

LEITFADEN CYBER RISK AND CRISIS MANAGEMENT

INHALTSVERZEICHNIS

1	EINLEITUNG UND ÜBERBLICK CYBER RISK MANAGEMENT	2
1.1	Zielsetzung und Verwendungszweck	2
1.2	Bestimmen eines zentralen Themenverantwortlichen	2
1.3	Etablieren eines Cyber Risk Managements	2
2	EINSCHÄTZUNG CYBER-KRISE	4
3	ROLLEN UND AUFGABEN IN DER KRISENBEWÄLTIGUNG	4
4	CHECKLISTEN ZUM KRISENMANAGEMENT	5
4.1	Checkliste Krisenstab	5
4.2	Checkliste IT-Vorfall	6
5	HILFSMITTEL UND VORLAGEN	8
5.1	Kopiervorlage Krisendokumentation	8
5.2	Kontaktlisten intern	8
5.3	Kontaktlisten extern	8
	KONTAKT	8

1 EINLEITUNG UND ÜBERBLICK CYBER RISK MANAGEMENT

1.1 Zielsetzung und Verwendungszweck

Der vorliegende Leitfaden soll Ihnen als Orientierung für die Etablierung eines Cyber Risk Managements dienen. Hierfür werden wesentliche Aspekte und Maßnahmen beschrieben, die Ihnen eine geeignete Prävention und Reaktion auf IT-bezogene Angriffe, inklusive der Entwicklung eines Krisenplans, ermöglichen.

Die präventiven (Kapitel 1) und reaktiven Aspekte (Kapitel 2-5) werden getrennt beschrieben. Der reaktive Teil soll Sie vor allem bei der Behandlung von Cyber-Krisen unterstützen und kann somit als separate Anleitung zum Krisenmanagement genutzt werden. Hier sind die grundlegenden Informationen, Checklisten und Vorlagen für den Ernstfall enthalten, die hinsichtlich der individuellen Bedürfnisse und Gegebenheiten ergänzt werden sollten. Für die individuelle Anpassung finden Sie in den einzelnen Kapiteln kurze Hinweise, die nach der Bearbeitung entfernt werden können. Eine digitale Version dieses Planes zur weiteren Bearbeitung erhalten Sie per Anfrage über die folgende Adresse: anfrage-hiscox@hisolutions.com.

Anschließend sollte das fertig bearbeitete Dokument an einer sicheren Stelle in elektronischer und gedruckter Form aufbewahrt werden.

1.2 Bestimmen eines zentralen Themenverantwortlichen

Ein effektives Cyber Risk Management betrifft unterschiedliche Bereiche und involviert verschiedene Rollen innerhalb einer Organisation. Je nach Organisationsstruktur sollte die Leitung daher einen zentralen Ansprechpartner benennen, der die relevanten Bereiche zusammenführt sowie die Durchführung und Weiterentwicklung der einzelnen Aspekte koordiniert. Dazu zählen unter anderem die folgenden Kernaufgaben:

- Erstellen von Leit- bzw. Richtlinien und Verfahrensanweisungen für Mitarbeiter
- Etablieren eines allgemein bekannten Eskalationsprozesses bei Verdachtsfällen
- Initiieren der regelmäßigen Aktualisierung der Sicherheitsinfrastruktur (bspw. Firewall, Virens Scanner etc.)
- Sensibilisieren der Mitarbeiter in Bezug auf Gefahren durch die Nutzung der Informationstechnik

1.3 Etablieren eines Cyber Risk Managements

Für die effektive Bewältigung von Cyber-Krisen greift das Krisenmanagement auf unterschiedliche Strukturen zurück und bündelt die existierenden Informationen und Ressourcen der Organisation. Für eine umfassendere Berücksichtigung von Cyber-Risiken im Allgemeinen sowie eine angemessene Prävention von Cyber-Krisen im Speziellen, ist daher die Etablierung folgender Kernfunktionen besonders erwägenswert.

Kernfunktion	Beschreibung und Leitfragen
Identifizieren	Entwickeln eines organisationsbezogenen Verständnisses für das Management von Risiken für Systeme, Informationen, Daten oder sonstige Werte. • Werden physikalische Geräte und Systeme sowie Software und Applikationen innerhalb der Organisation inventarisiert? • Werden externe Informationssysteme katalogisiert? • Liegt eine Leitlinie zur Informationssicherheit vor? • Sind Risikomanagementprozesse zur Identifizierung, Analyse und Bewertung von Bedrohungen und Schwachstellen etabliert?
Schützen	Entwickeln von Fähigkeiten zur Begrenzung der negativen Auswirkungen von sicherheitsrelevanten Ereignissen. • Sind der Zugang zu und Zugriff auf die identifizierten Werte für autorisierte Benutzer geregelt sowie die autorisierten Aktivitäten definiert? • Werden für Mitarbeiter und Geschäftspartner Sensibilisierungs- und Weiterbildungsmaßnahmen in Bezug auf Cyber-Sicherheit durchgeführt? • Werden Informationen und Aufzeichnungen (Daten) kategorisiert und entsprechend verwaltet, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu schützen? • Werden regelmäßig Wartungen und Reparaturen von Steuerungs- und Informationssystemkomponenten durchgeführt und protokolliert? • Sind Kommunikations- und Steuerungsnetze ausreichend geschützt? • Sind angemessene Schutzmaßnahmen nach dem Stand der Technik etabliert (z. B. Netztrennung, Firewalls, Virenschutz, Backup, ...)
Erkennen	Entwickeln und Umsetzen von geeigneten Maßnahmen, die eine verzugsfreie Identifikation von sicherheitsrelevanten Ereignissen ermöglicht. • Liegen geeignete Strukturen vor, um anormale Aktivitäten in angemessener Zeit festzustellen und hinsichtlich der potenziellen Auswirkungen zu analysieren? • Werden Netzwerk, physische Umgebung, Aktivitäten des Personals und von externen Dienstleistern überwacht (Monitoring), um potenzielle sicherheitsrelevante Ereignisse zu identifizieren? • Werden regelmäßig Schwachstellen-Prüfungen (Scans) durchgeführt?
Reagieren	Entwickeln von reaktiven Strukturen zur Bewältigung und Eingrenzung der Auswirkungen von sicherheitsrelevanten Ereignissen. • Sind Aktivitäten definiert, um das Schadensausmaß eines Ereignisses und dessen Expansion zu verhindern bzw. das Ereignis zu bewältigen? • Werden im Rahmen der Bewältigungsmaßnahmen die Information und Kommunikation der internen und externen Anspruchsgruppen berücksichtigt? • Wird die Eignung der Bewältigungsstrukturen im Rahmen der kontinuierlichen Verbesserung und aufgrund gewonnener Erkenntnisse bewertet?
Wiederherstellen	Entwickeln von Plänen zur Aufrechterhaltung der Geschäftstätigkeit und Wiederherstellung von beeinträchtigten Systemen oder Services sowie Rückführung in den Normalbetrieb. • Liegt ein Notfallkonzept vor, in dem Verfahren für die Aufrechterhaltung der Geschäftsfähigkeit, Wiederherstellung von beeinträchtigten Systemen oder Services sowie die Rückführung in den Normalbetrieb definiert werden?

2 EINSCHÄTZUNG CYBER-KRISE

[Hinweis: Die nachfolgende Checkliste dient als Orientierung zur Beantwortung der Frage, ob eine Cyber-Krise vorliegt. Je nach Organisationsstruktur sollten hier ggf. weitere Kriterien oder Definitionen ergänzt werden, um festzulegen, wann dieser Plan und die damit verbundene besondere Aufbauorganisation aktiviert werden.]

Eine Krise liegt vor, wenn mindestens eine der folgenden Fragen mit „ja“ beantwortet werden muss:

Nr.	Lage	Zutreffend?
1	Ein IT-Ausfall bedroht oder stört den Geschäftsbetrieb erheblich	☐
2	Ein erfolgreicher schwerwiegender Hackerangriff ist erfolgt	☐
3	Ein schwerwiegender IT-basierter Betrugsfall ist aufgetreten	☐
4	Vertrauliche Daten sind in erheblichem Maß abgeflossen	☐
5	Es wurde ein meldepflichtiger Gesetzesverstoß begangen	☐
6	Reputationsschäden durch Negativnachrichten sind zu erwarten	☐

Bei Vorliegen einer Krise – auch nur im Verdachtsfall – bitte die HiSolutions-Krisenhotline informieren unter der Telefonnummer:

+49 (30) 533 289-555

Anschließend ist die Krisenbewältigung mithilfe der Anweisungen in den nächsten Kapiteln einzuleiten.

3 ROLLEN UND AUFGABEN IN DER KRISENBEWÄLTIGUNG

[Hinweis: Für die Bewertung der Lage, die Entwicklung von Handlungsoptionen sowie das Treffen von Entscheidungen sind unterschiedliche interne und ggf. auch externe Experten erforderlich. Diese sollten vorab identifiziert werden und anschließend mit den jeweiligen Kompetenzen, Aufgaben und Verantwortlichkeiten im Krisenplan dokumentiert werden. Üblicherweise kommen bei IT-basierten Krisenszenarien die folgenden Rollen in Betracht: Krisenstabsleiter, Recht, Datenschutz, IT, Kommunikation.]

Rolle	Aufgabe	Besetzung / Vertretung
n.n.	- tbd	- tbd

4 CHECKLISTEN ZUM KRISENMANAGEMENT

4.1 Checkliste Krisenstab

Ein Krisenstab ist eine Personengruppe, die zur Lösung von Not- und Krisenfällen gebildet wird. Der Stab wird für die Dauer der Krise mit besonderen Berechtigungen ausgestattet, um schnell handlungsfähig zu sein. Diese Checkliste wird beim ersten Treffen des Krisenstabs verwendet und soll (a) eine allgemeine Struktur vorgeben und (b) die wichtigsten Punkte für alle Vorfälle abdecken, denen sofortige Aufmerksamkeit gewidmet werden muss. Auf Grundlage dieser Checkliste getroffene Einschätzungen sollten sowohl zu Beginn einer Krise als auch in regelmäßigen Abständen während der Krise durch erneutes Abarbeiten der Liste überprüft werden, insbesondere dann, wenn neue Informationen vorliegen oder wesentliche Entscheidungen anstehen.

Checkliste Krisenstab		
Erste Schritte	Erledigt	Nicht anwendbar
1. Zusammenfassen der bekannten Fakten der Krise	☐	☐
2. Zusammenfassen jeglicher bisher ergriffener Maßnahmen	☐	☐
Strategie	Erledigt	Nicht anwendbar
3. Krisenstab zusammensetzen und Handlungsfähigkeit überprüfen: a. Leiter des Krisenstabs b. Krisenstabsmitglieder aus den betroffenen Fachbereichen	☐ ☐ ☐	☐ ☐ ☐
4. Vereinbaren der grundlegenden Krisenmanagementstrategie, Ordnen von Zielen nach Prioritäten	☐	☐
Organisation	Erledigt	Nicht anwendbar
5. Festlegen der ereignisbezogenen Aufgaben/Aufteilung auf Rollen und Funktionen, sofern nicht präventiv geschehen	☐	☐
6. Sicherstellung der Protokollierung	☐	☐
7. Erschließen aller benötigten Schnittstellen und Informationsquellen	☐	☐
8. Verpflichtung aller Beteiligten zur Geheimhaltungswahrung (inkl. Dokumentation)	☐	☐
Lagebeurteilung und -bearbeitung	Erledigt	Nicht anwendbar
9. Klären, ob alle aktuellen Fakten zusammengetragen sind	☐	☐
10. Lagebeurteilung durch den Krisenstab: - Betrachten der bisher getroffenen Sofortmaßnahmen: Bestätigung oder Ergänzung(en) notwendig? - Festlegung möglicher Vorgehensweisen/Maßnahmen, die bereits zugeordnet wurden	☐	☐
11. Entwickeln möglicher Szenarien (beste/wahrscheinlichste/schlechteste Entwicklung)	☐	☐

4.2 Checkliste IT-Vorfall

Seite 6

4. Abwägen, ob ein qualifizierter Dienstleister mit der Durchführung einer forensischen Analyse bzw. der gerichtsfesten Beweissicherung beauftragt werden soll. Kontakt: HiSolutions, +49 (30) 533 289-555	☐	☐
Aufgaben der Sicherheitsvorfallbehandlung	Erledigt	Nicht anwendbar
5. Eindämmung als kurzfristige Aktion (Ziel: Unterbindung des weiteren Zugangs zum kompromittierten System, Vermeidung weiterer Schäden, Begrenzung des entstandenen Schadens)	☐	☐
6. Bereinigung als mittel- bis langfristige Aktion, um gleichartige Vorfälle zukünftig zu verhindern	☐	☐
7. Wiederherstellung als unmittelbare Maßnahme vor Aufnahme des Systembetriebs a. Festlegung der Anforderungen für die Wiederaufnahme (Rückgriff auf die Wiederanlaufpläne) b. _____	☐	☐

5 HILFSMITTEL UND VORLAGEN

5.1 Kopiervorlage Krisendokumentation

Jede Cyber-Krise wird in nachstehendem Formular dokumentiert. Dies ist insbesondere für die spätere Nachvollziehbarkeit der Handlungen während der Cyber-Krise erforderlich. In die Kopiervorlage werden neben den Namen der handelnden Personen Lageinformationen und Beschlüsse aufgrund der Lage fortlaufend erfasst. Das sich hieraus ergebende Tagebuch stellt damit den Verlauf der Cyber-Krise dar. Mit Beendigung der Cyber-Krise wird das Tagebuch abgeschlossen und sicher verwahrt. Für die Dokumentation der Cyber-Krise kann folgendes Tabellenlayout benutzt werden:

Tabellenvorlage in der elektronischen Version enthalten.

5.2 Kontaktlisten intern

Tabellenvorlage in der elektronischen Version enthalten.

5.3 Kontaktlisten extern

Tabellenvorlage in der elektronischen Version enthalten.

KONTAKT

HiSolutions AG

Fon +49 30 533 289 0

anfrage-hiscox@hisolutions.com

HiSolutions AG

Bouchéstraße 12

12435 Berlin

www.hisolutions.com