Anforderungen zur Umsetzung eines IT-Sicherheitskonzepts nach IT – Grundschutz (BSI) als Basis für Informationssicherheit

1. Einleitung

Referenz-Architektur

Festlegung des Untersuchungsgegenstands und des Geltungsbereichs
Geschäftsprozesse und optional kritische Geschäftsprozesse
räumliche Gegebenheiten/Infrastruktur (Liegenschaften, Gebäude, Räume)
eingesetzte Netze, Kommunikationsverbindungen und externe Schnittstellen
vorhandenen IT-Systeme (Clients, Server, Netzkopplungselemente, Mobile Devices, usw.)

Basis-Absicherung nach IT-Grundschutz als Einstig in den Aufbau eines Managementsystems für Informationssicherheit (ISMS)

- Die Basis-Absicherung ist für Institutionen interessant, die einen Einstieg in den IT-Grundschutz suchen und schnell alle relevanten Geschäftsprozesse mit Basismaßnahmen absichern möchten.
- Die Kern-Absicherung lenkt die Sicherheitsmaßnahmen auf die „Kronjuwelen" einer Institution, also besonders wichtige Geschäftsprozesse und Assets. Diese Variante zielt damit auf die vertiefte Absicherung der kritischsten Bereiche ab.
- Die Standard-Absicherung entspricht der empfohlenen IT-Grundschutz-Vorgehensweise (vgl. früherer BSI-Standard 100-2). Sie hat einen umfassenden Schutz für alle Prozesse und Bereiche der Institution als Ziel.

Sowohl die Basis- als auch die Kern-Absicherung können als Einstieg und Grundlage für eine umfassende Absicherung nach IT-Grundschutz dienen.

Struktur und Aufgaben beteiligter Projekte und Institutionen

Geltungsberreich:

Durch die gemeinsame Nutzung der räumlichen und technischen Infrastruktur in der Einrichtung entsteht ein IT-Verbund / IT-System. An diesem IT-Verbund / IT-System sind alle Projekte und Einrichtungen zu protokollieren.

Kooperierende Projekte und Partner:

Aufgaben und Ziele der einzelnen beteiligten Projekte und Einrichtungen sind kurz aufzuführen und im konzeptionellen Ablauf mitabzubilden

Aufbau des IT-Sicherheitskonzeptes:

Das IT-Sicherheitskonzept ist in ein Grundkonzept nach IT-Grundschutz-Kompendium des BSI (Bundesamt für Sicherheit in der Informationstechnik)

IT-Sicherheitsmanagementprozess:

Für die Strukturierung des Sicherheitsmanagements gibt es keine allgemein gültigen Regeln, vielmehr werden wir hier die speziellen Gegebenheiten der existierenden Managementstrukturen der Einrichtung berücksichtigen

Projektstand:

Benennung der Projekt-Verantwortlichen

2. Sicherheitsziele IT-Sicherheit

Wie lässt sich informationstechnische Sicherheit rechtlich steuern?

Welche informationstechnische Sicherheit muss zwingend gewährleistet werden?

Welche informationstechnische Sicherheitsinstrumente dürfen eingesetzt werden?

Welche informationstechnischen Sicherheitsinstrumente müssen eingesetzt werden, und was sind bei Nichteinsatz die Konsequenzen?

Aus betriebswirtschaftlicher Sicht stellen sich die nachfolgenden Fragen:

Wie hoch ist die Wahrscheinlichkeit eines Schadenseintritts?

Wie hoch ist in Relation hierzu die Höhe eines möglichen Schadens?

Wie ist das angemessene Verhältnis von Schutzmaßnahmen und Schutzzweck?

Definition und Abgrenzung von Risiken

Definition und Auswirkungen für Schäden in Folge von Risiken bei der Informationsverarbeitung, internen/externen (digitaler/mobiler) Kommunikation

Rechtliche Rahmenbedingungen

Datenschutzrecht

Perspektive Zivilrecht

Schadensersatzrisiken

Fazit und Handlungsrahmen

Gesetzliche Grundlagen

Datenschutzbestimmungen laut EU - Datenschutz-Grundverordnung

3. STRUKTURANALYSE (Bestandsanalyse)

Darstellung der vorhandenen IT-Systeme

Übersicht: Räume / IT-Systeme / IT-Anwendungen

Übersicht: Netzplan

Netzwerk

Arbeitsplatzrechner

IT Support

Darstellung und Zuordnung der IT-Anwendungen zu den IT-Systemen

4. Schutzbedarfsanalyse

Feststellung des Schutzbedarfs anhand der Grundbedrohungen:

Verlust der Vertraulichkeit

Verlust der Integrität

Verlust der Verfügbarkeit

Gesamtschutzbedarf:

Ergebnis der Schutzbedarfsanalyse

5. Risikoanalyse

Darstellung der Gefährdungen übergeordneter Komponenten:

Organisation, Personal, Notfallvorsorge, Datensicherung, Datenschutz

Darstellung der Gefährdungen von Infrastruktur-Komponenten:

Gebäude, Verkabelung, Büroräume, Serverräume/Rechenzentrum, Datenträgerarchiv, Räume für die technische Infrastruktur

Darstellung der Gefährdungen der betrachteten IT-Systeme:

Notfallvorsorge-Konzept, Datensicherungskonzept, Datenschutzkonzept

6. Maßnahmenkatalog

Technisch-organisatorische Maßnahmen:

Mindeststandards der Einrichtung zur Auftragsverarbeitung, Datenschutz und Informationssicherheit

7. Mitgeltende Anlagen

Organigramm Unternehmensführung

Geschäftsleitung, Mitarbeiter/Angestellte, Infrastruktur und der IT-Abteilung/Dienstleister

Compliance Policies

Corporate Compliance Handbuch

Hausinterne IT-Richtlinien:

Schließplan

Zutrittskontrolle

Berechtigungskonzept

Vertretungsplan: laut Organisationshandbuch

Mitarbeitersensibilisierung: Awareness-Kampagnen

Regelung zum Passwortgebrauch
Verschlüsselung von E-Mail-Anhängen

Wartungskonzept / Infrastruktur:

Entsprechend den Verantwortlichkeiten (aus Organisationshandbuch?)

Übersicht über die Infrastruktur, Logistik und zu wartende Technik:

Management und GF: - Management und GF-Struktur-Organigramm
IT- Rolle und Mitarbeiter IT: - EDV-Struktur_Organigramm
Infrastruktur & Logistik: Logistik-Struktur_Organigramm

Handhabungen Sicherheitsanlagen:

EDV/IT-Dienstleister: Wartungsvertrag EDV-Service/Sicherheitsagreement
Internetzugang / DSL-Anschluss: Handhabungen TK & Internetzugang
Daten- und Aktenvernichtung: Handhabungen Daten- und Aktenvernichtung
Hausverwaltung/Haustechnik : Handhabungen Hausverwaltung/Haustechnik
Brandmeldesystem: Handhabungen Brandmelderzentrale (BMZ)
Reinigungsservice: Handhabungen Reinigungsservice

Software Verwaltung:

Software-Lizenzen und Verträge
Regelung von IT-Sicherheit und IT-Verträgen

Virenschutzkonzept:

Antivirus Software
Endpoint Security

Notfallvorsorgekonzept:

Notfallhandbuch IT
Disaster Recovery Plan

Datensicherungskonzept:

Datensicherungsverfahren
Datenverfügbarkeit
Archivierung

Konzepte für hohen Schutzbedarf:

als Beispiel sind hier die Bankaufsichtliche Anforderungen an die IT (BAIT) der Bundesanstalt für Finanzdienstleistungsaufsicht für Finanzinstitute zu nennen

Technisch-organisatorische Maßnahmen:

Datenschutzkontrollen nach TOM
Berechtigungskonzept

Datenschutz-Löschfristen

Datenlöschung / Datenvernichtung

Virenschutzkonzept

IT-Grundschutz-Kompendium

IT-Grundschutz – BSI Kompendium

Datenschutz und Online Marketing
Berlin | Freiburg im Breisgau| Gelsenkirchen

WIEMER.ARNDT.