Cyber Incident Response Planung

DMEA 2025

XING LinkedIn

Besuchen Sie unseren Blog

Positionierung zwischen Strategie und Systemhaus

REWION

Strategie Beratung

Unabhängig

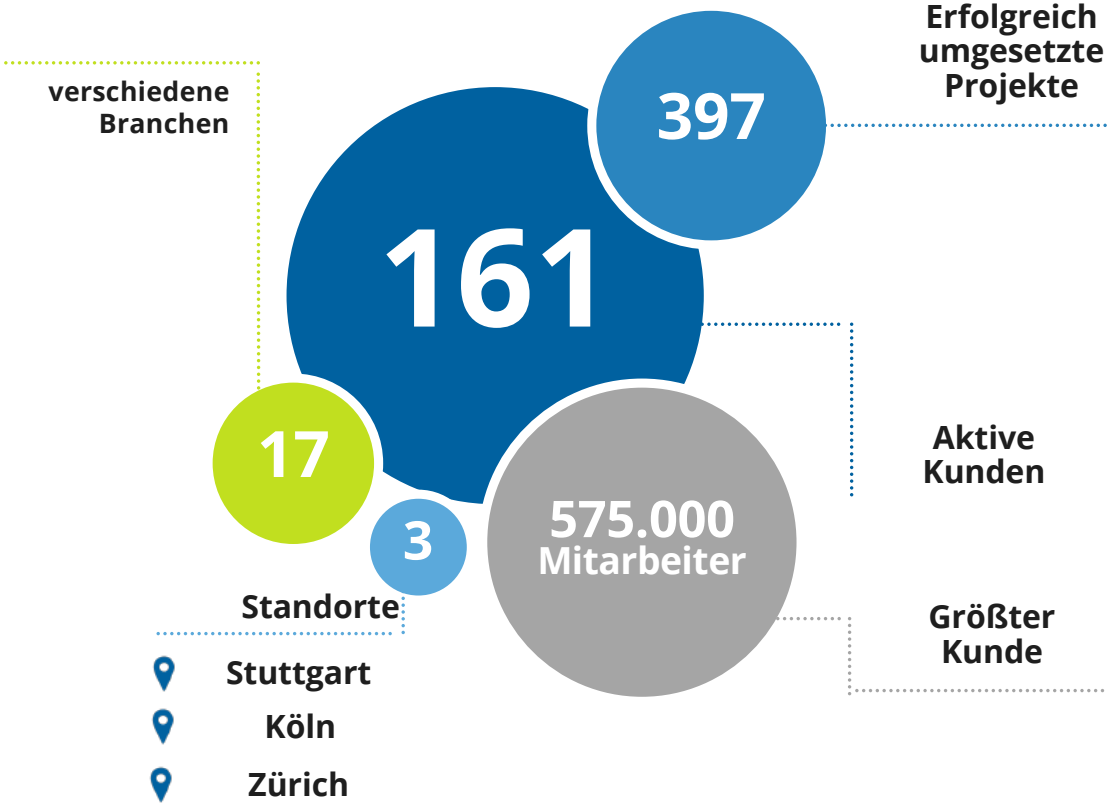
Ganzheitlich

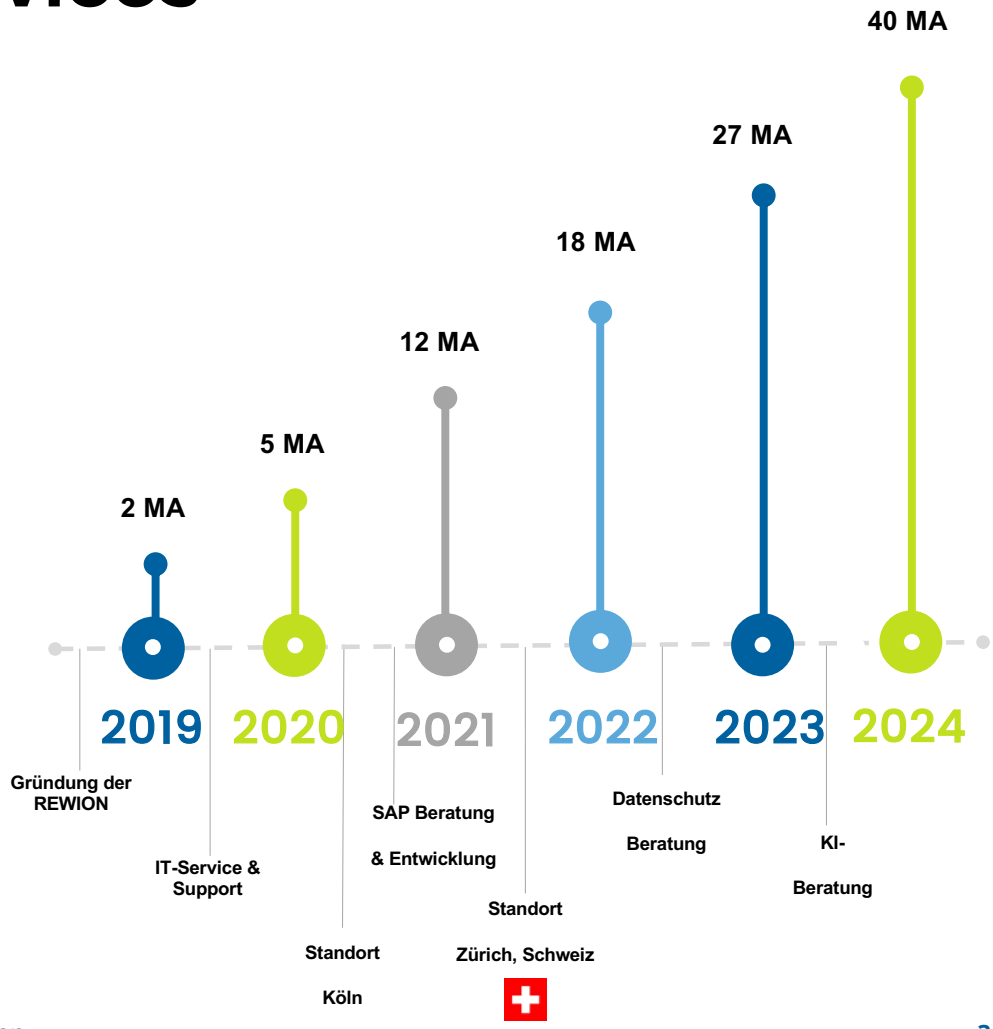
Umsetzungsstark

Systemhaus

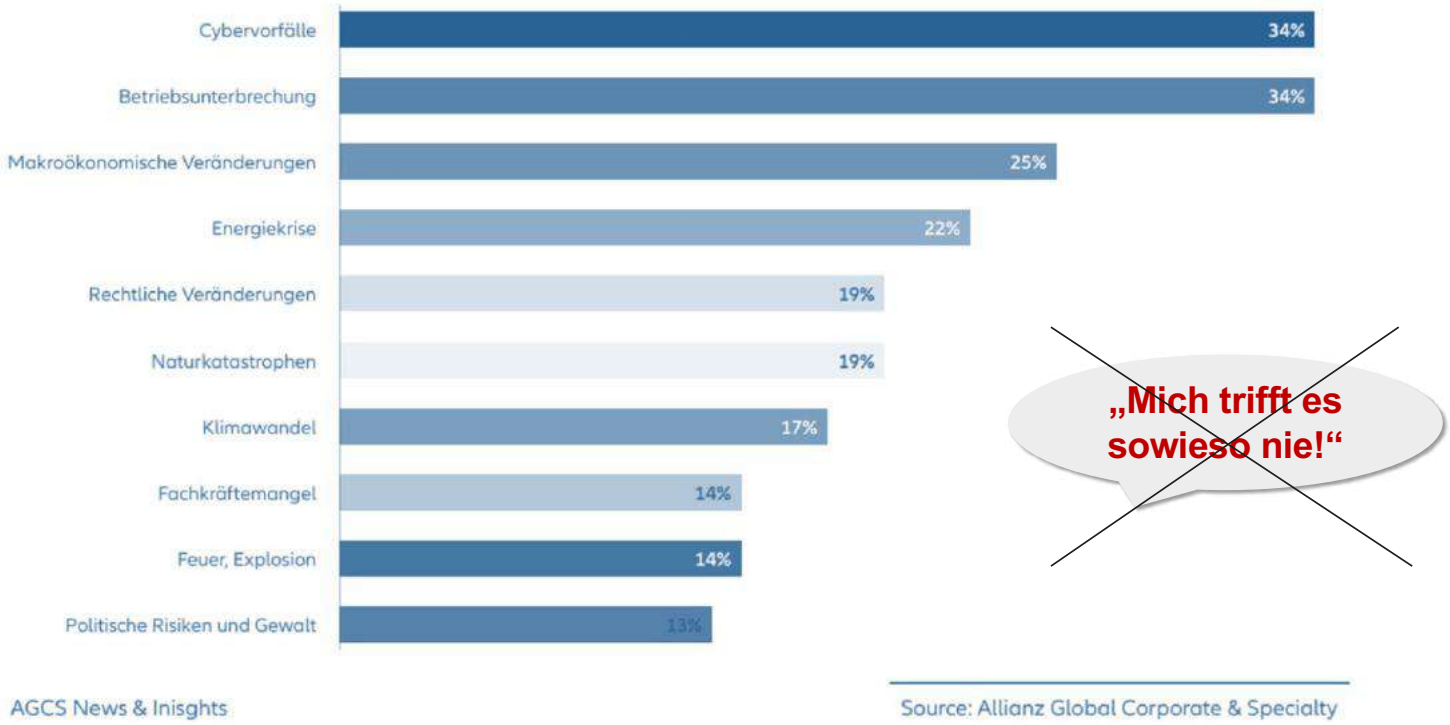
Unser Ziel: Ihr TRUSTED ADVISOR

Rewion – IT Beratung & Services





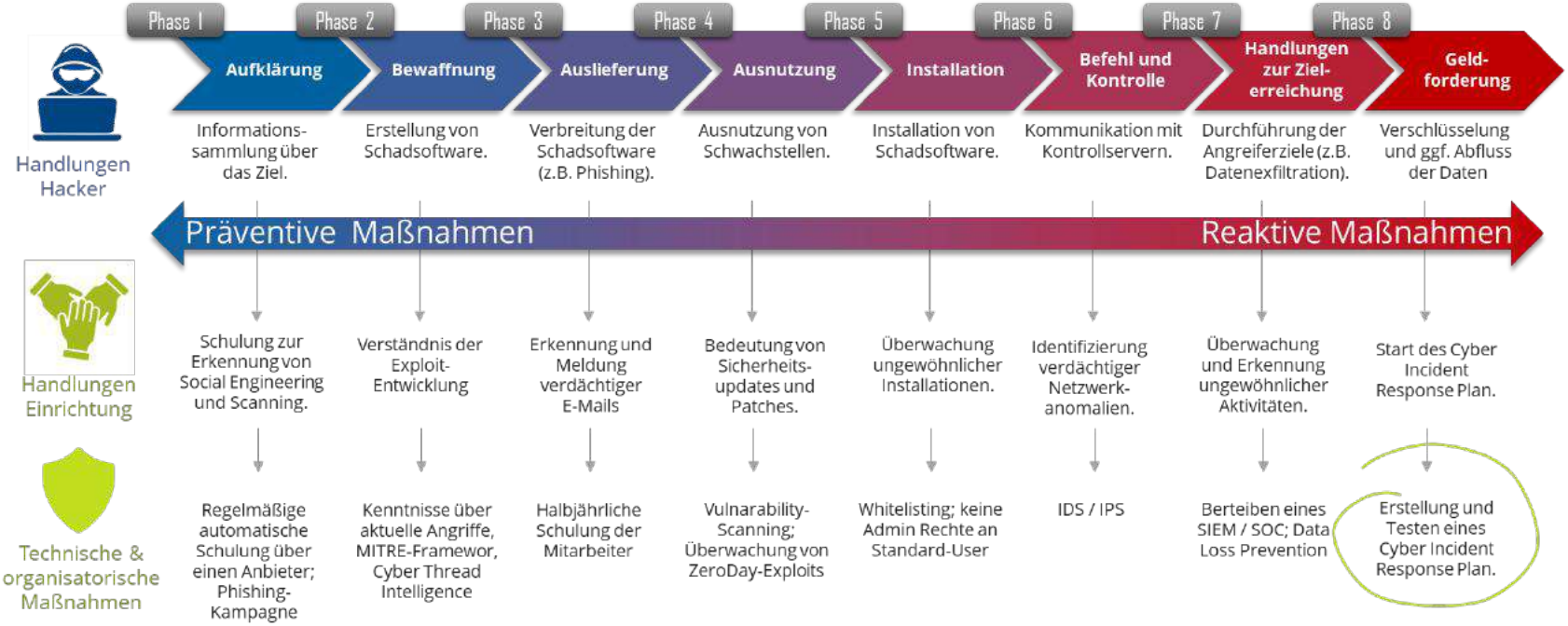
HERAUSFORDERUNGEN



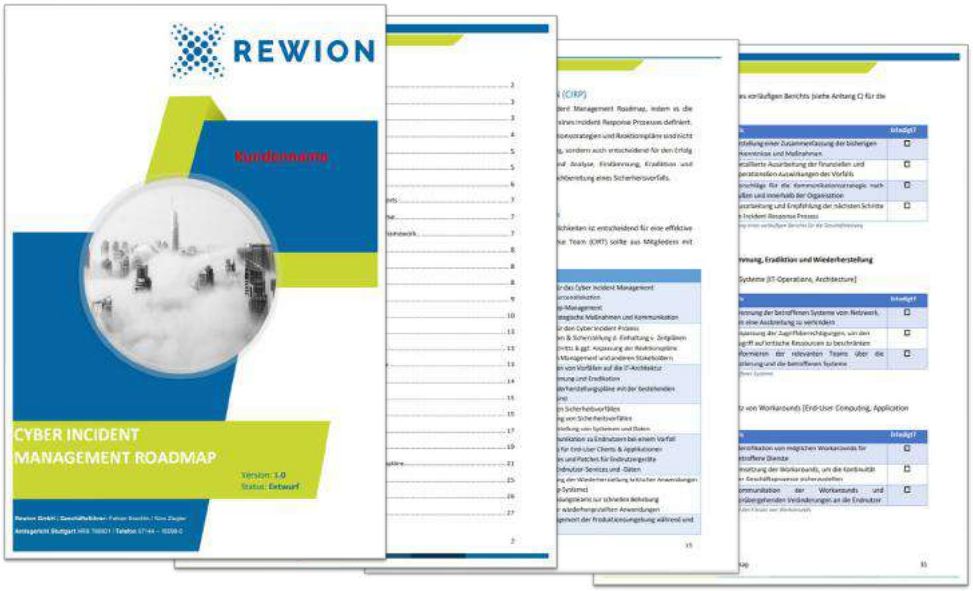
„Mich trifft es sowieso nie!“

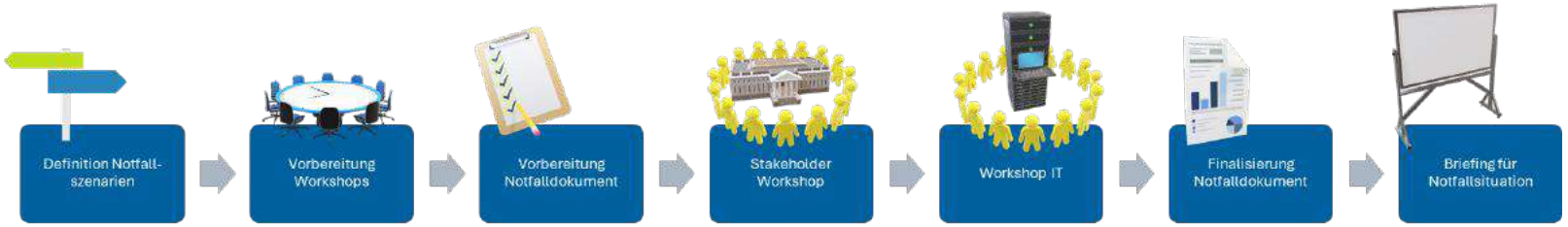
Cybervorfälle wurden zum größten Risiko!

Aufgabenstellung / Ziele



Lösung





Beispielszenario Totalausfall

Technology Recovery

◆ Business Acceptable

Business-as-Usual

Phase	#	Aufgabe	Verantwortlich	Dauer
Erkennung & Analyse	1.1	Vorfallidentifikation und -bewertung	Threat Management	8h Stunden
	1.2	Kommunikation des Vorfalls	Cyber Incident Response Coordinator	1 Stunde
	1.3	Erste Bewertung der Auswirkungen	Architecture, Production	4 Stunden
	1.4	Vorläufige Ursachenanalyse	Forensic Analyst, IT-Operations	20 Stunden
	1.5	Zusammenstellung eines vorläufigen Berichts für die Geschäftsleitung ◆	CIO	2 Stunde
Eindämmung & Eradiktion	1.6	Isolierung betroffener Systeme	IT-Operations, Architecture	10 Stunden
	1.7	Entwicklung und Einsatz von Workarounds	End-User Computing, Application Recovery	12 Stunden
	1.8	Entfernung von Schadsoftware / Wiederherstellung sicherer Zustände ◆	Forensic Analyst, IT-Operations	10 Stunden
Wieder-herstellung	1.9	Priorisierung der Wiederherstellungsaktivitäten	Cyber Incident Response Coordinator, ISB, CIO	2 Stunden
	1.10	Wiederherstellung kritischer Systeme und Daten	IT-Operations, Application Recovery, Production	24 Stunden
	1.11	Testen und Validieren der wiederhergestellten Systeme	IT-Operations, End-User Computing	24 Stunden
	1.12	Wiederaufnahme des normalen Betriebs ◆	Alle Teams	48 Stunden
Nach-bereitung	1.13	Durchführung einer Post-Incident-Analyse	ISB, Forensic Analyst	5 Tage
	1.14	Aktualisierung des Incident Response Plans	Cyber Incident Response Coordinator	2 Tag
	1.15	Schulungen und Informationsveranstaltungen für Mitarbeiter	HR, Communication	15 Tage
	1.16	Rechtliche Überprüfung und Compliance-Bewertung	Legal Advisor, DSB	4 Tage
	1.17	Erstellung eines Abschlussberichts für die Geschäftsleitung	CIO	2 Tage

Beispiel-Szenario 1: Totalausfall aller Systeme aufgrund Cyberangriff

Beispielszenario: Abfluss sensibler Daten

Phase	#	Aufgabe	Verantwortlich	Dauer
Erkennung & Analyse	3.1	Vorfallidentifikation und -bewertung	Threat Management	1 Stunde
	3.2	Kommunikation des Vorfalls	Cyber Incident Response Coordinator	30 Minuten
	3.3	Erste Bewertung der Auswirkungen	Architecture, Production, DSB	2 Stunden
	3.4	Zusammenstellung eines vorläufigen Berichts für die Geschäftsleitung	CIO, DSB	1 Stunde
Eindämmung & Eradiktion	3.5	Identifikation der Datenverlustquelle	IT-Operations, Production	6 Stunden
	3.6	Sicherung noch verfügbarer Daten	End-User Computing, Application Recovery	6 Stunden
	3.7	Sicherheitsmaßnahmen zur Verhinderung weiterer Verluste	ISB, IT-Operations, CIR Coordinator, DSB	8 Stunden
Wieder-herstellung	3.8	Wiederherstellung verlorener Daten aus Backups	IT-Operations, Application Recovery	24 Stunden
	3.9	Validierung der wiederhergestellten Daten	IT-Operations, Application Recovery, Production	24 Stunden
	3.10	Testen und Validieren der wiederhergestellten Systeme	IT-Operations, Application Recovery, Production	12 Stunden
	3.11	Wiederherstellung von Geschäftsprozessen	Alle Teams	48 Stunden
Nach-bereitung	3.12	Durchführung einer Post-Incident-Analyse (inkl. Ursachenanalyse)	ISB, DSB, Forensic Analyst	2 Tage
	3.13	Aktualisierung des Incident Response Plans und Datenschutzpraktiken	Cyber Incident Response Coordinator, DSB	1 Tag
	3.14	Schulungen und Informationsveranstaltungen für Mitarbeiter	HR, Communication, DSB	2 Tage
	3.15	Rechtliche Überprüfung, Compliance-Bewertung, Kommunikation mit Behörden und Betroffenen	Legal Advisor, DSB	2 Tage
	3.16	Erstellung eines Abschlussberichts für die Geschäftsleitung	CIO, DSB	2 Tage

Warum (noch) ein Notfallmanagement?

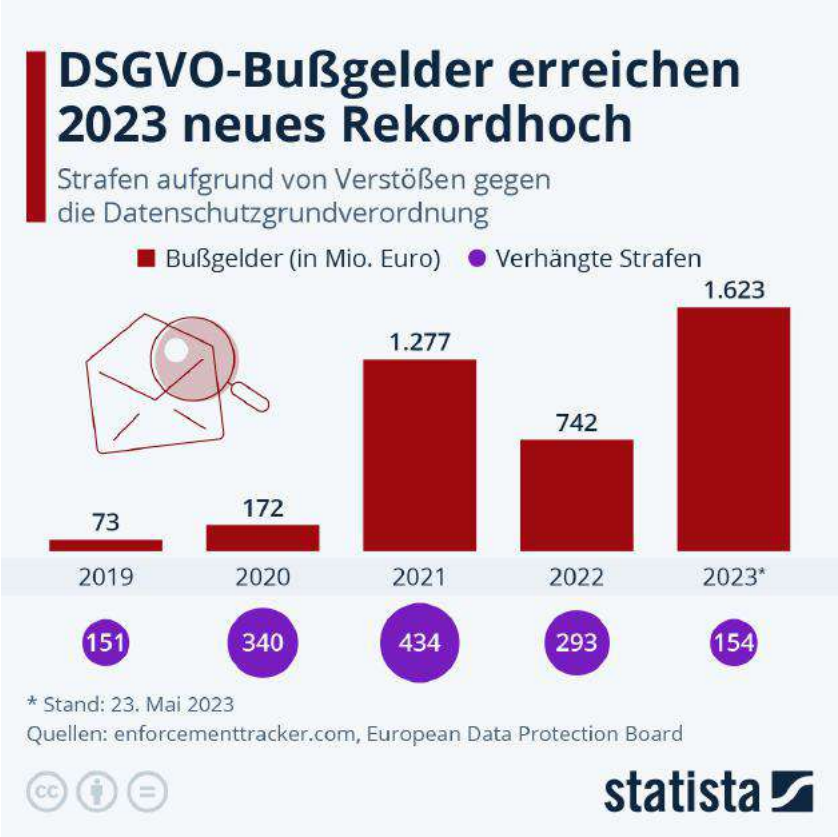


Abbildung 1: Bußgelder DSGVO

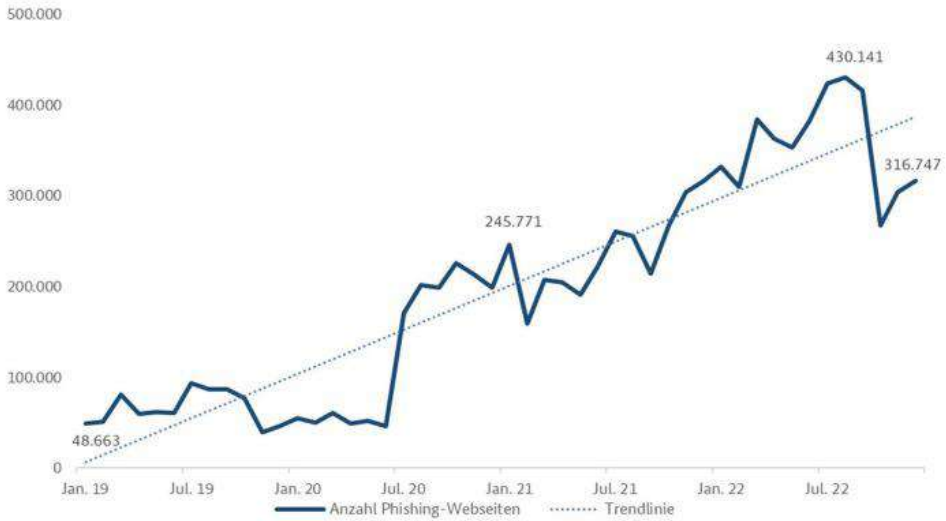


Abbildung 2: Aufkommen von Phishing als Cybercrime

Was ist eine Datenschutzverletzung?

Europäische Datenschutz-Grundverordnung (DSGVO)

„Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur **Vernichtung**, zum **Verlust**, zur **Veränderung**, oder zur **unbefugten Offenlegung** von beziehungsweise zum **unbefugten Zugang** zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden

Schutzziele der IT-Security

Der Klassiker:

Mitarbeiter A verliert einen USB-Stick mit sensiblen personenbezogenen Daten

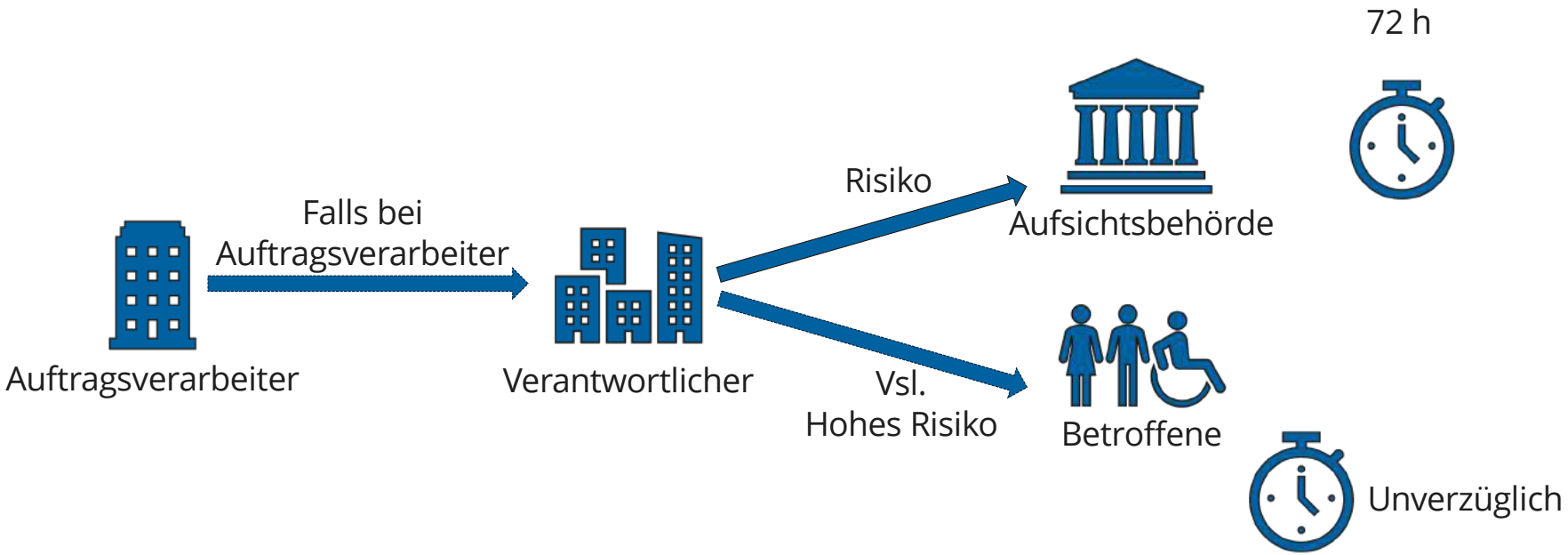
Der Dienstleister:

Dienstleister B hat eine Schwachstelle in seiner IT-Infrastruktur, woraufhin Datensätze zu Kunden ausgelesen wurden

Der Angriff:

Unternehmen C wird Opfer eines Hacking-Angriffs auf eigene IT-Systeme, die daraufhin per Ransomware verschlüsselt und zum Teil abgegriffen wurden

Welche Fristen und Anforderungen gelten?



Welche Fristen und Anforderungen gelten?

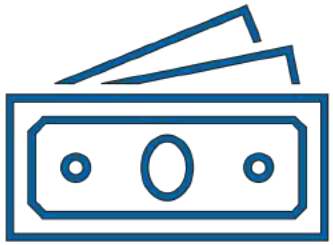
Beschreibung der Art der Verletzung, Angabe der Kategorien, ungefähre Zahl der Betroffenen, der betroffenen Kategorien und ungefähre Zahl der betroffenen personenbezogenen Datensätze;

Namen und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für Informationen;

Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Konsequenzen bei Nicht-Einhaltung



Bußgelder bis 10 Mio. Euro oder 2% des weltweiten (Konzern-)Umsatzes

Reputationsschäden

Zwischenfazit

- Datenschutzverletzungen sind ein Ereignis, das oft einen **Prozess** in Gang setzt, deren Bewältigung ab einem **festgelegten Risiko** abteilungsübergreifend stattfindet.
- Durch Fristen kommt es auf **Effizienz** an. Insofern macht eine **Vorbereitung** Sinn.
- Da personenbezogene Daten (immer mehr) mittels **Informations- und Kommunikationstechnik** verarbeitet werden, korrelieren Datenschutzverletzungen regelmäßig (auch) mit Notfällen oder Krisen in der IT.

→ Mögliche Lösung: **Datenschutz-Notfallmanagement**

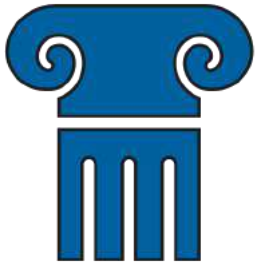
Was ist ein (Datenschutz-)Notfallmanagement?

„Notfall- und Krisenmanagement umfasst den systematischen Umgang mit Notfall-, Krisen- und Katastrophenlagen. Dazu gehört sowohl die allgemeine Prävention, als auch die Identifikation, Analyse, Einleitung und Verfolgung von Gegenmaßnahmen sowie das Entwickeln von abgestimmten Bewältigungsstrategien im Kontext von oben genannten Lagen.“ (Quelle: Wikipedia)

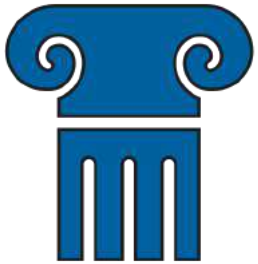
Vorfallsart	Erläuterung	Anwendung auf Datenschutz
Einfache Störung	Kurzzeitiger Ausfall von Prozessen oder Ressourcen mit nur geringem Schaden	Datenschutzverletzung mit (geringem) Risiko, wenige Stellen beteiligt
Notfall	Länger andauernder Ausfall von Prozessen oder Ressourcen mit hohem oder sehr hohem Schaden	Datenschutzverletzung mit Risiko, mehrere Stellen beteiligt, Fachwissen erforderlich
Krise	Im Wesentlichen auf die Institution begrenzter verschärfter Notfall, der die Existenz der Institution bedroht oder die Gesundheit oder das Leben von Personen beeinträchtigt	Datenschutzverletzung mit hohem Risiko und vielen Betroffenen, umfassende Ressourcen benötigt, Fachwissen erforderlich

Was ist ein (Datenschutz-)Notfallmanagement?

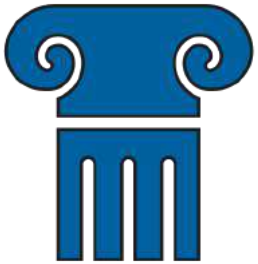
„Datenschutz-Notfallmanagement umfasst den systematischen Umgang mit Datenschutzverletzungen in einer Organisation. Dazu gehört sowohl die allgemeine Prävention, als auch die Identifikation, Analyse, Einleitung und Verfolgung von Gegenmaßnahmen sowie das Entwickeln von abgestimmten Bewältigungsstrategien im Kontext von oben genannten Lagen.“ (Quelle: Wikipedia)



Präventionsarbeit



Umgang mit Datenschutzverletzungen



Kontinuierliche Verbesserung

Exkurs: BCM nach BSI 200-4

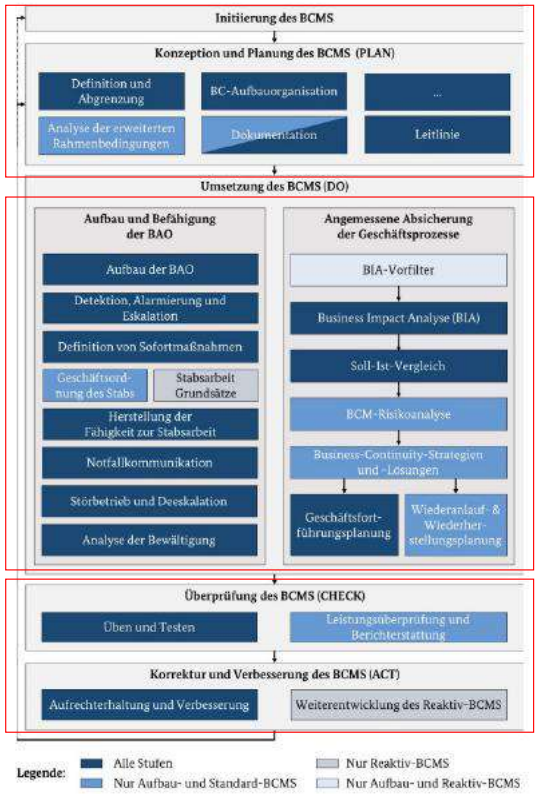
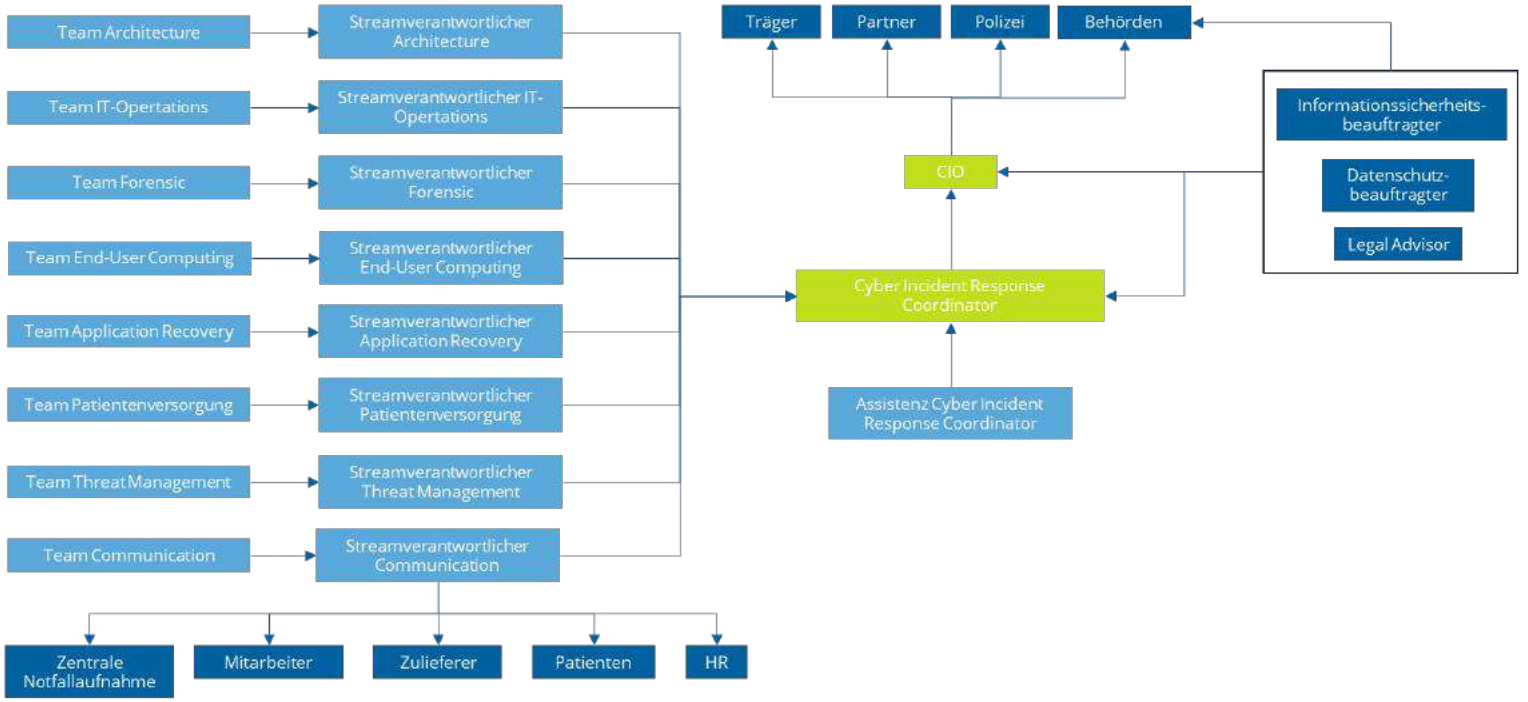


Abbildung 3: Das Business Continuity Management

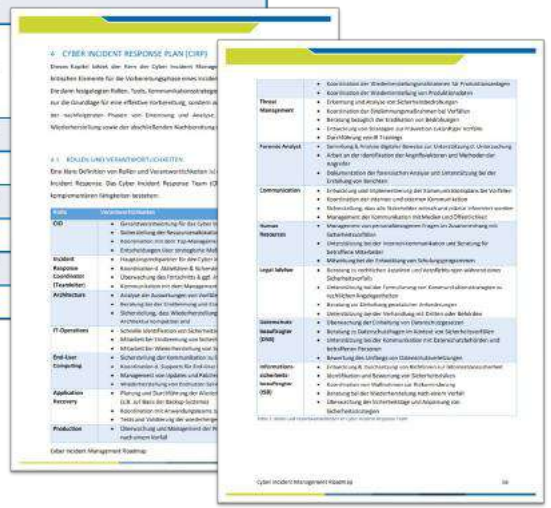
- Der BSI-Standard 200-4 stellt Organisationen Methoden und Werkzeuge bereit, um ihre Geschäftsprozesse hinsichtlich auftretender Risiken abzusichern oder schnellstmöglich die Wiederherstellung von Geschäftsprozessen zu ermöglichen.
- Umsetzung als Managementsystem über die Gesamtorganisation
- Wie in vielen Managementsystemen üblich, folgt der Aufbau dem Vierklang aus: PLAN-DO-CHECK-ACT
- Wir finden die eben aufgestellten Säulen wieder.
- WICHTIG: Ein Datenschutz-Notfallmanagement (DS-NM) kann und sollte stets ein Teil eines IT-Notfallmanagements (Business-Continuity-Managements) sein!

Komunikationsplan

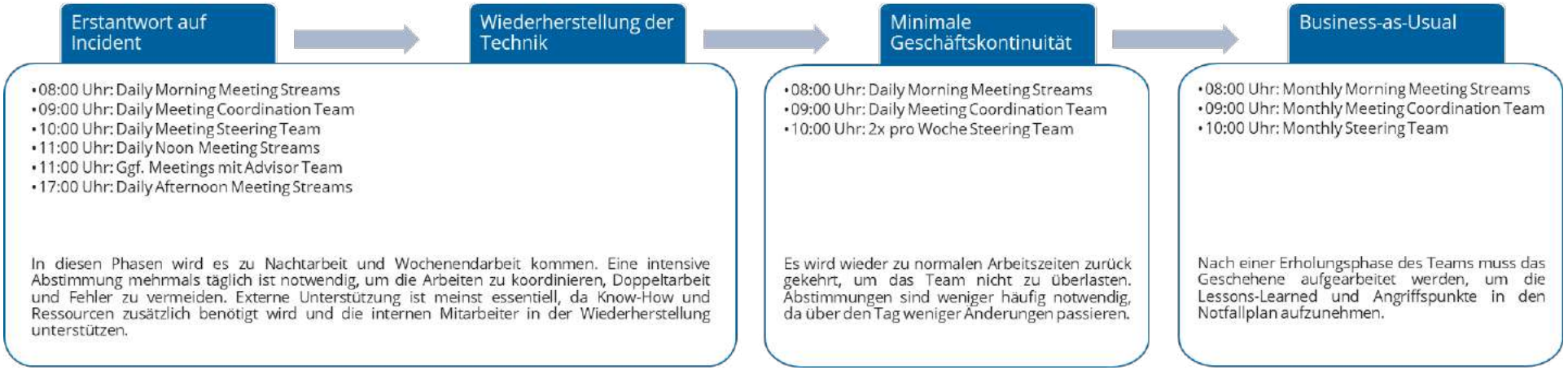


Gezielte Rollenzuweisung

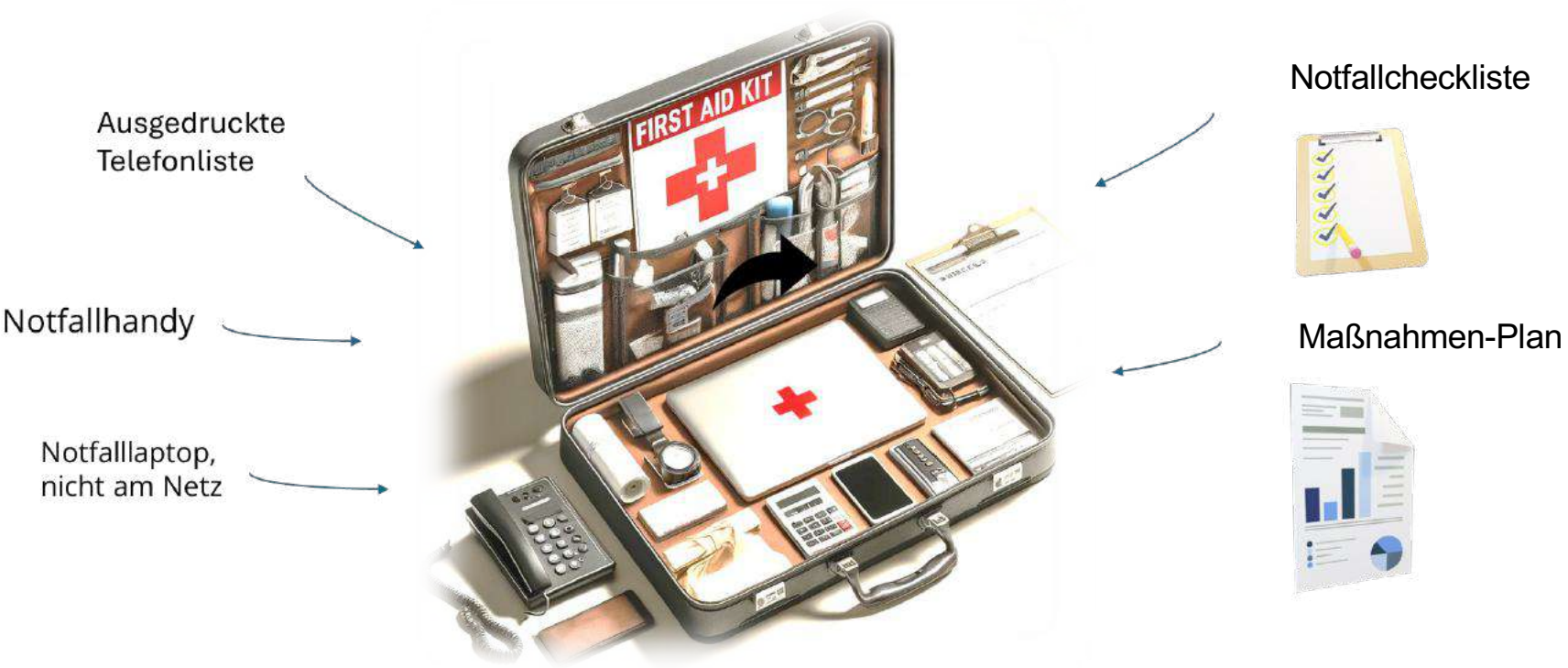
Rolle	Name	Verantwortlichkeit	Kontaktinformationen
CIO	*[Name Stream Lead]*	▪ Gesamtverantwortung für das Cyber Incident Management ▪ Koordination und Kommunikation mit Top Management	*[E-Mail / Telefon]*
IR Coordinator	*[Name Stream Lead]*	▪ Hauptansprechpartner für den Cyber Incident Prozess ▪ Koordination d. Aktivitäten & Sicherstellung d. Einhaltung v. Zeitplänen	*[E-Mail / Telefon]*
Architecture	*[Name Stream Lead]*	▪ Analyse der Auswirkungen von Vorfällen auf die IT-Architektur ▪ Beratung bei der Eindämmung und Eradikation	*[E-Mail / Telefon]*
IT-Operations	*[Name Stream Lead]*	▪ Schnelle Identifikation von Sicherheitsvorfällen ▪ Mitarbeit bei Eindämmung von Sicherheitsvorfällen & Wiederherstellung	*[E-Mail / Telefon]*
End-User Computing	*[Name Stream Lead]*	▪ Sicherstellung der Kommunikation zu Endnutzern bei einem Vorfall ▪ Koordination d. Supports für End-User Clients & Applikationen	*[E-Mail / Telefon]*
Application Recovery	*[Name Stream Lead]*	▪ Wiederherstellung kritischer Anwendungen inkl. Tests und Validierung	*[E-Mail / Telefon]*
Production	*[Name Stream Lead]*	▪ Koordination der Wiederherstellung von Daten	*[E-Mail / Telefon]*
Threat Management	*[Name Stream Lead]*	▪ Erkennung und Analyse von Sicherheitsbedrohungen ▪ Koordination der Eindämmungsmaßnahmen bei Vorfällen ▪ Entwicklung von Strategien zur Prävention zukünftiger Vorfälle ▪ Durchführung von IR Trainings	*[E-Mail / Telefon]*
Forensic Analyst	*[Name Stream Lead]*	▪ Sammlung & Analyse digitaler Beweise zur Unterstützung d. Untersuchung	*[E-Mail / Telefon]*
Communication	*[Name Stream Lead]*	▪ Entwicklung und Implementierung des Kommunikationsplans bei Vorfällen	*[E-Mail / Telefon]*
Human Resources	*[Name Stream Lead]*	▪ Unterstützung bei der internen Kommunikation und Mitwirkung bei Schulungen	*[E-Mail / Telefon]*
Legal	*[Name Stream Lead]*	▪ Beratung zu rechtlichen Aspekten & Verpflichtungen während eines Sicherheitsvorfalls	*[E-Mail / Telefon]*
DSB	*[Name Stream Lead]*	▪ Überwachung der Einhaltung von Datenschutzgesetzen	*[E-Mail / Telefon]*
ISB	*[Name Stream Lead]*	▪ Entwicklung & Durchsetzung von Richtlinien zur Informationssicherheit	*[E-Mail / Telefon]*



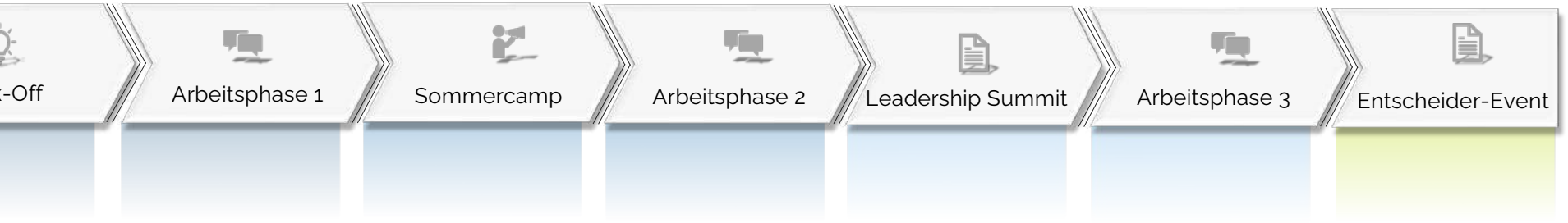
Möglicher Tagesplan in den Phasen



Zusammenfassung und Fazit



Projekttimeline mit den Partnern



REWION

Dr. Larissa Hütter.

Digital Health | IT Consultant

Termin vereinbaren

+49 160 92126810

larissa.huetter@rewion.com

www.rewion.com

Auf LinkedIn vernetzen.

REWION

David Morva.

Manager Datenschutz

Zertifizierter Berater im Datenschutzrecht (FernUniversität in Hagen)

+49 **7144 160 9894**

david.morva@rewion.com

www.rewion.com

Hier einen Termin vereinbaren