Online-Talk
"Cyber-Notfallplan für Hoteliers: Soforthilfe und Prävention bei Hackerangriffen“

05. Dezember 2024


Thomas Neusser

oehv.at

hoteliervereinigung
oehv.hoteliervereinigung
österreichische-hoteliervereinigung

FÜRWÄRTS. DIE ÖHV.

Agenda

- Notfallhandbuch
- Incident Response
- Meldepflichten
- Backup Konzept
- Busines Continuity Management
- Learnings
- To Do‘s

Notfallhandbuch

Ein Notfallhandbuch ist eine Ressource, die eine Reihe **kognitiver Hilfsmittel** oder **Checklisten** enthält, die für einen bestimmten klinischen Kontext relevant sind.

Das Notfallhandbuch wird in der Regel durch den BCM-Beauftragten erstellt. Es beinhaltet alle Aspekte zur **Notfallbewältigung** und kann auch zur **Krisenbewältigung** genutzt werden.

Ein Notfallhandbuch soll alle (realistisch) möglichen Notfälle abdecken. Dazu ist es notwendig, die **denkbaren Risiken** zu ermitteln.

Es enthält Informationen über die verschiedenen Arten von Notfällen, die auftreten können, sowie die entsprechenden Maßnahmen, die ergriffen werden müssen.

Beispiele

- Alarmierung und Eskalation
- Sofortmaßnahmen
- Geschäftsfortführung (BCM)
- Wiederherstellung
- Überführung in den Normalbetrieb
- Deeskalation
- Analyse und Bewertung des Vorfalles
- Aktualisierung des Notfallhandbuches

Incident Response

- Incident Response (manchmal auch Cybersecurity Incident Response genannt) bezieht sich auf die Prozesse und Technologien einer Organisation zum Erkennen und Reagieren auf Cyberbedrohungen, Sicherheitsverletzungen oder Cyberangriffe . Ein formeller Incident-Response-Plan ermöglicht es Cybersicherheitsteams, Schäden zu begrenzen oder zu verhindern.
- Reaktionszeit, Systemdokumentation, Verantwortliche, Backup

Cyber-Security Know-How

Arbeitsaufwand steigt

Anzahl und Komplexität der Attacken steigt

Geringe Security-Budgets

Personalmangel

VS

Angreifer spezialisieren sich

Spezialisierte Lieferketten

Cyber-Angriffe als Business-Model

Keine Strafverfolgung

Recruiting für Bedrohungsakteure

Meldepflichten

- Die Berichtspflichten laut NIS2 bei erheblichen Sicherheitsvorfällen(*) und signifikante Bedrohungen lauten wie folgt:
  - Frühwarnung (Verdacht): Unverzüglich bis max. 24 Stunden nach Kenntnisnahme
  - Meldung (erste Bewertung): Unverzüglich bis max. 72 Stunden nach Kenntnisnahme
  - Abschlussmeldung (ausführliche Beschreibung): 1 Monat nach Meldung

- (*) Ein Sicherheitsvorfall ist „erheblich“, wenn er schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann, bzw. er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

Kommunikationsaspekte

- Interne Benachrichtigung
- Gesetzlicher Meldepflichten – Datenschutzbehörde
- Versicherung
- Auftraggeber/Lieferanten/Partner
- Kunden – Öffentlichkeitsarbeit/Presse
- Exekutive – Strafanzeige
- Austausch mit CERT
- Meldestelle für Internetkriminalität:
  - E-Mail: against-cybercrime@bmi.gv.at

Backup Konzept

- Das Backup-Konzept enthält alle technischen und organisatorischen Maßnahmen zum Schutz von IT-Systemen und Daten vor Verlust oder Missbrauch sowie den Ablaufplan von Datensicherung und -wiederherstellung im Katastrophenfall.
- Die **3-2-1-Sicherungsstrategie** besagt einfach, dass Sie drei Kopien Ihrer Daten (Ihre Produktionsdaten und zwei Sicherungskopien) auf zwei verschiedenen Medien (Festplatte und Band) haben sollten, wobei sich eine Kopie für die Notfallwiederherstellung an einem externen Standort befindet .
- Zum Erstellen eines effektiven Sicherungsplans gehören die Ermittlung der kritischen Daten, die Auswahl einer geeigneten Lösung, die Erstellung eines Zeitplans für die Sicherungen und deren regelmäßige Tests .

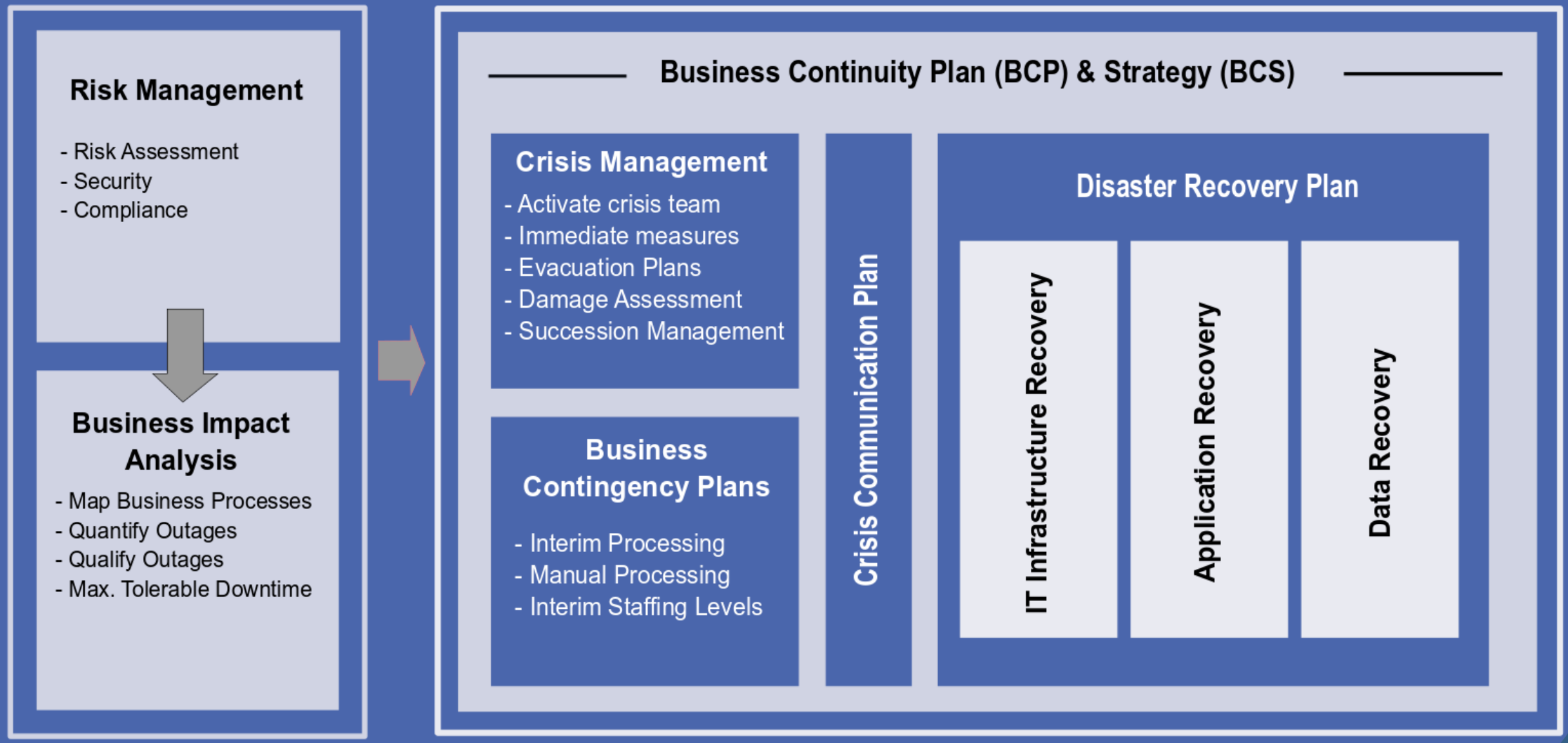
EINZIG WICHTIGE FOLIE

Best practice	Implementierung
Unveränderbar	▪ Write-only
Unabhängig	▪ Eigene Infrastruktur
Isoliert	▪ komplett getrenntes IAM ▪ KEINESFALLS im Active Directory
Versioniert	▪ inkrementell
Verifiziert	▪ regelmäßige Ende-zu-Ende-Prüfung
Überwacht	▪ Erfolg ▪ Integrität
Risiko-basiert	▪ Wiederherstellung des Geschäftsbetriebs

BCM - Business Continuity Management

- Mit Business Continuity Management (BCM) ist ein ganzheitlicher Managementprozess gemeint, um gravierende Risiken für eine Organisation frühzeitig zu erkennen und Maßnahmen dagegenzusetzen.
- Das Ziel von BCM besteht darin, der Organisation die Möglichkeit zu geben, auf Bedrohungen wie Naturkatastrophen oder Datenschutzverletzungen zu reagieren und dazu beizutragen, dass das Unternehmen kritische Funktionen aufrechterhalten und seinen täglichen Geschäftsbetrieb bestmöglich fortführen kann.

Business Continuity Planning



Learnings

- Analyse der Schwachstelle
- Findings aus Monitoring präzisieren
- Weitere Maßnahmen zur Systemhärtung
- IR-Prozess anpassen
- Reaktionswege adaptieren
- Playbooks anpassen

To Do’s

- Kontinuierliche Überprüfung aller Kontrollen
- Ständiges Hinterfragen der Prozesse
- Aktueller Stand aller Dokumentationen
- Regelmäßige Unterweisung aller Beteiligten

Fragen??

ÖHV-Veranstaltungstipps zum Thema

Weiterbildungen im ÖHV-Campus zum Thema Cybersicherheit

19.03.2025 & 16.09.2025	**Webinar „Cybergefahren im Hotel – Sensibilisierung der Mitarbeitenden“**

oehv.at/termine

DANKE FÜR IHRE AUFMERKSAMKEIT.

hoteliervereinigung
oehv.hoteliervereinigung
österreichische-hoteliervereinigung

FÜRWÄRTS. DIE ÖHV.