen lassen können, einzubringen. Meist geben Ihnen Teilnehmer Aufschluss über Sicherheitsprobleme, die ihnen täglich begegnen. Wenn Sie diese Probleme in Ihr Szenario einbinden, können Teilnehmer im Verlauf der Übung Lösungsansätze für die Zukunft ausarbeiten.

10. Skizzieren Sie Ihr Szenario

Erstellen Sie ein Flussdiagramm zum Ablauf Ihres simulierten Angriffs. So können Sie mögliche Lücken in Ihrer Story ermitteln. Holen Sie auch das Feedback von Mitarbeitern ein, die mit den in Ihrem Szenario thematisierten Problemen vertraut sind. Mit diesem Feedback schließen Sie die Lücken und gestalten Ihr Szenario realistisch.

11. Bereiten Sie Diskussionsfragen vor

Schreiben Sie alle Fragen auf, die bei der Ausarbeitung Ihres Szenarios aufkommen. So regen Sie die Diskussion unter den Teilnehmern an.

12. Überprüfen Sie Ihre Story

Arbeiten Sie Ihr Szenario mehrmals durch, bevor Sie es den Teilnehmern präsentieren. Es lässt sich nicht immer einfach abschätzen, wie lange die Teilnehmer benötigen, um das Szenario durchzuspielen. Planen Sie im Zweifelsfall mehr Zeit ein. Wenn Ihre Präsentation die den Teilnehmern zur Verfügung stehende Zeit übersteigt, überarbeiten Sie sie nach Bedarf.

13. Geben Sie den Ton für Ihre Übung vor

Ermutigen Sie alle Teilnehmer – unabhängig von ihrer Position und Erfahrung im Unternehmen – gleich bei ihrem Eintreffen, aktiv an der Übung mitzuwirken. Die Übung bietet allen Teilnehmern die Möglichkeit, sich aktiv einzubringen und den Sicherheitsstatus des Unternehmens zu verbessern. Je mehr Teilnehmer miteinander kommunizieren und zusammenarbeiten, desto größer ist der Nutzen, den alle aus der Übung ziehen.

14. Moderieren Sie die Übung

Damit die Übung inhaltlich und zeitlich nach Plan abläuft, muss sie angeleitet werden. Der Moderator darf sich jedoch nicht selbst beteiligen. Als Moderator können Sie den Teilnehmern das Szenario präsentieren und ihnen dabei helfen, es zu durchlaufen. Zudem können Sie den Teilnehmern Zeit einräumen, um verschiedene Aspekte des Szenarios zu diskutieren, und Diskussionsfragen und -anregungen einfließen lassen.

15. Dokumentieren Sie Probleme

Stellen Sie sicher, dass im Verlauf der Übung ermittelte Probleme aufgezeichnet werden. So gewinnen Sie Einblicke in Probleme, die die Wirkung Ihrer Story beeinträchtigen könnten.

16. Behalten Sie die Zeit im Auge

Erstellen Sie einen Zeitplan für die Übung und halten Sie ihn ein. Stellen Sie sicher, dass sich die Teilnehmer an die Zeitvorgaben halten, und fordern Sie sie bei Bedarf auf, weiter an der Story zu arbeiten.

17. Überprüfen Sie Ihre Ergebnisse

Überlegen Sie im Anschluss an die Übung, wie Sie die Ergebnisse in das Tagesgeschäft Ihrer Organisation/Ihres Unternehmens integrieren können. Wenn Sie die Übung beispielsweise auf der Basis von Compliance-Anforderungen durchgeführt haben, erstellen Sie ein PDF mit den Informationen, die Auditoren benötigen.

Sie können die Erkenntnisse auch mit den Teilnehmern teilen und die gleiche Übung zu einem späteren Zeitpunkt wiederholen. So lässt sich feststellen, ob im Rahmen der ersten Übung ermittelte Probleme behoben wurden.

Beispiel für eine Ransomware-Tabletop-Übung

Über folgenden Link können Sie ein Ransomware-Tabletop-Szenario nachlesen, das wir bei Sophos konzipiert und durchgeführt haben: Ransomware-Tabletop.

Sie können dieses gerne direkt verwenden oder als Grundlage für Ihre eigenen Szenarien nutzen.

Tabletop-Ressourcen zur Cybersicherheit

Die US-Behörde Cybersecurity and Infrastructure Security Agency (CISA) stellt Ressourcen bereit, die Unternehmen bei der Durchführung ihrer eigenen Tabletop-Übungen unterstützen sollen. Sie können mehr als 100 Tabletop-Übungen der CISA (CTEPs) abrufen, die diverse Bedrohungsszenarien nachbilden, wie etwa:

- ✓ Cybersecurity: Ransomware, interne Bedrohungen, Phishing, Kompromittierung von ICS (Industrial Control System) sowie weitere Cybersecurity-Szenarien.
- ✓ Physische Sicherheit: Amoklauf, mutwillige Fahrzeugkollision, improvisierter Sprengsatz, unbemanntes Luftfahrtsystem sowie weitere Szenarien aus dem Bereich der physischen Sicherheit.
- ✓ Kombination aus physischer und Cybersicherheit: Schwerpunkt auf physischen Bedrohungsvektoren und ihren Auswirkungen auf die Cybersicherheit.

Zudem bietet die CISA vorkonfigurierte Vorlagen, mit denen Sie Ihre eigenen Tabletop-Übungen entwickeln können.

Fazit

Da Tabletop-Übungen nachweislich funktionieren, spielen sie in der Cybersecurity von heute eine zentrale Rolle bei der Vorbereitung auf potenzielle Vorfälle. Cyberbedrohungen nehmen im digitalen Zeitalter immer größere Ausmaße an. Unternehmen und Organisationen, die Tabletop-Übungen einführen und weiterentwickeln, können sich besser vor Bedrohungen schützen. Durch Kenntnis der Grundlagen von Tabletop-Übungen und der Anwendung der Best Practices in diesem Guide sind Unternehmen und Organisationen in der Lage, ihre Resilienz gegenüber Cyberangriffen weiter zu stärken. So sind sie im Ernstfall bestens vorbereitet.

Sophos Trust Center – https://www.sophos.com/de-de/trust

Ransomware-Tabletop von Sophos – https://assets.sophos.com/X24WTUEQ/at/hvsj54g5zq5hhcfb3xrfnmk/sophos-ransomware-tabletop-exercise-overview.pdf

Tabletop-Übungen der CISA – https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

Transparenz ist eine zentrale Komponente unserer Unternehmensphilosophie.
Weitere Einblicke und Ressourcen finden Sie in unserem Trust Center: www.sophos.de/trust

2024-07-24 (WP-DD)

SOPHOS