Erstellung eines Sicherheitskonzeptes

Dr.-Ing. Peter Korduan, GDI-Service Rostock

Parchim, 07.11.2024

Inhalt

- Bedrohungslage
- Incident Response
- Business Continuity Management
- Notfallplan
- Sicherung
- Monitoring und Tests

Bedrohungslage

- Aufklärung und Sensibilisierung
- Cyberangriffe, vor allem Ransomware nimmt stetig zu
- Starker Anstieg in allen Branchen und Regionen
  https://kommunaler-notbetrieb.de/uebersichtskarte/
- Nicht nur Vorsorge
- Trotz Vorsorge kann es jeden treffen
- Auch Notfallmanagement
- Neue gesetzliche Regelungen (NIS2-Richtlinie ab 10/2024)

Von Cyberangriffen betroffene Institutionen im deutschen Raum

Quelle: Sammlung aus der medialen Berichterstattung 2023/2024

Angriff erfolgt im	Betroffene Institutionen (Auswahl)
Januar 23	• Adesso • Sky Deutschland • Flughafen Hamburg
Februar 23	• Bayerischer Rundfunk • Stadtwerke Karlsruhe • WISAG
März 23	• Rheinmetall • STEICO Gruppe • BIG direkt
April 23	• Evotec • Badische Stahlwerke • Bilstein Gruppe
Mai 23	• Verlagsgruppe VRM • Bremer Klinikverbund Gesundheit Nord • HHU Düsseldorf
Juni 23	• Deutsche Leasing • Medizinischer Dienst • Barmer
Juli 23	• Wildeboer • Chemnitzer Kunstsammlungen • Taubblindendienst e. V.
August 23	• Münchener Verlagsgruppe • Landesregierung Mecklenburg-Vorpommern • Stadtwerke Neumünster
September 23	• Motel One • Einrichtungshaus Segmüller • BaFin
Oktober 23	• Hochsauerland Wasser/Energie • Universitätsklinikum Frankfurt • Südwestfalen IT
November 23	• Bauer AG • KaDeWe • Toyota Financial Services Europe
Dezember 23	• Allgaier Automotive • Unfallkasse Thüringen • Katholische Hospitalvereinigung Ostwestfalen
Januar 24	• AnyDesk • Bezirkskliniken Mittelfranken • ODAV AG
Februar 24	• Thyssenkrupp • KIND Hörgeräte • Varta AG
März 24	• Festspielhaus Baden-Baden • H&G Hansen & Gieraths • Kreisverwaltung Fürth
April 24	• GBI-Genios Deutsche Wirtschaftsdatenbank GmbH • St. Elisabeth-Stiftung

Incident Response (IR)

- Proaktiv und reaktiv
- Sicherheitsvorfälle schneller erkennen
- Auswirkungen und Schaden minimieren
- Risiken reduzieren
- Verschiedene Vorfallsarten berücksichtigen
  - Vorbereitung
  - Identifikation und Analyse
  - Eindämmung
  - Bereinigung
  - Wiederherstellung
  - Was lernen wir

Vorbereitung

- Priorisierung von Sicherheitsfällen
  - Ist das System besonders schutzwürdig?
  - Sind betroffene Daten geschäftskritisch?
  - Ergeben sich gesetzliche Pflichten?
  - Welche Umgebung ist noch davon betroffen?
- Kommunikation
  - Interne und externe Meldewege festlegen
  - Welche Plattformen und Werkzeuge stehen noch zur Verfügung für Kommunikation und Dokumentation?
  - Wo liegt der Notfallplan und wie darauf zugreifen?
  - Zusammenstellen eines Teams (IRT) aus allen Bereichen

Playbook für IRT

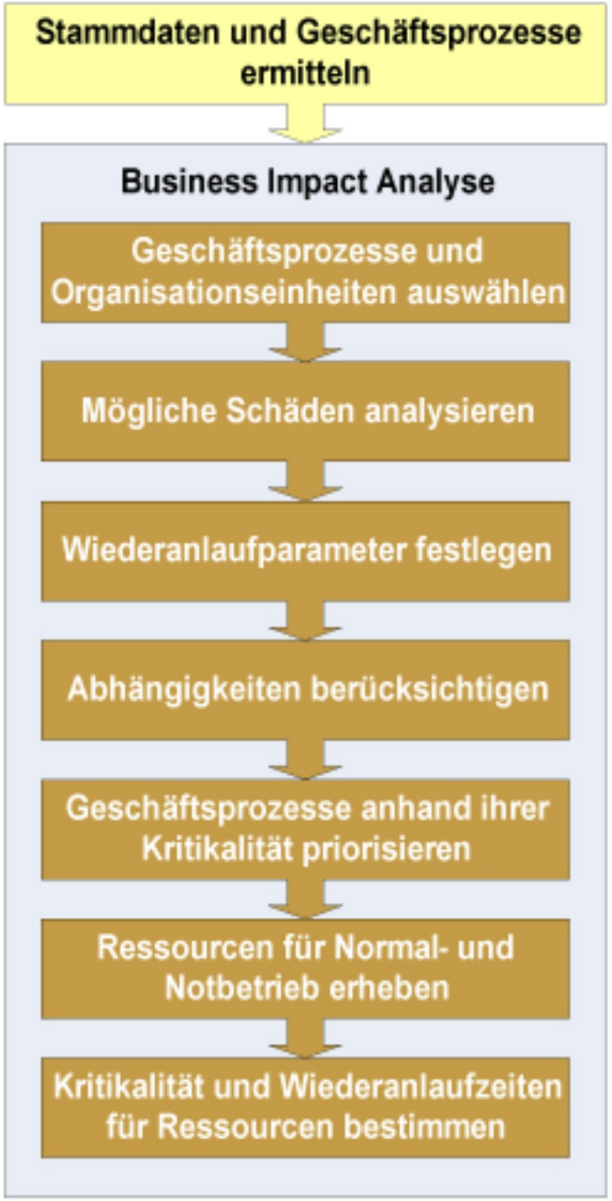
- Wer macht was?
- Wer trifft welche Entscheidungen?
- Vertretungsregelungen
- Umgang mit Checklisten, Verfahren und Werkzeugen üben
- Um welche Art von Vorfall handelt es sich?
- Wie sehen die Anzeichen für die Art aus (IoC)?
- Schritte um Ausbreitung zu verhindern
- Wiederherstellung der Funktionsfähigkeit
- Rückblickend auf die Bearbeitung schauen

Business Continuity Management (BCM)

- Welche Prozesse sind kritisch? (Impact-Analyse)
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-Notfallmanagement/3_BusinessImpactAnalysieren/BIA_node.html
- Absicherung von kritischen Geschäftsprozessen
- Maximal tolerierbare Ausfallzeit (MTPD) Maximum Tolerable Period of Disruption
- Wiederanlaufzeit in den Notbetrieb (RTO) Recovery Time Objective
- Maximal zulässiger Datenverlust (RPO) Recovery Point Objective
- Festlegung des Notbetriebsniveau (MBCO) Minimum Business Continuity Objective
- Zeithorizonte, Schadensszenarien, Schadenskategorien, Schadenspotenzial, Untragbarkeitsniveau

Schritte bei der Business Impact Analyse
nach BSI

- Vorarbeit: Zusammenstellung von aktuellen Informationen zu den Stammdaten und Geschäftsprozessen der betrachteten Institution
- Schritt 1: Geschäftsprozesse, die für die Ziele der Institution nicht wesentlich sind, können von den weiteren Analysen ausgenommen werden.
- Schritt 2: Bei der Schadensanalyse wird untersucht, welchen Schaden der Ausfall einzelner Geschäftsprozesse verursachen kann.
- Schritt 3: Anhand des zeitlichen Schadenverlaufs und der zu erwartenden Schadenshöhe werden Wiederanlaufparameter (maximal tolerierbare Ausfallzeit, Wiederanlaufzeit und -niveau) für jeden Geschäftsprozess festgelegt.
- Schritt 4: Wenn Abhängigkeiten zwischen Geschäftsprozessen oder strategische Geschäftsziele dies erfordern, werden die Wiederanlaufparameter entsprechend geändert.
- Schritt 5: Mit Hilfe der Ergebnisse aus Schadensanalyse und der ermittelten Parametern werden die Kritikalität der Prozesse und Prioritäten für deren Wiederanlauf festgelegt.
- Schritt 6: Es wird ermittelt, welche Ressourcen (Räumlichkeiten, technische Systeme, Informationen usw.) die als kritisch bewerteten Prozesse benötigen.
- Schritt 7: Im letzten Schritt werden Kritikalität und Wiederanlaufzeiten der Ressourcen bestimmt, die von den kritischen Prozessen benötigt werden.



Notfallplan

- Übergreifendes Dokument zur Bewältigung des Notfalls
- Alle übergreifenden Information zur Steuerung im Notfall

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_Vorlage_Notfallhandbuch.html

- Überführung in den Normalbetrieb
- Rückschau
- Verbesserungen

Sicherungen

- Zuverlässige Wiederherstellbarkeit von Daten
- Unter Einhaltung von
  - RPO Wie alt dürfen die wiederhergestellten Daten sein?
  - RTO Bis wann müssen die Daten wieder hergestellt sein?
- Festlegung ist Chefsache zusammen mit IT
- Speicherung abhängig vom Schutzbedarf
- Kapazität, Latenz, Schreib- und Lesegeschwindigkeit, Zuverlässigkeit, Langlebigkeit, Logistik und Lagerung

Backup-Varianten und Kosten

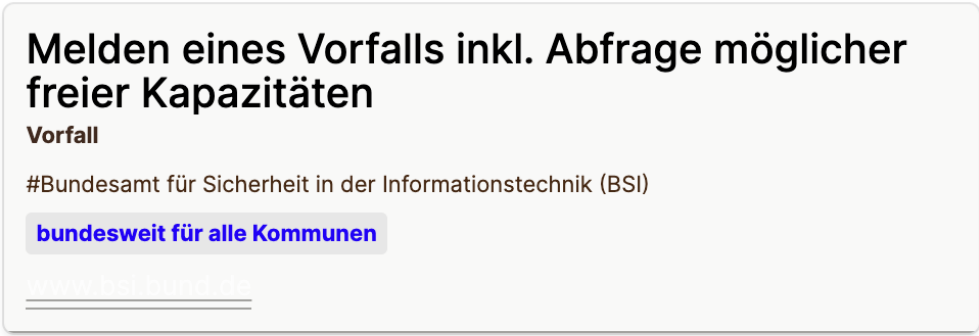
- Backup auf dem selben Server
- Kopie des Backup auf anderem Server oder Cloud bei externem Dienstleister
- Kopie auf einen Backup-Rechner bei GDI-Service
- Kopie auf externer Festplatte in einem anderen Haus
- integrierte Schutzmechanismen wie Imutable-Speicher
- Speicherung auf digital lesbaren Read-Only-Medien
- Ausdruck auf Papier / Karten / Microfish Wiederherstellung per Scan und Texterkennung

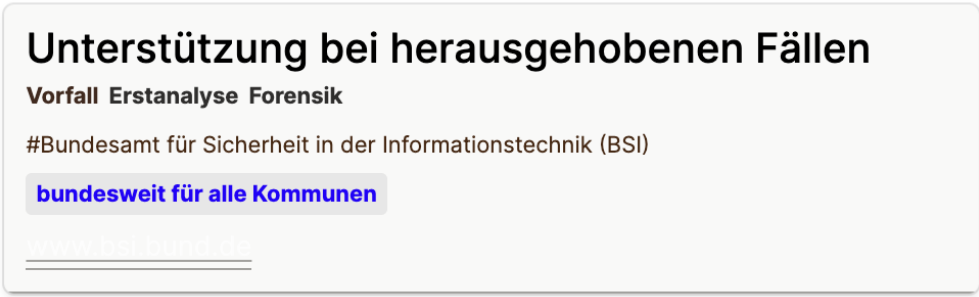
Verantwortlichkeiten

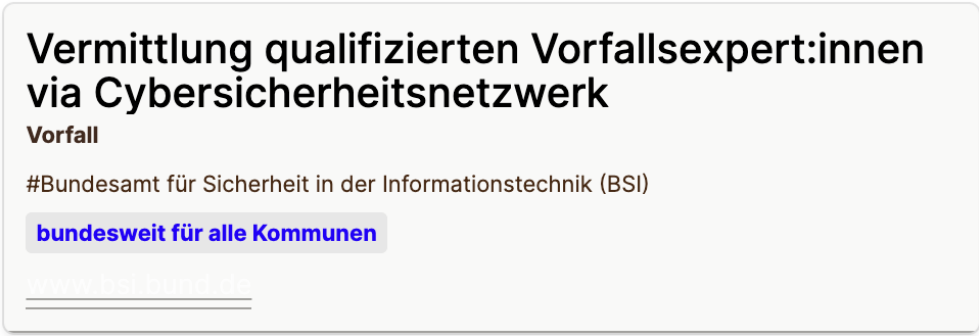
- Verantwortung für den Schutz und die Sicherheit der Daten festlegen
- Backups ständig überwachen und prüfen, nicht nur automatisch
- Auch Konfigurationen sichern
- Wiederherstellung regelmäßig testen
- Die absolute Sicherheit gibt es nicht!
- Backups können Schadsoftware enthalten
- Es geht um das Wesentliche und Risikominimierung

Unterstützung

- Auf der Seite https://cybersicherheitskompass.de noch keine speziellen Angebote für MV
- Beim BSI kann man
  - Vorfälle melden
  - Kapazitäten abfragen
  - Unterstützung bei besonderen Fällen
  - Vermittlung von qualifizierten Expert:innen via Cyber-sicherheitsnetzwerk







ToDo’s

- Beantwortung der für das Sicherheitskonzept zu stellenden Fragen
- Festlegung von Bedarfen und Maßnahmen
- Ausarbeitung der Dokumentation
- Verankerung in den Service-Level-Agreements
- Anpassung der Verträge und Preise
- Kontinuierliches Monitoring, Tests und Nachbessereungen