IT-SECURITY WORK

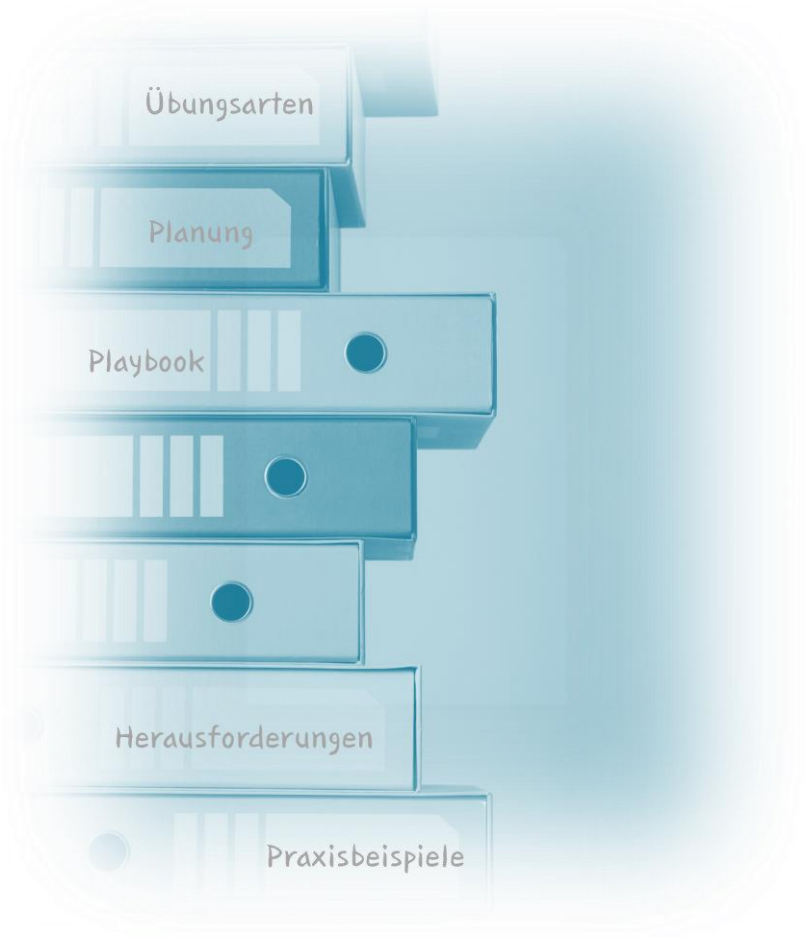
Praxis in Notfallübungen

Planung und Durchführung und wie man sie bewältigt - Praxisbeispiele

– vertraulich –

Agenda

- Kurzvorstellung Referent / ISW
- Übungsarten
- Planung der Notfallübung – Festlegung Übungsparameter
- Erstellung eines Playbooks
- Herausforderungen
- Praxisbeispiel: Versicherung Security Incident
- Praxisbeispiel: Krisenstabsübung DAX-Unternehmen
- Praxisbeispiel: Training der koordinierenden Stelle



Ihr Referent

Dirk Rauschenbach

Geschäftsführer und Informationssicherheitsberater

Mobil: +49 175 1836161

dirk.rauschenbach@isw-online.de

Über die IT-Security@Work GmbH (ISW)

Die IT-Security@Work GmbH (ISW) ist ein Beratungsunternehmen spezialisiert auf die Umsetzung aller Aspekte und Anforderungen der IT-Security in Verbindung mit Business- und Betriebsprozessen.

Wir unterstützen unsere Kunden dabei, aktuelle Entwicklungen und Trends, Aspekte der Informationssicherheit, IT-Risikomanagement, Compliance und des Datenschutzes mit ihrem Business in Einklang zu bringen.

Insbesondere kümmern wir uns darum, Business- und Betriebsprozesse so zu kombinieren, dass ein Optimum im Spannungsfeld Business, Betrieb (Work) und IT-/ Informationssicherheit erreicht wird.

Gemäß unserem Slogan: „**Mit Sicherheit ein Blick fürs Ganze**“ legen wir hierbei großen Wert auf nachhaltige und systemische IT-Beratung, mit Blick auf alle Umstände beim Kunden.

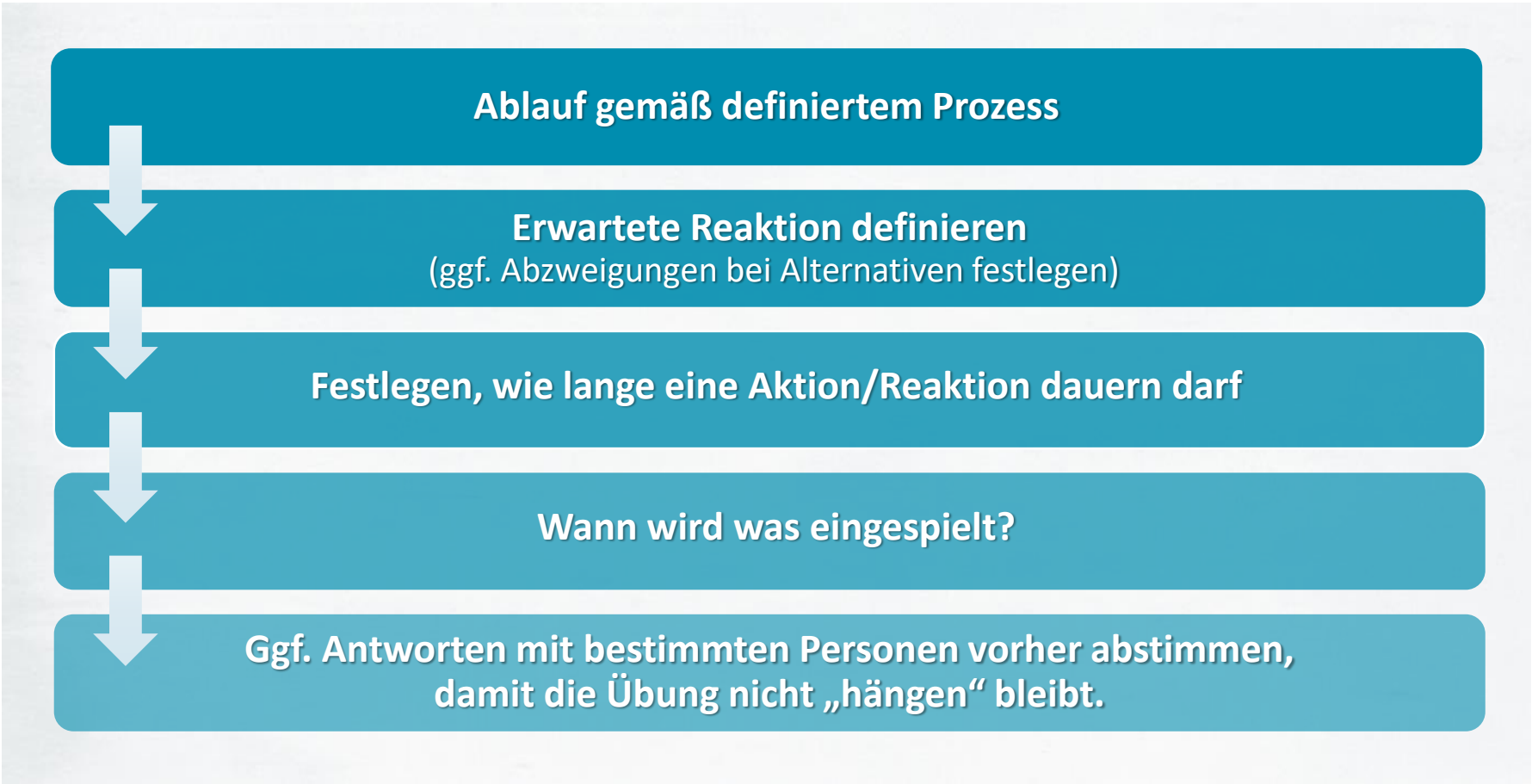
Übungsarten

- Feuer-/Brandschutzübung
- Alarmierungsübung
- Tabletop Test
- Disaster Recovery (DR) Test
- Failover Test
- Backup Restore Test

Festlegung der Übungsparameter

- **Scope**
  - Wer ist beteiligt? Krisenstab, IT, weiteres Management, Produktverantwortliche, Externe.
  - **Optionen für Ankündigung:** informiert / nicht informiert / nicht beteiligt (werden simuliert) / beteiligt, aber vorgefertigte Reaktion.
  - kann sich für verschiedene Beteiligte anders verhalten
  - Dauer (ggf. auch über einen Schichtwechsel)
- **Was ist der Auslöser?**
- **Definieren der Ziele: Was soll geübt werden?**
  - Alarmketten?
  - Prozessablauf
  - Reaktion / Anbindung von Externen
  - Toolunterstützung
  - Automatismen
- **Simulation vs. Echter Ausfall/Störung**

Erstellung eines Playbooks



Herausforderungen

- Unerwartete Reaktionen für zum Stopp der Übung.
- Auswirkungen der Übungen führen zu Störungen in der Produktion oder zu unerwarteten Meldungen.
  - Ausfall eines Systems
  - Meldung an Polizei, BSI, DSB
  - Mehrkosten bei externen Providern
- Personen, die nicht informiert werden sollten, haben Kenntnis und verfälschen das Übungsergebnis.

© JRCasas – stock.adobe.com

Praxisbeispiel:
Versicherung Security Incident

- **Ziel: Prüfung des Security Incident Prozesses**
  - **Teil 1:** Verlustmeldung von Handy und Laptop.
  - **Teil 2:** Einspielen einer Störung über das Ticketsystem an einem kritischen Produktionssystem, welches in der Analyse zu einem Security Incident wird.
- **Scope**
  - intern in der IT
  - Interne Funktionen wie ISB, DSM und Produktverantwortlicher sowie externe Partner wurden simuliert.
- **Herausforderungen**
  - **Teil 1:** Die Sperrung und Remote Löschung der Geräte wird nicht aktiv durchgeführt.
  - **Teil 2:** Unerwünschte „echte“ Einbindung von Internen und externen Partnern bei realistischen simulierten Rückmeldungen.

- Hoher Wert für die an der Übung beteiligten Personen.
- Einige Reaktionen nicht wie erwartet, aber handhabbar.
- Die definierten Prozessabläufe müssen nochmal nachgeschult werden.

Beispiel eines Playbooks: Verlustmeldung Laptop

Referenz auf Dokumentation

	Szenario 2: Verlust eines Gerätes / Loss of Device Übungsziel: Die korrekten Eskalationswege werden eingehalten und die korrekten Gremien werden informiert. Der Fehler wird behoben und es erfolgt eine saubere Nachbereitung							**Testdurchführender:** **Test Date:**
Schritt	**Run-book**	**geplante Uhrzeit**	**Maximale Dauer**	**Beschreibung**	**Meldung von / Aktivität durch**	**Meldung an / Benachrichtigung an**	**Ticketinhalt/Meldungshinhalt**	**Erwartetes Ergebnis**
1		10:30		**Anruf,** dass ein Gerät (Latop/Handy) verloren gegangen ist.	Übungsleiter	IT-Service Center	Von Manager 1 wurde der Laptop verloren. Anweisung, dass keine Änderungen durchgeführt werden und der Übungsleiter alle Ansprechpartner simuliert. Das Ticket wird mit dem Hinweis."Übung/Test" in der Beschreibung angelegt.	Protokollierung des Vorfalls im Ticketsystem
2	2.1			Analyse des Vorfalls	IT-Service Center			Ermittlung des konkreten Gerätes, Feststellung der potentiell betroffenen Daten. Es sind keine Personenbezogenen Daten betroffen.
2a	2.2			Meldung an verantwortliche Stelle	IT-Service Center	Datenschutzbeauftragter -> Simuliert durch Übungsleiter	Meldung des Vorfalls mit Informationen aus der Analyse oder Vorbereiten der Information und senden an Übungsleiter.	
2b	2.2a			~~Analyse und Meldung an Behörde~~	~~Datenschutzbeauftragter~~	~~IT-Service Center~~	~~Keine Meldung erforderlich~~	~~Keine Meldung erforderlich~~
3	3.1			Deaktivierung aller Accounts bezüglich des Gerätes	IT-Service Center			Ermittlung aller Accounts erfolgt und dokumentiert, eine Deaktivierung findet nicht statt. Die Dokumentation geht an den Übungsleiter. Es müssen keine Accounts deaktiviert werden.
4	3.2			Deaktivierung des Gerätes in der AD	IT-Service Center			Ermittlung des Gerätes in der AD erfolgt und dokumentiert, eine deaktivierung findet nicht statt. Es ist das Gerät mit der ID XXXXX
5	3.3			Löschung aller Infrastrukturelevanter Daten	IT-Service Center			Ermittlung alles infrastrukturrelevanten Systeme erfolgt und dokumentiert, eine deaktivierung findet nicht statt. Die Dokumentation geht an den Übungsleiter. Die MacAdresse wird ermittelt und am VPN-Konzentrator gelöscht.
6	3.4			Information der verantwortlichen Stellen	IT-Service Center	local ISO, Vorgesetzter beide -> Simuliert durch Übungsleiter	Verlustmeldung und ergriffene Maßnahmen	Ermittlung der relevanten Stellen erfolgt und Kontaktdaten ermittelt, eine Information findet nicht statt. Die Dokumentation geht an den Übungsleiter. Hier sind das Steiner (local ISO) und Peters
7	4.1			Bereitstellung des neuen Gerätes	IT-Service Center			Neues Gerät wird ermittelt, aber nicht bereit gestellt. Es wird dokumentiert, welches Gerät zugeordnet würde. Die Dokumentation geht an den Übungsleiter. Es wird ein freies Gerät aus dem Pool ermittelt.
8	4.2			Schließen des Tickets	IT-Service Center			Ticket wird in OTRS geschlossen.
9				Nachbesprechung				Fehlt im Runbook, ist aber Notwendig.
10		##########		Übungsende und				
							Ende Szenario 2	

Einplanung Nachbesprechung

Übungsleiter sitzt im IT-Service Center

Beispiel eines Playbooks: Störung kritisches Produktionssystem

Einbindung möglich durch bekannte Schwachstelle

Szenario 1: Ddos Angriff im Internet Verfügbaren Dienst Übungsziel: Die korrekten Eskalationswege werden eingehalten und die korrekten Gremien werden informiert. **Der Fehler wird behoben und es erfolgt eine saubere Nachbereitung**								Testdurchführender: Test Date:
Schritt	Run-book	Geplante Uhrzeit	Maximale Dauer	Beschreibung	Meldung von / Aktivität durch	Meldung an / Benachrichtigung an	Ticketinhalt/Meldungshinhalt	Erwartetes Ergebnis
1		14:30		Meldung des Sicherheitsvorfalls	Übungsleiter	IT-Service Center	Im Namen von XXX (Gruppenleiter Kundendienst) erfolgt die Meldung, das Fehler im Vermittlungsservice aufgetreten ist. Die Vermittler beschweren sich, das der Dienst sehr schwer erreichbar ist. Anweisung, dass keine Änderungen durchgeführt werden und der Übungsleiter alle Ansprechpartner ausser Rene und den IT-SO simuliert. Das Ticket wird mit dem Hinweis:"Übung/Test" in der Beschreibung	Entgegennahme des Ereignisses und Bestätigung der Meldung.
4	4.9			Follow the relevant subprocess if applicable	IT-Service Center			Der Richtige Subprozess wird ausgewählt: Intrusion, Dokumentation im Ticket
4a	I1			Intrusion: Collect and Review Vulnerability Information	IT-Service Center			Alle Informationen bezüglich der Schwachstelle werden aus dem TVM Tool (Qualys) ermittelt. Hierbei wird ermittelt, ob das System für die Schwachstelle anfällig ist.
4b	I2			Intrusion: Collect and Review Vulnerability Information	IT-Service Center	Security Provider		Security Provider wird kontaktiert um zusätzliche Informationen zu der Schwachstelle und Angreifbarkeit vorhanden sind.
4c				Bereitstellung Information über Schachstelle und Relevanz	Security Provider	IT-Service Center	Bereitstellung der Information über die Schwachstelle. Es wird die Schwachstelle XXX verwendet.	Dokumentation der Information im Ticket.
5	4.10			Notify IRT Chair	Informationssicherheit (e.g. German ISO)	IRT Chair	Information über Störung mit Kritikaltität und betroffenen Systemen und die bisher durchgeführten Analysen	IT-Service Desk informiert Manager A, er übernimmt dann die Rolle des IRT Chairs. IRT Chair wird mit allen Details, der Chair überprüft, ob das IRT informiert werden muss, dies ist nicht der Fall. Dies wird nicht durch den Übungsleiter simuliert.
	5.x			Containment				
6	5.1			Establish Timeline of Events	IT-Service Center & IRT Chair			Dokumentation des zeitlichen Ablaufs der Ereignisse. Es erfolgt im Zuge der Übung zu diesem Punkt keine Einbindung des ISAS.
7	5.2			Identify Resolver Group	IRT Chair			Die Gruppe verantwortlich für die Sofortmaßnahme wird identifiziert und im Ticket dokumentiert. In diesem Fall ist dies Infrastruktur-Teamumgebung Administrator A, sowie Security Provider, Ggf. Security Provider. Diese werden alle simuliert.
7a	5.2			Information of Resolver Group	IRT Chair	Resolver Group -> Simuliert durch Übungsleiter		Die Resolver Group wird informiert und mit eingebunden.
8	5.3			Review Gathered Information from Identification Phase	IRT Chair/Resolver Group			Sichtung aller Informationen und Finale festlegung der entsprechenden Sofoftmaßnahme. Diese sollte die Trennung des Systems vom Internet bzw. Trennung der Netzverbindungen sein.
9	5.4			Establish Available Response Strategies and Workarounds	Resolver Group -> Simuliert durch Übungsleiter			Die Maßnahme und das weitere Vorgehen werden besprochen und dokumentiert. Die Maßnahme hierbei ist das stoppen der VM.
9a	5.5			Notify IRT Chair	Resolver Group -> Simuliert durch Übungsleiter			Die Finale Dokumentation der Sofortmaßnahmen wird dem IRT Chair zur Freigabe vorgelegt.
10	5.6			Establish Timeline for Change	Resolver Group -> Simuliert durch Übungsleiter			Festlegung das es ein Emergency Change ist und Stellung des Emergency Changes. Wird durch Service Desk oder Übungsleiter

simulierte Meldungen

Auswahl einer bekannten Schwachstelle

Praxisbeispiel: Krisenstabsübung DAX-Unternehmen

- **Ziel: Krisenstabsübung**
  - IT-Ausfall sorgt für Störung der Produktionsprozesse mit direkten Auswirkungen auf Kunden und Partner, öffentlichkeitswirksam
- **Scope**
  - Krisenstab
  - Interne Funktionen wie ISB, DSM, IT sowie externe Partner wurden informiert und haben vordefinierte Antworten eingespielt.
  - 2 Tage Übungsdauer mit Schichtwechsel
- **Herausforderungen**
  - Starke Bindung des Krisenstabs (Top-Management) für die Übungsdauer.
  - hoher Definitionsaufwand
  - realistisches Einspielen von Rückmeldungen und externen Ereignissen (Pressemitteilungen usw.)

FAZIT

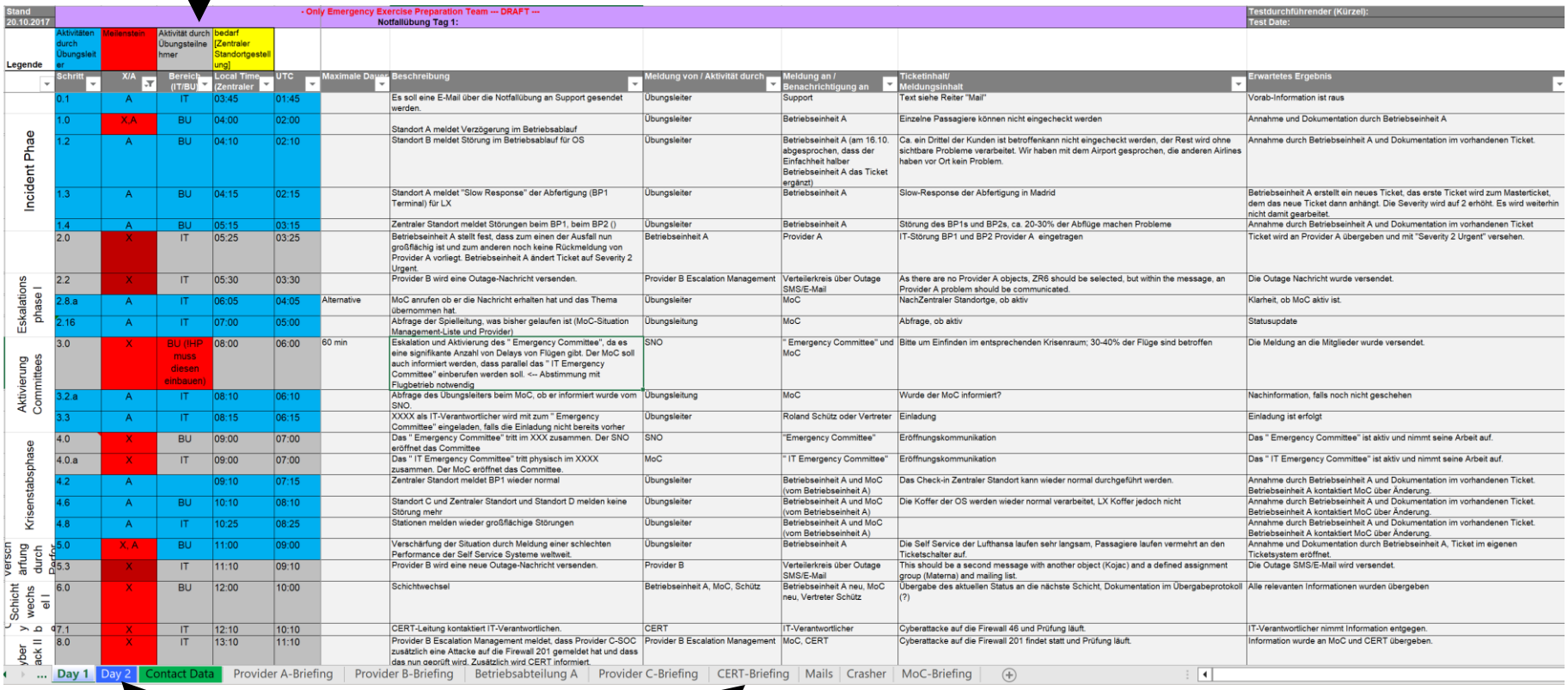
- Hoher Wert für die an der Übung beteiligten Personen.
- Kunde hat viel Erfahrung bei der Handhabung von Krisen.

Krisenstabsübung DAX-Unternehmen
– Details –

- **Emergency Committee**
  - Jede Rolle im Top-Management wurde während der Übungsdauer besetzt und hatte sich im Krisenstabsraum einzufinden.
  - Das IT Emergency Committee wurde ebenfalls physisch einberufen.
- **Dauer: 1,5 Tage**
  - Als Teil der Übung war für die Rollen in den Emergency Committees ein Schichtwechsel eingeplant und durchgeführt.
  - Übung wurde geplant um 17 Uhr nach Schichtwechsel angehalten. Am zweiten Tag wurde der Fahrplan fortgesetzt.
- **Briefing**
  - Externe Dienstleister wurden vorab informiert, um das Risiko negativer Auswirkungen zu minimieren.
  - Meldungen von Presse, IT und Standorten wurden nach einem vorbereiteten Zeitplan eingespielt.
- **Aufwendige Definition**
  - Der Fahrplan hatte für den ersten Tag 65 Schritte und für den zweiten Tag 17 Schritte.

Beispiel eines Playbooks: Störung kritisches Produktionssystem

Für den ersten Tag: 65 Teilschritte (Auszug einiger Meilensteine)



Stand 20.10.2017 — · Only Emergency Exercise Preparation Team --- DRAFT ---
Notfallübung Tag 1:
Testdurchführender (Kürzel):
Test Date:

Legende: Aktivitäten durch Übungsleiter | Meilenstein | Aktivität durch Übungsteilnehmer | bedarf [Zentraler Standortgestellung]

	Schritt	X/A	Bereich (IT/BU)	Local Time (Zentraler	UTC	Maximale Dauer	Beschreibung	Meldung von / Aktivität durch	Meldung an / Benachrichtigung an	Ticketinhalt/ Meldungsinhalt	Erwartetes Ergebnis
Incident Phase	0.1	A	IT	03:45	01:45		Es soll eine E-Mail über die Notfallübung an Support gesendet werden.	Übungsleiter	Support	Text siehe Reiter "Mail"	Vorab-Information ist raus
	1.0	X,A	BU	04:00	02:00		Standort A meldet Verzögerung im Betriebsablauf	Übungsleiter	Betriebseinheit A	Einzelne Passagiere können nicht eingecheckt werden	Annahme und Dokumentation durch Betriebseinheit A
	1.2	A	BU	04:10	02:10		Standort B meldet Störung im Betriebsablauf für OS	Übungsleiter	Betriebseinheit A (am 16.10. abgesprochen, dass der Einfachheit halber Betriebseinheit A das Ticket ergänzt)	Ca. ein Drittel der Kunden ist betroffenkann nicht eingecheckt werden, der Rest wird ohne sichtbare Probleme verarbeitet. Wir haben mit dem Airport gesprochen, die anderen Airlines haben vor Ort kein Problem.	Annahme durch Betriebseinheit A und Dokumentation im vorhandenen Ticket.
	1.3	A	BU	04:15	02:15		Standort A meldet "Slow Response" der Abfertigung (BP1 Terminal) für LX	Übungsleiter	Betriebseinheit A	Slow-Response der Abfertigung in Madrid	Betriebseinheit A erstellt ein neues Ticket, das erste Ticket wird zum Masterticket, dem das neue Ticket dann anhängt. Die Severity wird auf 2 erhöht. Es wird weiterhin nicht damit gearbeitet.
	1.4	A	BU	05:15	03:15		Zentraler Standort meldet Störungen beim BP1, beim BP2 ()	Übungsleiter	Betriebseinheit A	Störung des BP1s und BP2s, ca. 20-30% der Abflüge machen Probleme	Annahme durch Betriebseinheit A und Dokumentation im vorhandenen Ticket
Eskalations phase I	2.0	X	IT	05:25	03:25		Betriebseinheit A stellt fest, dass zum einen der Ausfall nun großflächig ist und zum anderen noch keine Rückmeldung von Provider A vorliegt. Betriebseinheit A ändert Ticket auf Severity 2 Urgent.	Betriebseinheit A	Provider A	IT-Störung BP1 und BP2 Provider A eingetragen	Ticket wird an Provider A übergeben und mit "Severity 2 Urgent" versehen.
	2.2	X	IT	05:30	03:30		Provider B wird eine Outage-Nachricht versenden.	Provider B Escalation Management	Verteilerkreis über Outage SMS/E-Mail	As there are no Provider A objects, ZR6 should be selected, but within the message, an Provider A problem should be communicated.	Die Outage Nachricht wurde versendet.
	2.8.a	A	IT	06:05	04:05	Alternative	MoC anrufen ob er die Nachricht erhalten hat und das Thema übernommen hat.	Übungsleiter	MoC	NachZentraler Standortge, ob aktiv	Klarheit, ob MoC aktiv ist.
	2.16	A	IT	07:00	05:00		Abfrage der Spielleitung, was bisher gelaufen ist (MoC-Situation Management-Liste und Provider)	Übungsleitung	MoC	Abfrage, ob aktiv	Statusupdate
Aktivierung Committees	3.0	X	BU (IHP muss diesen einbauen)	08:00	06:00	60 min	Eskalation und Aktivierung des " Emergency Committee", da es eine signifikante Anzahl von Delays von Flügen gibt. Der MoC soll auch informiert werden, dass parallel das " IT Emergency Committee" einberufen werden soll. <-- Abstimmung mit Flugbetrieb notwendig	SNO	" Emergency Committee" und MoC	Bitte um Einfinden im entsprechenden Krisenraum; 30-40% der Flüge sind betroffen	Die Meldung an die Mitglieder wurde versendet.
	3.2.a	A	IT	08:10	06:10		Abfrage des Übungsleiters beim MoC, ob er informiert wurde vom SNO.	Übungsleitung	MoC	Wurde der MoC informiert?	Nachinformation, falls noch nicht geschehen
	3.3	A	IT	08:15	06:15		XXXX als IT-Verantwortlicher wird mit zum " Emergency Committee" eingeladen, falls die Einladung nicht bereits vorher	Übungsleiter	Roland Schütz oder Vertreter	Einladung	Einladung ist erfolgt
Krisenstabsphase	4.0	X	BU	09:00	07:00		Das " Emergency Committee" tritt im XXX zusammen. Der SNO eröffnet das Committee	SNO	"Emergency Committee"	Eröffnungskommunikation	Das " Emergency Committee" ist aktiv und nimmt seine Arbeit auf.
	4.0.a	X	IT	09:00	07:00		Das " IT Emergency Committee" tritt physisch im XXXX zusammen. Der MoC eröffnet das Committee.	MoC	" IT Emergency Committee"	Eröffnungskommunikation	Das " IT Emergency Committee" ist aktiv und nimmt seine Arbeit auf.
	4.2	A		09:10	07:15		Zentraler Standort meldet BP1 wieder normal	Übungsleiter	Betriebseinheit A und MoC (vom Betriebseinheit A)	Das Check-in Zentraler Standort kann wieder normal durchgeführt werden.	Annahme durch Betriebseinheit A und Dokumentation im vorhandenen Ticket. Betriebseinheit A kontaktiert MoC über Änderung.
	4.6	A	BU	10:10	08:10		Standort C und Zentraler Standort und Standort D melden keine Störung mehr	Übungsleiter	Betriebseinheit A und MoC (vom Betriebseinheit A)	Die Koffer der OS werden wieder normal verarbeitet, LX Koffer jedoch nicht	Annahme durch Betriebseinheit A und Dokumentation im vorhandenen Ticket. Betriebseinheit A kontaktiert MoC über Änderung.
	4.8	A	IT	10:25	08:25		Stationen melden wieder großflächige Störungen	Übungsleiter	Betriebseinheit A und MoC (vom Betriebseinheit A)		Annahme durch Betriebseinheit A und Dokumentation im vorhandenen Ticket. Betriebseinheit A kontaktiert MoC über Änderung.
Verschärfung durch Performance	5.0	X, A	BU	11:00	09:00		Verschärfung der Situation durch Meldung einer schlechten Performance der Self Service Systeme weltweit.	Übungsleiter	Betriebseinheit A	Die Self Service der Lufthansa laufen sehr langsam, Passagiere laufen vermehrt an den Ticketschalter auf.	Annahme und Dokumentation durch Betriebseinheit A, Ticket im eigenen Ticketsystem eröffnet.
	5.3	X	IT	11:10	09:10		Provider B wird eine neue Outage-Nachricht versenden.	Provider B	Verteilerkreis über Outage SMS/E-Mail	This should be a second message with another object (Kojac) and a defined assignment group (Materna) and mailing list.	Die Outage SMS/E-Mail wird versendet.
Schichtwechsel I	6.0	X	BU	12:00	10:00		Schichtwechsel	Betriebseinheit A, MoC, Schütz	Betriebseinheit A neu, MoC neu, Vertreter Schütz	Übergabe des aktuellen Status an die nächste Schicht, Dokumentation im Übergabeprotokoll (?)	Alle relevanten Informationen wurden übergeben
Cyber Attack II	7.1	X	IT	12:10	10:10		CERT-Leitung kontaktiert IT-Verantwortlichen.	CERT	IT-Verantwortlicher	Cyberattacke auf die Firewall 46 und Prüfung läuft.	IT-Verantwortlicher nimmt Information entgegen.
	8.0	X	IT	13:10	11:10		Provider B Escalation Management meldet, dass Provider C-SOC zusätzlich eine Attacke auf die Firewall 201 gemeldet hat und dass das nun geprüft wird. Zusätzlich wird CERT informiert.	Provider B Escalation Management	MoC, CERT	Cyberattacke auf die Firewall 201 findet statt und Prüfung läuft.	Information wurde an MoC und CERT übergeben.

Day 1 | Day 2 | Contact Data | Provider A-Briefing | Provider B-Briefing | Betriebsabteilung A | Provider C-Briefing | CERT-Briefing | Mails | Crasher | MoC-Briefing

über 1,5 Tage

Briefing der Provider

Praxisbeispiel:
Training der koordinierenden Stelle

- **Ziel: Übung der Verantwortlichkeit der koordinierenden Rolle**
  - Einspielen von mehreren Vorfällen als Meldung bei der koordinierenden Rolle.
- **Scope**
  - Funktion der koordinierenden Stelle
  - Tabletop Test live vor Ort mit allen Personen, die diese Stelle einnehmen können.
  - Meldung an ein Lagezentrum (vorab informiert).
- **Herausforderungen**
  - realistische Meldungen

- Diskussion hat den Beteiligten deutliche Klarheit für das Verhalten gegeben.
- Sicherheit im Umgang mit dem Lagezentrum gewonnen.

Training der koordinierenden Stelle
– Details –

- **Verantwortliche der koordinierenden Stelle**
  - Alle Personen, die die Rolle der koordinierenden Stelle einnehmen können, waren anwesend.
  - Der Mitarbeiter mit Rufbereitschaft für die koordinierende Stelle hat ebenfalls teilgenommen.
- **Übungsinhalte**
  - Im ersten Schritt wurden Szenarien durchgesprochen.
  - Szenarien wurden aus den vorab dokumentierten Worst-Case-Szenarien entnommen, wie z. B. Ausfall eines RZ oder Virenbefall zentraler Systeme.
  - Im zweiten Schritt wurde eine Meldung (Personenschaden im RZ) von außen eingespielt, die Reaktion besprochen und die Kommunikation mit der zentralen Lagestelle durchgeführt.
- **Briefing**
  - Die zentrale Lagestelle war vorab über die Übung informiert.

Urheberrechtshinweis

Urheberrecht
Die Bilder und Inhalte dieser Präsentation unterliegen dem deutschen Urheberrecht. Beiträge von Dritten sind als solche gekennzeichnet. Die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung außerhalb der Grenzen des Urheberrechts bedürfen der schriftlichen Zustimmung der IT-Security@Work GmbH (ISW).

Bildnachweis
Agenda / pile of ring binders in the archive – © stokkete – stock.adobe.com (editiert)
Herausforderungen / businessman looks at his computer – © JRCasas – stock.adobe.com
Keyboard Illustration "Sicherheit – © mindscanner – stock.adobe.com
privacy icon on blue background – © Tex vector – stock.adobe.com
Metal Wheel Concept – © EtiAmmos – stock.adobe.com