Leitfaden
Krisenstabsübung Cyber-Attacke

controllit
Business Continuity Management

Inhalt

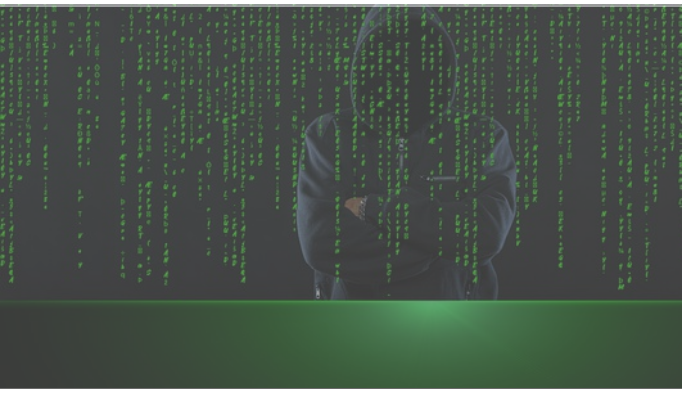
03
EINLEITUNG

04
PRÄVENTIVE MASSNAHMEN

06
REAKTIVE MASSNAHMEN

13
RÜCKKEHR IN DEN NORMALBETRIEB UND NACHBEREITUNG

EINLEITUNG



Schlagzeilen wie „Cyber Crime“, „2 Millionen Kundendaten abgeflossen“, „Hacker-Angriff legt Unternehmen für Wochen lahm“ lesen wir immer wieder in den Medien. Trotz aller risikomindernden Maßnahmen und betrieblicher Vorsorge gibt es dieses Szenario auch in Deutschland jedes Jahr mehrfach mit Schäden in Millionenhöhe.

Ist Ihr Unternehmen auf dieses Szenario vorbereitet?

In diesem Leitfaden zu einer Krisenstabsübung (KSÜ) Cyber-Attacke wollen wir die wesentlichen Themenfelder zur erfolgreichen Handhabung einer solchen Krise darstellen.
Dabei achten wir insbesondere auf die klassischen Ziele des Krisenmanagements:

- **Schutz von Menschenleben**/Unversehrtheit von Menschen und Umwelt
- **Schadensbegrenzung** Vermeidung/Minimierung von wirtschaftlichem Schaden, Vermeidung von Imageschäden, Absicherung der (zeit-)kritischen Geschäftsprozesse
- **Schutz des Normalbetriebs** nicht betroffener Betriebsteile

Ein weiterer Fokus liegt auf der effektiven und effizienten Zusammenarbeit der Mitglieder Ihres Krisenstabs (KS) auf der Basis der grundlegenden **Aufgaben eines Krisenstabs**:

- Identifikation und Analyse von Krisensituationen
- Festlegung einer Strategie zur Krisenbewältigung
- Entwicklung von Handlungsoptionen
- Bewertung der Erfolgsaussichten, Risiken und Chancen
- Priorisierung und Entscheidungsfindung
- Informieren über getroffene Maßnahmen
- Delegieren und Kontrolle von Maßnahmen
- Evaluation und Neubewertung

Präventive Maßnahmen

Krisenmanagement ist ein reaktiver Prozess. Selbstverständlich bereiten Sie Ihre Krisenmanagementorganisation aber auch mit präventiven Maßnahmen auf ihre Aufgaben vor.

Hier fassen wir die wesentlichen Maßnahmen mit Perspektive auf das Szenario „Cyber-Attacke“ zusammen:

Prüfen Sie, ob alle verantwortlich Mitwirkenden Ihrer Krisenorganisation handlungsfähig und einsatzbereit sind (z. B. durch regelmäßige Schulungen, Meeting-Struktur, regelmäßigen Informationsaustausch, Awareness-Maßnahmen):

- Krisenstabsmitglieder inklusive deren Stellvertreter
- Mitwirkende der taktischen Ebene (Abteilungsleiter etc.)
- Durchführende der operativen Ebene (Mitarbeiter in den Fachabteilungen)

Nutzen Sie Ihr Business-Continuity-Managementsystem (BCM), wenn implementiert:

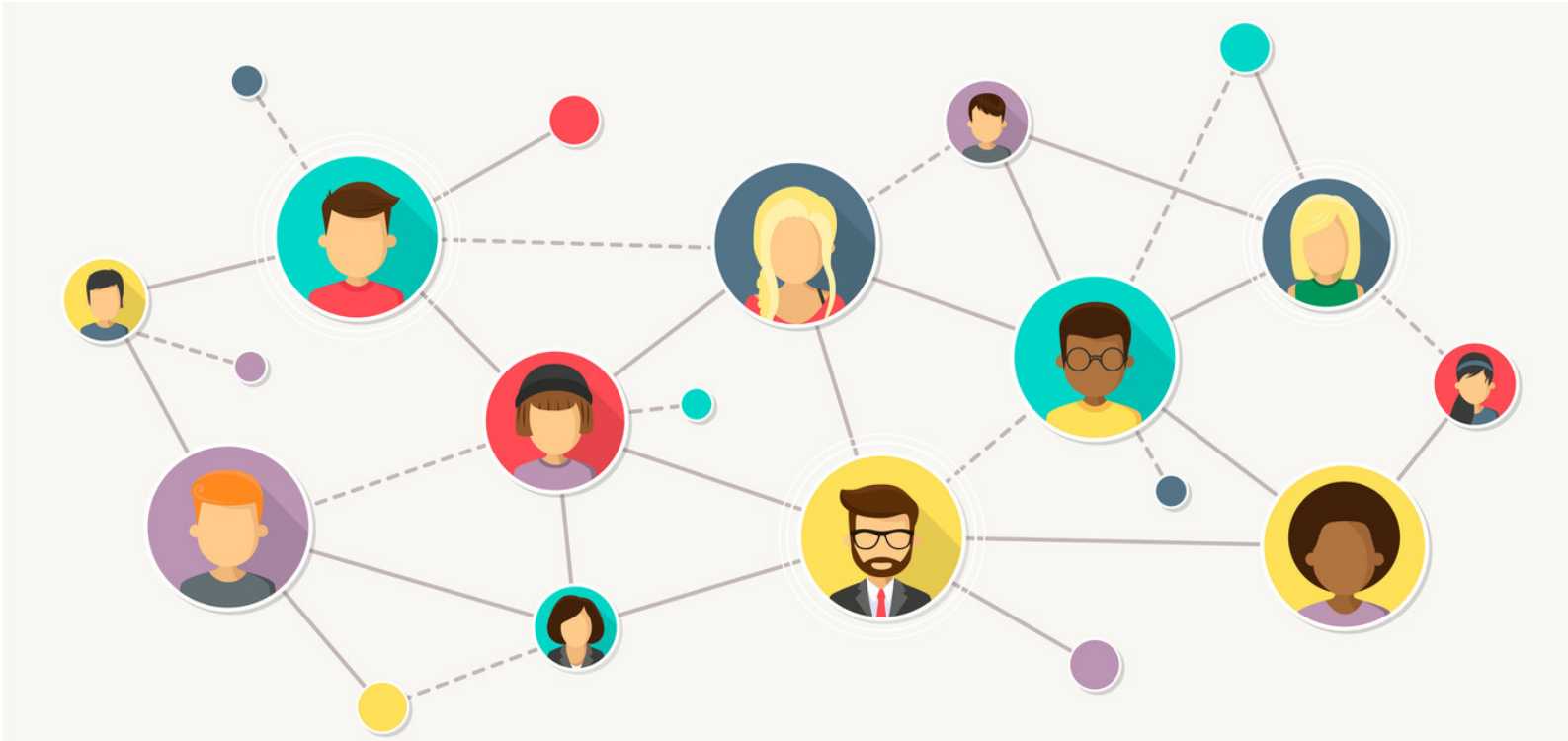
- Überprüfung der Aktualität und Wirksamkeit der Business-Continuity-Pläne für das Szenario IT-Ausfall:
  - → Sind die eingesetzten Lösungsoptionen beim IT-Ausfall in der Lage, einen Ausfall der Geschäftsprozesse temporär zu kompensieren (insbesondere auch bezüglich der implementierten Workarounds)?
  - → Sind Ihre Sicherungsmaßnahmen wie Hot- bis Cold-Standby etc. wirksam und anwendbar?
- Haben Sie kein BCMS implementiert, prüfen Sie Ihre Einsatzfähigkeit anhand der aufgeführten Themen

Nutzen Sie Ihr IT-Service-Continuity-Management-System (ITSCM) und Informationssicherheitsmanagementsystem (ISM), wenn implementiert:

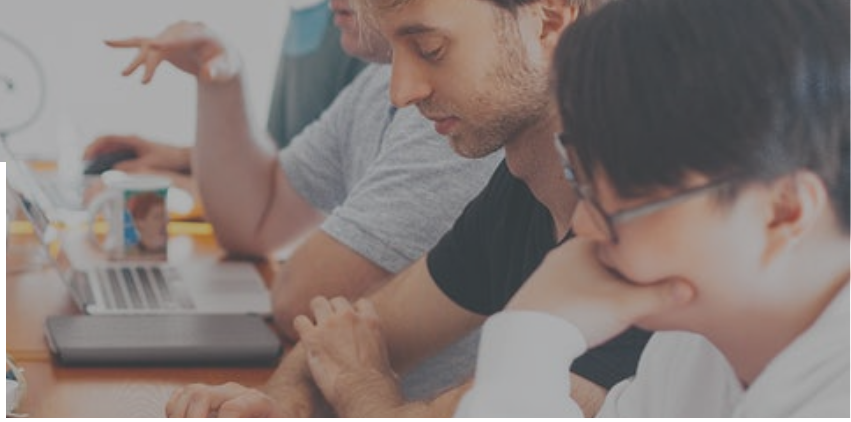
- Sind die eingesetzten Lösungsoptionen beim IT-Ausfall in der Lage, einen Ausfall der Geschäftsprozesse temporär zu kompensieren?
- Können Ihre IT-Zielwerte wie Recovery Time Objective (RTO) und Recovery Point Objective (RPO) eingehalten werden?
- Wird die Verfügbarkeit der IT-Services aus Sicht des ITSCM ausreichend gewährleistet?
- Ist die Ressource Recovery bezüglich eines Angriffs im ITSCM angemessen gewährleistet?
- Werden die Schutzziele des ISM angemessen abgesichert?
- Haben Sie kein ITSCM und/oder ISM implementiert, prüfen Sie Ihre Einsatzfähigkeit anhand der aufgeführten Themen

Präventive Maßnahmen

Nutzen Sie den Aufbau und die Pflege durch den Krisenverantwortlichen zu externen Schnittstellen (hier insbesondere Behörden wie Landeskriminalamt (LKA), BaFin, BSI etc.).



Schaffen Sie Verständnis und Bewusstsein sowie Verfahrenssicherheit für das Thema (Awareness-Maßnahmen).



Reaktive Maßnahmen

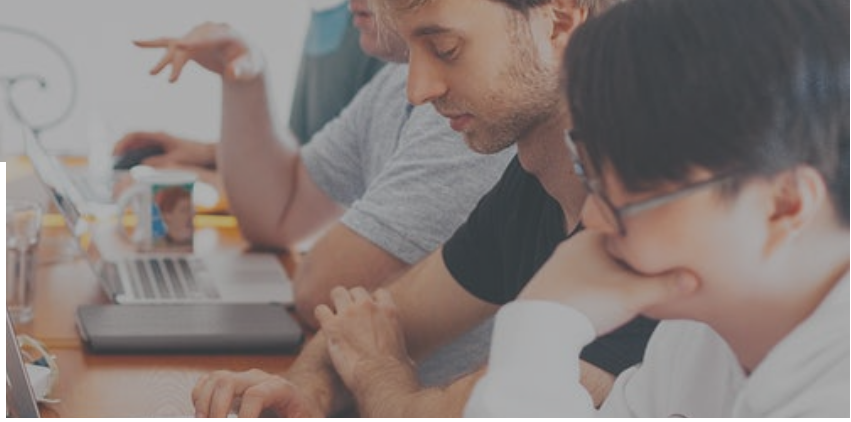
Die reaktiven Maßnahmen im Ereignisfall stehen in einer Krisenstabsübung (aber auch bei dem tatsächlichen Eintritt des Ereignisses) im Vordergrund. Dabei geht es um eine geordnete Arbeitsaufnahme Ihres Krisenstabs unterstützt durch eine allgemeine Themenübersicht. Im Folgenden werden die ersten Schritte sowie detaillierte Punkte für einzelne Krisenstabsmitglieder dargestellt.

Allgemeine Themenübersicht

Bei einer Cyber-Attacke werden initial Maßnahmen unter Einbindung des ITSCM/ISM sowie gegebenenfalls unter Einbindung von externen Behörden eingeleitet: Der Fokus liegt unmittelbar auf Schadensbegrenzung und Sicherungsmaßnahmen.

Darüber hinaus sind folgende Maßnahmen und Überlegungen wesentlich:

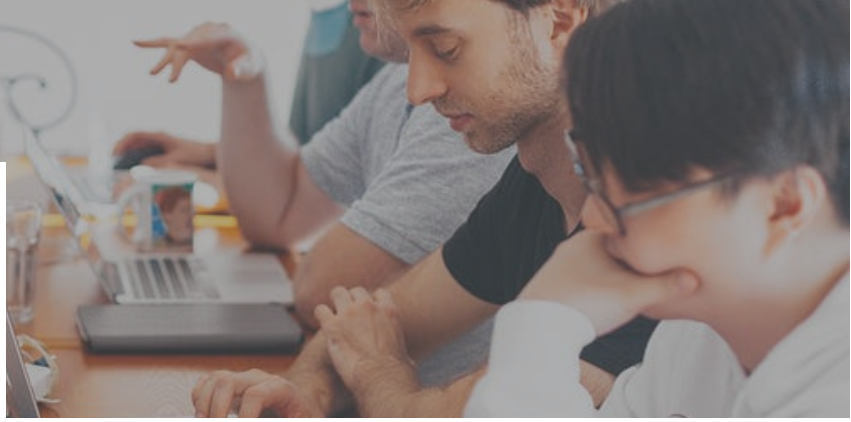
- Beachten Sie bei Alarmierung und Konstituierung des KS folgende Punkte:
  - → Krisenstabsraum nutzbar (eventuell Nutzung des alternativen KS-Raums)?
    - Ist Ihr Krisenraum bezüglich einzelner oder mehrerer IT-Komponenten gegebenenfalls autark nutzbar?
    - Virtuelle Tools mit Anbindung an das Unternehmenssystem stehen vermutlich nicht zur Verfügung!
  - → Identifikation von verfügbaren IT-Systemen und Software (von Telefon über Web-seite bis Notfall-Laptops)
  - → Zügige Kommunikation intern/extern
    - Erstinfo: Bestätigung des Ereignisses auf Basis vorgefertigter Wordings (ideal innerhalb von zehn Minuten)
    - Besondere Beachtung verdient die Positionierung des Unternehmens und die externe Kommunikationsstrategie (Verantwortlichkeit, Täter/Opfer etc.)
  - → Identifikation und Eingrenzung des aktuellen und potenziellen Ausmaßes des Schadens (Schnittstelle ITSCM/IT)
  - → Aktivierung der BCPs und des IT-Recovery-Plans (wenn vorhanden)
  - → Budget-Freigabe einholen (sofern notwendig)



Reaktive Maßnahmen

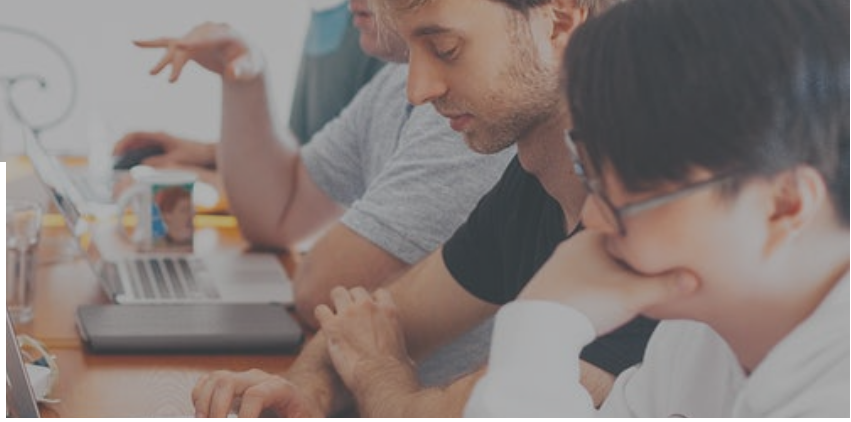
- Beachten Sie eine dynamische Auswirkungskaskade (diese ist durchaus wahrscheinlich): Meist entsteht ein Domino-Effekt innerhalb der IT-Systeme.
- Beachten Sie die extrem hohe Anfangsdynamik und den voraussichtlichen Druck (durch die insgesamt hohe IT-Abhängigkeit) der Chaosphase insbesondere in Bezug auf Informationen (Überfluss und Mangel).
- Führen Sie die Kernaufgaben Initialisierung und Sicherstellung des Notbetriebs durch.
- Nutzen Sie Ihre Organisationsform: Gibt es ein Assistenz- und Service-Team (AST), Kommunikationsteam oder sind Mitglieder des Krisenstabs (KS) für strukturierte Anbindung der Fachbereiche (FB) verantwortlich?
  - → Wie sehen die Melde- und Informationswege aus?
  - → Wie integrieren Sie die Schnittstellenvertreter BCM, ITSCM und ISM in den KS?
- Nutzen Sie die Anbindung der Fachbereiche zum AST bzw. KS zur Lagefeststellung:
  - → Welche Fachbereiche sind betroffen?
  - → Welche Fachbereiche sind arbeitsfähig/nicht arbeitsfähig?
  - → Welche IT-Services sind betroffen?
  - → Welche IT-Services können genutzt werden?
  - → Sind Mitarbeiter und/oder Kundendaten betroffen?
  - → Welche Sicherungsmaßnahmen sind erfolgreich/können priorisiert werden?

- Stellen Sie den Informationsfluss und die koordinierte Anbindung zu externen Schnittstellen (z. B. Behörden wie LKA, BaFin, BSI) sowie die zeitgerechte Umsetzung der Meldepflichten sicher:
  - → Ggf. Integration LKA oder externe Experten (z.B. IT-Forensik) in Krisenstab
  - → Einhaltung der Meldefristen gemäß Unternehmens- und Branchenvorgaben



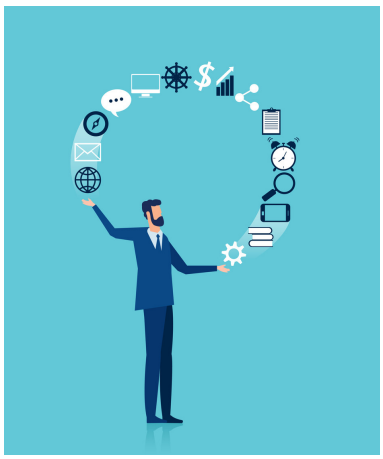
Reaktive Maßnahmen

- Steuern Sie die erweiterte Lagefeststellung: Nutzen Sie eine Visualisierung zur Übersicht!
  - → Internes und externes Schadensausmaß: Welche IT-Services sind betroffen?
  - → Welche RTA und RPA sind aktuell realistisch? Welche Daten sind betroffen?
  - → Welche Fachbereiche sind betroffen? Insbesondere: Welche zeitkritischen Geschäftsprozesse und welche RTO gibt es?
  - → Welche Fachbereiche sind arbeitsfähig/nicht arbeitsfähig? Gibt es verfügbare Business-Recovery-Optionen?
  - → Welche IT-Services werden im Notbetrieb benötigt und sind nutzbar/wiederherstellbar? Priorisierung auf der Zeitschiene?
  - → Verantwortlichkeit für Ereignis: Eigenverschulden/Fremdverschulden/Einhaltung Fürsorgepflicht
  - → Maßnahmenübersicht und Statuskontrolle
  - → Ursachenermittlung zur optimierten Schadensbegrenzung (z. B. über IT-Forensik)
- Nutzen Sie Ihre Schwellenwerte!
  - → Sind Schwellenwerte definiert und welche Schwellenwerte werden überschritten? Schwellenwert potenziell überschritten für:
    - IT-Ausfall
    - Ausfall IT-Dienstleister
    - Ggf. Schwellenwerte ITSCM (wenn vorhanden)
- Beachten Sie die Auswirkungen auf Home-Office und Remote Working.
  - → VPN-Verbindungen können Auswirkungen auch auf Privatgeräte der Mitarbeiter haben (Bring-your-own-Device).
- Schätzen Sie die Perspektive für Ihren Krisenstab ein.
  - → Bei IT-Ausfall voraussichtlich längerer Einsatz des KS (abhängig von der Art und dem Umgang mit der Cyber-Attacke)
- Starten Sie die Sicherstellung des Wiederherstellungsprozesses parallel zum Notbetrieb (IT-Recovery).
- Prüfen Sie Ihren Versicherungsschutz und Meldepflichten (z. B. Betriebsunterbrechungsversicherung).
- Wenden Sie besondere Aufmerksamkeit auf die Betreuung der Hotlines.
  - → Wenn die Telefonie noch funktioniert, ist ein hohes Zusatzvolumen zu erwarten (Kunden- und Medienanfragen)



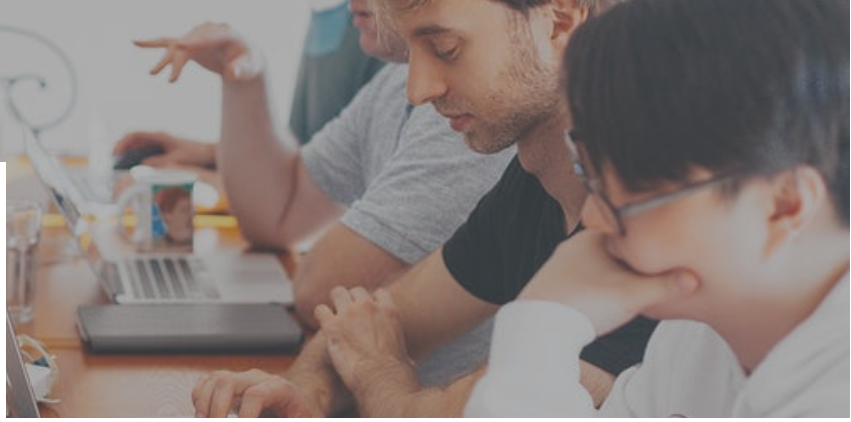
Reaktive Maßnahmen

Besondere Aufgaben der Mitglieder des Krisenstabs



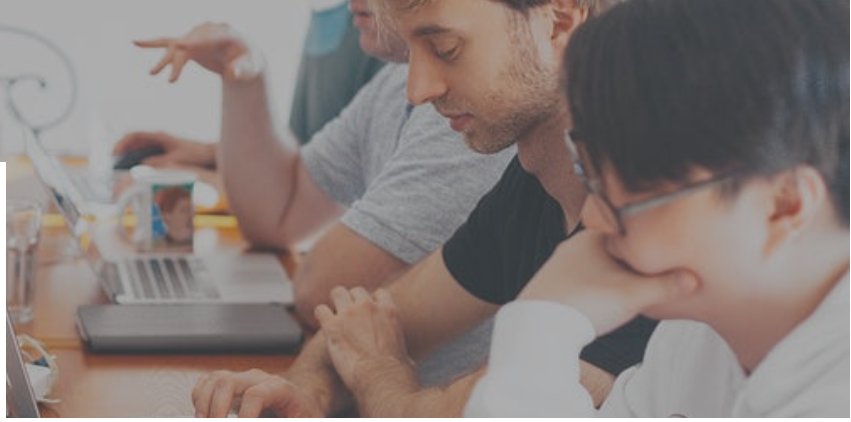
Einige Mitglieder Ihres Krisenstabs können im Szenario „Cyber-Attacke“ ihre Aufgaben gemäß Checkliste bearbeiten (z. B. die Funktionsträger Moderation, Logbuchführung, Visualisierung, Assistenz, Recht und Finanzen). Im Folgenden werden Besonderheiten der Funktionsträger mit Perspektive auf das Szenario „Cyber-Attacke“ dargestellt:

- **Leiter Krisenstab:**
  - → Stellen Sie die Arbeitsfähigkeit des Krisenstabs sicher (initial und regelmäßig)
    - Einbindung relevanter Funktionen und Rollen
    - Verfügbarkeit ausreichender Ressourcen (technisch, räumlich etc.)
  - → Stellen Sie funktionierende Rahmenbedingungen für die Zusammenarbeit her
    - Zeitplan, Briefings, Dokumentation
  - → Beachten Sie die Meldepflichten im Unternehmenskontext (ggf. Kooperation mit Legal)
  - → Steuern Sie aktiv die Zusammenarbeit mit Behörden (ggf. Integration Mitarbeiter LKA, IT-Forensik)
    - Integration von Behördenmitgliedern in Krisenstab (wenn möglich!)
  - → Bei Bedarf und betrieblicher Einschränkung: Konsolidieren Sie die Priorisierung zu Betrieb und Stakeholdern
    - Kerngeschäft/Kernprozesse
    - Was geht mit welchen Mitteln (Stichwort IT-Verfügbarkeit)?
  - → Prüfen Sie den sinnvollen Einsatz von Experten und Dienstleistern
  - → Stellen Sie proaktive Informationen für Geschäftsführung/Decision Making Authoritiy (DMA) und Gremien bereit
    - Abstimmung von Information vor Presseauftritten (in Kooperation mit dem Verantwortlichen Kommunikation)
  - → Beachten Sie die Einhaltung von FORDEC
  - → Führen Sie unbedingt die Maßnahmenkontrolle und eine Wirksamkeitsprüfung durch
  - → Behalten Sie Budget und Finanzkontrolle im Blick
  - → Betreiben Sie aktives Informationsmanagement
  - → Praktizieren Sie aktive Fürsorge (auch dieses Szenario kann belasten)



Reaktive Maßnahmen

- **Verantwortungsbereich Kommunikation:**
  - → Prüfen Sie, welche Medien in der aktuellen Situation verfügbar sind (initial und im Verlauf der Krise)
    - Nutzen Sie die verfügbaren Medien (intern, extern, Social Media)
    - Nutzen Sie ggf. Ihre Dienstleister zur Kommunikation
  - → Beachten Sie die Einheitlichkeit und Verlässlichkeit Ihrer externen und internen Kommunikation
    - Erstinfo: Bestätigung des Ereignisses auf Basis vorgefertigter Wordings (idealerweise innerhalb der ersten zehn Minuten)
    - Angemessene Kommunikationsstrategie (Täter/Opfer, Verantwortlichkeit, Offenheit etc.)
    - Zeitnahe Erweiterung der Kommunikation auf alle Stakeholder
    - Abstimmung innerhalb des KS, insbesondere mit IT bzgl. zu erwartender Zeitlinien (interne/externe Erwartungshaltung aktiv steuern)
  - → Beachten Sie das hohe Interesse an der Verantwortlichkeit für das Ereignis
  - → Nutzen und erstellen Sie FAQs (für internen und externen Bedarf)
    - Betreiben Sie aktives Informationsmanagement mit den relevanten Schnittstellen
  - → Unterstützen Sie Ihre Hotlines (und ggf. Dienstleister) mit Wording-Vorlagen zur Sicherstellung einer einheitlichen externen Kommunikation



Reaktive Maßnahmen

- **Verantwortungsbereich Personal (HR):**
  - → Koordinieren Sie den potenziellen Personalmangel und -überschuss (flexibler Mitarbeitereinsatz):
    - Welche Abteilungen haben Personalbedarf?
    - Welche Abteilungen können Personal zur Verfügung stellen?
    - Welche Skills haben/benötigen die Mitarbeiter (aktives Skill-Management)?
  - → Koordinieren Sie die Datensteuerung und Zugriffsrechte
  - → Stellen Sie sicher, dass bei Bedarf Personalakten für den KS verfügbar und sonst gesperrt sind (z. B. bei Innentäter)
  - → Koordinieren Sie das Informationsmanagement zum Betriebsrat/Personalrat
  - → Beraten Sie bei Bedarf zu Mehrarbeit und Arbeitsrecht (manuelle Workarounds bei IT-Ausfall benötigen meist mehr Zeit und Personal)
  - → Prüfen Sie Zahlungsverpflichtungen
  - → Nutzen Sie die Ressourcen Ihrer Dienstleister
  - → Koordinieren Sie Personaldienstleistungsanfragen nach Bedarf
  - → Betreiben Sie aktives Informationsmanagement

- **Verantwortungsbereich IT:**
  - → Informieren Sie Ihre Dienstleiter (inkl. RZs)
  - → Klären Sie die Zuständigkeiten innerhalb der IT
    - Nutzung des IT-Notfallhandbuchs
  - → Recherchieren Sie und geben Sie eine Einschätzung über das Ausmaß des IT-Ausfalls (Schadensausmaß siehe oben)
  - → Erarbeiten Sie eine Prognose zur Schadensausbreitung
  - → Zeigen Sie Optionen auf bzgl. Zeitlinien und Wiederherstellung der IT
    - Priorisierungsvorschläge seitens der IT
    - Beachten Sie dabei die Priorisierungen durch den KS
    - Beachten Sie Priorisierungen aus dem BCM/ITSCM
    - Integrieren Sie zeitliche und wirtschaftliche Aspekte (Machbarkeit)
  - → Leiten Sie die Umsetzungsinitiative zur Wiederherstellung der IT-Services ein
  - → Identifizieren und koordinieren Sie sinnvolle IT-Dienstleister/-Experten (inkl. IT-Forensik)
    - für den Notbetrieb
    - zur Wiederherstellung
  - → Betreiben Sie aktives Schnittstellenmanagement zu ISM, Datenschutzbeauftragten
  - → Betreiben Sie aktives Informationsmanagement

Reaktive Maßnahmen

- **Verantwortungsbereich Fachbereich:**
  - → Prüfen Sie das Schadensausmaß in Ihrem Bereich
  - → Konsolidieren und kommunizieren Sie die Anforderungen in Ihrem Bereich (bzgl. IT und ggf. Zusatzpersonal)
  - → Prüfen und nutzen Sie Ihre Priorisierungen hinsichtlich der Kernaufgaben
  - → Nutzen und prüfen Sie die Funktionalität und Wirksamkeit Ihrer Überbrückungsmaßnahmen
  - → Nutzen Sie Ihre Fachkenntnisse zur flexiblen und kreativen Anwendung von Lösungsoptionen
  - → Betreiben Sie aktives Informationsmanagement
    - Richtung KS
    - Kooperation mit anderen Fachbereichen

- **Verantwortungsbereich ISM und Datenschutz:**
  - → Prüfen Sie, ob Schutzziele aus dem ISM betroffen sind
  - → Prüfen Sie die Effektivität der ISM-Maßnahmen und passen Sie diese bedarfsorientiert und gesetzeskonform an
  - → Halten Sie die Meldepflichten in Ihrem Verantwortungsbereich ein und betreiben Sie aktives Informationsmanagement zu den entsprechenden Behörden
  - → Betreiben Sie aktives Schnittstellenmanagement zu ITSCM, BCM und Datenschutzbeauftragten
  - → Betreiben Sie aktives Informationsmanagement
    - inkl. Beratung KS zu allen ISM- und Datenschutz-Themen

Rückkehr in den Normalbetrieb und Nachbereitung

Die Rückkehr in den Normalbetrieb nach dem aktiven Einsatz des Krisenstabs bedarf der üblichen vorgesehenen Maßnahmen:

- **Stellen Sie die Rückkehr in den Normalbetrieb gemäß Ihres Wiederherstellungsprozesses sicher.**
  - ⟶ Sicherstellung der Basisfunktionalität der IT-Services
    - Organisation der abgesicherten und vielleicht noch nicht vollumfänglich verfügbaren IT-Services (z. B. Umgang mit Performance-, Funktions-, Nutzereinschränkungen)
  - ⟶ Koordinierte Übergabe der Arbeitspakete in die Fachabteilungen
  - ⟶ Organisation der Aufarbeitung des Backlogs
  - ⟶ Geordnete Beendigung der Arbeit des Krisenstabs (inkl. Übergabe, Informationslinien, Sicherung von Dokumenten und Unterlagen)

- **Stellen Sie die strukturierte Nachbereitung bzw. Aufarbeitung der Geschehnisse sicher (Lessons-Learned-Prozess/Post-Mortem-Analyse).**

Controllit AG
Kühnehöfe 20
22761 Hamburg
Deutschland
www.controll-it.de

Stand: Oktober 2021

Die Controllit AG ist Ihr Partner für Business Continuity Management (BCM). Seit unserer Gründung entwickeln wir integrative Konzepte und Produkte für das Business Continuity Management, IT Service Continuity Management und Krisenmanagement. Wir helfen Ihnen mit strategischen, organisatorischen und technischen Konzepten, Ihre Geschäftsprozesse gegen Bedrohungen abzusichern und für Notfälle vorzusorgen.

Die Inhalte dieses Dokuments dienen der Information über eine Krisenstabsübung "Cyber-Attacke". Nachträgliche Änderungen sind möglich.

Fotonachweise: S. 4: iStock.com/alphaspirit; S. 5: iStock.com/alphaspirit; iStock.com/Maike Hildebrandt; iStock.com/tudmeak; S. 7: iStock.com/SurfUpVector; S. 9: iStock.com/Feodora Chiosea; S. 10: iStock.com/ipuwadol