Tabletop Exercise

Den Umgang mit Gefahrensituationen erspielen

Jochen Kurz
Referent Informationssicherheit bwInfoSec

bwInfoSec

Tabletop Übungen – Umgang mit Gefahrensituationen

Wie übe ich einen Notfall?

Tabletop Übungen – Umgang mit Gefahrensituationen

Notfallübungen

Tabletop Übungen – Umgang mit Gefahrensituationen

Notfallübung im Rechenzentrum

Tabletop Übungen – Umgang mit Gefahrensituationen

Rollenspiele?!

Tabletop Übungen – Umgang mit Gefahrensituationen

Was ist das?

Eine Tabletop-Übung (auch TTX oder Tabletop Exercise genannt) ist eine Art von Übung, die in verschiedenen Bereichen, wie beispielsweise im Krisenmanagement, in der **Informationssicherheit**, im Notfallmanagement und in anderen Bereichen, durchgeführt wird.

Die Übung erhält ihren Namen, weil sie oft an einem Tisch (englisch: "table") stattfindet. Während der Übung präsentiert ein **Moderator** oder ein Facilitator den Teilnehmern ein **Szenario**, das eine bestimmte Krise, einen Notfall oder ein Problem simuliert

Tabletop-Übungen sind eine nützliche Methode, um das **Krisenmanagement** und die **Notfallvorbereitung** in verschiedenen Organisationen zu **verbessern**. Sie helfen, Schwachstellen in bestehenden Plänen aufzudecken, das Bewusstsein für potenzielle Risiken zu schärfen und die Teamzusammenarbeit zu fördern.

Tabletop Übungen – Umgang mit Gefahrensituationen

Allgemeine Vorteile

Riskante Situationen ohne reale Gefahren

Tabletop-Übungen ermöglichen es, riskante oder kritische Situationen zu simulieren, ohne tatsächliche Gefahren oder negative Auswirkungen für Menschen oder Ressourcen zu verursachen. Dies erlaubt es den Teilnehmern, in einer sicheren Umgebung zu üben und zu lernen

Erkennen von Schwachstellen

Die Übungen helfen dabei, Schwachstellen und Lücken in bestehenden Plänen und Prozessen aufzudecken, ohne dass es zu echten Katastrophen oder Sicherheitsvorfällen kommt. Dies ermöglicht es, frühzeitig Korrekturen vorzunehmen..

Reaktionen und Entscheidungsfindung üben

Die Teilnehmer können ihre Reaktionsfähigkeit auf verschiedene Szenarien und Bedrohungen üben, Entscheidungen treffen und Lösungen entwickeln, ohne dass echte Schäden entstehen.

Planung und Vorbereitung

Tabletop-Übungen sind ein wichtiger Bestandteil der Notfall- und Krisenplanung. Sie helfen, Pläne zu entwickeln, zu überarbeiten und sicherzustellen, dass alle Mitarbeiter wissen, wie sie in Notfällen reagieren sollen

Kontinuierliche Verbesserung

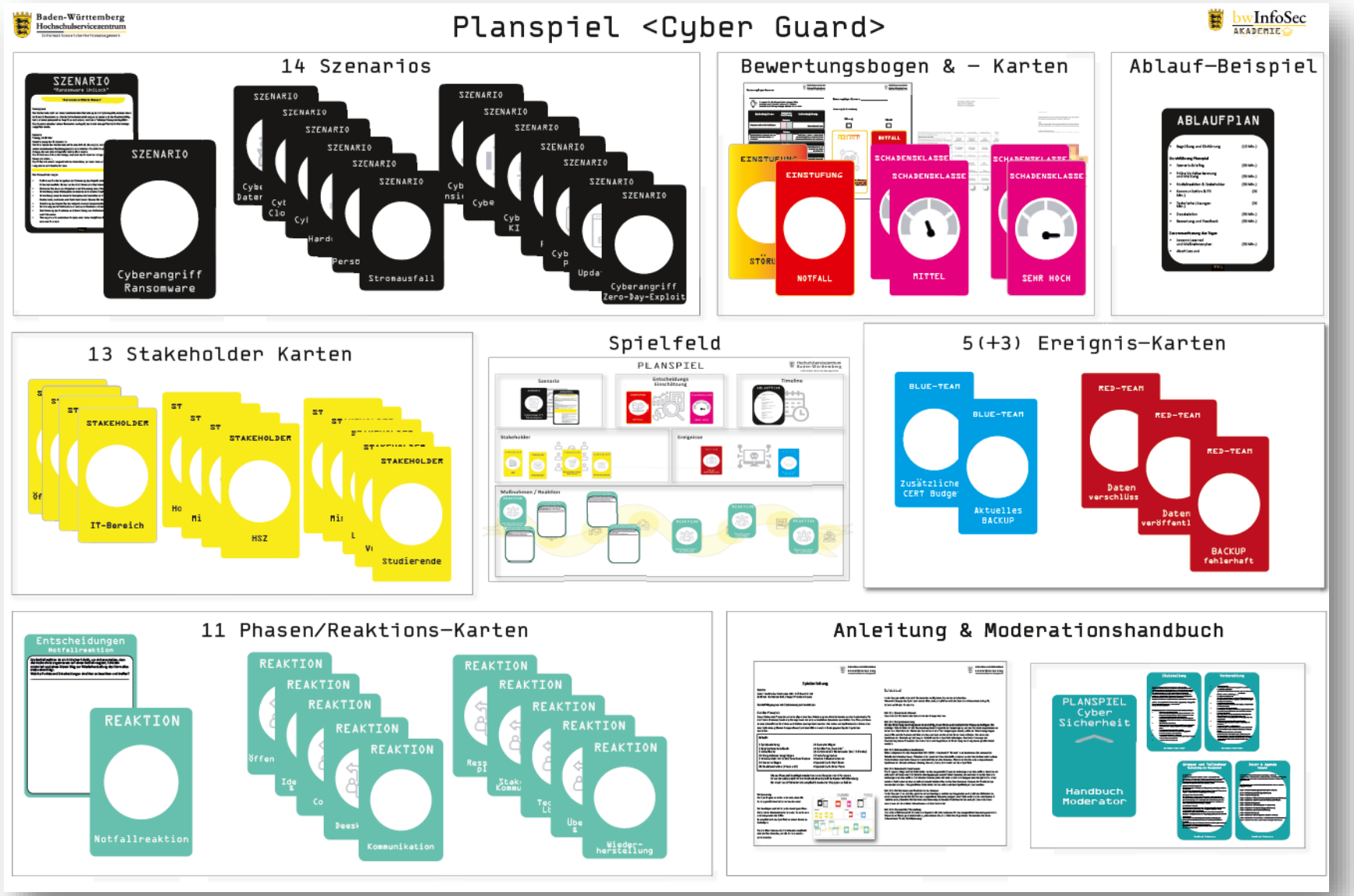
Nach einer Übung können Sie die Ergebnisse analysieren, Schwachstellen identifizieren und Maßnahmen zur Verbesserung ergreifen.
Dies unterstützt die kontinuierliche Verbesserung von Prozessen und Plänen.

Planspiel
<Cyber Guard>

bwInfoSec

Tabletop Übungen – Umgang mit Gefahrensituationen

Übersicht



Tabletop Übungen – Umgang mit Gefahrensituationen

Wie baue ich eine Übung auf?

Szenario-Dokumente
Dokumente, die das Szenario und die Hintergrundgeschichte beschreiben

Kommunikationsmittel
Erforderliche Kommunikationsmittel vor, die während der Übung verwendet werden sollen. (E-Mail-Vorlagen, Meldungen, …)

Checklisten und Vorlagen
Checklisten und Vorlagen, die den Teilnehmern bei der Durchführung bestimmter Aufgaben und Entscheidungen während der Übung helfen.

Zeitpläne und Ablaufpläne
Entwickeln Sie einen detaillierten Zeitplan, der den Ablauf der Übung festlegt.

Protokolle und Dokumentation
Sicherstellen, dass Sie die notwendigen Materialien für die Protokollierung und Dokumentation der Übung haben.

Präsentationsmittel
Falls erforderlich, bereiten Sie Präsentationsmittel wie Folien, Diagramme oder Visualisierungen vor.

Testumgebung In einigen Übungen kann eine Testumgebung erforderlich sein, um das Szenario zu simulieren.

Zugang zu Fachleuten und Ressourcen: Stellen Sie sicher, dass Sie Zugang zu Fachleuten oder Ressourcen haben, die während der Übung als Experten oder Ratschläge konsultiert werden können. Dies kann externe Sicherheitsberater oder interne Experten einschließen.

Bewertungs- und Verbesserungsmaterialien
Materialien, um die Ergebnisse der Übung zu bewerten und Verbesserungsempfehlungen zu dokumentieren.

Tabletop Übungen – Umgang mit Gefahrensituationen

Team-Setup

Tabletop-Übungen sind Gruppenübungen!

Gruppengröße
Es ist empfehlenswert, dass jede Gruppe groß genug ist, um verschiedene Fachkenntnisse und Verantwortlichkeiten abzudecken, einschließlich IT-Sicherheit, Kommunikation, Management usw.
Eine typische Gruppengröße könnte etwa **4 bis 8 Personen** betragen, abhängig von der Anzahl der verfügbaren Fachkenntnisse und Rollen.

Gesamtanzahl der Teilnehmer:
Die Gesamtanzahl der Teilnehmer hängt von der Anzahl der erstellten Gruppen ab.
Eine moderate Gesamtanzahl könnte zwischen **12 und 24 Teilnehmern** liegen, wenn drei bis vier Gruppen gebildet werden.

Tabletop Übungen – Umgang mit Gefahrensituationen

Team-Setup

Gegeneinander spielen

- Das Einführen von Wettbewerbselementen, bei denen mehrere Gruppen gegeneinander spielen, kann die **Übung dynamischer und interaktiver gestalten**.
- Es kann den Wettbewerbsgeist anregen, die Zusammenarbeit fördern und den Druck simulieren, den Teams in einer **realen Krisensituation erleben** könnten.

Überlegungen

- Sicherstellen, dass jede Gruppe eine angemessene Menge an Informationen und Ressourcen hat, um die Übung realistisch zu gestalten.

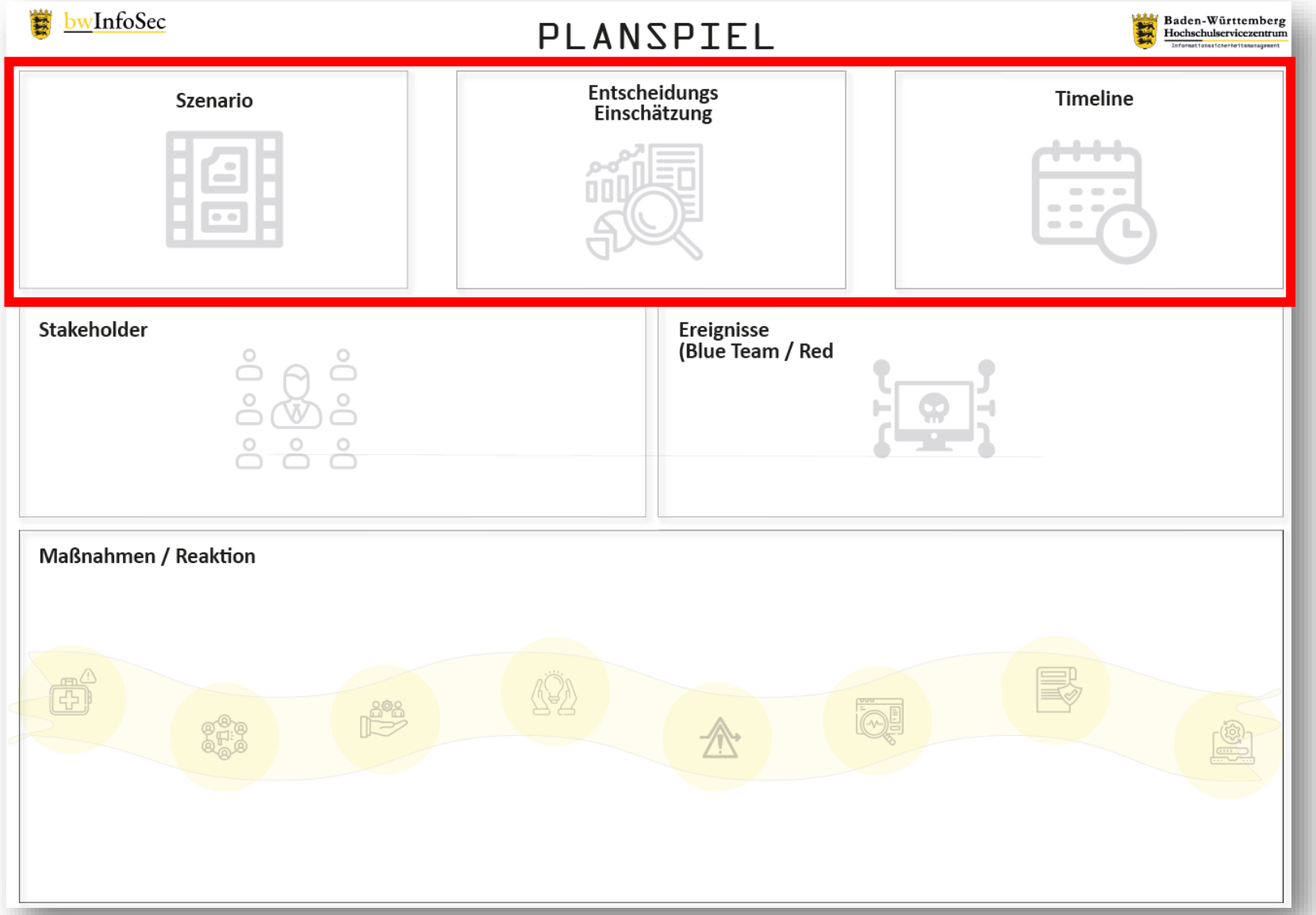
- Darauf achten, dass die Anzahl der Teilnehmer und Gruppen auch den Zeitaufwand für die Übung beeinflussen kann.

- Sicherstellen, dass genügend Zeit für Diskussionen, Reflexion und Feedback vorhanden ist.

- Es ist wichtig, die **Ziele der Übung zu berücksichtigen**.
    - Wenn das Hauptziel darin besteht, Teamarbeit und Zusammenarbeit zu fördern, könnte es sinnvoll sein, Gruppen kooperativ anstatt gegeneinander arbeiten zu lassen.
    - Wenn jedoch Wettbewerb und Druck wichtige Aspekte Ihrer Ziele sind, kann das Spielen mehrerer Gruppen gegeneinander sinnvoll sein.

Tabletop Übungen – Umgang mit Gefahrensituationen

Phase 1



Tabletop Übungen – Umgang mit Gefahrensituationen

Ablaufplan

Tabletop-Übung - Ransomware-Attacke

Bsp. Agenda:

09:00 - 09:15 Uhr: Begrüßung und Einführung (15 Minuten)

09:15 - 09:45 Uhr: Szenario-Briefing (30 Minuten)

09:45 - 10:15 Uhr: Schritt 1 - Frühe Vorfallserkennung und Meldung (30 Minuten)

10:15 - 10:30 Uhr: Kaffeepause

10:30 - 11:00 Uhr: Schritt 2 - Notfallreaktion (30 Minuten)

11:00 - 11:30 Uhr: Schritt 3 - Technische Lösungen (30 Minuten)

11:30 - 12:00 Uhr: Schritt 4 - Öffentlichkeitsarbeit (30 Minuten)

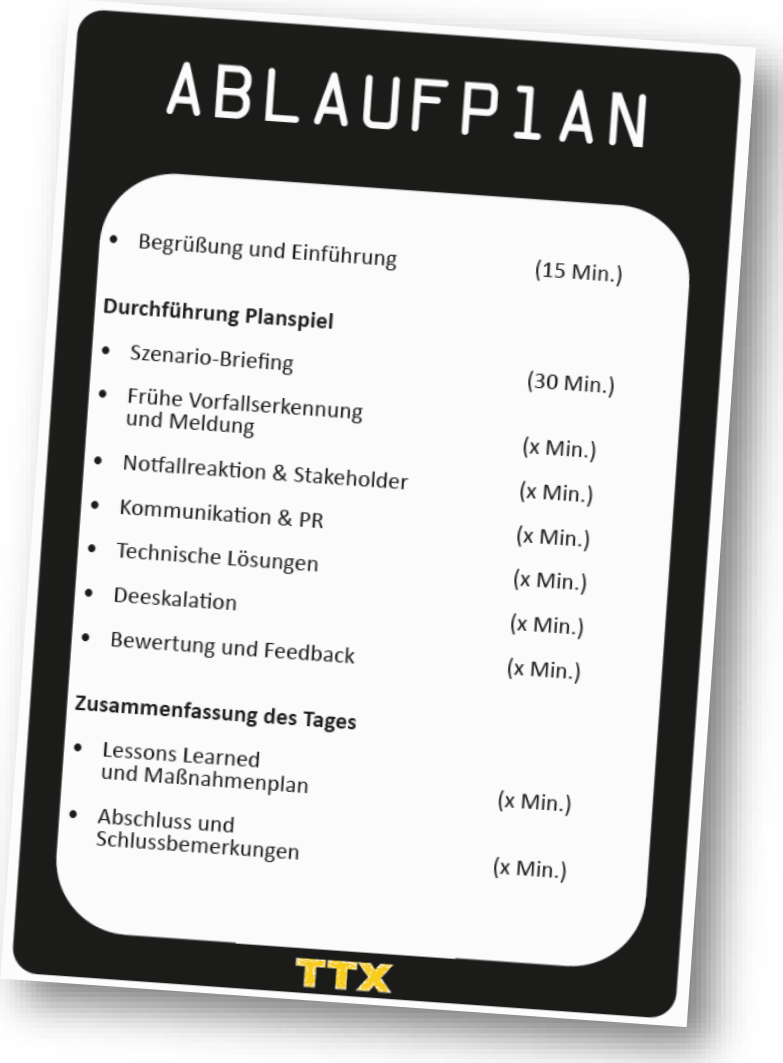
12:00 - 13:00 Uhr: Mittagspause

13:00 - 13:30 Uhr: Schritt 5 - Deeskalation (30 Minuten)

13:30 - 14:00 Uhr: Schritt 6 - Bewertung und Feedback (30 Minuten)

14:00 - 14:30 Uhr: Schritt 7 - Lessons Learned und Maßnahmenplan (30 Minuten)

14:30 - 15:00 Uhr: Abschluss und Schlussbemerkungen (30 Minuten)



Tabletop Übungen – Umgang mit Gefahrensituationen

Weitere Szenario-Optionen

Cyber-Angriff Szenarios (Auszug)

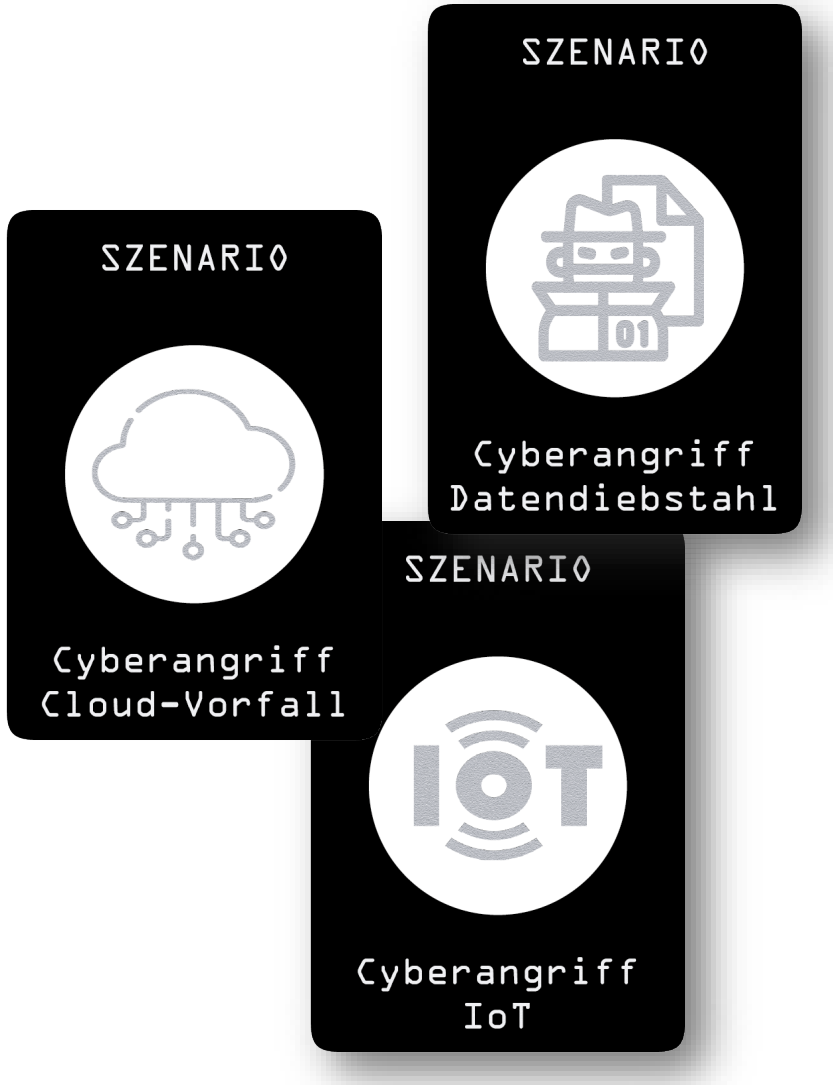
Ransomware-Angriff
Eine Organisation wird Opfer eines Ransomware-Angriffs, bei dem kritische Systeme verschlüsselt werden. Die Angreifer fordern Lösegeld für die Entschlüsselung.

Phishing-Attacke
Mitarbeiter erhalten gefälschte E-Mails, die dazu dienen, Zugangsdaten zu stehlen oder schädliche Anhänge zu verbreiten. Die Organisation muss auf eine breite Phishing-Kampagne reagieren.

Insider-Bedrohung
Ein Mitarbeiter, absichtlich oder unbeabsichtigt, stellt vertrauliche Daten frei oder führt schädliche Handlungen aus. Die Organisation muss auf eine interne Bedrohung reagieren.

Distributed Denial of Service (DDoS)
Die Website oder die Online-Dienste der Organisation werden Ziel eines DDoS-Angriffs, der den Zugang für Benutzer blockiert. Die Organisation muss den Angriff abwehren und den Service wiederherstellen.

Zero-Day-Exploit
Eine bisher unbekannte Schwachstelle wird von Angreifern ausgenutzt, um in das Netzwerk einzudringen. Die Organisation muss auf die Entdeckung und Behebung der Schwachstelle reagieren.



Tabletop Übungen – Umgang mit Gefahrensituationen

Szenario-Karten (Bsp. Ransomware-Attacke)

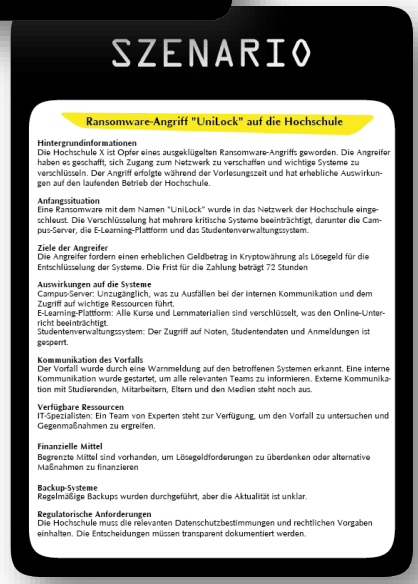
Ransomware-Angriff "UniLock" auf die Hochschule

Hintergrundinformationen
Die Hochschule X ist Opfer eines ausgeklügelten Ransomware-Angriffs geworden. Die Angreifer haben es geschafft, sich Zugang zum Netzwerk zu verschaffen und wichtige Systeme zu verschlüsseln. Der Angriff erfolgte während der Vorlesungszeit und hat erhebliche Auswirkungen auf den laufenden Betrieb der Hochschule.

Anfangssituation
Eine Ransomware mit dem Namen "UniLock" wurde in das Netzwerk der Hochschule eingeschleust. Die Verschlüsselung hat mehrere kritische Systeme beeinträchtigt, darunter die Campus-Server, die E-Learning-Plattform und das Studentenverwaltungssystem.

Ziele der Angreifer
Die Angreifer fordern einen erheblichen Geldbetrag in Kryptowährung als Lösegeld für die Entschlüsselung der Systeme. Die Frist für die Zahlung beträgt 72 Stunden

Auswirkungen auf die Systeme
Campus-Server: Unzugänglich, was zu Ausfällen bei der internen Kommunikation und dem Zugriff auf wichtige Ressourcen führt.
E-Learning-Plattform: Alle Kurse und Lernmaterialien sind verschlüsselt, was den Online-Unterricht beeinträchtigt.
Studentenverwaltungssystem: Der Zugriff auf Noten, Studentendaten und Anmeldungen ist gesperrt.



Tabletop Übungen – Umgang mit Gefahrensituationen

Verschiedene Zielgruppen

Szenarios (Auszug), Ziele und Zielgruppen

Szenario-Name	Ziel	Geeignet für Zielgruppe(n)
Datendiebstahl an der Hochschule	Ermittlung der Angriffsmethode und Begrenzung der weiteren Verbreitung von gestohlenen Daten	Alle Mitarbeitenden
Defekter Switch im Rechenzentrum	Eindämmung des Problems und Wiederherstellung der Netzwerkverbindung.	IT-Abteilung
Pandemie-bedingter Notfall an der Hochschule	Evaluierung der Wirksamkeit von Remote-Lern- und Arbeitsplänen sowie der Unterstützung von Gesundheit.	Verwaltung, Gesundheitsdienste, IT-Abteilung
Unerwarteter Personalengpass	Entwicklung von kurzfristigen Lösungen zur Deckung der wichtigsten Funktionen.	Verwaltung, Personalabteilung
Phishing-Attacke an der Hochschule	Ãœberprüfung der Authentizität von E-Mails und Entwicklung von Kommunikationsstrategien zur Warnung.	Verwaltung, IT-Abteilung
Ransomware-Angriff	Ermittlung des Ausmaßes der kompromittierten Systeme und Entwicklung von Maßnahmen zur Wiederherstellung.	IT-Abteilung, Kommunikation
Stromausfall an der Hochschule	Sicherstellung der Geschäftskontinuität und Bewältigung der Auswirkungen auf den regulären Betrieb.	IT-Abteilung, Verwaltung Notfallteam

Tabletop Übungen – Umgang mit Gefahrensituationen

Phase 2

bwInfoSec

PLANSPIEL

Baden-Württemberg Hochschulservicezentrum
Informationssicherheitsmanagement

Szenario

Entscheidungs Einschätzung

Timeline

Stakeholder

Ereignisse (Blue Team / Red

Maßnahmen / Reaktion

bwl

Tabletop Übungen – Umgang mit Gefahrensituationen

Entscheidungs-/Diskussionspunkte – Bsp. Ransomware-Attacke

1	**Identifikation & Bewertung**	Wie wird die Ransomware-Attacke erkannt: • Über eine Warnmeldung, verdächtige Aktivitäten • Oder Benutzerberichte?
2	**Meldung**	Wann und wie werden die verschiedenen Teams (IT, Hochschulleitung, PR) intern und extern über die Ransomware-Attacke informiert?
3	**Notfallreaktion**	Welche Sofortmaßnahmen werden ergriffen, um die Ausbreitung der Ransomware zu stoppen: • Abschalten von Systemen? • Trennen des Netzwerks?
4	**Ressourcen-zuweisung**	Wie werden Ressourcen wie IT-Spezialisten, finanzielle Mittel und Hardware für die Bewältigung des Vorfalls zugewiesen?
5	**Stakeholder-Kommunikation**	Wie und wann werden die Studierenden, Hochschulmitarbeiter, Eltern und externe Partner über die Ransomware-Attacke informiert?

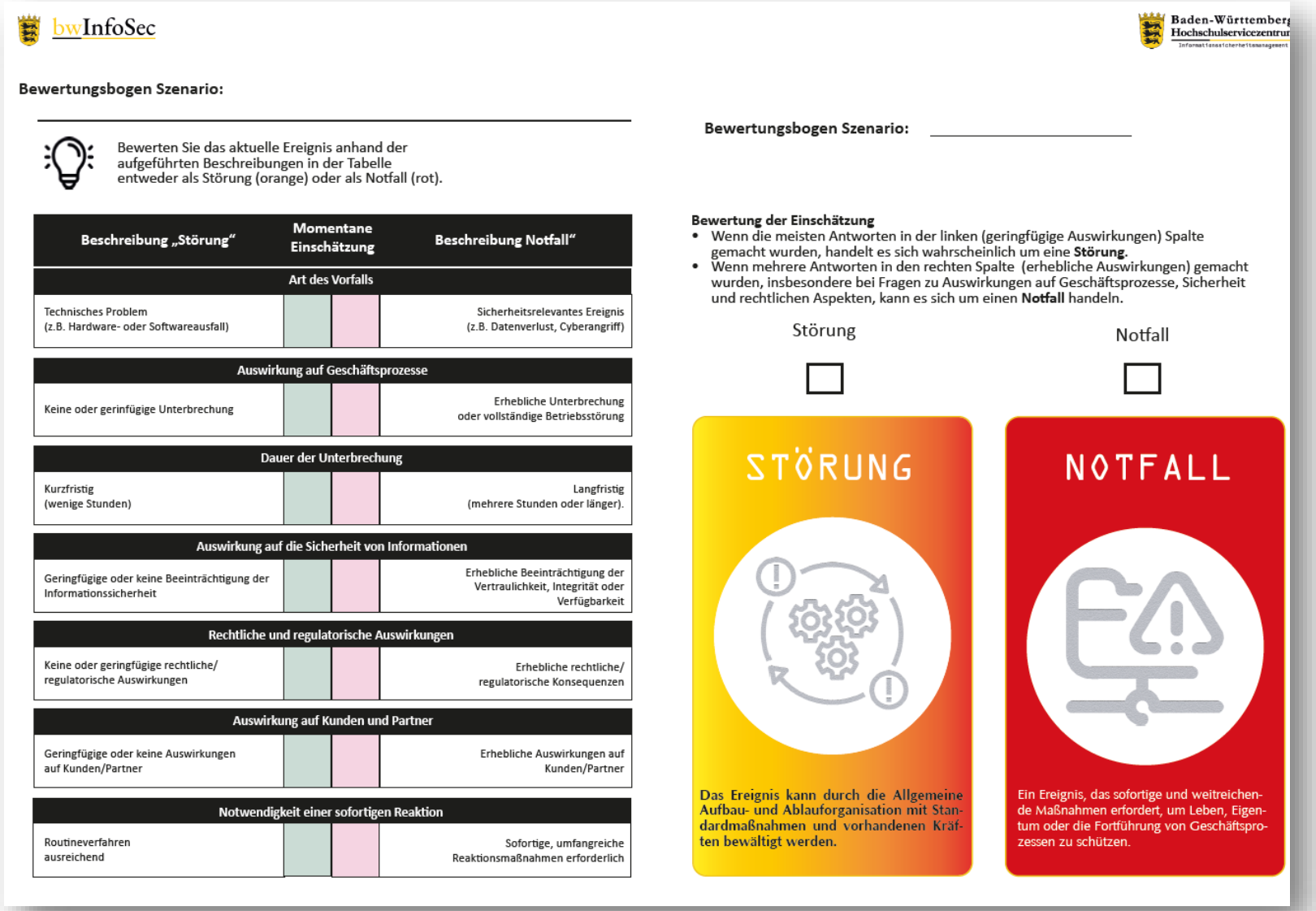
Tabletop Übungen – Umgang mit Gefahrensituationen

Entscheidungs-/Diskussionspunkte – Bsp. Ransomware-Attacke

6	**Entscheidungen zu Compliance**	Wie wird mit den regulatorischen Anforderungen und Compliance-Fragen im Zusammenhang mit dem Vorfall umgegangen?
7	**Technologische Lösungen**	Welche technologischen Lösungen werden eingesetzt, um die Ransomware zu **identifizieren**, zu **entfernen** und die Systeme **wiederherzustellen**?
8	**Öffentlichkeits-Arbeit**	Wie wird die Hochschule die Öffentlichkeit über den Vorfall informieren und dabei den Ruf schützen?
9	**Deeskalation**	Welche Schritte werden unternommen, um den Vorfall zu deeskalieren und die negativen Auswirkungen zu minimieren?
10	**Wiederherstellung**	Wie wird die Wiederherstellung der betroffenen Systeme und Daten koordiniert, um den normalen Hochschulbetrieb wieder aufzunehmen?
11	**Überwachung & Lernen**	Wie wird der Vorfall überwacht, um daraus zu lernen und Maßnahmen zur Stärkung der Sicherheit zu ergreifen?

Tabletop Übungen – Umgang mit Gefahrensituationen

Step: Bewertung der Situation



bwInfoSec

Bewertungsbogen Szenario:

Bewerten Sie das aktuelle Ereignis anhand der aufgeführten Beschreibungen in der Tabelle entweder als Störung (orange) oder als Notfall (rot).

Beschreibung „Störung“	Momentane Einschätzung		Beschreibung Notfall“
Art des Vorfalls			
Technisches Problem (z.B. Hardware- oder Softwareausfall)			Sicherheitsrelevantes Ereignis (z.B. Datenverlust, Cyberangriff)
Auswirkung auf Geschäftsprozesse			
Keine oder gerinfügige Unterbrechung			Erhebliche Unterbrechung oder vollständige Betriebsstörung
Dauer der Unterbrechung			
Kurzfristig (wenige Stunden)			Langfristig (mehrere Stunden oder länger).
Auswirkung auf die Sicherheit von Informationen			
Geringfügige oder keine Beeinträchtigung der Informationssicherheit			Erhebliche Beeinträchtigung der Vertraulichkeit, Integrität oder Verfügbarkeit
Rechtliche und regulatorische Auswirkungen			
Keine oder geringfügige rechtliche/ regulatorische Auswirkungen			Erhebliche rechtliche/ regulatorische Konsequenzen
Auswirkung auf Kunden und Partner			
Geringfügige oder keine Auswirkungen auf Kunden/Partner			Erhebliche Auswirkungen auf Kunden/Partner
Notwendigkeit einer sofortigen Reaktion			
Routineverfahren ausreichend			Sofortige, umfangreiche Reaktionsmaßnahmen erforderlich

Bewertungsbogen Szenario: _____

Bewertung der Einschätzung

- Wenn die meisten Antworten in der linken (geringfügige Auswirkungen) Spalte gemacht wurden, handelt es sich wahrscheinlich um eine **Störung**.
- Wenn mehrere Antworten in den rechten Spalte (erhebliche Auswirkungen) gemacht wurden, insbesondere bei Fragen zu Auswirkungen auf Geschäftsprozesse, Sicherheit und rechtlichen Aspekten, kann es sich um einen **Notfall** handeln.

Störung ☐ Notfall ☐

STÖRUNG

Das Ereignis kann durch die Allgemeine Aufbau- und Ablauforganisation mit Standardmaßnahmen und vorhandenen Kräften bewältigt werden.

NOTFALL

Ein Ereignis, das sofortige und weitreichende Maßnahmen erfordert, um Leben, Eigentum oder die Fortführung von Geschäftsprozessen zu schützen.

Tabletop Übungen – Umgang mit Gefahrensituationen

Step: Bewertung der Situation – Festlegen der Schadensklasse

Definition Schadensklasse für Szenario: _____

Bewerten Sie das aktuelle Ereignis anhand der aufgeführten Beschreibungen in der Tabelle auf den zu erwartenden Schaden je Kategorie.

Kriterium	Schadensklasse			
	niedrig	mittel	hoch	sehr hoch
Finanzielle Auswirkungen Die direkten und indirekten Kosten, die durch den Vorfall entstehen, einschließlich der Kosten für die Behebung des Vorfalls, möglicher Ausfallzeiten, Geldstrafen und rechtlicher Kosten.	Geringfügige Kosten	Moderate Kosten	Erhebliche Kosten	Existenz-bedro-hende Kosten
Auswirkungen auf Betriebskontinuität Das Ausmaß, in dem der Vorfall die normalen Geschäftsabläufe stört oder unterbricht, einschließlich der Dauer der Betriebsunterbrechung und der Effekte auf kritische Geschäftsprozesse.	Kurzfristige Unterbrechung	Mittelfristige Unterbrechung	Langfristige Unterbrechung	Vollständige Betriebs-störung
Reputationsschäden Das Ausmaß, in dem der Vorfall die normalen Geschäftsabläufe stört oder unterbricht, einschließlich der Dauer der Betriebsunterbrechung und der Effekte auf kritische Geschäftsprozesse.	Geringe negative Wahrnehmung	Moderate negative Wahrnehmung	Hohe negative Wahrnehmung	Sehr hohe negative Wahrnehmung
Rechtliche und regulatorische Auswirkungen Die Konformität mit Datenschutzgesetzen, Complian-ce-Richtlinien und anderen rechtlichen Anforderungen, einschließlich möglicher Rechtsstreitigkeiten und Strafen.	Geringfügige Verstöße	Moderate Verstöße	Schwere Verstöße	Existenzielle Verstöße
Auswirkung auf Informationssicherheit Der Grad der Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und IT-Systemen.	Geringfügige Beeinträchtigung	Moderate Beeinträchtigung	Hohe Beeinträchtigung	Sehr hohe Beeinträchtigung
Personelle und physische Sicherheit Auswirkungen auf die Sicherheit und das Wohlergehen von Mitarbeitern oder anderen Personen sowie auf die physische Sicherheit von Einrichtungen und Ausrüs-tung.	Geringfügige Auswirkung	Moderate Auswirkung	Hohe Auswirkung	Sehr hohe Auswirkung
Auswirkung auf Kunden und Partner Die Auswirkungen des Vorfalls auf Kunden, Lieferanten und andere Geschäftspartner, einschließlich des Verlusts von Kunden- oder Partnerdaten und der Unterbrechung von Dienstleistungen.	Geringfügige Beeinträchtigung	Moderate Beeinträchtigung	Hohe Beeinträchtigung	Sehr hohe Beeinträchtigung
Langfristige Folgen Potenzielle langfristige Auswirkungen auf die Organisa-tion, wie der Verlust von Wettbewerbsvorteilen oder langfristige Schäden an der Infrastruktur oder dem Ruf.	Geringfügige Auswirkung	Moderate Auswirkung	Erhebliche Auswirkung	Katashtrophale Langzeitfolgen

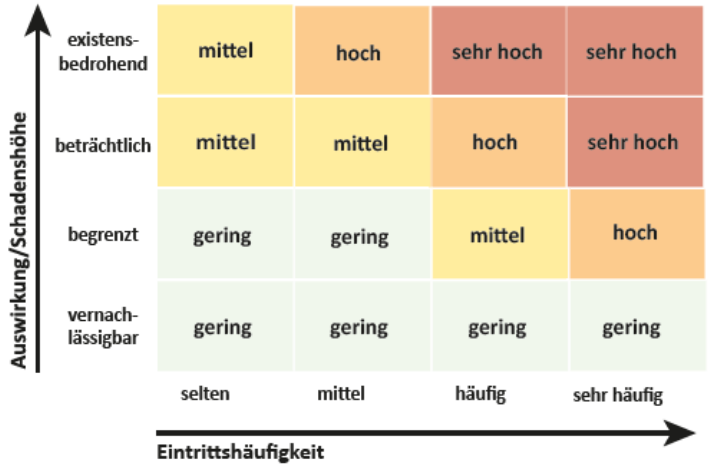
Risiko-Matrix - Definition „Risiko-Appetit“

Szenario: _____

1. Definition von Risiko:
Risiko im Informationssicherheitskontext wird als die Kombination aus der Wahrscheinlichkeit eines Sicherheitsvorfalls und dessen potenziellem Schaden definiert.

2. Rolle der Risikobewertung:
Die Risikobewertung hilft dabei, potenzielle Sicherheitsvorfälle nach ihrer Bedeutung zu priorisieren. Sie gibt an, wie wahrscheinlich ein Vorfall ist und wie gravierend seine Auswir-kungen sein könnten.

3. Verbindung zur Schadensklassenbewertung:
Die Schadensklassenbewertung ist ein Teil der Risikobewertung. Sie fokussiert sich auf die Einschätzung der potenziellen Schäden, die durch einen Vorfall verursacht werden könnten.



Eine Risikomatrix veranschaulicht die Beziehung zwischen der Eintrittswahrscheinlichkeit eines Vorfalles und dessen potenziellem Schaden. Sie unterstützt die Entscheidungsfindung, indem sie aufzeigt, welche Risiken akzeptabel sind und welche einer Reaktion bedürfen.

Die Bestimmung der der Schadensklasse kann dazu genutzt werden, Risiko-Bewertung zu trainiert

bwl

Tabletop Übungen – Umgang mit Gefahrensituationen

Step: Notfallreaktion

Sofortmaßnahmen
- Übung von schnellen Maßnahmen zur Eindämmung und zum Schutz kritischer Systeme.

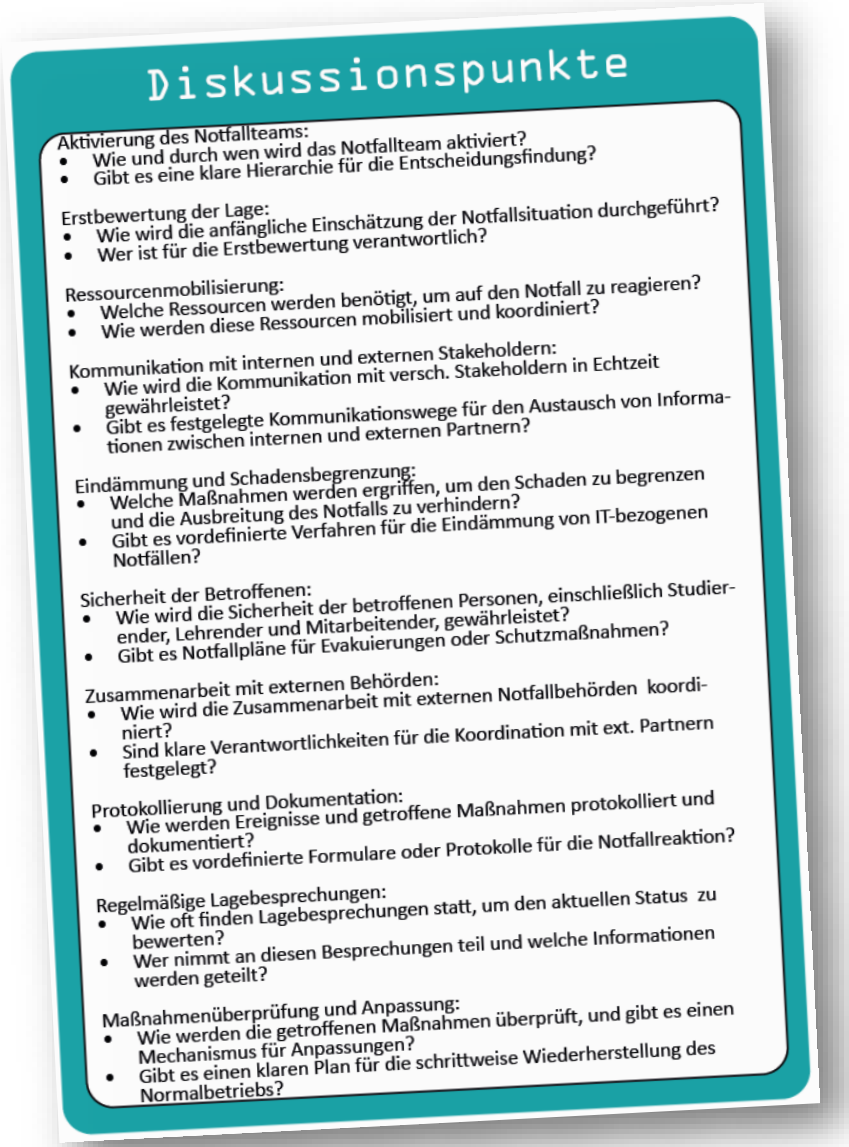
Koordination mit dem IT-Team
- Betonung der Zusammenarbeit zwischen Sicherheitsexperten und IT-Personal.

Forensik und Untersuchung
- Simulierte Szenarien zur Identifizierung von Angriffsquellen und -methoden.

Wiederherstellungsplanung
- Simulation der Planung für die Wiederherstellung betroffener Systeme.

Zeitliche Koordination
- Klare Zeitpläne für Sofortmaßnahmen, Forensik, Kommunikation und Wiederherstellung.

Dokumentation
- Dokumentation von Aktionen, Entscheidungen und Ergebnissen für die Nachanalyse.



Tabletop Übungen – Umgang mit Gefahrensituationen

Step: Kommunikation

Interne Kommunikation:

- Festlegen von Verantwortlichkeiten und Kommunikationswegen innerhalb der Organisation und zwischen Abteilungen bei Sicherheitsvorfällen.

Externe Kommunikation:

- Definieren von Verfahren für die Kommunikation mit externen Parteien, einschließlich Medien und Stakeholdern.
- Hauptansprechpartner und Kommunikationsrichtlinien klären.

Presse- und Social Media Management:

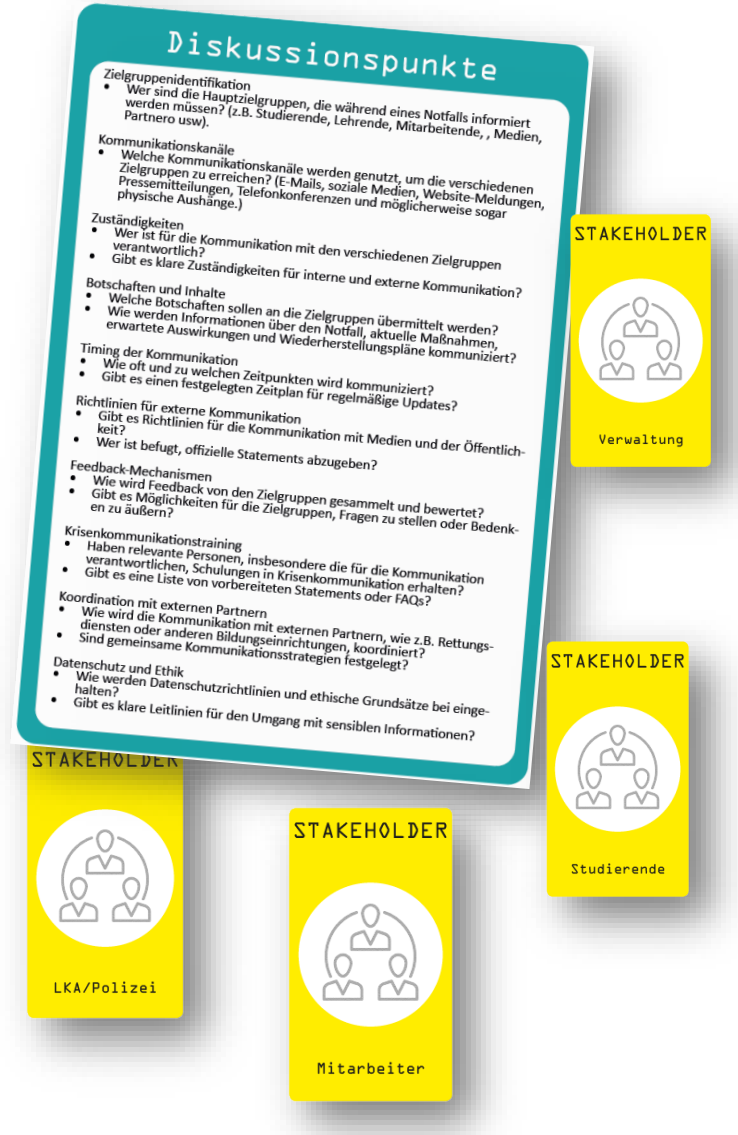
- Vorbereitung und Übung im Erstellen von Pressemitteilungen gemäß rechtlichen Anforderungen.
- Bestimmung der Rolle und des Managements von Social Media.

Kommunikation mit Betroffenen und externen Dienstleistern:

- Üben der direkten Kommunikation mit betroffenen Personen und der Koordination mit externen Beratern wie Forensikexperten.

Informationsaktualisierung und Compliance:

- Regelmäßige Aktualisierung der kommunizierten Informationen, um Unsicherheit zu minimieren und Vertrauen zu wahren.
- Sicherstellung, dass alle Kommunikationsmaßnahmen mit Datenschutzbestimmungen und rechtlichen Anforderungen übereinstimmen.



Tabletop Übungen – Umgang mit Gefahrensituationen

Step: Technologische Lösungen

Wie identifiziert und implementiert das Team technische Gegenmaßnahmen und Lösungen, um den Angriff zu stoppen, betroffene Systeme zu bereinigen und die Sicherheit der Infrastruktur wiederherzustellen

Identifikation der Angriffsmethode

- Durch Simulationen wird die spezifische Methode eines Ransomware-Angriffs analysiert und identifiziert.

Implementierung von Schutzmaßnahmen

- Um die Ausbreitung zu stoppen, werden sofort Schutzmaßnahmen wie die Anpassung von Firewall-Regeln, das Schließen von Sicherheitslücken und die Aktualisierung von Sicherheitsrichtlinien implementiert.

Systembereinigung

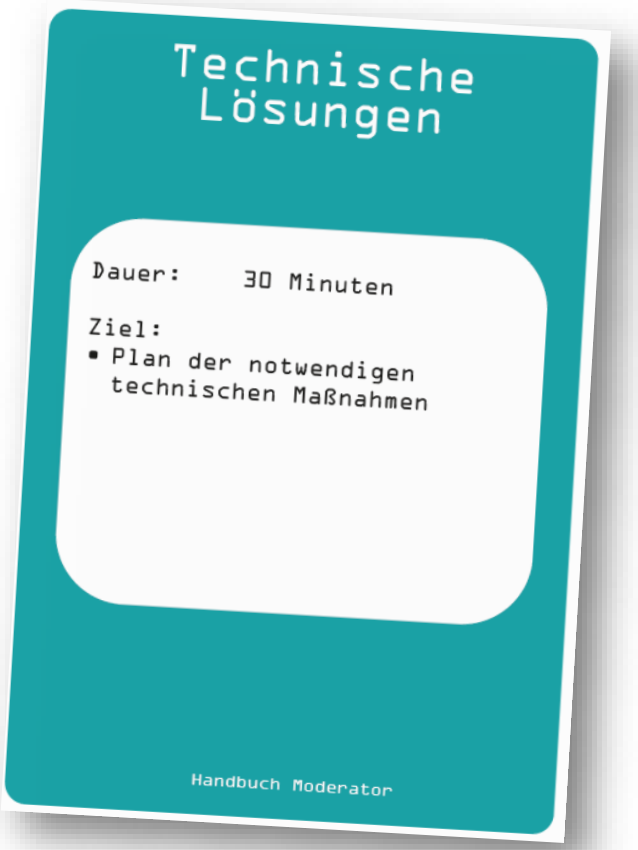
- Durchführung simulierter Szenarien zur Bereinigung infizierter Systeme, einschließlich Scannen, Entfernen schädlicher Software und Wiederherstellen der Systeme.

Koordination und Überprüfung

- Enge Koordination mit dem IT-Team zur effektiven Umsetzung der technischen Lösungen und Überprüfung der Backup-Systeme zur Sicherstellung der Datenwiederherstellung.

Zeitliche Koordination und Dokumentation

- Festlegung klarer Zeitpläne für die Implementierung der Maßnahmen und sorgfältige Dokumentation aller Schritte und Entscheidungen zur Ressourcenallokation.



Tabletop Übungen – Umgang mit Gefahrensituationen

Step: Deeskalation

Ziel ist es Strategien und Maßnahmen zu entwickeln und zu üben, um die Situation zu beruhigen, potenzielle Schäden zu minimieren, das Vertrauen der Stakeholder wiederherzustellen und den normalen Betrieb der Organisation wieder aufzunehmen

Krisenreaktionsplan:

- Simulation der Anwendung des Krisenreaktionsplans, um eine effektive Deeskalation des Vorfalls zu gewährleisten.

Überarbeitung der Kommunikationsstrategie:

- Anpassung der Kommunikationsstrategie durch Übungen, um deeskalierende Elemente zu integrieren und eine beruhigende Kommunikation sicherzustellen.

Stakeholder-Besänftigung:

- Durchführung simulierter Maßnahmen zur Beruhigung besorgter Stakeholder, einschließlich der direkten Adressierung ihrer Bedenken und Ängste.

Interne Mitarbeiterunterstützung & Psychologische Unterstützung:

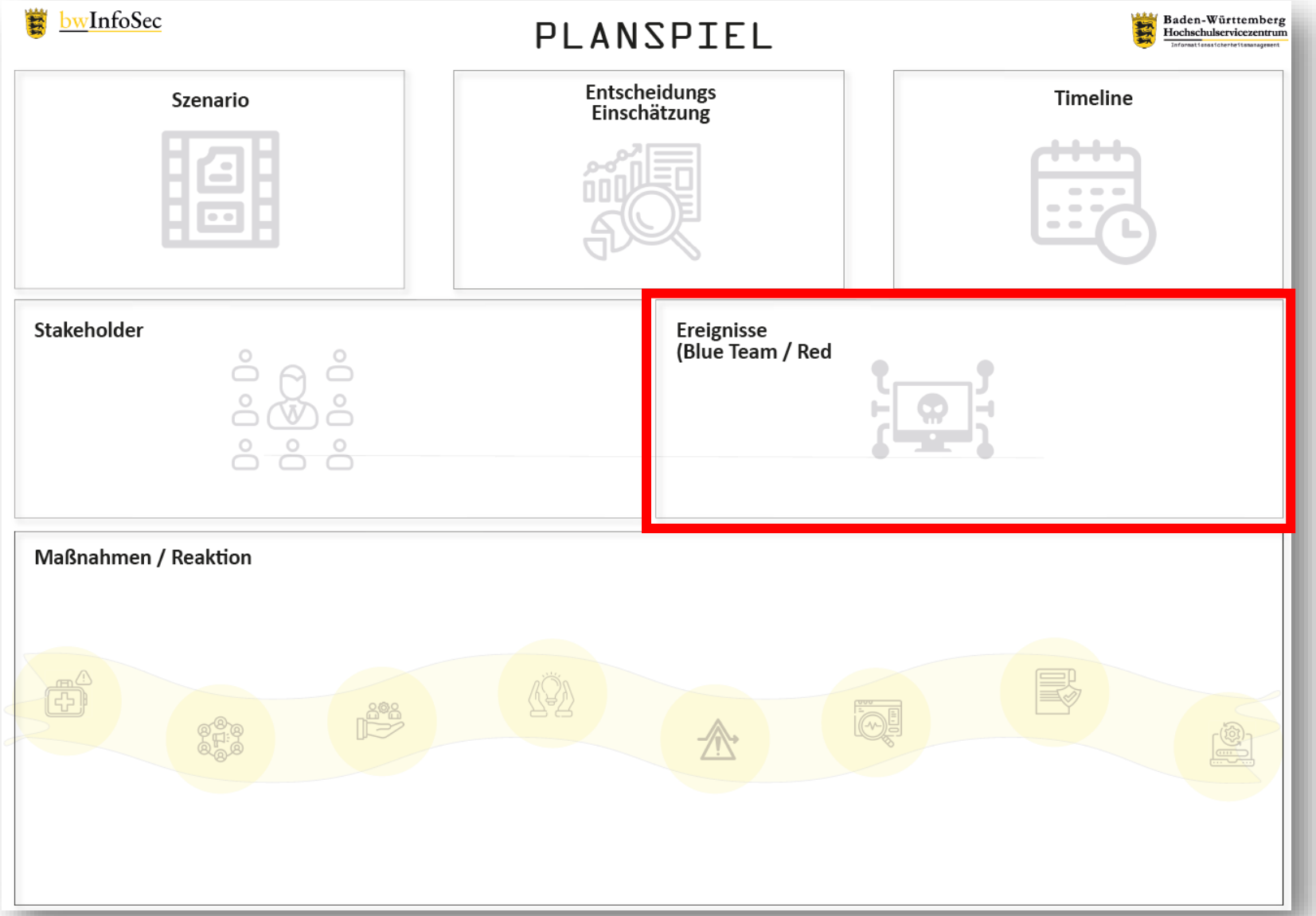
- Koordination interner Ressourcen zur Unterstützung und psychologischen Betreuung von Mitarbeitern, die direkt von dem Vorfall betroffen sind.

Wiederherstellung und Zeitmanagement:

- Simulation von Maßnahmen zur Wiederherstellung des Vertrauens und Stabilisierung des normalen Betriebs, einschließlich der Festlegung klarer Zeitpläne für alle Deeskalationsaktivitäten und sorgfältiger Dokumentation zur Nachanalyse.

Tabletop Übungen – Umgang mit Gefahrensituationen

Add-Ons



Tabletop Übungen – Umgang mit Gefahrensituationen

Szenario-Karten (Bsp. Ransomware-Attacke)

Ransomware-Angriff "UniLock" auf die Hochschule – Blue Team

Verfügbare Ressourcen

- IT-Spezialisten: Ein Team von Experten steht zur Verfügung, um den Vorfall zu untersuchen und Gegenmaßnahmen zu ergreifen.

Finanzielle Mittel

- Begrenzte Mittel sind vorhanden, um Lösegeldforderungen zu überdenken oder alternative Maßnahmen zu finanzieren.

Backup

- Regelmäßige Backups wurden durchgeführt, und können sofort eingespielt werden.

Tabletop Übungen – Umgang mit Gefahrensituationen

Szenario-Karten (Bsp. Ransomware-Attacke)

Ransomware-Angriff "UniLock" auf die Hochschule - RED TEAM

Besondere Herausforderungen

- Die Angreifer drohen mit der Veröffentlichung von sensiblen Daten, wenn das Lösegeld nicht gezahlt wird.
- Die finanziellen Mittel sind begrenzt, und die Hochschule steht unter öffentlichem Druck.

Entwicklung des Szenarios

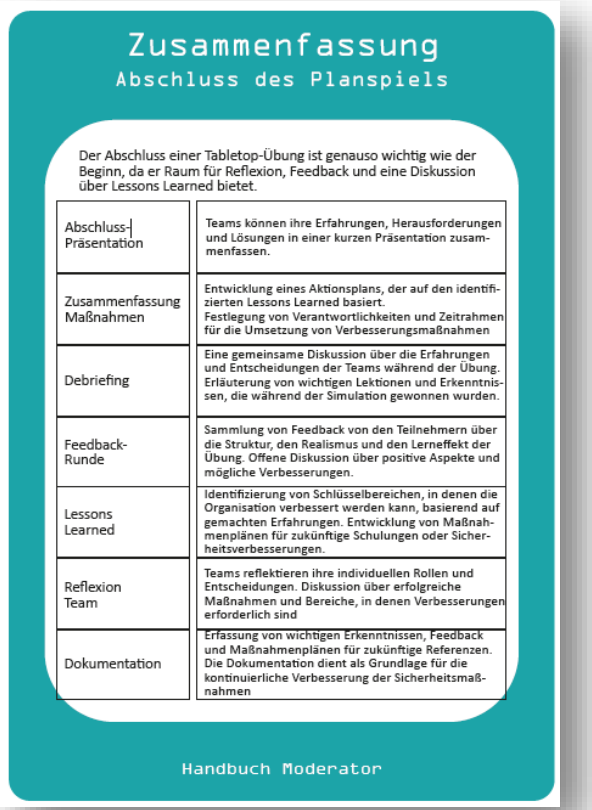
- Nach 24 Stunden erhöhen die Angreifer den Druck, indem sie einige verschlüsselte Dateien als Beweis
  für ihre Forderungen veröffentlichen.
  Der Countdown für das Lösegeld läuft weiter.

Tabletop Übungen – Umgang mit Gefahrensituationen

Abschluss

Der Abschluss einer Tabletop-Übung ist genauso wichtig wie der Beginn, da er Raum für Reflexion, Feedback und eine Diskussion über Lessons Learned bietet.

Abschluss-Präsentation	Teams können ihre Erfahrungen, Herausforderungen und Lösungen in einer kurzen Präsentation zusammenfassen.
Debriefing	Gemeinsame Diskussion über die Erfahrungen und Entscheidungen der Teams während der Übung. Erläuterung von wichtigen Lektionen und Erkenntnissen, gewonnen wurden.
Feedback-Runde	Sammlung von Feedback von den Teilnehmern über die Struktur, den Realismus und den Lerneffekt der Übung. Offene Diskussion über positive Aspekte und mögliche Verbesserungen.
Lessons Learned	Identifizierung von Schlüsselbereichen, in denen die Organisation verbessert werden kann, basierend auf gemachten Erfahrungen. Entwicklung von Maßnahmenplänen für zukünftige Schulungen oder Sicherheitsverbesserungen.
Team-Reflexion	Teams reflektieren ihre individuellen Rollen und Entscheidungen. Diskussion über erfolgreiche Maßnahmen und Bereiche, in denen Verbesserungen erforderlich sind.
Zusammenfassung Maßnahmen	Entwicklung eines Aktionsplans, der auf den identifizierten Lessons Learned basiert. Festlegung von Verantwortlichkeiten und Zeitrahmen für die Umsetzung von Verbesserungsmaßnahmen.



Tabletop Übungen – Umgang mit Gefahrensituationen

Zusammenfassung

Szenario-Dokumente
Dokumente, die das Szenario und die Hintergrundgeschichte beschreiben

Kommunikationsmittel
Erforderliche Kommunikationsmittel vor, die während der Übung verwendet werden sollen. (E-Mail-Vorlagen, Meldungen, …)

Checklisten und Vorlagen
Checklisten und Vorlagen, die den Teilnehmern bei der Durchführung bestimmter Aufgaben und Entscheidungen während der Übung helfen.

Zeitpläne und Ablaufpläne
Entwickeln Sie einen detaillierten Zeitplan, der den Ablauf der Übung festlegt.

Protokolle und Dokumentation
Sicherstellen, dass Sie die notwendigen Materialien für die Protokollierung und Dokumentation der Übung haben.

Präsentationsmittel
Falls erforderlich, bereiten Sie Präsentationsmittel wie Folien, Diagramme oder Visualisierungen vor.

Testumgebung In einigen Übungen kann eine Testumgebung erforderlich sein, um das Szenario zu simulieren.

Zugang zu Fachleuten und Ressourcen: Stellen Sie sicher, dass Sie Zugang zu Fachleuten oder Ressourcen haben, die während der Übung als Experten oder Ratschläge konsultiert werden können. Dies kann externe Sicherheitsberater oder interne Experten einschließen.

Bewertungs- und Verbesserungsmaterialien
Materialien, um die Ergebnisse der Übung zu bewerten und Verbesserungsempfehlungen zu dokumentieren.

Tabletop Übungen – Preview Planspiel

Basis Version des Planspiels verfügbar unter:

https://bwsyncandshare.kit.edu/s/sXdJPpwtafSJ3gc

Danke für Ihre Aufmerksamkeit.

Baden-Württemberg
Hochschulservicezentrum