Networking Academy

it bildungsnetz

Akademie für Lehrerfortbildung und Personalführung

IT-Grundschutz Schutzbedarfsanalyse (LF 4)

Guido Häckmanns, freiberuflicher Dozent

20. Nationaler Akademietag der Bildungsinitiative Networking
22./23. April 2021

Die Idee des IT-Grundschutz

Typische Gefährdungen,
Schwachstellen und Risiken

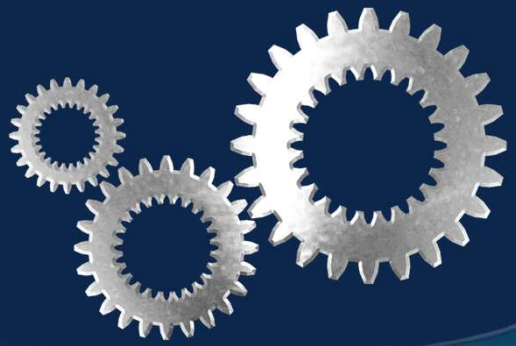
Empfehlung geeigneter Standard-Sicherheitsanforderungen und teilweise auch Maßnahmen (“Best Practice“-Ansätze).

Ziel des IT-Grundschutzes

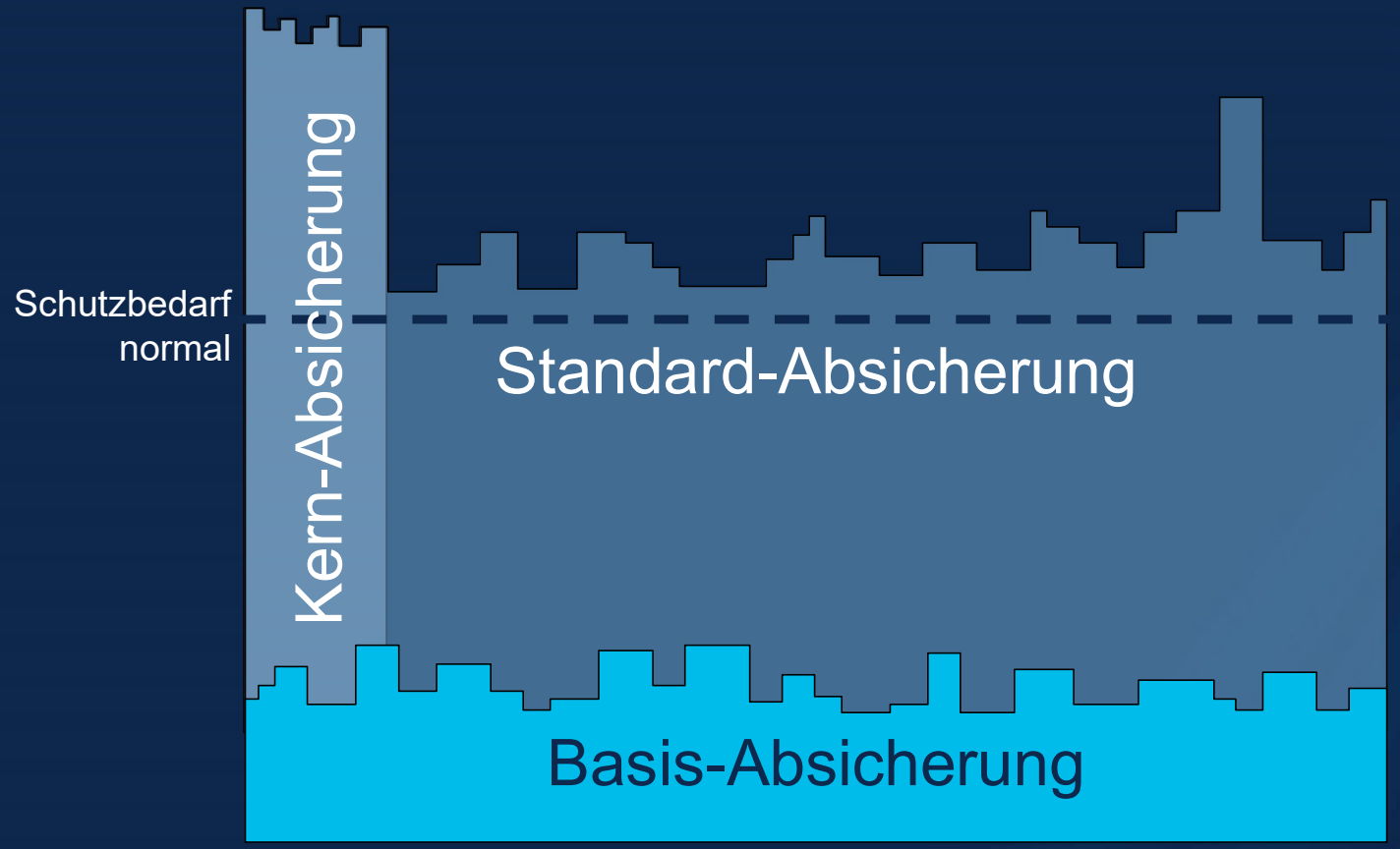
IT-Grundschutz verfolgt einen
ganzheitlichen Ansatz

Standard-
Sicherheitsniveau

**Geschäftsrelevante Prozesse
und Informationen**

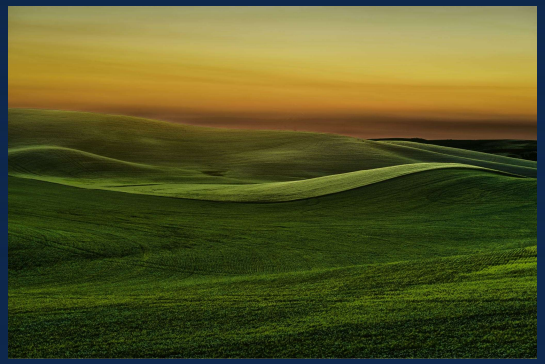


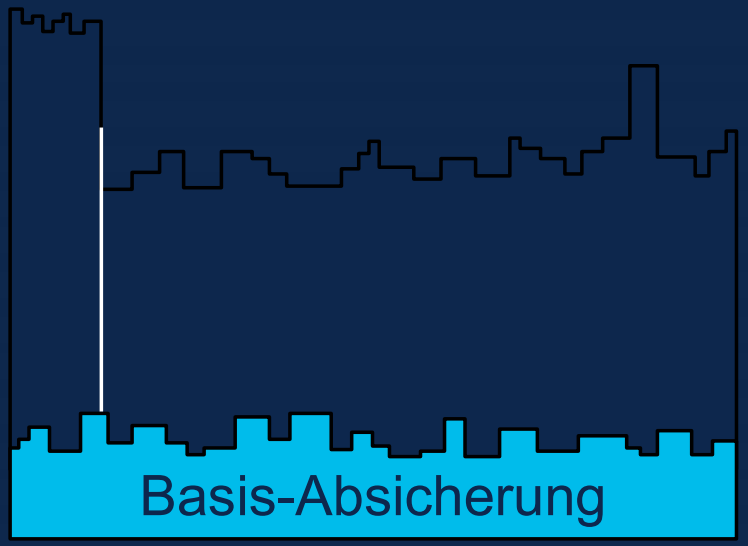
Überblick Vorgehensweisen



Die Basis-Absicherung

Von Null auf…



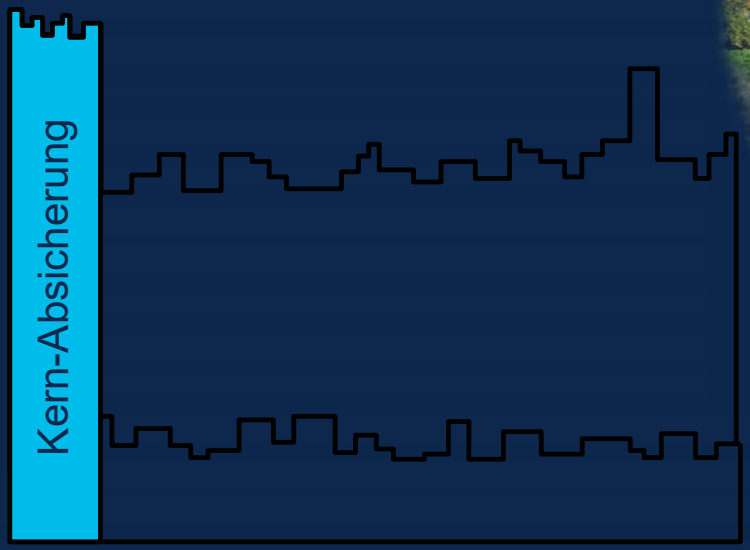


… ein bisschen

Die Standard-Absicherung

Die Kern-Absicherung

Schutz der Kronjuwelen



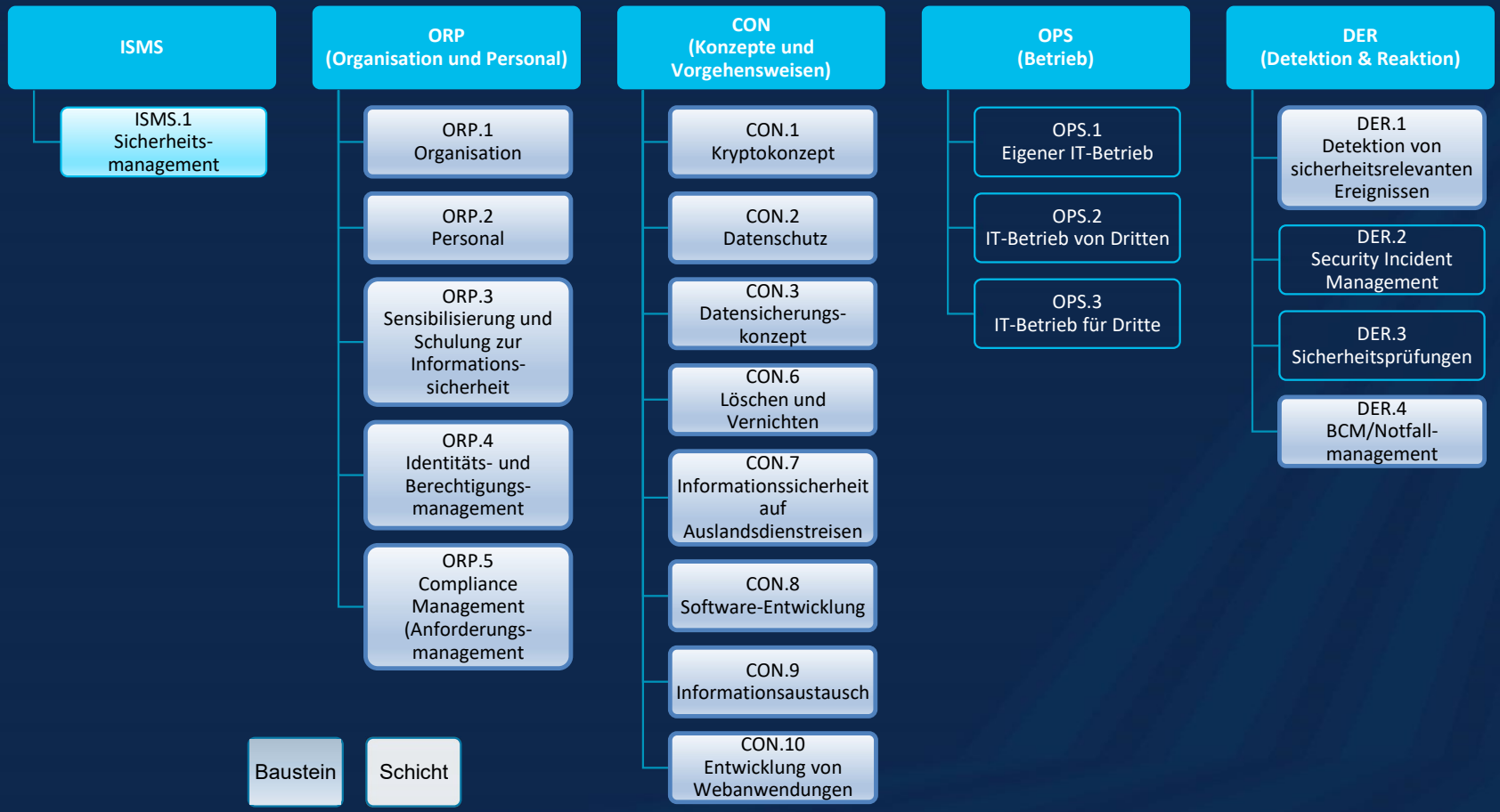
IT-Grundschutz BSI

- 97 Bausteine
  - Online in verschiedenen Formaten
  - Druckversion beim Bundesanzeigerverlag bestellbar

- Umsetzungshinweise (nicht Teil des Kompendiums)
  - 49 Umsetzungshinweise
  - Sammeldokument als PDF

Quelle: BSI

Prozess-Bausteine 2021



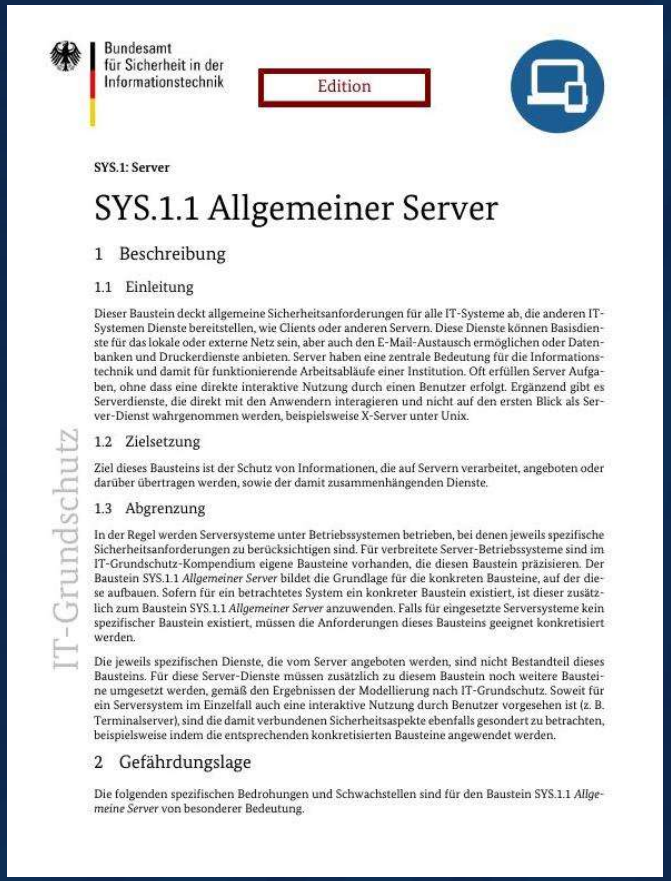
Quelle: BSI

System-Bausteine 2021

Quelle: BSI

Bausteine - Dokumentenstruktur

- Umfang: ca. 10 Seiten!
  - Beschreibung
  - Einleitung
  - Zielsetzung
  - Abgrenzung und Modellierung
  - Zuständige ~~Verantwortliche~~
- Spezifische Gefährdungslage
- Anforderungen (keine Maßnahmen)
  - Basis-Anforderungen (B)
  - Standard-Anforderungen (S)
  - Anforderungen bei erhöhtem Schutzbedarf (H)
- Referenzen auf weiterführende Informationen (Fließtext)
- Anlage: Kreuzreferenztabelle (Angabe CIA)



Bundesamt
für Sicherheit in der
Informationstechnik

Edition

SYS.1: Server

SYS.1.1 Allgemeiner Server

1 Beschreibung

1.1 Einleitung

Dieser Baustein deckt allgemeine Sicherheitsanforderungen für alle IT-Systeme ab, die anderen IT-Systemen Dienste bereitstellen, wie Clients oder anderen Servern. Diese Dienste können Basisdienste für das lokale oder externe Netz sein, aber auch den E-Mail-Austausch ermöglichen oder Datenbanken und Druckerdienste anbieten. Server haben eine zentrale Bedeutung für die Informationstechnik und damit für funktionierende Arbeitsabläufe einer Institution. Oft erfüllen Server Aufgaben, ohne dass eine direkte interaktive Nutzung durch einen Benutzer erfolgt. Ergänzend gibt es Serverdienste, die direkt mit den Anwendern interagieren und nicht auf den ersten Blick als Server-Dienst wahrgenommen werden, beispielsweise X-Server unter Unix.

1.2 Zielsetzung

Ziel dieses Bausteins ist der Schutz von Informationen, die auf Servern verarbeitet, angeboten oder darüber übertragen werden, sowie der damit zusammenhängenden Dienste.

1.3 Abgrenzung

In der Regel werden Serversysteme unter Betriebssystemen betrieben, bei denen jeweils spezifische Sicherheitsanforderungen zu berücksichtigen sind. Für verbreitete Server-Betriebssysteme sind im IT-Grundschutz-Kompendium eigene Bausteine vorhanden, die diesen Baustein präzisieren. Der Baustein SYS.1.1 *Allgemeiner Server* bildet die Grundlage für die konkreten Bausteine, auf der diese aufbauen. Sofern für ein betrachtetes System ein konkreter Baustein existiert, ist dieser zusätzlich zum Baustein SYS.1.1 *Allgemeiner Server* anzuwenden. Falls für eingesetzte Serversysteme kein spezifischer Baustein existiert, müssen die Anforderungen dieses Bausteins geeignet konkretisiert werden.

Die jeweils spezifischen Dienste, die vom Server angeboten werden, sind nicht Bestandteil dieses Bausteins. Für diese Server-Dienste müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz. Soweit für ein Serversystem im Einzelfall auch eine interaktive Nutzung durch Benutzer vorgesehen ist (z. B. Terminalserver), sind die damit verbundenen Sicherheitsaspekte ebenfalls gesondert zu betrachten, beispielsweise indem die entsprechenden konkretisierten Bausteine angewendet werden.

2 Gefährdungslage

Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.1.1 *Allgemeine Server* von besonderer Bedeutung.

IT-Grundschutz

Neu seit 2020

Quelle: BSI

Einleitung und Zielsetzung

APP.3.2: Webserver

1 Beschreibung

1.1 Einleitung

Ein Webserver ist die Kernkomponente jedes Webangebotes: Er nimmt Anfragen der Clients über einen Browser entgegen und liefert die entsprechenden Inhalte zurück. Der Transport der Daten erfolgt in der Regel über das Hypertext Transfer Protocol (HTTP) oder dessen mit Transport Layer Security (TLS) verschlüsselte Variante HTTP Secure (HTTPS). Da Webserver eine einfache Schnittstelle zwischen Serveranwendungen und Benutzern bieten, werden sie auch häufig für interne Informationen und Anwendungen in Institutionsnetzen, wie dem Intranet, eingesetzt.

Webserver sind in der Regel direkt im Internet verfügbar und bieten somit eine exponierte Angriffsfläche. Deswegen müssen sie durch geeignete Schutzmaßnahmen abgesichert werden.

1.2 Zielsetzung

Ziel dieses Bausteins ist der Schutz des Webservers und der Informationen, die durch den Webserver bereitgestellt oder damit verarbeitet werden.

APP.3.2: Webserver

1 Beschreibung

1.1 Einleitung

Ein Webserver ist die Kernkomponente jedes Webangebotes: Er nimmt Anfragen der Clients über einen Browser entgegen und liefert die entsprechenden Inhalte zurück. Der Transport der Daten erfolgt in der Regel über das Hypertext Transfer Protocol (HTTP) oder dessen mit Transport Layer Security (TLS) verschlüsselte Variante HTTP Secure (HTTPS). Da Webserver eine einfache Schnittstelle zwischen Serveranwendungen und Benutzern bieten, werden sie auch häufig für interne Informationen und Anwendungen in Institutionsnetzen, wie dem Intranet, eingesetzt.

Webserver sind in der Regel direkt im Internet verfügbar und bieten somit eine exponierte Angriffsfläche. Deswegen müssen sie durch geeignete Schutzmaßnahmen abgesichert werden.

1.2 Zielsetzung

Ziel dieses Bausteins ist der Schutz des Webservers und der Informationen, die durch den Webserver bereitgestellt oder damit verarbeitet werden.

Abgrenzung und Modellierung

1.3 Abgrenzung und Modellierung

Der Baustein muss auf alle Webserver des Informationsverbunds angewendet werden.

Die Bezeichnung Webserver wird sowohl für die Software verwendet, welche die HTTP-Anfragen beantwortet, als auch für die IT-Systeme, auf denen diese Software ausgeführt wird. In diesem Baustein wird vorrangig die Webserver-Software betrachtet. Sicherheitsaspekte des IT-Systems, auf dem die Webserver-Software installiert ist, werden in den entsprechenden Bausteinen der Schicht SYS *IT-Systeme* behandelt (siehe SYS.1.1 *Allgemeiner Server* sowie beispielsweise SYS.1.3 *Server unter Linux und Unix* oder SYS.1.2.2 *Windows Server 2012*).

Empfehlungen, wie Webserver in die Netzarchitektur zu integrieren und mit Firewalls abzusichern sind, finden sich in den Bausteinen NET.1.1 *Netzarchitektur und -design* bzw. NET.3.2 *Firewall*.

Der Baustein behandelt grundsätzliche Aspekte, die für die Bereitstellung von Webinhalten wichtig sind. Dynamische Inhalte, die durch Webanwendungen bereitgestellt werden, sind nicht Gegenstand des vorliegenden Bausteins. Diese werden im Baustein APP.3.1 *Webanwendungen* behandelt. Ebenso werden hier keine Webservices betrachtet.

In der Regel werden die Verbindungen zu Webservern verschlüsselt. Der Baustein CON.1 *Kryptokonzept* beschreibt, wie die dazu notwendigen kryptografischen Schlüssel sicher verwaltet werden können.

Werden Webserver nicht selbst betrieben, sondern über einen Hosting-Anbieter bereitgestellt, ist der Baustein OPS.2.1 *Outsourcing für Kunden* zu beachten.

Gefährdungslage und Zuständige

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein APP.3.2 *Webserver* von besonderer Bedeutung:

2.1 Reputationsverlust

Schaffen es Angreifer, eine Webseite zu manipulieren bzw. umzugestalten (Defacement), so kann der Ruf der Institution geschädigt werden. Ebenso kann die Veröffentlichung falscher Informationen (etwa fehlerhafter Produktbeschreibungen) dazu führen, dass die Reputation der Institution in der Öffentlichkeit verloren geht oder dass die Institution abgemahnt wird. Ein Schaden kann auch entstehen, wenn die Webseite nicht verfügbar ist und potenzielle Kunden deshalb zu Mitbewerbern wechseln.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.3.2 *Webserver* 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 zuständig, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche, Leiter IT

Basis-Anforderungen (Beispiel)

Die folgenden Anforderungen **MÜSSEN** für den Baustein APP.3.2 Webserver vorrangig erfüllt werden:

APP.3.2.A6 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.2.A7 Rechtliche Rahmenbedingungen für Webangebote [Fachverantwortliche] (B)

Werden über den Webserver Inhalte für Dritte publiziert oder Dienste angeboten, **MÜSSEN** dabei die relevanten rechtlichen Rahmenbedingungen beachtet werden. So **MÜSSEN** die jeweiligen Telemedien- und Datenschutzgesetze sowie das Urheberrecht eingehalten werden. Auch **SOLLTEN** die Anforderungen an die Barrierefreiheit gemäß Behindertengleichstellungsgesetz beachtet werden.

Standard-Anforderungen (Beispiel)

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein APP.3.2 Webserver. Sie **SOLLTEN** grundsätzlich erfüllt werden.

APP.3.2.A8 Planung des Einsatzes eines Webservers (S)

Es **SOLLTE** geplant und dokumentiert werden, für welchen Zweck der Webserver eingesetzt werden soll. Außerdem **SOLLTE** festgelegt werden, wie er in die vorhandene IT-Infrastruktur integriert wird. In der Dokumentation **SOLLTEN** auch die Informationen oder Dienstleistungen des Webangebots und die jeweiligen Zielgruppen beschrieben werden. Für den technischen Betrieb und die Webinhalte **SOLLTEN** geeignete Verantwortliche festgelegt werden.

Anforderungen bei erhöhtem Schutzbedarf (Beispiel)

Im Folgenden sind für den Baustein APP.3.2 Webserver **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.

APP.3.2.A15 Redundanz (H)

Webserver **SOLLTEN** redundant ausgelegt werden. Auch die Internetanbindung des Webservers und weiterer IT-Systeme, wie etwa der Webanwendungsserver, **SOLLTEN** redundant ausgelegt sein.

APP.3.2.A17 Einsatz erweiterter Authentisierungsmethoden für Webserver (H)

Es **SOLLTEN** erweiterte Authentisierungsmethoden eingesetzt werden, wie z. B. Client-Zertifikate oder eine Mehr-Faktor-Authentisierung.

Weiterführende Informationen und Kreuzreferenztabelle

4 Weiterführende Informationen

4.1 Wissenswertes

Das Bundesamt für Sicherheit in der Informationstechnik hat folgende weiterführende Dokumente veröffentlicht, die für den Betrieb von Webservern relevant sein können:

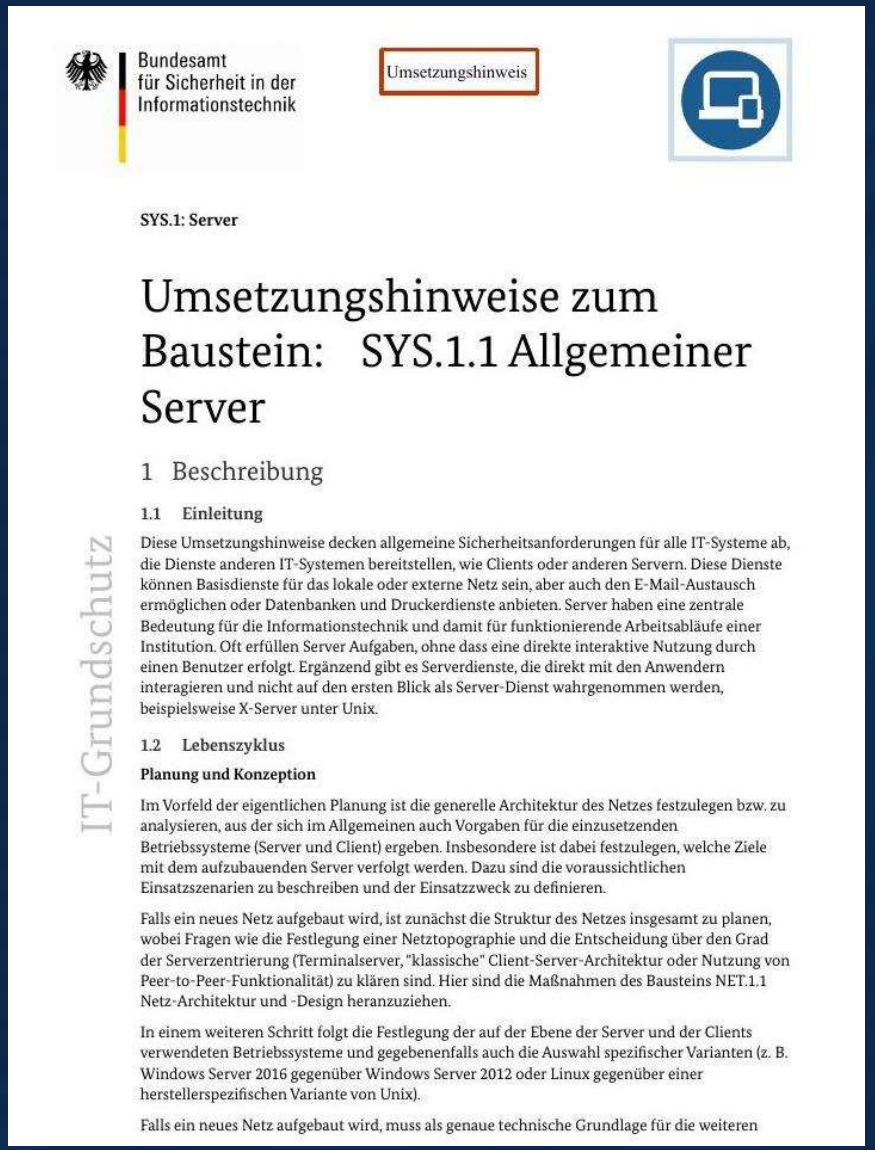
- Migration auf TLS 1.2 – Handlungsleitfaden
- Sicheres Webhosting: Handlungsempfehlung für Webhoster
- Sicheres Bereitstellen von Webangeboten (ISi-Webserver)

Das National Institute of Standards and Technology (NIST) stellt in seinem Dokument „Guideline on Securing Public Web Servers" Hinweise zur Absicherung von Webservern zur Verfügung.

Elementare Gefährdungen Anforderungen	CIA-Werte	G 0.11	G 0.15	G 0.18	G 0.19
APP.3.2.A1					X
APP.3.2.A2					X
APP.3.2.A3					X
APP.3.2.A17	CI				
APP.3.2.A18	A				
APP.3.2.A19					

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-Grundschutz-Bausteine, Studien, Herstellerdokumentation etc.



Bundesamt für Sicherheit in der Informationstechnik

Umsetzungshinweis

SYS.1: Server

Umsetzungshinweise zum Baustein: SYS.1.1 Allgemeiner Server

IT-Grundschutz

1 Beschreibung

1.1 Einleitung

Diese Umsetzungshinweise decken allgemeine Sicherheitsanforderungen für alle IT-Systeme ab, die Dienste anderen IT-Systemen bereitstellen, wie Clients oder anderen Servern. Diese Dienste können Basisdienste für das lokale oder externe Netz sein, aber auch den E-Mail-Austausch ermöglichen oder Datenbanken und Druckerdienste anbieten. Server haben eine zentrale Bedeutung für die Informationstechnik und damit für funktionierende Arbeitsabläufe einer Institution. Oft erfüllen Server Aufgaben, ohne dass eine direkte interaktive Nutzung durch einen Benutzer erfolgt. Ergänzend gibt es Serverdienste, die direkt mit den Anwendern interagieren und nicht auf den ersten Blick als Server-Dienst wahrgenommen werden, beispielsweise X-Server unter Unix.

1.2 Lebenszyklus

Planung und Konzeption

Im Vorfeld der eigentlichen Planung ist die generelle Architektur des Netzes festzulegen bzw. zu analysieren, aus der sich im Allgemeinen auch Vorgaben für die einzusetzenden Betriebssysteme (Server und Client) ergeben. Insbesondere ist dabei festzulegen, welche Ziele mit dem aufzubauenden Server verfolgt werden. Dazu sind die voraussichtlichen Einsatzszenarien zu beschreiben und der Einsatzzweck zu definieren.

Falls ein neues Netz aufgebaut wird, ist zunächst die Struktur des Netzes insgesamt zu planen, wobei Fragen wie die Festlegung einer Netztopographie und die Entscheidung über den Grad der Serverzentrierung (Terminalserver, "klassische" Client-Server-Architektur oder Nutzung von Peer-to-Peer-Funktionalität) zu klären sind. Hier sind die Maßnahmen des Bausteins NET.1.1 Netz-Architektur und -Design heranzuziehen.

In einem weiteren Schritt folgt die Festlegung der auf der Ebene der Server und der Clients verwendeten Betriebssysteme und gegebenenfalls auch die Auswahl spezifischer Varianten (z. B. Windows Server 2016 gegenüber Windows Server 2012 oder Linux gegenüber einer herstellerspezifischen Variante von Unix).

Falls ein neues Netz aufgebaut wird, muss als genaue technische Grundlage für die weiteren

Quelle: BSI

Umsetzung der IT-Grundschutz-Vorgehensweise

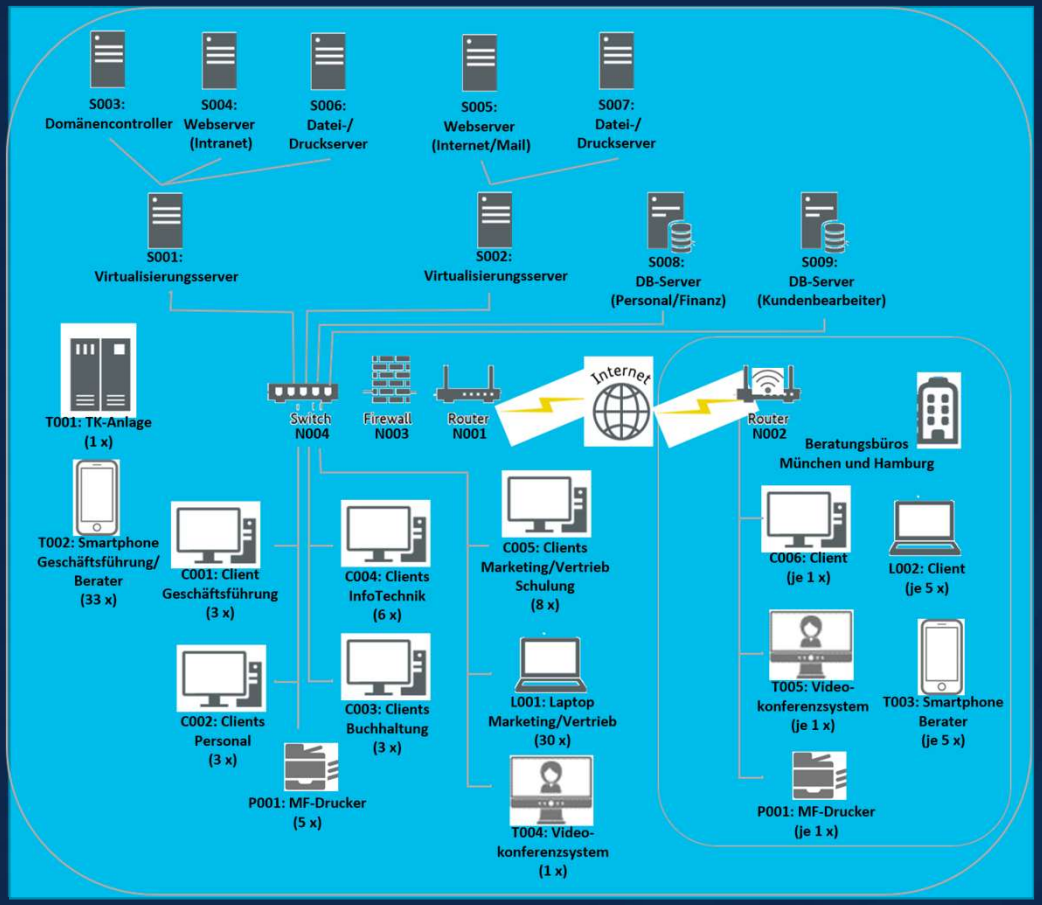
Strukturanalyse

Geschäftsprozesse

Anwendungen

Informationen

Netzplan erstellen



Komplexitätsreduktion durch Gruppenbildung

Objekte können dann ein und derselben Gruppe zugeordnet werden, wenn die Objekte alle vom gleichen Typ sind,

- ähnliche Aufgaben haben,
- ähnlichen Rahmenbedingungen unterliegen und
- den gleichen Schutzbedarf aufweisen.

Schutzbedarfsfeststellung

Die Schutzbedarfsfeststellung für den Informationsverbund gliedert sich in mehrere Schritte:

- Definition der Schutzbedarfskategorien
- Schutzbedarfsfeststellung für
  - Geschäftsprozesse und Anwendungen,
  - IT-Systeme, (inkl. IoT und ICS),
  - Gebäude, Räume, Werkhallen etc.,
  - für Kommunikationsverbindungen
- Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung

Definition der Schutzbedarfskategorien

Schutzbedarf meist nicht quantifizierbar, daher Beschränkung im IT-Grundschutz im Weiteren auf qualitative Aussagen

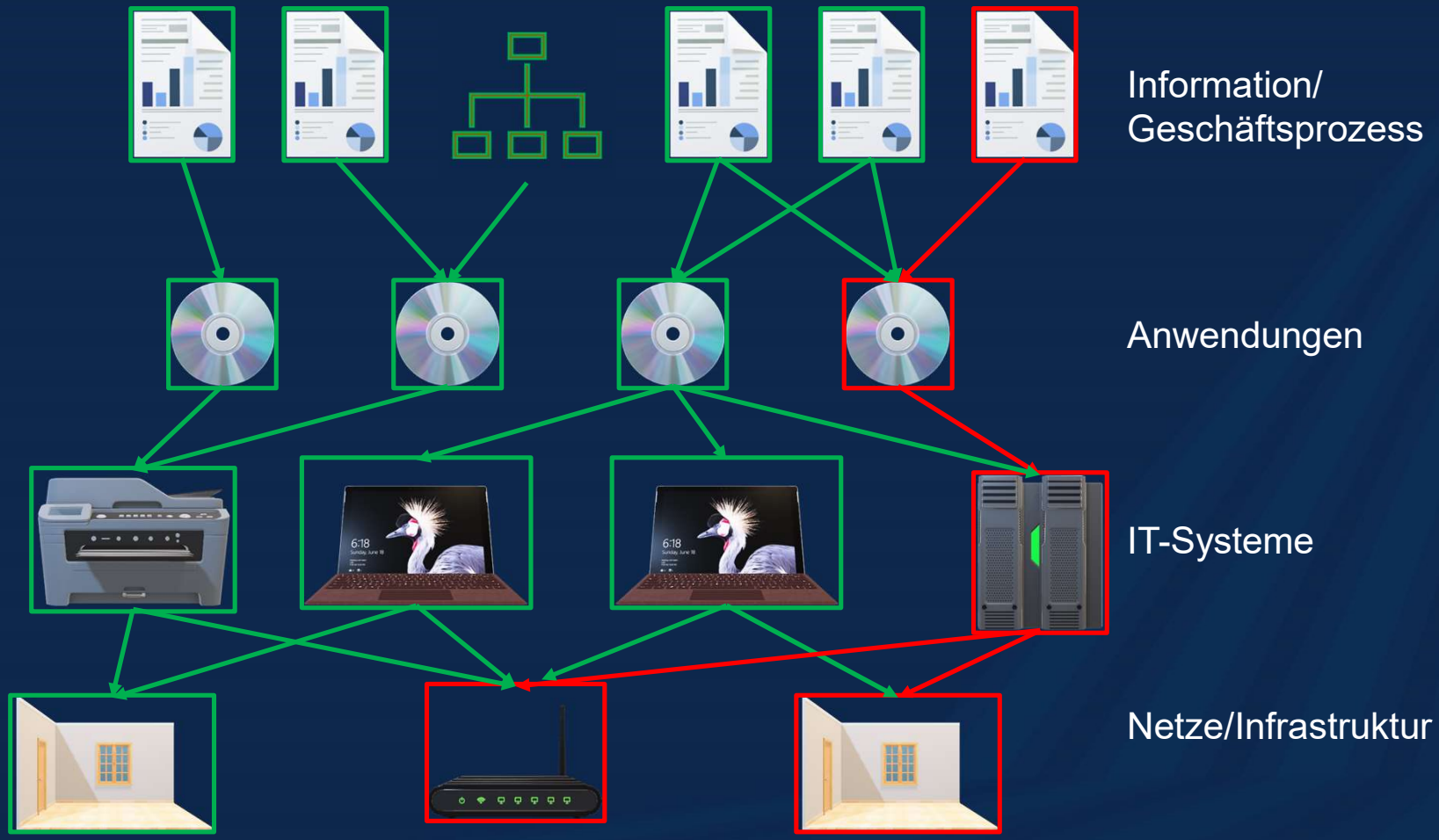
Typische Schadensszenarien

Zuordnung von Kategorien zu Schadensszenarien

Schutzbedarfskategorie "normal"	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung erscheint nicht möglich.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 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.

Tabelle 1: Schutzbedarfskategorie „normal“

Feststellung/Vererbung des Schutzbedarfs

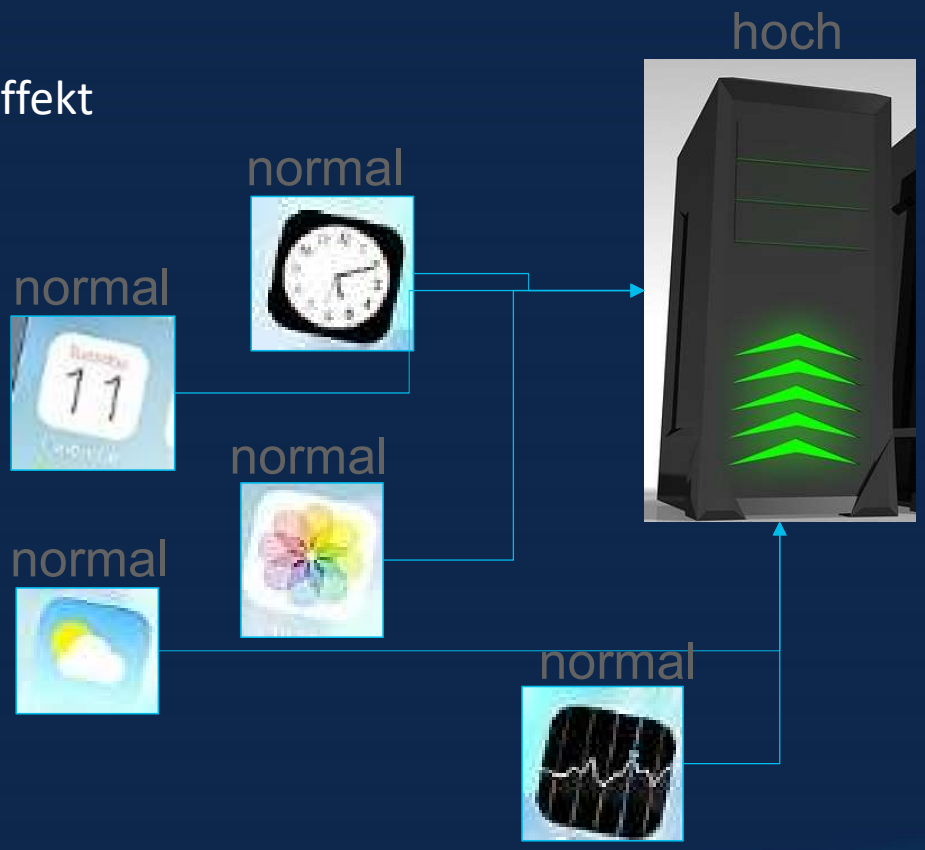


Prinzipien der Vererbung des Schutzbedarfs

- Maximum-Prinzip

Prinzipien der Vererbung des Schutzbedarfs

- Kumulationseffekt



Prinzipien der Vererbung des Schutzbedarfs

- Verteilungseffekt

Beispiel einer Schutzbedarfsfeststellung

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH

Bezeichnung	Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	Plattform / Baustein	Verantwortlich / Administrator	Vertraulichkeit	Begründung für die Vertraulichkeit	Integrität	Begründung für die Integrität	Verfügbarkeit	Begründung für die Verfügbarkeit
A003	Textverarbeitung, Tabellenkalkulation	Office-Produkt 2010	IT-Betrieb	normal	Die Anwendung selbst enthält keine Informationen.	normal	Die Anwendung selbst enthält keine Informationen	normal	Die Anwendung wird lokal installiert. Die Lizenzen sind entsprechend aufgehoben, so dass eine Neuinstallation schnell ermöglicht werden kann. Eine Ausfallzeit von mehr als 24 Stunden ist tolerierbar.
A007	Lotus Notes	Lotus Notes	IT-Betrieb	hoch	Über das E-Mailsystem werden viele, teilweise vertrauliche Informationen versendet. Durch die Anwendung werden alle E-Mails verschlüsselt.	normal	Durch eine Signatur kann die Integrität einer E-Mail festgestellt werden.	sehr hoch	Das Mailsystem sollte auch dann zur Verfügung stehen, falls andere Kommunikationsmittel ausfallen (z.B. Faxserver)
C002	Laptop Verwaltung	Client unter Windows 10	IT-Betrieb	normal	Maximumprinzip Auf dem Arbeitsplatzrechner werden keine Informationen gespeichert	normal	Maximumprinzip Auf dem Arbeitsplatzrechner werden keine Informationen gespeichert	normal	Es ist ein Ausfall von höchstens 4 Stunden tolerierbar.

Schlussfolgerung aus den Ergebnissen der Schutzbedarfsfeststellung

Schutzwirkung von Sicherheitsanforderungen nach IT-Grundschutz	
Schutzbedarfskategorie „normal"	Sicherheitsanforderungen nach IT-Grundschutz sind im Allgemeinen ausreichend und angemessen.
Schutzbedarfskategorie „hoch"	Sicherheitsanforderungen nach IT-Grundschutz liefern eine Standard-Absicherung, sind aber unter Umständen alleine nicht ausreichend. Weitergehende Maßnahmen sollten auf Basis einer Risikoanalyse ermittelt werden.
Schutzbedarfskategorie „sehr hoch"	Sicherheitsanforderungen nach IT-Grundschutz liefern eine Standard-Absicherung, reichen aber alleine im Allgemeinen nicht aus. Die erforderlichen zusätzlichen Sicherheitsmaßnahmen müssen individuell auf der Grundlage einer Risikoanalyse ermittelt werden.

Tabelle 5: Schutzwirkung von Sicherheitsanforderungen nach IT-Grundschutz

Bausteine für einen Home Office-Client

Inf. 8 Häuslicher Arbeitsplatz

OPS 1.2.4 Telearbeit

SYS.2.1 Allgemeiner Client

SYS.2.2.3 Client unter Windows 10

SYS.3.1 Laptop

NET2.1 WLAN Betrieb

NET2.2 WLAN Nutzung

APP.6 Allgemeine Software

APP.1.1 Office Produkte

APP.5.3 Allgemeiner E-Mail-Client/-Server

APP.5.2 Microsoft Exchange und Outlook

Zu diesen Bausteine, kommen noch Anforderungen übergeordneter Prozessbausteine hinzu (z.B. ORP.3 Sensibilisierung und Schulung zur Informationssicherheit), die meist auf den ganzen Informationsverbund gelten.

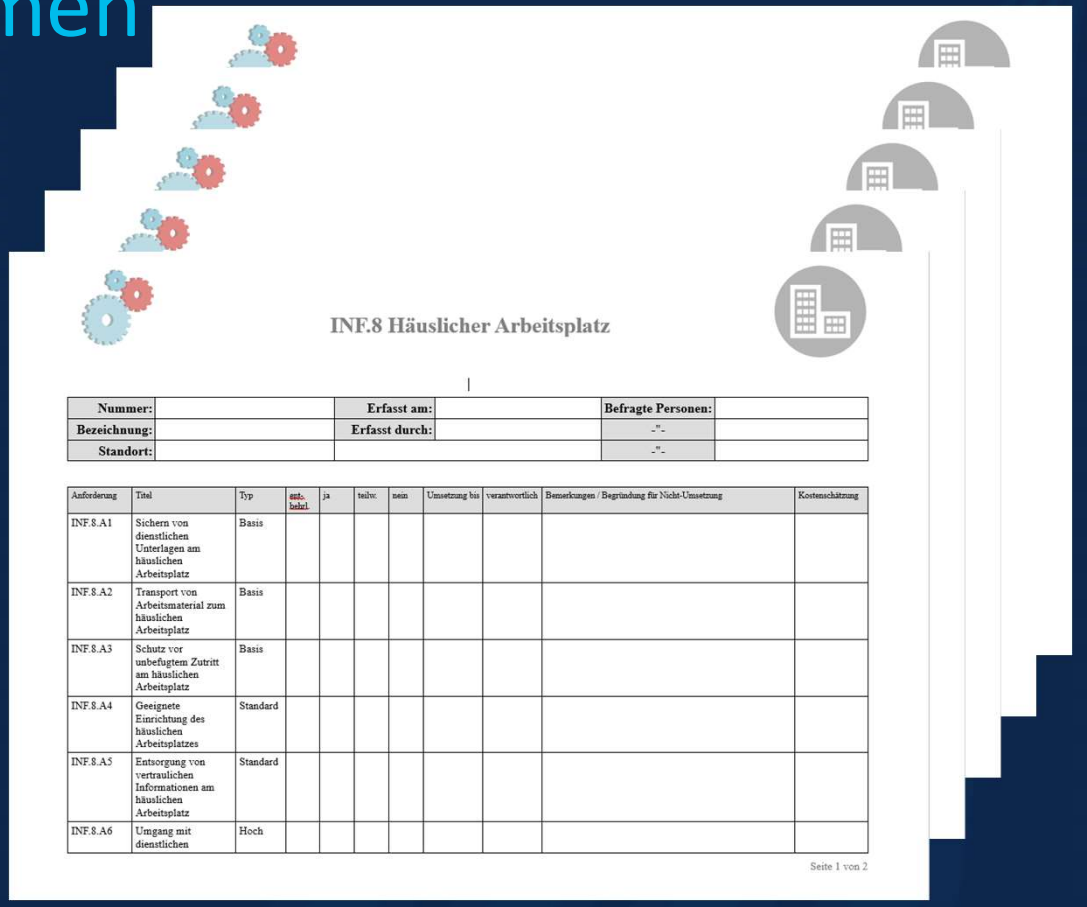
Ist-Aufnahme mit Fragebögen

INF.8 Häuslicher Arbeitsplatz

Nummer:		**Erfasst am:**		**Befragte Personen:**	
Bezeichnung:		**Erfasst durch:**		-"-	
Standort:				-"-	

Anforderung	Titel	Typ	entbehrl.	ja	teilw.	nein	Umsetzung bis	verantwortlich	Bemerkungen / Begründung für Nicht-Umsetzung	Kostenschätzung
INF.8.A1	Sichern von dienstlichen Unterlagen am häuslichen Arbeitsplatz	Basis								
INF.8.A2	Transport von Arbeitsmaterial zum häuslichen Arbeitsplatz	Basis								
INF.8.A3	Schutz vor unbefugtem Zutritt am häuslichen Arbeitsplatz	Basis								
INF.8.A4	Geeignete Einrichtung des häuslichen Arbeitsplatzes	Standard								
INF.8.A5	Entsorgung von vertraulichen Informationen am häuslichen Arbeitsplatz	Standard								
INF.8.A6	Umgang mit dienstlichen	Hoch								

Ableitung weiterer Maßnahmen



INF.8 Häuslicher Arbeitsplatz

Nummer:		**Erfasst am:**		**Befragte Personen:**	
Bezeichnung:		**Erfasst durch:**		-"-	
Standort:				-"-	

Anforderung	Titel	Typ	entbehrl.	ja	teilw.	nein	Umsetzung bis	verantwortlich	Bemerkungen / Begründung für Nicht-Umsetzung	Kostenschätzung
INF.8.A1	Sichern von dienstlichen Unterlagen am häuslichen Arbeitsplatz	Basis								
INF.8.A2	Transport von Arbeitsmaterial zum häuslichen Arbeitsplatz	Basis								
INF.8.A3	Schutz vor unbefugtem Zutritt am häuslichen Arbeitsplatz	Basis								
INF.8.A4	Geeignete Einrichtung des häuslichen Arbeitsplatzes	Standard								
INF.8.A5	Entsorgung von vertraulichen Informationen am häuslichen Arbeitsplatz	Standard								
INF.8.A6	Umgang mit dienstlichen	Hoch								

Seite 1 von 2

Fragen?