Die Senatorin für Finanzen

08.07.2013

Dr. Hagen

Tel. 4746

**Vorlage für die Sitzung des Senats am 16.07.2013**

# „Informationssicherheitsmanagementsystem (ISMS) für die FHB“

## A. Problem

In der Freien Hansestadt Bremen ist ein Informationssicherheitsmanagementsystem aufzubauen. Primärer Anlass dafür ist der aktuelle Abstimmungsprozess mit Bund und Ländern bei der Realisierung von Sicherheit im Verbindungsnetz (siehe hierzu auch IT-NetzG). Eine gemeinsame Leitlinie für Informationssicherheit wurde vom IT-Planungsrat im März 2013 verabschiedet.

Diese Informationssicherheitsleitlinie von Bund und Ländern hat direkte Auswirkungen auf die FHB, insbesondere die verpflichtende Anwendung von Standards für ein ISMS.

Die Notwendigkeit, ein ISMS aufzubauen, ergibt sich auch aus den IT-Sicherheitserfordernissen der eigenen IT-Systeme der Bremer Verwaltung und ihrer Weiterentwicklung, z.B. für mobile Endgeräte. Es muss dabei ein transparenter Abwägungsprozess zwischen gewünschten Funktionalitäten und Sicherheit stattfinden. „Voraussetzung für einen sicheren Betrieb ist ein funktionierendes Informationssicherheitsmanagements für das Land Bremen (vgl. 32. Jahresbericht der LfDI, Ziffer 4.1).“

Insbesondere müssen einheitliche Sicherheitsstandards für IT-Verfahren oder Verbünde festgelegt werden. Dabei müssen die Anforderungen von gemeinsamen IT- Verfahren in Trägerschaft der norddeutschen Länder (bei Dataport) sowie das Zusammenwirken der beiden Kommunen Stadtgemeinde Bremen und Bremerhaven berücksichtigt werden.

Die FHB muss in diesen Fragen eine abgestimmte Zielplanung verfolgen, um in den diversen Gremien (z.B. dem IT-Planungsrat) verbindliche Aussagen treffen zu können.

Weiterhin sind Aufträge des Senates aus 2009 (vgl. Senatsvorlage vom 29.7.2009) zu erledigen, in der die SF gebeten wurde, sich für ein Rahmenwerk („Framework“) für die Informationssicherheit zu entscheiden.

Der Bund arbeitet zudem an einem IT-Sicherheitsgesetz, das Auswirkungen auf die bremische Verwaltung haben wird (insbesondere in sog. „Kritischen Sektoren“[1]). Zu erwarten sind zumindest Meldepflichten für Sicherheitsvorfälle. Die bremische Verwaltung wäre einerseits betroffen als Betreiber von Einrichtungen in kritischen Sektoren und andererseits als möglicher Adressat von Meldungen und Ad hoc Empfehlungen. Die entsprechenden Schnittstellen sind für beide Aspekte von der FHB zu definieren bzw. zur Verfügung zu stellen.

**B. Lösung**

Die SF schlägt vor, das ISMS auf der Basis von ISO 27001 einzuführen und es in der Folge binnen 5 Jahren zu einem BSI IT-Grundschutz konformen Management weiterzuentwickeln. Das ermöglicht die Definition einer bremischen Informationssicherheitsleitlinie im Konsens mit Bund und Ländern. Sie stellt die normative Mindestanforderung dar. Die schrittweise Vorgehensweise trägt auch den Anforderungen nach mehr Gestaltungsmöglichkeiten Rechnung. Anforderungen des Datenschutzes an Institutionen der öffentlichen Verwaltung können auf diesem Weg ebenfalls effektiv integriert werden.
Sowohl ISO 27001 als auch IT-Grundschutz schreiben für den Informationssicherheitsprozess den Aufbau eines ISMS und die Institutionalisierung eines IT-Sicherheitsbeauftragten vor. Diese Funktion muss auch in der Linie abgebildet werden.
Für die organisatorische Einbindung des ISMS empfiehlt das BSI zwei verschiedene Ansätze (Schaubild). Die SF schlägt vor, von den beiden Modellen das Modell einer „größeren Institution“ auf die FHB anzuwenden.
Als Alternative zu diesem Modell wären die Geschäftsbereiche des Senats (sowie Bremerhaven) jeweils als jeweils mittelgroße Institution (ggf. mit weiterer Untergliederung) aufzufassen. Dieses Vorgehen angesichts der Ressourcenknappheit (insbesondere qualifiziertes Personal im Bereich des IT Sicherheitsmanagements), der Existenz eines

[1] Mit einem IT-Sicherheitsgesetz sollen einschlägige Mindeststandards für Betreiber kritischer Infrastrukturen wie Energie, Informations- und Kommunikationstechnologien etc. verabschiedet werden.

funktionsfähigen gemeinsamen Verwaltungsnetzes und der engen Kooperationsanforderungen untereinander nicht sinnvoll.

Beim Aufbau des ISMS können das bestehende Informationssicherheitskonzept von 2010 und die Vorarbeiten zum Aufbau eines gemeinsamen CERT bei Dataport (CERT-Nord) einbezogen werden.

Die Benennung eines eigenen IT-Sicherheitsbeauftragten für die FHB ist ein weiterer erforderlicher Schritt (s.u.), der in allen Rahmenwerken zwingend vorgesehen ist.

Informationssicherheit und Datenschutz bedienen sich ähnlicher Methoden. Allerdings bleibt festzuhalten, dass hier ein Interessenkonflikt besteht (z.B. bei den Anforderungen an die Protokollierung von Ereignissen in Anwendungs- und IT- Systemen).

Die Rollen sind daher zu trennen. Informationssicherheitsmanagement mit IT-Sicherheitsbeauftragten bzw. Ansprechpartner sowie ggf. parallel ein Datenschutzmanagement mit schon jetzt bestehendem Datenschutzbeauftragtem. Die Betroffenheitsrechte der BürgerInnen müssen insbesondere in dieser Konstellation Berücksichtigung finden, da das ISMS nicht auf die Betroffenheit des Individuums orientiert ist.

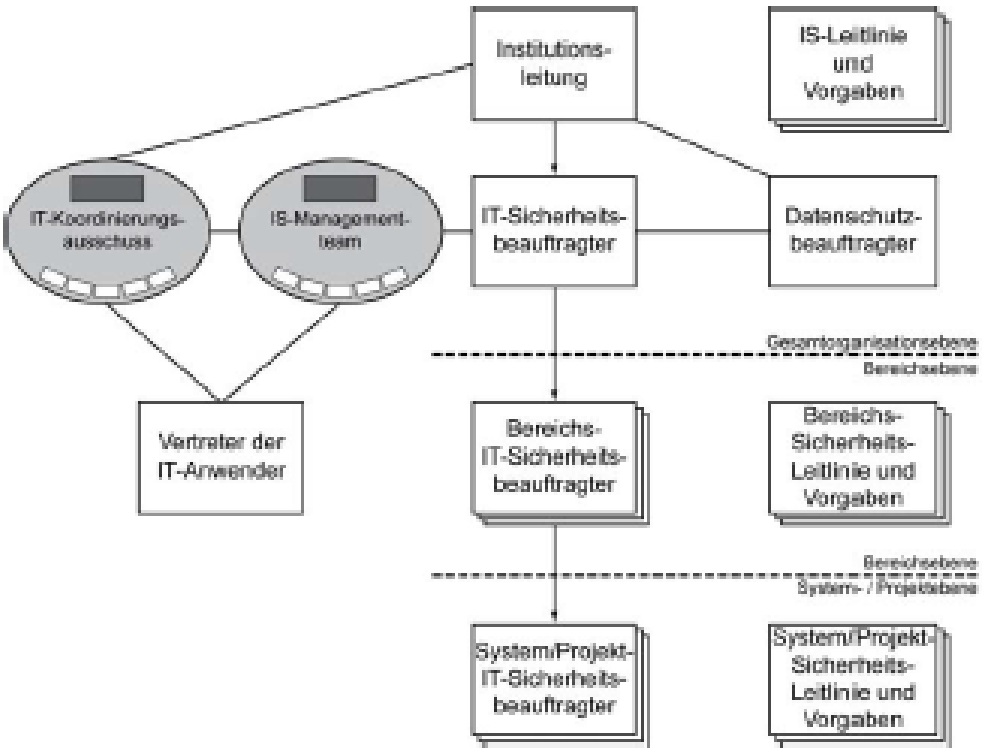


Abbildung 3.1: Aufbau einer IS-Organisation in einer großen Institution

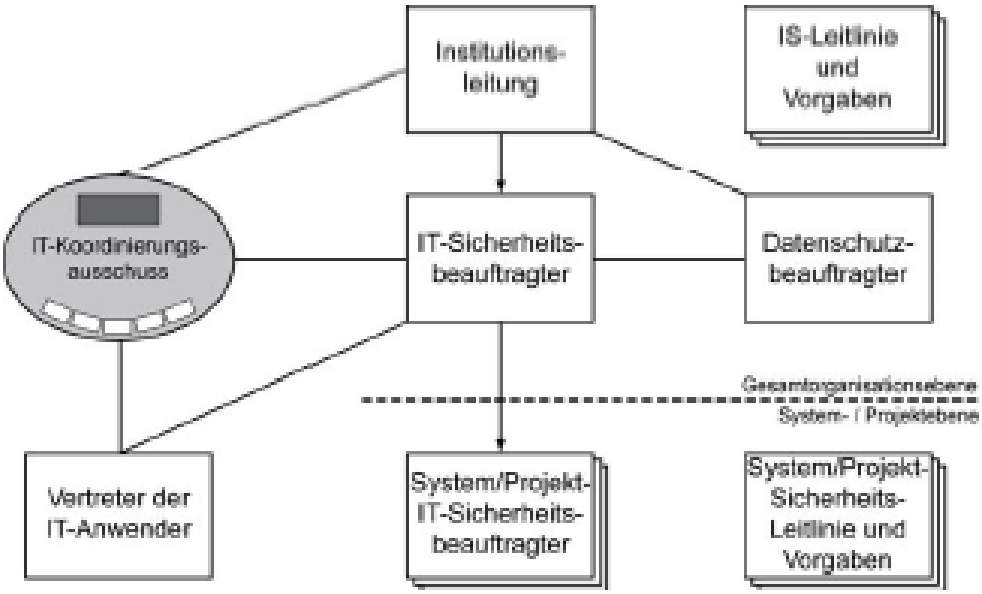


Abbildung 3.2: Aufbau der IS-Organisation in einer mittelgroßen Institution

Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

Folgende Maßnahmen zum Aufbau eines ISMS für die FHB sollen jetzt ergriffen werden:

1. Umarbeitung des FHB IT-Sicherheitskonzeptes von 2010 zu einer „echten“ Informationssicherheitsleitlinie.

2. Organisatorische Einbettung des IT-Sicherheitsbeauftragten der FHB.

3. Definition dezentraler Verantwortungsbereiche: Die direkt am BVN angeschlossenen Einheiten sollen mindestens pro Ressort die Aufgabe eines Ansprechpartners für die IT-Sicherheit übernehmen (incl. Vertretungsregelung). Der Ansprechpartner stellt die Schnittstelle auch zur Org. und Verwaltung, so dass ein zusammenlegen de Funktion des Sicherheitsbeauftragten kleinerer Dienststellen (außer bei gleich gelagerten Aufgaben) grundsätzlich nicht zu empfehlen ist.
   Für getrennte Netze, z.B. das Netz der Polizei, muss ein vollwertiges Sicherheitsmanagement mit IT-Sicherheitsbeauftragten gegeben sein.

4. Erstellung eines Fortbildungskonzeptes mit Durchführung von Schulungs- und Sensibilisierungsmaßnahmen.

5. Errichtung eines Computer Emergency Response Teams (CERT). Ein CERT wirkt bei der Lösung von konkreten IT-Sicherheitsvorfällen (z. B. Bekanntwerden neuer Sicherheitslücken in bestimmten Anwendungen) als Koordinator mit, gibt Warnungen vor Sicherheitslücken und Ratschläge heraus. Zum Bereithalten eines CERT auf Länderebene ist die FHB durch die gemeinsame Informationsleitlinie verpflichtet. Geplant ist der Aufbau des CERT-Nord bei Dataport (Trägerländer CERT) inklusive seiner Einbettung in den nationalen Verwaltungs-CERT Verbund. Wegen möglicher Interessenkonflikte herauszulösende und demnach bei der FHB verbleibende Aufgaben müssen identifiziert und im Land abgebildet werden. Außerdem ist die Einbettung anderer Institutionen wie z.B. dem Magistrat Bremerhaven zu klären.

6. Aufbau eines Systems für Meldewege und Eskalation als Ad hoc Maßnahme, Aktualisierung der bestehenden Verteiler (z.B. Admin-Info).

7. Festlegung von Schutzbedarfskategorien ggf. erweiterte Risikobetrachtung. Dieser Prozess ist unterschiedlich weit entwickelt und einheitlich zu definieren.

8. Überprüfung, ggf. Erstellung, Zentralisierung der Datenhaltung und Konsolidierung von IT-Sicherheitskonzepten sowie Datenschutzkonzepten von Informationsverbünden bei der aufzubauenden Organisation (Dokumentationsanforderung und Dokumentationslenkung) und ihrer gestuften und zielgruppengerechten Veröffentlichung .

9. Aufbau eines Evaluationskonzeptes bis hin zu einer Audit- oder Zertifizierungsreife.

**C. Alternativen**

Aufgrund der Anforderungen aus dem Bund-/Länder-Verbindungsnetz ist die FHB zum Aufbau eines ISMS verpflichtet. Eine Verschiebung ist riskant, da der Aufbau erfahrungsgemäß einige Zeit in Anspruch nimmt.

**D. Finanzielle / Personalwirtschaftliche Auswirkungen / Genderprüfung:**

1. Personalwirtschaftliche Auswirkungen

Die Stelle eines zentralen Sicherheitsbeauftragten für die Freie Hansestadt Bremen ist dauerhaft zu verorten. Die Senatorin für Finanzen wird für die zentralen IT-Sicherheitsaufgaben ein Finanzierungskonzept erarbeiten und durch die IT-Steuerungsgruppe beschließen lassen. Die dezentralen Ansprechpartner in den Ressorts und Dienststellen sind grundsätzlich über die bestehende Personalausstattung abzudecken, da es sich auch nicht um eine neue Aufgabe handelt sondern vielmehr eine Erreichbarkeit sicherstellt.

Bei Etablierung eines vollwertigen IT-Sicherheitsbeauftragten und Management in einem dezentralen Bereich (wie z.B. der Polizei, dem Bildungsbereich der SfBuW oder in Bremerhaven) sind Mitarbeiter im Rahmen der Personalentwicklung entsprechend zu qualifizieren (s.u.).

2. Dauerhafte konsumtive Auswirkungen

Für die beabsichtigte Beauftragung von Dataport mit dem zentralen CERT-Nord fallen voraussichtlich laufende Kosten in Höhe von 0,35 Mio p.a. an: Erwartet wird dort eine Personalausstattung von 8 Personenjahren (1500,- Stunden x 105 € x 8 x Bremer Anteil – mindestens 9%, eher 20%, vor allem da z.B. Niedersachsen bereits ein eigenes CERT betreibt). Zusätzlich zu veranschlagen sind dort Sachkosten für Ausstattung sowie ggf. von Dataport extern zu erteilende externe Beauftragungen (insgesamt mindestens 0,5 Mio, zu verteilen gem. Bremer Anteil.). Die Beteiligung der FHB ist vor diesem Hintergrund zu prüfen.

3. Investitionen in den Aufbau eines ISMS

Gesonderte Beauftragungen durch die FHB (konzeptionelle Unterstützung beim Aufbau von Schnittstellen zu anderen Landes-Institutionen. etc.) sind in 2014/2015 mit insgesamt 100.000 € vorzusehen

4. Konsumtive Ausgaben in 2014 /2015

Für FHB bezogene Schulungen wird eine Mittelausstattung in den Haushalten 2014 und 2015 von insgesamt 50.000 € erforderlich. Die Kooperation mit der BAKÖV

(Bundesakademie für Öffentliche Verwaltung) wird zu einer Entlastung führen, so dass primär Reisekosten zu veranschlagen sind.

Die Geschlechterperspektive im Sinne des Gender Mainstreaming wird beim Aufbau des ISMS nicht berührt.

**E. Abstimmung**

Die Vorlage wurde mit allen Ressorts abgestimmt.

**F. Öffentlichkeitsarbeit/Veröffentlichung nach dem IFG.**

Geeignet. Einer Veröffentlichung im IFG-Register gemäß IFG steht nichts entgegen.

**G. Beschluss**

1. Der Senat bittet die Senatorin für Finanzen um Wahrnehmung der Funktionen eines zentralen IT-Sicherheitsbeauftragten für die FHB.
2. Der Senat bittet die Ressorts um Mitwirkung beim Aufbau des Informationssicherheits-Managementsystem und um die Ausweisung von Ansprechpartnern für IT-Sicherheit und im Bedarfsfall auch gesonderter IT-Sicherheitsbeauftragten
3. Der Senat legt die ISO 27001 als normative Mindestanforderung für den Aufbau eines Sicherheitsmanagements fest.
4. Der Senat bittet die Senatorin für Finanzen um Erstellung eines Umsetzungsplans (UP Bremen) zu vollständigen Umsetzung von „IT-Grundschutz“ gemäß BSI bis Ende 2018.
5. Der Senat bittet die Senatorin für Finanzen, in Abstimmung mit den Ressorts ein Finanzierungskonzept für die zentralen IT-Sicherheitsaufgaben zu erarbeiten und durch die IT-Steuerungsgruppe (ITSG) beschließen zu lassen.