Bundesamt
für Sicherheit in der
Informationstechnik

Modernisierung des IT-Grundschutz

Berlin, den 15. September 2015

Inhalt

1. Ausgangslage
2. Digitale Agenda
3. Allianz für Cyber-Sicherheit
4. IT-Grundschutz-Modernisierung
   - Motivation und Zeitplan
   - Vorgehensweisen
   - Struktur der Kataloge
   - Profile und Tools

1. Ausgangslage

Snowden-Enthüllungen

Angriffsvektor „Strategische Aufklärung“

- Knotenpunkte und Internet-Dienstleister

Angriffsvektor „Individuelle Angriffe“

- interessante Personen und Institutionen

Angriffsvektor „Standards / Implementierungen“

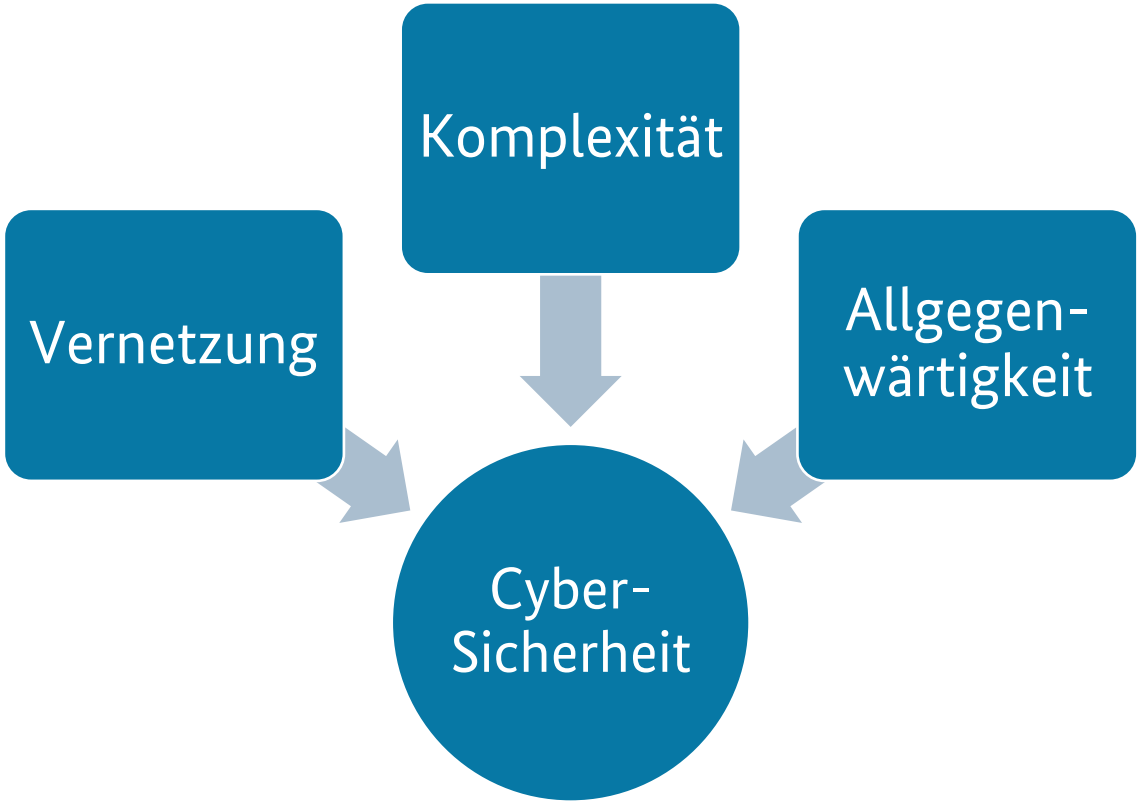
- Schwächung von Krypto-Standards, etc.

Angriffsvektor „Manipulation von IT-Equipment“

- Eingriffe in Bestellung, Lieferung, Service, etc.

- Dass staatliche Stellen die Kommunikation im Internet und in anderen öffentlichen Netzen überwachen, ist nicht neu.
- Selbst Fachleute waren jedoch über das enorme Ausmaß und die Dichte der Überwachungs-maßnahmen überrascht.
- Aber: Die Gefährdungslage im Cyber-Raum darf nicht auf nachrichtendienstliche Aktivitäten reduziert werden.

Digitalisierung



Konsequenzen:

- Klassischer Perimeterschutz reicht schon lange nicht mehr aus.
- Mit der zunehmenden Vernetzung werden Cyber-Sicherheit und IT-Sicherheit immer deckungsgleicher.

Aber:

- Deutschland kann auf die ökonomischen und gesellschaftlichen Potenziale der Digitalisierung nicht verzichten!

2. Digitale Agenda

Digitale Agenda 2014 – 2017

- Digitale Infrastrukturen
- Digitale Wirtschaft und digitales Arbeiten
- Innovativer Staat
- Digitale Lebenswelten in der Gesellschaft gestalten
- Bildung, Forschung, Wissenschaft, Kultur und Medien
- Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft
- Europäische und internationale Dimension der Digitalen Agenda

Bundesverkehrsminister Alexander Dobrindt, Bundesinnenminister Dr. Thomas de Maizière und Bundeswirtschaftsminister Sigmar Gabriel (v.l.n.r.)

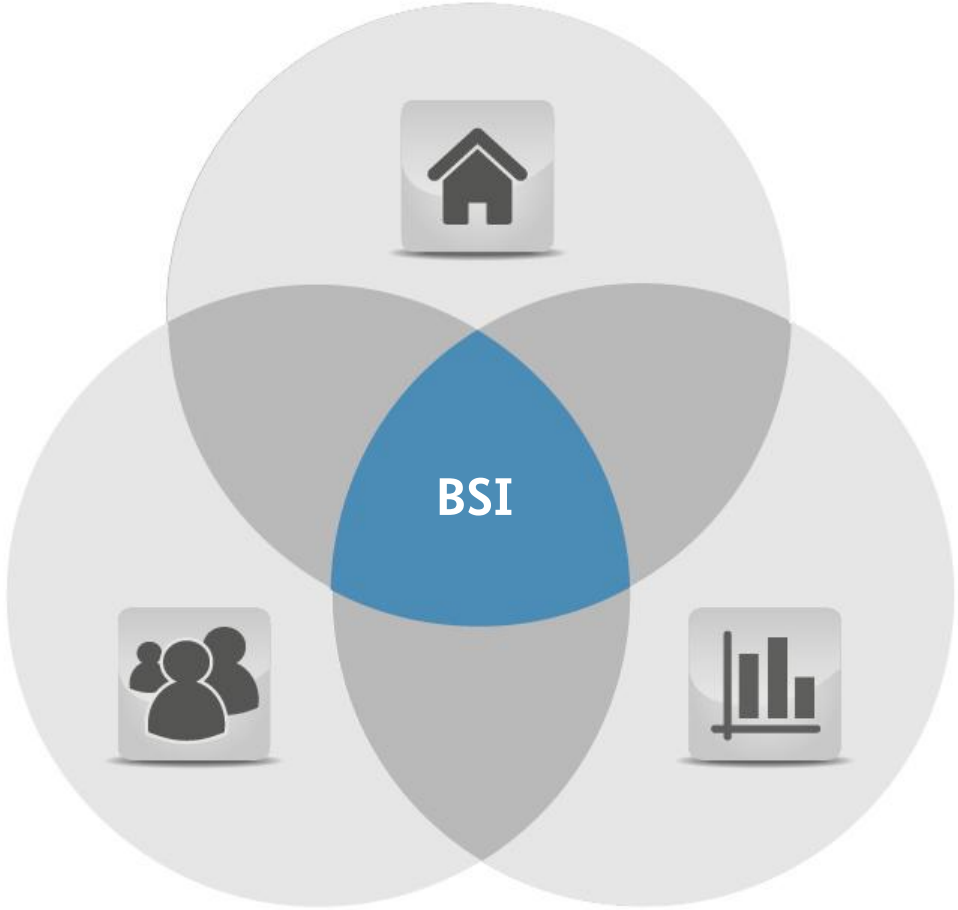
Digitale Agenda 2014 – 2017

www.digitale-agenda.de

- Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft
  - Mehr Schutz für Bürgerinnen und Bürger und Unternehmen im Netz
  - Moderner Datenschutz für das Informationszeitalter
  - Verbraucherschutz in der digitalen Welt
  - Digitale Infrastrukturen als Vertrauensraum stärken
  - Mehr Sicherheit im Cyberraum

3. Allianz für Cyber-Sicherheit

Zielgruppen des BSI



Operativ
- Bundesverwaltung

Informativ
- Bürgerinnen und Bürger

Kooperativ
- Wirtschaft
- Forschung
- Medien

Bundesamt
für Sicherheit in der
Informationstechnik

Akteure der Allianz für Cyber-Sicherheit

Bundesamt für Sicherheit in der Informationstechnik

Beirat

» BITKOM
» BDI » DIHK
» GI » VDMA
» VOICE » ZVEI
» BMI » BSI

Angebote

» Info-Pool
» Partner-Beiträge
» Meldestelle
» Veranstaltungen
» Erfahrungsaustausch

Teilnehmer:	**Partner:**	**Multiplikatoren:**
über 1.300	über 80	über 40

4. IT-Grundschutz-Modernisierung

Motivation und Zeitplan

20 Jahre IT-Grundschutz – und nun?

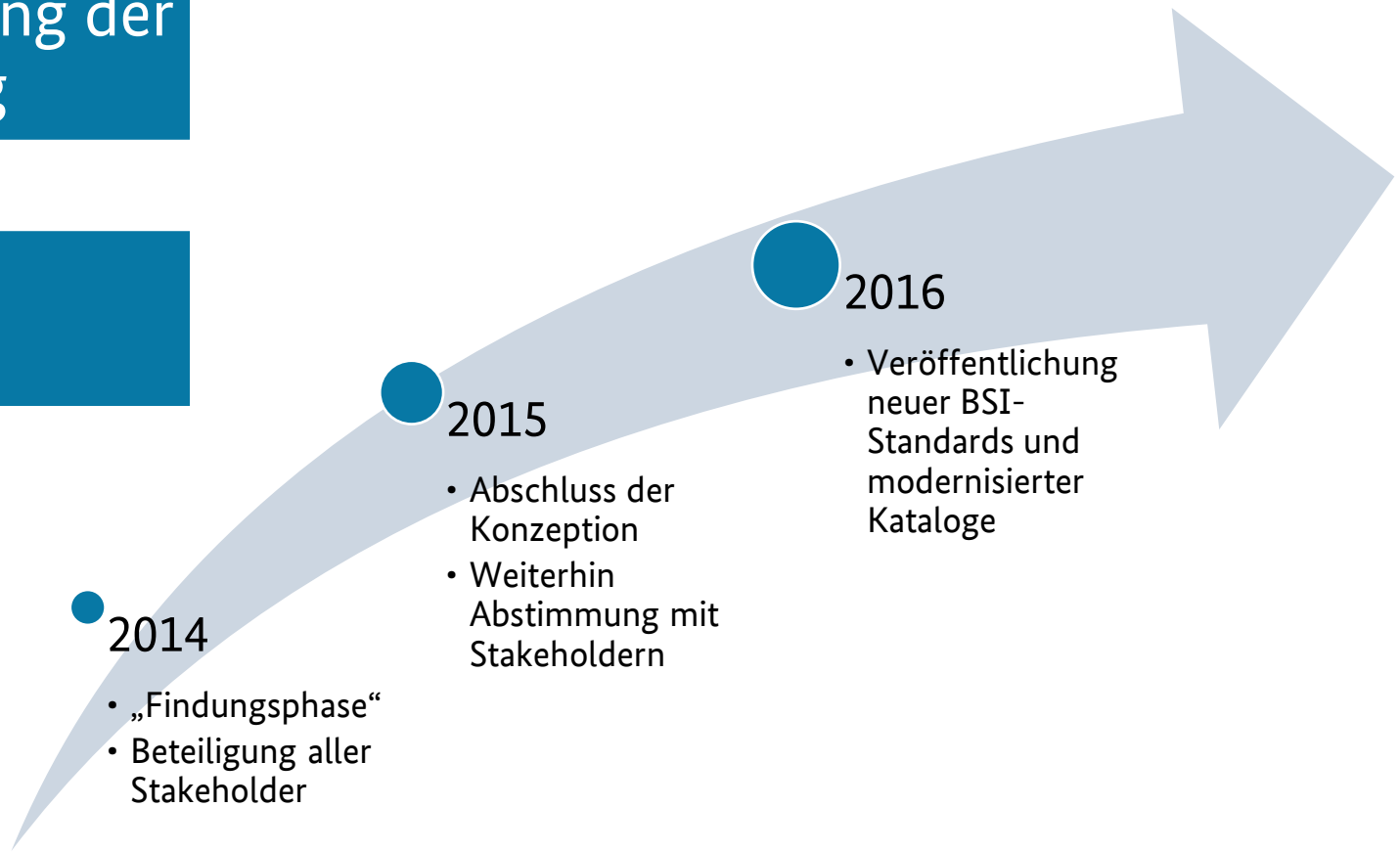
- Neue Anforderungen nach 20 Jahren
- Optimierung und Aktualisierung der Vorgehensweise und IT-Grundschutz-Kataloge
- Der „neue“ IT-Grundschutz muss dem Bedarf der Anwender an einem aktuellen und praxisnahen Verfahren gerecht werden
- Gewährleistung der Kontinuität:
  - Weiterentwicklung der „alten“ IT-Grundschutz-Welt
  - Neuausrichtung durch (größtenteils) separate Ressourcen
- Ziel:
  - Erhöhung der Attraktivität und Wegbereitung für die nächsten 20 Jahre

Zeitliche Planung

Parallele Veröffentlichung der 15. Ergänzungslieferung

GSTOOL-Pflege:

- Metadaten-Updates für die Ergänzungslieferungen
- Austauschschnittstelle
- Support bis mindestens Ende 2016

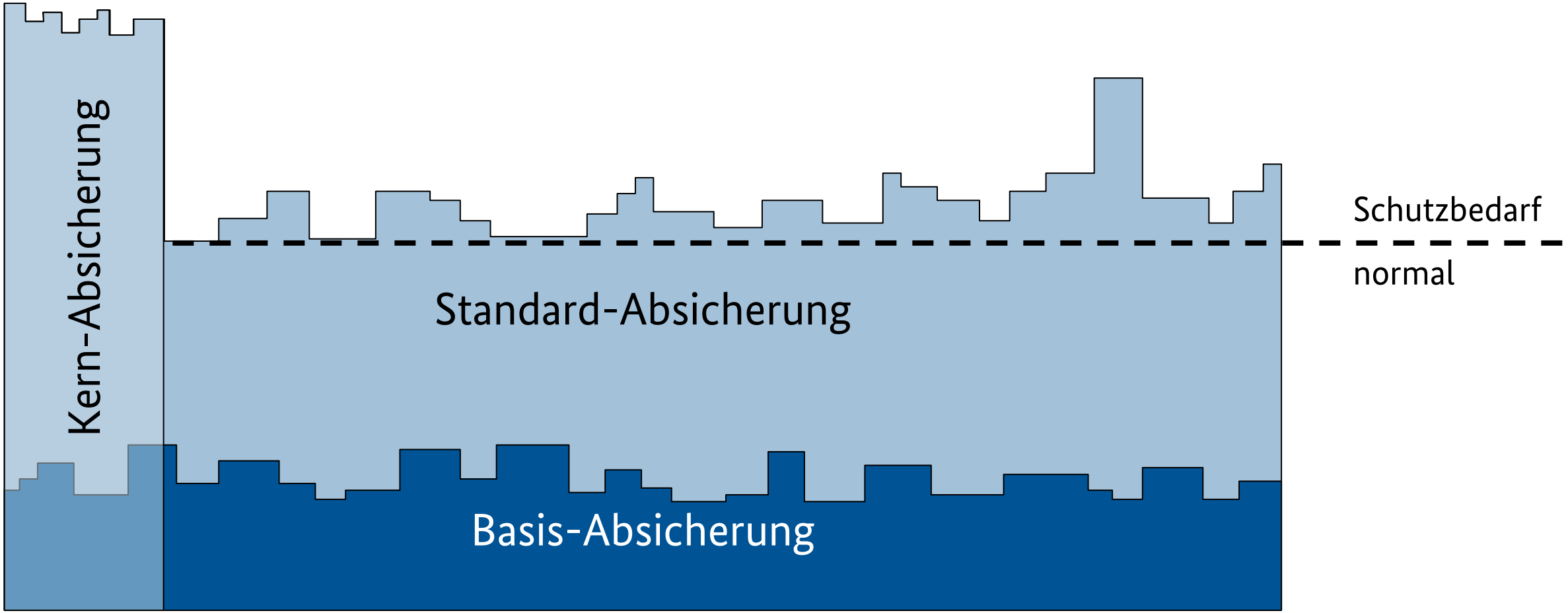


Bundesamt für Sicherheit in der Informationstechnik

4. IT-Grundschutz-Modernisierung

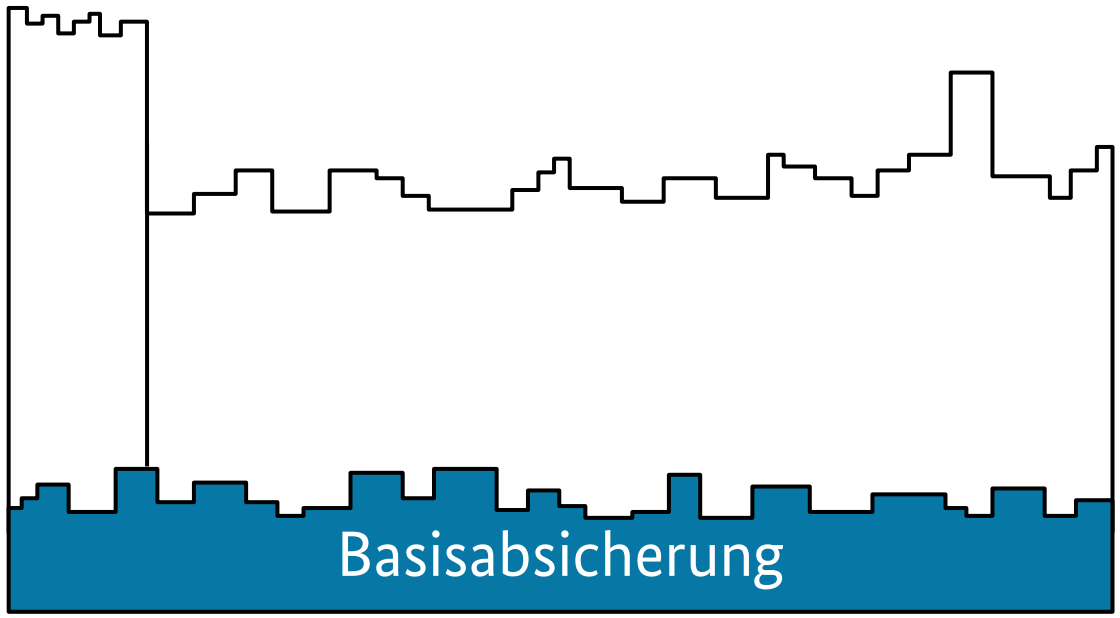
Vorgehensweisen

Vorgehensweisen – Überblick

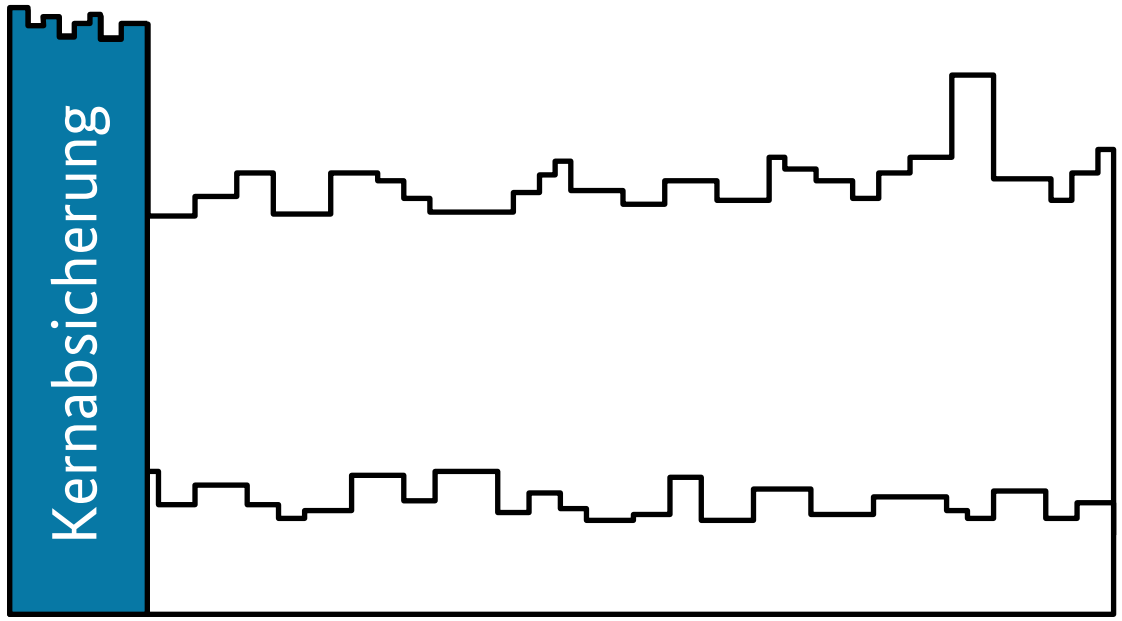


Vorgehensweisen – Basisabsicherung

- Vereinfachter Einstieg in das Sicherheitsmanagement
- Grundlegende Erstabsicherung der Geschäftsprozesse und Ressourcen
  - Erstabsicherung in der Breite
  - Umsetzung essentieller Anforderungen
- Auf die Bedürfnisse von KMUs zugeschnitten
- Auch für kleine Institutionen geeignet



Vorgehensweisen – Kernabsicherung



- Schutz herausragender, besonders gefährdeter Geschäftsprozesse und Ressourcen („Kronjuwelen“)
- Unterschied zu IT-Grundschutz Classic: Fokussierung auf einen kleinen, aber sehr wichtigen Informationsverbund
- Zeitersparnis im Vorgehen
- beschleunigte Absicherung dieser Ressourcen in der Tiefe

Vorgehensweisen – Standardabsicherung

- Die Methode bleibt in den Grundzügen unverändert.
- Implementierung eines vollumfänglichen Sicherheitsprozesses nach (jetzigem) BSI-Standard 100-2
- Weiterhin ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz vorgesehen

Vorgehensweisen – Einstieg

Entscheidung der Leitungsebene, Informationssicherheit zu verbessern

Benennung des Verantwortlichen für Informationssicherheit

Konzeption und Planung: Einstieg Informationssicherheit

- Ermittlung Rahmenbedingungen
- Formulierung allgemeiner Sicherheitsziele
- Bestimmung angestrebtes Sicherheitsniveau

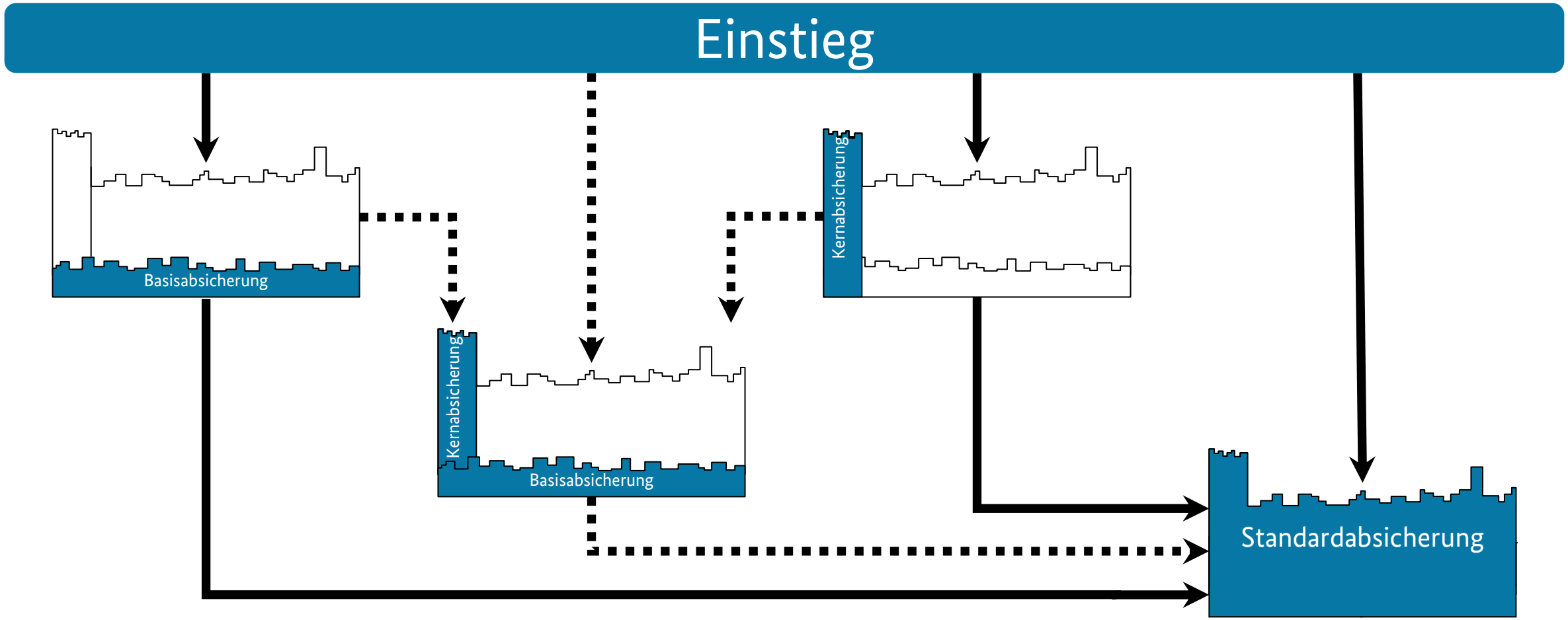
Ersterfassung

- Von Geschäftsprozessen/Fachaufgaben, Anwendungen und IT-Systemen

Entscheidung über weitere Vorgehensweise

- Legt Geltungsbereich fest

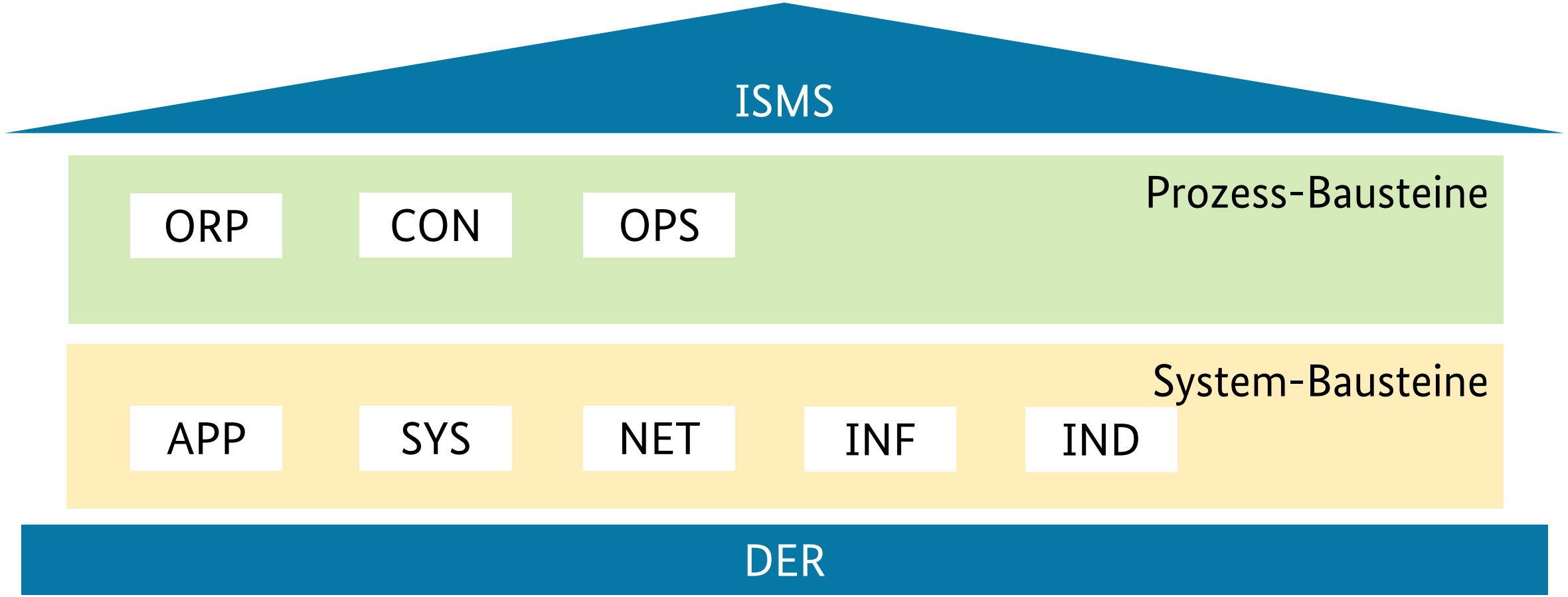
Vorgehensweisen – Wege zur Standardabsicherung



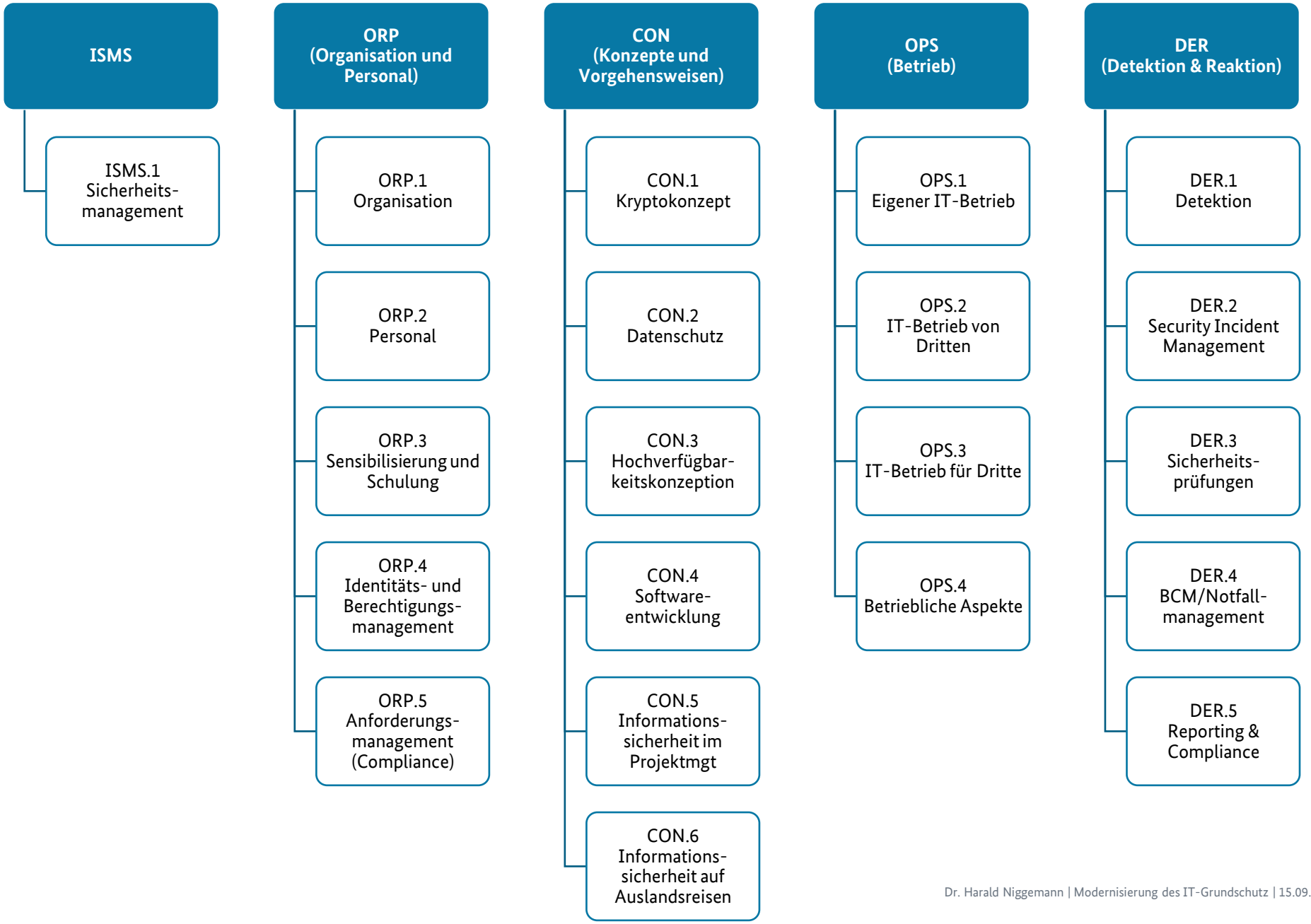
4. IT-Grundschutz-Modernisierung

Struktur der Kataloge

Kataloge – Nachfolger des Schichtenmodells

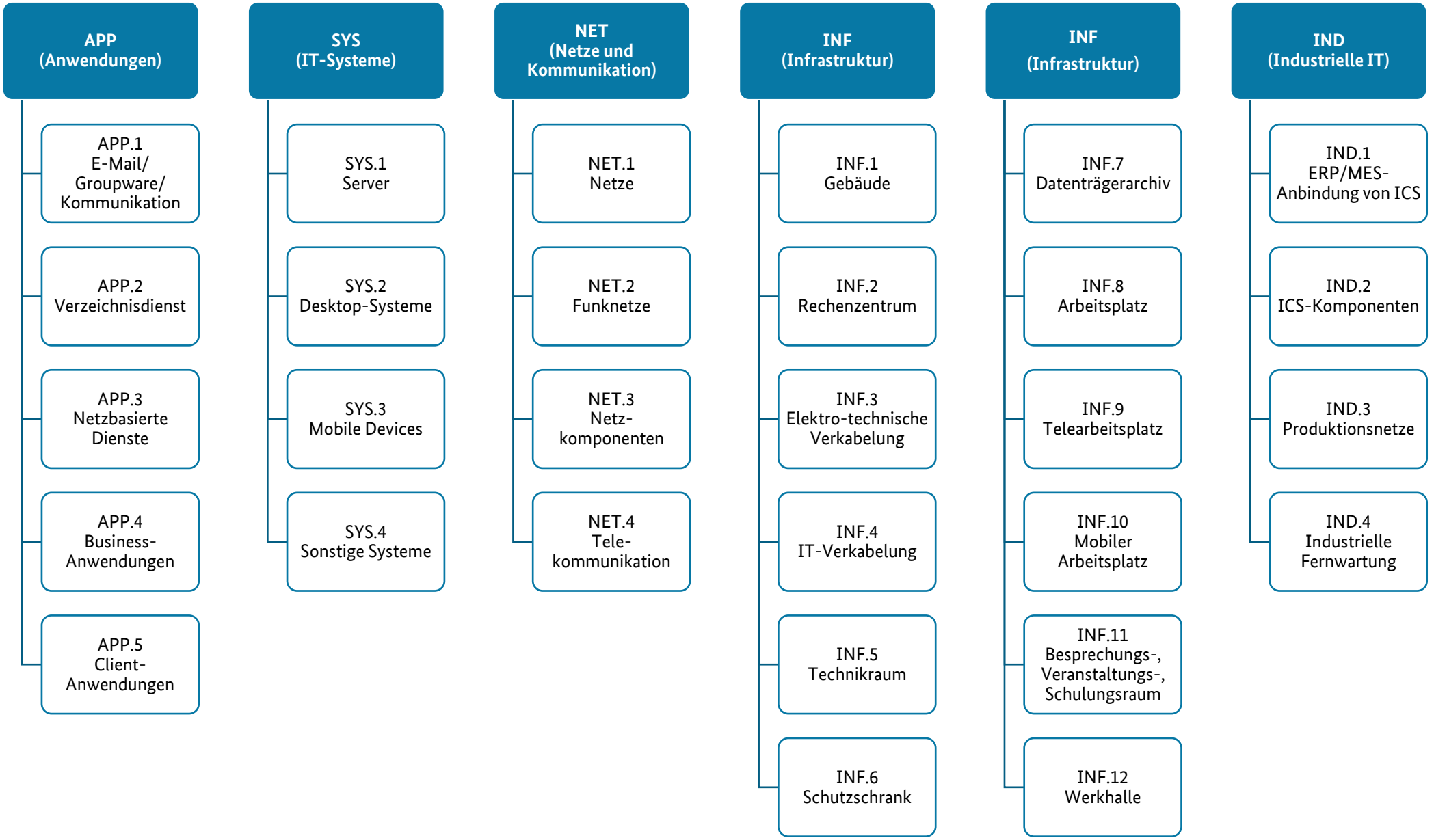


Kataloge – Prozess-Bausteine



Bundesamt für Sicherheit in der Informationstechnik

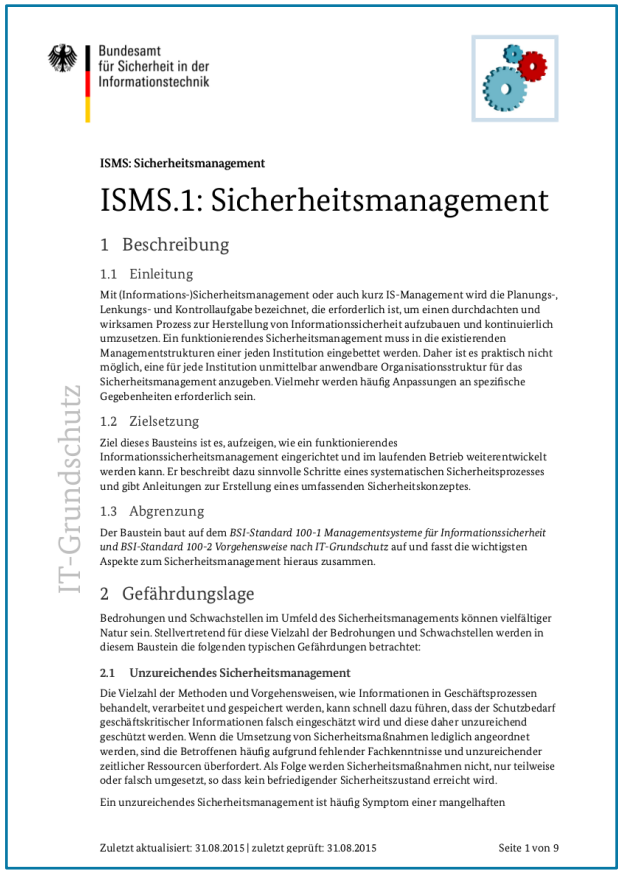
Kataloge – System-Bausteine



Bundesamt für Sicherheit in der Informationstechnik

Kataloge – modernisierte Bausteine

- Umfang: ca. 10 Seiten!
- Beschreibung: Einleitung, Zielsetzung, Abgrenzung, Verantwortliche
- Spezifische Gefährdungslage
- Keine Maßnahmen, sondern Anforderungen:
  - Basis-Anforderungen
  - Standard-Anforderungen
  - Anforderungen bei erhöhtem Schutzbedarf
- Referenzen auf weiterführende Informationen
- Anlage:
  Kreuzreferenztabelle Anforderungen ←→ Elementare Gefährdungen



Bundesamt
für Sicherheit in der
Informationstechnik

ISMS: Sicherheitsmanagement

ISMS.1: Sicherheitsmanagement

1 Beschreibung

1.1 Einleitung

Mit (Informations-)Sicherheitsmanagement oder auch kurz IS-Management wird die Planungs-, Lenkungs- und Kontrollaufgabe bezeichnet, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen. Ein funktionierendes Sicherheitsmanagement muss in die existierenden Managementstrukturen einer jeden Institution eingebettet werden. Daher ist es praktisch nicht möglich, eine für jede Institution unmittelbar anwendbare Organisationsstruktur für das Sicherheitsmanagement anzugeben. Vielmehr werden häufig Anpassungen an spezifische Gegebenheiten erforderlich sein.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, aufzeigen, wie ein funktionierendes Informationssicherheitsmanagement eingerichtet und im laufenden Betrieb weiterentwickelt werden kann. Er beschreibt dazu sinnvolle Schritte eines systematischen Sicherheitsprozesses und gibt Anleitungen zur Erstellung eines umfassenden Sicherheitskonzeptes.

1.3 Abgrenzung

Der Baustein baut auf dem *BSI-Standard 100-1 Managementsysteme für Informationssicherheit und BSI-Standard 100-2 Vorgehensweise nach IT-Grundschutz* auf und fasst die wichtigsten Aspekte zum Sicherheitsmanagement hieraus zusammen.

2 Gefährdungslage

Bedrohungen und Schwachstellen im Umfeld des Sicherheitsmanagements können vielfältiger Natur sein. Stellvertretend für diese Vielzahl der Bedrohungen und Schwachstellen werden in diesem Baustein die folgenden typischen Gefährdungen betrachtet:

2.1 Unzureichendes Sicherheitsmanagement

Die Vielzahl der Methoden und Vorgehensweisen, wie Informationen in Geschäftsprozessen behandelt, verarbeitet und gespeichert werden, kann schnell dazu führen, dass der Schutzbedarf geschäftskritischer Informationen falsch eingeschätzt wird und diese daher unzureichend geschützt werden. Wenn die Umsetzung von Sicherheitsmaßnahmen lediglich angeordnet werden, sind die Betroffenen häufig aufgrund fehlender Fachkenntnisse und unzureichender zeitlicher Ressourcen überfordert. Als Folge werden Sicherheitsmaßnahmen nicht, nur teilweise oder falsch umgesetzt, so dass kein befriedigender Sicherheitszustand erreicht wird.

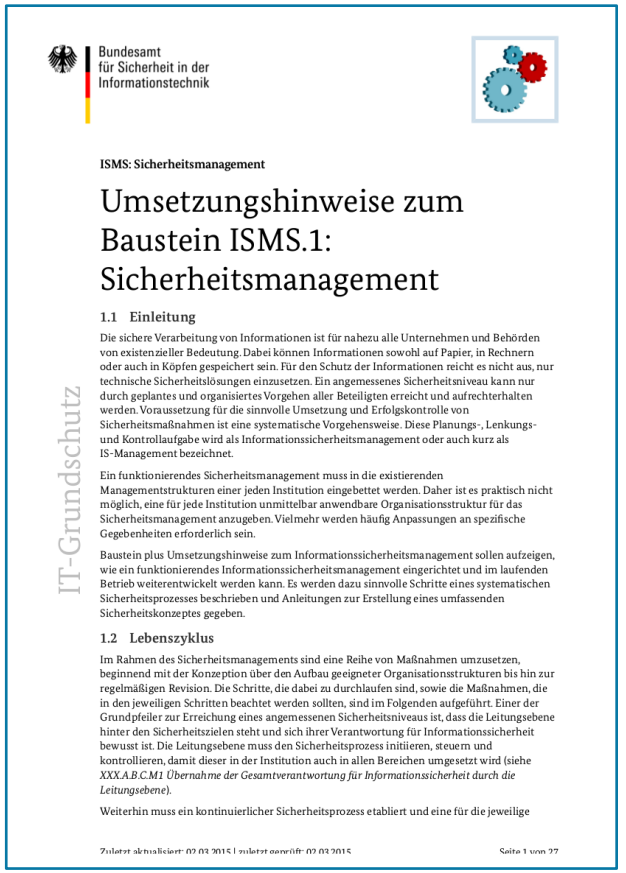
Ein unzureichendes Sicherheitsmanagement ist häufig Symptom einer mangelhaften

Zuletzt aktualisiert: 31.08.2015 | zuletzt geprüft: 31.08.2015 Seite 1 von 9

IT-Grundschutz

Kataloge – Umsetzungshinweise

- Umfang: beliebig
- Gliederung lehnt sich an Bausteine an
- Beschreibung: Einleitung, Lebenszyklus
- Maßnahmen als Umsetzungshilfen
  - Basis-Maßnahmen
  - Standard-Maßnahmen
  - Maßnahmen bei erhöhtem Schutzbedarf
- Referenzen auf weiterführende Informationen
  - Alte IT-GS-Bausteine, Studien, Herstellerdokumentation etc.



Bundesamt
für Sicherheit in der
Informationstechnik

ISMS: Sicherheitsmanagement

Umsetzungshinweise zum Baustein ISMS.1: Sicherheitsmanagement

1.1 Einleitung

Die sichere Verarbeitung von Informationen ist für nahezu alle Unternehmen und Behörden von existenzieller Bedeutung. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Für den Schutz der Informationen reicht es nicht aus, nur technische Sicherheitslösungen einzusetzen. Ein angemessenes Sicherheitsniveau kann nur durch geplantes und organisiertes Vorgehen aller Beteiligten erreicht und aufrechterhalten werden. Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von Sicherheitsmaßnahmen ist eine systematische Vorgehensweise. Diese Planungs-, Lenkungs- und Kontrollaufgabe wird als Informationssicherheitsmanagement oder auch kurz als IS-Management bezeichnet.

Ein funktionierendes Sicherheitsmanagement muss in die existierenden Managementstrukturen einer jeden Institution eingebettet werden. Daher ist es praktisch nicht möglich, eine für jede Institution unmittelbar anwendbare Organisationsstruktur für das Sicherheitsmanagement anzugeben. Vielmehr werden häufig Anpassungen an spezifische Gegebenheiten erforderlich sein.

Baustein plus Umsetzungshinweise zum Informationssicherheitsmanagement sollen aufzeigen, wie ein funktionierendes Informationssicherheitsmanagement eingerichtet und im laufenden Betrieb weiterentwickelt werden kann. Es werden dazu sinnvolle Schritte eines systematischen Sicherheitsprozesses beschrieben und Anleitungen zur Erstellung eines umfassenden Sicherheitskonzeptes gegeben.

1.2 Lebenszyklus

Im Rahmen des Sicherheitsmanagements sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über den Aufbau geeigneter Organisationsstrukturen bis hin zur regelmäßigen Revision. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt. Einer der Grundpfeiler zur Erreichung eines angemessenen Sicherheitsniveaus ist, dass die Leitungsebene hinter den Sicherheitszielen steht und sich ihrer Verantwortung für Informationssicherheit bewusst ist. Die Leitungsebene muss den Sicherheitsprozess initiieren, steuern und kontrollieren, damit dieser in der Institution auch in allen Bereichen umgesetzt wird (siehe *XXX.A.B.C.M1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene*).

Weiterhin muss ein kontinuierlicher Sicherheitsprozess etabliert und eine für die jeweilige

Zuletzt aktualisiert: 02.03.2015 | zuletzt geprüft: 02.03.2015 Seite 1 von 27

IT-Grundschutz

4. IT-Grundschutz-Modernisierung

Profile und Tools

IT-Grundschutz-Profile – Überblick

- Werkzeug für anwenderspezifische Empfehlungen
- Berücksichtigt Möglichkeiten und Risiken der Institution
- Profile beziehen sich auf typische IT-Szenarien, zum Beispiel:
  - Kommunalverwaltung in Bundesland XY
  - Krankenhaus
  - Wasserwerk als kritische Infrastruktur
- Profile werden in der Regel durch Dritte (Verbände, Branchen, …) erstellt, nicht durch das BSI
- Nicht als BSI-Vorgabe zu verstehen
- Nachweis für Umsetzung (z. B. Testat) wird diskutiert

IT-Grundschutz-Profile als pauschalisierte Vorauswahl

Beschreibung des Informationsverbunds	• Übersicht der berücksichtigten Objekte • Eventuell Referenzarchitektur
Basierende Vorgehensweise	• Beschreibt die Anwendung des Profils • Vereinfacht die Vergleichbarkeit mit anderen Profilen
Auswahl Bausteine	• Portfolio aus „offiziellen“ und „benutzerdefinierten“ Bausteinen
Auswahl Anforderungen	• Zusammenstellung aus ausgewählten Bausteinen
(opt.) Ergänzende Anforderungen	• Einzelne Anforderungen aus nicht ausgewählten Bausteinen • Branchenspezifische Anforderungen

GSTOOL

- Support des GSTOOLs bis Ende 2016
- Die Verfügbarkeit einer geeigneten zukünftigen Toolunterstützung wird sichergestellt:
  - Enger Austausch mit Herstellern
  - Offenlegung der GSTOOL-Exportschnittstelle
  - Unterstützung der Migration „alt“ auf „neu“
  - Definition eines Austauschformats zwischen Tools
- Prüfung der Möglichkeit einer zentralen Finanzierung für Bundesbehörden (z. B. über einen zentralen Sondertatbestand)
- Ziel: Markt stellt geeignete Tools im Jahr 2016 bereit

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Dr. Harald Niggemann
Cyber Security Strategist
harald.niggemann@bsi.bund.de
Tel. +49 (0) 228 99 9582 5368
Fax +49 (0) 228 99 109582 5368

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185 - 189
53175 Bonn
www.bsi.bund.de
www.bsi-fuer-buerger.de

Bundesamt
für Sicherheit in der
Informationstechnik