Incident Response Exercise

Lektion

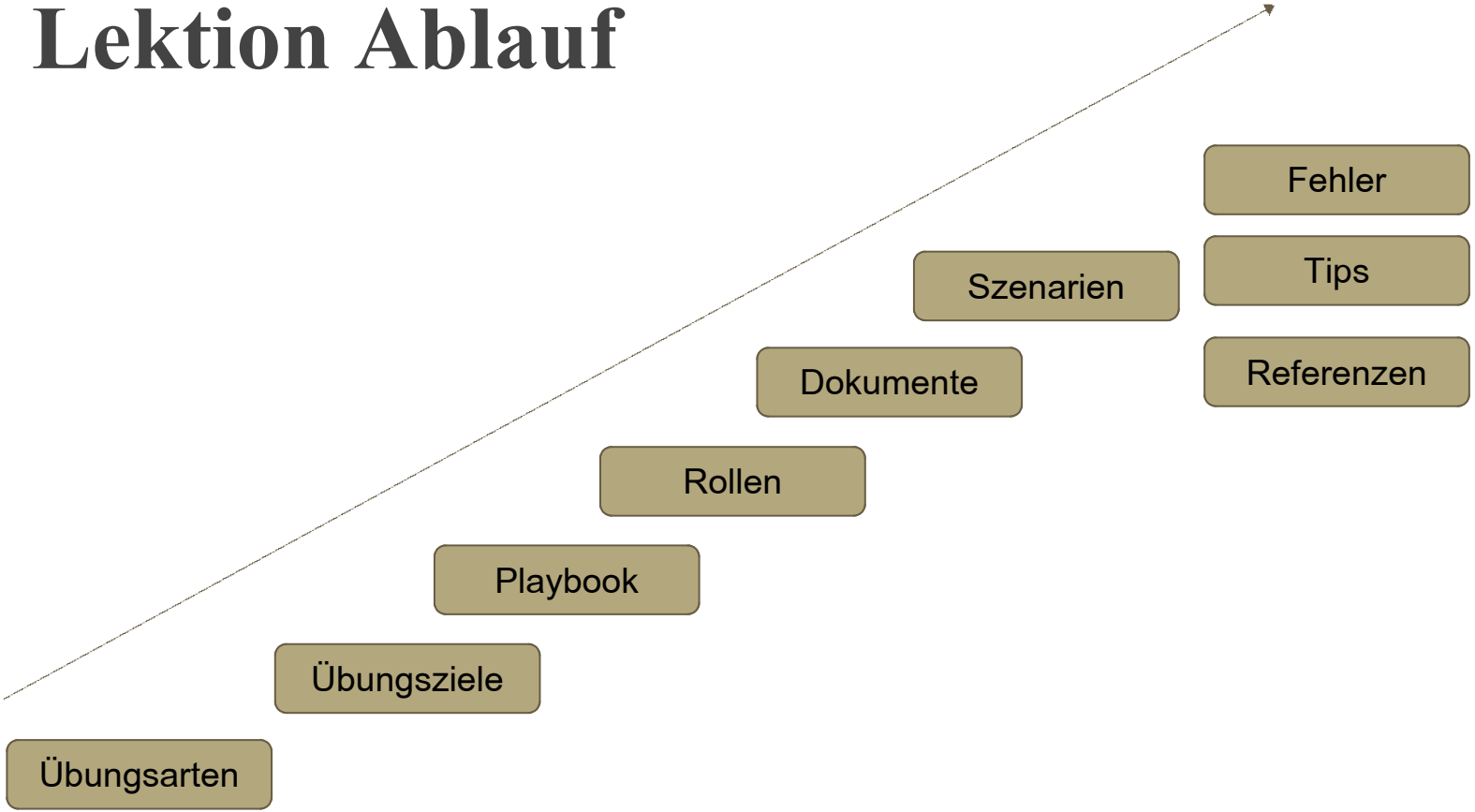
Sie sind auf die Planung und Durchführung einer Incident Response Übung vorbereitet?

Mentimeter

https://www.menti.com/al2w4zj2u8iz

Bitte lasst auch Kommentare da. Vor allem, wenn es Bedarf für Verbesserung gibt.

Lektion Ablauf



Hintergrund

1. Das Kennen von Prozessen, Policies und Richtlinien ist eine wichtige Voraussetzung, um einen Cyber Sicherheitsvorfall zu begegnen.
2. Ähnlich wie bei Brandbekämpfungs- oder Erste-Hilfe-Übungen kann es sinnvoll sein, den entsprechenden Prozess der Reaktion auf einen Zwischenfall zu üben.
3. In der Praxis kann sogar davon ausgegangen werden, dass ohne Übung ein sonst vermeidbarer Schaden entsteht.
4. Angemessene Übungen sind derzeit nur selten systematisch* zu finden.

Ziel der Lektion

Sie wissen:

- welche Arten von Übungen durchgeführt werden können
- wie Sie die entsprechende Übung vorbereiten
- wie Sie die Wirksamkeit der Übung bewerten
- welche Art von Modellen und Leitlinien verfügbar sind

Kein Ziel:

- das Durchführen bzw. Üben von Übungen
- Red/Blue Team Übungen

Übungsarten

“Table Top Exercises”
Sämtliche Aktivitäten werden theoretisch exerziert. Im Idealfall lehnt sich die Übung an reale Fälle an oder imitiert diese.
Wann: Prozessablauf - und Inhalte Training. *Nachteil*: weniger Praxisbezug
“Functional Exercises”
Auch “Real” genannt wird hier mit einem echten System agiert. Es erfolgen tatsächliche forensische Analysen und Angriffe werden durchgeführt. Die Umgebung ist möglichst real.
Wann: Technisches Training. *Nachteil*: Hoher Zeitaufwand, höhere Kosten.
“Mixed/hybrid Exercises”
Die Table Top Übung wird um funktionale Elemente angereichert. So wird dem Übungsteam zum Beispiel ein reales Log vorgelegt oder eine Image-Auswertung zur Verfügung gestellt.
Wann: Gezieltes Training von technischen Elementen in Verbindung mit Prozesselementen. Oder didaktische Aufwertung der Table Top Übung. *Nachteil*: Höhere Komplexität.

Einordnung

1. Incident Response heißt, den Prozess zur Identifizierung, dem Management und der Analyse von Sicherheitsbedrohungen und Ereignissen in “Echtzeit” zu absolvieren.
2. Eine Incident Response Übung ist kein Hackathon oder eine RT/BT Übung.
3. Es können technische Elemente wie forensische Analyse, Scan-Techniken verwendet werden, sind aber weniger das direkte Objekt der Übung.

Ziel der Übung

Verifizieren und Verbessern
- der **Wirksamkeit** des implementierten IR Prozesses.
- der Prozess-
- **Kenntnisse** der beteiligten Personen.

Training des Prozesses.

Nachweis/Bewertung von Effektivität von Schulungsmaßnahmen.

Aufdeckung von systematischen Schwach-stellen.

Marketing (gemeinsam mit Kunden)

Awareness auf nicht-technischen Ebenen

Playbook/Script/Drehbuch

Eine Übung kann ähnlich einem Rollenspiel vorbereitet und durchgeführt werden.
Es werden definierte Szenarien “durchgespielt” und ggf. miteinander kombiniert.
Neben der “Spielleitung” gibt es auch die Rolle der Beobachter, die am Ende in der Lage sind, die erwarteten Qualitätsberichte nutzbringend zu erstellen.

Vergleich: Pen & Paper Rollenspiele

Funktionen

Planung
Moderation
Beobachtung
Protokollierung
Incident Response Team/Training Audience
SMEs

Dokumente

Szenario Beschreibung
Moderator Handbuch
Teilnehmer Handbuch
Report
Templates
Prozessbeschreibung
Checklisten

Szenario Beschreibung

Vorbereitung

Soll die Übung eher Table Top, eher Real oder mixed sein?

Wieviel Zeit steht zur Verfügung? (Stunden, Tage, Echtzeit)

Was soll erreicht werden?

Prozessverbesserung?

Training?

Vermitteln?

Nachweis?

etc.

Welche Verhaltensweisen sollen behandelt werden?

Welche Injects sind zu beschreiben?

Je nach Entwurf, muss Technologie bereitgestellt werden.

E-Mail, Malware, Chat, Logfiles, Images, packet captures, etc.

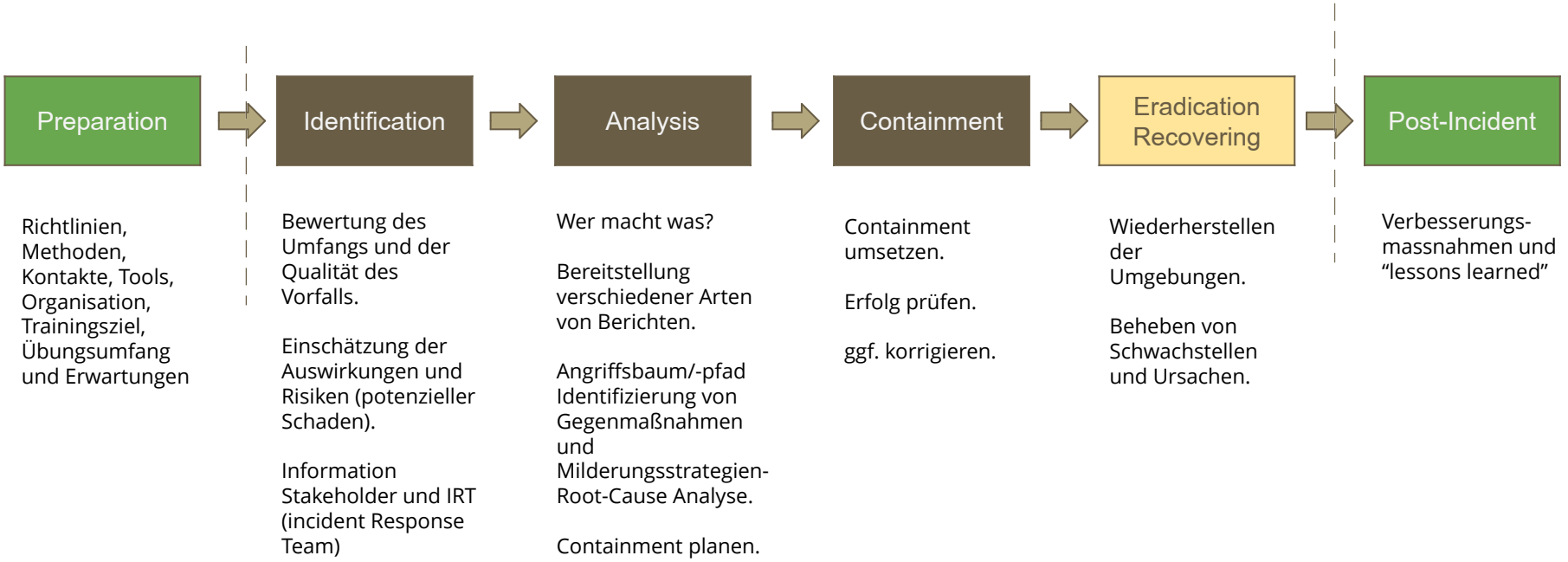
Inhalt, Erwartung und Ablauf werden beschrieben.

Die Beschreibung erfolgt jeweils für alle Rollen.

Szenario wird ausformuliert.

IR Übungsstruktur

Der hier gezeigte grobe “Incident Response” Ablauf stellt zugleich die möglichen Trainingselement dar.



Szenarien

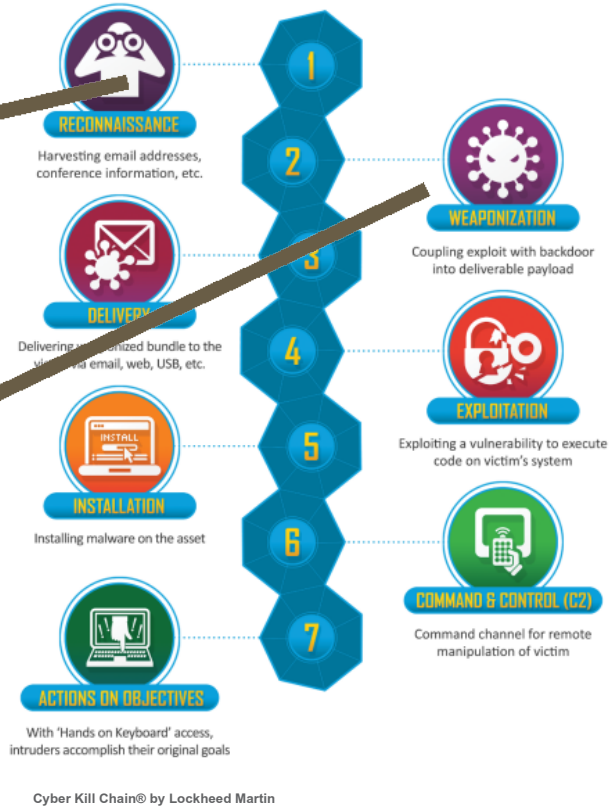
Was ist ein Szenario?

Hund beißt Mensch.

Chronologie eines Angriffs

Während der Reconnaissance Phase ist die Möglichkeit der Erkennung eines Angriffs begrenzt. Dennoch könnten suspekte Kontaktaufnahmen per E-Mail, Telefon oder persönlich auf eine Recon Phase hinweisen. Es ist auch denkbar, dass bereits ab hier eine Incident Situation erklärt wird. Letztlich hängt es auch von Branche und Kritikalität ab.
Eine Übung würde hier vor allem mit Themen der Kommunikation und des Social Engineering erfolgen.

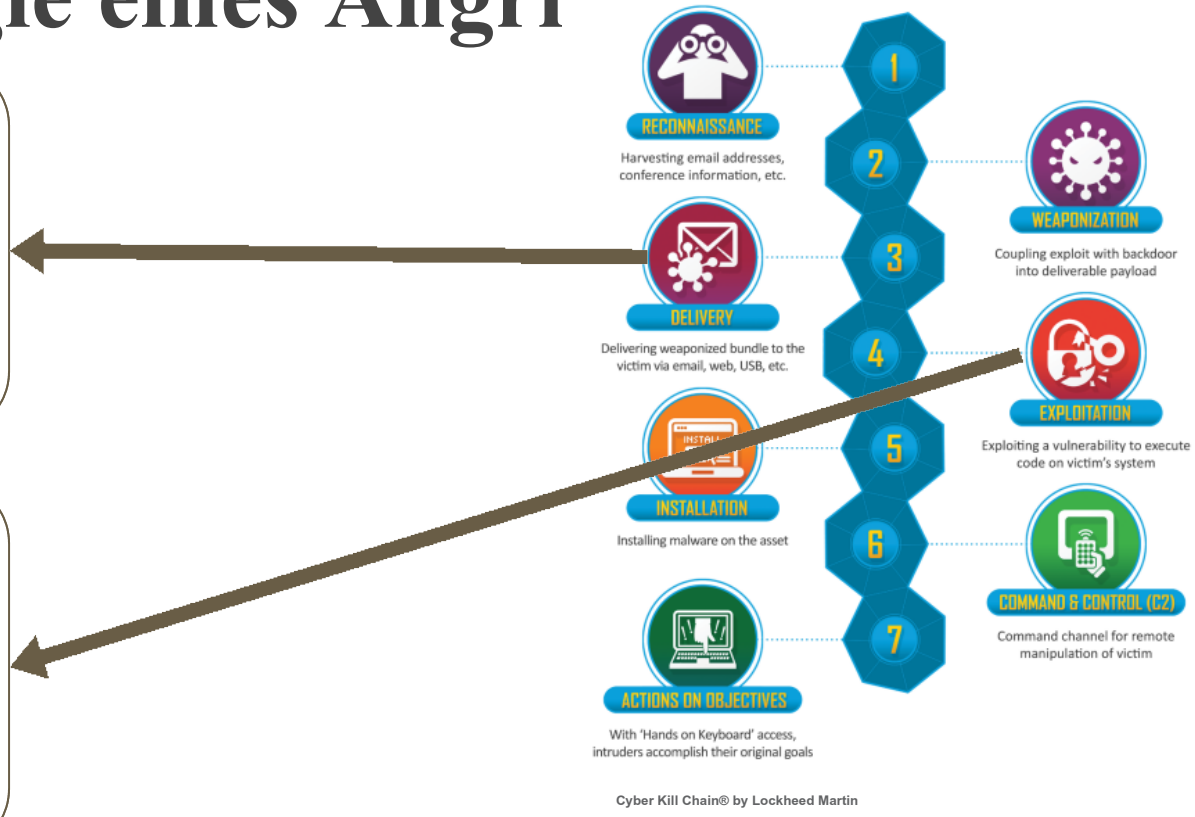
Der Weaponization-Phase lassen sich Übungen eher technischer Art entgegensetzen. Haben wir Security Controls, die die üblichen Angreifer-Werkzeuge frühzeitig erkennen oder abwehren? Passende Übungen dafür werden in Red/Blue-Team-Szenarien absolviert.



Chronologie eines Angriffs

Die “Delivery” Phase begegnet uns, z.B. wenn Phishing-Mails eingehen. Aber manipulierte USB-Sticks und schlecht konfigurierte Firewalls oder VPN-Konzentratoren sind willkommene Angriffsvektoren. Im Rahmen einer Übung geht es vor allem darum, im Nachhinein herauszufinden, welcher dies Angriffsvektoren genutzt wurde.Aber auch welchen Vektor man bis zur Klärung geschlossen halten muss.

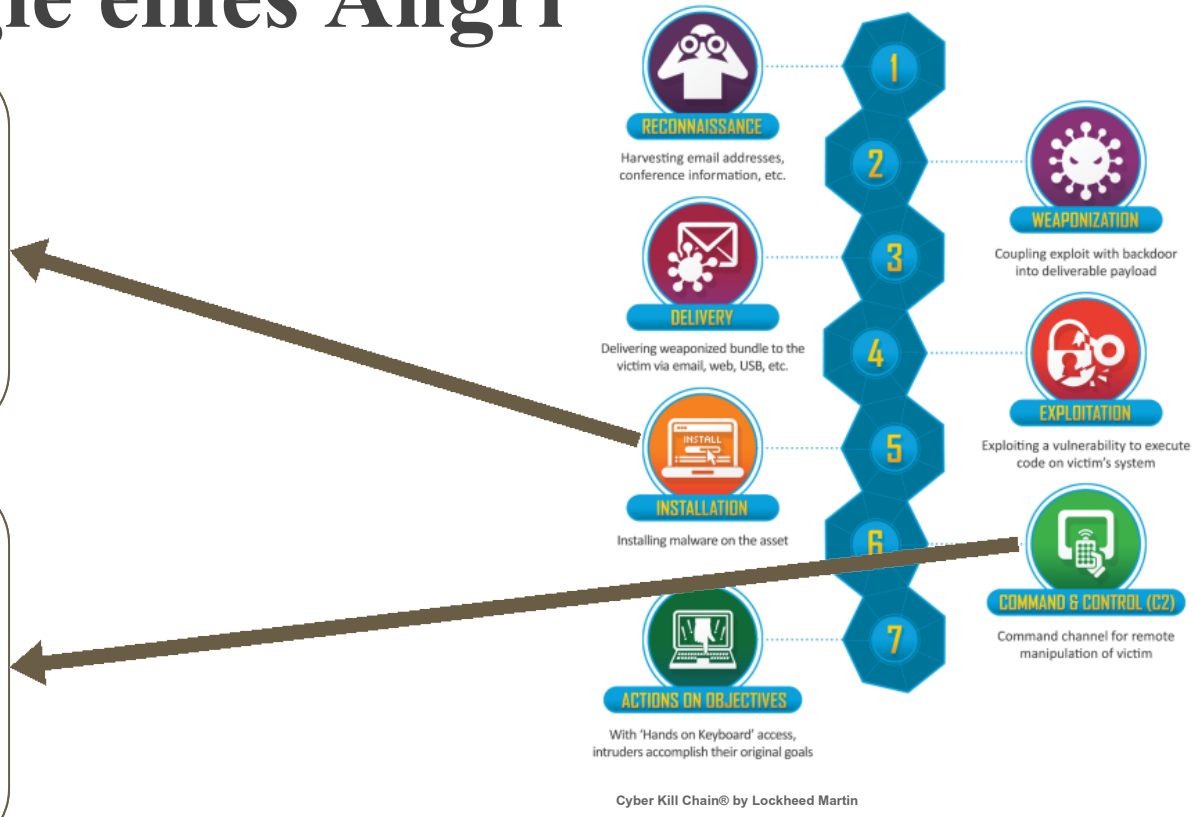
Die “Exploitation” erfolgt auf Basis von Schwächen in Systemen, Services oder Applikationen. Im Rahmen der Übung kann herausgefunden werden, ob das Vulnerability Management ausreichend etabliert ist und verstanden wird. Im Idealfall erhält man schnell und verständlich eine Übersicht der Schwachstellen-Lage.



Chronologie eines Angriffs

Die “Installations” Phase umfasst auch internes Scannen durch die TAs und in Folge das “lateral movement”. Da in der Regel flache Netze und legacy Systeme als besonders nützlich für TAs gelten, kann das auch der Ansatzpunkt in einer Übung sein. In der Praxis führt eine nicht ausreichende Segregation aber zur Entscheidung über den vollständigen Lockdown.

“C&C” (Command und Control) ist nicht zwingend Bestandteil eines erfolgreichen Angriffs. Die aktuell bekannten Ransomware-Szenarien benutzen C&C zum einen für die Seitwärtsbewegung innerhalb der Infrastruktur, aber auch für den Scan nach weiteren Schwachpunkten sowie für das Holen von zusätzlichen Payload. Während einer Übung kann das über Injects abgebildet werden: “Unkown network connections” identified oder “Finde unbekannte, suspekte Netzwerkverbindungen!”



Angriffsziele (Auszug)

1. Genereller Informationsdiebstahl
2. Exfiltrieren von Informationen der Konkurrenz
3. Generelle Kompromittierung
4. Blackmailing
5. Disruption/Störung
6. Rache/Revenge/embarrassment
7. Privileged access (own the box)

Während Übungen wird gern lange und ausgiebig über die Motivation von Angreifern philosophiert.
Hier empfiehlt es sich, eine oder zwei Annahmen zu treffen und nur begrenzt Zeit zu investieren.
Die Motivation ist relevant, aber relevanter ist in der Regel: "das es aufhört”.

Übungsszenarien/Threats

Unauthorized Access and Control
(Manipulieren von Informationen und Funktionen)
Exfiltration/Data Breach
(Spionage oder Bloßstellung)
Malware/Ransomware
(Erpressung, Störung)
Session interception
(Spionage)
Man-in-the-Middle (New: Adversary in the Middle)
(Spionage, Manipulation)
Physical compromising
(Everything)

Device/s stolen
(Everything)
flooded by phishing messages
(Erpressung, Störung)
legacy malware detected
(Nothing)
Supply Chain compromised
(Manipulieren von Informationen und Funktionen, Spionage,Störung)
Frequency/increased phishing
Undefined Compromise
(Lockdown, undefined)

*TA = Threat Actor

Angriffsvektoren (Auszug)

3rd/4rth party vendors
Weak encryption in Transit
(User|Network| System) interfaces
Legacy systems/not maintained systems
Flat (not segregated) Networks
Vulnerabler/schwacher code/service/applications
Texting| E-Mail Phishing

Eine “social engineering” empfängliche Belegschaft

Schwächen (Auszug)

1. Encryption
2. AV/Malicious code protection
3. Staff Awareness
4. Security Monitoring
5. Security Assessment
6. Security Testing
7. Segregation
8. Access protection

MITRE Table 10 Example [6]

Table 10. Sample Cyber Injects

ID	Title	Description	Objective[1]	Outcome[2]
IA-1	Network virus	The RT sends the training audience a spearphishing email, supposedly signed by the exercise leader, indicating the need to view a webpage for updated exercise information that contains the simulated eicar virus test string. The email is designed to simulate the installation of malicious software and trigger incident reporting.	01, 02, 04, 07, 08, 09, 10, 11	01, 03, 06, 07, 08, 10
IA-2	Network Denial of Service (DoS)	The RT generates an abnormally high amount of network traffic against the training network in order to simulate reduced network capabilities visible in system performance statistics and volume of log data. Additional notification from the training audience about reduced network capability or inability to access website should prompt the incident response process and associated troubleshooting.	01, 02, 03, 04, 06, 07, 08, 09, 10, 11, 12	03, 04, 06, 07, 08, 10
IA-3	Unauthorized computer on network	The RT attempts to connect an unauthorized laptop to the training network to see if it is detected.	01, 02, 04, 07, 08, 09, 10, 11	02, 03, 06, 07, 08, 10
IA-4	Malicious external scanning	The RT executes an external scan of the exercise network to see if it detected. May also be used to facilitate training and education about firewalls and IDS.	01, 02, 03, 04, 06, 07, 08, 09, 10, 11	02, 03, 06, 07, 08, 10

Das MITRE Playbook fokussiert stark auf die technische Prüfung und Weiterbildung.
Die MITRE Methodik lässt sich auf andere Klassen abstrahieren.

Beispiel Szenario

Typ: Tabletop

Beschreibung (kurz): Ein beim Kunden nicht über ein Netzwerk durch uns administrierbares Produkt ist neben anderen Kundensystemen von einer Schadsoftware betroffen.

Herausforderung

Bei prozessualen Übungen geht es um Fragen wie:

Haben wir es mit einem Incident zu tun?
Wie groß ist der Schaden oder welcher Schaden wird erwartet?
Welche Fehler zeigen sich im Prozess?
Wie werden die prozessrelevanten Templates und Tools eingesetzt?
Welche Fehler zeigen sich im formalen Training?
Timing? Funktionieren Kommunikation und Zulieferung?
Effizienztraining: Können überflüssige Diskussionen erkannt und vermieden werden?
Sind die Vorbereitungen auf einen solchen Fall angemessen (gewesen)?

Injects

Inject Beispiele

Inject I: 16:06
Außendienst: meldet einen Ausfall am Standort des Kunden. *(beim CSA* noch unbekannt)*

Inject II: 16:35
Außendienst: Der Kunde erklärt, es gäbe einen Ransomware-Vorfall. Und ordnet das Issue dem CSA zu.

Inject III: 17:25
Außendienst: Bei der Ransomware handelt es sich um Lockbit **6**.0.

Inject IV: 17:45
Cyber Security SME: Bei LB 6.0 kann es auch zu einer “Data Exfiltration” und einer Datenmanipulation kommen.
Es gäbe noch nicht sehr viele Informationen zu 6.0

Inject V: 17:47
Außendienst: Der Kunde hat alle betroffenen Systeme und Systeme, die betroffen sein könnten, abgeschaltet.

Inject VI: 20:30
Außendienst: Der Kunde hat den Patienten Null entdeckt. Aber es ist keines unserer Systeme. Aber der “Lockdown” ist noch nicht beendet.

Inject VII: 03:34
Außendienst: Die Gegenseite erklärt dem Kunden, dass die abgerufenen Informationen offengelegt werden, wenn bis zum Ablauf von 24 Stunden kein Geld gezahlt wird. Der Kunde will nicht zahlen.

Inject VIII: 05:30
Cyber Security SME: Lockbit 6.0 kann sich im System "verstecken", um jederzeit Angriff erneut durchführen zu können.

Inject IX: 09:00
Beliebige SIRT-Personen: Die Presse berichtet lokal über den Kunden und den Ransomware-Befall.

.....

*CSA = Cyber Security Analyst

Inject Beispiele Erwartung

Inject I: 16:06
Außendienst: meldet einen Ausfall am Standort des Kunden.

Issue Ticket wurde vollständig erstellt?

Es gibt keinen Zweifel mehr daran, dass es sich um einen CY Incident handelt.

Inject II: 16:35
Außendienst: Der Kunde erklärt, es gäbe einen Ransomware-Vorfall. Und ordnet das Issue dem CSA zu.

Die Investigation wird angemessen gestartet?

Inject III: 17:25
Außendienst: Bei der Ransomware handelt es sich um Lockbit **6**.0.

Die SIRT Rollen übernehmen die jeweiligen Aufgaben?

Inject IV: 17:45
Cyber Security SME: Bei LB 6.0 kann es auch zu einer “Data Exfiltration” und einer Datenmanipulation kommen.
Es gäbe noch nicht sehr viele Informationen zu 6.0

Die initiale Risiko/Impact Bewertung findet statt? (und wird protokolliert)

Inject V: 17:47
Außendienst: Der Kunde hat alle betroffenen Systeme und Systeme, die betroffen sein könnten, abgeschaltet.

Sofortmassnahmen sind beschlossen?

Inject VI: 20:30
Außendienst: Der Kunde hat den Patienten Null entdeckt. Aber es ist keines unserer Systeme. Aber der “Lockdown” ist noch nicht beendet.

“Lockup” Kriterien sind definiert.?

Inject VII: 03:34
Außendienst: Die Gegenseite erklärt dem Kunden, dass die abgerufenen Informationen offengelegt werden, wenn bis zum Ablauf von 24 Stunden kein Geld gezahlt wird. Der Kunde will nicht zahlen.

Der Entscheidungs- und Kommrahmen wird erweitert?

Inject VIII: 05:30
Cyber Security SME: Lockbit 6.0 kann sich im System "verstecken", um jederzeit Angriff erneut durchführen zu können.

…….

Inject IX: 09:00
Beliebige SIRT-Personen: Die Presse berichtet lokal über den Kunden und den Ransomware-Befall.

…….

Observation Log

Mögliche Fehler während der Übung

“Ich weiss nicht was ich machen soll.”	Unklare Zielsetzung
“Davon haben wir noch nie gehört.”	Kein Schulung/Training ([6] Table 11)
“grrrgrrrgrrr?”	no vital stimulus/kein vitaler Reiz
“Jetzt müsste eigentlich …”	Keine Übung zur Übung.
“Wer kümmert sich eigentlich um…?”	Unvollständige Incident Response Pläne

will be continued …

Tips

1. **Überfrachten** Sie das Training nicht mit zu komplexen Szenarien und zu vielen Ereignissen.
2. Überlegen Sie während der Vorbereitung gut, ob wirklich alle **Prozessschritte** in einer Übung zu trainieren sind.
3. Führen Sie die Übung möglichst **multimedial** durch (z.B. Mails, Chats, Videos, Karten).
4. Führen Sie **Trainingsregeln** ein: “Entscheidungen sind keine Präzedenzfälle.”
5. Wenn es bei allen Beteiligten zu große Unterschiede im Wissen gibt, wird entweder die Übung darauf abgerichtet, die Lücken zu füllen oder **fachfremde Themen** werden jeweils **vermieden**.
6. Richten Sie einen **Übungsraum** ein, der physisch, virtuell oder beides für Übungsszenarien benutzt werden kann. (mit Reset-Optionen, ohne Vermischung mit realer Umgebung, schnell wiederherstellbar)**.**
7. Alle **Elemente** der Übung sollten in **Relation** zueinander stehen.
8. Am Ende muss immer ein entsprechend nützliches Ergebnis sichtbar sein (**outcome**) ([6] Table 3 und 10).

Standards, Frameworks, Modelle

Es gibt derzeit wenige nutzbare Modelle für die Durchführung einer IRT Übung.

Erwähnenswert ist die **NIST SP 800-84**
Ein Leitfaden für Test-,Schulungs- und Trainingsprogramme.
Der Leitfaden stellt im Anhang zahlreiche Muster zur Verfügung.

References

[1] UK NCSC Training Tool
https://exerciseinabox.service.ncsc.gov.uk/

[2] NIST Guide to Test, Training and Exercise
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf

[3] ISACA Cybersecurity Incident Response Exercise Guidance
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance

[4] 16 Common Attack Vectors in 2023
https://www.upguard.com/blog/attack-vector

[5] MITRE ATT&CK Knowledge Base
https://attack.mitre.org/

[6] MITRE Cyber Exercise Playbook
https://www.mitre.org/sites/default/files/2022-09/pr_14-3929-cyber-exercise-playbook%20.pdf

[7] CISA Tabletop Exercise Packages
https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

[8] JOINT TRAINING MANUAL FOR THE ARMED FORCES OF THE UNITED STATES (CJCSM 3500.03E)
https://www.jcs.mil/Portals/36/Documents/Library/Manuals/m350003.pdf

Übung

Entwerfen Sie ein Incidents Übungszenario.
Erstellen Sie dazu mindestens 10 Injects.
Die Injects werden in einer Tabelle geführt und enthalten folgende Spalten (Beispiel auf der nächsten Seite):

- ID
- Inject Text
- Description
- IR Team Response/Reaction (Was ist die erwartete Team-Reaktion)
- Dry Run Information (Interne Hinweise für die Übungsdurchführung)
- Expected response/outcome by the participants (Erwarteter Nutzen des Injects)
- Started IR Prozess-Step (Wo befinden wir uns im IR Prozess)

Inject Beispieleinträge

ID	Inject Text	Description	own/IR Team Response/Reactio	Dry Run Information	Expected response/outcome by the particip	Started IR Prozess-Step
Initial Report	Customer/FSE creates a Ticket/Case.	We (Cyber) don't get anything from this ticket yet. It is only about the system being slower than usual.	own sends out a technician.	That can be simulated only and will be a part of the final report.	Case created. Case ID available.	Assessment
Inject 0	FSE informs that a **Ransom NOTE** has been found	The customer informed that a ransom note appeared on the screen. They stopped their work and informed own.	Infoms Cybersecurity. It is instructed to pull the network cable.	A real ransom note is provided to the participants.	At this point, at the latest, a Cyber Security Incident should be declared and the IR convened. Are the appropriate participants involved? Are the IR roles clear? Does everyone know what they have to do? The team is discussing whether a shutdown or lockdown (pull network cable) of the system is needed! IR minutes started. Templates used. First containment measures has to be done.	Containment
Inject 1	System problems since two days. **Ticket was created -1 day**.	The ransomware has been on the system for at least two days.	FSR is supposed to find out how long the ransomware has really been on the system. Moreover, it should find out which ransomware it is exactly. Other questions should also be asked at this point.	Are we relying on 2 days being correct or has the ransomware been on the system for longer.	The IR calls for further analysis. Is only ours affected? What other cases are there with the customer? (A memory dump is arranged.)? ...	Analysis
Inject 3	**FSR found encrypted files**. And a readme.txt ransom note including a bitcoin id.	The technician finds another ransom note from which IR SME determines that it is the CockBit NG ransomware.	The IR team assigns the CSA (Forensic) to find out what the ransomware is all about.	From here on, it can go in different directions. Ransomware is an invention. However, it is unknown to the IR team.	The team discusses and clarifies whether the files need to be decrypted, or whether it is sufficient to restore a backup or only a reinstallation is required.	Eradiction/Revovery
Inject 4	The customer detected **suspicious network activity.**	The customer reports that from our system they try to reach other systems in the network. There is communication at the network level, but also login attempts.	The IR team is asking for more information. Ideally a Network Package Capture.	At this point, it is important to know when to request more information and have a plan in place when it is not provided.	The IR team decides to wait for the packet capture (or its evaluation) and until then to assume that the system was under alien control.	Assessment
Inject 5	Management asks what it's all about and wants an immediate statement. (Inject)	The team asks what exact information is expected in addition to the IR Minutes.	The insight will be added to the IR Minutes.	At this point, a disruption can be built in. Conceivable is the uncertainty of the parties involved.		Fault activity
Inject 5	The FSR reports that no packet	The customer did not find any evidence	The insight will be added to the			

Beispiel Szenarien

Scenario

Ransomware on the XYZ Hospital network affects the Grandmaster 2000 application server.

Andere denkbare Szenarien:

- Suspect unauthorized access
- Data breach authorized access
- Compromise Social Engineering
- Compromise System Ransomware
- Cloud Resources misused for Crypto Mining
- Computing device
- Data Breach Database Server
- Data Breach Backup Media
- Data Breach Combined Cloud
- Network Compromise Router
- Network Compromise Wireless
- Network Service DDOS
- Unauthorized Sharing Information