# Reaktions-Training

## Üben von Incident-Response für IT-Sicherheitsvorfälle

**Egal ob man bislang noch weitgehend ungeschoren davongekommen ist oder der alltägliche Wahnsinn weniger häufig benötigte Werkzeuge, Prozesse und Fertigkeiten ins Abseits drängt: Nur Übung macht den Meister und ist als Vorbereitung für eine angemessene und schnelle Reaktion auf IT-Sicherheitsvorfälle unabdingbar. Unser Autor liefert dazu einen Überblick über verschiedene Optionen und die damit verbundenen Aufwände sowie die erreichbaren Übungsziele.**

*Von Michael Brügge, Heilbronn*

Seit Langem gilt bei IT-Sicherheitsvorfällen: „Die Frage ist nicht, ob es einen trifft, sondern wann es einen trifft." Es ist davon auszugehen, dass jedes Unternehmen früher oder später von einem IT-Sicherheitsvorfall betroffen sein wird. Daher ist es einerseits notwendig, über die entsprechenden Fähigkeiten zu verfügen, um diese Angriffe frühzeitig erkennen zu können – ebenso wichtig ist nach einer erfolgreichen Erkennung jedoch auch die Reaktion darauf. Denn das bloße Wissen um einen IT-Sicherheitsvorfall allein führt ja noch nicht zu dessen Eindämmung und Beseitigung, wozu es der passenden Reaktionsfähigkeiten bedarf.

Wie so oft geht es auch hier allerdings nicht nur um die Verfügbarkeit entsprechender technischer Werkzeuge, sondern gleichzeitig um die notwendigen organisatorischen Prozesse und schlussendlich den kühlen Kopf zu deren Umsetzung. In der Praxis stellen sowohl der Umgang mit Werkzeugen als auch organisatorische Abläufe oft eine ernst zu nehmende Herausforderung dar – besonders wenn sie nicht regelmäßig geschult und vor allem auch geübt werden. Daher ist es empfehlenswert, sich frühzeitig und regelmäßig in Übungssituationen auf den Ernstfall vorzubereiten.

## Unterschiedliche Varianten

Für derartige Übungssituationen gibt es im Wesentlichen drei verschiedene Ansätze: Table-Top-Übungen, War-Gaming oder ein vollumfängliches Red-Team-Assessment. Bei Table-Top-Übungen liegt der Fokus primär auf den Incident-Response-Prozessen sowie der internen und externen Kommunikation – War-Gaming-Übungen zielen hingegen vorrangig auf die korrekte Nutzung der vorhandenen technischen Werkzeuge zur Erkennung und Reaktion ab.

Bei einem Red-Team-Assessment (vgl. [1]) ist das Üben des richtigen Umgangs mit IT-Sicherheitsvorfällen ein wesentlicher Bestandteil, jedoch geht es in einem derartigen Projekt vor allem auch um die Identifikation von Schwachstellen bei einem bewusst offenen Scope. Dieser offene Rahmen erschwert die Definition konkreter Übungsinhalte, da sich im Vorfeld eines Projekts nicht vollständig abschätzen lässt, welche Angriffsvektoren genutzt werden und letztlich zu einem Erfolg führen könnten. Daher ist ein Red-Team-Assessment zwar eine sehr gute Gelegenheit, die korrekte Reaktion auf realitätsnahe Angriffe zu üben, allerdings aufgrund des hohen Aufwands sowie des offenen Rahmens nicht für regelmäßige und gezielte Übungen geeignet. Aus diesem Grund geht es nachfolgend nur noch um die verschiedenen Table-Top- und War-Gaming-Varianten.

### Auswahl der passenden Übungs-Form

Die Auswahl der zweckmäßigen Variante beim Üben ist maßgeblich von den gewünschten Zielen abhängig – daher ist zunächst festzulegen, was man mit der Übung konkret erreichen will (vgl. Tab. 1). Eine wesentliche Fragestellung ist der Fokus der Übung: Stehen primär die Prozesse im Mittelpunkt oder soll der technische Umgang mit Erkennungs- und Reaktionswerkzeugen geübt werden? Die Antwort auf diese Frage liefert bereits einen entscheidenden Hinweis zur Auswahl der geeigneten Übungsvariante.

## Table-Top-Übungen

Die Durchführung von Table-Top-Übungen findet, wie der Name bereits andeutet, an einem Tisch statt. Ein unbeteiligter Leiter* führt durch die Übung während in aller Regel eine weitere unbeteiligte Person den Verlauf

protokolliert. Derartige Übungen beruhen auf einem angenommenen Szenario, dass den Rahmen der Übung vorgibt und anschließend in Form von Diskussionen bearbeitet wird.

Da es sich um fiktives Szenario handelt, also keine IT-Systeme tatsächlich betroffen sind, existieren auch keine Artefakte beziehungsweise sogenannte Indicators of Compromise (IoCs), die von technischen Erkennungslösungen erkannt und gemeldet werden können. Das bedeutet, dass Table-Top-Übungen bewusst ohne Interaktion mit technischen Werkzeugen zur Erkennung- und Reaktion ablaufen. Vielmehr beschreiben Teilnehmer im Rahmen der Übung, welche Maßnahmen sie aus welchem Grund treffen und beeinflussen damit den Verlauf der Übung. Diese Rahmenbedingungen verdeutlichen bereits, dass eine Table-Top-Übung weniger auf technische Details einer Vorfallsbehandlung abzielt, sondern primär den Fokus auf Prozesse, Kommunikation und Interaktion mit anderen Parteien legt.

## Fokus auf Security-Incident-Response-Prozesse

Hinsichtlich vorhandener Incident-Response-Prozessen bietet eine derartige Übung eine sehr gute Gelegenheit, den Teilnehmern aufzuzeigen, welche Prozesse und Richtlinien in diesem Zusammenhang existieren und welche Prozessschritte zu durchlaufen sind. In der Praxis zeigt sich, dass häufig vielen Beteiligten die Prozesse nur teilweise oder sogar gar nicht bekannt sind.

Aber auch Defizite in definierten Prozessen lassen sich so aufdecken, denn oft werden die Prozesse nicht umfassend befolgt oder sind für das gewählte Szenario nicht vollständig anwendbar. Aus diesem Grund bietet eine Table-Top-Übung eine gute Gelegenheit, bestehende Prozesse zu schulen, zu üben und Mängel zu erkennen.

Ein weiterer wesentlicher Aspekt einer Table-Top-Übung ist es, dass jeder Teilnehmer die Rolle übernimmt, die er auch bei einem realen Angriff hätte – und so in einer Übungssituation lernt, welche Tätigkeiten in seinen Zuständigkeitsbereich fallen. Die Teilnehmer üben dabei nicht nur ihre eigenen Aufgaben, sondern für sie werden gleichzeitig auch die Rollen der anderen involvierten Personen sichtbar. Dies ermöglicht im Ernstfall eine bewusstere Aufgabenverteilung und Abgrenzung, sodass sich IT-Sicherheitsvorfälle effizienter bearbeiten lassen.

## Kommunikations-Training

Ein ebenso wichtiger Teil der eigenen Rolle ist das Erlernen der richtigen Verständigung während eines IT-Sicherheitsvorfalls: Bei der Vorfallsbearbeitung ist eine klare Kommunikation mit anderen Teammitgliedern, Verantwortlichen sowie internen und externen Parteien unerlässlich. In der Praxis zeigt sich, dass bei Teilnehmern oft eine gewisse Zurückhaltung dahingehend herrscht, bestimmte Personen oder Parteien zu informieren oder sogar aktiv zu involvieren. Diese Scheu ist in einer Übungssituation häufig weniger stark ausgeprägt. Daher berichten Teilnehmer nach Übungen oft, dass sie sich nun selbstbewusster fühlen und es ihnen beispielsweise leichter fällt, das Top-Level-Management aktiv über einen IT-Sicherheitsvorfall zu informieren.

Neben den menschlichen Faktoren der Kommunikation lassen sich auch organisatorische und technische Aspekte gut überprüfen. Dies können beispielsweise Fragestellungen sein wie „Ist tatsächlich jemand unter der Bereitschaftsnummer zu erreichen?“ oder „Ist die hinterlegte Telefonnummer für eine bestimmte Person/Rolle korrekt?“ Dies weicht zwar aufgrund der tatsächlichen Durchführung von Aktionen von dem klassischen Verständnis einer Table-Top-Übung ab, lässt sich aber bei entsprechender Planung im Vorfeld gut abbilden.

Die zuvor genannten Übungsaspekte stellen die typischen Fokuspunkte dar. Je nach konkretem Bedarf kann man aber auch weitere Aspekte in eine Übung mit aufnehmen. Dazu zählt zum Beispiel das Protokollieren eines IT-Sicherheitsvorfalls. Auch problematische Rahmenbedingungen, wie beispielsweise Defizite bei der technischen Ausstattung des Krisenraums, lassen sich während solcher Übungen gut identifizieren.

*Tabelle 1: Vergleich verschiedener Übungsvarianten zur Incident-Response*

| Form | Aufwand | Fokus | Regelmäßigkeit | Bezug des Szenarios |
|---|---|---|---|---|
| Table-Top-Übung, generisch | gering | Prozesse und Kommunikation | gut geeignet | gering |
| Table-Top-Übung, individuell | mittel | Prozesse und Kommunikation | gut geeignet | mittel bis hoch |
| War-Gaming | hoch | technische Erkennungs- und Reaktionsfähigkeiten | gut geeignet | hoch |
| Red-Team-Assessment | sehr hoch | Prozesse, Kommunikation und technische Erkennungs- und Reaktionsfähigkeiten | ungeeignet | sehr hoch |

### Übungsablauf: generisch oder individualisiert?

Im Wesentlichen gibt es zwei grundsätzliche Ansätze für Table-Top-Übungen: generisch oder individuell auf das Unternehmen abgestimmt.

Bei einer **generischen Table-Top-Übung** kommen vordefinierte und allgemein gehaltene Szenarien zum Einsatz. Dies hat auf der einen Seite den Vorteil, dass nur ein sehr geringer Vorbereitungsaufwand nötig ist – auf der anderen Seite sind die allgemeinen Szenarien möglicherweise nicht zu 100 % passend. Geht beispielsweise das Szenario davon aus, dass die initiale Infektion eines Clients über ein Makro in einem Excel-Anhang erfolgt, entsprechende Anhänge in der Umgebung jedoch gar nicht zugestellt werden, basiert das gesamte anschließende Szenario auf einer unrealistischen Annahme. Das kann in der Praxis schnell zu einer Art Abwehrhaltung der Teilnehmer führen.

Darüber hinaus können generische Table-Top-Übungen weniger mitreißend sein, da die Gefahr besteht, dass die Teilnehmer sich in allgemeinen Szenarien weniger wiedererkennen. Da bei Table-Top-Übungen keine tatsächliche Kompromittierung vorliegt und sich die gesamte Übung lediglich als „Gedankenspiel" beziehungsweise Diskussion abspielt, ist es jedoch besonders wichtig, dass die Teilnehmer einen Bezug zu dem jeweiligen Szenario aufbauen können.

Im Gegensatz zu einer generischen Übung existiert mit der **individuellen Table-Top-Variante** die Möglichkeit, den genannten Defiziten einer allgemeinen Übung bewusst entgegenzuwirken. Das erfordert zwar einen höheren Vorbereitungsaufwand, ermöglicht es jedoch, ein exakt auf die Lernziele und Kundenumgebung abgestimmtes Szenario zu gestalten. Dies führt der Erfahrung nach zu einer deutlich höheren Akzeptanz bei den Teilnehmern, da sie sich in dem Szenario und der Umgebung wiedererkennen – dass das gewählte Szenario tatsächlich eine realistische Eintrittswahrscheinlichkeit und somit auch Relevanz für das Unternehmen hat, ist dabei offensichtlich.

Allem voran sind es aber Details bei der Ausgestaltung des Szenarios, die schlussendlich dazu führen, dass es von den Teilnehmern als realistisch und mitreißend beschrieben wird. Dazu zählen beispielsweise passende Computer- oder Servernamen, die Wahl existierender Webseiten als Einfallstor und damit verbunden auch die tatsächliche Involvierung der entsprechenden Applikati-

onsverantwortlichen. Dadurch nimmt jeder Teilnehmer seine eigene Rolle entsprechend seiner konkreten Verantwortlichkeiten wahr und übt sie. Damit das funktioniert, sollte man eine individuelle Übung immer auch an die bestehenden Prozesse anpassen: So können ausgewählte Prozessschritte konkret geschult oder gezielt die Interaktion zwischen zwei Parteien herbeigeführt werden.

## War-Gaming-Übung

Wie bereits erläutert, stehen bei Table-Top-Übungen primär organisatorische Aspekte und Prozesse im Fokus und bilden die Basis für eine strukturierte Vorfallsbearbeitung. Demgegenüber kommt jedoch kaum ein IT-Sicherheitsvorfall ohne technische Erkennungs- und Reaktionsfähigkeiten aus. Typische Ziele einer War-Gaming-Übung sind daher der Test konkreter Erkennungsfähigkeiten und das Üben gezielter Reaktionen auf IT-Sicherheitsvorfälle – hier steht also die tatsächliche technische Eindämmung im Vordergrund.

### Technische Aspekte im Fokus

Angriffe werden beim War-Gaming nicht nur diskutiert, sondern tatsächlich in der eigenen Umgebung ausgeführt. Entsprechende Events und Alarme der durchgeführten Angriffe sollen dabei in den vorhandenen Erkennungslösungen sichtbar sein. Das ermöglicht auf der einen Seite das Aufdecken von Defiziten in den technischen Erkennungsfähigkeiten und auf der anderen Seite das Einüben der angemessenen Reaktion auf den Ernstfall in der realen Umgebung.

Obwohl entsprechende Angriffe in der eigenen Umgebung durchgeführt werden, sind War-Gaming-Übungen explizit nicht als Sicherheitsüberprüfung oder Penetrationstest zu verstehen, denn im Gegensatz zu diesen steht hier nicht die Suche nach Schwachstellen im Fokus: Vielmehr folgen die Angriffe einem zuvor festgelegten Drehbuch, das ein bestimmtes Szenario abbildet und konkrete Angriffsketten vorsieht. Diese werden dabei gegebenenfalls erst durch gezielte Vorbereitungen ermöglicht, beispielsweise durch den bewussten Einbau einer Schwachstelle zur lokalen Rechteerweiterung auf einem konkret ausgewählten Server. Der klar vorgegebene Rahmen der Angriffsdurchführung führt dabei dazu, dass sich typischerweise keine unerwarteten Beeinträchtigungen für betroffene Systeme ergeben, da sämtliche Angriffe, betroffene Systeme und Nutzer sowie Auswirkungen bereits im Vorfeld feststehen.

Analysten haben in einem solchen Übungsszenario die Möglichkeit, in ihrer bekannten Umgebung mit ihren vertrauten Werkzeugen in einer sicheren Übungssituation auf einen simulierten IT-Sicherheitsvorfall zu reagieren. Dabei übt man den korrekten Umgang mit den Werkzeugen und kann mögliche Einschränkungen identifizieren, die dabei zutage treten.

Der Vorteil einer derartigen War-Gaming-Übung ist, dass sich ganz gezielt bestimmte Erkennungs- und/oder Reaktionsfähigkeiten testen und üben lassen. Beispiele hierfür sind etwa die Einführung einer neuen Endpoint-Detection-and-Response-(EDR)-Lösung oder die Implementierung eines neuen Use-Cases zur Angriffserkennung. Da es sich hierbei um einen individuellen Ansatz handelt, erfordert dieser allerdings – wie auch individuelle Table-Top-Übungen – einen gewissen Vorbereitungsaufwand.

## Die Lehren einer Übung

Unabhängig davon, welche Übungsvariante angewendet wird, ergeben sich bei der Durchführung wertvolle Erkenntnisse auf unterschiedlichen Ebenen – sowohl bei den Teilnehmern, aber auch bei unbeteiligten Beobachtern und dem Übungsleiter.

Um diese Erkenntnisse zu sammeln und zu strukturieren, darf eine Lessons-Learned-Runde am Ende der Übung nicht fehlen, denn genau in diesem Rahmen kristallisieren sich neben den offensichtlichen Erkenntnissen in aller Regel weitere wichtige Lehren heraus. Diese reichen häufig von fehlenden prozessualen Vorgaben und unzulänglicher Ausrüstung über falsche Telefonnummern bis hin zu zwischenmenschlichen Erfahrungen. Am Ende ist jedoch das Entscheidende, aus den gewonnenen Einblicken auch die richtigen Schlüsse zu ziehen und identifizierte Defizite aktiv anzugehen.

### Nach der Übung ist vor der Übung

Die heutige Bedrohungslage setzt sich aus einer Vielzahl verschiedener Angriffsvektoren und -techniken zusammen. Im Rahmen einer Übung lässt sich allerdings nur ein Bruchteil davon gezielt adressieren und üben. Daher sollten Unternehmen das Üben ihrer Prozesse sowie Erkennungs- und Reaktionsfähigkeiten als kontinuierlichen Prozess verstehen. Dazu empfiehlt es sich, über das Jahr verteilt mehrere kleinere, dafür aber gezielte Übungen anstelle einer großen und besonders komplexen Übung durchzuführen. ■

*Michael Brügge ist Leitender Berater bei cirosec.*

## Literatur

**[1]** Michael Brügge, Der ultimative Pentest, Red-Team-Assessments – „echte“ Angriffe für mehr Sicherheit, <kes> 2019#2, S. 13

# <kes>+

Die Zeitschrift für Informations-Sicherheit

NEU

## Mit <kes>+ bleiben Sie auf dem Laufenden über die Entwicklungen in der Informationssicherheit:

- **Fachzeitschrift** <kes> **inkl. Specials** 6x jährlich per Post und digital
- Zugang zu **aktuellen Online-Fachartikeln** und **Studien** sowie zu dem **kompletten Online-Archiv**
- Exklusiver Zugriff auf **aktuelle Videos** und **Webinaraufzeichnungen**
- **10 % Rabatt** auf DATAKONTEXT-Online-Schulungen im Bereich Informationssicherheit
- nur 199,00 € im Jahr (inkl. Mwst. und Versand)


## Jetzt bestellen: www.kes.de