Rechercheplane

Fraunhofer SIT

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

FORSCHUNGSFÖRDERUNG CYBERSICHERHEIT HESSEN
Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz

5 – Rechercheplane
Fragenkatalog für die interne Bestandsaufnahme

Dieser Fragenkatalog dient zunächst nur der internen Aufklärung in akuten Krisenfällen und als Grundlage für erste Überlegungen sowie als Einstufungshilfe für kommunale Cybersicherheitsvorfälle. Die Fragen müssen fallspezifisch angepasst werden.

Es sind jedoch auch typische Fragen, wie sie in Krisenfällen von Presse und interessierter Öffentlichkeit gestellt werden können. Viele dieser Informationen sollten jedoch nicht zur Kommunikation nach außen gegeben werden, vor allem, solange die Untersuchungen noch laufen.

In einem zweiten Schritt kann deshalb auf Grundlage Ihrer Vorarbeiten ein Fragen-/Antworten-Katalog zur Vorbereitung auf Interviews und Pressekonferenzen erstellt werden, bzw. auch eine Pressemitteilung formuliert werden. → *7 – Checkliste Presseinformation*.

Geplante Veröffentlichungen zum Vorfall immer vorab mit der involvierten Polizeibehörde und/oder Datenschutzaufsichtsbehörde abstimmen.

Fragenkatalog

Allgemeine Angaben

- **Wichtigste Daten zur Einrichtung**: Anschrift, Zahl der Mitarbeiterinnen und Mitarbeiter
- **Angaben zu Vorfall**
  - Was ist geschehen? (Handelt es sich z.B. um eine IT-Störung, die bspw. durch einen technischen Defekt oder einen Stromausfall verursacht wurde, um einen Datenschutzvorfall oder einen Cyberangriff durch externe Akteure?)
  - Wann ist der Vorfall/die Störung (vermutlich) eingetreten?
  - Wann wurde der Vorfall entdeckt und gemeldet?
  - Ist der Vorfall andauernd oder bereits behoben?
  - Mit welchen Einrichtungen/Behörden wird bei der Behebung zusammengearbeitet? (Polizei, Datenschutzaufsichtsbehörde, BSI, LandesCERT, IT-Dienstleister, andere Kommunen)

Zur Strukturierung der Herangehensweise bei der Einordnung des Vorfalls und dessen Auswirkungen sowie daraus resultierende Datenschutzverletzungen kann es hilfreich sein, entlang der Cybersicherheits-Schutzziele der *Vertraulichkeit*, *Verfügbarkeit* und *Integrität* von Daten und Systemen zu arbeiten.

Verfügbarkeit

- **Technisch:** Welche Systeme oder Daten sind nicht verfügbar (bestimmte Datenbanken, Webseite, E-Mail-Server etc.)?
- **Organisatorisch:** Welche Leistungen und Funktionsbereiche sind durch die Nicht-Verfügbarkeit? Welche konkreten Dienste, Verfahren oder Handlungen können nicht oder nur eingeschränkt durch Mitarbeiterinnen und Mitarbeiter der Kommune oder Bürgerinnen und Bürger durchgeführt werden?
- **Örtlich:** Welcher Standort ist von der Nicht-Verfügbarkeit betroffen?

Vertraulichkeit

- Welche **Arten von Daten** sind von der Störung der Vertraulichkeit potenziell betroffen?
  - Personenbezogene Daten (Personaldaten von Mitarbeiterinnen und Mitarbeitern oder Abgeordneten, Daten von Bürgerinnen und Bürgern -> wenn möglich Eingrenzung aus welchem Bereich)
  - Verschlusssachen
  - andere Arten von Daten
- **Welche Bereiche** sind von der Verletzung der Vertraulichkeit betroffen?
  - **Technisch:** welche Systeme, IT-Anwendungen oder Datenbanken?
  - **Organisatorisch:** welche Fachbereiche oder Ämter?
  - **Örtlich:** welche Standorte
- Durch wen war ein unbefugter Zugriff möglich (Mitarbeiterinnen und Mitarbeiter innerhalb der Organisation, die zu weitgehende Berechtigungen hatten, Angreifer im Rahmen eines Cyberangriffs, ggf. sogar Veröffentlichung erbeuteter Daten im Darknet)?
- War ein unbefugter Zugriff nur grundsätzlich möglich oder gibt es Hinweise, dass der Zugriff auch tatsächlich stattgefunden hat?

Integrität

(Vollständigkeit und Korrektheit von Daten und die korrekte Funktionsweise eines Systems)

- Welche Systeme oder Daten sind von der Verletzung der Integrität betroffen (technisch, organisatorisch, örtlich)?
- Um welche Form bzw. Art der Störung der Integrität handelt es sich?

Auswirkungen und Abhilfemaßnahmen aus der internen Perspektive

- Hat das Ereignis Auswirkungen auf die Umgebung, wie bspw. Landkreise?
- Was wird von wem gegen den Vorfall / die Störung unternommen (Maßnahmen)?
- Welche Auswirkungen hat der Vorfall auf Bürgerinnen und Bürger bzw. ortsansässige Betriebe?
- Liegt eine meldepflichtige Datenschutzverletzung vor?
- Liegt eine Datenschutzverletzung vor, bei der auch betroffene Personen benachrichtigt werden müssen?
- Welche Risiken entstehen ggf. für betroffene Personen in Folge der Verletzung des Schutzes von personenbezogenen Daten? (bspw. durch missbräuchliche Verwendung der Daten wie Identitätsdiebstahl, Phishing)
- Liegen aktuell bereits Hinweise auf eine missbräuchliche Verwendung vor?
- Welche Abhilfe- bzw. Schutzmaßnahmen wurden für betroffene Personen eingeleitet?
- Welche Abhilfemaßnahmen bzw. Vorkehrungen können betroffene Personen selbst treffen, um sich vor Auswirkungen zu schützen?
- Wie lange ist die erwartete Dauer der Störung bzw. wie lange ist der Dienst voraussichtlich nicht erreichbar?
  - Wenn Dienste erst nach und nach wiederhergestellt werden: Wie werden diese priorisiert? Was wird schnell wiederhergestellt, wo wird es länger dauern?
- Gibt es Alternativen oder Ausweichmöglichkeiten für betroffene Dienste/Standorte?
- Muss die Arbeit eingestellt werden?
  - Ganz/teilweise/bis wann?
  - Ist mit Schadensersatzansprüchen zu rechnen?
- Wodurch ist das Schadensereignis eingetreten? *VORSICHT! Keine vorschnelle Schuldübernahme, bevor nicht alle Fakten geklärt sind*