BSI IT-Grundschutz, ISO 27001 & Datenschutz

neam IT-Services GmbH

Wie identifiziere und begegne ich Risiken bei der Digitalisierung?

Kai Wittenburg, *Geschäftsführer*

Ihre IT in ***sicheren*** Händen

neam IT-Services GmbH

- gegründet 1996
- Paderborn, Wiesbaden & Berlin
- ca. 80 Mitarbeiter
  - ISO27001 Lead Auditoren
  - ISO27001 Lead Implementer
  - BSI-Auditoren

IT-Sicherheit
GANZHEITLICHE SICHERHEITS-KONZEPTE
FÜR UNTERNEHMEN

IT-Systemhaus
IT-SERVICES MIT
SUPPORTGARANTIE & KOSTENKONTROLLE

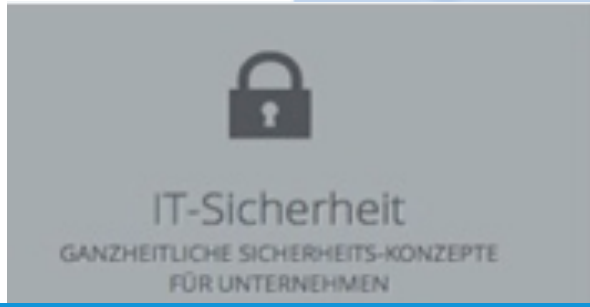
Schulungen
SEMINARE ZU ALLEN BEREICHEN
DER IT-SICHERHEIT

Ihre IT in ***sicheren*** Händen

Informationssicherheit

neam IT-Services GmbH

- Managementsysteme (ISMS)
  - ISO27001
  - BSI Grundschutz
- Business Continuity
  - Notfallvorsorge
  - Notfallbehandlung
- Zertifizierung & Audits



Informationssicherheit

neam IT-Services GmbH

- Penetrationstests
  - Infrastruktur
  - Webanwendungen
  - Social Engineering
- Schulungen & Mitarbeiter-sensibilisierung

EU-DSGVO Art. 32
Sicherheit der Verarbeitung

neam IT-Services GmbH

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke **der Verarbeitung** sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des ***Risikos*** für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem ***Risiko*** angemessenes Schutzniveau zu gewährleisten;

Informationssicherheitsmanagement-system

- ISMS basierend auf
  - ISO 27001 (Zertifikat)
    - Leitlinien & allgemeine Prinzipien
    - Maßnahmenziele & Maßnahmen (Anhang A)
  - ISO 27002
    - Umsetzungsempfehlungen für Maßnahmen
    - Ergänzend: BSI Grundschutzkataloge
- Unterstützt: Datenschutzmanagementsystem

Informationssicherheitsmanagement-system

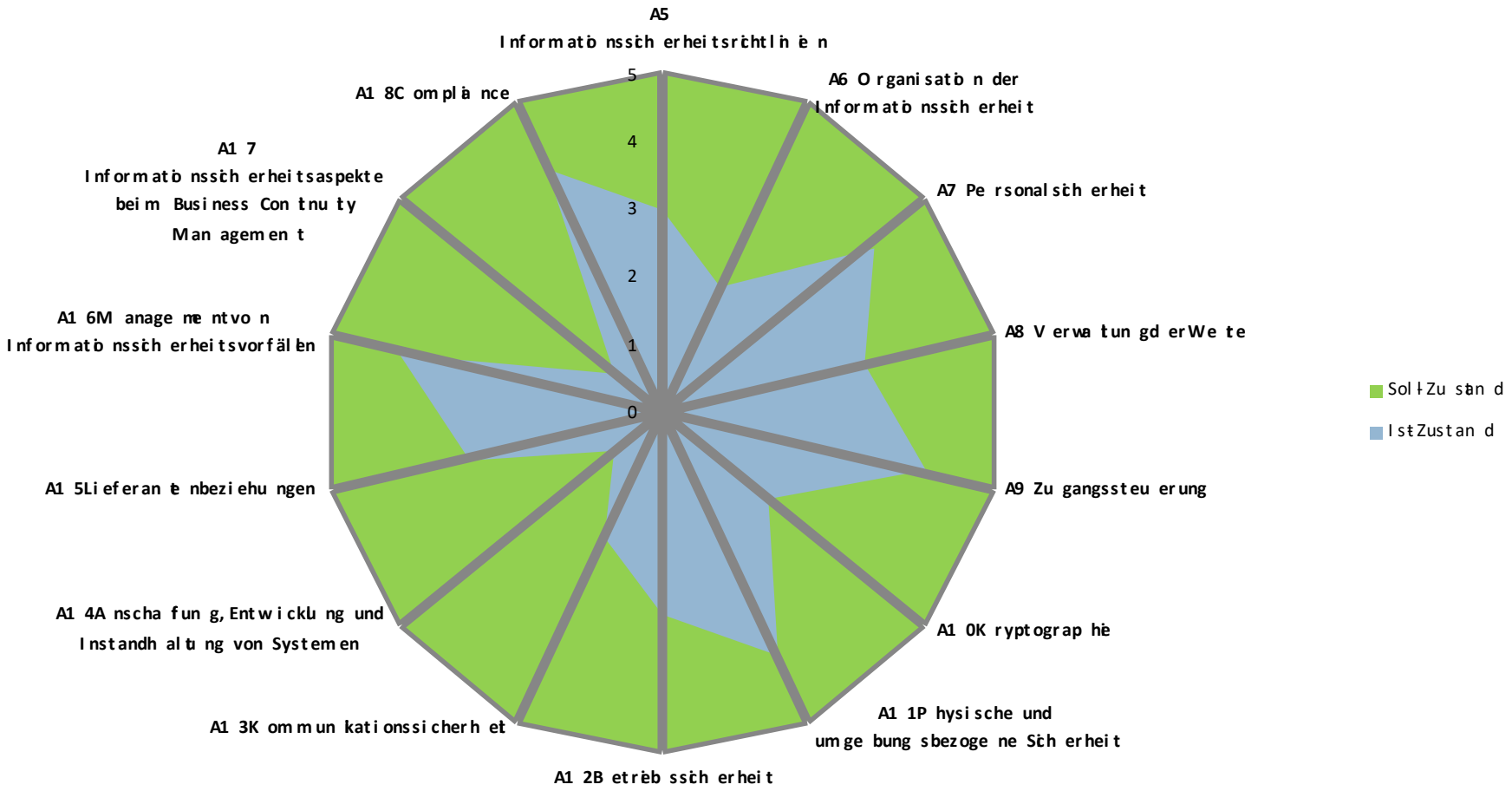
- ISMS basierend auf
  - ISO 27001 (Zertifikat)
    - Leitlinien & allgemeine Prinzipien
    - Maßnahmenziele & Maßnahmen (Anhang A)
  - ISO 27002
    - Umsetzungsempfehlungen für Maßnahmen
    - Ergänzend: BSI Grundschutzkataloge

Bundesdatenschutzgesetz (BDSG)
§ 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

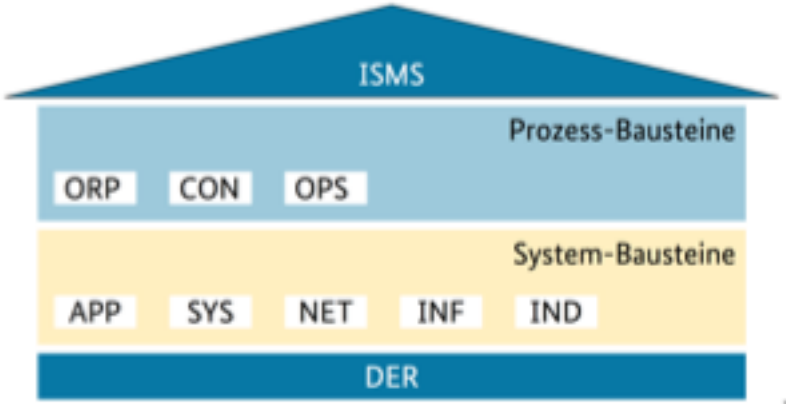
ISO 27002

- ISO 27001 Anhang A



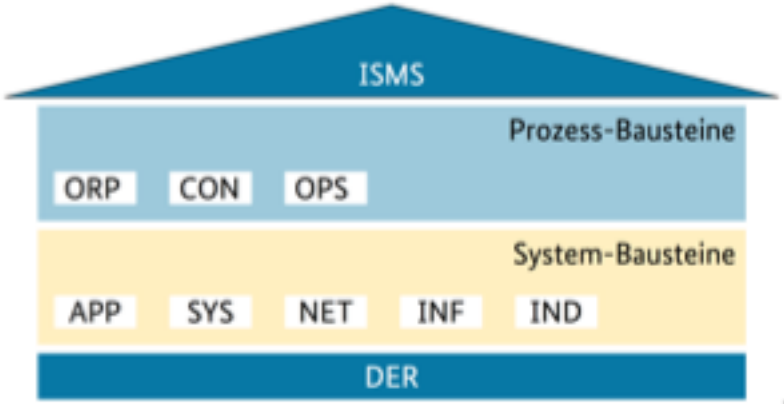
BSI IT-Grundschutz

- Bausteine im IT-Grundschutz-Kompendium
  - Prozessorientierte Schichten
    - ISMS
    - ORP (Organisation & Personal)
    - CON (Konzepte)
    - OPS (Betrieb)
    - DER (Detektion & Reaktion)

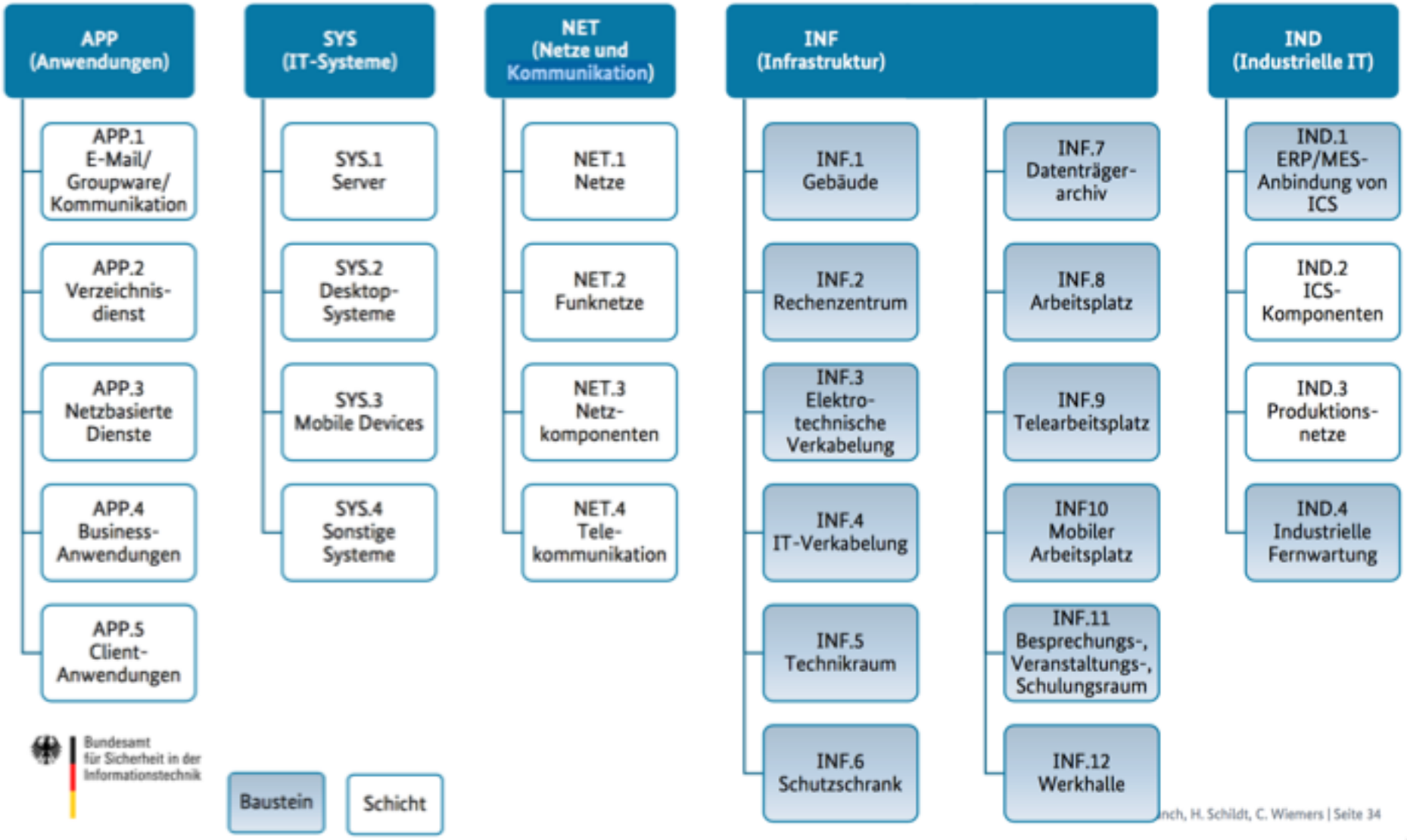


BSI IT-Grundschutz

- Bausteine im IT-Grundschutz-Kompendium
  - Systemorienterte Schichten:
    - INF (Infrastruktur)
    - NET (Netze und Kommunikation)
    - SYS (IT-Systeme)
    - APP (Anwendungen)
    - IND (Industrielle IT)



BSI IT-Grundschutz



Einführung ISMS nach ISO 27001

neam IT-Services GmbH

Planung

- Kick-Off, Organisationsanalyse; Analyse der bisherigen IS-Bemühungen; Definition des Geltungsbereichs; ISMS- und IS-Leitlinie; **Risikoanalyse & -behandlung**; Anwendbarkeitserklärung

Umsetzung

- IS-Organisationsstruktur; Dokumentenverwaltung; Prozess- und Verfahrensentwicklung; Kommunikationsplanung; Schulung- und Sensibilisierung; Umsetzung von IS-Maßnahmen; Incident-Management

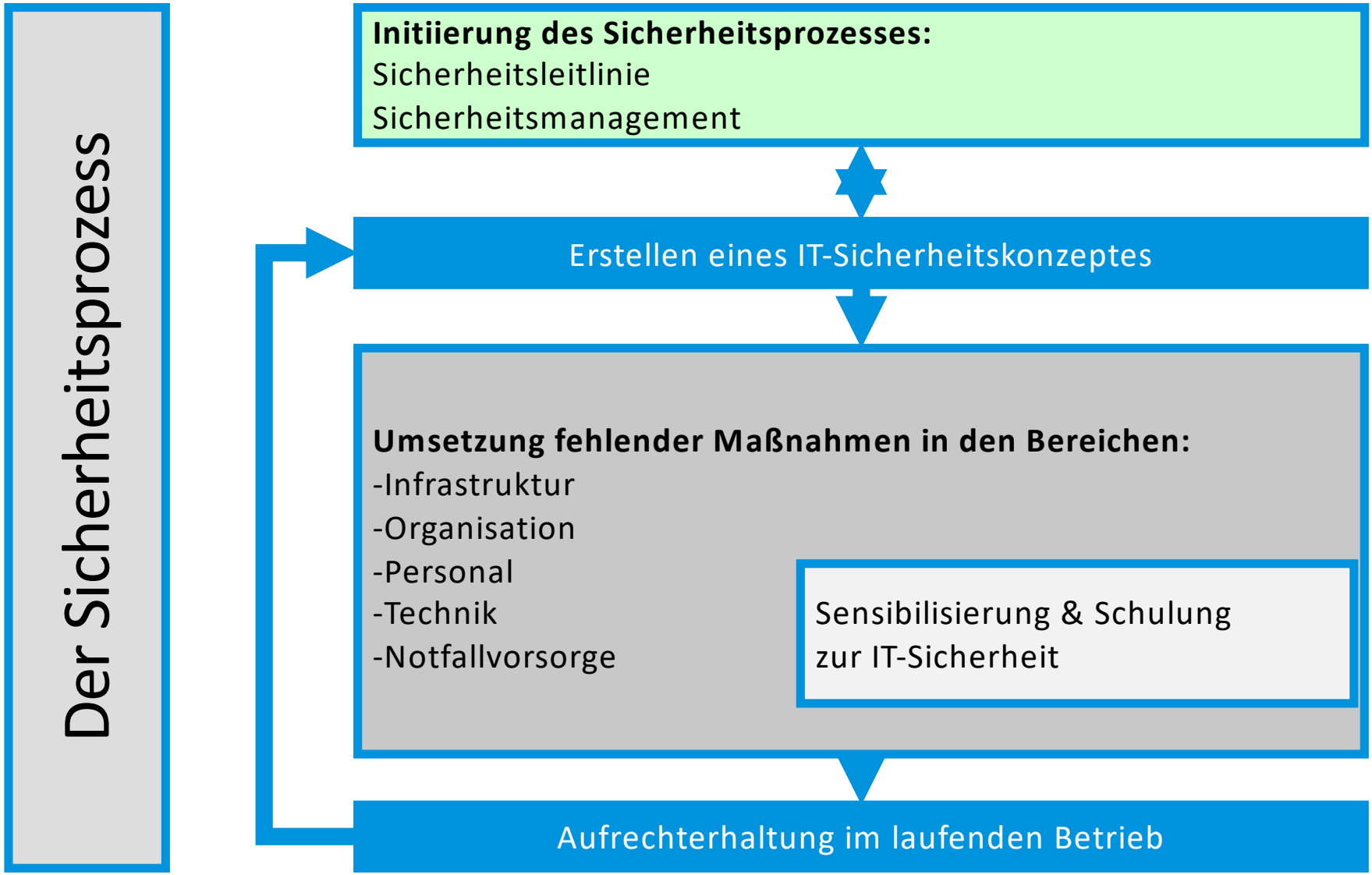
Kontrolle

- Überwachung, Bewertung und Überprüfung; Interne Audits; Managementüberprüfung

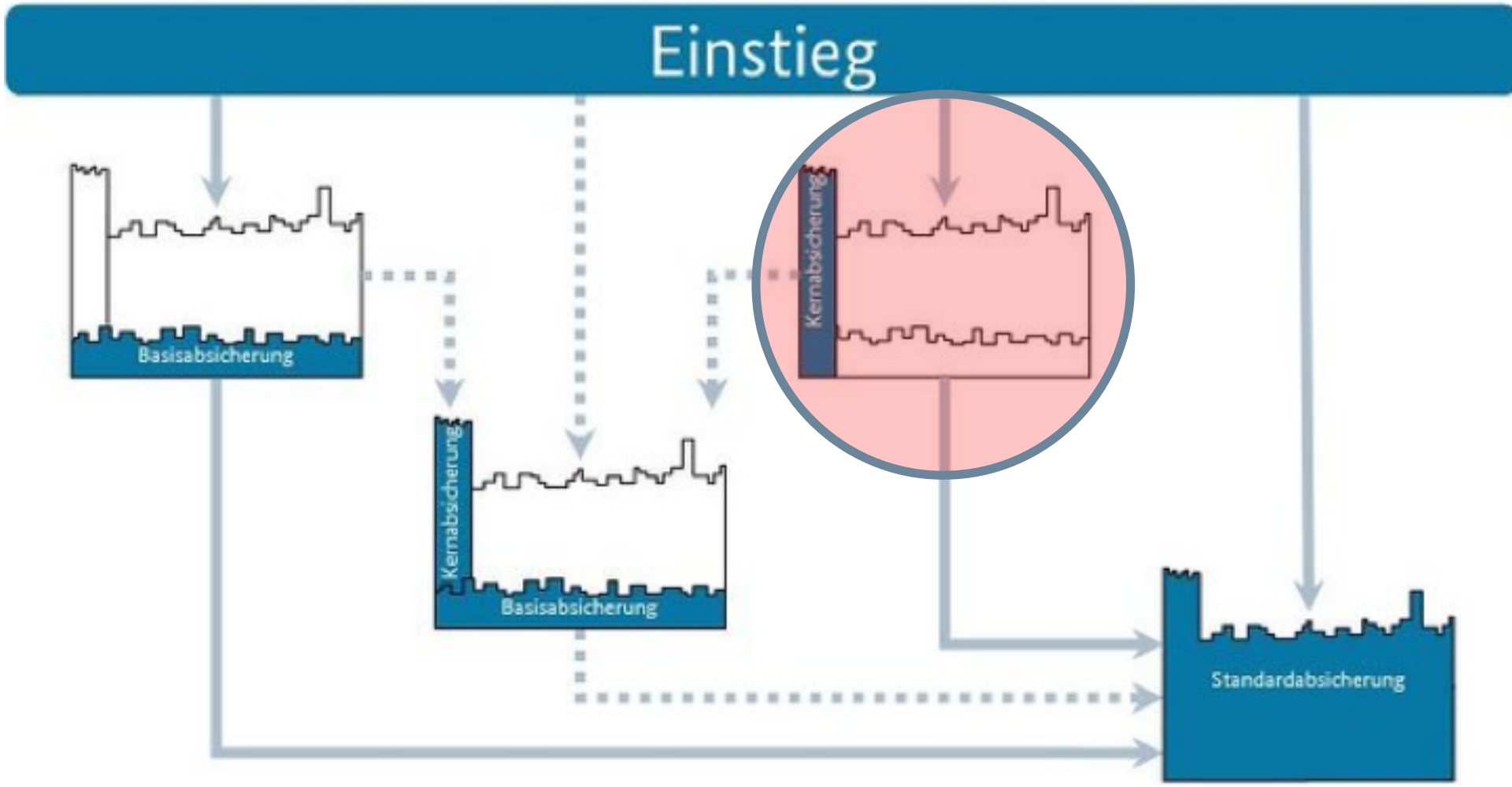
Anpassung

- Behandlung von Abweichungen; kontinuierliche Verbesserung

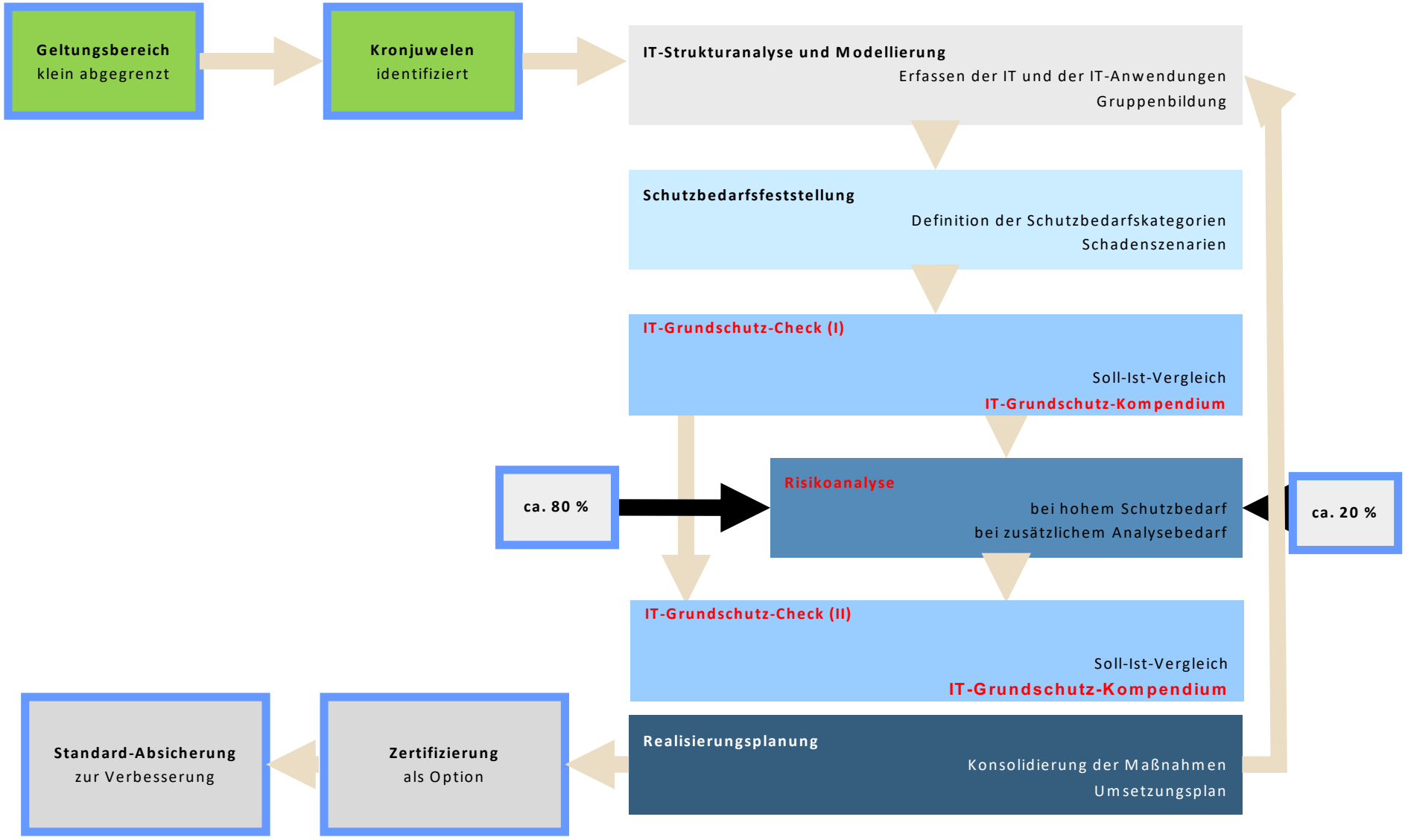
Sicherheitsprozess



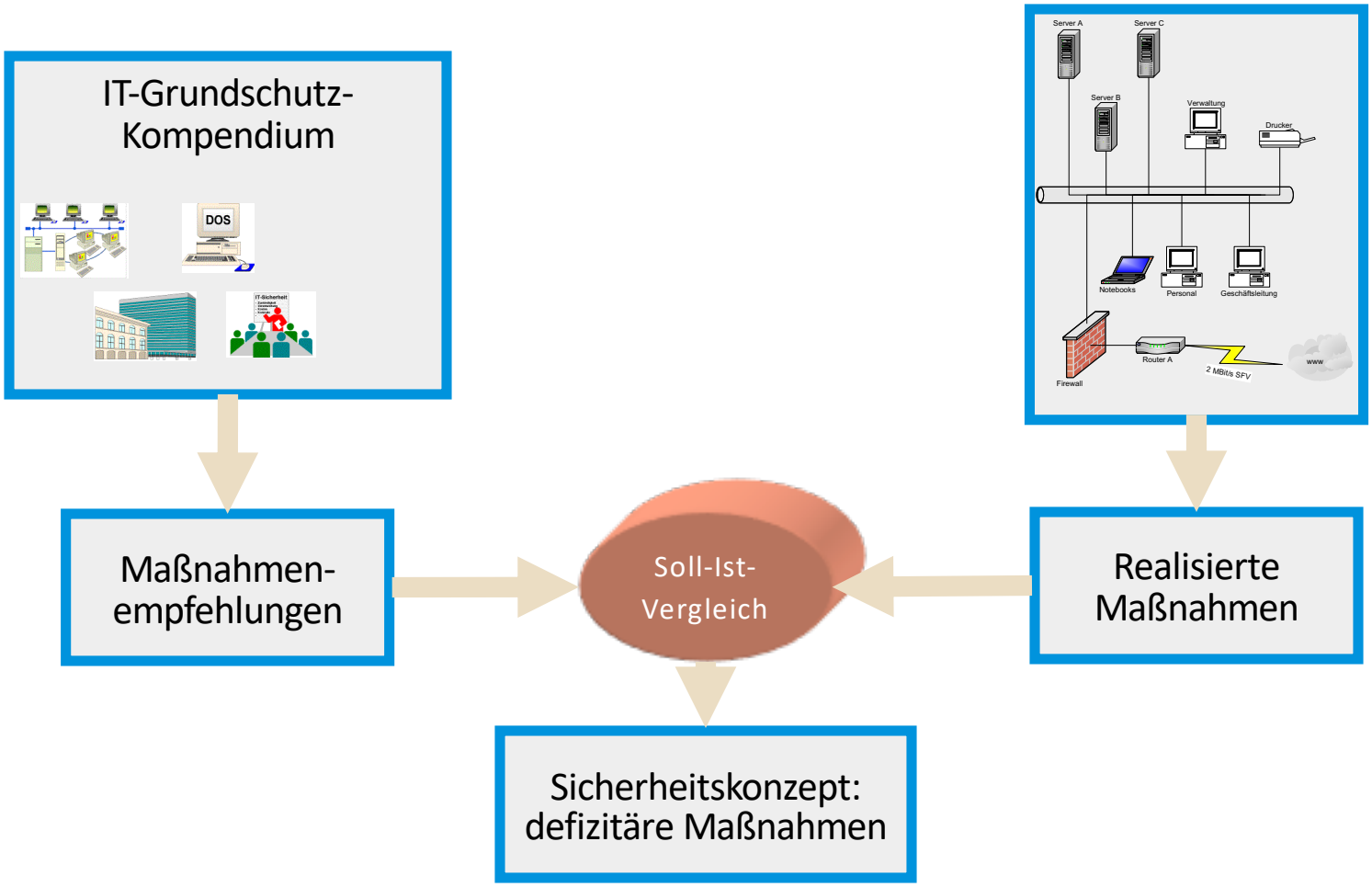
Vorgehensweisen nach BSI-Standard 200-2



Schritte zur Kern-Absicherung



BSI IT-Grundschutz



Schutzbedarfsfeststellung

Definition der Schutzbedarfs-kategorien

- Normal
  - Schadensauswirkungen sind begrenzt und überschaubar.
- Hoch
  - Schadensauswirkungen können beträchtlich sein.
- Sehr hoch
  - Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Normal

Schutzbedarfskategorie "normal"	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	- Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	**Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts würde durch den Einzelnen als tolerabel eingeschätzt werden. Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.** **Es handelt sich dabei um personenbezogene Daten, die frei zugänglich sind (Telefon-, Adressverzeichnisse) bzw. deren unsachgemäße Handhabung keine besondere Beeinträchtigung erwarten lässt.** **Entsprechend der Schutzstufen (LfD Niedersachsen):** **A – frei zugänglich** **B – berechtigtes Interesse des Einsichtnehmenden**
3. Beeinträchtigung der persönlichen Unversehrtheit	
4. Beeinträchtigung der Aufgabenerfüllung	- Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden.
5. Negative Innen- oder Außenwirkung	- Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	- Der finanzielle Schaden bleibt für die Institution tolerabel.

Hoch: „besonders schützenswerte Daten“

Schutzbedarfskategorie "hoch"	
1. Verstoß gegen Gesetze/Vorschriften/Verträge	Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen (Ansehen und Existenz). Hierunter fallen medizinische Daten sowie Personaldaten (z.B. Gewerkschaftszugehörigkeit, Personalaktendaten, Beurteilungen, Kontodaten, gesundheitliche Verhältnisse, strafbare Handlungen, religiöse oder politische Anschauungen, arbeitsrechtliche Verhältnisse, Steuer- und Sozialdaten, Schulden, Pfändungen, psychologische Daten) Entsprechend der Schutzstufen (LfD Niedersachsen): C – Beeinträchtigungen möglich D – erhebliche Beeinträchtigungen möglich
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	
3. Beeinträchtigung der persönlichen Unversehrtheit	
4. Beeinträchtigung der Aufgabenerfüllung	
5. Negative Innen- oder Außenwirkung	- Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	- Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.

Sehr hoch: „besonders schützenswerte Daten“

Schutzbedarfskategorie "sehr hoch"	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	Eine besonders bedeutende Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. Ein möglicher Missbrauch personenbezogener Daten würde für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten (Gefahr für Gesundheit, Leben oder Freiheit des Betroffenen). Entsprechend der Schutzstufen (LfD Niedersachsen): E – Gefahr für Gesundheit, Leben bzw. Freiheit
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	
3. Beeinträchtigung der persönlichen Unversehrtheit	Unversehrtheit sind möglich. - Gefahr für Leib und Leben
4. Beeinträchtigung der Aufgabenerfüllung	- Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. - Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
5. Negative Innen- oder Außenwirkung	- Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, evtl. sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	- Der finanzielle Schaden ist für die Institution existenzbedrohend.

Planungsphase
Schutzbedarfsfeststellung

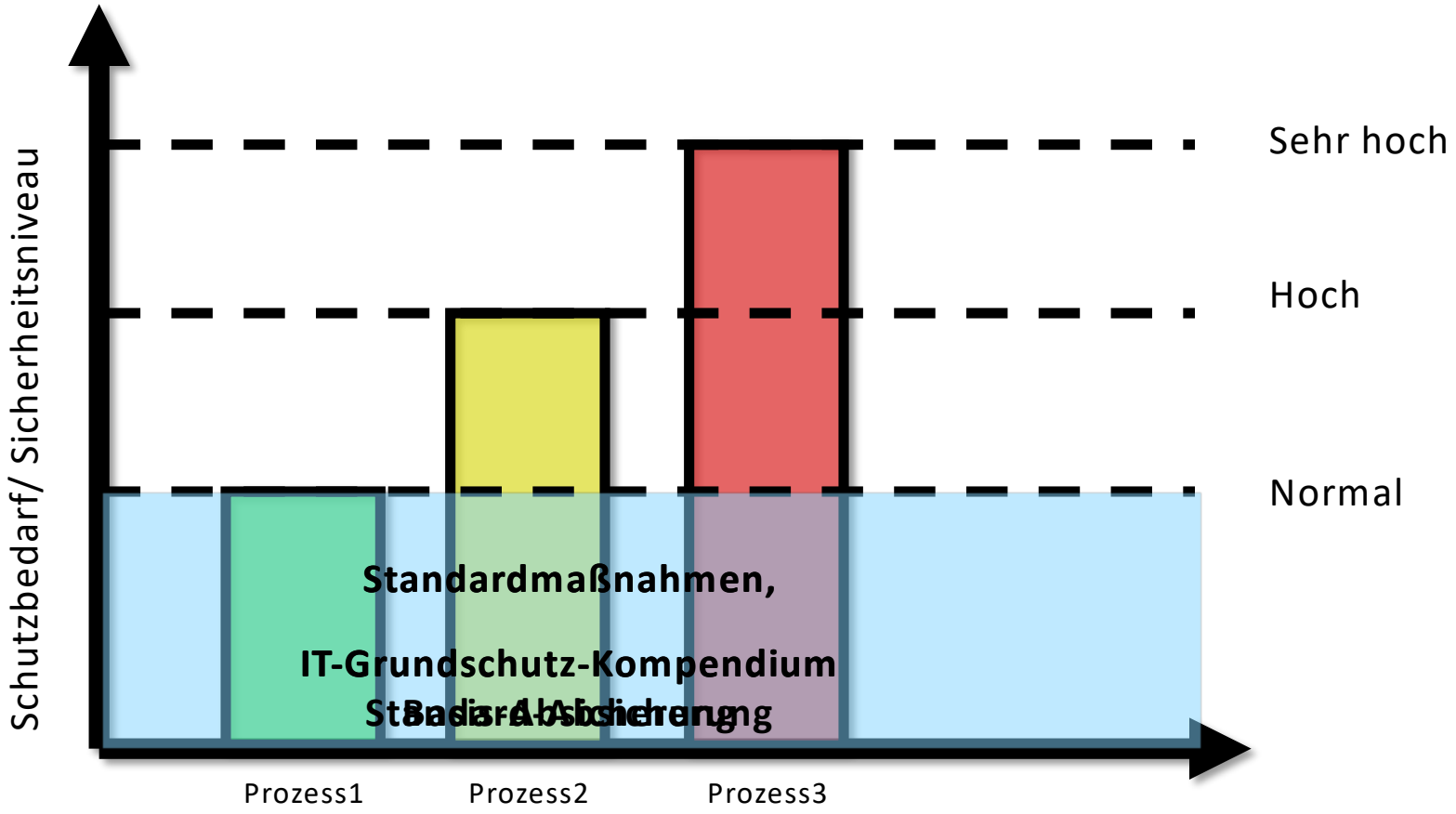
Typische Schadensszenarien

- Zuordnung der Schäden durch Verlust der ***Vertraulichkeit***, ***Integrität*** *und Verfügbarkeit* anhand folgender Szenarien:
  - Verstoß gegen Gesetze/Vorschriften/Verträge,
  - Beeinträchtigung des informationellen Selbstbestimmungsrechts,
  - Beeinträchtigung der persönlichen Unversehrtheit,
  - Beeinträchtigung der Aufgabenerfüllung,
  - negative Außenwirkung und
  - finanzielle Auswirkungen.

Schutzbedarfsfeststellung

Nr.	IT-Anwendung / Informationen	Pers.-bez. Daten	Grund-wert	Schutz-bedarf	Begründung
A1	Branchensoftware		Vertraulich-keit	normal	Es handelt sich um frei zugängliche Daten, deren Bekanntwerden zu keinen Schaden führen würde.
			Integrität	normal	Fehler können schnell erkannt und korrigiert werden.
			Verfügbar-keit	normal	Wichtige Informationen können aus anderen Quellen bezogen werden.
A2	Personalverwaltung	X	Vertraulich-keit	hoch	Es handelt sich um pers.-bez. Daten, deren bekanntwerden den Betroffen erheblich beeinträchtigen kann.
			Integrität	normal	Fehler können schnell erkannt und korrigiert werden.
			Verfügbar-keit	normal	Ausfälle können mit manuellen Verfahren bis zu einer Woche überbrückt werden.

Risikomanagement



SYS: IT-Systeme

SYS.2.2.3: Client unter Windows 10

1 Beschreibung

Zu diesem Baustein existieren bisher noch keine Umsetzungshinweise. Umsetzungshinweise können auch über den großen Erfahrungsschatz von IT-Grundschutz-Anwendern erstellt und erweitert werden. IT-Grundschutz-Anwender, die praxiserprobte Sicherheitsmaßnahmen oder Best-Practice-Empfehlungen zum Einsatz von Windows 10 haben, können uns diese unter grundschutz@bsi.bund.de mitteilen, Stichwort "Windows 10". Das IT-Grundschutz-Team bereitet diese zeitnah auf und stellt diese als Startpunkt für Umsetzungshinweise zu Windows 10 zur Verfügung.

1.1 Einleitung

Mit Windows 10 hat Microsoft sein Client-Betriebssystem Windows an eine neue Unternehmensstrategie angepasst. Verändert hat sich insbesondere auch die Designphilosophie des Betriebssystems weg von dem bisherigen Prinzip des „lokalen Betriebssystems" hin zu einem Dienst („Windows as a Service"), welcher neben den bisherigen Betriebssystemfunktionalitäten auch darüber hinausgehende – insbesondere Cloud-basierte - Anwendungen mit sich bringt und deswegen auf eine enge Anbindung an die Server-Infrastruktur des Herstellers angewiesen ist. Der verstärkte Datenaustausch zwischen Client und Herstellerinfrastruktur sowie die zunehmende Auslagerung von sicherheitskritischen Kernbestandteilen einer Windows-Infrastruktur wie z.B. Authentisierung in die Cloud sind dabei wichtige und vor einem Einsatz unbedingt zu bewertende neue Aspekte im Vergleich zu den bisherigen Windows-Versionen.

1.2 Zielsetzung

Zielsetzung dieses Bausteins ist der Schutz von Informationen, die durch und auf Windows 10-Clients verarbeitet werden.

1.3 Abgrenzung

Dieser Baustein ist auf alle Zielobjekte anzuwenden, die unter dem Betriebssystem Windows 10 betrieben werden. Die Anforderungen aus dem Baustein „Allgemeiner Client" müssen entsprechend der Anforderungskategorie umgesetzt werden.

2 Gefährdungslage

Die folgenden spezifischen Bedrohungen und Schwachstellen sind für Clients auf Basis von Windows 10 von besonderer Bedeutung:

3 Anforderungen

Im Folgenden sind spezifische Anforderungen für den Schutz von Windows 10 aufgeführt. Grundsätzlich ist *der IT-Betrieb* für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese werden in den entsprechenden Anforderungen gesondert erwähnt.

Bausteinverantwortlicher	*IT-Betrieb*
weitere Verantwortlichkeiten	*Benutzer*

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

SYS.2.2.3.A1 Geeignete Auswahl einer Windows 10-Version

Der Funktionsumfang einer Windows-Version MUSS vor der Beschaffung auf die Einsatzfähigkeit geprüft und eine geeignete Version ausgewählt werden. Es sind bevorzugt 64-Bit Versionen einzusetzen, da in diesen erweiterte Sicherheitsfunktionen enthalten sind. Bei Windows 10 werden durch die Updatefunktion des Betriebssystems neben Sicherheitsupdates für bestehende Funktionen auch funktionale Updates, d. h. Änderungen an der Betriebssystemfunktionalität durchgeführt. Bei jedem funktionalen Update MUSS daher überprüft werden, ob alle Anforderungen aus dem IT-Grundschutz auch nach dem Einspielen des Updates weiterhin erfüllt werden.

SYS.2.2.3.A2 Datenübertragungen an den Hersteller

Es MUSS sichergestellt werden, dass Datenübertragungen an den Hersteller nur in dem Umfang erfolgen, wie sie für den Betrieb benötigt werden.

SYS.2.2.3.A3 Schutz vor Schadsoftware

Sofern nicht gleich- oder höherwertige andere Maßnahmen (z. B. eine Anwendungskontrolle in Verbindung mit Anwendungsisolation sowie Maßnahmen zur Exploit-Mitigation) zum Schutz des IT-Systems vor einer Infektion mit Schadsoftware getroffen wurden, MUSS der Einsatz einer spezialisierten Komponente zum Schutz vor Schadsoftware auf Windows 10-Clients umgesetzt sein.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik zum Schutz von Windows 10. Sie SOLLTEN grundsätzlich umgesetzt werden.

SYS.2.2.3.A4 Beschaffung von Windows 10

Gegenüber früheren Windows-Versionen sind die Anforderungen oder Empfehlungen an die einzusetzende Hardware, wie beispielsweise UEFI (Unified Extensible Firmware Interface), von Windows 10-Systemen gestiegen. Diese Anforderungen SOLLTEN gemäß der Windows Hardware Certification Requirements bei der Beschaffung von Windows 10 bzw. der entsprechenden Hardware für das Windows 10-System berücksichtigt werden. Des weiteren SOLLTEN die zu beschafferden Systeme über eine Firmware-Konfigurationsoberfläche für UEFI SecureBoot und für das TPM (sofern vorhanden) verfügen, die die Kontrolle durch den Eigentümer ermöglichen. Der Beschaffungsprozess von Windows 10 SOLLTE die Auswahl des Lizenzmodells enthalten.

SYS.2.2.3.A5 Konfiguration zum Schutz von Anwendungen in Windows 10

Die Datenausführungsverhinderung für alle Programme und Dienste (Opt-Out Modus) SOLLTE aktiviert werden.

SYS.2.2.3.A6 Schutz der Anmeldeinformationen in Windows 10

Sofern Windows 10 in der Enterprise-Version auf einem physikalischen System installiert ist, SOLLTE die Nutzung des „Virtual Secure Mode" für die Speicherung lokaler Passwörter genutzt werden. Ist dies nicht möglich SOLLTE für den Betrieb des für die Verwaltung der Anmeldeinformationen zuständigen LSAS-Dienstes der geschützte Modus (PPL – Protected Process Light) aktiviert werden. Die Netzwerkanmeldung von lokalen Konten SOLLTE verboten werden.

SYS.2.2.3.A7 Lokale Sicherheitsrichtlinien

Alle sicherheitsrelevanten Einstellungen SOLLTEN bedarfsgerecht konfiguriert, getestet und regelmäßig überprüft werden. Die Sicherheitsrichtlinien SOLLTEN gemäß den Empfehlungen des Betriebssystemherstellers und dem voreingestellten Standardverhalten konfiguriert werden, sofern das Standardverhalten nicht anderen Anforderungen aus dem Grundschutz oder der Organisation widerspricht. Abweichungen SOLLTEN dokumentiert und begründet werden. Alle nicht benötigten Anwendungen und

Individuelle Risikoanalyse

- Prozesse mit (sehr) hohem Schutzbedarf
  1. Assetliste des Prozesses
  2. Erstellung einer Gefährdungsübersicht
  3. Ermittlung zusätzlicher Gefährdungen
  4. Gefährdungsbewertung
  5. Risikobehandlungsplan

Individuelle Risikoanalyse

- Identifikation der Assets (CMDB)
- Vererbung des Schutzbedarfs

Nr.	IT-Anwendung / Informationen	Pers.-bez. Daten	IT-Systeme									
			C1	C2	C3	C4	L1	S1	S2	N1	N2	TK1
A1	Branchensoftware		X		X				X	X	X	
A2	Personalverwaltung	X				X			X	X		
A3	Onlinebanking	X	X					X			X	

Individuelle Risikoanalyse

- Prozesse mit (sehr) hohem Schutzbedarf
  1. Assetliste des Prozesses
  2. Erstellung einer Gefährdungsübersicht
     - BSI Gefährdungsliste
     - Reduziert: 46 „elementare Gefährdungen“
     - Beispiele und Beschreibungen
  3. Ermittlung zusätzlicher Gefährdungen
     - Workshop (Brainstorming)
  4. Gefährdungsbewertung
  5. Risikobehandlungsplan

Individuelle Risikoanalyse

- Prozesse mit (sehr) hohem Schutzbedarf
  1. Assetliste des Prozesses
  2. Erstellung einer Gefährdungsübersicht
  3. Ermittlung zusätzlicher Gefährdungen
  4. Gefährdungsbewertung
     - Eintrittswahrscheinlichkeit
     - Auswirkung
  5. Risikobehandlungsplan

Individuelle Risikoanalyse

- Gefährdungsbewertung – Bewertungskriterien
  - Eintrittswahrscheinlichkeit

Eintrittswahrscheinlichkeit		
Stufe	**Häufigkeit des Eintritts**	**Wert**
sehr gering	sehr unwahrscheinlich, noch nie vorgekommen	1
gering	Unwahrscheinlich, ist in der Branche bereits vorgekommen	2
mittel	Möglich, ist in NRW schon vorgekommen	3
hoch	Wahrscheinlich, ist in Paderborn mehrfach vorgekommen	4
sehr hoch	Häufig, monatlich	5

Individuelle Risikoanalyse

- Gefährdungsbewertung – Bewertungskriterien
  - Auswirkung

Schutzbedarf für Vertraulichkeit	Wert
normal	1
hoch	2
sehr hoch	3

Schutzbedarf für Integrität	Wert
normal	1
hoch	2
sehr hoch	3

Schutzbedarf für Verfügbarkeit	Wert
normal	1
hoch	2
sehr hoch	3

Schutzbedarf = Summe (für Vertraulichkeit, Integrität und Verfügbarkeit)

Individuelle Risikoanalyse

- Risikoakzeptanz

Risikomatrix					
Schadensauswirkung des zugeordneten Assets	Eintrittswahrscheinlichkeit der Gefährdung (Risikoszenarios)				
	sehr gering	gering	mittel	hoch	sehr hoch
	1	2	3	4	5
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25
6	6	12	18	24	30
7	7	14	21	28	35
8	8	16	24	32	40
9	9	18	27	36	45

Risikowert je Gefährdung = (Summe von Vertraulichkeit + Integrität + Verfügbarkeit) * Eintrittswahrscheinlichkeit der Gefährdung

Individuelle Risikoanalyse

- Bewertung

Risikoeinschätzung:	ohne Maßnahmen		
elementare Gefährdungen nach BSI-Grundschutz	Auswirkung	Eintritt	RKZ
Feuer	6	5	30
Ungünstige klimatische Bedingungen	6	1	6
Wasser	6	2	12
Verschmutzung, Staub, Korrosion	6	1	6
Naturkatastrophen	6	1	6
Katastrophen im Umfeld	6	1	6
Großereignisse im Umfeld	6	1	6
Ausfall oder Störung der Stromversorgung	6	4	24
Ausfall oder Störung von Kommunikationsnetzen	6	5	30
Ausfall oder Störung von Versorgungsnetzen	6	2	12

Individuelle Risikoanalyse

neam IT-Services GmbH

- Bewertung

Risikoeinschätzung:	ohne Maßnahmen			mit Maßnahmen			
elementare Gefährdungen nach BSI-Grundschutz	Auswirkung	Eintritt	RKZ	vorhandene Maßnahmen	Auswirkung	Eintritt	RKZ
Feuer	6	5	30	- Verbot Brandlasten (-1) - Rauchverbot (-1) - Brandmeldeanlage (-1)	6	2	12
Ungünstige klimatische Bedingungen	6	1	6		6	1	6
Wasser	6	2	12		6	2	12
Verschmutzung, Staub, Korrosion	6	1	6		6	1	6
Naturkatastrophen	6	1	6		6	1	6
Katastrophen im Umfeld	6	1	6		6	1	6
Großereignisse im Umfeld	6	1	6		6	1	6
Ausfall oder Störung der Stromversorgung	6	4	24		6	4	24
Ausfall oder Störung von Kommunikationsnetzen	6	5	30		6	5	30
Ausfall oder Störung von Versorgungsnetzen	6	2	12		6	2	12

Individuelle Risikoanalyse

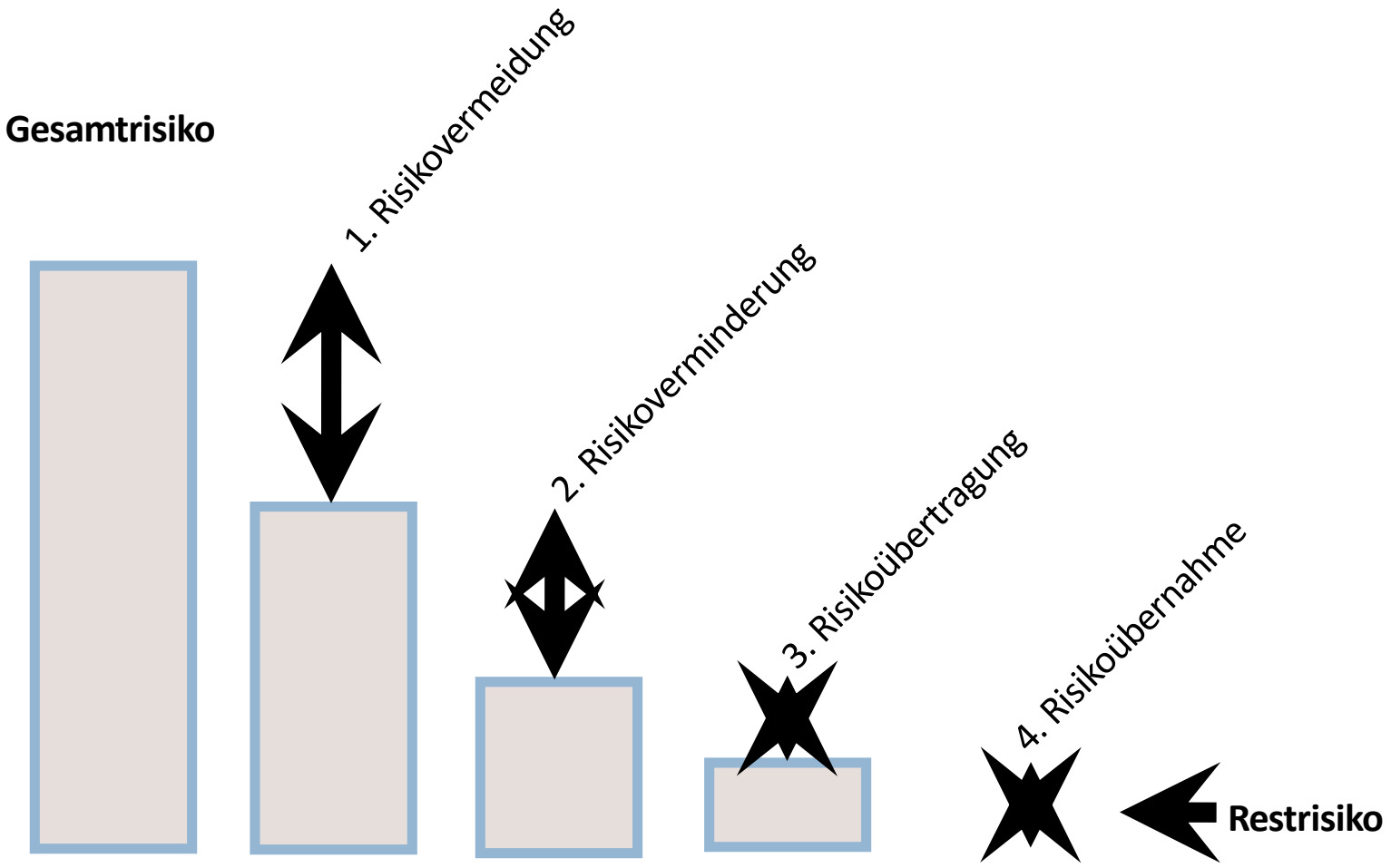
- Bewertung

Risikoeinschätzung:	ohne Maßnahmen			mit Maßnahmen				mit noch einzuführenden Maßnahmen			
elementare Gefährdungen nach BSI-Grundschutz	Auswirkung	Eintritt	RKZ	vorhandene Maßnahmen	Auswirkung	Eintritt	RKZ	geplante Maßnahmen	Auswirkung	Eintritt	RKZ
Feuer	6	5	30	- Verbot Brandlasten (-1) - Rauchverbot (-1) - Brandmeldeanlage (-1)	6	2	12	- Löschanlage (-1)	6	1	6
Ungünstige klimatische Bedingungen	6	1	6		6	1	6		6	1	6
Wasser	6	2	12		6	2	12		6	2	12
Verschmutzung, Staub, Korrosion	6	1	6		6	1	6		6	1	6
Naturkatastrophen	6	1	6		6	1	6		6	1	6
Katastrophen im Umfeld	6	1	6		6	1	6		6	1	6
Großereignisse im Umfeld	6	1	6		6	1	6		6	1	6
Ausfall oder Störung der Stromversorgung	6	4	24		6	4	24		6	4	24
Ausfall oder Störung von Kommunikationsnetzen	6	5	30		6	5	30		6	5	30
Ausfall oder Störung von Versorgungsnetzen	6	2	12		6	2	12		6	2	12

Individuelle Risikoanalyse

- Prozesse mit (sehr) hohem Schutzbedarf
  1. Assetliste des Prozesses
  2. Erstellung einer Gefährdungsübersicht
  3. Ermittlung zusätzlicher Gefährdungen
  4. Gefährdungsbewertung
  5. Risikobehandlungsplan

Individuelle Risikoanalyse



SYS.2.2.3: Client unter Windows 10

1 Beschreibung

Zu diesem Baustein existieren bisher noch keine Umsetzungshinweise. Umsetzungshinweise können auch über den großen Erfahrungsschatz von IT-Grundschutz-Anwendern erstellt und erweitert werden. IT-Grundschutz-Anwender, die praxiserprobte Sicherheitsmaßnahmen oder Best-Practice-Empfehlungen zum Einsatz von Windows 10 haben, können uns diese unter grundschutz@bsi.bund.de mitteilen, Stichwort "Windows 10". Das IT-Grundschutz-Team bereitet diese zeitnah auf und stellt diese als Startpunkt für Umsetzungshinweise zu Windows 10 zur Verfügung.

1.1 Einleitung

Mit Windows 10 hat Microsoft sein Client-Betriebssystem Windows an eine neue Unternehmensstrategie angepasst. Verändert hat sich insbesondere auch die Designphilosophie des Betriebssystems weg von dem bisherigen Prinzip des „lokalen Betriebssystems" hin zu einem Dienst („Windows as a Service"), welcher neben den bisherigen Betriebssystemfunktionalitäten auch darüber hinausgehende – insbesondere Cloud-basierte - Anwendungen mit sich bringt und deswegen auf eine enge Anbindung an die Server-Infrastruktur des Herstellers angewiesen ist. Der verstärkte Datenaustausch zwischen Client und Herstellerinfrastruktur sowie die zunehmende Auslagerung von sicherheitskritischen Kernbestandteilen einer Windows-Infrastruktur wie z.B. Authentisierung in die Cloud sind dabei wichtige und vor einem Einsatz unbedingt zu bewertende neue Aspekte im Vergleich zu den bisherigen Windows-Versionen.

1.2 Zielsetzung

Zielsetzung dieses Bausteins ist der Schutz von Informationen, die durch und auf Windows 10-Clients verarbeitet werden.

1.3 Abgrenzung

Dieser Baustein ist auf alle Zielobjekte anzuwenden, die unter dem Betriebssystem Windows 10 betrieben werden. Die Anforderungen aus dem Baustein „Allgemeiner Client" müssen entsprechend der Anforderungskategorie umgesetzt werden.

2 Gefährdungslage

Die folgenden spezifischen Bedro
Windows 10 von besonderer Bed

4 Weiterführende Informationen

Weiterführende Informationen zu Gefährdung und Schutz von Windows 10 finden sich unter anderem in folgenden Veröffentlichungen:

- https://technet.microsoft.com/en-us/library/dn408187.aspx (Aktivierung von RunAsPPL für LSASS)

3.3 Anforderungen für erhöhten Schutzbedarf

Im Folgenden sind exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung

vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.2.2.3.A17 Einsatz einer Festplattenverschlüsselung (C, I)

Eine Festplattenverschlüsselung SOLLTE zum Schutz der Vertraulichkeit der auf der Festplatte gespeicherten Daten im ruhenden Zustand (d. h. wenn der Client ausgeschaltet ist) eingesetzt werden. Wenn auf mehreren Systemen eine Festplattenverschlüsselung eingesetzt wird, SOLLTE eine Planung des Schlüsselmanagements und der gewünschten Authentisierung durchgeführt werden. Eine Konzeption unterstützt dabei, alle Entscheidungen zum Einsatz der Verschlüsselung zu dokumentieren. In diesem Zusammenhang SOLLTEN folgende Inhalte geregelt werden: Authentisierung (z.B. Passwort, PIN, Token), Ablage der Wiederherstellungsinformationen, zu verschlüsselnde Laufwerke, Schreibrechte auf unverschlüsselte Datenträger und wie sicher gestellt wird, dass die Wiederherstellungsinformationen nur Berechtigten Personen zugänglich sind.

Benutzer SOLLTEN darüber aufgeklärt werden, wie sie sich bei Verlust eines Authentisierungsmittels zu verhalten haben.

SYS.2.2.3.A18 Verwendung des Encrypting File Systems EFS (C, I)

Das Encrypting File System (EFS) schützt die verwendeten Schlüssel mit dem Passwort des Benutzers. Daher SOLLTE ein komplexes Passwort für den Schutz der mit EFS verschlüsselten Daten verwendet werden. Zusätzlich können restriktive Zugriffsrechte die mit EFS verschlüsselte Dateien schützen. Statt des Administrators SOLLTE ein dediziertes Konto der Wiederherstellungsagent sein. In diesem Zusammenhang ist es notwendig, dessen privaten Schlüssel zu sichern und aus dem System zu entfernen. Dabei SOLLTEN von allen privaten Schlüsseln Datensicherungen erstellt werden. Beim Einsatz von EFS mit lokalen Benutzerkonten, SOLLTE die Verschlüsselung der lokalen Passwortspeicher mittels syskey verwendet werden. Dies kann entfallen, wenn die Betriebssystemfunktion Credential Guard genutzt wird. Beim Einsatz von EFS SOLLTEN die Benutzer im korrekten Umgang mit EFS geschult werden.

SYS.2.2.3.A19 Windows PowerShell (C, I, A)

Wenn die Windows PowerShell (WPS) nicht benötigt wird, SOLLTE sie deinstalliert werden. Bei Windows 10 lässt sich die PowerShell-Skriptumgebung allerdings nur noch entfernen, wenn auch das .NET-Framework deinstalliert wird. Falls das .NET-Framework auf dem Client benötigt wird, SOLLTE alternativ die Ausführung der WPS-Dateien nur den Gruppen der Administratoren gestattet werden. Die Protokollierung von Schreib- und Lesezugriffen auf das Windows PowerShell-Profil SOLLTE aktiviert und für eine regelmäßige Kontrolle der Protokolle gesorgt werden. Die Ausführung von Windows PowerShell-Skripten SOLLTE mit dem Befehl Set-Execution Policy AllSigned eingeschränkt werden, um zumindest die versehentliche Ausführung unsignierter Skripte zu verhindern.

SYS.2.2.3.A20 Erweiterter Schutz der Anmeldeinformationen in Windows 10 (C, I)

Auf UEFI-basierten Systemen SOLLTE SecureBoot verwendet und der Status des geschützten Modus

rden (vgl. hierzu SYS.2.2.3.X – Schutz der Anmeldeinformatio-
g der Client-Systeme mittels RDP vorgesehen, SOLLTE bei Ein-
dem Funktionslevel 2012 R2 von der Option „RestrictedAd-

Last-Access-Zeitstempels (A)
eitskonzeptes für ein solches System SOLLTE geprüft werden,

Projektvorgehensweise zur Einführung ISMS nach ISO 27001

neam IT-Services GmbH

Planung

- Kick-Off, Organisationsanalyse; Analyse der bisherigen IS-Bemühungen; Definition des Geltungsbereichs; ISMS- und IS-Leitlinie; Risikoanalyse & -behandlung; Anwendbarkeitserklärung

Umsetzung

- IS-Organisationsstruktur; Dokumentenverwaltung; Prozess- und Verfahrensentwicklung; Kommunikationsplanung; Schulung- und Sensibilisierung; Umsetzung von IS-Maßnahmen; Incident-Management

Kontrolle

- Überwachung, Bewertung und Überprüfung; Interne Audits; Managementüberprüfung

Anpassung

- Behandlung von Abweichungen; kontinuierliche Verbesserung

Umsetzungsphase

- Umsetzung von IS-Maßnahmen
  - Umsetzungsplan für noch umzusetzende IS-Maßnahmen
  - Unterstützung bei der Umsetzung von IS-Maßnahmen
- Schulung und Sensibilisierung
  - Analyse des Schulungs- und Sensibilisierungsstandes
  - Durchführung von Sensibilisierungsschulungen
- Incident-Management
  - Planung, Einführung und Dokumentation einer Vorgehensweise zum Umgang mit Vorfällen innerhalb der Organisation

Projektvorgehensweise zur Einführung ISMS nach ISO 27001

neam IT-Services GmbH

Planung

- Kick-Off, Organisationsanalyse; Analyse der bisherigen IS-Bemühungen; Definition des Geltungsbereichs; ISMS- und IS-Leitlinie; Risikoanalyse & -behandlung; Anwendbarkeitserklärung

Umsetzung

- IS-Organisationsstruktur; Dokumentenverwaltung; Prozess- und Verfahrensentwicklung; Kommunikationsplanung; Schulung- und Sensibilisierung; Umsetzungsplanung von Maßnahmen; Incident-Management

Kontrolle

- Überwachung, Bewertung und Überprüfung; Interne Audits; Managementüberprüfung

Anpassung

- Behandlung von Abweichungen; kontinuierliche Verbesserung

Projektvorgehensweise zur Einführung ISMS nach ISO 27001

neam IT-Services GmbH

Planung

- Kick-Off, Organisationsanalyse; Analyse der bisherigen IS-Bemühungen; Definition des Geltungsbereichs; ISMS- und IS-Leitlinie; Risikoanalyse & -behandlung; Anwendbarkeitserklärung

Umsetzung

- IS-Organisationsstruktur; Dokumentenverwaltung; Prozess- und Verfahrensentwicklung; Kommunikationsplanung; Schulung- und Sensibilisierung; Umsetzungsplanung von Maßnahmen; Incident-Management

Kontrolle

- Überwachung, Bewertung und Überprüfung; Interne Audits; Managementüberprüfung

Anpassung

- Behandlung von Abweichungen; kontinuierliche Verbesserung

Projektvorgehensweise zur Einführung ISMS nach ISO 27001

neam IT-Services GmbH

Planung

- Kick-Off, Organisationsanalyse; Analyse der bisherigen IS-Bemühungen; Definition des Geltungsbereichs; ISMS- und IS-Leitlinie; Risikoanalyse & -behandlung; Anwendbarkeitserklärung

Umsetzung

- IS-Organisationsstruktur; Dokumentenverwaltung; Prozess- und Verfahrensentwicklung; Kommunikationsplanung; Schulung- und Sensibilisierung; Umsetzungsplanung von Maßnahmen; Incident-Management

Kontrolle

- Überwachung, Bewertung und Überprüfung; Interne Audits; Managementüberprüfung

Anpassung

- Behandlung von Abweichungen; kontinuierliche Verbesserung

neam IT-Services GmbH

Technologiepark 8
D-33100 Paderborn

+49 5251 1652-0
+49 5251 1652-444

http://www.neam.de