

Tabletop-Übung: Reagieren auf Vorfälle



Dauer
Zwei Stunden



**Anzahl der
Teilnehmenden**
Max. 30

Zielgruppe

Mitarbeitende von Unternehmen mit beliebigen technischen Vorkenntnissen, die im Incident-Response-Plan ihrer Organisation eine Rolle spielen

Überblick

Eine Tabletop-Übung ist eine angeleitete Simulation, in der die Teilnehmenden verschiedene Szenarien durchspielen. Dabei werden „in ruhigen Zeiten“ Abstimmungslücken und Schwachstellen identifiziert sowie Resilienz für den tatsächlichen Krisenfall aufgebaut, wenn es auf Echtzeit-Koordination ankommt. Es geht nicht um Perfektion, sondern darum, auf bestimmte Szenarien vorbereitet zu sein.

Lernziele

Nach der Übung können die Teilnehmenden:

- erläutern, wie wichtig ein Incident-Response-Plan im Arbeitsumfeld ist
- Rollen und Verantwortlichkeiten während eines Sicherheitsvorfalls identifizieren
- eine Situation schnell einordnen und während eines Sicherheitsvorfalls effektive Entscheidungen treffen

Materialien

- Incident-Response-Checkliste
- Timer oder Stoppuhr
- Rollenkarten für Teilnehmende (Leitung der IT-Sicherheit, Leitung der Vorfallkoordination, Leitung der Kommunikation, rechtlicher Beistand, Vertretung der Personalabteilung und Abteilungsleitung)
- Szenarienkarten für das Rollenspiel
- Whiteboard oder Flipchart
- Filzstifte
- Kugelschreiber und Notizblöcke

Funktionen in der Tabletop-Übung

Moderation: Aufgaben – Geschwindigkeit festlegen, Diskussionen anleiten, Szenarien anpassen, alle Teilnehmenden einbinden und Informationen bereitstellen

Teilnehmende: Aufgaben – entsprechende Rolle während der Simulation übernehmen, eigene Denkprozesse darlegen, Teammitglieder unterstützen und gemäß den Verantwortlichkeiten der Rolle reagieren

Bewertende: Aufgaben – Stärken und Schwächen beurteilen, Berichte für die Nachbesprechung erstellen und Übereinstimmung mit vorhandenen Plänen und Verfahren einschätzen

Beobachtende: Aufgaben – Fachwissen bereitstellen (ohne direkte Teilnahme an der Übung), Teilnehmende durch Stellen relevanter Fragen unterstützen und ggf. Anweisungen geben

Protokollführende: Aufgaben – Übungsaktivitäten dokumentieren, Diskussionen protokollieren, Lücken ermitteln, mit den offiziellen Verfahren vergleichen und Verbesserungen vorschlagen

Einführung

 **Dauer: 10 Minuten**

Wer effektiv auf Vorfälle reagieren will, benötigt klare Kommunikation, definierte Rollen und Anpassungsfähigkeit. Vermitteln Sie den Teilnehmenden, dass Szenarien und Herausforderungen simuliert werden, die so oder in ähnlicher Form eintreten können. Die Übung dient dazu, wichtige Kompetenzen im Umgang mit solchen Situationen zu entwickeln. Beim Umgang mit Vorfällen sind **Teamkoordination** und **schnelle Entscheidungsfähigkeit** gefordert.

Aktivität 1: Checkliste mit Sofortmaßnahmen

 **Dauer: 30 Minuten**

Materialien

- Timer oder Stoppuhr
- Kugelschreiber und Notizblöcke
- Incident-Response-Checkliste (Anhang zu Aktivität 1)

Aktivität

In dieser Aktivität werden der Incident-Response-Plan, die Kommunikationsstrategie und der Entscheidungsfindungsprozess getestet.

Präsentieren Sie das folgende Szenario:

„Ein wichtiger Server Ihrer Organisation wurde nach einem Ransomware-Angriff verschlüsselt. Die Kriminellen fordern für die Entschlüsselung einen hohen Betrag in einer Kryptowährung.“

Im Anschluss:

1. Händigen Sie allen Teilnehmenden die Incident-Response-Checkliste aus. Darauf sind gängige Schritte zum Reagieren auf Vorfälle in zufälliger Reihenfolge aufgeführt.
2. Alle Teilnehmenden erhalten 10 Minuten Zeit, die Schritte auf der Checkliste selbständig in die richtige Reihenfolge für das Ransomware-Szenario zu bringen.
3. Danach werden kleine Gruppen mit 3–4 Personen gebildet, in denen 10 Minuten lang die geordneten Checklisten durchgegangen werden. Jede Person schließt die Aufgabe jedoch eigenständig ab.
4. In den letzten 10 Minuten werden die Schritte zur effektiven Reaktion sowie die beste Reihenfolge in der gesamten Gruppe besprochen.

Antwortschlüssel

Laut branchenüblichen Best Practices gehören die folgenden wichtigen Elemente auf die Checkliste:

1. Vorfall sofort melden (gemäß der Eskalationsrichtlinie der Organisation)
2. Incident-Response-Team mobilisieren
3. Betroffene Systeme isolieren
4. Zeitlichen Verlauf des Vorfalls dokumentieren
5. Datenbackup-Status bewerten
6. Kommunikationsplan der Organisation aktivieren
7. Vorfall gemäß den geltenden Verfahren an Behörden melden
8. Rechtlichen Beistand in Anspruch nehmen
9. Richtlinie der Organisation zum Reagieren auf Lösegeldforderungen befolgen
10. Strafverfolgungsbehörden kontaktieren (gemäß der Richtlinie der Organisation)

Aktivität 2: Incident-Response-Simulation

 **Dauer: 35–60 Minuten**

Materialien

- Referenzkarten zur Organisation (Anhang zu Aktivität 2)
- Szenarienkarten mit Komplikationen (Anhang zu Aktivität 2)
- Timer oder Stoppuhr
- Whiteboard oder Flipchart
- Filzstifte
- Kugelschreiber und Notizblöcke
- Aktueller Incident-Response-Plan der Organisation

Aktivität

Im Rahmen dieser Aktivität werden funktionsübergreifende Reaktionsfähigkeiten anhand echter Rollen, interner und externer Kommunikationsstrategien und Entscheidungsfindungsprozessen in einer Vorfallsimulation mit Komplikationen getestet.

Bilden Sie Gruppen, die jeweils ein Incident-Response-Team darstellen. Die Teilnehmenden übernehmen ihre tatsächliche Rolle beim Reagieren auf Vorfälle oder wählen die Karte mit der ähnlichsten Rolle aus.

Anweisungen:

1. Jede Gruppe erhält eine Szenarienkarte, auf der ein Sicherheitsvorfall mit Komplikationen beschrieben wird.
2. Die Gruppen erhalten 20 Minuten Zeit, eine Reaktionsstrategie zu besprechen und zu formulieren – in den jeweils zugewiesenen Rollen und gemäß den Verfahren der Organisation.
3. Jede Gruppe präsentiert ihren Plan (5 Minuten pro Gruppe).
4. Im Anschluss wird eine Komplikation eingeführt (z. B. „Medien haben von dem Vorfall erfahren“).
5. Alle Gruppen erhalten nochmals 10 Minuten Zeit, um ihre Pläne basierend auf den neuen Informationen gemäß geltender Verfahren anzupassen.
6. Im Anschluss werden die angepassten Pläne präsentiert und erörtert, wie diese in das Regelwerk der Organisation passen.

Zusätzliche Anweisungen für Gruppen:

- Bei der Besprechung auf den tatsächlichen Incident-Response-Plan der Organisation Bezug nehmen
- „Laut denken“, um den Entscheidungsfindungsprozess sichtbar zu machen
- Beteiligung aller Teilnehmenden sicherstellen; dabei tatsächliche Verantwortlichkeiten berücksichtigen
- Konzentration auf realistische Handlungen im Rahmen der eigenen Rolle

Diskussion

 **Dauer: 15 Minuten**

Fragen

- Inwiefern hat die Übung zur Anordnung der erforderlichen Schritte aus Aktivität 1 bei der Vorbereitung auf die Simulation mit den zugewiesenen Rollen geholfen?
- Welche Herausforderungen bestanden bei der Anwendung der tatsächlichen Verfahren Ihrer Organisation?
- Welche Lücken konnten im aktuellen Incident-Response-Verfahren identifiziert werden?
- Wie gut hat die funktionsübergreifende Kommunikation während der Übungen funktioniert?
- Welche zusätzlichen Trainings oder Ressourcen würden Ihnen Ihrer Meinung nach helfen, in Ihrer Rolle besser auf solche Szenarien vorbereitet zu sein?

Mögliche Antworten/Aufgaben

- Herausforderungen: Koordinierung zwischen Abteilungen, Zugriff auf Kontaktdaten, Klärung der tatsächlichen Verantwortlichkeiten und Klärung der Entscheidungsmacht
- Lücken: keine festgelegten Eskalationspfade, veraltete Kontaktdaten, keine festgelegten Autoritäten, fehlende Benachrichtigungsvorlagen
- Verbesserungen: regelmäßiges, abteilungsübergreifendes Training, aktualisierte Kontaktlisten, übersichtlichere Entscheidungsbäume, rollenspezifische Schnellanleitungen
- Ressourcen: rollenspezifische Reaktionskarten, regelmäßige Übungen im Team, aktualisiertes IR-Plan-Training

Fazit

 **Dauer: 5 Minuten**

Wichtige Erkenntnisse aus beiden Übungen zusammentragen:

- Die Übung zur Anordnung der erforderlichen Schritte hat mehr Verständnis für die Verfahren zum Reagieren auf Vorfälle der Organisation geschaffen. Die Simulation mit den Rollen hat Herausforderungen bei der Koordination ans Licht gebracht.
- Sowohl die individuelle Vorbereitung wie auch die koordinierte Reaktion im Team anhand von tatsächlichen Rollen sind für ein effektives Reagieren auf Vorfälle wichtig.
- Mit Komplikationen ist nahezu immer zu rechnen. Der Erfolg ist abhängig von der Anpassungsfähigkeit etablierter Verfahren.

Nächste Schritte

- Aktualisierung des Incident-Response-Plans Ihrer Organisation basierend auf den identifizierten Lücken
- Aktualisierung von Kontaktlisten und Kommunikationsprotokollen
- Schließen der identifizierten Lücken
- Planung regelmäßiger Tabletop-Übungen mit Mitgliedern des Incident-Response-Teams für kontinuierliche Verbesserungen

Anhang zu Aktivität 1 – Incident-Response-Checkliste

Drucken Sie die Checkliste für alle Teilnehmenden aus. Schneiden Sie entlang der Linien, um einzelne Karten für die Teilnehmenden zu erhalten. Wenn Sie diese auf Karton oder schwerem Papier drucken, können Sie die Karten öfter wiederverwenden.



Checkliste mit Sofortmaßnahmen

- ☐ Betroffene Systeme isolieren
- ☐ Vorfall sofort melden (gemäß der Eskalationsrichtlinie der Organisation)
- ☐ Datenbackup-Status bewerten
- ☐ Strafverfolgungsbehörden kontaktieren (gemäß der Richtlinie der Organisation)
- ☐ Rechtlichen Beistand in Anspruch nehmen
- ☐ Richtlinie der Organisation zum Reagieren auf Lösegeldforderungen befolgen (Beratung erforderlich)
- ☐ Kommunikationsplan der Organisation aktivieren
- ☐ Zeitlichen Verlauf des Vorfalls dokumentieren
- ☐ Vorfall gemäß den geltenden Verfahren an Behörden melden
- ☐ Incident-Response-Team mobilisieren

Checkliste mit Sofortmaßnahmen

- ☐ Betroffene Systeme isolieren
- ☐ Vorfall sofort melden (gemäß der Eskalationsrichtlinie der Organisation)
- ☐ Datenbackup-Status bewerten
- ☐ Strafverfolgungsbehörden kontaktieren (gemäß der Richtlinie der Organisation)
- ☐ Rechtlichen Beistand in Anspruch nehmen
- ☐ Richtlinie der Organisation zum Reagieren auf Lösegeldforderungen befolgen (Beratung erforderlich)
- ☐ Kommunikationsplan der Organisation aktivieren
- ☐ Zeitlichen Verlauf des Vorfalls dokumentieren
- ☐ Vorfall gemäß den geltenden Verfahren an Behörden melden
- ☐ Incident-Response-Team mobilisieren

Checkliste mit Sofortmaßnahmen

- ☐ Betroffene Systeme isolieren
- ☐ Vorfall sofort melden (gemäß der Eskalationsrichtlinie der Organisation)
- ☐ Datenbackup-Status bewerten
- ☐ Strafverfolgungsbehörden kontaktieren (gemäß der Richtlinie der Organisation)
- ☐ Rechtlichen Beistand in Anspruch nehmen
- ☐ Richtlinie der Organisation zum Reagieren auf Lösegeldforderungen befolgen (Beratung erforderlich)
- ☐ Kommunikationsplan der Organisation aktivieren
- ☐ Zeitlichen Verlauf des Vorfalls dokumentieren
- ☐ Vorfall gemäß den geltenden Verfahren an Behörden melden
- ☐ Incident-Response-Team mobilisieren

Checkliste mit Sofortmaßnahmen

- ☐ Betroffene Systeme isolieren
- ☐ Vorfall sofort melden (gemäß der Eskalationsrichtlinie der Organisation)
- ☐ Datenbackup-Status bewerten
- ☐ Strafverfolgungsbehörden kontaktieren (gemäß der Richtlinie der Organisation)
- ☐ Rechtlichen Beistand in Anspruch nehmen
- ☐ Richtlinie der Organisation zum Reagieren auf Lösegeldforderungen befolgen (Beratung erforderlich)
- ☐ Kommunikationsplan der Organisation aktivieren
- ☐ Zeitlichen Verlauf des Vorfalls dokumentieren
- ☐ Vorfall gemäß den geltenden Verfahren an Behörden melden
- ☐ Incident-Response-Team mobilisieren

Checkliste mit Sofortmaßnahmen

- ☐ Betroffene Systeme isolieren
- ☐ Vorfall sofort melden (gemäß der Eskalationsrichtlinie der Organisation)
- ☐ Datenbackup-Status bewerten
- ☐ Strafverfolgungsbehörden kontaktieren (gemäß der Richtlinie der Organisation)
- ☐ Rechtlichen Beistand in Anspruch nehmen
- ☐ Richtlinie der Organisation zum Reagieren auf Lösegeldforderungen befolgen (Beratung erforderlich)
- ☐ Kommunikationsplan der Organisation aktivieren
- ☐ Zeitlichen Verlauf des Vorfalls dokumentieren
- ☐ Vorfall gemäß den geltenden Verfahren an Behörden melden
- ☐ Incident-Response-Team mobilisieren

Checkliste mit Sofortmaßnahmen

- ☐ Betroffene Systeme isolieren
- ☐ Vorfall sofort melden (gemäß der Eskalationsrichtlinie der Organisation)
- ☐ Datenbackup-Status bewerten
- ☐ Strafverfolgungsbehörden kontaktieren (gemäß der Richtlinie der Organisation)
- ☐ Rechtlichen Beistand in Anspruch nehmen
- ☐ Richtlinie der Organisation zum Reagieren auf Lösegeldforderungen befolgen (Beratung erforderlich)
- ☐ Kommunikationsplan der Organisation aktivieren
- ☐ Zeitlichen Verlauf des Vorfalls dokumentieren
- ☐ Vorfall gemäß den geltenden Verfahren an Behörden melden
- ☐ Incident-Response-Team mobilisieren

Anhang zu Aktivität 2 – Referenzkarten zur Organisation und Szenarienkarten

Drucken Sie diesen Anhang aus und schneiden Sie die Karten entlang der auf der Seite dargestellten Linien aus.
Wenn Sie diese auf Karton oder schwerem Papier drucken, können Sie die Karten öfter wiederverwenden.



Rollenkarte für Teilnehmende Leitung der IT-Sicherheit

Verantwortlich für technische Eindämmung des Vorfalls sowie Analysen
Beurteilung von Umfang und Art des Sicherheitsvorfalls
Implementierung von Sofortmaßnahmen zur Eindämmung
Leitung der forensischen Analyse
Abstimmung mit externen Sicherheitspartnern



Rollenkarte für Teilnehmende Leitung der Vorfallkoordination

Verantwortlich für Reaktions- und Entscheidungsfindungsstrategie
Koordination aller Teamaktivitäten
Strategische Entscheidungen
Kommunikation mit der Unternehmensleitung
Zuweisung von Ressourcen und Prioritäten



Rollenkarte für Teilnehmende Leitung der Kommunikation

Steuerung der internen und externen Kommunikation
Ausführung vorhandener Kommunikationspläne
Benachrichtigung der Stakeholder
Koordination der Kommunikation mit Medien und PR-Team
Überwachung von Social Media und Nachrichten



Rollenkarte für Teilnehmende Rechtlicher Beistand

Beratung zu rechtlichen und regulatorischen Konsequenzen
Verantwortlich für die Einhaltung geltender Gesetze
Anweisungen bezüglich der Beweissicherung
Genehmigung der gesamten externen Kommunikation
Abstimmung mit Strafverfolgungsbehörden



Rollenkarte für Teilnehmende Vertretung der Personalabteilung

Umgang mit allen, die Mitarbeitenden betreffenden Incident-Response-Aspekten
Steuerung der internen Kommunikation
Untersuchung von Insider-Bedrohungen
Koordination des Supports für die Mitarbeitenden
Berücksichtigung der Anforderungen an die Aufrechterhaltung des laufenden Betriebs



Rollenkarte für Teilnehmende Abteilungsleitung

Repräsentation der betroffenen Geschäftseinheit
Bewertung der Auswirkungen auf die Abteilung
Einleitung von Maßnahmen zur Aufrechterhaltung des laufenden Betriebs
Abstimmung mit anderen Abteilungen
Statusmeldungen an die Leitung der Vorfallkoordination



Szenario Ransomware-Angriff mit Datendiebstahl

“ Die Dateiserver Ihrer Organisation wurden durch einen Ransomware-Angriff verschlüsselt. Bei dem Angriff wurden auch Finanzdaten von Kundinnen und Kunden gestohlen. Es wird damit gedroht, die Daten zu veröffentlichen, wenn das Lösegeld nicht innerhalb von 24 Stunden gezahlt wird. Komplikation: Die Backup-Systeme wurden anscheinend bereits vor zwei Wochen kompromittiert. ”



Szenario Business Email Compromise

“ Das E-Mail-Konto des CFO wurde kompromittiert und eine Überweisung über 500.000 € auf ein unbekanntes Konto autorisiert. Die Transaktion wurde am Morgen abgeschlossen. Komplikation: Betrügerische E-Mails mit der Aufforderung, die Zahlungsinformationen zu aktualisieren, wurden auch an Konten von drei Großkunden gesendet. ”



Szenario Datendiebstahl durch Insider

“ Ein scheidendes Teammitglied aus der IT-Abteilung wurde beim Kopieren sensibler Kundendaten auf einen privaten USB-Stick ertappt. Das Sicherheitspersonal konnte das Teammitglied beim Verlassen des Büros festhalten. Dieses behauptete jedoch, es handelt sich um persönliche Arbeitsdateien. Komplikation: Das Teammitglied hat auf LinkedIn bereits kryptische Nachrichten gepostet, in denen es davon spricht, „wertvolle Erfahrungen in die neue Position einzubringen.“ ”

Anhang zu Aktivität 2 – Szenarienkarten und weitere Komplikationskarten

Drucken Sie diesen Anhang aus und schneiden Sie die Karten entlang der auf der Seite dargestellten Linien aus. Wenn Sie diese auf Karton oder schwerem Papier drucken, können Sie die Karten öfter wiederverwenden.



Szenario

Kompromittierung in der Lieferkette

“ Ein wichtiger Softwareanbieter Ihrer Organisation informiert Sie darüber, dass der Updateserver kompromittiert und möglicherweise schädlicher Code an Kunden verteilt wurde. Ihre Systeme wurde gestern aktualisiert. Komplikation: Der Softwareanbieter weigert sich aufgrund eigener laufender Untersuchungen, technische Details bereitzustellen. ”



Szenario

Physischer Sicherheitsvorfall

“ Im Serverraum wurde nach Feierabend eine unbefugte Person entdeckt, deren Laptop mit dem Netzwerk verbunden war. Das Sicherheitsteam hat die Person der Büroräume verwiesen. Diese behauptete jedoch, beim IT-Support zu arbeiten. Komplikation: Die Zugriffsprotokolle der Ausweise mehrerer Mitarbeitender weisen ungewöhnliche Aktivitäten außerhalb der Arbeitszeiten auf, die die Mitarbeitenden selbst nicht verursacht haben. ”



Szenario

Kompromittierter Cloud-Dienst

“ Ihr Cloud-Dienst meldet unautorisierte Zugriffe auf das Repository Ihrer Organisation mit Kundendaten und Geschäftsgeheimnissen. Der Beginn des Vorfalls liegt eventuell bereits einige Wochen zurück. Komplikation: Die erste Mitteilung des Cloud-Anbieters enthält widersprüchliche Informationen über Ablauf und Umfang. ”



Komplikationen

“ Medienaufmerksamkeit: Ein Technologieblog hat einen Artikel über den Sicherheitsvorfall in Ihrer Organisation mit spezifischen, noch nicht offengelegten Details veröffentlicht. ”



Komplikationen

“ Auskunftersuchen der Aufsichtsbehörde: Die Aufsichtsbehörde Ihrer Branche hat Sie aufgefordert, sofort Informationen über den Vorfall und die von Ihnen ergriffenen Maßnahmen bereitzustellen. ”



Komplikationen

“ Kundendruck: Ihr wichtigster Kunde hat ein Notfallmeeting angesetzt. Der Kunde fürchtet um die Sicherheit seiner Daten und droht mit der Kündigung des Vertrags. ”



Komplikationen

“ Internes Leck: Die Mitarbeitenden der Organisation besprechen den Vorfall im internen Messenger; einige Informationen scheinen ungenau zu sein. ”



Komplikationen

“ Systemfehler: Während Sie Schritte zur Problembehebung umsetzen, fällt ein kritisches Unternehmenssystem aus – möglicherweise aufgrund der von Ihnen ergriffenen Maßnahmen. ”



Komplikationen

“ Rechtliche Konsequenzen: Sie erhalten einen Brief von einer Kanzlei, die betroffene Kundinnen und Kunden vertritt. Sie werden aufgefordert, ausführliche Informationen über den Vorfall sowie die ergriffenen Maßnahmen bereitzustellen. ”