Effiziente Risikoanalyse

anhand praktischer Erfahrungsbeispiele

Manfred Holzbach

Zentrum für sichere Informationstechnologie-Austria

Gliederung

- Zielsetzung und Aufgabenstellungen
- Bsp.1: Cyber-Sicherheits-Check bei einem Förderungsgeber
- Bsp.2: Schalenmodell in einem Hochrisikobereich
- Bsp.3: Risikoanalyse im Rahmen einer Akkreditierung
- Fazit

Anliegen meines Vortrags

- Ergänzung der wissenschaftlichen Betrachtungen
- Erfahrungswerte aus der Praxis
- Erörterung:
  - Situativ unterschiedliche Herangehensweisen
  - Umgang mit limitierten Ressourcen und Möglichkeiten
- Bedeutung von Kreativität und Interaktion

A-SIT

Anliegen meines Vortrags

- Ergänzung der wissenschaftlichen Betrachtungen
- Erfahrungswerte aus der Praxis
- Erörterung:
  - Situativ unterschiedliche H
  - Umgang mit li and Möglichkeiten
- Bedr at und Interaktion

! Kein Thema hier:
Inhaltliche Ergebnisse der Risikoanalysen

A-SIT

Zielsetzung, Aufgabenstellung

- Risikoanalyse ist als Voraussetzung für Risikomanagement unabdingbar.
- Nicht „ob“ (große/kleine Einheiten/Zulieferer als potenzielle points of failure für Gesamtsysteme)

➔ Verlust von Informationen wird existenzbedrohend

- Sondern „wie“ (zeitliche, personelle, materielle Ressourcen, Flüchtigkeit)

➔ Effizienz durch Anpassung Breite und Tiefe an Problem, Größenordnung, Ressourcen

(1) Cyber-Check (Förderungsgeber)

Ausgangssituation:

Servicestelle des Landes Stmk für Innovations-Förderungswerber – *vergleichsweise kleine Organisation ca 60MA*

Ausgelagerte IT

Assets *(Dokumente der Förderungswerber):*

- Nachweis der Innovation in Detailunterlagen
- Diese können Top-Assets für die Förderungswerber darstellen

Schadenspotenziale:

- Schadenersatz
- Compliance-Verletzungen
- Imageschaden auch für das Land

(1) Cyber-Check (Förderungsgeber)

Ausgangssituation:

Servicestelle des Landes Stmk für Innovatio

Förderungswerber – *vergleichsweise kl* *60MA*

Ausgelagerte IT

Assets *(Dokumente der Förder*

- Nachweis der Innova *lagen*
- Diese können T *Förderungswerber darstellen*

Schadenspot

- Scha
- C *tzungen*
- Im *auch für das Land*

Sicherheitsproblem in der Servicestelle oder beim IT-Supplier könnte das Förderungsmodell insgesamt gefährden

(1) Cyber-Check (Förderungsgeber)

Worauf kam es an:

Sensiblen Daten darf nichts geschehen

- Unbeschadet der ausgelagerten IT

Identifizierung von Gefahren und Bedrohungen

Wirksamkeit der Maßnahmen (auch mittels Pen-Test)

Quantifizierung: Grobe Bewertung ausreichend, jeder Vorfall wäre äußerst schädlich (Max.-Risk-Prinzip)

A-SIT

(1) Cyber-Check (Förderungsgeber)

Worauf kam es an:

Sensiblen Daten darf nichts geschehen

- Unbeschadet der ausgelagerten

Identifizierung von Gefahren ungen

Wirksamkeit der Maßn mittels Pen-Test)

Quantifizierung tung ausreichend, jeder Vorfall wär adlich (Max.-Risk-Prinzip)

Daher Interesse und aktive Mitwirkung der Geschäftsleitung während des Cyber-Check

(1) Cyber-Check (Förderungsgeber)

„Cyber-Sicherheits-Check (Kooperation BSI + ISACA):“

- Bestimmung des Status der Cyber-Sicherheit auf Basis der Cyber-Sicherheits-Exposition (⇔ Bedrohungen)
- Grundlage: Basismaßnahmen der Cyber-Sicherheit (BSI)
- Dauer: ein bis zu mehreren Tagen
- Kann durch qualifiziertes, eigenes Personal, oder durch externe Dienstleister .. durchgeführt werden.
- Zuordnung der Maßnahmenziele zu bekannten Standards der Informationssicherheit (IT-Grundschutz, ISO 27001, COBIT, PCI DSS).

A-SIT

(1) Cyber-Check (Förderungsgeber)

Durchführung – „Exposition“:

- ganzheitliche Cyber-Bedrohungsanalyse der Elemente der Infrastruktur, gespeicherten und übertragenen Daten sowie Verarbeitungsprozesse
- Kompakte und plakative Darstellung der Erkenntnisse
- Grundlage für die Bewertung von implementierten oder geplanten Maßnahmen auf Notwendigkeit, Angemessenheit und Wirtschaftlichkeit
- Erreicht wird damit zügige und interaktive Kommunikation zwecks gemeinsamer Sichtweisen mit dem Management.

A-SIT

(1) Cyber-Check (Förderungsgeber)

Durchführung – „Exposition“:

- ganzheitliche Cyber-Bedrohungsanalyse d… Infrastruktur, gespeicherten und üb… sowie Verarbeitungsprozesse
- Kompakte und plakativ… kenntnisse
- Grundlage für di… plementierten oder geplanten M… wendigkeit, Angemessenheit und W…
- … zügige und interaktive Kommunikation z… einsamer Sichtweisen mit dem Management.

- Bemerkenswert : Beschränkung auf „Cyber“ – Bedrohungen, Keine Berücksichtigung von Perimeter-, Insider- und Safety-Aspekten

(1) Cyber-Check (Förderungsgeber)

Durchführung – „Exposition“:

- Standardisierte Fragestellungen zu:
  - **Wert der Daten und Prozesse,**
  - **Art der Angreifer,**
  - **Attraktivität und Transparenz für Angreifer,**
  - **zu erwartende Zielgerichtetheit von Angriffen,**
  - **Angriffe i.d. Vergangenheit,**
  - **zu erwartender max. Bedrohungsgrad**
- jeweils unterschieden zwischen Vertraulichkeit, Verfügbarkeit und Integrität.
- Interaktive Bewertungen – vorgegebener Gewichtungsschlüssel

(1) Cyber-Check (Förderungsgeber)

Durchführung – „Cyber-Sicherheits-Status“

- Bewertung der implementierten / geplanten Maßnahmen nach vorgegebenem Katalog von Maßnahmenzielen
- Aufzeigen allfälliger Mängel
- Bewertung der Wirksamkeit der Maßnamen (Ampel-Indikatoren + verbal ausgeführt)
- Ergebnis: Priorisierung ausgehend von der Exposition
- Parallel dazu auf Wunsch der Organisation zusätzliche Schwachstellen Scans beim IT-Supplier

Interaktives Walkthru mit GF, dann schriftlicher Bericht

(1) Cyber-Check (Förderungsgeber)

Erfahrung:

- Methode eignet sich gut für vergleichsweise kleine Organisationen (v.a. Ressourcenbedarf).
- Erreicht aufgrund standardisierter Fragestellungen, Bewertungsschlüssel und Berichtsmuster effizient realistische Erkenntnisse.
- Im interaktiven Prozess wird die Sicht auf die eigenen Prozesse, Maßnahmen und Besonderheiten geschärft.
- Voraussetzung sind Bereitschaft und Offenheit des Top-Managements zur Mitwirkung.

A-SIT

(1) Cyber-Check (Förderungsgeber)

Erfahrung:

- Realistische Einschätzung unbeschadet der Beschränkung auf „Cyber“.
- Vorgegebene Bewertungsschlüssel können Ergebnis massiv beeinflussen und wurden in einem Fall modifiziert.

(2) Hochrisikobereich (Gesundheitsdaten)

Ausgangssituation:

Kein System *„aus einem Guß“,* sondern komplexe heterogene Landschaft

- Entitäten mit unterschiedlichen Größen, Aufgaben
- Historisch gewachsen
- Funktionalität und Termine politisch vorgegeben
- Unterschiedliche Assets, Eigner, Zuständigkeiten Entscheidungsstrukturen und Sicherheitslevels
- Gemeinsames Berechtigungskonzept

A-SIT

(2) Hochrisikobereich (Gesundheitsdaten)

Ausgangssituation:

Kein System *„aus einem Guß“*, sond… …ke heterogene Landschaft

- Entitäten mit unterschi… …isen, Aufgaben
- Historisch gewach…
- Funktionalit… …ine politisch vorgegeben
- Unters… …ssets, Eigner, Zuständigkeiten Er… …strukturen und Sicherheitslevels
- Ge… …sames Berechtigungskonzept

Sicherheitsproblem in einer Entität bedeutet Beschädigung des Gesamtsystems

(2) Hochrisikobereich (Gesundheitsdaten)

Was begründet die Hochrisiken:

- Art der Daten (Gesundheitsdaten)
- Heterogene Landschaft der Aufbewahrungsorte
- Zugriffsberechtigungen unterschiedlicher Reichweite (lokal / flächendeckend)

(2) Hochrisikobereich (Gesundheitsdaten)

Worauf kommt es an:

Umgang mit Struktur-immanenten Bedrohungen bei:

- Nicht beeinflussbaren exponierte Umgebungen
- Vertrauensstellungen
- Weitreichenden Funktionalitäten
- Lokalen heterogenen Implentierungen

Fokus: Finden und Härten struktureller Schwachstellen,
weniger auf Quantifizierung (Maximum-Risk)

A-SIT

(2) Hochrisikobereich (Gesundheitsdaten)

R.A.: Weitere Vorgehensweise – Schalenmodell:

Welche Bereiche kann man als hinreichend abgesichert ansehen ?

Technische Maßnahmen (Krypto, robuste Mechanismen)

Welche Risiken lassen sich ohne Detailanalyse bewerten ?

Bereits zertifizierte Bereiche, Prozesse

Welche nicht ?

A-SIT

(2) Hochrisikobereich (Gesundheitsdaten)

Erfahrung:

- Obwohl sehr breit angelegte und aufwä… …n einer derart komplexen, heteroge… Systemlandschaft nicht mö… …und ihr Zusammenwirken…
- Fokus auf leb… …echanismen, die deren F… …sichern.
- A… …lich (Berater, Tools)
- Se… …ssen, Erfahrung und Kreativität der be… …perten.

Methode: schnelle Erkenntnisse, die zielgerichtet vertieft werden können.
Modell: funktioniert gleichermaßen für große wie kleine Organisationseinheiten.

(3) Risikoanalyse für Akkreditierung

Ausgangssituation (eigene Organisation):
R.A. ist verpflichtender Bestandteil des QMS
Pflichtversicherung mit Mindestdeckung erforderlich

- Zugehörige Risiken
  - identifizieren
  - bewerten
  - mit Versicherungsschutz in Einklang bringen
  - mit Prozessen und Leitfäden in Einklang bringen

- Keine brauchbaren Vorlagen > selbsterstellte Methode

A-SIT

(3) Risikoanalyse für Akkreditierung

Worauf kam es an:

Dokumentation und Nachweis

- Auseinandersetzung mit Gefahren und Risiken
- Identifizierung der Risiken

Quantifizierung

Aktive Maßnahmen (Aufbau- und Ablauforganisation)

Passive Maßnahmen (Versicherung)

(3) Risikoanalyse für Akkreditierung

Worauf kam es an:

Dokumentation und Nachweis

- Auseinandersetzung mit Gefahren
- Identifizierung der Risiken

Quantifizierung

Aktive Maßnahmen (Ablauforganisation)

Passive Maßnahmen)

Leitung hat Maßnahmen vorgesehen und dokumentiert, begegnet Risiko der schuldhaften oder fahrlässigen Unterlassung

(3) Risikoanalyse für Akkreditierung

Detail: Hauptrisiken:

- Finanzielle Gebarung: Out of Business
- Schadenersatz aus inhaltlicher Tätigkeit
- Schadenersatz aus Umgang mit vertraulichen Informationen
- Mangelhafte Unparteilichkeit
- Allgemeiner Bürobetrieb

(3) Risikoanalyse für Akkreditierung

Hauptrisiken – Bewertungsmethoden:

- Wenn max. Schadenshöhe abschätzbar:
  diese anzusetzen
- Wenn nicht abschätzbar:
  da kaum oder geringe Eintrittswahrscheinlichkeit,
  Nachvollziehen der gesetzlichen Mindest-
  versicherungssumme (750 T€ für Schaden)
- Diese wurde noch um Reservepolster aufgestockt
  (für Prozessrisiko)

Schadenersatzrisiken aus Tätigkeit: nicht alle zugleich schlagend

(3) Risikoanalyse für Akkreditierung

Erfahrung:

- Selbsterstellte Methode wurde gewählt, weil es sehr spezielle Tätigkeitsbereiche betrifft.
- Es gibt praktisch keine brauchbaren Erfahrungswerte für die Quantifizierung (weder für Höhe noch WS)
- Im interaktiven Prozess wird dennoch die Sicht auf die eigenen Risiken, Prozesse und Maßnahmen geschärft.
- Erfolgsfaktor: langjährige Erfahrung der Mitwirkenden.

Fazit

Verbliebene Fragen:

- 100% Sicherheit nicht möglich > Zumutbare Compliance?
- Grenzen der Prävention > Grenzen der Verteidigung?
- Wieviel an Haftung kann durch Zertifizierungen verringert werden?
- Wieviel Restrisiko darf in Kauf genommen werden?
- Was kann rechtliche Beratung hier leisten?

Erkenntnis:

- Ablösen von Risikosträngen mit gering eingestufter Priorität (Schalen) lassen sich effizient durchführen und führen zu zuverlässigen, nachvollziehbaren und vor allem aktuellen Ergebnissen.
- Kritische Erfolgsfaktoren: Mitwirkung des Top-Management Know-how, Erfahrung und Kreativität der Durchführenden.

A-SIT

Danke für Ihre Aufmerksamkeit

Manfred Holzbach
Stabsstelle
Zentrum für sichere Informationstechnologie-Austria (A-SIT)

Manfred.holzbach@a-sit.at