DVZ community LIVE 2025

18 - 20. MÄRZ 2025
IHK ZU SCHWERIN

DAS MULTI-EVENT FÜR DEN PUBLIC SECTOR

IN MECKLENBURG-VORPOMMERN UND DARÜBER HINAUS

Eine Veranstaltung der

DVZ Datenverarbeitungszentrum
Mecklenburg-Vorpommern GmbH

DVZ community LIVE 2025

Sicherheit mit System

Der Aufbau solider Sicherheitskonzepte

Agenda

1. **Sicherheitskonzept im Überblick**
   Definitionen und Verbindlichkeit
2. **Sicherheitskonzepte in MV**
   Behörden und DVZ im Zusammenspiel
3. **Die Sicherheitskonzeption im Detail**
   Einzelne Schritte und Praxisbeispiele aus dem Prozess
4. **Herausforderungen**
   Die Grenzen in der Bearbeitung und der Methodik
5. **Fragen und Anregungen**

DVZ community LIVE 2025

Sicherheitskonzept im Überblick

Ziele des Sicherheitskonzeptes

- **Schutz der IT-Systeme und Daten:** Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit.
- **Risikominimierung:** Erkennen und Reduzieren von Bedrohungen und Schwachstellen.
- **Standardisierte Sicherheitsmaßnahmen:** Umsetzung bewährter Schutzmaßnahmen aus dem IT-Grundschutz-Kompendium.
- **Kontinuierliche Verbesserung:** Regelmäßige Überprüfung und Anpassung des Sicherheitskonzepts.
- **Vorbereitung auf Sicherheitsvorfälle:** Entwicklung von Notfall- und Incident-Response-Strategien.

Definition Sicherheitskonzept (1/2)

Sicherheitskonzept

Ein Sicherheitskonzept dient zur **Umsetzung der Sicherheitsstrategie** und beschreibt die **geplante Vorgehensweise**, um die gesetzten Sicherheitsziele einer Institution zu erreichen.
Das Sicherheitskonzept ist das **zentrale Dokument im Sicherheitsprozess** eines Unternehmens bzw. einer Behörde. Jede konkrete Sicherheitsmaßnahme muss sich letztlich darauf zurückführen lassen.

Sicherheitskonzeption

Die Sicherheitskonzeption ist eine der **zentralen Aufgaben** des Informationssicherheitsmanagements. Aufbauend auf den Ergebnissen von Strukturanalyse und Schutzbedarfsfeststellung werden hier die erforderlichen **Sicherheitsmaßnahmen identifiziert und** im Sicherheits-konzept **dokumentiert**.

Quelle: IT-Grundschutz-Kompendium 2023

Auf welcher Grundlage werden Sikos erstellt?

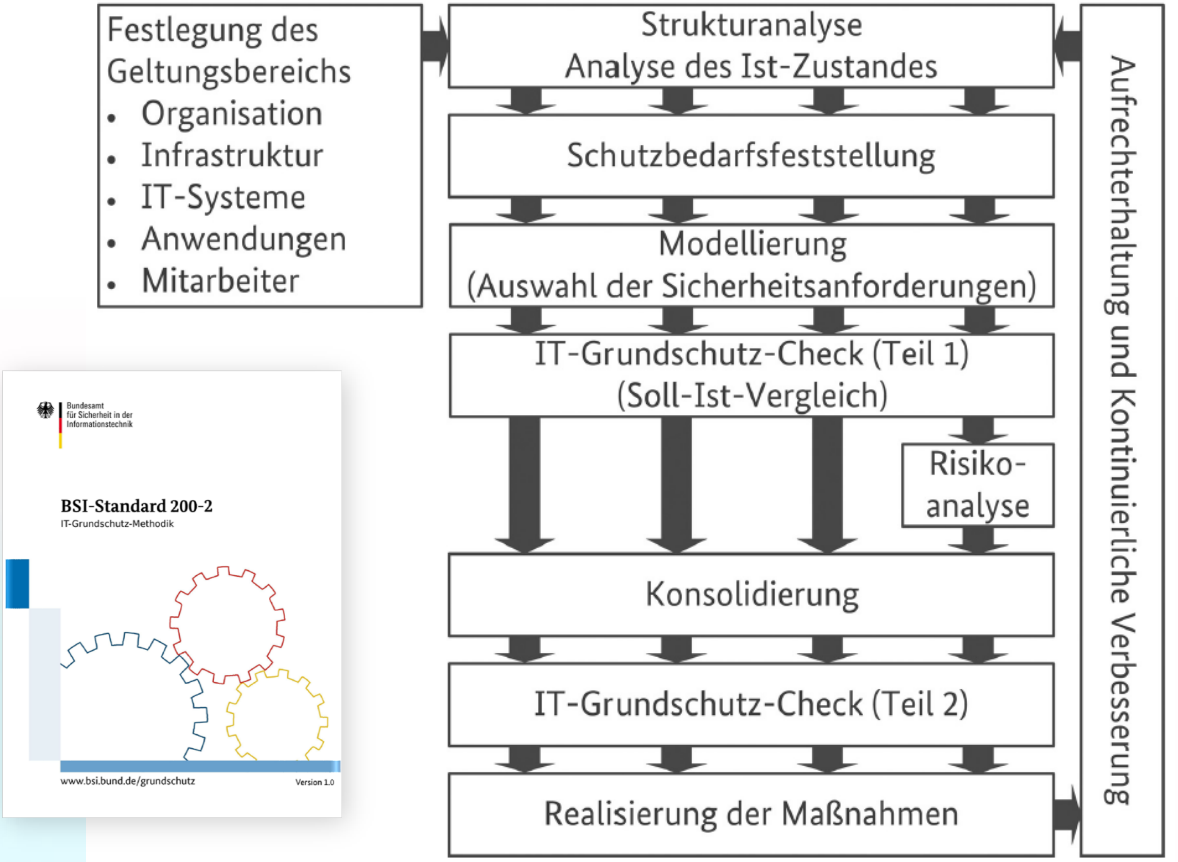
- **Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung,** 2018, Arbeitsgruppe Informationssicherheit des IT-PLR
- **Leitlinie zur Gewährung der Informationssicherheit in der Landesverwaltung M-V** (IS-Leitlinie M-V), 2014

- **Landeshaushaltsordnung**, VV Nr. 6.1.2 zu §§ 70-80 LHO (Anschlussbedingungen an HKR)
- **Schuldatenschutzverordnung** (SchulDSVO M-V), 2020

[…]

Definition Sicherheitskonzept (2/2)

- Ein auf Anforderungen und Risiken basierter Soll-Ist-Vergleich, basierend auf einem festgelegten Prozess
- Grundlage bildet BSI-Standard 200-2 „IT-Grundschutz-Methodik“
- Prozess liegt im Fokus, nicht das einzelne IT-System
- Ergebnis ist Umsetzungsplan mit dem Ziel der grundschutzkonformen Absicherung



Quelle: BSI Standard 200-2

IT-Grundschutz im Kontext einer Institution

ISMS: Sicherheitsmanagement

ORP: Organisation und Personal

CON: Konzeption und Vorgehensweise

OPS: Betrieb

DER: Detektion und Reaktion

APP: Anwendungen

SYS: IT-Systeme

NET: Netze und Kommunikation

INF: Infrastruktur

- Das Sicherheitskonzept erstreckt sich auf die gesamte Institution
- IT-Grundschutz konzentriert sich dabei auf die Organisation, Prozesse und Anwendungen
- Ein Siko für einzelne Fachverfahren, ist in der Methodik nicht vorgesehen

Sicherheitskonzepte in MV

IT-Grundschutz im Kontext MV (1/2)

ISMS: Sicherheitsmanagement

ORP: Organisation und Personal

CON: Konzeption und Vorgehensweise

DER: Detektion und Reaktion

INF: Infrastruktur

ISMS: Sicherheitsmanagement

ORP: Organisation und Personal

CON: Konzeption und Vorgehensweise

OPS: Betrieb

DER: Detektion und Reaktion

APP: Anwendungen

SYS: IT-Systeme

NET: Netze und Kommunikation

INF: Infrastruktur

IT-Grundschutz im Kontext MV (2/2)

ISMS: Sicherheitsmanagement

ORP: Organisation und Personal

CON: Konzeption und Vorgehensweise

DER: Detektion und Reaktion

INF: Infrastruktur

APP: Anwendungen
SYS: IT-Systeme

ISMS: Sicherheitsmanagement

ORP: Organisation und Personal

CON: Konzeption und Vorgehensweise

OPS: Betrieb

DER: Detektion und Reaktion

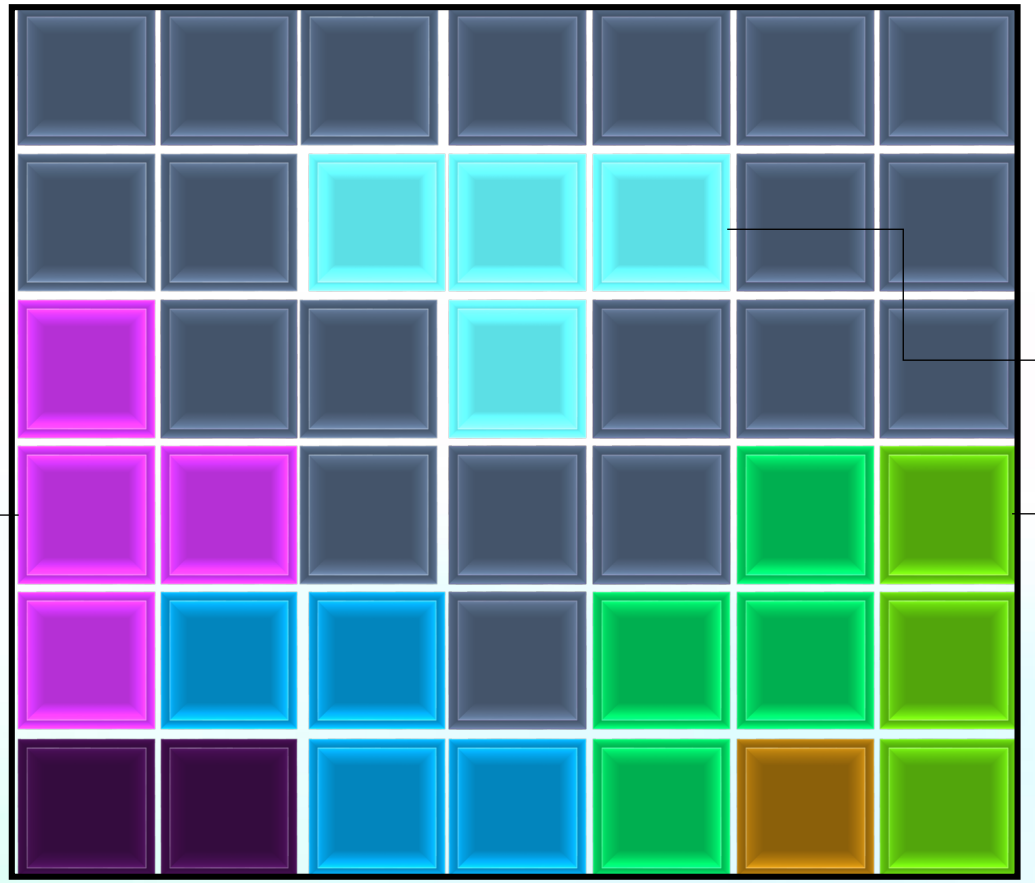
P: Anwendungen

S: IT-Systeme

T: Netze und Kommunikation

: Infrastruktur

Zusammenhang Sicherheitskonzepte



SiKo Fachverfahren

Webanwendungen
Testprozesse
Patch- und Änderungsmanagement

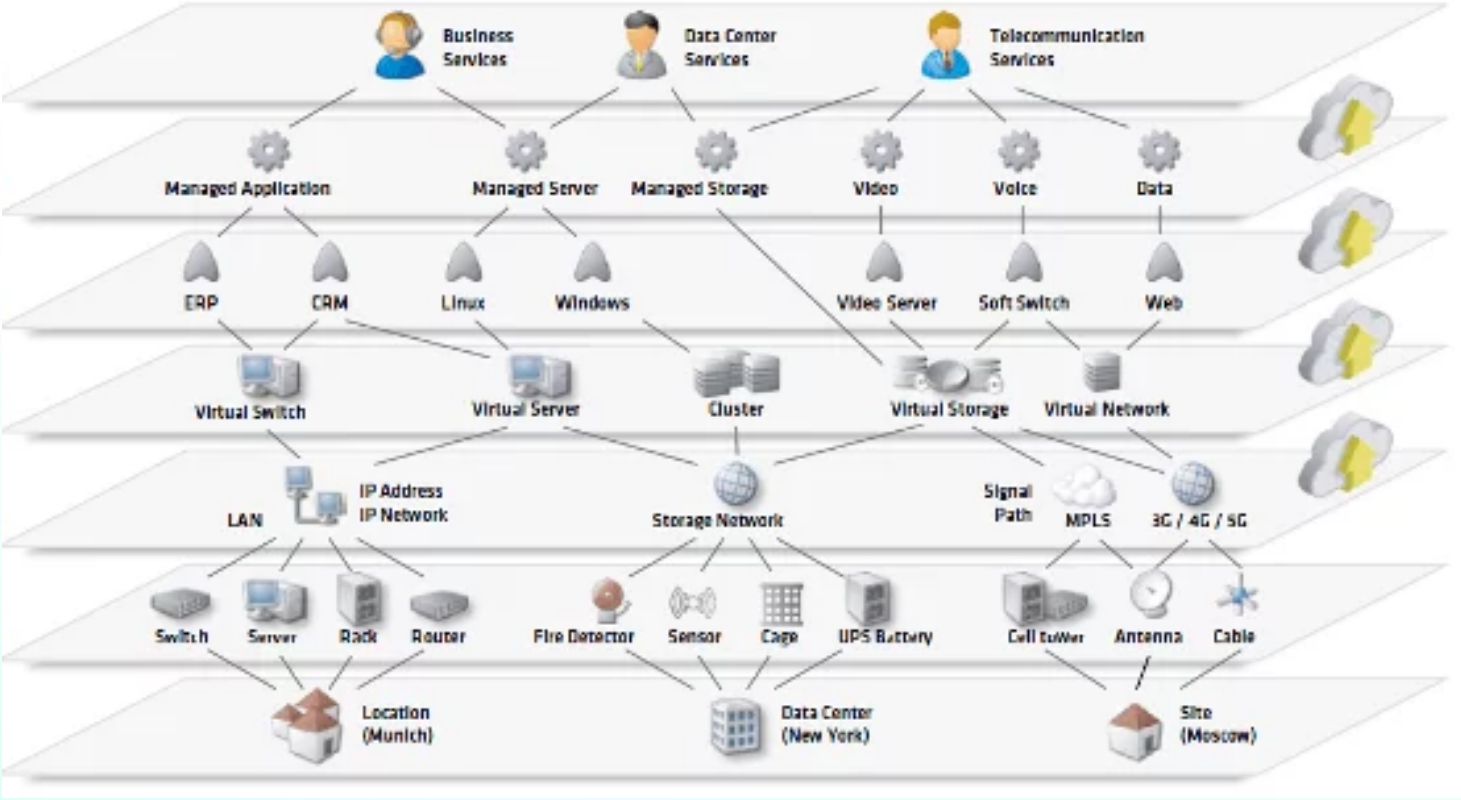
Sicherheitsrahmen-konzept DVZ M-V GmbH

Sicherheitsrahmen-konzept Behörde

Die Sicherheitskonzeption

Strukturanalyse

- Analyse und Aufnahme von
  - Prozessen / Informationen
  - Anwendungen
  - IT-Systemen
  - Netzwerken
  - Gebäuden, Räumen
- Gruppierung von Zielobjekten
- [Optional] Erstellung eines Netzplanes



Schutzbedarfsfeststellung

- Strukturierte Ermittlung des Schutzbedarfes der Informationen
  - Vertraulichkeit,
  - Integrität,
  - Verfügbarkeit
- Ableitung des Schutzbedarfes von IT-Systemen
  - Maximumprinzip
  - Verteilungseffekt
  - Kommulationseffekt

SCHUTZBEDARFSFESTSTELLUNG FÜR ANWENDUNGEN

Bezeichnung und Beschreibung	Schutzziel und Schutzbedarf	Begründung
A001 Textverarbeitung, Präsentation, Tabellenkalkulation	Vertraulichkeit: **normal**	Die Office-Anwendung selbst enthält keine Informationen
	Integrität: **normal**	Die Office-Anwendung selbst enthält keine Informationen
	Verfügbarkeit: **normal**	Die Anwendung ist lokal installiert; eine Neuinstallation ist schnell möglich. Die Lizenzen sind sicher verwahrt. Eine Ausfallzeit von 24 Stunden oder mehr ist akzeptabel.
A002 Lotus Notes	Vertraulichkeit: **hoch**	Es werden Mails mit vertraulichem Inhalt bearbeitet; die Informationen über Geschäftskontakte und Treffen mit Partnern oder Kunden sind vertraulich.
	Integrität: **normal**	Fehlerhafte Daten können in der Regel leicht erkannt werden.

Quelle: BSI Webkurs

Schutzbedarfsfeststellung – Tool DVZ

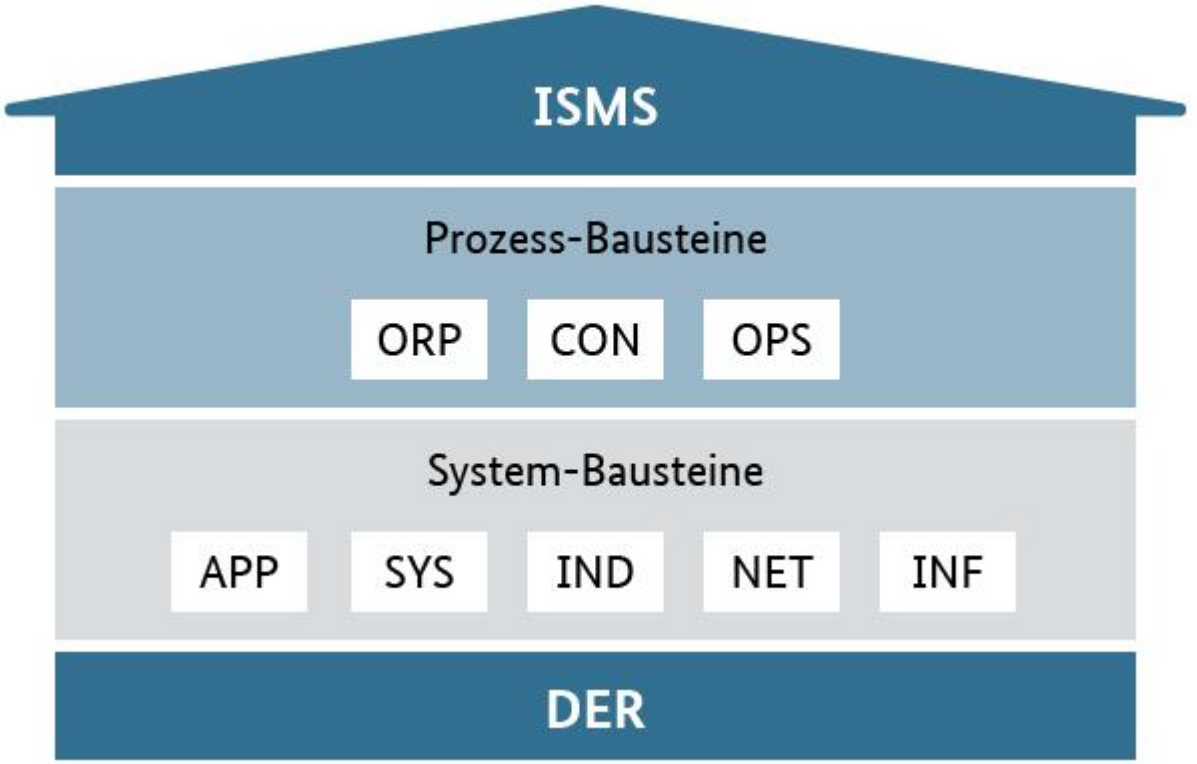
Schutzbedarf Verfügbarkeit:	☐ **Normal**	☐ **Hoch**	☐ **Sehr Hoch**
Schutzbedarf Integrität:	☐ **Normal**	☐ **Hoch**	☐ **Sehr Hoch**
Schutzbedarf Vertraulichkeit:	☐ **Normal**	☐ **Hoch**	☐ **Sehr Hoch**

Schadenskategorie	Schutzbedarfsklasse: Normal	Schutzbedarfsklasse: Hoch	Schutzbedarfsklasse: Sehr hoch	Angesprochenes Schutzziel
Gesetzliche Anforderungen				
Abfrage: Ist auf Basis bestehender Gesetze ein besonderer Schutzbedarf für die verarbeiteten Informationen definiert?	☑ Es besteht keine gesetzliche Einstufung der Informationen	☐ Auf Basis von ((Gesetz)) ist der Schutzbedarf als hoch einzustufen (z.B. Sozialdaten)	☐ Auf Basis von ((Gesetz)) ist der Schutzbedarf als sehr hoch einzustufen (z.B. Verschlusssachen)	
Beeinträchtigung der Aufgabenerfüllung				
Abfrage: Welche Ausfallzeit ist für das betrachtete Verfahren/System maximal tolerabel?	☑ mehr als 12 Stunden	☐ maximal 12 Stunden	☐ maximal 4 Stunden	Verfügbarkeit
Abfrage: Ergibt sich durch den Ausfall des Verfahren/Systems eine Beeinträchtigung der Aufgabenerfüllung?	☑ keine oder tolerable/geringe Beeinträchtigung	☐ nicht tolerablen und Handlungsunfähigkeit für einzelne zentrale Bereiche	☐ nicht tolerabel und Handlungsunfähigkeit der gesamten Behörde zu befürchten	Verfügbarkeit
Finanzielle Auswirkungen				
Abfrage: Welche finanziellen Schäden entstehen durch den *Ausfall* der Daten des FV/Systems?	☑ geringe finanzielle Schäden möglich (im üblichen Projekt-Budgetrahmen)	☐ erhebliche finanzielle Schäden möglich (Institutsbudget ausreichend)	☐ übermäßige finanzielle Schäden möglich (Institutsbudget nicht ausreichend)	Verfügbarkeit
Abfrage: Welche finanziellen Schäden entstehen durch die *Verfälschung und Manipulation* der Daten des FV/Systems?	☑ geringe finanzielle Schäden möglich (im üblichen Projekt-Budgetrahmen)	☐ erhebliche finanzielle Schäden möglich (Institutsbudget ausreichend)	☐ übermäßige finanzielle Schäden möglich (Institutsbudget nicht ausreichend)	Integrität
Abfrage: Welche finanziellen Schäden entstehen durch die *unbefugte Veröffentlichung* der Daten des FV/Systems?	☑ geringe finanzielle Schäden möglich (im üblichen Projekt-Budgetrahmen)	☐ erhebliche finanzielle Schäden möglich (Institutsbudget ausreichend)	☐ übermäßige finanzielle Schäden möglich (Institutsbudget nicht ausreichend)	Vertraulichkeit
Negative Innen-/Außenwirkung				
	keine oder geringe Ansehens- oder	erhebliche Ansehens- oder Vertrauensbeeinträchtigung	übermäßiger Ansehens- oder	

Modellierung

- Anhand der Strukturanalyse werden passende Bausteine aus dem IT-Grundschutz-Kompendium ausgewählt

- Sofern keine passenden Bausteine bestehen, muss für das Zielobjekt eine Risikoanalyse erstellt werden



Quelle: BSI Webkurs

IT-Grundschutz-Kompendium (1/2)

- Anforderungen basierend auf einer vorgelagerten Risikoanalyse
- Von 2018 bis 2023 jährlich im Februar durch BSI fortgeschrieben

111
Bausteine

858
Seiten

10
Anforderungs-
schichten

IT-Grundschutz-Kompendium (2/2)

ISMS: Sicherheitsmanagement

- ISMS.1 Sicherheitsmanagement

ORP: Organisation und Personal

- ORP.1 Organisation
- ORP.2 Personal
- ORP.3 Sensibilisierung und Schulung zur Informationssicherheit
- ORP.4 Identitäts- und Berechtigungsmanagement
- ORP.5 Compliance Management (Anforderungsmanagement)

CON: Konzeption und Vorgehensweise

- CON.1 Kryptokonzept
- CON.2 Datenschutz
- CON.3 Datensicherungskonzept
- CON.6 Löschen und Vernichten
- CON.7 Informationssicherheit auf Auslandsreisen
- CON.8 Software-Entwicklung
- CON.9 Informationsaustausch
- CON.10 Entwicklung von Webanwendungen
- CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)

OPS: Betrieb

- OPS.1.1.1 Allgemeiner IT-Betrieb
- OPS.1.1.2 Ordnungsgemäße IT-Administration
- OPS.1.1.3 Patch- und Änderungsmanagement
- OPS.1.1.4 Schutz vor Schadprogrammen
- OPS.1.1.5 Protokollierung
- OPS.1.1.6 Software-Tests und -Freigaben
- OPS.1.1.7 Systemmanagement
- OPS.1.2.2 Archivierung
- OPS.1.2.4 Telearbeit
- OPS.1.2.5 Fernwartung
- OPS.1.2.6 NTP -Zeitsynchronisation
- OPS.2.2 Cloud-Nutzung
- OPS.2.3 Nutzung von Outsourcing
- OPS.3.2 Anbieten von Outsourcing

DER: Detektion und Reaktion

- DER.1 Detektion von sicherheitsrelevanten Ereignissen
- DER.2.1 Behandlung von Sicherheitsvorfällen
- DER.2.2 Vorsorge für die IT-Forensik
- DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle
- DER.3.1 Audits und Revisionen
- DER.3.2 Revision auf Basis des Leitfadens IS-Revision
- DER.4 Notfallmanagement

APP: Anwendungen

- APP.1.1 Office-Produkte
- APP.1.2 Webbrowser
- APP.1.4 Mobile Anwendung (Apps)
- APP.2.1 Allgemeiner Verzeichnisdienst
- APP.2.2 Active Directory Domain Services
- APP.2.3 OpenLDAP
- APP.3.1 Webanwendungen und Webservices
- APP.3.2 Webserver
- APP.3.3 Fileserver
- APP.3.4 Samba
- APP.3.6 DNS-Server
- APP.4.2 SAP-ERP-System
- APP.4.3 Relationale Datenbanksysteme
- APP.4.4 Kubernetes
- APP.4.6 SAP ABAP-Programmierung
- APP.5.2 Microsoft Exchange und Outlook
- APP.5.3 Allgemeiner E-Mail-Client und -Server
- APP.5.4 Unified Communications und Collaboration
- APP.6 Allgemeine Software
- APP.7 Entwicklung von Individualsoftware

SYS: IT-Systeme

- SYS.1.1 Allgemeiner Server
- SYS.1.2.2 Windows Server 2012
- SYS.1.2.3 Windows Server
- SYS.1.3 Server unter Linux und Unix
- SYS.1.5 Virtualisierung
- SYS.1.6 Containerisierung
- SYS.1.7 IBM Z
- SYS.1.8 Speicherlösungen
- SYS.1.9 Terminalserver

NET: Netze und Kommunikation

- NET.1.1 Netzarchitektur und -design
- NET.1.2 Netzmanagement
- NET.2.1 WLAN-Betrieb
- NET.2.2 WLAN-Nutzung
- NET.3.1 Router und Switches
- NET.3.2 Firewall
- NET.3.3 VPN
- NET.3.4 Network Access Control
- NET.4.1 TK-Anlagen
- NET.4.2 VoIP
- NET.4.3 Faxgeräte und Faxserver

INF: Infrastruktur

- INF.1 Allgemeines Gebäude
- INF.2 Rechenzentrum sowie Serverraum
- INF.5 Raum sowie Schrank für technische Infrastruktur
- INF.6 Datenträgerarchiv
- INF.7 Büroarbeitsplatz
- INF.8 Häuslicher Arbeitsplatz
- INF.9 Mobiler Arbeitsplatz
- INF.10 Besprechungs-, Veranstaltungs- und Schulungsraum
- INF.11 Allgemeines Fahrzeug
- INF.12 Verkabelung
- INF.13 Technisches Gebäudemanagement
- INF.14 Gebäudeautomation

Modellierung – Baustein Aufbau (1/2)

APP.3.1 Webanwendungen und Webservices

1. Beschreibung

1.1. Einleitung

Webanwendungen bieten bestimmte Funktionen und dynamische (sich verändernde) Inhalte. Dazu nutzen Webanwendungen die Internetprotokolle HTTP (Hypertext Transfer Protocol) oder HTTPS. Bei HTTPS wird die Verbindung durch das Protokoll TLS (Transport Layer Security) kryptografisch abgesichert. Webanwendungen stellen auf einem Server Dokumente und Bedienoberflächen, z. B. in Form von Eingabemasken, bereit und liefern diese auf Anfrage an entsprechende Programme auf den Clients aus, wie z. B. an Webbrowser.

Webservices sind Anwendungen, die das HTTP(S)-Protokoll verwenden, um Daten für andere Anwendungen bereitzustellen. In der Regel werden sie nicht unmittelbar durch Benutzende angesteuert.

Um eine Webanwendung oder einen Webservice zu betreiben, sind in der Regel mehrere Komponenten notwendig. Üblich sind Webserver, um Daten auszuliefern und Applikationsserver, um die eigentliche Anwendung oder den Webservice zu betreiben. Außerdem werden zusätzliche Hintergrundsysteme benötigt, die oft als Datenquellen über unterschiedliche Schnittstellen angebunden sind, z. B. Datenbanken oder Verzeichnisdienste.

Webanwendungen und Webservices werden sowohl in öffentlichen Datennetzen als auch in lokalen Netzen einer Institution (Intranet) eingesetzt, um Daten und Anwendungen bereitzustellen. In der Regel müssen sich Clients authentisieren, um auf eine Webanwendung oder einen Webservice zugreifen zu können.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, Webanwendungen und Webservices sicher einzusetzen sowie Informationen zu schützen, die durch sie verarbeitet werden.

1.3. Abgrenzung und Modellierung

Der Baustein ist auf jede Webanwendung und jeden Webservice anzuwenden, die im Informationsverbund eingesetzt werden.

Anforderungen an Webserver und an die redaktionelle Planung eines Webauftritts werden in diesem Baustein nicht behandelt. Sie sind im Baustein APP.3.2 *Webserver* zu finden. Die Entwicklung von Webanwendungen wird im Baustein CON.10 *Entwicklung von Webanwendungen* behandelt.

Webservice-Schnittstellen werden oft via Representational State Transfer (REST) und Simple Object Access Protocol

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.3.1 *Webanwendungen und Webservices* von besonderer Bedeutung.

2.1. Unzureichende Protokollierung von sicherheitsrelevanten Ereignissen

Wenn sicherheitsrelevante Ereignisse von der Webanwendung oder dem Webservice unzureichend protokolliert werden, können diese unter Umständen zu einem späteren Zeitpunkt nur schwer nachvollzogen werden. Die Ursachen für ein Ereignis sind dann möglicherweise nicht mehr ermittelbar. So können z. B. kritische Fehler oder unerlaubte Änderungen in der Konfiguration der Webanwendung übersehen werden.

2.2. Offenlegung sicherheitsrelevanter Informationen bei Webanwendungen und Webservices

Webseiten und Daten, die von einer Webanwendung oder einem Webservice generiert und ausgeliefert werden, können Informationen zu den Hintergrundsystemen enthalten, z. B. Angaben zu Datenbanken oder Versionsständen von Frameworks. Diese Informationen können es bei Angriffen erleichtern, gezielt Webanwendungen oder Webservices anzugreifen.

2.3. Missbrauch einer Webanwendung durch automatisierte Nutzung

Wenn Funktionen einer Webanwendung oder eines Webservices automatisiert genutzt werden, können so zahlreiche Vorgänge in kurzer Zeit ausgeführt werden. Mithilfe eines wiederholt durchgeführten Login-Prozesses kann so z. B. versucht werden, gültige Kombinationen von Konten und Passwörtern zu erraten (Brute-Force). Außerdem kann eine Liste mit gültigen Konten erzeugt werden (Enumeration), falls die Webanwendung oder der Webservice Informationen über vorhandene Konten zurück gibt. Darüber hinaus können wiederholte Aufrufe von ressourcenintensiven Funktionen wie z. B. komplexen Datenbankabfragen für Denial-of-Service-Angriffe auf Anwendungs-

Modellierung – Baustein Aufbau (2/2)

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

APP.3.1.A1 Authentisierung (B)

Der IT-Betrieb MUSS Webanwendungen und Webservices so konfigurieren, dass sich Clients gegenüber der Webanwendung oder dem Webservice authentisieren müssen, wenn diese auf geschützte Ressourcen zugreifen wollen. Dafür MUSS eine angemessene Authentisierungsmethode ausgewählt werden. Der Auswahlprozess SOLLTE dokumentiert werden.

Der IT-Betrieb MUSS geeignete Grenzwerte für fehlgeschlagene Anmeldeversuche festlegen.

APP.3.1.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.1.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.1.A4 Kontrolliertes Einbinden von Dateien und Inhalten (B)

Falls eine Webanwendung oder ein Webservice eine Upload-Funktion für Dateien anbietet, MUSS diese Funktion durch den IT-Betrieb so weit wie möglich eingeschränkt werden. Insbesondere MÜSSEN die erlaubte Dateigröße, erlaubte Dateitypen und erlaubte Speicherorte festgelegt werden. Es MUSS festgelegt werden, welche Clients die Funktion verwenden dürfen. Auch MÜSSEN Zugriffs- und Ausführungsrechte restriktiv gesetzt werden. Zudem MUSS sichergestellt werden, dass Clients Dateien nur im vorgegebenen erlaubten Speicherort speichern können.

APP.3.1.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.1.A6 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.1.A7 Schutz vor unerlaubter automatisierter Nutzung (B)

Der IT-Betrieb MUSS sicherstellen, dass Webanwendungen und Webservices vor unberechtigter automatisierter Nutzung geschützt werden. Dabei MUSS jedoch berücksichtigt werden, wie sich die Schutzmechanismen auf die Nutzungsmöglichkeiten berechtigter Clients auswirken. Wenn die Webanwendung RSS-Feeds oder andere Funktionen enthält, die explizit für die automatisierte Nutzung vorgesehen sind, MUSS dies ebenfalls bei der Konfiguration der Schutzmechanismen berücksichtigt werden.

APP.3.1.A14 Schutz vertraulicher Daten (B)

Diese Anforderung ist entfallen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.3.1.A20 Einsatz von Web Application Firewalls (H)

Institutionen SOLLTEN Web Application Firewalls (WAF) einsetzen. Die Konfiguration der eingesetzten WAF SOLLTE auf die zu schützende Webanwendung oder den Webservice angepasst werden. Nach jedem Update der Webanwendung oder des Webservices SOLLTE die Konfiguration der WAF geprüft werden.

APP.3.1.A24 ENTFALLEN (H)

Diese Anforderung ist entfallen.

APP.3.1.A25 ENTFALLEN (H)

Diese Anforderung ist entfallen.

4. Weiterführende Informationen

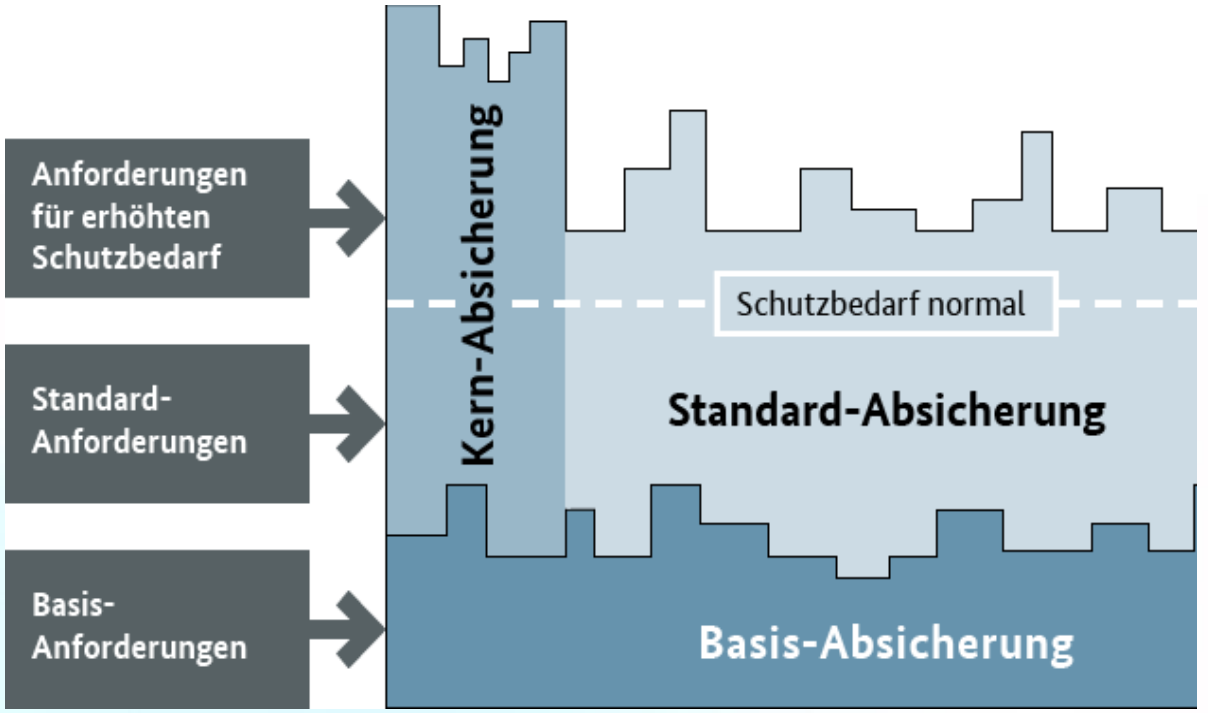
4.1. Wissenswertes

Das Open Web Application Security Projekt (OWASP) stellt auf seiner Webseite Hinweise zur Absicherung von Webanwendungen und Webservices zur Verfügung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt im Dokument „Kryptographische Verfahren: Empfehlungen und Schlüssellängen: BSI TR-02102" Hinweise zur Anwendung kryptografischer Verfahren zur Verfügung.

IT-Grundschutzcheck

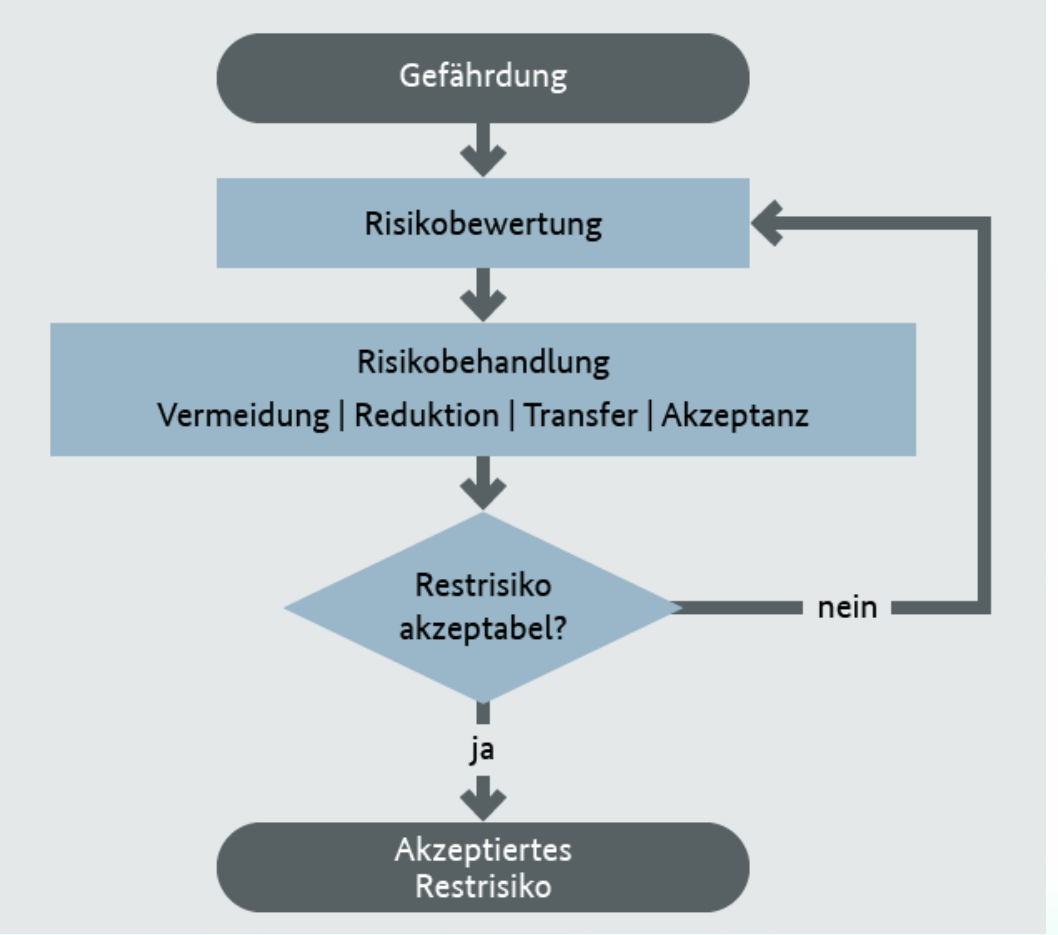
- IT-Grundschutzcheck ist eine Befragung im Rahmen von Interviews
- Umsetzungsstatus der Anforderungen werden beim Fachbereich befragt
- Modalverben
  - Muss / Darf nicht
  - Soll / Sollte nicht
  - Kann / Darf



Quelle: BSI Webkurs

Risikoanalyse (1/2)

- Basierend auf 47 elementaren Gefährdungen, wie Feuer, Wasser, Sabotage, Datenverlust etc.
- Bewertung bezieht Häufigkeit und Schaden/Auswirkung ein
- 4 Behandlungsoptionen
  - Vermeidung: Das Risiko umgehen
  - Reduktion: Das Risiko minimieren
  - Transfer: Versicherungen oder Outsourcing
  - Akzeptanz: Das Risiko wird akzeptiert



Quelle: BSI Webkurs

Risikoanalyse (2/2)

		Ohne zusätzliche Maßnahmen			Risikobehandlung	
Zielobjekt	Gefährdung	Eintritts-häufigkeit	Auswirkung	Risiko	Risikobehandlung	Erläuterung zur Risikobehandlung
A_002	G 0.14 Ausspähen von Informationen (Spionage)	mittel	beträchtlich	mittel	Akzeptanz	Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
A_002	G 0.15 Abhören	mittel	begrenzt	mittel	Akzeptanz	Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
A_002	G 0.18 Fehlplanung oder fehlende Anpassung	mittel	beträchtlich	mittel	Akzeptanz	Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
A_002	G 0.19 Offenlegung schützenswerter Informationen	selten	begrenzt	gering	Akzeptanz	Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
A_002	G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle	selten	begrenzt	gering	Akzeptanz	Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
A_002	G 0.21 Manipulation von Hard- oder Software	selten	begrenzt	gering	Akzeptanz	Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
A_002	G 0.22 Manipulation von Informationen	mittel	beträchtlich	mittel	Akzeptanz	Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
A_002	G 0.25 Ausfall von Geräten oder Systemen	mittel	begrenzt	mittel	Akzeptanz	Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
A_002	G 0.27 Ressourcenmangel	mittel	vernachlässigbar	gering	Akzeptanz	Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
A_002	G 0.28 Software-Schwachstellen oder -Fehler	mittel	beträchtlich	mittel	Akzeptanz	Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
A_002	G 0.29 Verstoß gegen Gesetze oder Regelungen	selten	vernachlässigbar	gering	Akzeptanz	Aufgrund der bereits umgesetzten Maßnahmen wird das Restrisiko als vertretbar eingeschätzt.
A_002	G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	selten	begrenzt	gering	Akzeptanz	Aufgrund der bereits umgesetzten Maßnahmen

Umsetzungsplan

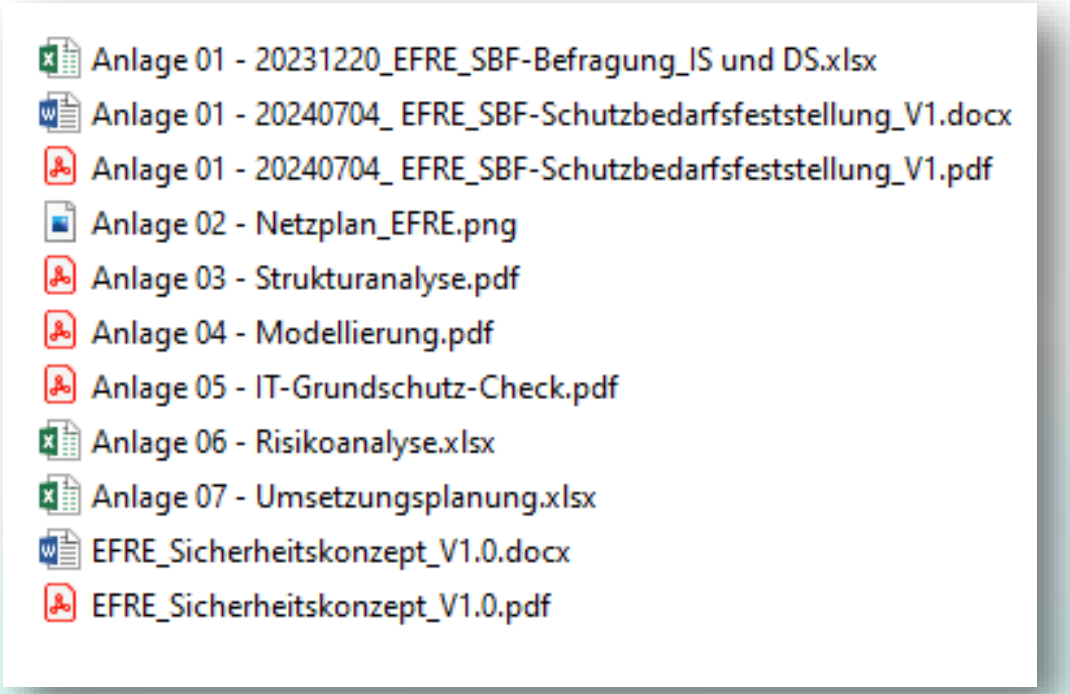
- Auflistung aller nicht oder teilweise umgesetzten Anforderungen
- Priorisierung der Umsetzungspunkte
- Termin und Budget für die Umsetzung
- Verantwortlichkeiten

UMSETZUNGSPLAN

Anforderung: Umzusetzende Maßnahme	Termin	Budget	Umsetzung durch
SYS.1.1.A3 *Restriktive Rechtevergabe:* Die verbliebenen Gruppenberechtigungen müssen aufgelöst werden.	Drittes Quartal des Jahres	keine Kosten	Herr Schmitt (IT-Betrieb)
SYS.1.1.A4 *Rollentrennung:* Separate Benutzerkennungen für jeden Administrator einrichten	31. Juli des Jahres	keine Kosten	Herr Schmitt (IT-Betrieb)
SYS.1.1.A8 *Regelmäßige Datensicherung:* Die Datensicherungen	Erstes Quartal im Folgejahr	Anschaffung: 15.000 € Betrieb: noch offen	Frau Meyer (Einkauf)

Quelle: BSI Webkurs

Finalisierung



- Die Dokumentation in verinice ist für ein Sicherheitskonzept ausreichend.
- Das DVZ erstellt für seine Kunden mehrere Dokumente, die die Ergebnisse der Sicherheitskonzeption nachvollziehbar machen

Herausforderungen

Herausforderungen bei der Bearbeitung

- Sehr umfangreich in der initialen Erarbeitung
- Aufwändig in der Pflege
  - Empfohlen wird eine jährliche Fortschreibung
- Bindet Ressourcen auch auf der Arbeitsebene (z.B. im Rahmen von Befragungen)
- Softwarenahe Dienste, insbesondere bei externen Dienstleistern und Herstellern, sind schwierig zu analysieren und zu befragen.
- Bearbeitungszeitpunkt bei Projekten ist schwierig: Projekte brauchen konkrete Vorgaben aber das Siko braucht einen konkreten „finalen“ Untersuchungsgegenstand.

Herausforderungen bei der Methodik

- Schaut nur auf einzelne Zielobjekte, ein Fachverfahren mit mehreren Komponenten wird nicht im Zusammenhang gesehen
- Spagat zwischen detaillierter und übergreifender Betrachtung in den Anforderungen
- Die Methodik gibt kein Vorgehen für Fachverfahren oder einzelne Betrachtungen.

Fragen und Anregungen?

Kontakt

Martin Möller

m.moeller@dvz-mv.de

+49 385 4800 181 // +49 160 7441 278