Krisenstabsübungen

Know-how to go – Das Wissensfrühstück zum Thema Cyberkrisen

20.06.2022

Alina Trippe

Alina Trippe

Fachliche Schwerpunkte:

- Business Continuity Management
- Aufbau und Ausbildung von reaktiven Bewältigungsorganisationen
- Konzeptionierung, Steuerung und Auswertung von Notfall- und Krisenübungen
- Gastdozententätigkeit für Führungs- und Stabslehre an der Bundesakademie für Bevölkerungsschutz und Zivile Verteidigung

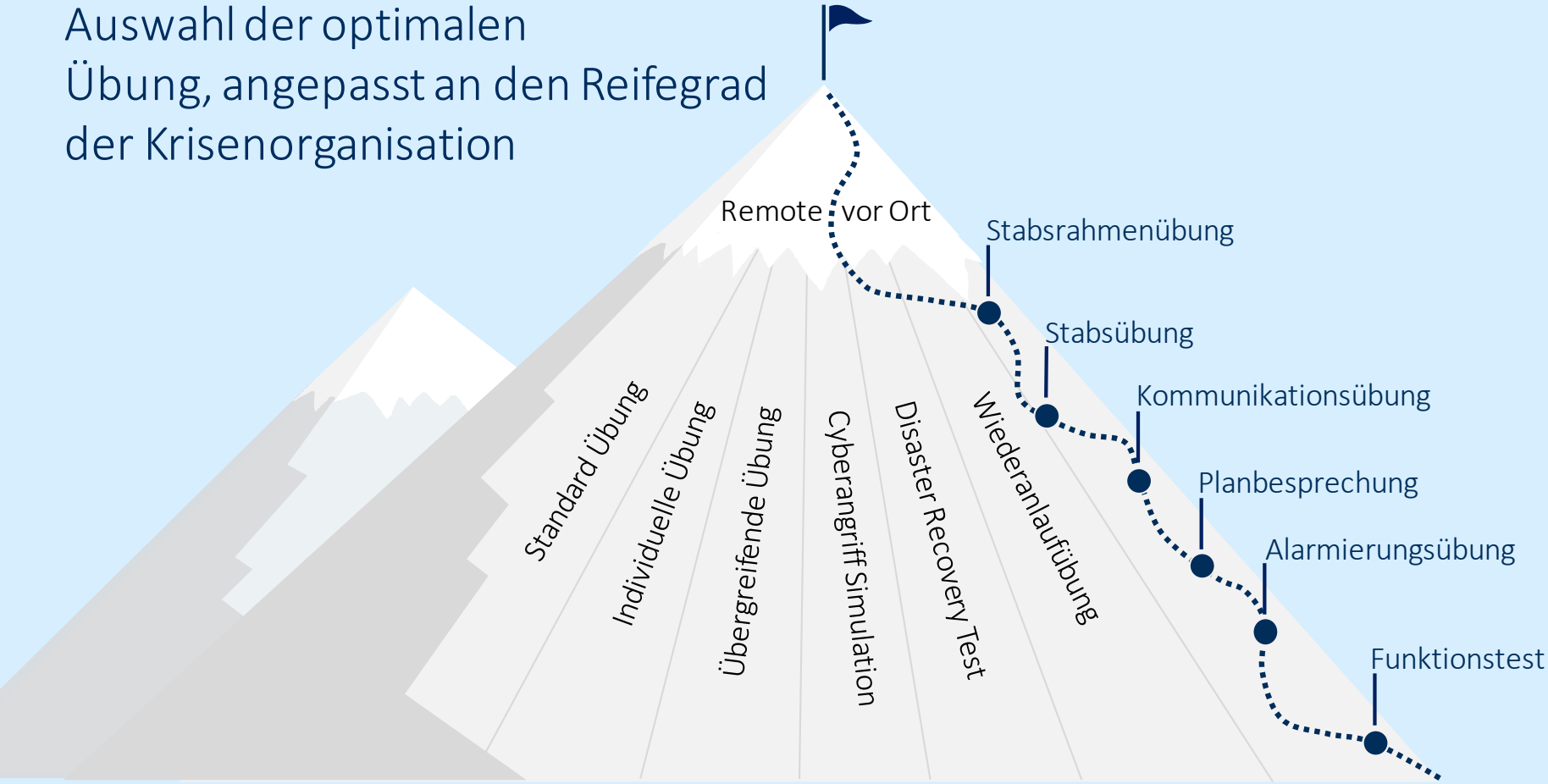
Agenda

Einblick in das Themenfeld

Ablauf einer Krisenstabsübung

Einblick in das Themenfeld

Auswahl der optimalen Übung, angepasst an den Reifegrad der Krisenorganisation



- Lagebild aufbauen
- Erste Meldung (intern & extern)
- Continuityprozesse anstoßen
- Abwägen von Datenschutzvorfällen
- …

Was macht eine erfolgreiche Krisenstabsübung aus?

Umfangreiche Vorbereitung
in enger Abstimmung mit Krisenorganisation

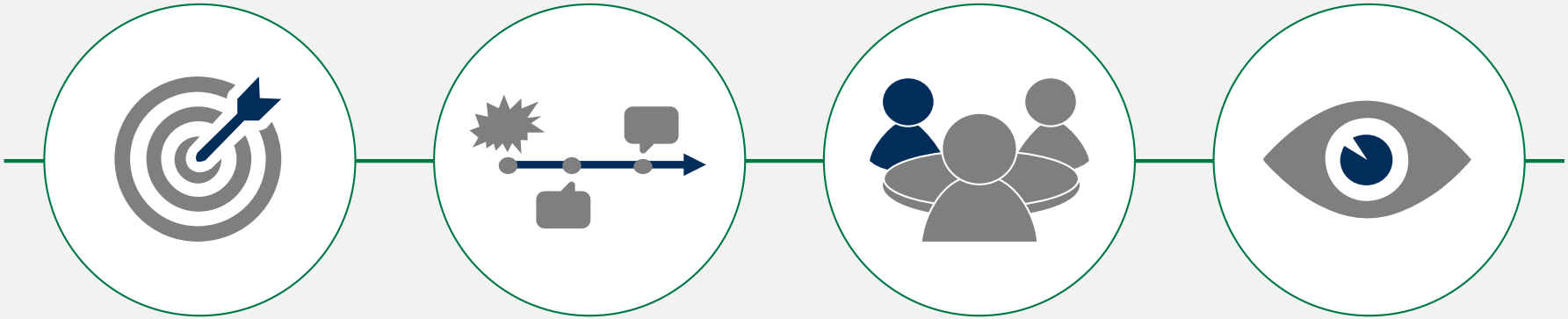
Einbezug aller Teilnehmenden
in allen Phasen des Krisenmanagements

Realistische Übungsszenarien
durch langjährige Übungs- und Einsatzerfahrung

Regelmäßige Übungen
als Teil des zyklischen Krisenmanagement

Ablauf einer Krisenstabsübung

Die vier Elemente einer Krisenstabsübung



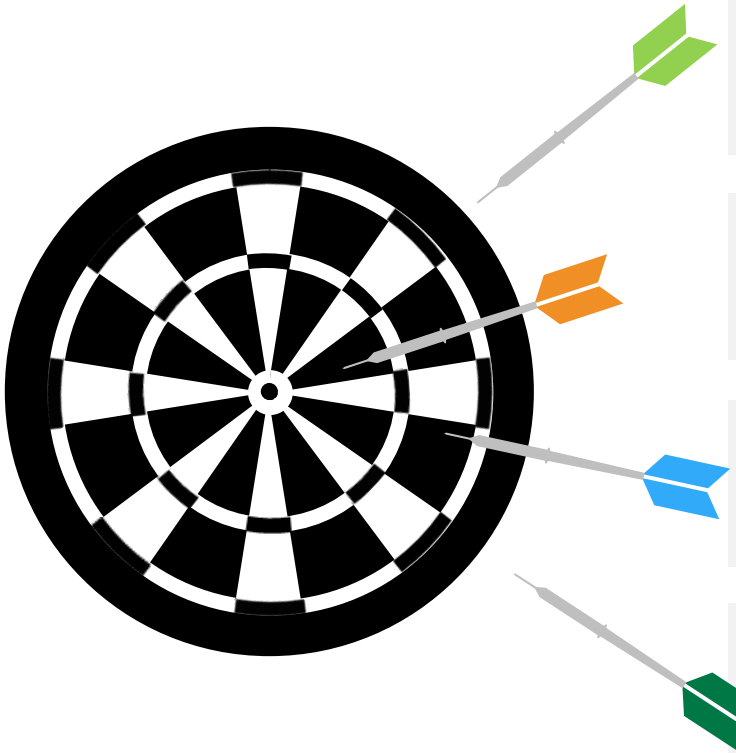
Rahmenbedingungen und Übungsziele

Entwicklung Übungsdrehbuch

Begleitete Übungsdurchführung

Übungsauswertung

Mögliche Übungsziele einer Krisenstabsübung



1. Sensibilisierung der Krisenstabsmitglieder für ihre jeweilige Rolle und der damit verbundenen Aufgaben unter realitätsnahen Bedingungen

2. Praktische Anwendung und Plausibilisierung der Notfalldokumentation

3. Überprüfung der Remote-Arbeitsmittel in Krisensituationen

4. Überprüfung der Kommunikationsfähigkeiten und -abläufe (intern/extern) in Krisensituationen

Erstellung eines Übungskonzeptes und eines Drehbuchs

Einschließlich mitwirkender Dokumentation

Blanko-Drehbuch „Bankotet Sofortabschaltung“

Handlungsstrang	Zeit	Auslöser / Einspielender	Art der Übermittlung	Empfänger	Ereignisbeschreibung	Hilfsspalte	E
Einleitung		Übungsleitung	PPTX	Krisenstab	Einleitung: Begrüßung + Vorstellung HiSo-Mitarbeiter/Übungsteam + Übungskünstlichkeiten + Regeln (keine externe Kommunikation/ Übung, Übung, Übung) + Außenwelt durch HiSolutions Fokus ist nicht die Lösung aller Probleme, sondern die Diskussion über Optionen und der Prozess der Stabsarbeit		
Ausgangslage		Übungsleitung	PPTX	Krisenstab	Ausgangslage: - Am <Tag ergänzen> stellte die IT des <Kunde ergänzen> aufgrund von vermehrten Meldungen von Mitarbeitern über Anomalien in E-Mail-Postfächern einen Sicherheitsvorfall fest. - Nach ersten Untersuchungen konnte festgestellt werden, dass sich die Malware "Fake-otet", eine abgewandelte Form des Emotet-Virus, im Netzwerk des <Kunde ergänzen> verbreitet hat. Wie es zu dem Befall kommen konnte, ist noch unklar. - Zur Untersuchung wurde in der IT ein Notfallteam gebildet. - Nachdem das Notfallteam die Nacht die Systeme untersucht hatte, konnte heute morgen <Zeit ergänzen> mit Sicherheit bestätigt werden, dass es sich um die Malware Fake-otet handelt. - Aufgrund der erhöhten Risikolage wurde die gesamte Exchange Infrastruktur abgeschaltet. - Daraufhin wurde der <Notfallbeauftragte> alarmiert, welcher nach kurzer Beratung den Krisenstab einberief	- Wer stellt das Ereignis fest? - Würde die IT eigenständig die Untersuchungen anstoßen oder gibt es einen externen Dienstleister? - Wer würde von der IT alarmiert werden? Wie findet die Eskalation statt? - Wer hat Admin-Rechte auf den PCs?	
1. Lagevortrag		zu ergänzen	PPTX	zu ergänzen	**Ausgangslage:** Wir haben heute Morgen gegen <Zeit ergänzen> einen Befall unseres Mailservers durch die Malware Fake-otet eine abgewandelte Form des Emotet-Virus, festgestellt. Der Befall begann wohl gestern gegen ca. <Zeit ergänzen>. Sehr wahrscheinlich ist, dass der Befall durch einen korrupten E-Mail Anhang, welcher die Malware enthielt, ins Netz kam. Bei Malware dieser Art beziehen sich die Mails mit den verseuchten Anhängen oft auf reale Geschäftsvorfälle, da die Malware Mailverläufe erkennen und verwenden kann. Zudem wird in vielen Fällen weitere Schadsoftware über eine Kommandoinfrastruktur nachgeladen. Unsere Mitarbeiter der IT bemerkten dies zunächst durch Meldungen von mehreren Anomalien in verschiedenen E-Mail Postfächern. Gestern Abend wurde daraufhin ein Notfallteam in der IT zur Untersuchung gegründet. Nachdem wir heute Nacht zusammen die Exchange-Infrastruktur untersucht haben, können wir seit heute morgen <Zeit ergänzen> mit Sicherheit bestätigen, dass es sich um Fake-otet handelt. Aufgrund des enormen Risikopotenzials entschied unsere IT die gesamte Exchange-Infrastrukur der Kunde ergänzen> abzuschalten. Damit wurde der Hauptverbreitungsweg von Fake-otet blockiert, so dass wir eine weitere Verbreitung verhindern und unsere Exchange-Infrastruktur schützen können. Dies hat jedoch zur Auswirkung, dass kein E-Mail Verkehr im gesamten <Kunde ergänzen> mehr möglich ist. Dies muss jedoch noch entsprechend im Haus kommuniziert werden. Zudem wissen wir inzwischen über welchen PC der Anhang geöffnet und die Malware aktiviert wurde. Wir konnten auch feststellen, dass dieser Rechner nach außen an die Fake-otet-Kommandoinfrastruktur kommuniziert hat. Ob Schadsoftware nachgeladen wurde wissen wir aktuell noch nicht. Zur Feststellung des Schadensausmaßes sollten neben den Servern auch die Clients gescannt werden. Die Ergebnisse des Scans liegen erst in den nächsten Stunden vor. **Entscheidung:** Da Fake-otet schon bei anderen <Unternehmensbranche ergänzen> aktiv war, wissen wir, dass Fake-otet eine "Zero Day" Schwachstelle in der Exchange-Infrastruktur dazu ausnutzt, höhere Rechte zu erhalten und diese Systeme zu infizieren. Entsprechend haben wir Ihnen als erste Maßnahme zwei Optionen zur Entscheidung vorbereitet: Option 1: Wir scannen erst und warten die Ergebnisse der Scans ab. Diese Option hätte das Risiko, dass sich währenddessen mögliche nachgeladene Schadsoftware verbreitet und eventuell unsere Systeme und Daten beschädigt oder abgreift. Wir hätten aber geringere Beeinträchtigung unseres Geschäftsbetriebes, da nur E-Mail nicht möglich ist. ob tatsächlich Schadsoftware nachgeladen wurde erung vermeiden. Unser Geschäftsbetrieb wäre	- Wer führt die Scan durch? Eigene IT oder externer Dienstleister? - Welche Auswirkungen wären bei Abschalten möglich? - Lässt sich die Exchange-Infrastruktur abkoppeln, ohne dass andere Systeme betroffen wären? - Kann der Scan remote durchgeführt werden? - Welche Auswirkungen hätte eine komplette Abschaltung der IT?	- Lagebesprech - Gegebene Info - Stakeholder A - Entscheidungs Entscheidung be unbedingt mit p - Kommunikation
Flurfunk		zu ergänzen	PPTX	zu ergänzen	h wundern sich, warum E-Mail nicht funktioniert. Über den Flurfunk verbreitet sich wohl, dass wir "gehackt" wurden. Die Mitarbeiter fragen, ob ihre eigenen Rechner in Gefahr sind. Außerdem fragen sie, wie sie sich nun verhalten sollen. Können Sie mir dazu eine Sprachregelung geben?	- Welche Auswirkungen hat die Abschaltung der Exchange-Infrastruktur	- Mitarbeiterkom Sprachregelung
merkwürdige Mails		zu ergänzen	PPTX	zu ergänzen	Einige unserer Kunden <ggf. Name ergänzen> haben sich heute morgen gemeldet und berichten von merkwürdigen E-Mails in unserem Namen. Was darf ich denen sagen?		- Sprachregelun
Datenschutzvorfall		zu ergänzen	PPTX	zu ergänzen	Wir können nun bestätigen, dass geschäftliche E-Mails <Thema ergänzen> abgeflossen sind, bevor wir die Exchange-Infrastruktur abschalten konnten. Damit liegt ein Datenschutzvorfall vor. Wir empfehle Ihnen daher eine Datenschutzmeldung innerhalb der Meldefrist abzusetzen. Wir halten Sie auf dem Laufenden.	- In welchen Themen werden per Mail personenbezogene Daten versendet?	- Datenschutzme - Information an

Durchführung der Krisenstabsübung

Auf Grundlage des entwickelten Szenarios

Unter Begleitung der Übungsleitung

Übung

Start der Übung

Einspieler für Beispiel Cyberangriff

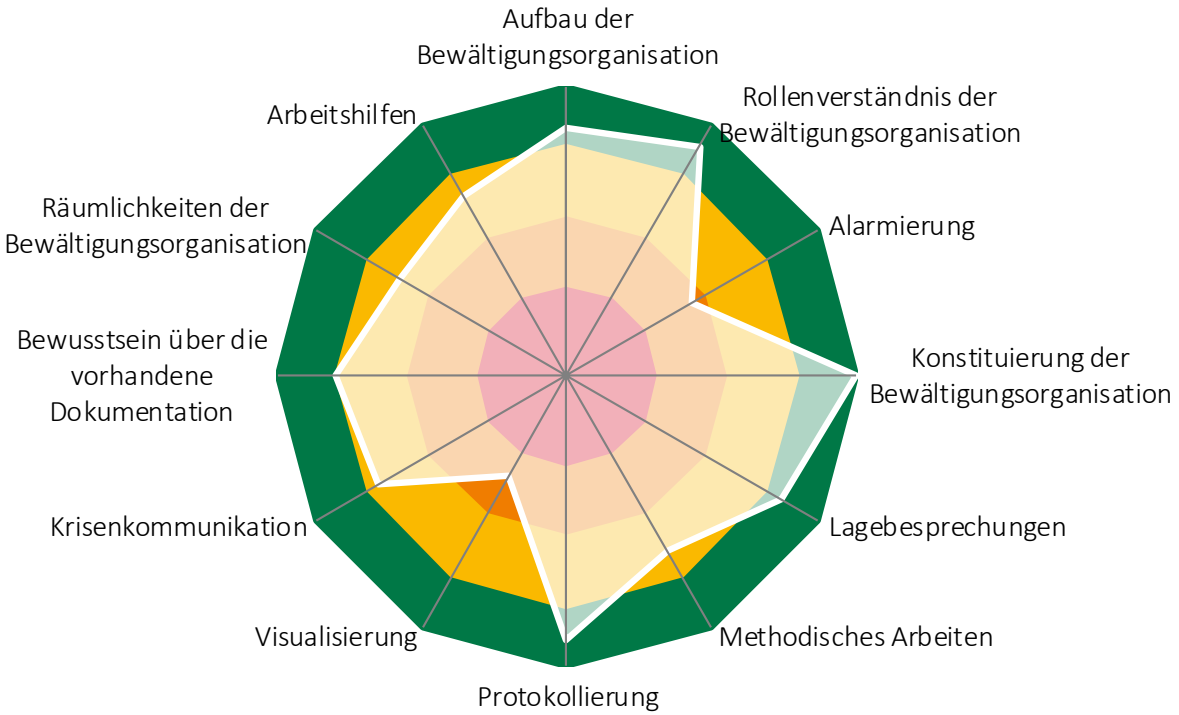
Übung

Ende der Übungszeit

Nachbesprechung der Übung

Auswertung durch Übungsbeobachtung

Grafische Darstellung der Übungsauswertung



Der letzte Schritt der Übung …

… sollte gleichzeitig der Beginn der Planung der nächsten Schritte des Krisenmanagements sein

Haben Sie Fragen?

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com