



CYBER-KRISENMANAGEMENTPLAN

Status: **Final**

Stand: **01.01.2026**

Version: **2026-1.5**

Dokumentenname: Draft KMP 1.5.docx

INHALTE

INHALTE	1
HINWEISE ZUR NUTZUNG UND ABLAGEORT	1
1 CHECKLISTE SOFORTMAßNAHMEN FÜR MITARBEITENDE	2
2 CHECKLISTE SOFORTMAßNAHMEN IT-BETRIEB	3
3 LAGEBEWERTUNG	5
4 CHECKLISTE KONTAKTAUFNAHME KRISENHOTLINE	6
5 ABLAUF DER FALLANNAHME ÜBER DIE HISCOX KRISENHOTLINE	7
6 EREIGNISBEWÄLTIGUNG	8
7 ZEITKRITISCHE PROZESSE/PRODUKTE/DIENSTLEISTUNGEN	10
8 KRITISCHE DATENSICHERUNGEN	13
9 ALARMIERUNG DES KRISENMANAGEMENTS	14
10 INFRASTRUKTUR	16
10.1 Standorte	16
10.2 Arbeitsmittel & Arbeitshilfen	18
11 AUFBAUORGANISATION DES KRISENMANAGEMENTS	20
11.1 Rollen im Krisenmanagement	21
11.2 Lagedokumentation und Visualisierung	23
12 GRUNDSÄTZE ZUR KRISENKOMMUNIKATION	24
ANHANG A FÜHRUNGSZYKLUS	26
ANHANG B WICHTIGE INTERNE ANSPRECHPARTNER	27
ANHANG C WICHTIGE EXTERNE KONTAKTE	29
ANHANG D ANSPRECHSTELLEN CYBERCRIME DEUTSCHLAND	30
ANHANG E ANSPRECHSTELLEN CYBERCRIME ÖSTERREICH	32
ANHANG F ANSPRECHSTELLEN CYBERCRIME SCHWEIZ	33
ANHANG G PROTOKOLLVORLAGE	34
ANHANG H VORLAGEN KRISENKOMMUNIKATION	36
H.1 Meldung an interne Mitarbeiter	36
H.2 Kundenmeldung Unterbrechung der Leistungen	38
H.3 Muster für Journalistenanfragen	40
H.4 Fragen und Antworten (FAQs)	41
ANHANG I BEGRIFFE	43
I.1 Störung	43
I.2 Notfall	43
I.3 Krise	43
KONTAKT	44

HINWEISE ZUR NUTZUNG UND ABLAGEORT

Schwarze Texte sind essenziell für das Dokument, sollten aber vor Übernahme hinreichend überprüft werden. Mit der Funktion „Alle Anzeigen“ (Strg + Shift + *) können weitere Hinweise in *blauer* Farbe zur Bearbeitung eingeblendet werden. Diese Texte werden nicht mitgedruckt.

Ablageort	Digital	1.	2.
	Analog	1.	2.

Eine digitale Version dieses Planes zur weiteren Bearbeitung erhalten Sie per Anfrage über die folgende Adresse: anfrage-hiscox@hisolutions.com.

Kapitel und Abschnitte des Dokuments

Kapitel 1 - 6	Dokumente und Hilfsmittel zur ad-hoc Verwendung.
Kapitel 7 - 12	Dokumente und Hilfsmittel zur Unterstützung ihrer Präventionsmaßnahmen
Anhänge	Nachgelagerte Hilfsmittel für den Einsatz in der Krise

1 CHECKLISTE SOFORTMAßNAHMEN FÜR MITARBEITENDE

Die folgende Checkliste unterstützt Sie bei der Ergreifung von Sofort-Maßnahmen nachdem ein Schaden erkannt wurde.

Checkliste Sofortmaßnahmen für Mitarbeitende	Erledigt	Nicht anwendbar
1. Beenden der unerwünschten Verbindungen oder Prozesse auf dem betroffenen System	☐	☐
2. Trennen der Verbindung der betroffenen Systeme zum Internet oder sonstigen Netzwerken	☐	☐
3. Gegebenenfalls hartes Ausschalten (NICHT herunterfahren) der betroffenen Systeme	☐	☐
4. Betroffenes System NICHT erneut starten, bevor nicht eindeutig klar ist, dass dadurch nicht weiterer Schaden verursacht wird	☐	☐
5. Interne IT-Hotline des Unternehmens anrufen	☐	☐

Tabelle 1 Checkliste Sofortmaßnahmen für Mitarbeitende

2 CHECKLISTE SOFORTMAßNAHMEN IT-BETRIEB

Die folgende Checkliste unterstützt Sie bei der Ergreifung von Sofortmaßnahmen nachdem ein Schaden erkannt wurde.

Checkliste Sofortmaßnahmen für den IT-Betrieb	Erledigt	Nicht anwendbar
1. Trennen Sie SOFORT SÄMTLICHE Verbindungen von identifizierten Systemen	☐	☐
a) ...zum Internet, damit Schadsoftware bzw. Angreifer keine weiteren Aktionen nachladen bzw. durchführen können	☐	☐
b) ...zu Partnern und Dienstleistern, damit diese nicht ebenfalls infiziert werden	☐	☐
c) ...zu Datenspeichern (NAS, Fileserver, Exchange), damit diese nicht weiter verschlüsselt werden.	☐	☐
d) ...zu Datensicherungssystemen, insbesondere Netzwerkspeichern (NAS) und USB-Festplatten	☐	☐
e) ...zu kritischen Unternehmensbereichen, etwa einer Produktions-IT (OT)	☐	☐
2. Bei Virtualisierung: Erstellen Sie von allen betroffenen virtualisierten Servern sowie virtualisierten AD-Controllern einen Snapshot (mit Arbeitsspeicher), damit forensische Daten möglichst unverändert erhalten bleiben.	☐	☐
3. Bei Ransomware: Stellen Sie anhand des Besitzers der verschlüsselten Dateien fest, unter welchem Nutzerkonto die Ransomware lief (Rechtsklick auf die Datei, Eigenschaften, Reiter: Sicherheit, Erweitert, oben: Besitzer). Wenn ein eindeutig identifiziertes Domänenbenutzerkonto verwendet wird, das kein essentielles Service- oder Systemkonto ist, sperren Sie dieses.	☐	☐
4. Stellen Sie anhand von Systemlogdateien oder üblicher Nutzungszuordnung fest, welcher PC von diesem Benutzer verwendet wurde, und trennen Sie diesen vom Netzwerk. Bitte arbeiten Sie nicht ohne Rücksprache an diesem Gerät, da sonst forensische Daten zerstört werden könnten.	☐	☐

5. Bitte sichern Sie die Logdateien von Firewalls, Proxys und Windows Domain Controllern (C:\Windows\System32\winevt\Logs*.evtx), so dass diese nicht auslaufen oder anderweitig verloren gehen.	☐	☐
6. Bitte schalten Sie die betroffenen Server nicht aus und arbeiten Sie nicht ohne Rücksprache an diesen, da sonst forensische Daten zerstört werden könnten.	☐	☐
7. Bitte überprüfen Sie auf Routern und Firewalls noch einmal sämtliche Fernzugänge, insbesondere Port-Forwarding für RDP, und löschen bzw. sperren Sie diese. Fernzugänge sollten ausschließlich über ein mehrfaktor-gesichertes VPN (Zertifikat, Token, etc.) möglich sein.	☐	☐
8. Fassen Sie die bekannten Fakten für die Kontaktaufnahme mit den Experten zusammen (siehe 4 Checkliste Kontaktaufnahme)	☐	☐
9. Kontaktaufnahme Krisenhotline: +49 (89) 545 801 708	☐	☐
10. Nehmen Sie ggf. Kontakt mit der Polizei auf (nach Rücksprache mit dem Krisenstab).	☐	☐

Tabelle 2 Checkliste Sofortmaßnahmen IT-Betrieb

3 LAGEBEWERTUNG

Das vorliegende Dokument unterstützt Hiscox-Kunden bei der Behandlung von Cyber-Krisen und kann als Anleitung zum Cyber-Krisenmanagement genutzt werden. Eine Cyber-Krise liegt vor, wenn mindestens eine der folgenden Fragen mit „zutreffend“ beantwortet werden muss:

Nr.	Lage	Zutreffend?
1	Ein IT-Ausfall ist existenzbedrohend oder stört den Geschäftsbetrieb erheblich (zeitkritische IT-Services siehe Zeitkritische Prozesse/Produkte Seite 10).	☐
2	Ein schwerwiegender Hackerangriff ist erfolgt.	☐
3	Ein schwerwiegender IT-basierter Betrugs-/Erpressungsfall ist aufgetreten.	☐
4	Vertrauliche Daten sind abgeflossen.	☐
5	Reputationsschäden durch Negativnachrichten sind zu erwarten.	☐
6	Es wurde ein meldepflichtiger Gesetzesverstoß begangen.	☐

Tabelle 3 Checkliste Lagebewertung

Bei Vorliegen einer Cyber-Krise – auch nur im Verdachtsfall – informieren Sie bitte für technische Maßnahmen und zur Unterstützung bei der Krisenkommunikation umgehend die Krisenhotline unter:

+49 (89) 545 801 708 (bitte Versicherungsnummer bereithalten)

Direkte Unterstützung von Experten in einem Krisenfall ist in ihrer HISCOX Police mit inbegriffen.

Zudem bitte jeden Vorfall auch an Ihren Versicherer Hiscox melden. Hiscox steht Ihnen für die Bewertung von Versicherungsschutz und Kostenübernahme sowie zur Koordination des Ablaufs zur Verfügung. Sie erreichen Ihren Ansprechpartner unter: +49 (89) 545 801 300 oder hiscox.schaden@hiscox.de

4 CHECKLISTE KONTAKTAUFNAHME KRISENHOTLINE

Um eine möglichst schnelle und zielgerichtete Hilfe durch die Experten von msg systems und HiSolutions sicherzustellen, sollte die folgende Checkliste vor der Kontaktaufnahme durch eine/n IT-Verantwortliche/n oder den IT-Dienstleister genutzt werden.

Allgemeine Angaben	
Wer meldet den Schaden? - Name der meldenden Person sowie Kontaktdaten - betroffene Organisation - Versicherungsnummer - Weitere Kontaktdaten von IT-Mitarbeitern oder Dienstleistern	
Was ist konkret passiert? - Handelt es sich um einen akuten oder älteren Vorfall? - Wie und wann wurde der Vorfall entdeckt? - Was sind beobachtete Symptome? - Gibt es Hypothesen zur Ursache?	
Was ist betroffen? - IT-Systeme (Clients, Server, OT, Cloud)? - Befinden sich die betroffenen IT-Systeme im Eigen- oder Fremdbetrieb? - Bestehen Netzwerkverbindungen zu anderen Unternehmen? - Sind betroffene Datenarten absehbar (Personendaten, Betriebsgeheimnisse)?	
Welche Auswirkungen hat der Vorfall auf den Geschäftsbetrieb? - Liegt eine vollständige oder teilweise Betriebsunterbrechung vor? Falls ja, seit wann? - Welche Auswirkungen hat der Vorfall auf andere Organisationen?	
Was wurde bereits getan? - Wurden Sofortmaßnahmen umgesetzt? - Wurden Systeme isoliert, ausgeschaltet oder neu gestartet? - Wurden Benutzerkonten gesperrt oder Passwörter geändert? - Liegen etwaige Meldepflichten vor und wurden diese bereits wahrgenommen?	
Sind Datensicherungen vorhanden? - Welche Sicherungsverfahren und -medien existieren? - Sind Sicherungssysteme gesichert bzw. isoliert? - Welche Sicherungsstände (Generationen) liegen vor?	

5 ABLAUF DER FALLANNAHME ÜBER DIE HISCOX KRISENHOTLINE

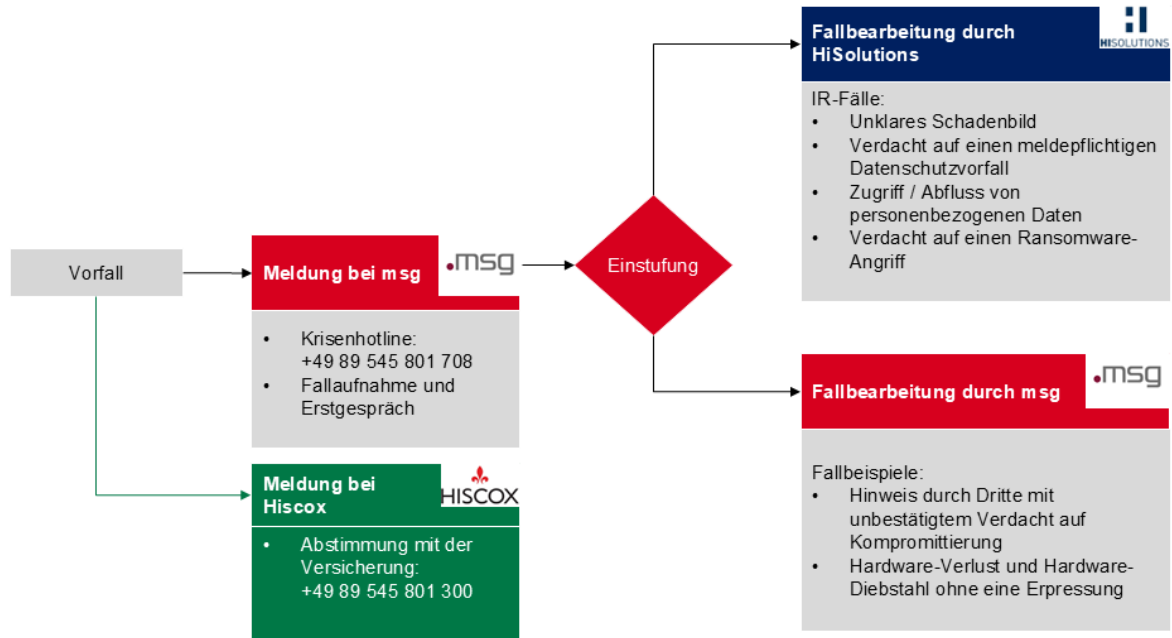


Abbildung 1 Verlauf der Fallannahme ihres Schadensfalls

6 EREIGNISBEWÄLTIGUNG

Nach der Aktivierung des Krisenstabs beginnt dieser mit der aktiven Bewältigung der Krise. Um eine strukturierte Arbeitsweise sicherzustellen, sollten zunächst die folgenden Punkte bearbeitet werden.

Checkliste Sofortmaßnahmen Krisenstab	Beauftragt	Erledigt
1. Ist ein Krisenstab eingerichtet und arbeitsfähig? - Sind alle Funktionen anwesend? - Wurden Arbeitsmaterialien bereitgestellt? - Sind Arbeitsmittel wie z. B. Flipcharts verfügbar?	☐	☐
2. Stellen Sie die Protokollierung sicher. - Nutzen Sie die Protokollvorlage (Seite 34 ff.) - Notieren Sie alle relevanten Informationen und Entscheidung (soweit möglich inkl. Entscheidungsgrundlage). - Notieren Sie die Kontakte/Kontaktversuche zu relevanten Stellen, Dienstleistern und Behörden.	☐	☐
3. Visualisieren Sie zur Übersicht - Organisierung ausreichender digitaler und physischer Arbeitsmittel und Materialien zur Visualisierung - Digital: z.B. Laptop (inkl. Ladekabel und relevantem Zubehör), Beamer - Physisch: z.B. Moderationskoffer, Metaplanwände, Flipcharts, Taktikfolie - Einholen von relevanten Lageinformationen für die Visualisierung - Erstellung des Maßnahmentrackings mit den bereits bekannten Aufgaben	☐	☐
4. Gewährleisten Sie die Kommunikationshoheit - Verpflichten Sie alle Beschäftigten initial zur Geheimhaltung. - Vermeiden Sie unkontrollierte Kommunikation	☐	☐
5. Sammeln Sie alle bekannten Fakten zu dem Ereignis. - Wer und/oder was ist betroffen? - Seit wann besteht der Zustand? - Welche Maßnahmen wurden bereits ergriffen? - Welche Fehlfunktion/en liegt/liegen vor?	☐	☐
6. Wägen Sie ab, ob die Durchführung einer forensischen Analyse bzw. der gerichtsfesten Beweissicherung sowie die Einbeziehung einer Kommunikationsagentur sinnvoll ist. Kontaktaufnahme Krisenhotline: +49 (89) 545 801-708	☐	☐

7. Legen Sie mithilfe der Hinweise aus Kapitel 12 fest, wie und von wem nach extern und intern kommuniziert wird. Nutzen Sie die goldenen Regeln der Krisenkommunikation und ggf. weitere vorbereitete Unterlagen/Maßnahmen (FAQs, Pressemitteilungen, Darksite etc.)	☐	☐
8. Informieren Sie alle Beschäftigten über den Vorfall und über die Kommunikationsstrategie. Informieren Sie die Mitarbeiter so umfassend wie nötig (Was ist passiert? Welche Systeme sind betroffen? Wie wird mit dem Problem umgegangen?).	☐	☐
9. Legen Sie Maßnahmen fest, um den Geschäftsbetrieb aufrechtzuerhalten. Es können unternehmensspezifische initiale Maßnahmen eingetragen werden.	☐	☐
10. Informieren Sie alle externen interessierten Parteien - Geben Sie zielgruppenspezifische Informationen heraus. - Beachten Sie die unterschiedlichen Interessen (ggf. erhalten besondere Kunden detailliertere Informationen als andere) - Prüfen Sie ob die Medien frühzeitig eingebunden werden sollen (proaktive Einbindung) oder nach Priorisierung behandelt werden (Reaktion auf Medienereignisse).	☐	☐
11. Legen Sie langfristige Maßnahmen fest, um den Geschäftsbetrieb aufrechtzuerhalten, bis z. B. die IT wiederhergestellt ist. Analog zum Punkt 9 können unternehmensspezifische, denkbare Maßnahmen (sog. Workarounds) eingetragen werden, um langfristig den Geschäftsbetrieb aufrechtzuerhalten.	☐	☐

Tabelle 4 Checkliste Sofortmaßnahmen Krisenstab

Überprüfen Sie in regelmäßigen Abständen die Wirksamkeit und Notwendigkeit der eingeleiteten Maßnahmen.

Gehen Sie bei der Arbeit im Krisenstab strukturiert vor. Nutzen Sie z. B. den Führungszyklus, der detailliert im Anhang A abgebildet ist.

7 ZEITKRITISCHE PROZESSE/PRODUKTE/DIENSTLEISTUNGEN

Gerade für Unternehmen mit mehreren kritischen Vorgängen, und Anwendungen empfehlen wir dringend die Durchführung zumindest einer vereinfachten Business Impact Analyse in der hier vorgestellten Form. Diese dient dazu, für Sie zeitkritische Vorgänge und die dazu notwendigen Hilfsmittel aufzuzeigen. Zeitkritisch bedeutet, aufgrund ihrer Bedeutung für die Organisation führt ein Ausfall dieser Vorgänge zeitnah zu einem großen bis existenzbedrohenden Schaden.

Für Unternehmen aus dem Mittelstand empfehlen wir, die BIA nicht mehr im vereinfachten Schema durchzuführen und stattdessen die kostenlosen Hilfsmittel des Standards BSI-Standard 200-4: Business Continuity Management zu nutzen. Hinweise und Herleitungen zur Erstellung einer solchen finden Sie im BSI-Standard selbst.

Ein Schaden für die VN kann aus unterschiedlichen Auswirkungen in unterschiedlicher Höhe entstehen. Die folgende Skala hilft der Einordnung und bei der Befüllung der Business Impact Analyse

Auswirkungsklasse 1 - "keine"	Auswirkungsklasse 2 - "gering"	Auswirkungsklasse 3 - "mittel"	Auswirkungsklasse 4 - "groß"
- Keine Verstöße gegen Vorschriften, Verträge und Gesetze	- Verstöße gegen Vorschriften, Verträge und Gesetze mit geringfügigen Konsequenzen	- Verstöße gegen Vorschriften, Verträge und Gesetze mit spürbaren, aber noch tolerierbaren Konsequenzen	- Verstöße gegen Vorschriften, Verträge und Gesetze mit erheblichen, teilweise existenzbedrohenden Konsequenzen
- Keine Beeinträchtigung des Geschäftsbetriebs	- Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. Der durch die Ressource unterstützte Geschäftsprozess bzw. Fachaufgabe kann mit tolerierbarem Mehraufwand mit anderen Mitteln (z.B. manuell) durchgeführt werden.	- Der Geschäftsprozess bzw. die Fachaufgabe kann nur mit erhöhtem Mehraufwand mit anderen Mitteln durchgeführt werden. Die Beeinträchtigung würde von Betroffenen als noch tolerabel eingeschätzt.	- Der Geschäftsprozess bzw. die Fachaufgabe kann ohne die Ressource überhaupt nicht durchgeführt werden. Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden.
- Es ist keine Ansehens- oder Vertrauensbeeinträchtigung zu erwarten	- Eine geringe Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten	- Es sind Ansehens- oder Vertrauensverluste zu erwarten. Diese werden noch akzeptiert.	- Eine sehr hohe Ansehens- oder Vertrauensbeeinträchtigung, evtl. sogar existenzgefährdender Art, ist denkbar.
- Der finanzielle Schaden bleibt für die Institution tolerierbar	- Der finanzielle Schaden bleibt für die Institution tolerabel, aber spürbar	- Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend	- Der finanzielle Schaden ist für die Institution existenzbedrohend

Kritischer Vorgang für Ihr Unternehmen	Auswirkung nach Zeithorizonten				Begründung / Beschreibung	On Premise / In Cloud	Notwendige Daten
	1 Tag	3 Tage	7 Tage	14 Tage			
Produktion Produkt für Kunden							
oder							
Für Kunden erbrachte Dienstleistung							
Kritischer interner Prozess							
Kritische Anwendung							

8 KRITISCHE DATENSICHERUNGEN

Sind die Daten oder Informationen für Prozesse, Produkte oder Dienstleistungen nicht verfügbar, fallen diese zumeist aus. Aus diesem Grund muss bekannt sein, welche Informationen für welche Prozesse/Produkte/Dienstleistungen benötigt werden.

Nr.	Datenbeschreibung	Prozesse/ Produkte/ Dienstleistungen	Ort/ Detail	Backup-Typ/ Zyklus	Ort/ Detail
D1	Produktinformationen	1 Produkt „XY“	Online/ AWS	Vollsicherung/ Woche	Online/ AWS
D2	Kundendaten	3 Dienstleistung „XY“; 4 Prozess „YZ“, ...	Offline/ Storage RZ03	Inkrementelle Sicherung/ Tag	Offline/ Storage RZ03
...					

Tabelle 5 Anforderungen an die Datensicherungen

9 ALARMIERUNG DES KRISENMANAGEMENTS

Die folgende Abbildung zeigt den etablierten Alarmierungsprozess. Wird ein Ereignis als (potenzielle) Krise definiert, ist der Krisenstab zu aktivieren. Wird ein Ereignis zunächst als Störung definiert, die jedoch nicht durch die Fachabteilung behoben werden kann, ist eine Neubewertung durchzuführen und ggf. eine Krise auszurufen.

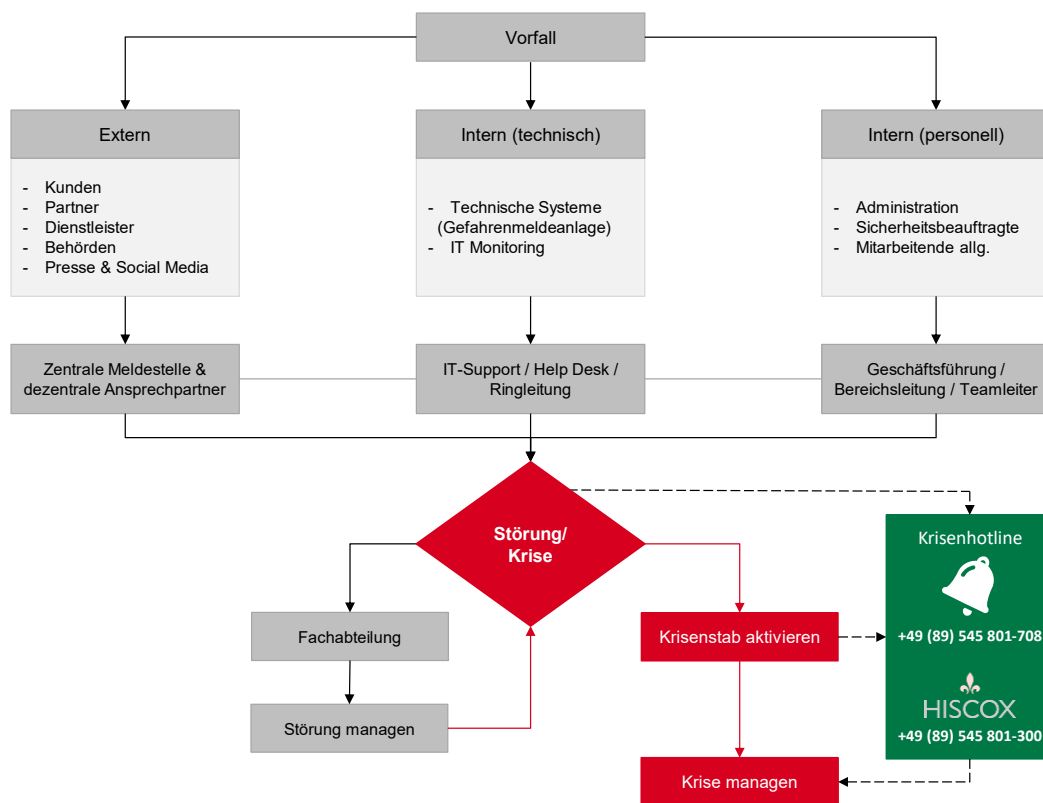


Abbildung 2 Alarmierungsprozess

10 INFRASTRUKTUR

10.1 Standorte

Alle Mitglieder des Krisenstabs finden sich nach der Alarmierung im Krisenstabsraum ein. Sollte der Hauptstandort ausfallen, trifft sich der Krisenstab an einem Ausweichstandort

Hauptstandort	<i>Musterfelder Straße 207b, 3541 Musterstadt</i> <i>Hauptgebäude, 3. Etage, Raum 302</i> <i>Zutritt bei Pförtner anmelden, der die Räume aufschließt und den Sicherheitsdienst informiert</i>
Ausweichstandort	<i>Musterfelder Straße 207b, 3541 Musterstadt</i> <i>Hauptgebäude, 3. Etage, Raum 302</i> <i>Zutritt bei Pförtner anmelden, der die Räume aufschließt und den Sicherheitsdienst informiert</i>

Microsoft Teams-Besprechung	<i>Nehmen Sie auf dem Computer, in der mobilen App oder im Raumgerät teil:</i> <i>Bitte hier den Link zur Teams-Besprechung einfügen.</i> <i>Besprechungs-ID: 333 777 999 333</i> <i>Passcode: 1Krise23</i> <i>Oder rufen Sie an (nur Audio)</i> <i>+49 30 123458800</i> <i>Telefonkonferenz-ID: #1029384756</i>
Remote-Schaltung	<i>Telefonkonferenz 030-12345-8800 PIN: 4590</i>

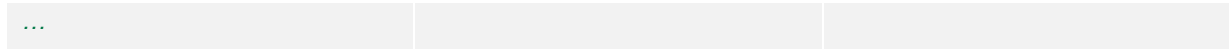
10.2 Arbeitsmittel & Arbeitshilfen

Im Krisenstabsraum wird eine Basisausrüstung vorgehalten, um die Arbeit des Krisenstabs zu ermöglichen. Nach erfolgter Alarmierung sind die aufgeführten Personen dafür verantwortlich diese Ausrüstung zu aktivieren.

Arbeitsmittel und Arbeitshilfen für den Krisenstab		
Bezeichnung	Aufbewahrungsort	Verantwortlich für Beschaffung/Pflege
<i>Laptops</i>		
<i>Beamer (inkl. Verkabelung)</i>		
<i>Metaplanwand</i>		
<i>Flipchart</i>		
<i>Moderationskoffer</i>		
...		
Unterstützende Materialien und Handbücher		
Bezeichnung der mitgeltenden Unterlage	Ablageort	Verantwortlich
<i>Wiederherstellungspläne</i>		
<i>Geschäftsfortführungspläne</i>		
<i>Betriebsanleitungen (z.B. NEA)</i>		
<i>Notfallplan bei Ausfall Dienstleister</i>		
<i>Pandemieplan</i>		

Cyber-Krisenmanagementplan

HiSolutions AG © 2025



11 AUFBAUORGANISATION DES KRISENMANAGEMENTS

Für die Bewältigung einer Krise, die Entwicklung von Handlungsoptionen und das Treffen von Entscheidungen, können unterschiedliche interne (ggf. auch externe) Experten nötig sein. Die Mindestbesetzung des Krisenstabs als zentrales reaktives Gremium besteht aus einer Krisenstabsleitung, den Rollen „Protokoll/Visualisierung“ und dem/der IT-Verantwortlichen bzw. dem IT-Dienstleister. Alle Rollen dieser Mindestbesetzung verfügen über eine Stellvertretung, die im Falle der Abwesenheit oder nicht Erreichbarkeit, über dieselben Aufgaben, Kompetenzen und Verantwortungen – die im Vorfeld dokumentiert wurden – verfügen. Wird der Bedarf an zusätzlichen Kompetenzen identifiziert, werden weitere Rollen durch die Krisenstabsleitung herangezogen.

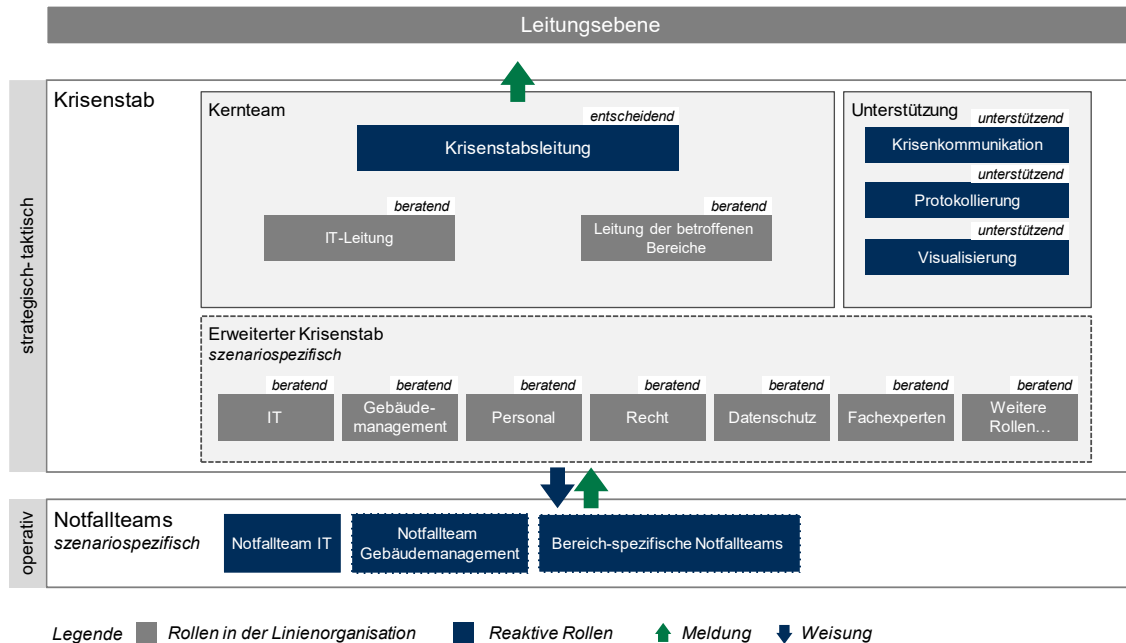


Abbildung 3 Best Practice Aufbau Krisenstab (Bewältigungsorganisation)

Die im Normalbetrieb geltenden Pflichten und Kompetenzen sind auch im Notfall gültig und werden im Vertretungsfall an die festgelegten Personen übertragen. Zusätzliche Pflichten oder Kompetenzen werden im Vorfeld zugewiesen, um eine schnelle Reaktion im Krisenfall zu ermöglichen. Vertretungsregelungen, auch für die festgelegten Rollen, werden in den Kontaktlisten festgehalten (vgl. Anhang B).

11.1 Rollen im Krisenmanagement

Die nachfolgende Tabelle fasst die wichtigsten Aufgaben, Verantwortlichkeiten und Kompetenzen der Mindestbesetzung des Krisenstabs zusammen.

Cyber-Krisenmanagementplan

HiSolutions AG © 2025

Rolle	Aufgaben	Verantwortlichkeiten	Kompetenzen und Befugnisse
Krisenstabsleitung	▪ Kontakt zu Krisenmanagement-Experten herstellen und halten bzw. initiieren ▪ Bestätigen der Krise ▪ Festlegen der Kommunikationsstrategie ▪ Krisenkommunikation	▪ Treffen von Entscheidungen ▪ Abwehr von weiteren Schäden ▪ Geschäftsfortführung sicherstellen ▪ Weisungsbefugnis gegenüber Mitarbeitern ▪ Bereitstellen von Ressourcen ▪ Einbindung weiterer interner Bereiche wie z. B. Recht oder Personal	▪ Entscheidungsbefugnisse (Prokura) ▪ Personalbefugnisse (Weisungsbefugnisse und Zugriff auf Personal)
IT-Leitung	▪ Darstellung des Schadens aus Sicht IT ▪ Fachliche Beratung ▪ Ggf. Kontakt zur Krisenhotline herstellen	▪ Aufzeigen von Handlungsoptionen ▪ Koordination/Durchführung der IT-Wiederherstellungsmaßnahmen	▪ Fachkompetenz ▪ Kenntnis zu vorhandener IT-Betriebs- und Notfalldokumentation
Leitung der betroffenen Bereiche	▪ Folgenabschätzung für den eigenen Bereich ▪ Beratung des Krisenstabsleiters bei der Situations-einschätzung ▪ Mitwirkung in der Maßnahmenentscheidung ▪ Einbringen der Expertise ▪ Ableitung operativer Maßnahmen für die bereichsinternen Notfallteams	▪ Ist innerhalb seines Bereichs und gegenüber den Mitarbeitern weisungsbefugt	▪ Befugnisse gemäß Normalbetrieb.

Tabelle 6 Krisenstab Rollenkarten

Externe Erweiterung	
Rolle	Aufgaben
HiSolutions AG	Im Fall einer Cyber-Krise mit einer konkreten Risikolage (z. B. Hacker-Angriff, Datenmissbrauch etc.), reaktive Unterstützung gemäß den vertraglichen Vorgaben.
Cyber-Krisen-kommunikation	Im Fall einer Cyber-Krise mit einer konkreten Risikolage (z. B. Hacker-Angriff, Datenmissbrauch etc.), reaktive Unterstützung gemäß den vertraglichen Vorgaben. Die Bereitstellung erfolgt in Abstimmung mit der Krisenhotline.

Tabelle 7 Krisenstab externe Erweiterung

11.2 Lagedokumentation und Visualisierung

Die Protokollierung einer Krise sollte frühzeitig beginnen. Im Protokoll müssen alle wichtigen eingehenden Informationen, Entscheidungsgrundlagen und Entscheidungen eingetragen werden. Eine unbeteiligte Person muss den Verlauf der Krise, samt Informationsstand und Entscheidungen des Krisenstabs zu jedem Zeitpunkt nachvollziehen können. Das Protokoll muss im Anschluss an eine Krise durch den/die Schriftführer/in und die Krisenstabsleitung unterschrieben und sicher abgelegt werden. Eine Protokollvorlage ist im Anhang G hinterlegt.

Die Visualisierung stellt sicher, dass alle Informationen übersichtlich aufbereitet allen Mitgliedern des Krisenstabs zur Verfügung stehen. Hierfür sollten geeignete Arbeitsmittel und -hilfen sowie Visualisierungsmethoden zur Verfügung stehen.

12 GRUNDSÄTZE ZUR KRISENKOMMUNIKATION

Bei Eintritt einer Cyber-Krise ist über die in Kapitel „Rollen im Krisenmanagement“ festgelegten Verantwortlichkeiten geregelt, welche Rolle für die zentrale Krisenkommunikation verantwortlich ist und definierte Zielgruppen mit Informationen versorgt. Die Informationstiefe wird situativ entschieden.

Für die initiale interne Kommunikation zur Krise, wie auch zur Aufnahme von Medienanfragen sollten die in Anhang H „Vorlagen Krisenkommunikation“ aufgeführten Vorlagen genutzt werden.

Die goldenen Regeln der Krisenkommunikation

- | | |
|----|---|
| 1. | One voice policy: Mit einer Stimme sprechen. Nur die Geschäftsführung bzw. Krisenstabsleitung sollte nach außen kommunizieren. In jedem Fall gibt die Geschäftsführung bzw. Krisenstabsleitung die Kommunikationsstrategie für alle Beschäftigten vor. |
| 2. | Formulieren Sie aktiv, eindeutig und positiv. |
| 3. | Kommunizieren Sie abgesicherte Fakten und auf keinen Fall Unwahrheiten. |
| 4. | Erzählen Sie offen und ehrlich – aber nicht alles. |
| 5. | Zeigen Sie Verständnis für Ärger oder Ängste betroffener Personen. |
| 6. | Lassen Sie sich nicht unter Druck setzen. |

Die goldenen Regeln der Krisenkommunikation

- | | |
|----|------------------------------------|
| 7. | Unterlassen Sie Schuldzuweisungen. |
|----|------------------------------------|

Tabelle 8 Die goldenen Regeln der Krisenkommunikation

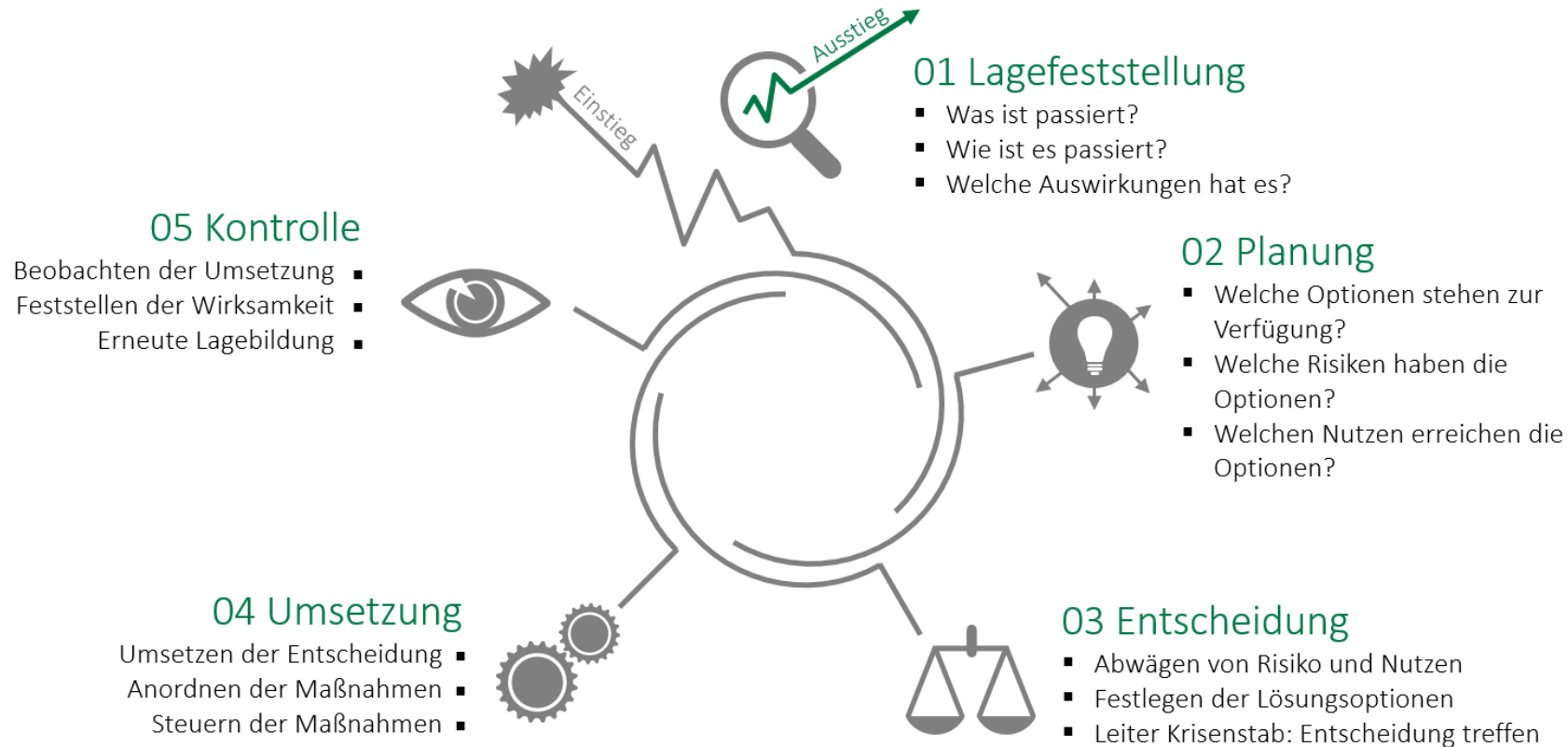
Für den Verlauf der Cyber-Krise sind alle an der Bewältigung beteiligten Personen dahingehend einzuweisen, dass alle Vorfalls- und Statusmeldungen wie z. B.

- Verschärfungen oder Eskalationen des Ereignisses
- Entschärfungen des Ereignisses
- Wesentliche Schritte der Bewältigung (inkl. positivem/negativem Ergebnis)
- Sonstige kommunikationsrelevante Aspekte

unverzüglich und vollständig an den Krisenstab berichtet werden müssen.

Werden externe Stellen (z. B: Polizei, Feuerwehr, Aufsichtsbehörden) direkt informiert, muss hierüber im Anschluss sofort eine Meldung an die Krisenstäbe erfolgen. Ein Kontakt zur Staatsanwaltschaft erfolgt über die Geschäftsleitung, ggf. in Abstimmung mit der Rechtsabteilung.

ANHANG A FÜHRUNGSZYKLUS



ANHANG B WICHTIGE INTERNE ANSPRECHPARTNER

Funktion	Name	Kontaktdaten	Vertreter	Kontaktdaten
Leitung Krisenstab		Telefon: Mobil: E-Mail:		Telefon: Mobil: E-Mail:
Stellv. Leitung		Telefon: Mobil: E-Mail:		Telefon: Mobil: E-Mail:
Protokoll		Telefon: Mobil: E-Mail:		Telefon: Mobil: E-Mail:
Visualisierung		Telefon: Mobil: E-Mail:		Telefon: Mobil: E-Mail:
IT-Verantwortliche/r		Telefon: Mobil: E-Mail:		Telefon: Mobil: E-Mail:
Informationssicherheit		Telefon: Mobil: E-Mail:		Telefon: Mobil: E-Mail:

Funktion	Name	Kontaktdaten	Vertreter	Kontaktdaten
Datenschutz		Telefon: Mobil: E-Mail:		Telefon: Mobil: E-Mail:
Business Continuity Management		Telefon: Mobil: E-Mail:		Telefon: Mobil: E-Mail:
Recht		Telefon: Mobil: E-Mail:		Telefon: Mobil: E-Mail:
Compliance		Telefon: Mobil: E-Mail:		Telefon: Mobil: E-Mail:
Kommunikation		Telefon: Mobil: E-Mail:		Telefon: Mobil: E-Mail:

ANHANG C WICHTIGE EXTERNE KONTAKTE

Kontakt	Name	Kontaktdaten	Vertreter	Kontaktdaten
Lokale Polizeidienststelle		Telefon: Mobil: E-Mail:		Telefon: Mobil: E-Mail:
Landeskriminalamt		Telefon: Mobil: E-Mail:		Telefon: Mobil: E-Mail:
Zentrale Meldestelle für Internetkriminalität		Telefon: Mobil: E-Mail:		Telefon: Mobil: E-Mail:
Feuerwehr		Telefon: Mobil: E-Mail:		Telefon: Mobil: E-Mail:
Krisenhotline		Telefon: +49 (89) 545 801-708		
Hiscox		Telefon: +49 (89) 545-801 300 E-Mail: hiscox.schaden@hiscox.de		
Landesdatenschutz-beauftragter		Telefon: Mobil: E-Mail:		Telefon: Mobil: E-Mail:
[...]		Telefon: Mobil: E-Mail:		Telefon: Mobil: E-Mail:

ANHANG D ANSPRECHSTELLEN CYBERCRIME DEUTSCHLAND

Land/Bund	Telefonnummer	E-Mailadresse/Website
Baden-Württemberg	+49 711 5401-2444	cybercrime@polizei.bwl.de
Bayern	+49 89 1212-3300	zac@polizei.bayern.de
Berlin	+49 30 4664-972972	zac@polizei.berlin.de
Brandenburg	+49 3334 388-8686	zac@polizei.brandenburg.de
Bremen	+49 421 362-19820	cybercrime@polizei.bremen.de
Hamburg	+49 40 4286-75455	zac@polizei.hamburg.de
Hessen	+49 611 83-8377	Kontaktformular auf Website: https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html
Mecklenburg-Vorpommern	+49 3866 64-9494	Kontaktformular auf Website: https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html
Niedersachsen	+49 511 9873-6230	zac@lka.polizei.niedersachsen.de
Nordrhein-Westfalen	+49 211 939-4040	cybercrime.lka@polizei.nrw.de
Rheinland-Pfalz	+49 6131 65-64760	lka.cybercrime@polizei.rlp.de
Saarland	+49 681 962-2448	cybercrime@polizei.slpol.de
Sachsen	+49 351 855-3226	zac.lka@polizei.sachsen.de
Sachsen-Anhalt	+49 391 250-2909	zac.lka@polizei.sachsen-anhalt.de
Schleswig Holstein	+49 431 160 42727	cybercrime@polizei.landsh.de
Thüringen	+49 361 57431-4545	cybercrime.lka@polizei.thueringen.de

Land/Bund	Telefonnummer	E-Mailadresse/Website
Bundeskriminalamt	+49 611 55-15037	Kontaktformular auf Website: https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html

ANHANG E ANSPRECHSTELLEN CYBERCRIME ÖSTERREICH

Institution	Telefonnummer	E-Mailadresse/Website
Bundeskriminalamt - Cyber-Crime- Competence Center (C4)	+43 (0) 800 888 133	against-cybercrime@bmi.gv.at https://www.onlinesicherheit.gv.at/erste_hilfe/startseite.html https://bundeskriminalamt.at/306/
CERT.at	+43 1 5056416-78	reports@cert.at https://cert.at/de/

ANHANG F ANSPRECHSTELLEN CYBERCRIME SCHWEIZ

Institution	Telefonnummer	E-Mailadresse/Website
Nationales Zentrum für Cybersicherheit (NCSC, ehem. MELANI)		https://www.ncsc.admin.ch/ incidents@ncsc.ch
Kantonspolizei Zürich Abteilung Cybercrime	+41 58 648 48 48	Formular auf Website https://www.cybercrimepolice.ch/ http://www.kapo.zh.ch
Kantonspolizei Bern Kriminalabteilung Dezernat Wirtschaftsdelikte	+41 31 638 81 11	Formular auf Website http://www.police.be.ch
Bundesamt für Polizei fedpol		http://www.fedpol.admin.ch
Police cantonale vaudoise Brigade Analyse Traces Technologiques - Division Enquête Cyber	+41 (0)21 644 44 44	info.police@vd.ch https://votrepolice.ch/cybercriminalite/
Kantonspolizei Schwyz Fachbereich Cybercrime	+41 41 819 29 29 (24h)	cybercrime.polizei@sz.ch http://www.sz.ch/polizei

ANHANG G PROTOKOLLVORLAGE

Ereignis	
Auftreten/Erkennen des Ereignisses	
Beginn der Protokollierung	
Besetzung der Rolle Protokoll	
Unterschrift Protokoll	
Unterschrift Leitung Krisenstab	

Mitglieder im Krisenstab			
Rolle	Name	Anwesend	
		von	bis
Leitung Krisenstab			
Protokoll/Visualisierung			
IT-Verantwortliche/r			
(...)			

Protokollvorlage Ereignis: _____ Datum: _____ Zeit: _____		
Nr.	Uhrzeit	Aktivität/Ereignis/Anmerkung
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		

ANHANG H VORLAGEN KRISENKOMMUNIKATION

H.1 Meldung an interne Mitarbeiter

Interne Information an alle Mitarbeiter, dass es zum vorliegenden Ereignis eine zentral gesteuerte Kommunikation an die Kunden und andere externe Stellen gibt.

Vertraulich!

Sehr geehrte Kolleginnen und Kollegen,

am <Wochentag>, den <TT.MM.JJJJ> um <HH:MM> Uhr, hat es in unserer IT-Umgebung eine Störung gegeben.

Ich möchte Sie darüber informieren, dass diese Störung als Krise eingestuft wurde. Der für diesen Fall obligatorische Krisenstab wird bereits einbestellt.

Bitte beachten Sie, dass die weitere Kommunikation an Kunden und Geschäftspartner ausschließlich über die Geschäftsleitung gesteuert wird.

Mit freundlichen Grüßen,

<Name, Vorname>

Leiter des Krisenstabs

English version

Confidential!

Dear colleagues,

There was an incident in our IT environment, on [weekday], <DD/MM/YYYY>, at <HH:MM> a.m./p.m.

I wish to inform you that this incident has been classified as a major incident. The crisis team have already been summoned.

Please note that further communication with clients and business partners will be carried out exclusively via the Executive Board.

Kind regards,

<Name>

Head of crisis team

H.2 Kundenmeldung Unterbrechung der Leistungen

Sehr geehrter <Kundenname>,

bedauerlicherweise besteht zurzeit eine Störung unserer IT-Umgebung. Unsere Leistungen entsprechen daher momentan nicht der von Ihnen gewohnten Qualität. Da wir Sie zeitnah informieren möchten, senden wir Ihnen eine erste Einschätzung zur voraussichtlichen Dauer der Störung.

Art der Störung: <bspw. Kundenportal Verbindung gestört>

Auswirkungen: <bspw. Kundenportal steht teilweise nicht zur Verfügung>

Beginn der Störung: <TT.MM.JJJJ> um <HH:MM> Uhr

Voraussichtliches Ende der Störung: <TT.MM.JJJJ> um <HH:MM> Uhr <bspw. Zurzeit ist eine Einschätzung für das Ende der Störung nicht möglich, Sie erhalten hierzu zeitnah weitere Informationen.>

Eingeleitete Aktionen: <bspw. Problemlösung durch Second-Level Support>

Referenznummer für Rückfragen: <Wenn Ticketsystem genutzt wird, kann darauf verwiesen werden>
Wir bedauern die Beeinträchtigung und arbeiten mit allen verfügbaren Kräften an der Fehlerbehebung. In Bezug auf den aktuellen Stand der Veränderungen halten wir Sie auf dem Laufenden. Wir bitten um Ihr Verständnis.

Mit freundlichen Grüßen

<Kunden Service>

<Adresse>, <E-Mail-Adresse>, <Telefon>, <Website>, <übliche Signatur>

English version

Dear <customer name>,

Unfortunately, there is currently a disruption in our IT environment. Therefore, our services currently do not correspond to the quality you are used to. As we would like to inform you immediately, we will send you an initial estimate of the expected duration of the disruption.

Type of incident: <e. g. onlineshop connection disrupted>

Impact: <e. g., application is partially not available>

Start of incident: : <TT.MM.JJJJ>, <HH:MM>

Estimated end of incident: : <TT.MM.JJJJ>, <HH:MM>, <e. g., It is currently not possible to estimate when the incident will end. We will provide you with further information as soon as possible.>

Actions initiated: <e. g., troubleshooting with second level support>

Reference number for inquiries: <When ticket system is used, it can be referred to>

We wish to apologize for any impact this may have on your services. We are directing all of our available resources into resolving the error. We will make sure to keep you up to date and inform you if anything changes. Thank you for your patience.

Kind regards,

<Customer Service>

<Address>, <E-Mail-address>, <Phone>, <Website>, <Common Signatur>

H.3 Muster für Journalistenanfragen

Auskünfte an Journalisten müssen entsprechend der definierten Vorgaben von der entsprechenden Stelle des Krisenstabs, dem Krisenstabsleiter oder der Geschäftsführung freigegeben werden

Vorname und Name des aufnehmenden Mitarbeiters

Tel: _____

E-Mail: _____

Journalistenanfrage

Anfrage vom:

Medium:

Name:

Telefon:

E-Mail:

Inhalt:

Termin:

weitergeleitet an: <Organisationseinheit und Name>

Freigabe durch:

Folgende Auskunft gegeben – wie (schriftlich, mündlich) und wann (Datum):

H.4 Fragen und Antworten (FAQs)

Frage	Antwort(en)
Es heißt, das Unternehmen ist von einem Cyber-Angriff betroffen. Was ist passiert?	Das ist leider richtig. Das Unternehmen ist Opfer eines kriminellen Cyber-Angriffs geworden. Seit heute <Datum> wissen wir, dass von unseren Systemen <Web- und Mailzugangsdaten von Kunden> entwendet worden sind.
Wie hat das Unternehmen von dem Vorfall erfahren?	Unser Frühwarnsystem hat heute verdächtige Vorgänge gemeldet. Daraufhin wurden automatisch intensive Überprüfungen durch unsere IT-Spezialisten eingeleitet, zu der gesicherten Erkenntnis führten, dass <Vorfall>.
Um welche Daten handelt es sich?	- Es handelt sich um: <Kontodaten> <E-Mail-Adressen, etc.>
Welche Maßnahmen zum Schutz Ihrer Systeme haben Sie getroffen?	Wir verfügen über sehr hohe Sicherheitsstandards. Eine hundertprozentige Sicherheit kann jedoch aufgrund möglichen individuellen menschlichen Versagens oder krimineller Energie niemals garantiert werden. Selbstverständlich werden wir die Erkenntnisse aus dem aktuellen Fall analysieren und in unser Sicherheitskonzept einfließen lassen.
Wie konnte es zu so einem Vorfall kommen? Hat das Unternehmen zu wenig Wert auf Sicherheitsmaßnahmen gelegt?	Wir legen höchsten Wert auf bestmöglichen Schutz der Daten unserer Kunden. Die Sicherheitsmaßnahmen werden laufend überprüft und angepasst. <Beispielsweise haben wir im vergangenen Jahr etwa das neue Frühwarnsystem installiert, das bei diesem Angriff auch sofort funktioniert hat.> Aber gegen einen komplexen Angriff, wie er nun erfolgt ist, gibt es leider keinen hundertprozentigen Schutz.
Wie viele und welche Kunden sind betroffen?	Das lässt sich zum aktuellen Zeitpunkt nicht seriös beantworten. Der <Anbieter für Produktbeschreibung, Dienstleistungsbeschreibung> in <Land> und hat in diesem Bereich <Anzahl> Kunden. Wie viele davon betroffen sind, können wir derzeit nicht abschätzen.

Frage	Antwort(en)
Wurden die Betroffenen schon informiert? Was haben Sie ihnen gesagt?	Wir bedauern die Vorkommnisse natürlich sehr und haben die betroffenen Unternehmen und Personen umgehend über den Vorfall informiert. Wir konnten ihnen versichern, dass die Sicherheitslücke inzwischen geschlossen ist. Sollte ein Schaden entstanden sein, werden wir dies prüfen und entsprechend dafür aufkommen.
Wieso habe ich als Kunde von diesem Hackerangriff erst aus den Medien erfahren bzw. noch keine Nachricht von Ihnen erhalten?	- Wir sind dabei, die kompromittierten Server neu aufzusetzen und die Sicherheitsmaßnahmen drastisch zu erhöhen – das nimmt leider einige Zeit in Anspruch. - Die Information an unsere Kunden ist in Vorbereitung – allerdings müssen die technischen Voraussetzungen gegeben sein, um die aktuelle Situation zu klären. Sobald dies erreicht ist, werden unsere Kunden umgehend informiert und erhalten genaue Anweisungen, wie sie ihren Account wieder sicher nutzen können.
Warum sind Sie nicht schon früher an die Öffentlichkeit gegangen bzw. haben die Kunden informiert?	- Die Analyse, was bei einem Hackerangriff tatsächlich passiert und welcher Schaden entstanden ist, ist leider sehr komplex und zeitaufwendig. - Sobald wir gesichertes Wissen über den Vorfall erlangt haben, werden wir unsere Kunden umgehend informieren.
Was können Sie darüber sagen, wie die Daten möglicherweise missbraucht werden können?	- Wir wissen, dass von unseren Servern Daten entwendet worden sind. Bislang ist uns noch keine missbräuchliche Verwendung der entwendeten Daten bekannt, sie kann aber nicht ausgeschlossen werden. - Wir können auch nicht ausschließen, dass weitere Daten entwendet wurden. Fakt ist, dass wir mit Hochdruck daran arbeiten, gemeinsam mit unseren Kunden weitere verschärfte Sicherheitsmaßnahmen einzuführen.

ANHANG I BEGRIFFE

Unterbrechungen von Geschäftsprozessen können unterschiedliche Ursachen und Auswirkungen haben. Um zu verdeutlichen, welche Schadensereignisse im Rahmen eines Notfallmanagements betrachtet werden, folgt an dieser Stelle eine kurze Erläuterung der Begriffe „Störung“, „Notfall“ und „Krise“, wie sie im Rahmen des Standards BSI 200-4 des deutschen Bundesamtes für Sicherheit in der Informationstechnik verstanden werden.

I.1 Störung

Eine Störung ist eine Situation, in der Prozesse oder Ressourcen nicht wie vorgesehen zur Verfügung stehen. Störungen werden in der Regel innerhalb des Normalbetriebs durch die AAO (Allgemeine Aufbauorganisation) der Institution behoben. Hierzu wird auf vorhandene Prozesse zur Störungsbeseitigung oder des Vorfalldmanagements (auch Incident-Management genannt) zurückgegriffen. Daher sind Störungen nicht Betrachtungsgegenstand dieses Standards. Störungen können jedoch zu einem Notfall eskalieren, wenn sie nicht in einer angemessenen Zeit behoben werden können.

I.2 Notfall

Ein Notfall im Sinne dieses Standards ist eine Unterbrechung des Geschäftsbetriebs, die mindestens einen zeitkritischen Geschäftsprozess betrifft, der nicht im Normalbetrieb innerhalb der maximal tolerierbaren Ausfallzeit wiederhergestellt werden kann. Im Gegensatz zu Störungen wird zur Bewältigung von Notfällen eine BAO (Besondere Aufbauorganisation) benötigt. Im Gegensatz zur Krise liegen geeignete Pläne zur Bewältigung vor oder bestehende Pläne können adaptiert werden. Der Notfall kann auch ausgerufen werden, bevor das Schadensereignis zu einer Unterbrechung des Geschäftsbetriebs führt, um schnell reagieren zu können. Es genügt die Gefahr, dass durch das Schadensereignis der Geschäftsbetrieb unterbrochen wird.

I.3 Krise

Als Krise im Sinne dieses Standards wird ein Schadensereignis bezeichnet, das sich in erheblicher Weise negativ auf die Institution auswirkt und dessen Auswirkungen auf die Institution nicht im Normalbetrieb bewältigt werden können. Im Gegensatz zu einem Notfall liegen zur Bewältigung einer Krise jedoch keine spezifischen Notfallpläne vor. Vorhandene Notfallpläne können nicht oder nur bedingt adaptiert werden oder greifen schlicht nicht. Innerhalb der Institution wird die Krise durch eingeleitete Maßnahmen der BAO bewältigt.

KONTAKT

HiSolutions AG

Schloßstraße 1

12163 Berlin

info@hisolutions.com

www.hisolutions.com

Fon +49 30 533 289 0

Fax +49 30 533 289 900

Standort Frankfurt am Main

Design Offices
Wiesenhüttenplatz 25
60329 Frankfurt am Main

Fon +49 30 533 289 0
Fax +49 30 533 289 900

Standort Bonn

Friedrich-Breuer-Straße
19
53225 Bonn

Fon +49 228 52 268 175
Fax + 49 30 533 289 900

Standort Nürnberg

Design Office
Bahnhofstraße 2 | 3. OG
90402 Nürnberg

Fon +49 911 8819 7263
Fax + 49 30 533 289 900

Standort Wien

HiSolutions AT GmbH
Ungargasse 37
AT-1030 Wien

Fon +49 30 533 289-0
Fax + 49 30 533 289-900

Rechtliche Hinweise

© 2025

Weitergehende Veröffentlichungen, Nachdruck, Vervielfältigungen oder Speicherung - gleich in welcher Form, ganz oder teilweise - sind nur mit Zustimmung von HiSolutions/Hiscox zulässig. Ebenso darf diese Dokumentation Dritten gegenüber nur mit ausdrücklicher Zustimmung von HiSolutions/Hiscox oder entsprechend den zwischen HiSolutions/Hiscox und dem Kunden/Auftraggeber getroffenen Regelungen weitergegeben werden.