Tipps zur Anwendung des neuen IT-Grundschutzes

Verinice.XP

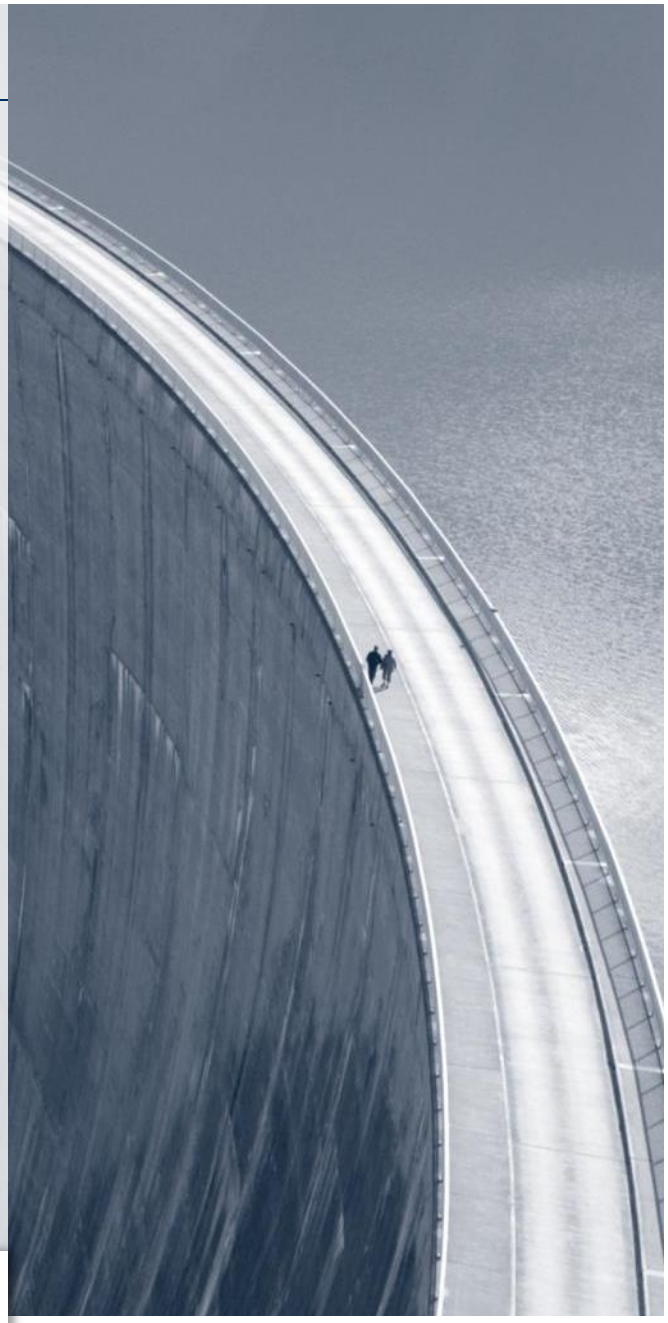
Philipp Neumann

Information Security Management Consultant

HISOLUTIONS

AGENDA

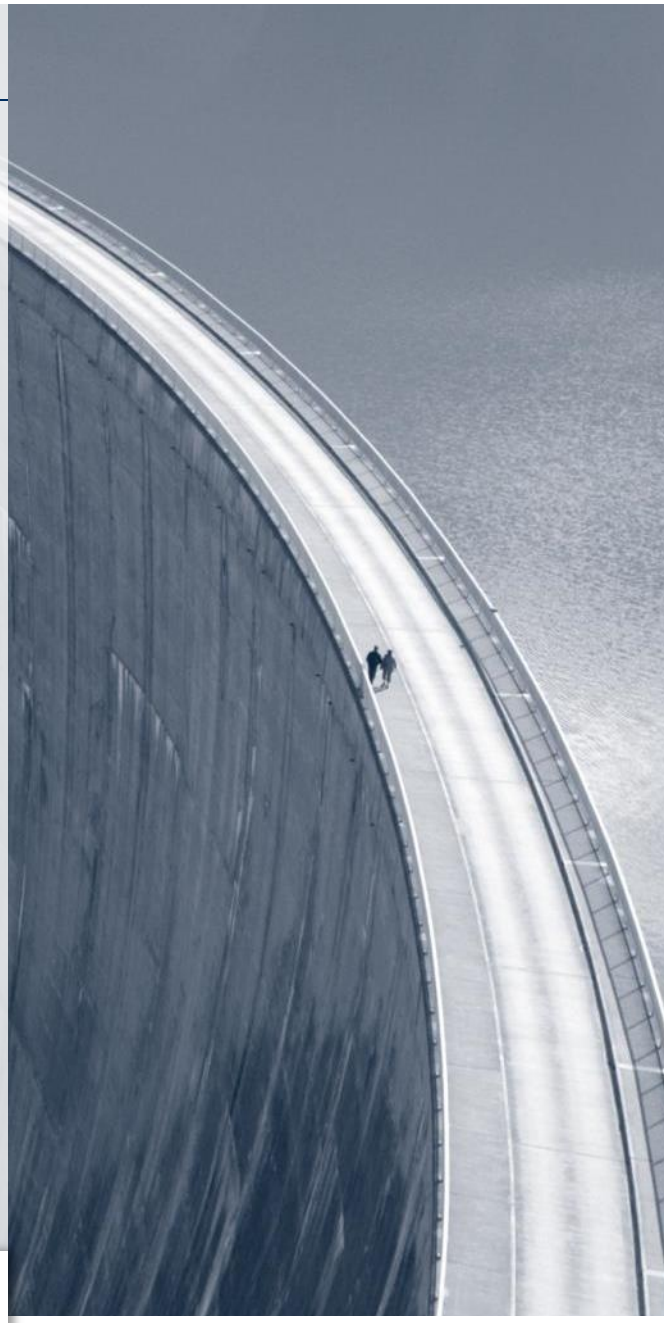
1 Vorstellung
2 Wissenswertes zur Grundschutzmodernisierung für Anwender
3 Migration
4 Zusammenfassung



HISOLUTIONS

AGENDA

1 **Vorstellung**
2 Wissenswertes zur Grundschutzmodernisierung für Anwender
3 Migration
4 Zusammenfassung



HISOLUTIONS

Vorstellung

Philipp Neumann

Consultant
Information Security Management, HiSolutions AG

Qualifikationen

- Lead Implementer gem. ISO 27001
- IHK-Sachkunde § 34a GewO
- Luftsicherheit
- verinice.PARTNER

Beruflicher Hintergrund

- Mitarbeiter der Objektleitung, Gegenbauer Sicherheitsdienste GmbH
- Information Security Management Consultant, HiSolutions AG

Tätigkeitsbereiche

- Vorbereitung der Zertifizierung nach ISO/IEC 27001 auf Basis von BSI-IT-Grundschutz und ISO/IEC 27001 native
- Zertifizierungsvorbereitung ISO 27001
- Erstellung von Sicherheitsrichtlinien und -konzepten
- verinice/verinice.PRO (ISMS-Tool)
- HiScout (ISMS-Tool)

Vorstellung HiSolutions AG

Gründung	**1992**
Eigentümer	**Gründergeführt und unabhängig** ⇨ Michael Langhoff, Torsten Heinrich und Prof. Timo Kob
Märkte	**International (Kerngeschäft D/A/CH)**
Kunden	**500+** ⇨ alle Branchen ⇨ 50 % der DAX-Unternehmen und stark im Mittelstand ⇨ 75 % der deutschen Top20-Banken ⇨ öffentliche Verwaltung in Bund, Ländern und Kommunen ⇨ Non-Profit-Organisationen
Projekte	**200+ jährlich**
Mitarbeiter	**120** ⇨ kontinuierlich langsam wachsend
Engagement	**Lehrtätigkeit an verschiedenen Hochschulen in Deutschland und Österreich**

HISOLUTIONS

Vorstellung HiSolutions AG

Leistungsportfolio

Business Security & Crisis Management

Business Continuity & Risk Management

IT Risk & Information Security Management

System Security

IT-Strategy & Governance

IT-Service Management

Security – Governance – Risk – Compliance

HISOLUTIONS

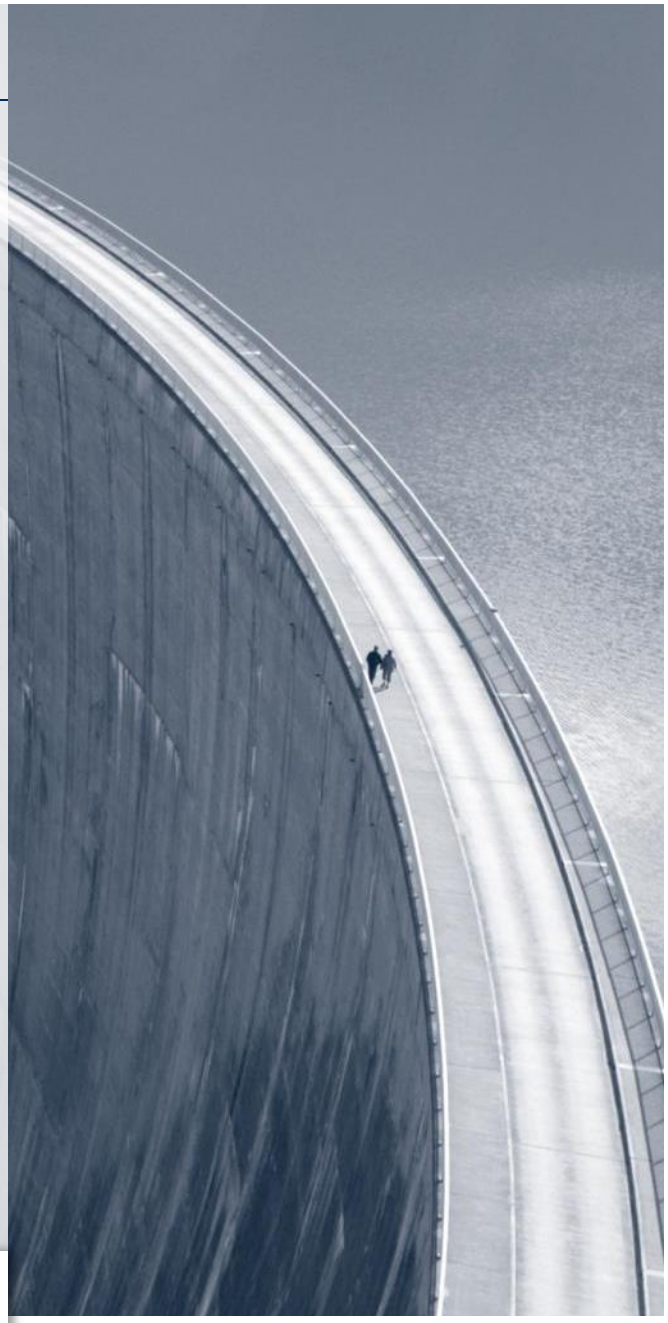
AGENDA

1 Vorstellung

2 Wissenswertes zur Grundschutzmodernisierung

3 Migration

4 Zusammenfassung



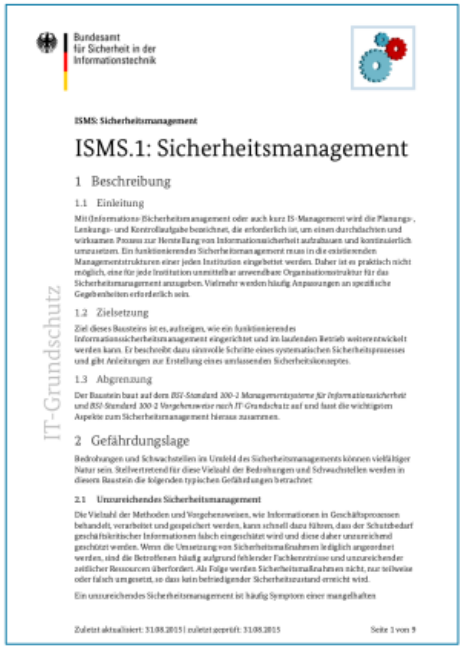
HISOLUTIONS

Wissenswertes zur Grundschutzmodernisierung

Modernisierte Bausteine
Dokumentenstruktur

- Umfang: ca. 10 Seiten!
- Beschreibung
  - Einleitung
  - Zielsetzung
  - Abgrenzung
  - Verantwortliche
- Spezifische Gefährdungslage
- Anforderungen (keine Maßnahmen)
  - Basis-Anforderungen
  - Standard-Anforderungen
  - Anforderungen bei erhöhtem Schutzbedarf
- Referenzen auf weiterführende Informationen

Anlage: Kreuzreferenztabelle



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, aufzuzeigen, 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

Bundesamt
für Sicherheit in der
Informationstechnik

HISOLUTIONS

Wissenswertes zur Grundschutzmodernisierung

Bausteine

Kapitel 1.1 Abgrenzung:

- Indirekte Modellierungsvorschläge

Kapitel 2 Gefährdungslage:

- Kapitel dient zur Sensibilisierung der Anwender
- Die spezifischen Gefährdungen bestehen aus:
  1. Erläuterung
  2. Ursache
  3. Wirkung/Auswirkung

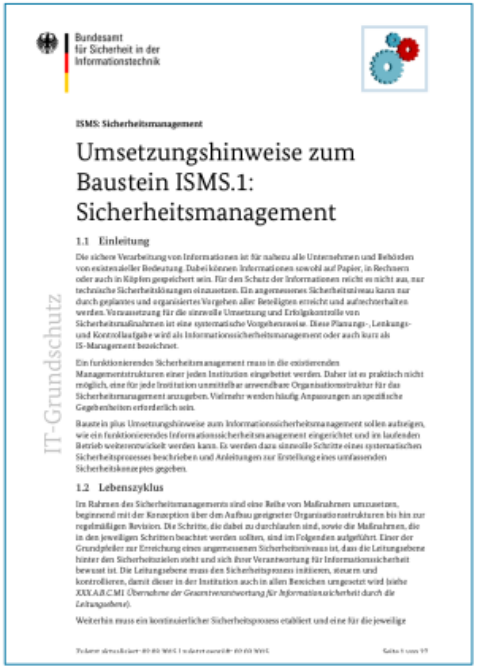
Kapitel 3 Anforderungen:

- Bausteinverantwortlicher ist verantwortlich für Erfüllung der Anforderungen
- Einbindung des Informationssicherheitsbeauftragten bei strategischen Entscheidungen

Wissenswertes zur Grundschutzmodernisierung

Umsetzungshinweise
Dokumentenstruktur

- 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

IT-Grundschutz

1.2 Lebenszyklus

Bundesamt
für Sicherheit in der
Informationstechnik

HISOLUTIONS

Wissenswertes zur Grundschutzmodernisierung

Umsetzungshinweise

Kapitel 1.2 Lebenszyklus:

- Indirekte Modellierungsvorschläge in der Lebenszyklusphase „Planung und Konzeption“

Kapitel 3.1 Wissenswertes:

- Bildet alte W-Maßnahmen (Hintergrundwissen) des BSI IT-Grundschutzes ab

HISOLUTIONS

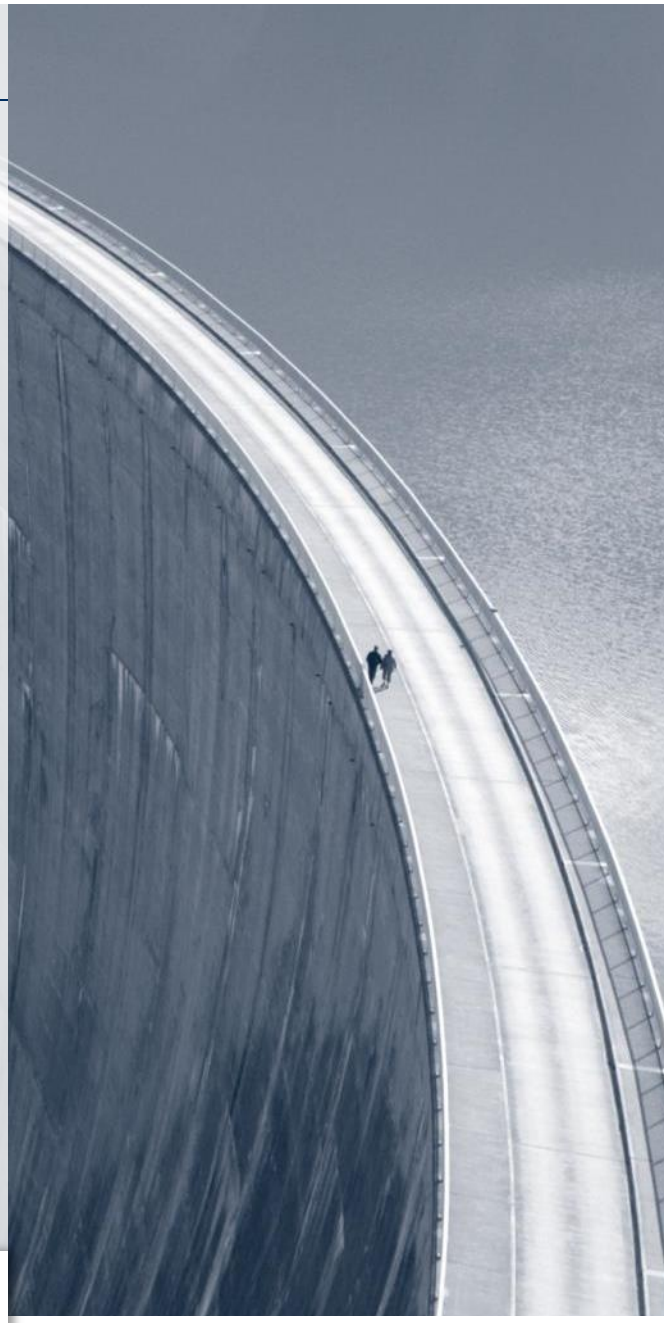
Wissenswertes zur Grundschutzmodernisierung

Begleitdokumente

- Liste mit Fachtermini zu Bausteinen (Deutsch/Englisch)
- Vorschläge für Änderungen/Ergänzungen an bereits veröffentlichten Inhalten der IT-Grundschutzmodernisierung
- Glossar (Begriffsdefinitionen)
- Abkürzungsverzeichnis

AGENDA

1 Vorstellung
2 Wissenswertes zur Grundschutzmodernisierung
3 Migration
4 Zusammenfassung



HISOLUTIONS

Migration - Ausgangsbasis

Basis:

- Bausteine aus dem BSI IT-Grundschutz und der BSI IT-Grundschutzmodernisierung
- Community Drafts der neuen Bausteine und Umsetzungshinweise
- Migrationstabellen

Ziel:

- Generisches Migrationskonzept
- Erprobung am bestehenden IT-Sicherheitskonzept eines mittelständischen Unternehmens
- Erstellung eines Migrationstools

Hinweis
Abweichungen sind aufgrund der fortwährenden Entwicklung der BSI IT-Grundschutzmodernisierung möglich!

Migration - Vorgehensweise

Methodik:

- Entwicklung einer einheitlichen Methodik zur Untersuchung der vom BSI veröffentlichten Community Drafts und Migrationstabellen
- Entwurf eines Migrationsmodels auf Basis der Stichprobe
- Anwendung des Migrationsmodels auf die äquivalenten Bausteine des BSI IT-Grundschutzes
- Verprobung der entwickelten Methodik am bestehenden IT-Sicherheitskonzept eines mittelständischen Unternehmens

Ergebnis:

Identifizierte Szenarien	
1:1	Alte und neue Maßnahmen wurden 1:1 gemappt
1:1+	Die neue Maßnahme wurde um zusätzliche Anforderungen ergänzt
1:n	Eine alte Maßnahme wurde auf mehrere neue Maßnahmen gemappt
n:1	Mehrere alte Maßnahmen gehören zu einer neuen Maßnahme
n:n	Mehrere alte Maßnahmen mappen auf mehrere neue Maßnahmen
0:1	Es gab noch kein Vorgehen im alten IT-Grundschutz – komplett neu Umzusetzen
1:0	Der neue Grundschutz sieht die Umsetzung bei Basis-Schutzbedarf nicht vor

Migration - Ergebnisse

Szenario 1 - Anforderung wurde **1:1** gemappt

- Eine alte Maßnahme mappt auf genau eine neue Anforderung
- Keine weiteren Schritte erforderlich
- Ein 1:1 Szenario kann sich zu einem 1:n Szenario entwickeln (Anforderung in unterschiedlichen Bausteinen)

Beispiel 1:1

Alte Maßnahme:
M 4.399 - Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen

Neue Maßnahme:
APP.3.1.M4 Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen

Migration - Ergebnisse

Szenario 2 - Anforderung wurde **1:1+** gemappt

- Eine alte Maßnahme mappt auf genau eine neue Anforderung, welche jedoch um weitere neue Aspekte ergänzt wurde
- Keine weiteren Schritte erforderlich

Beispiel 1:1+

Alte Maßnahme: M 2.306 – Verlustmeldung

Neue Maßnahme: SYS.3.4.A2 Verlustmeldung mobiler Datenträger

Migration - Ergebnisse

Szenario 3 - Anforderung wurde **1:n** gemappt

- Eine alte Maßnahme mappt auf mehrere neue Anforderungen
- Themen werden ggf. unter differenzierten Gesichtspunkten oder in unterschiedlichen Bausteinen betrachtet
- Die Aufteilung einer alten Maßnahme könnte zudem für eine differenzierte Betrachtung nach dem Schutzbedarf eines Zielobjektes genutzt werden

Beispiel 1:n

Alte Maßnahme: M 2.315 Planung des Servereinsatzes

Neue Maßnahmen:

- SYS.1.1.A12 *Planung des Server-Einsatzes*
- SYS.1.1.A20 *Beschränkung des Zugangs über Netze*
- SYS.1.1.A26 *Mehr-Faktor-Authentisierung (C)*

Migration - Ergebnisse

Szenario 4 - Anforderung wurde **n:1** gemappt

- Mehrere alte Maßnahmen mappen auf eine neue Anforderung
- Keine weiteren Schritte erforderlich

Beispiel n:1

Alte Maßnahmen:

- M 2.486 Dokumentation der Architektur von Webanwendungen und Web-Services
- M 4.404 Sicherer Entwurf der Logik von Webanwendungen
- M 5.169 Systemarchitektur einer Webanwendung

Neue Maßnahme: APP.3.1.A8 *Systemarchitektur einer Webanwendung*

Migration - Ergebnisse

Szenario 5 - Anforderung wurde **n:n** gemappt

- Mehrere alte Maßnahmen mappen auf mehrere neue Anforderungen
- Szenario wird durch **1:n** und **n:1** abgedeckt

Beispiel 1:n

Alte Maßnahme: M 2.315 Planung des Servereinsatzes

Neue Maßnahmen:

- SYS.1.1.A12 *Planung des Server-Einsatzes*
- SYS.1.1.A20 *Beschränkung des Zugangs über Netze*
- SYS.1.1.A26 *Mehr-Faktor-Authentisierung (C)*

Beispiel n:1

Alte Maßnahmen:

- M 2.486 Dokumentation der Architektur von Webanwendungen und Web-Services
- M 4.404 Sicherer Entwurf der Logik von Webanwendungen
- M 5.169 Systemarchitektur einer Webanwendung

Neue Maßnahme: APP.3.1.A8 *Systemarchitektur einer Webanwendung*

Migration - Ergebnisse

Szenario 6 - Anforderung wurde **0:1** gemappt

- Es existiert keine alte Maßnahme zu der neu definierten Anforderung
- Neue Anforderungen/Maßnahmen müssen betrachtet werden
- Dient zur Identifikation von weiteren Aufwänden

Hinweis
Neue Bausteine müssen prinzipiell neu angewendet werden!

Migration - Ergebnisse

Szenario 7 - Anforderung wurde **1:0** gemappt

- Eine alte Maßnahme mappt auf keine neue Anforderung
- Maßnahme ggf. während IT-Grundschutzmodernisierung ersatzlos gestrichen

Beispiel 1:0
Alte Maßnahme: M 2.488 Web-Tracking (im neuen IT-Grundschutz nun unter „Wissenswertes“ bei Webanwendungen aufgeführt)

Szenario 8 - Anforderung wurde **0:0** gemappt

- Undefinierter Zustand, daher keine Betrachtung notwenig

Migration - Ergebnisse

Migrationstool

Automatisches Mapping alter BSI IT-Grundschutz Bausteine und Maßnahmen auf neue Bausteine und Anforderungen durch praxiserprobtes Migrationstool.

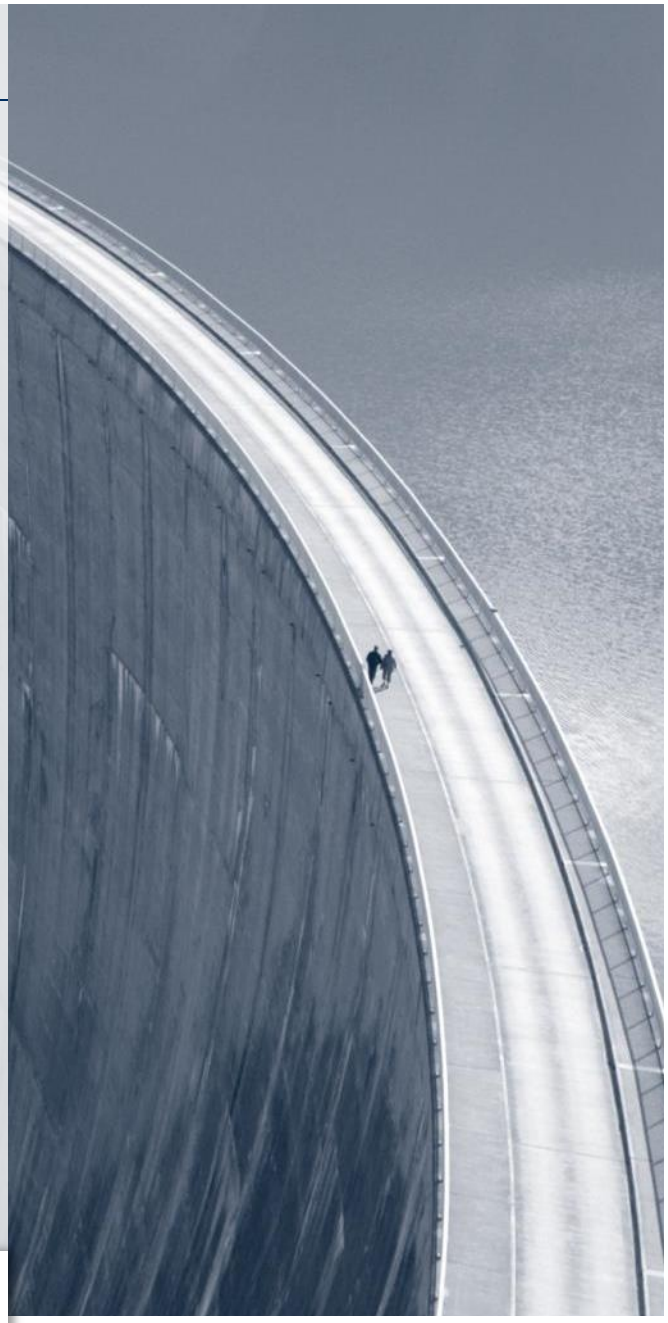
Maßnahme	Lebenszyklusphase	Maßnahme Grundschutz neu	Maßnahme Grundschutz neu (laut Dokument)
M 2.318 Sichere Installation eines IT-Systems	3 - Umsetzung	SYS.1.1.A12 Sichere Installation	
M 4.239 Sicherer Betrieb eines Servers	4 - Betrieb	SYS.1.1.A13 Einsatzfreigabe	
M 4.432 Sichere Konfiguration von Serverdiensten	1 - Planung und Konzeption	SYS.1.1.A14 Verschlüsselung der Kommunikationsverbindungen	
M 4.238 Einsatz eines lokalen Paketfilters	4 - Betrieb	SYS.1.1.A15 Einrichtung lokaler Paketfilter	
M 4.238 Einsatz eines lokalen Paketfilters	4 - Betrieb	SYS.1.1.A15 Einrichtung lokaler Paketfilter	
M 2.315 Planung des Servereinsatzes	1 - Planung und Konzeption	SYS.1.1.A16 Beschränkung des Zugriffs über Netze	SYS.1.1.A20 Beschränkung des Zugangs über Netze
M 4.239 Sicherer Betrieb eines Servers	4 - Betrieb	SYS.1.1.A17 Betriebsdokumentation	
M 4.237 Sichere Grundkonfiguration eines IT-Systems	3 - Umsetzung	SYS.1.1.A19 Systemüberwachung (A)	
M 4.237 Sichere Grundkonfiguration eines IT-Systems	3 - Umsetzung	SYS.1.1.A19 Systemüberwachung (A)	
M 4.237 Sichere Grundkonfiguration eines IT-Systems	3 - Umsetzung	SYS.1.1.A2 Restriktive Rechtevergabe	
M 4.237 Sichere Grundkonfiguration eines IT-Systems	3 - Umsetzung	SYS.1.1.A2 Restriktive Rechtevergabe	
M 4.432 Sichere Konfiguration von Serverdiensten	1 - Planung und Konzeption	SYS.1.1.A2 Restriktive Rechtevergabe	

Mapping | Ohne Mapping | Eine Alte auf mehrere Neue | Ersatzlos gestrichen | Mehrere Alte auf eine Neue | n zu n | Komplett neue

HISOLUTIONS

AGENDA

1 Vorstellung
2 Wissenswertes zur Grundschutzmodernisierung
3 Migration
4 **Zusammenfassung**



HISOLUTIONS

Zusammenfassung

Acht Szenarien zur Migration vom BSI IT-Grundschutz zur Grundschutzmodernisierung identifiziert

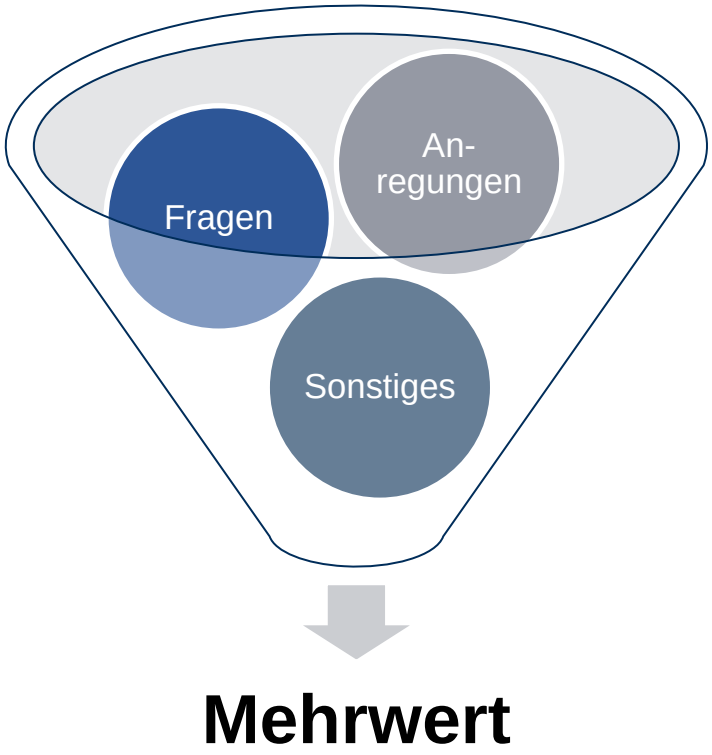
Zwei Szenarien (0:0, n:n) finden keine Anwendung

Identifikation von bereits behandelten Anforderungen bei bestehendem IT-Sicherheitskonzept dient zur Kalkulation der Migrationsaufwände

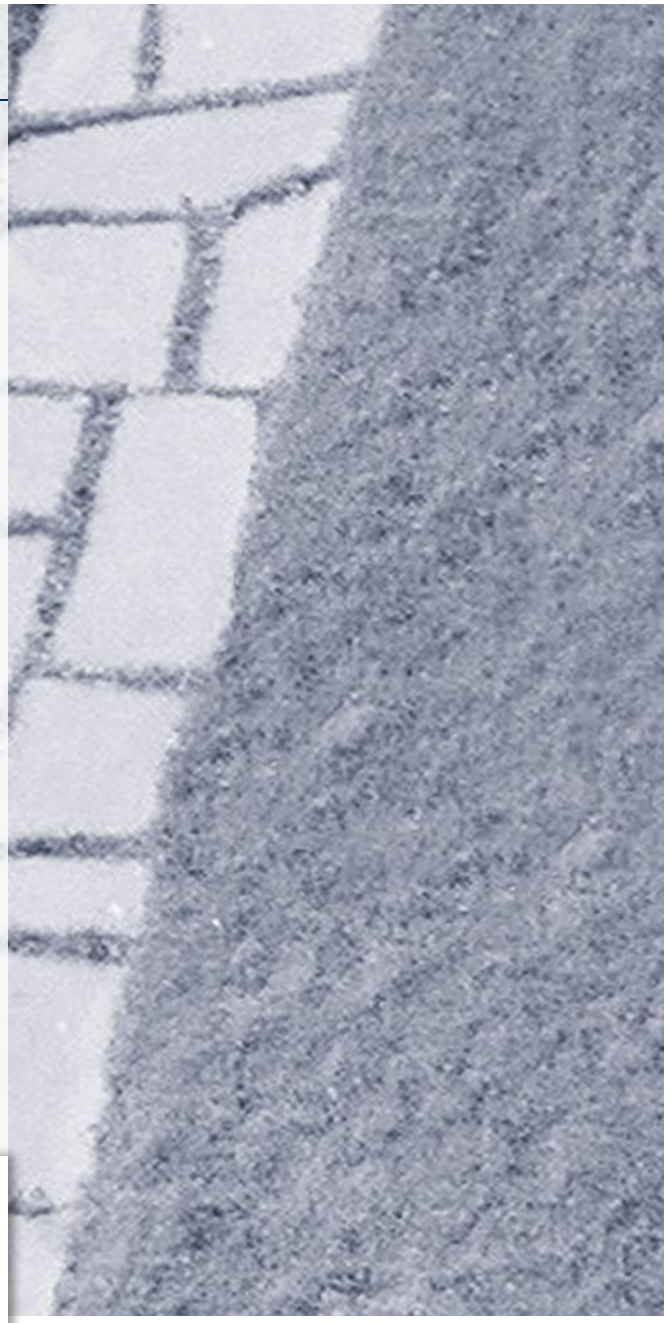
Migrationsaufwand ist initial von der Größe des Informationsverbundes abhängig

Vom BSI als Community Drafts veröffentlichte Migrationstabellen sind fehlerhaft

Fragen und Antworten



HISOLUTIONS BEDANKT SICH FÜR IHRE AUFMERKSAMKEIT



HiSolutions AG
Philipp Neumann
Information Security Management Consultant

Bouchéstraße 12
12435 Berlin
Neumann@hisolutions.com
www.hisolutions.com
+49 30 533 289 0

HISOLUTIONS