

Datenschutz und Kryptographie

Modul DSKRY-40 im Studiengang Informatik

Referent: Dr. Hendrik Siegmund

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Das ISMS aufbauen – Phasen
 - Sicherheitsprozess beginnen
 - Organisation aufbauen
 - Sicherheitsprozess umsetzen
 - Kontrollieren und Optimieren
- ...im Detail doch etwas komplexer:

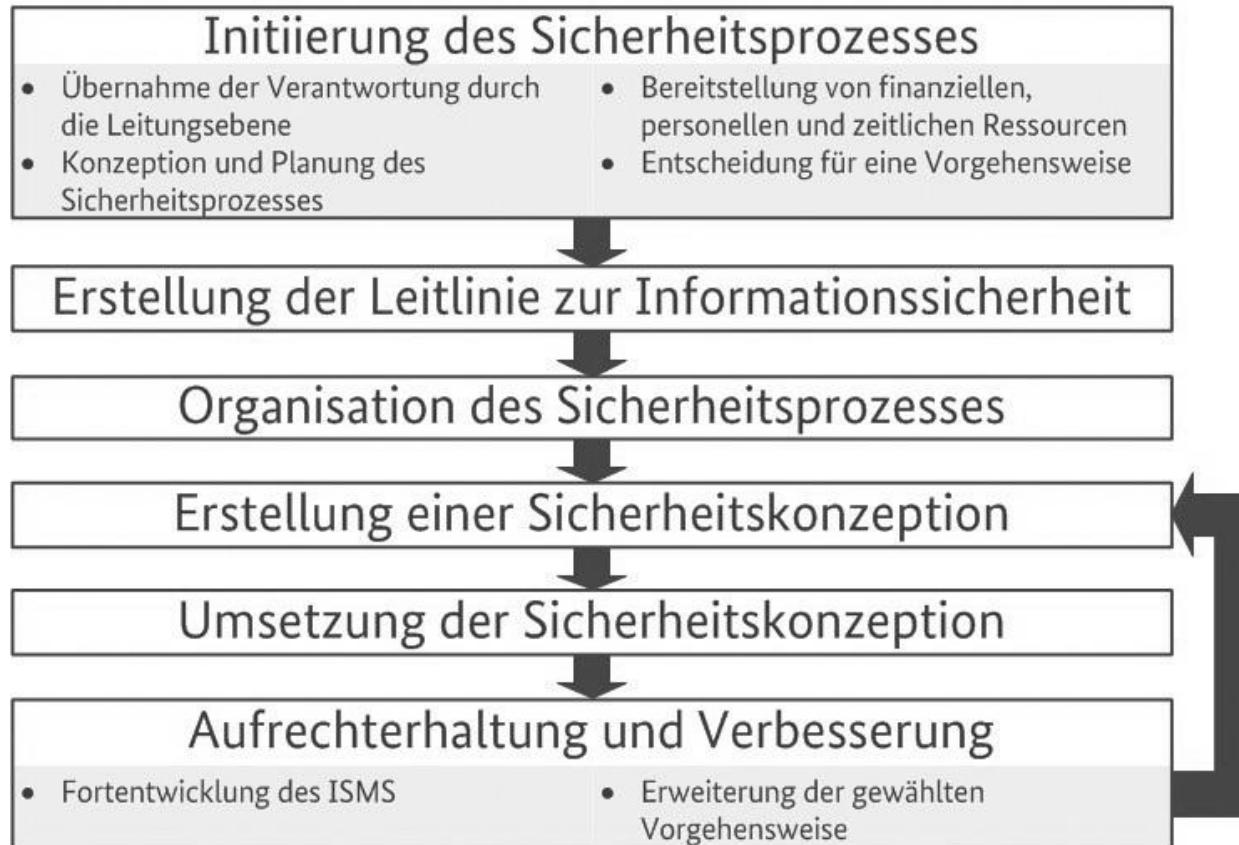
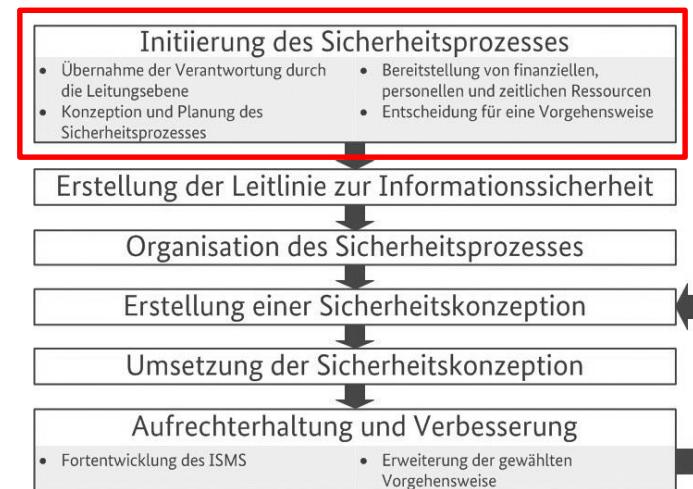


Abb.: BSI-Standard 200-2

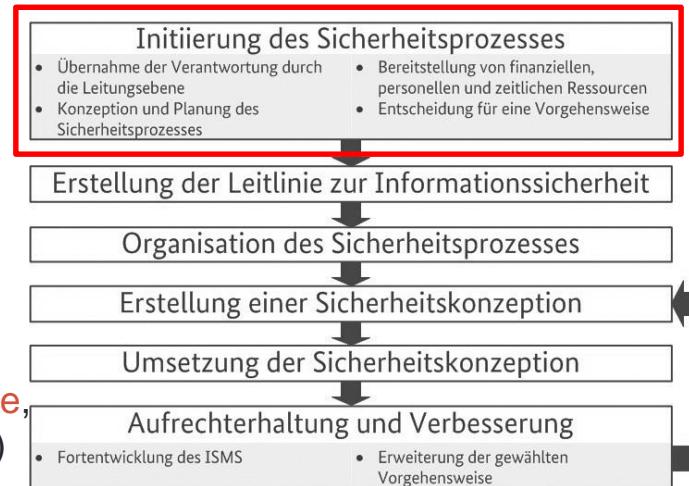
IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Das ISMS aufbauen – konkrete Aufgaben 1
 - Initiierung des Sicherheitsprozesses 1
 - **Wer:** Oberste Leitungsebene
 - **Was:** Verantwortung übernehmen
 - Sich über Risiken und Konsequenzen fehlender Informationssicherheit informieren
 - Evtl. schon eine(n) ISB benennen
 - Sicherheitsprozess auf den Weg bringen



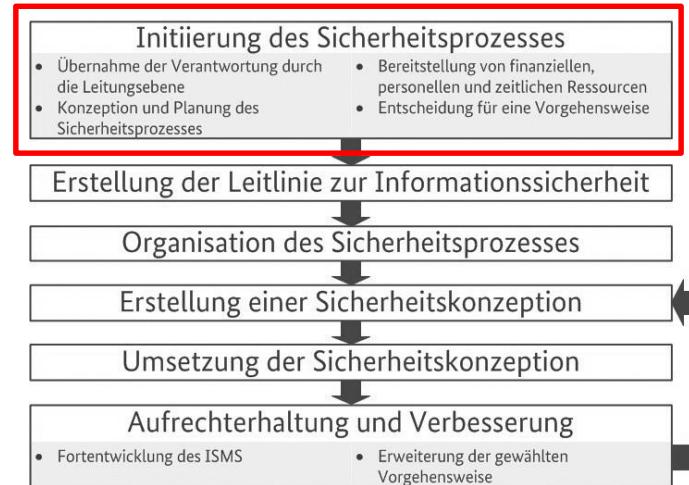
IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Das ISMS aufbauen – konkrete Aufgaben 1
 - Initiierung des Sicherheitsprozesses 2
 - **Wer:** Oberste Leitungsebene, ggf. ISB
 - **Was:** Sicherheitsprozess entwickeln
 - Rahmenbedingungen analysieren
 - Sicherheitsziele definieren
 - Sicherheitsniveau ermitteln:
normal, hoch, sehr hoch (S. 24-25 BSI 200.2)
 - Ersterfassung **Prozesse, Anwendungen, Systeme**, geringe Beschreibungstiefe (S. 26-28 BSI 200-2)



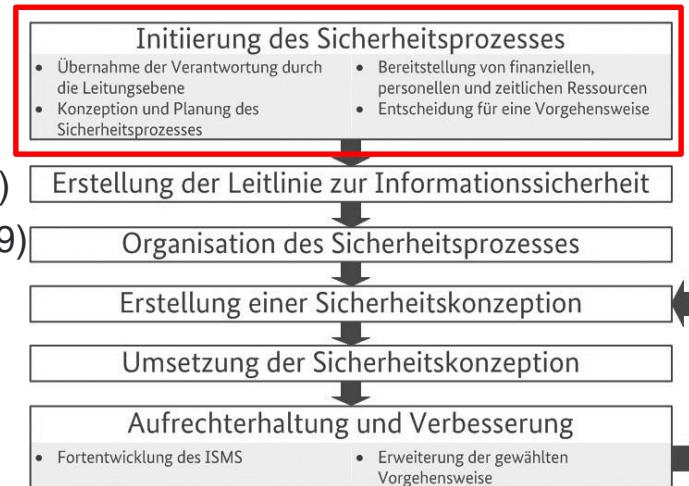
IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Das ISMS aufbauen – konkrete Aufgaben 1
 - Initiierung des Sicherheitsprozesses 3
 - **Wer:** Oberste Leitungsebene
 - **Was:** Ressourcen bereitstellen
 - Finanzielle
 - Zeitliche
 - Personelle
 - **Spätestens jetzt ISB benennen**



IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Das ISMS aufbauen – konkrete Aufgaben 1
 - Initiierung des Sicherheitsprozesses 4
 - **Wer:** Oberste Leitungsebene
 - **Was:** Für eine Vorgehensweise entscheiden
 - **Basis-Absicherung:** Einstieg oder für KMU (S.29)
 - **Kern-Absicherung:** Einstieg für Teilbereiche (S.29)
 - **Standard-Absicherung:** Normalfall für alle (S.30)
 - Geltungsbereich festlegen
 - **Oder:** Auswahl einer anderen Vorgehensweise, z.B. ISO 27001



IT-Sicherheit

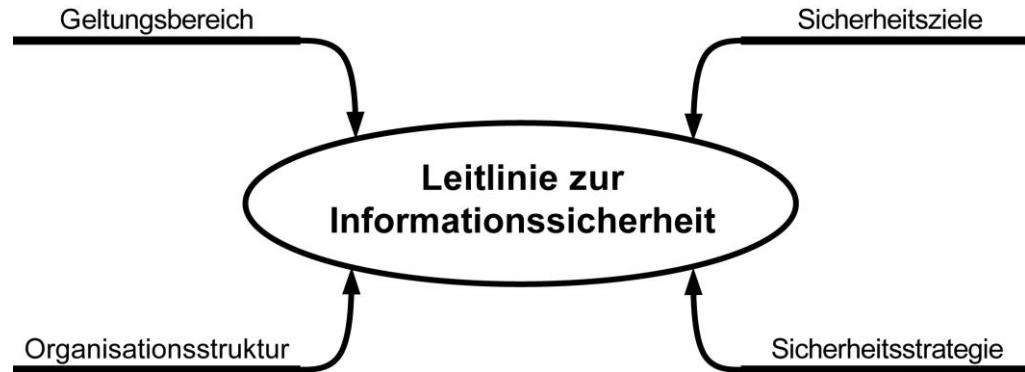
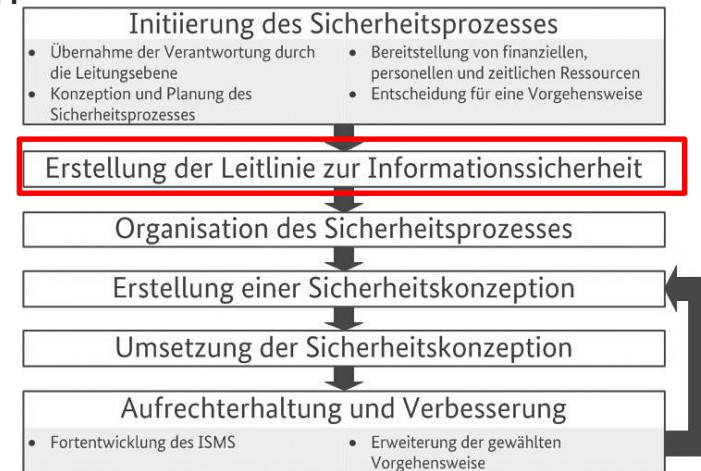


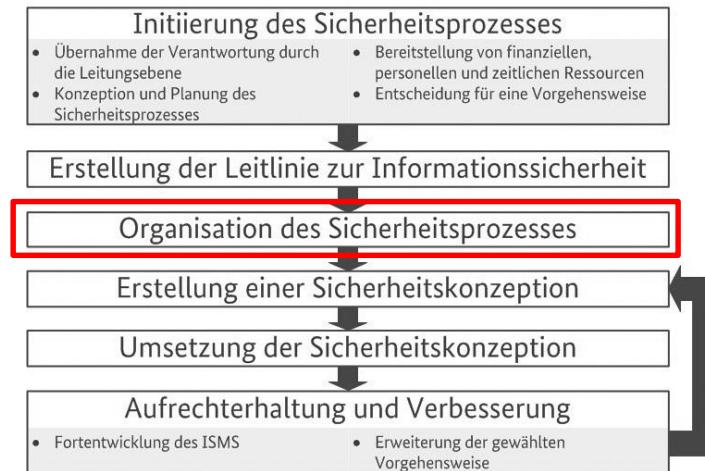
Abb.: BSI-Standard 200-2

- IT-Sicherheit – BSI Grundschutz - Methodik
- Das ISMS aufbauen – konkrete Aufgaben 2
 - Leitlinie zur Informationssicherheit erstellen
 - **Wer:** Oberste Leitungsebene, ISB
 - **Was:** Strategiepapier
 - Bekenntnis zur Informationssicherheit
 - Beschreibung des **Geltungsbereichs**
 - Beschreibung der **Sicherheitsziele**
 - Beschreibung der **Organisationsstruktur**
 - Beschreibung der **Sicherheitsstrategie**
 - Informationssicherheitsleitlinie veröffentlichen



IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Das ISMS aufbauen – konkrete Aufgaben 3
 - Sicherheitsprozess organisieren 1
 - **Wer:** Leitungsebene, ISB, DSB, Fachverantwortliche
 - **Was:** Aufbau einer Informationssicherheitsorganisation
 - Rollen, Verantwortlichkeiten, Zuständigkeiten definieren
 - Datenschutzbeauftragte(n) einbeziehen



IT-Sicherheit

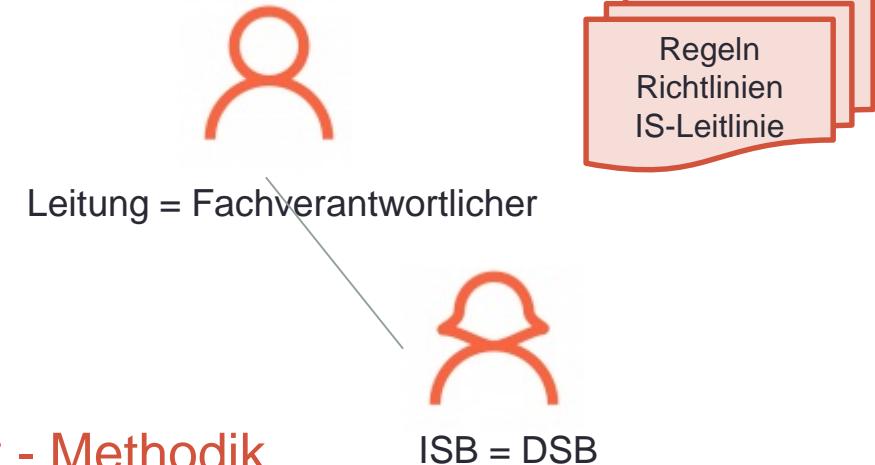
- IT-Sicherheit – BSI Grundschutz - Methodik
- Das ISMS aufbauen – konkrete Aufgaben 3
 - Sicherheitsprozess organisieren 2
 - **Wer:** Leitungsebene, ISB, DSB, Fachverantwortliche (Business Owner)...
 - **Was:** Aufbau einer Informationssicherheitsorganisation
 - Verschiedene Varianten, abhängig von Organisationsgröße und Branche

Minimale IS-Organisation nach BSI 200-2

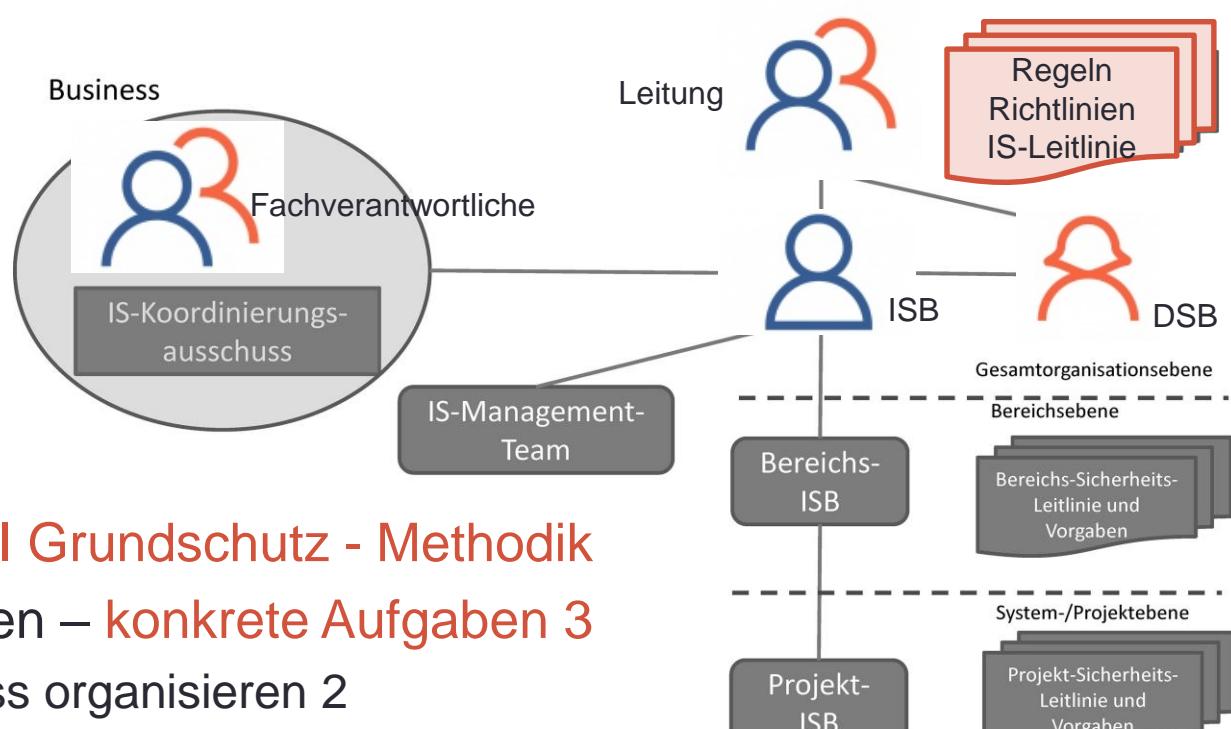


IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Das ISMS aufbauen – konkrete Aufgaben 3
 - Sicherheitsprozess organisieren 2
 - **Wer:** Leitungsebene, ISB, DSB, Fachverantwortliche (Business Owner)...
 - **Was:** Aufbau einer Informationssicherheitsorganisation
 - Verschiedene Varianten, abhängig von Organisationsgröße und Branche
 - **In KMU können und dürfen Rollen verschmelzen**



IT-Sicherheit

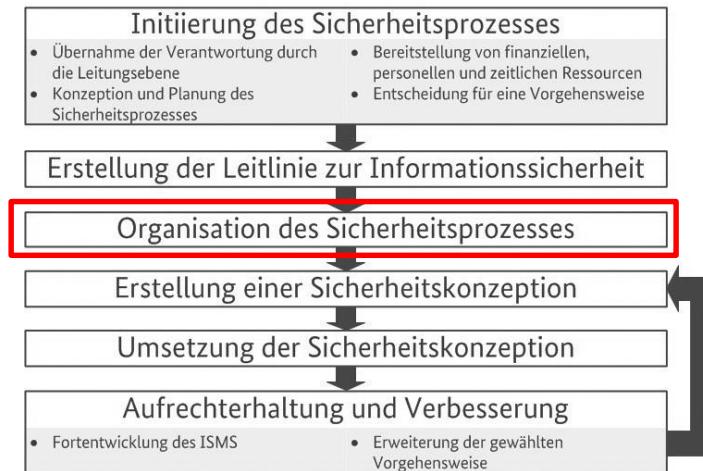


- IT-Sicherheit – BSI Grundschutz - Methodik
- Das ISMS aufbauen – konkrete Aufgaben 3
 - Sicherheitsprozess organisieren 2
 - **Wer:** Leitungsebene, ISB, DSB, Fachverantwortliche (Business Owner)...
 - **Was:** Aufbau einer Informationssicherheitsorganisation
 - Verschiedene Varianten, abhängig von Organisationsgröße und Branche
 - **In großen Unternehmen werden Bereiche und Teams gebildet**
 - **Bei Bedarf separate Strukturen für Projekte**

Abb.: Verändert aus BSI-Standard 200-2

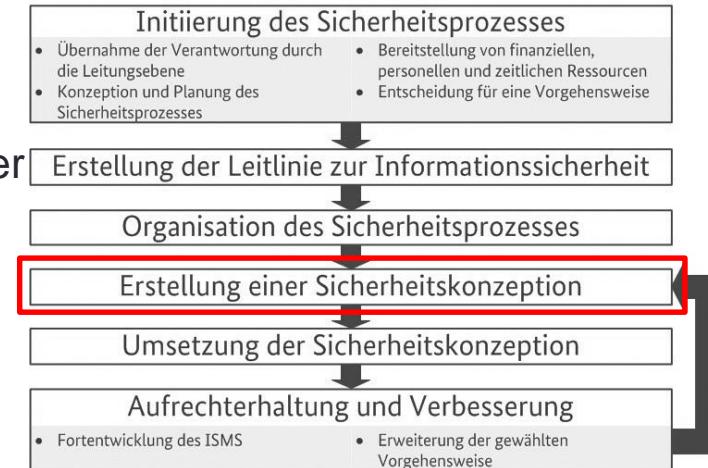
IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Das ISMS aufbauen – konkrete Aufgaben 3
 - Sicherheitsprozess organisieren 3
 - **Wer:** Leitungsebene, ISB, DSB, Fachverantwortliche
 - **Was:** Sicherheitsorganisation in das Unternehmen integrieren
 - Fachverantwortliche beteiligen
 - IT-Abteilung einbeziehen
 - Evtl. Externe Sicherheitsexperten hinzuziehen
 - Dokumentieren



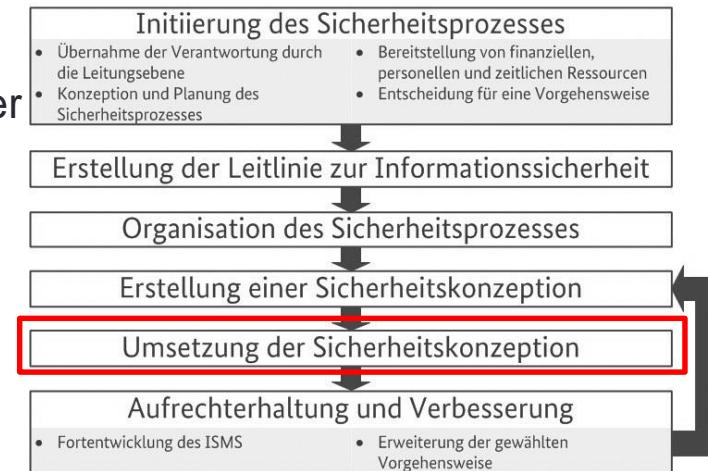
IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Das ISMS aufbauen – konkrete Aufgaben 4
 - Sicherheitskonzept erstellen
 - **Wer:** Koordination durch ISB, Zuarbeit DSB, Fachverantwortliche, IT-Abteilung
 - **Was:** Konkrete Auswahl und Modellierung der Bausteine für Informationssicherheit im gegebenen Unternehmen
 - Verschiedene Vorgehensweisen für **Basis-Absicherung**, **Kern-Absicherung** und **Standard-Absicherung**



IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Das ISMS aufbauen – konkrete Aufgaben 5
 - Sicherheitskonzept umsetzen
 - **Wer:** Koordination durch ISB, Umsetzung Fachverantwortliche, IT-Abteilung, Mitarbeiter
 - **Was:** Kosten- und Aufwand abschätzen
 - Umsetzungsreihenfolge festlegen
 - Mitarbeiter sensibilisieren und schulen
 - Maßnahmen durchführen

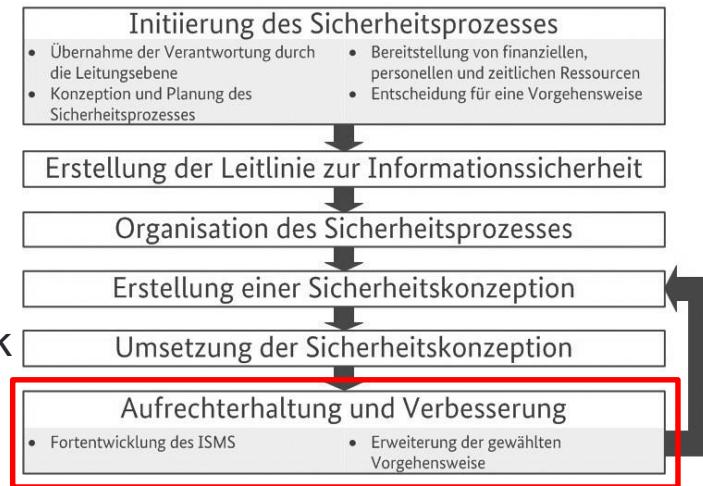


IT-Sicherheit

Reifegrad	Erläuterung
0	Es existiert kein ISMS und es ist auch nichts geplant.
1	ISMS ist geplant, aber nicht etabliert.
2	ISMS ist zum Teil etabliert.
3	ISMS ist voll etabliert und dokumentiert.
4	Zusätzlich zum Reifegrad 3 wird das ISMS regelmäßig auf Effektivität überprüft.
5	Zusätzlich zum Reifegrad 4 wird das ISMS regelmäßig verbessert.

Tabelle: BSI-Standard 200-2

- IT-Sicherheit – BSI Grundschutz - Methodik
- Das ISMS aufbauen – konkrete Aufgaben 6
 - Aufrechterhalten und verbessern
 - **Wer:** Sammlung durch ISB, Kontrolle durch Leitungsebene
 - **Was:** Kennzahlen
 - Ausfallzeiten, Verfügbarkeit...
 - Bewertung mit Reifegradmodell
 - Sicherheitsrevision, Cyber-Sicherheits-Check
 - Feedback in das Sicherheitskonzept
 - Bei Bedarf Zertifizierung

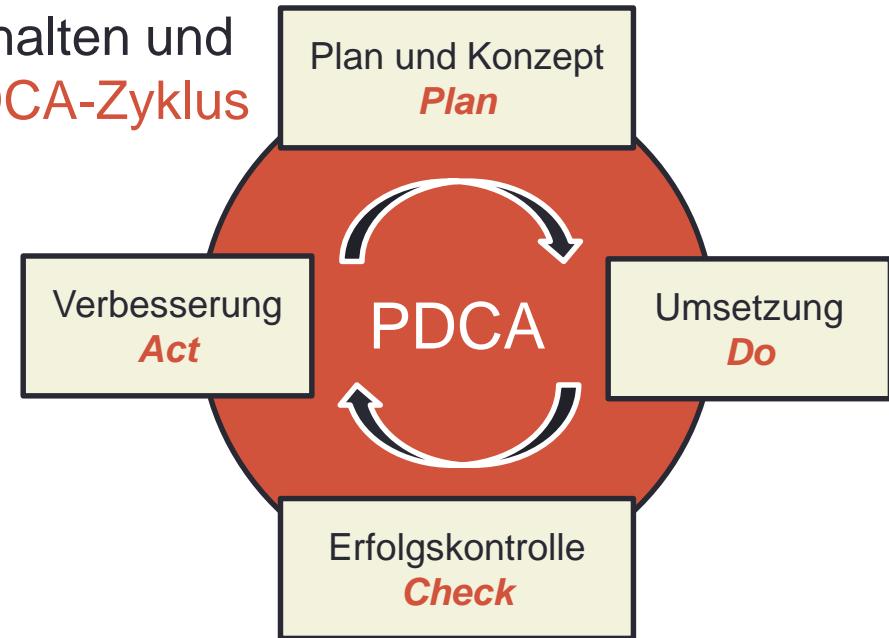


IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Informationssicherheit aufrechterhalten und kontinuierlich verbessern:
Der Lebenszyklus im ISMS
 - Planen **Plan**
 - Umsetzen bzw. durchführen **Do**
 - Erfolg und Zielerreichung kontrollieren **Check**
 - Mängel beseitigen, verbessern und optimieren **Act**
- ...und das alles im Kreislauf: **PDCA-Zyklus**

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Informationssicherheit aufrechterhalten und kontinuierlich verbessern: Der PDCA-Zyklus



IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz – Methodik
- Exkurse:
 - Informationssicherheitsbeauftragter (ISB oder ITSB)
 - Sicherheitskonzeption, auch IT-Sicherheitskonzept

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz – Methodik
- Exkurse:
 - Informationssicherheitsbeauftragter (ISB)
 - Zuständigkeiten und Aufgaben
 - Anforderungsprofil
 - Organisatorische Einordnung
 - Verhältnis zum Datenschutzbeauftragten



Quelle: vdi-wissensforum

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz – Methodik
- Exkurse:
 - Informationssicherheitsbeauftragter (ISB)
 - Zuständigkeiten und Aufgaben
 - Informationssicherheitsprozess steuern, koordinieren und daran mitwirken
 - Leitungsebene zur Informationssicherheit beraten, unterstützen und berichten
 - Erstellung von Sicherheitskonzept, Notfallkonzept usw. koordinieren
 - Sicherheitsvorfälle untersuchen und ggf. melden
 - Mitarbeiter sensibilisieren und schulen



Quelle: BSI - Webkurs IT-Grundschutz

IT-Sicherheit

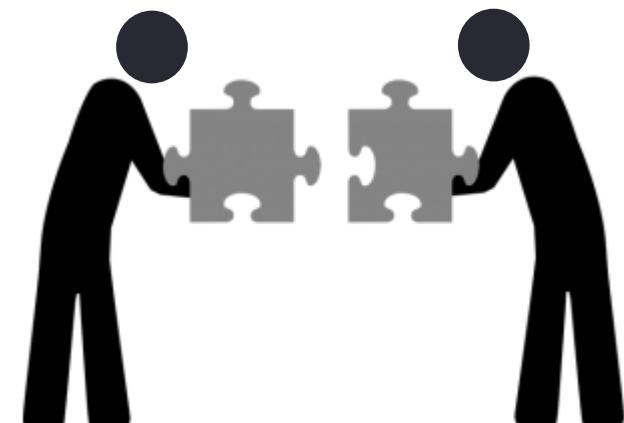
- IT-Sicherheit – BSI Grundschutz – Methodik
- Exkurse:
 - Informationssicherheitsbeauftragter (ISB)
 - Anforderungsprofil
 - Identifikation mit den Zielen der Informationssicherheit
 - Hohe Kooperations- und Teamfähigkeit
 - Hohe Kommunikationsfähigkeit
 - Projektmanagementerfahrung
 - Kenntnisse der Geschäftsprozesse und Fachverfahren des Unternehmens
 - Hohe Eigeninitiative und Bereitschaft zur ständigen Fort- und Weiterbildung

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz – Methodik
- Exkurse:
 - Informationssicherheitsbeauftragter (ISB)
 - Organisatorische Einordnung
 - Unabhängiges Arbeiten muss gewährleistet sein
 - Einordnung als Stabsstelle direkt unter Leitungsebene
 - Keine Weisungen von anderen Organisationseinheiten
 - NICHT der IT-Abteilung zugeordnet
 - Beschränkung auf Sicherheit von IT-Systemen
 - Interessenkonflikt, Administrator kontrolliert sich selbst

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz – Methodik
- Exkurse:
 - Informationssicherheitsbeauftragter (ISB)
 - Verhältnis zum DSB
 - Enge Zusammenarbeit
 - Personalunion möglich wenn Aufgabenbereiche sauber definiert sind und für beide Aufgaben genügend Ressourcen zur stehen (Zeit)



Quelle: brands-consulting

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz – Methodik
- Exkurse:
 - Sicherheitskonzeption, IT-Sicherheitskonzept
 - Grundsätzliches Vorgehen und Ziele
 - Varianten
 - Vorgehensweise in der konkreten Variante

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz – Methodik
- Exkurse:
 - Sicherheitskonzeption, IT-Sicherheitskonzept
 - Grundsätzliches Vorgehen und Ziele
 - Ist-Analyse des Informationsverbundes (alle Systeme im Geltungsbereich)
 - Risikoanalyse auf Basis des Ist-Standes durchführen
 - Strategie zur Risikobehandlung entwickeln
 - Sicherheitsmaßnahmen auswählen und dokumentieren
 - Das Sicherheitskonzept ist das zentrale Dokument des Sicherheitsprozesses
 - Prüfungsgrundlage z.B. für Wirtschaftsprüfung

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz – Methodik
- Exkurse:
 - Sicherheitskonzeption, IT-Sicherheitskonzept
 - Varianten
 - Basis-Absicherung
 - Kern-Absicherung
 - Standard-Absicherung (bevorzugt)

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz – Methodik
- Exkurse:

- Sicherheitskonzeption, IT-Sicherheitskonzept
 - Basis-Absicherung: Schnell und ohne großen Overhead
 - Weitere Schritte nötig:
 - Kern-Absicherung oder
 - Standard-Absicherung

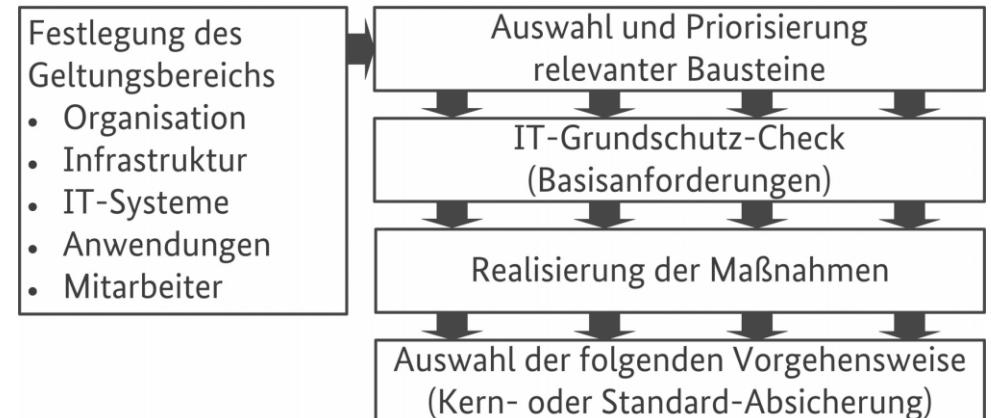


Abb.: BSI-Standard 200-2

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz – Methodik
- Exkurse:
 - Sicherheitskonzeption, IT-Sicherheitskonzept
 - **Kern-Absicherung:** Sorgfältige Absicherung der wichtigsten Assets
 - Weitere Schritte nötig:
 - Standard-Absicherung

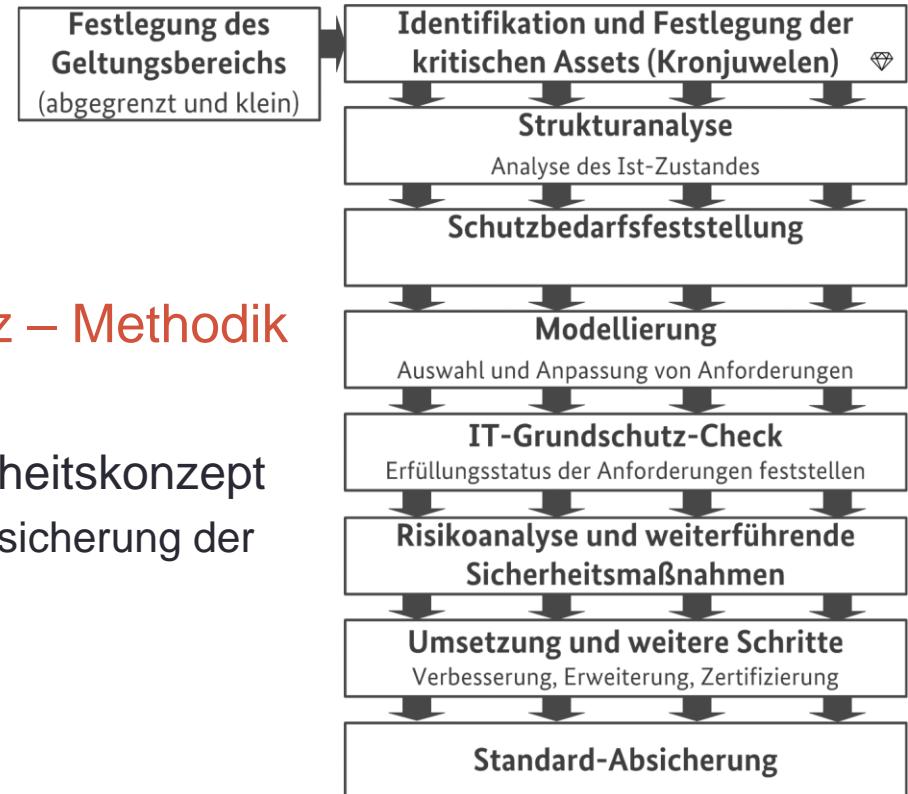


Abb.: BSI-Standard 200-2

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Sicherheitskonzept erstellen
 - Variante Standard-Absicherung
 - Vom BSI bevorzugt, „pragmatisch und effektiv“
 - Letzter Schritt auch der übrigen Varianten
 - Ist de facto komplex und aufwändig

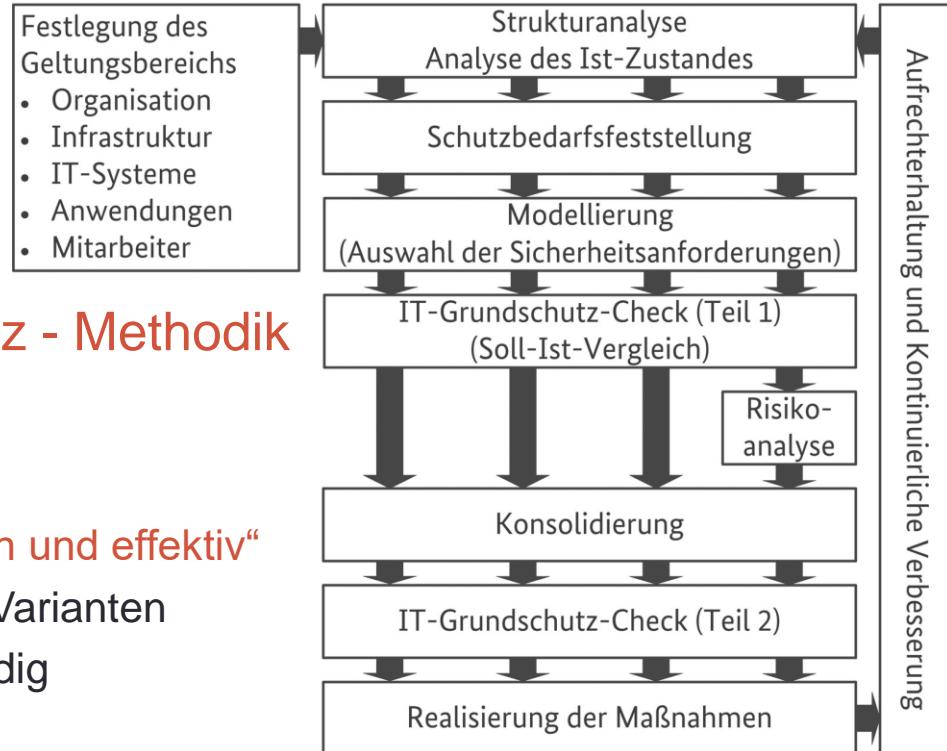


Abb.: BSI-Standard 200-2

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Sicherheitskonzept erstellen
 - Standard-Absicherung 1
 - Festgelegten Geltungsbereich übernehmen (aus Initiierung des Sicherheitsprozesses)
 - Ganzes Unternehmen oder Teilbereich
 - Im Grundschutz bezeichnet als **Informationsverbund**

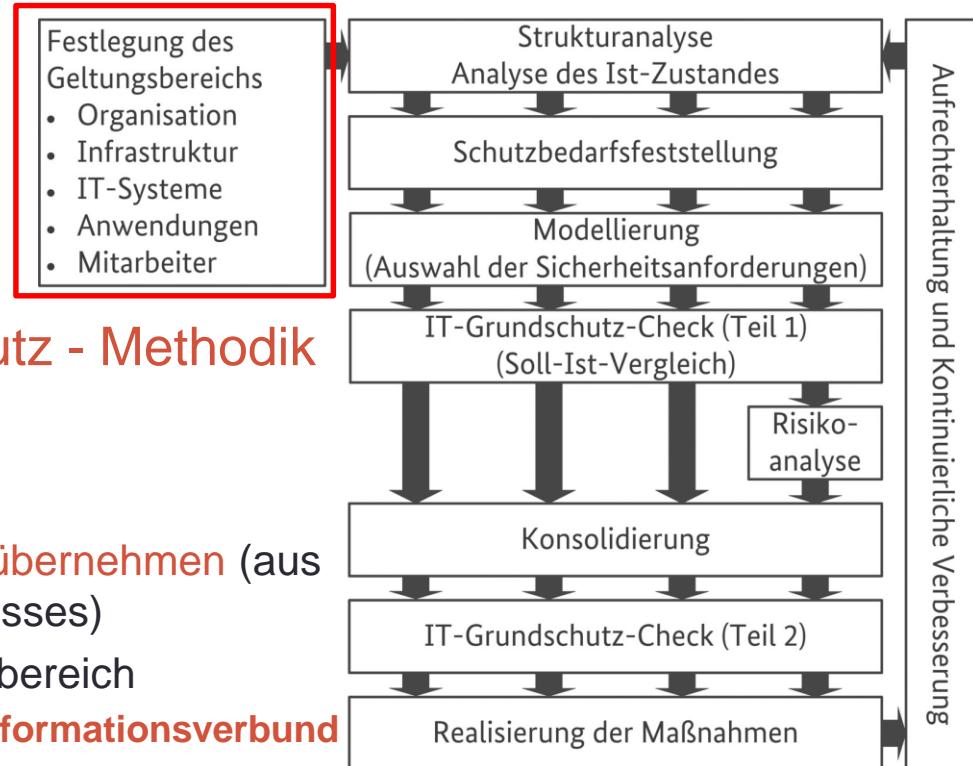


Abb.: BSI-Standard 200-2

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Sicherheitskonzept erstellen
 - Standard-Absicherung 2
 - Struktur analysieren
 - Geschäftsprozesse, Anwendungen und Informationen erfassen **Tabelle**
 - Netzplan erstellen, inklusive interner und externer Kommunikationsverbindungen **Grafik**
 - IT-Systeme erfassen, ggf. alle weiteren sicherheitsrelevanten Systeme (IoT-Geräte...) **Tabelle**
 - Räume und Gebäude erfassen, ggf. auch Produktionsstätten sofern IT-gesteuert **Tabelle**

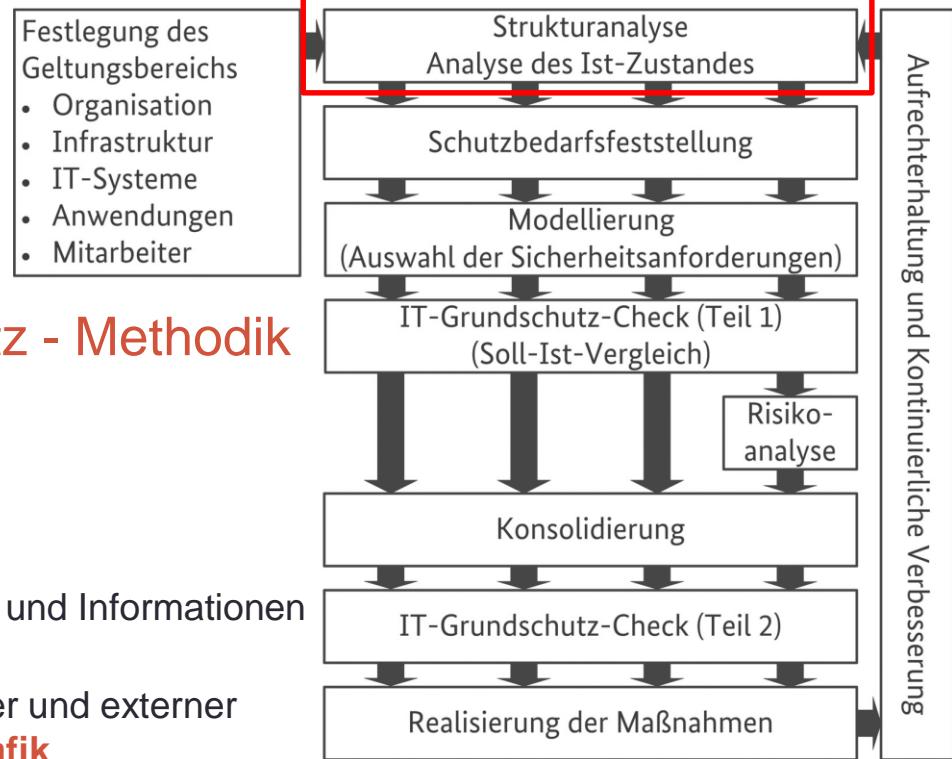


Abb.: BSI-Standard 200-2

IT-Sicherheit

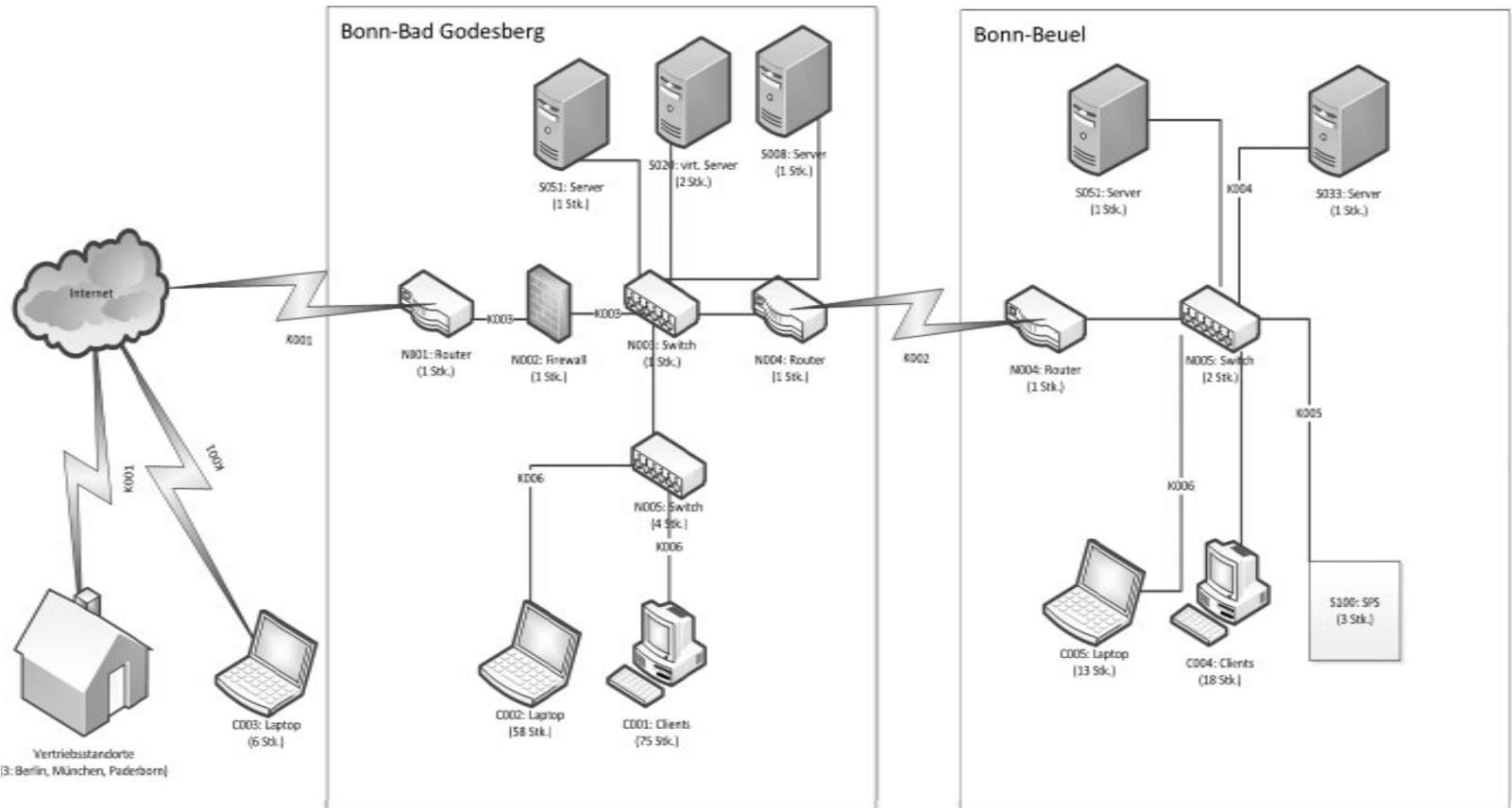


Abb.: BSI-Standard 200-2

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Sicherheitskonzept erstellen
 - Standard-Absicherung 3
 - Schutzbedarf feststellen 1
 - Schutzbedarfskategorien definieren
 - Schutzbedarf abhängig von Konsequenzen eines Ausfalls oder Schadens

Schutzbedarfskategorien	
„normal“	Die Schadensauswirkungen sind begrenzt und überschaubar.
„hoch“	Die Schadensauswirkungen können beträchtlich sein.
„sehr hoch“	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle: BSI-Standard 200-2

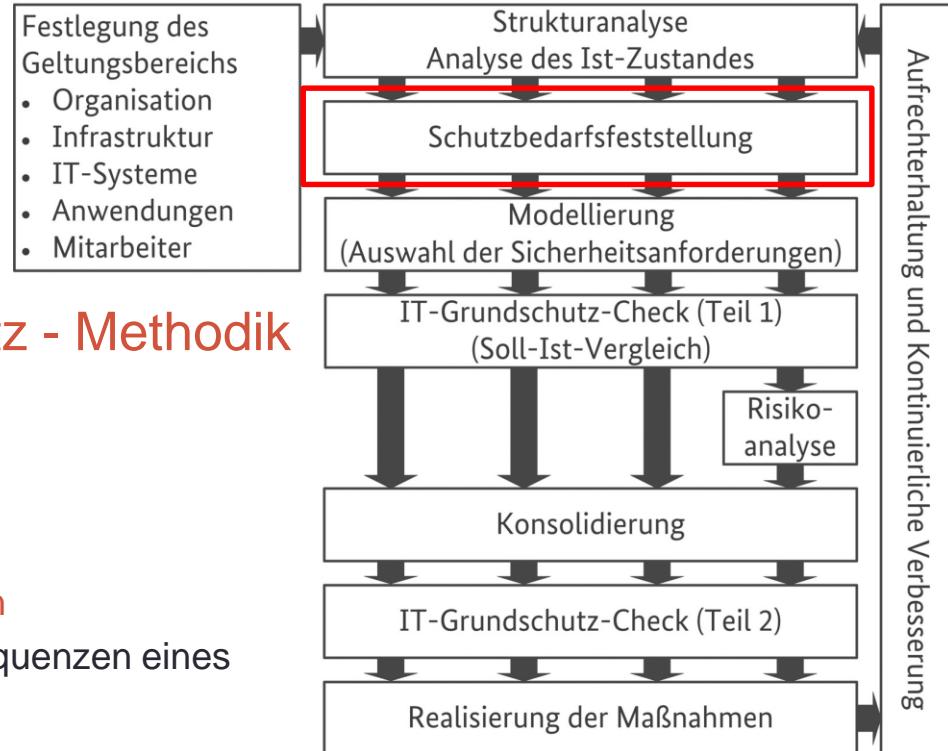


Abb.: BSI-Standard 200-2

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Sicherheitskonzept erstellen
 - Standard-Absicherung 3
 - Schutzbedarf feststellen 2
 - Schutzbedarfskategorien Schadensszenarien zuordnen
 - Verstoß gegen Gesetze/Vorschriften/Verträge
 - Beeinträchtigung des informationellen Selbstbestimmungsrechts
 - Beeinträchtigung der persönlichen Unversehrtheit
 - Beeinträchtigung der Aufgabenerfüllung
 - negative Innen-oder Außenwirkung
 - finanzielle Auswirkungen.
 - Darstellen in Tabellen

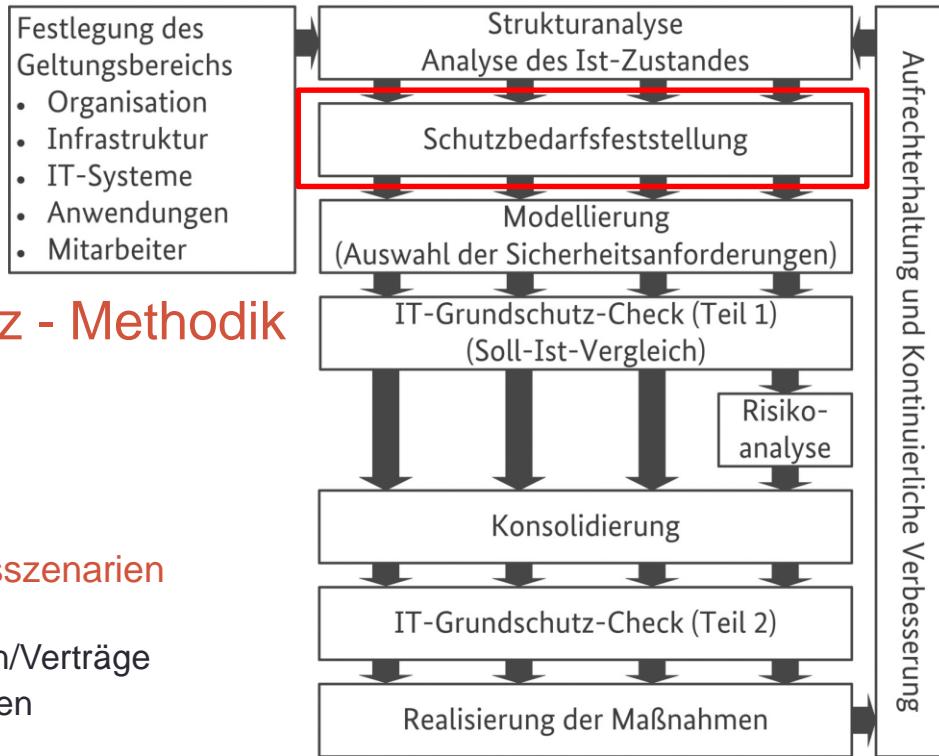


Abb.: BSI-Standard 200-2

IT-Sicherheit

Schutzbedarfskategorie „normal“		Schutzbedarfskategorie „sehr hoch“	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	<ul style="list-style-type: none"> Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen 	1. Verstoß gegen Gesetze/ Vorschriften/Verträge	<ul style="list-style-type: none"> Fundamentaler Verstoß gegen Vorschriften und Gesetze Vertragsverletzungen, deren Haftungsschäden ruinös sind
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	<ul style="list-style-type: none"> Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann. 	2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	<ul style="list-style-type: none"> Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
3. Beeinträchtigung der persönlichen Unversehrtheit	<ul style="list-style-type: none"> Eine Beeinträchtigung erscheint nicht möglich. 	3. Beeinträchtigung der persönlichen Unversehrtheit	<ul style="list-style-type: none"> Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. Gefahr für Leib und Leben
4. Beeinträchtigung der Aufgabenerfüllung	<ul style="list-style-type: none"> Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 Stunden. 	4. Beeinträchtigung der Aufgabenerfüllung	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten. 	5. Negative Innen- oder Außenwirkung	<ul style="list-style-type: none"> Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	<ul style="list-style-type: none"> Der finanzielle Schaden bleibt für die Institution tolerabel. 	6. Finanzielle Auswirkungen	<ul style="list-style-type: none"> Der finanzielle Schaden ist für die Institution existenzbedrohend.

Tabellen: BSI-Standard 200-2

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Sicherheitskonzept erstellen
 - Standard-Absicherung 3
 - Schutzbedarf feststellen 3, durchführen für:
 - Geschäftsprozesse und Anwendungen
 - IT-Systeme und –Geräte
 - Infrastruktur (Räume, Gebäude)
 - Kommunikationsverbindungen
 - Darstellung wieder in Tabellenform
 - Besonderheiten bei Virtualisierung beachten
 - Kumulation und Verteilung

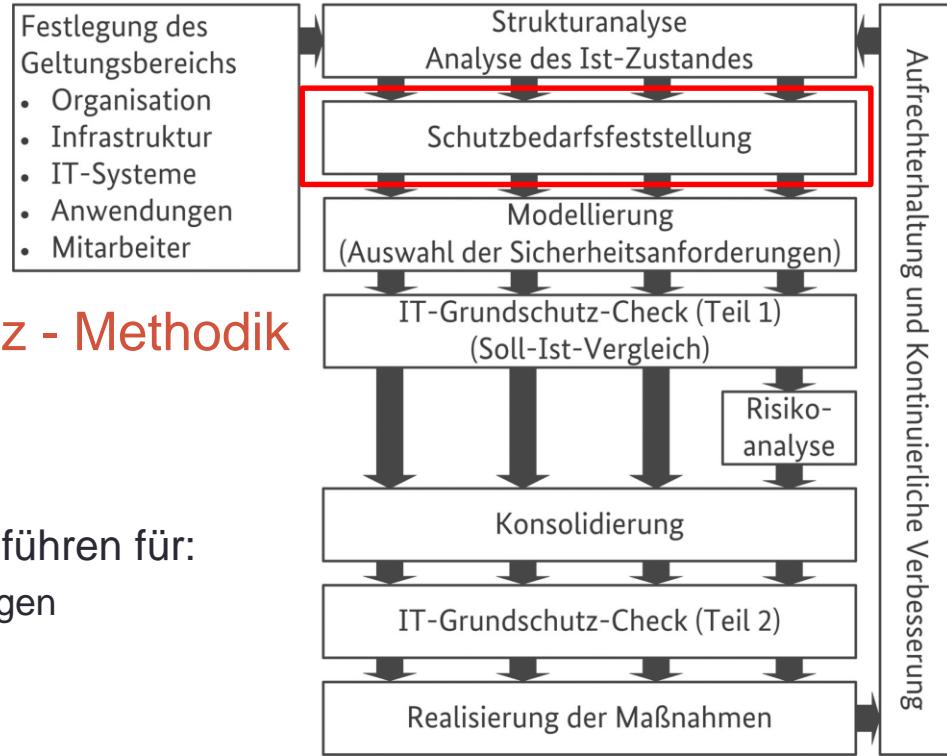


Abb.: BSI-Standard 200-2

IT-Sicherheit

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH								
Bezeichnung	Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	Plattform / Baustein	Vertraulichkeit	Begründung für die Vertraulichkeit	Integrität	Begründung für die Integrität	Verfügbarkeit	Begründung für die Verfügbarkeit
N001	Router Internetanbindung	Router und Switches	hoch	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Ersatzgerät liegt auf Lager und kann schnell durch den IT-Betrieb ausgetauscht werden
N002	Firewall Internet-Eingang	Firewall	hoch	Die Konfigurationseigenschaften müssen vertraulich bleiben. Diese regeln den Datenverkehr zwischen dem Internet und der RECPLAST	normal	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Ersatzgerät liegt auf Lager und kann schnell durch den IT-Betrieb ausgetauscht werden
N003	Switch – Verteilung	Router und Switches	normal	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Ersatzgerät liegt auf Lager und kann schnell durch den IT-Betrieb ausgetauscht werden
N004	Router Bonn BG – Beuel	Router und Switches	normal	Die Konfigurationseigenschaften müssen vertraulich bleiben. Diese regeln den Datenverkehr zwischen den Standorten der RECPLAST	normal	Zutritt, Zugang und Zugriff nur für autorisierte Personen möglich	normal	Ersatzgerät liegt auf Lager und kann schnell durch den IT-Betrieb ausgetauscht werden

Tabelle: BSI-Standard 200-2

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Sicherheitskonzept erstellen
 - Standard-Absicherung 4
 - Modellierung
 - Auswahl der Bausteine aus dem Grundschutz-Kompendium gemäß Schutzbedarfsfeststellung
 - Aufbau eines Soll – Systems: Was müsste getan werden, um mit den Bausteinen die aus der Schutzbedarfsfeststellung ermittelten Sicherheitsanforderungen zu erhalten?
 - Festlegung einer Umsetzungsreihenfolge

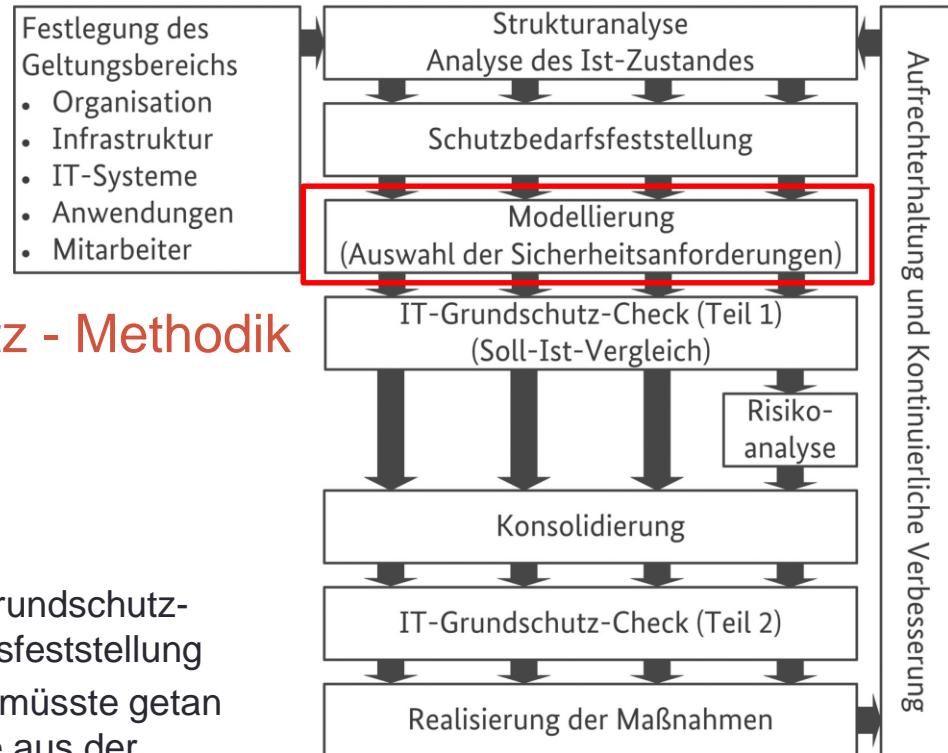


Abb.: BSI-Standard 200-2

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Sicherheitskonzept erstellen
 - Standard-Absicherung 5
 - Grundschutz-Check Teil 1 (Soll-Ist-Vergleich)
 - Checklisten erstellen
 - Umsetzungsstatus der Sicherheitsanforderungen ermitteln/erfragen
 - Stichproben durchführen
 - Ergebnisse dokumentieren und den Beteiligten mitteilen

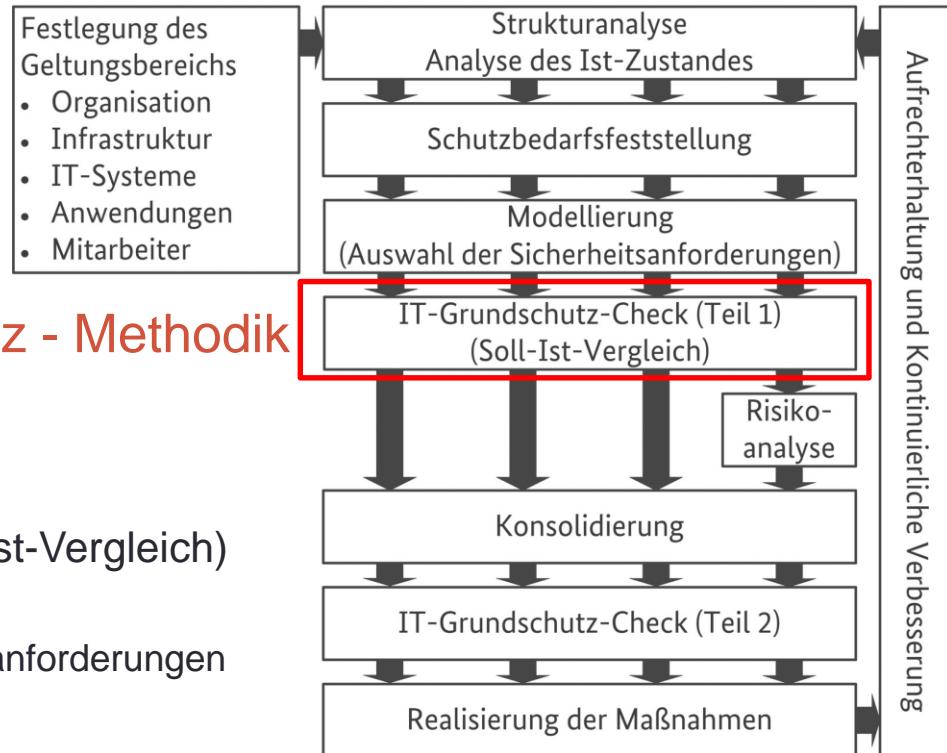


Abb.: BSI-Standard 200-2

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Sicherheitskonzept erstellen
 - Standard-Absicherung 6
 - Risikoanalyse
 - Gefährdungsübersicht erstellen
 - Risiken einstufen
 - Einschätzen
 - Bewerten
 - Risiken behandeln
 - Vermeiden
 - Reduzieren, Transferieren
 - Akzeptieren

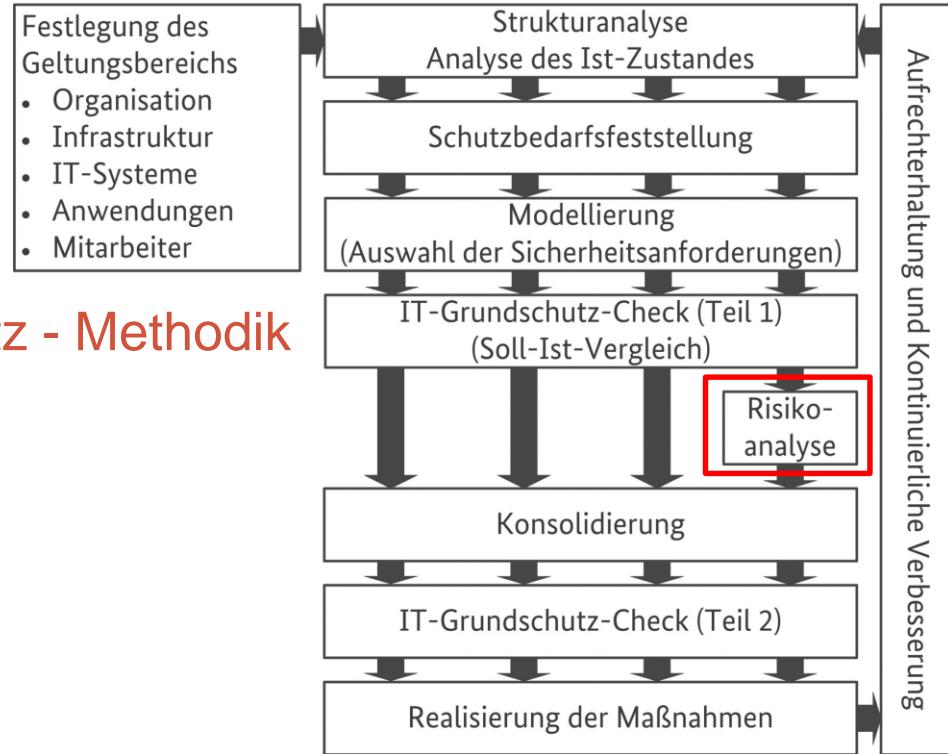


Abb.: BSI-Standard 200-2

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Sicherheitskonzept erstellen
 - Standard-Absicherung 7
 - Konsolidierung
 - Übernahme der Änderungen durch die Risikobehandlung in das Sicherheitskonzept

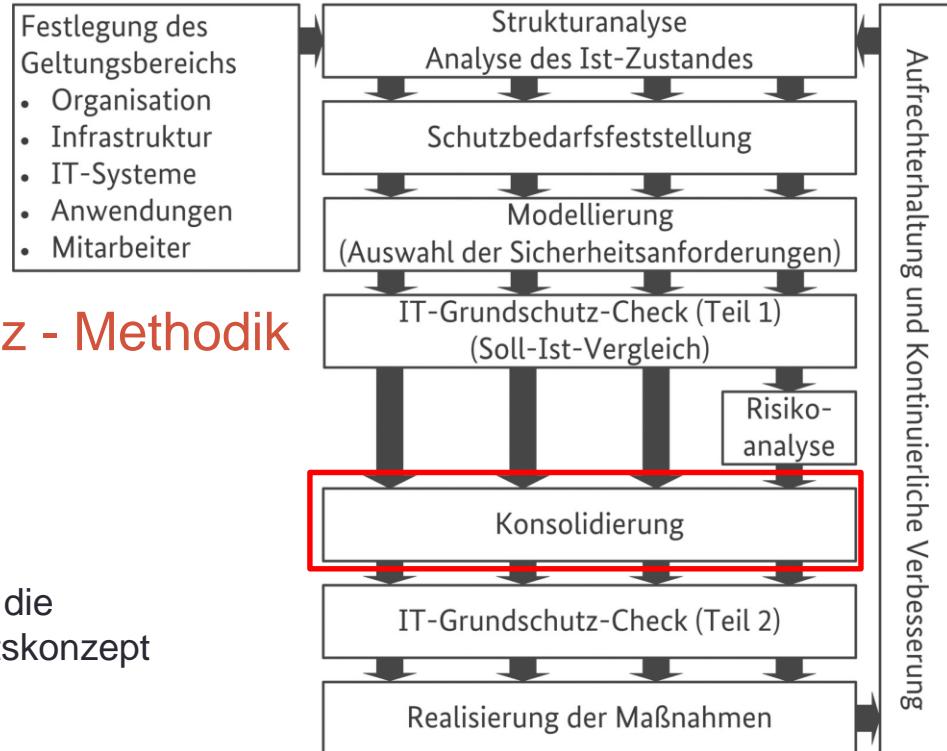


Abb.: BSI-Standard 200-2

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Sicherheitskonzept erstellen
 - Standard-Absicherung 8
 - IT-Grundschutz-Check Teil 2
 - Passt das konsolidierte Sicherheitskonzept jetzt?
 - Sprich: Sind die durch Behandlung der in Teil 1 erkannten Risiken Änderungen ausreichend, um das verbleibende Restrisiko auf ein erträgliches Minimum zu reduzieren?
 - **Ja:** nächster Schritt
 - **Nein:** Wiederholung Risikobehandlung bis **Ja**

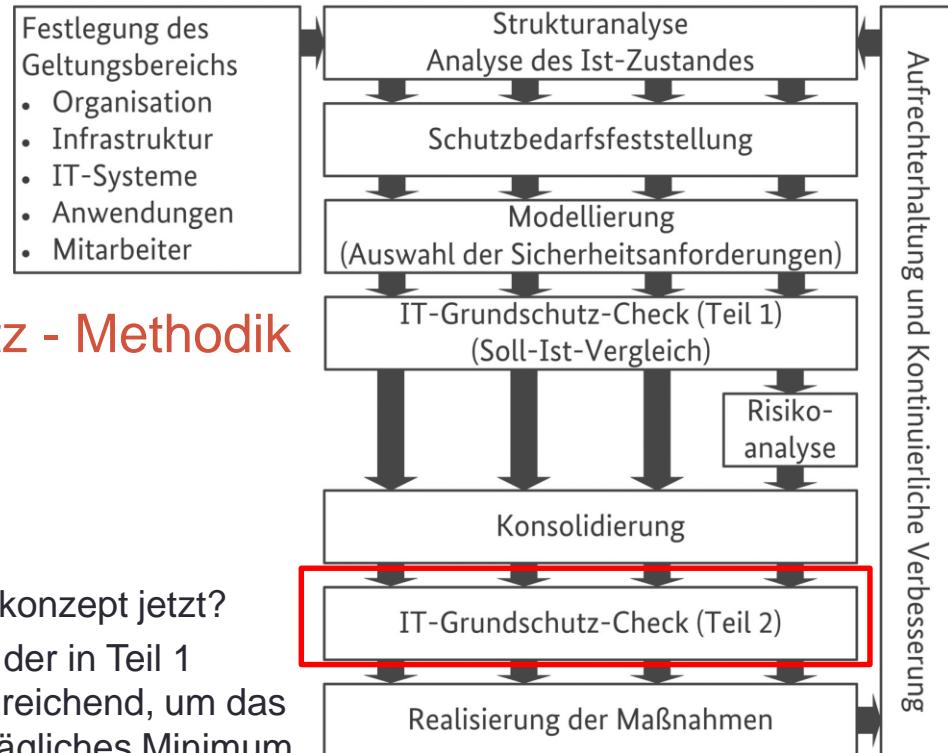


Abb.: BSI-Standard 200-2

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Sicherheitskonzept erstellen
 - Standard-Absicherung 9
 - Maßnahmen realisieren
 - Vorgehen siehe ISMS aufbauen - konkrete Aufgaben 5
 - Kosten- und Aufwand abschätzen
 - Umsetzungsreihenfolge festlegen
 - Mitarbeiter sensibilisieren und schulen
 - Maßnahmen durchführen

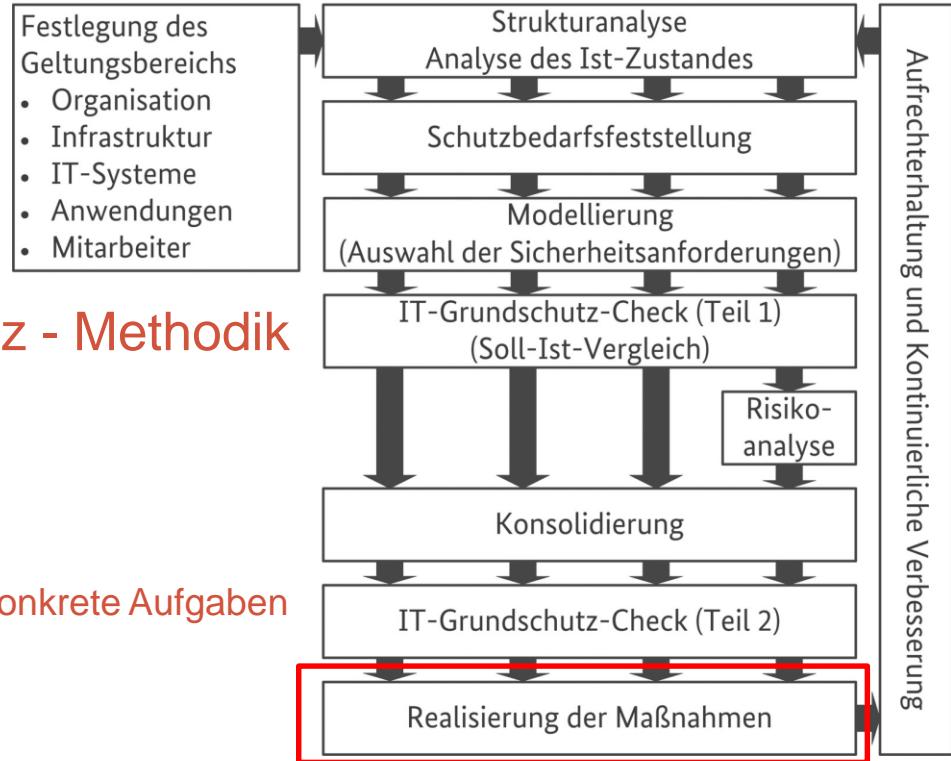


Abb.: BSI-Standard 200-2

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz - Methodik
- Sicherheitskonzept erstellen
 - Standard-Absicherung 9
 - Maßnahmen realisieren
 - Vorgehen siehe ISMS aufbauen - konkrete Aufgaben 5
 - Kosten- und Aufwand abschätzen
 - Umsetzungsreihenfolge festlegen
 - Mitarbeiter sensibilisieren und schulen
 - Maßnahmen durchführen

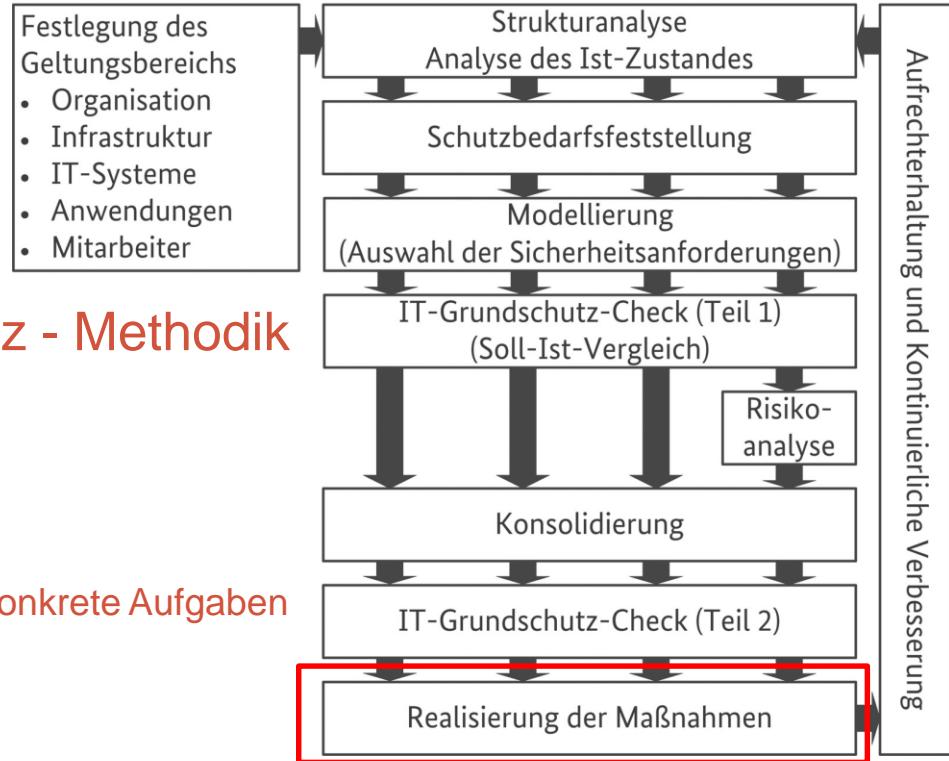


Abb.: BSI-Standard 200-2

IT-Sicherheit

- IT-Sicherheit – BSI Grundschutz
- Quasi-Standard zu Schutzmaßnahmen für Daten und Informationen
 - Grundgedanken und Modell
 - Begriffe
 - Komponenten
 - Methodik
 - Anwendungsbeispiele
 - Firewall
 - Datensicherung



Grafiken: Bundesamt für Sicherheit in der Informationstechnik



IT-Sicherheit

- IT-Sicherheit – Firewall
 - Grundlagen und Begriffe
 - Firewall-Typen und Einsatzformen
 - Firewalls – Empfehlungen nach BSI-Grundschutz

IT-Sicherheit

- Firewall – Grundlagen und Begriffe
 - Definition(en) 1: Cisco

„Eine Firewall ist eine Netzwerksicherheitsvorrichtung, die eingehenden und ausgehenden Netzwerkverkehr überwacht und auf Grundlage einer Reihe von definierten Sicherheitsregeln entscheidet, ob bestimmter Datenverkehr zugelassen oder blockiert wird.“

Eine Firewall basiert entweder auf Hardware, auf Software oder auf einer Kombination aus beidem.“

https://www.cisco.com/c/de_de/products/security/firewalls/what-is-a-firewall.html

IT-Sicherheit

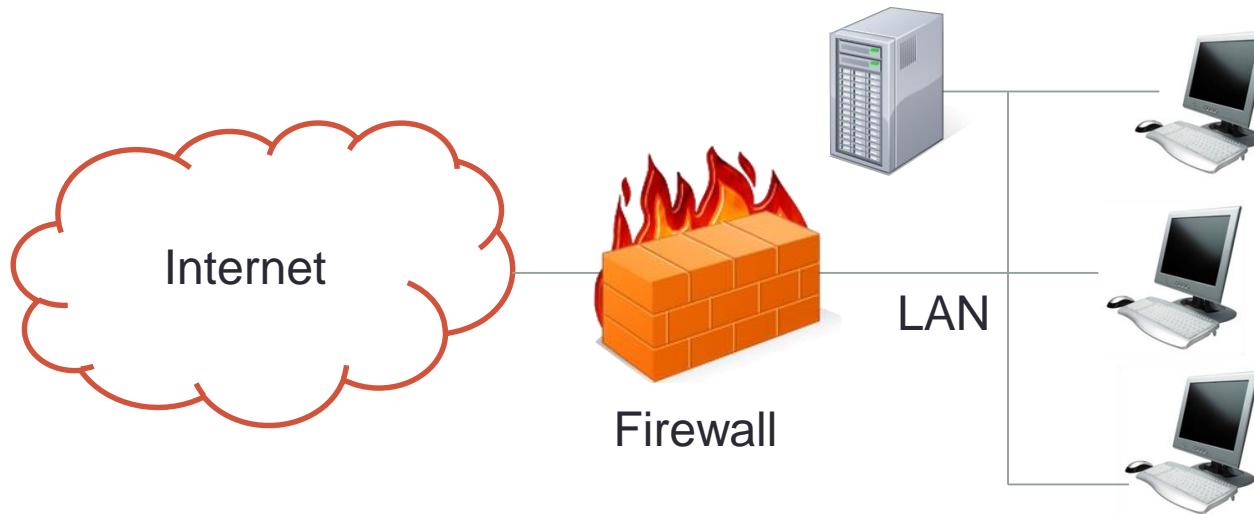
- Firewall – Grundlagen und Begriffe
 - Definition(en) 2: BSI

„Eine Firewall ist ein System aus soft- und hardwaretechnischen Komponenten, das dazu eingesetzt wird, IP-basierte Datennetze sicher zu koppeln. Dazu wird mithilfe einer Firewall-Struktur die technisch mögliche auf die in einer Sicherheitsrichtlinie als sicher definierte Kommunikation eingeschränkt. Sicherheit bedeutet hierbei, dass ausschließlich die erwünschten Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen werden.“

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_3_2_Firewall.html

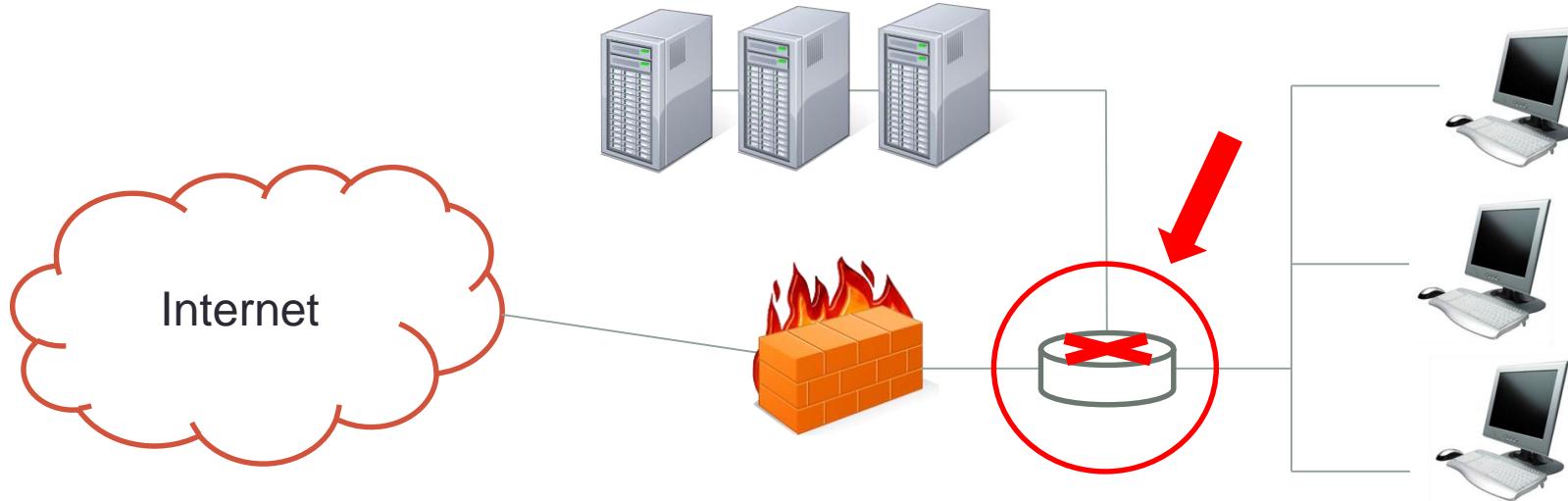
IT-Sicherheit

- Firewall – Grundlagen und Begriffe
 - Positionen von Firewalls
 - Klassisch und obligatorisch: Am Übergabepunkt zwischen LAN und Internet



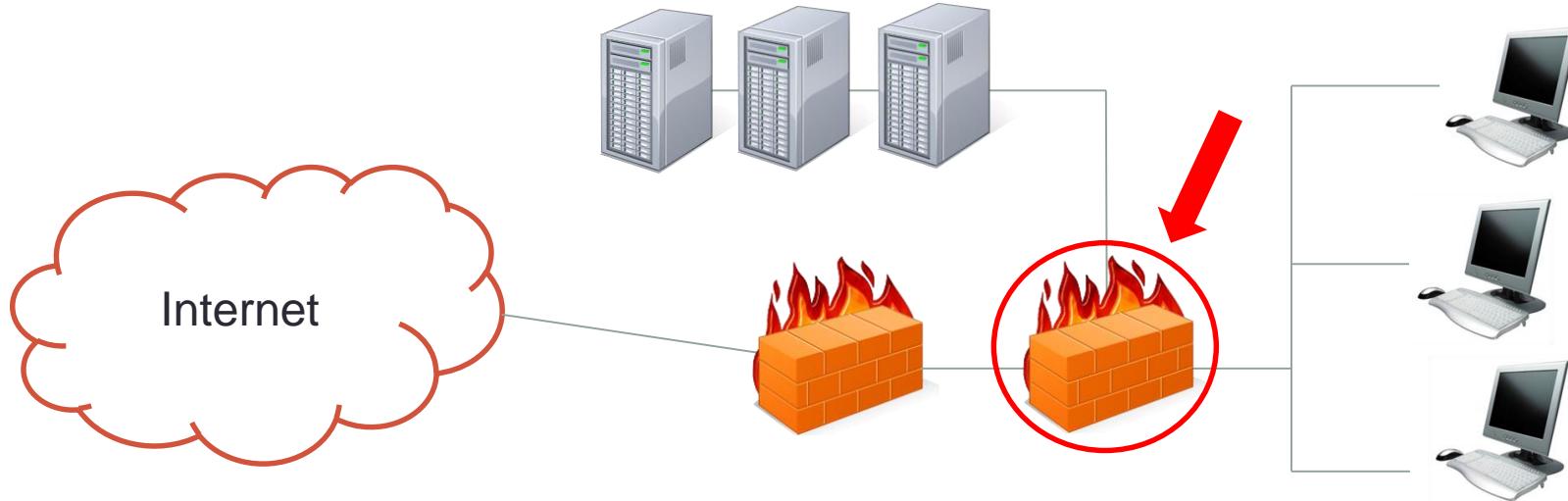
IT-Sicherheit

- Firewall – Grundlagen und Begriffe
 - Positionen von Firewalls
 - Bei höheren Sicherheitsanforderungen: Auch an relevanten Netzwerkknoten



IT-Sicherheit

- Firewall – Grundlagen und Begriffe
 - Positionen von Firewalls
 - Bei höheren Sicherheitsanforderungen: Auch an relevanten Netzwerkknoten

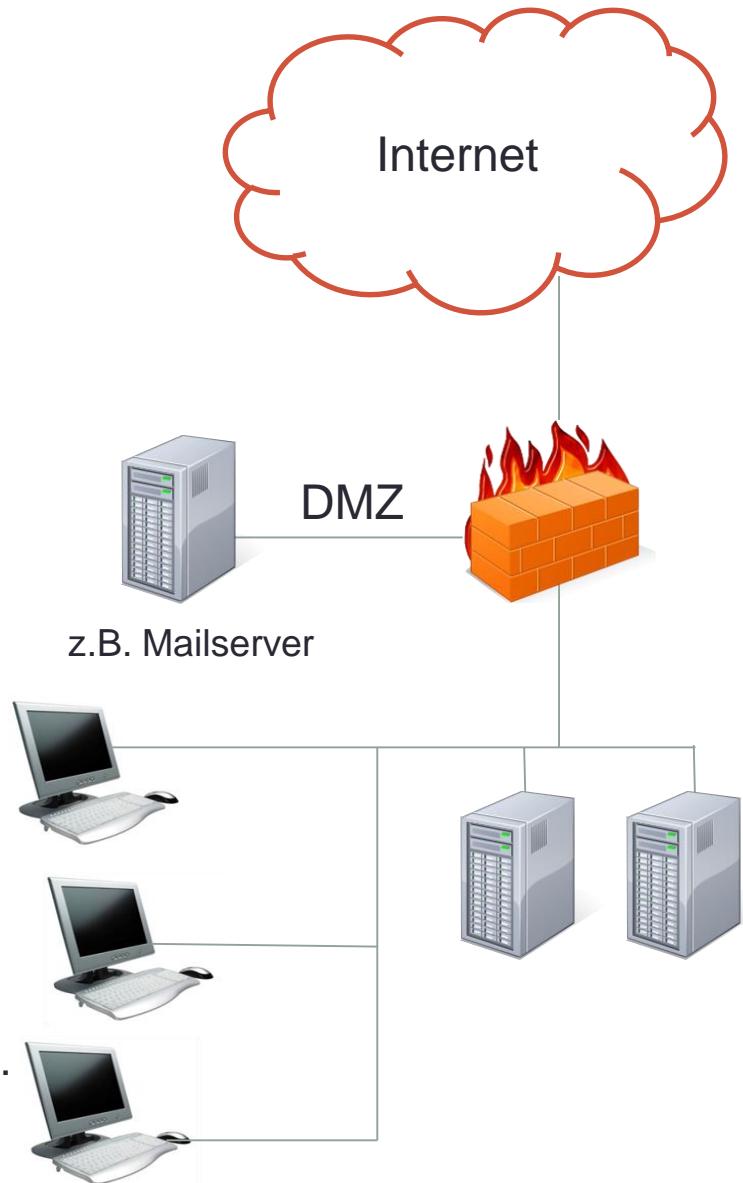


IT-Sicherheit

- Firewall – Grundlagen und Begriffe
 - Positionen von Firewalls
 - Bei höheren Sicherheitsanforderungen und veröffentlichten Diensten:
 - Demilitarisierte Zone **DMZ**, engl. auch **Perimeter Network**
 - Durch Firewall(s) getrenntes Netzwerk zwischen dem LAN und dem Internet.
 - Veröffentlichte Server stehen in der DMZ
 - Für die DMZ gelten verschiedene Sicherheitsregeln zum Internet und zum LAN
 - **Ratio:** Wenn veröffentlichte Server angegriffen und kompromittiert werden, bleibt das LAN trotzdem geschützt.

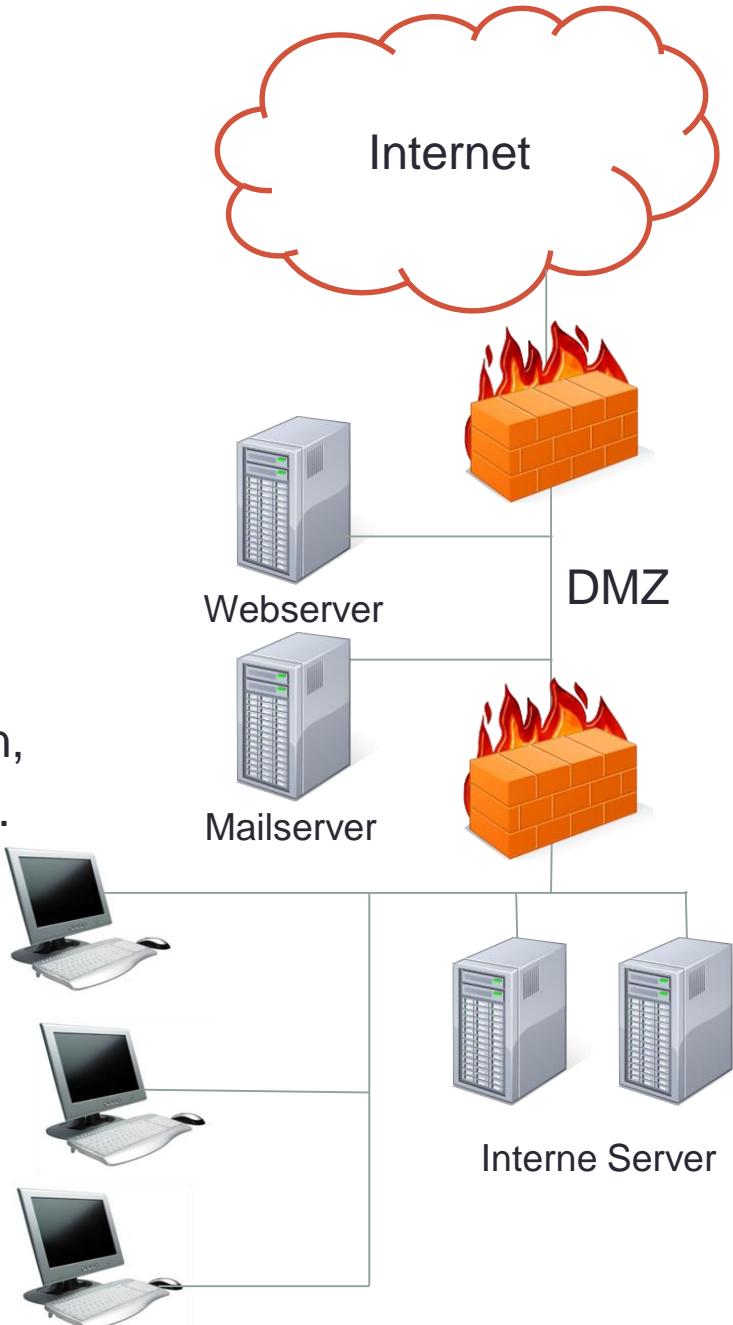
IT-Sicherheit

- Firewall – Grundlagen und Begriffe
 - Positionen von Firewalls – DMZ „light“
 - Eine Firewall mit mehreren Netzwerkschnittstellen
 - **Pro:**
 - Kostengünstig
 - Einfach einzurichten
 - **Contra:**
 - Nur etwas mehr Sicherheit als ohne DMZ.
Ist die Firewall kompromittiert, ist wahrscheinlich auch das LAN betroffen



IT-Sicherheit

- Firewall – Grundlagen und Begriffe
 - Positionen von Firewalls – **echte DMZ**
 - Zwei Firewalls mit Netzwerk dazwischen,
 - Unterschiedliche Regeln auf beiden FW.
 - **Pro:**
 - Höchste Sicherheit, besonders mit verschiedenen Firewall-Produkten
 - **Contra:**
 - Teuer, besonders mit Hochverfügbarkeit
 - Komplexere Konfiguration und Wartung



IT-Sicherheit

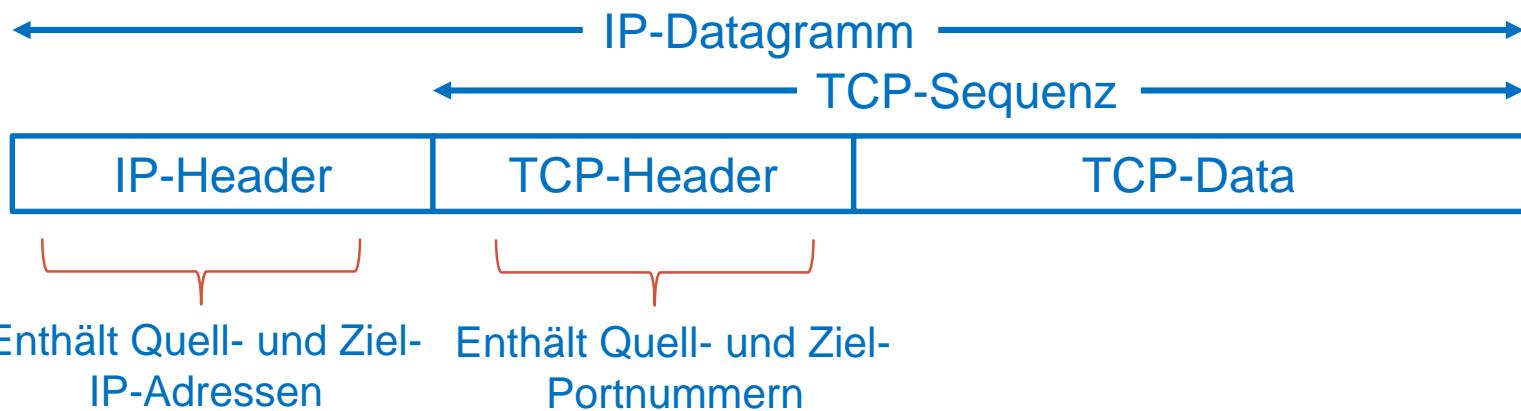
- Firewall – Grundlagen und Begriffe
 - Positionen von Firewalls
 - In Windows Netzen empfohlen: Auf Clients und Servern Windows-Firewall aktivieren. Blockiert unerwünschte Kommunikation vom Netz aus zu jedem System.
 - Warum?
 - Immer häufiger kommt ein Angriff aus dem LAN. Dabei hat die Firewall am Übergang zum Internet keine Schutzfunktion

IT-Sicherheit

- Firewall – Firewall-Typen
- Nach Schutzfunktionen und Funktionsumfang
 - Paketfilter
 - Stateful Inspection Firewall
 - Application Level Firewall
 - Next Generation Firewall
 - Unified Threat Management Firewall

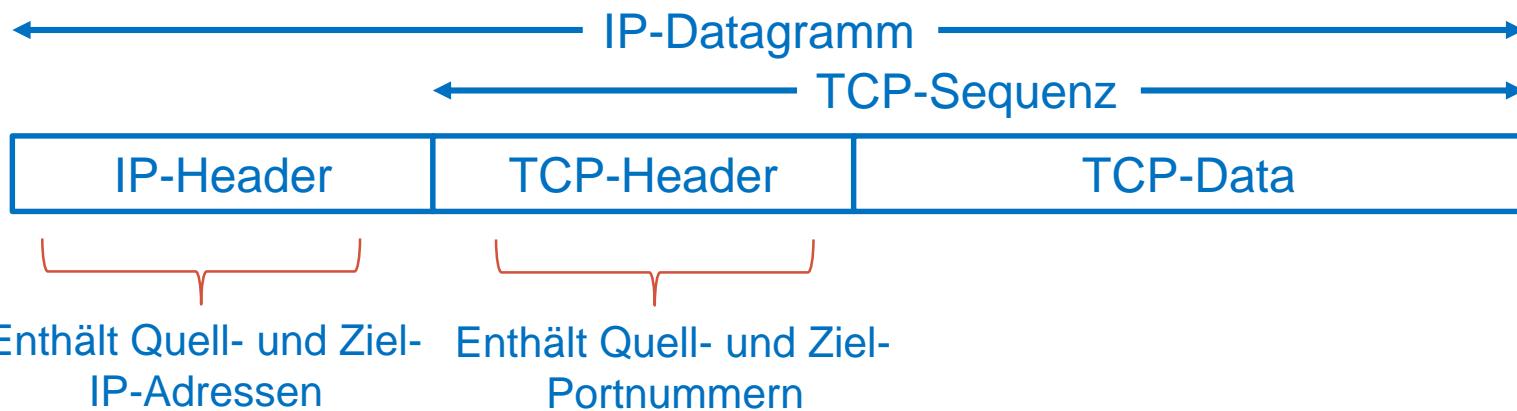
IT-Sicherheit

- Firewall – Firewall-Typen
- Nach Schutzfunktion und Funktionsumfang: Paketfilter
 - TCP/IP und UDP/IP Datenpakete werden auf Basis von IP-Adressen und TCP- oder UDP-Portnummern weitergeleitet oder verworfen



IT-Sicherheit

- Firewall – Firewall-Typen
- Nach Schutzfunktion und Funktionsumfang: Paketfilter
 - IP-Adressen identifizieren Absender und Empfänger
 - Portnummern identifizieren angefragte Services/Protokolle



IT-Sicherheit

- **Firewall – Firewall-Typen**
- Nach Schutzfunktion und Funktionsumfang: Paketfilter
 - TCP/IP und UDP/IP Datenpakete werden aufgrund definierter Regeln anhand IP-Adressen und Portnummern weitergeleitet oder verworfen, OSI-Schichten 3 und 4
 - Optionale Zusatzfunktion: **Network Address Translation**, IP-Adressen des Absenders werden bei Bedarf durch IP-Adressen der Paketfilter-Firewall ersetzt, => Firewall wird zum **Proxy**.
 - Paketfilter und NAT sind Grundfunktionen jeder modernen Firewall, auch fritzbox und Co.

IT-Sicherheit

- Firewall – Firewall-Typen
- Nach Schutzfunktion und Funktionsumfang: Paketfilter
 - Schützen auf Basis von Absendern, Empfängern und Services
- Pro:
 - Einfach per Software zu realisieren (vgl. Windows Firewall)
- Contra:
 - Heute nur noch rudimentäre Sicherheit
 - Keine Analyse der Inhalte
 - IP-Spoofing und Anfragen über „falsche“ Protokolle umgehen Paketfilter

IT-Sicherheit

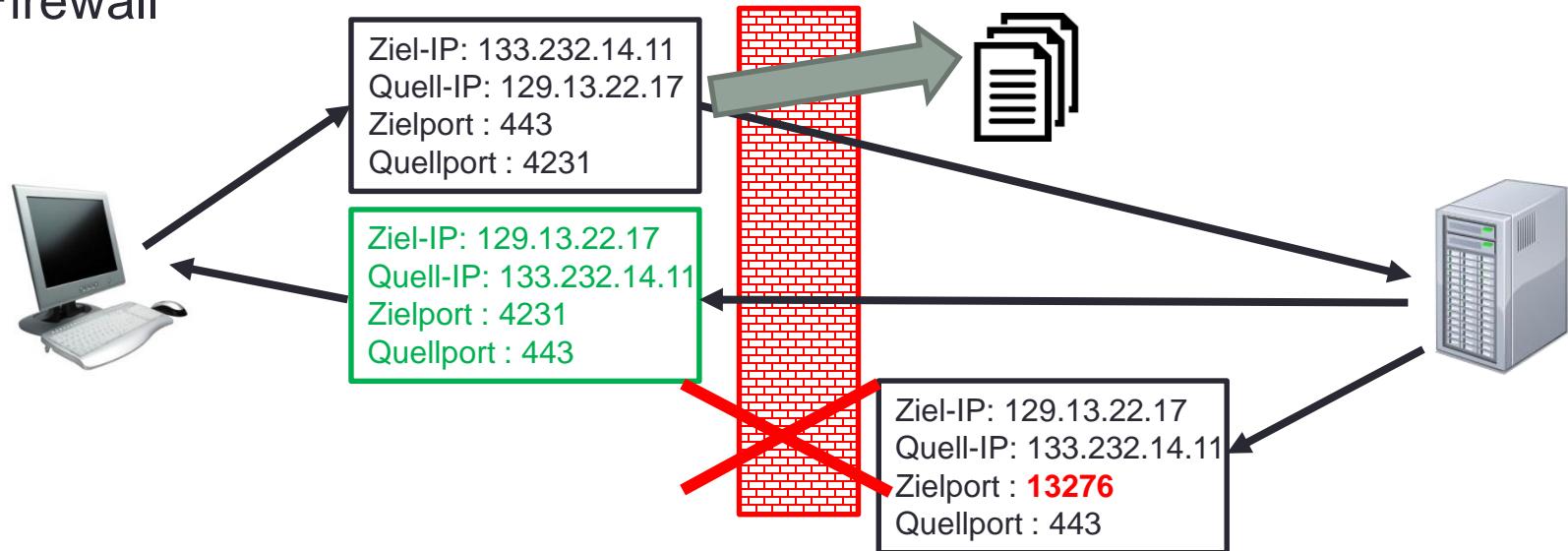
- Firewall – Firewall-Typen
- Nach Schutzfunktionen und Funktionsumfang: **Stateful Inspection Firewall**
 - Paketfilter mit Analyse des Verbindungsstatus und Protokollkommandos
 - **Verbindung** ist eindeutig beschrieben durch vier Parameter. Diese bleiben bei „normalen“ TCP- oder UDP-Verbindungen bis zum Abschluss gleich.
 - Ziel-IP-Adresse
 - Quell-IP-Adresse
 - Zielport
 - Quellport

IT-Sicherheit

- Firewall – Firewall-Typen
- Nach Schutzfunktionen und Funktionsumfang: Stateful Inspection Firewall
 - Stateful Inspection Firewall schreibt alle aktiven Verbindungen einen Status-Cache
 - Alle weiteren Pakete derselben Verbindung werden mit Eintrag im Cache verglichen. Abweichende Ports sind unzulässig und werden verworfen:

IT-Sicherheit

- Firewall – Firewall-Typen
- Nach Schutzfunktionen und Funktionsumfang: Stateful Inspection Firewall



IT-Sicherheit

- Firewall – Firewall-Typen
- Nach Schutzfunktionen und Funktionsumfang: Stateful Inspection Firewall
- Pro:
 - Kein Senden von Daten, wenn keine Verbindung (mehr) besteht
 - => Schutz gegen bestimmte Angriffsversuche
 - Optional Funktionen:
 - Kontrolle von Standardbefehlen in bekannten Protokollen wie TELNET, FTP usw.
 - Pakete mit unzulässigen Befehle werden verworfen

IT-Sicherheit

- Firewall – Firewall-Typen
- Nach Schutzfunktionen und Funktionsumfang: Stateful Inspection Firewall
- Contra:
 - Keine Inhaltliche Prüfung, z.B. auf korrekte angeforderte oder übergebene URLs
 - Heute nur noch wenig mehr Sicherheit als reine Paketfilter.

IT-Sicherheit

- Firewall – Firewall-Typen
- Nach Schutzfunktionen und Funktionsumfang – Application Level Firewall
 - Führt Deep Packet Inspection durch, auf den Schichten 5 und 7 des OSI-Modells
 - Analysiert Inhalte, Kommandos usw. im Datenstrom und vergleicht diese mit vordefinierten Regeln.
 - Verwirft Datenpakete, die nicht ausschließlich und genau die zulässigen Inhalte und Kommandos enthalten

IT-Sicherheit

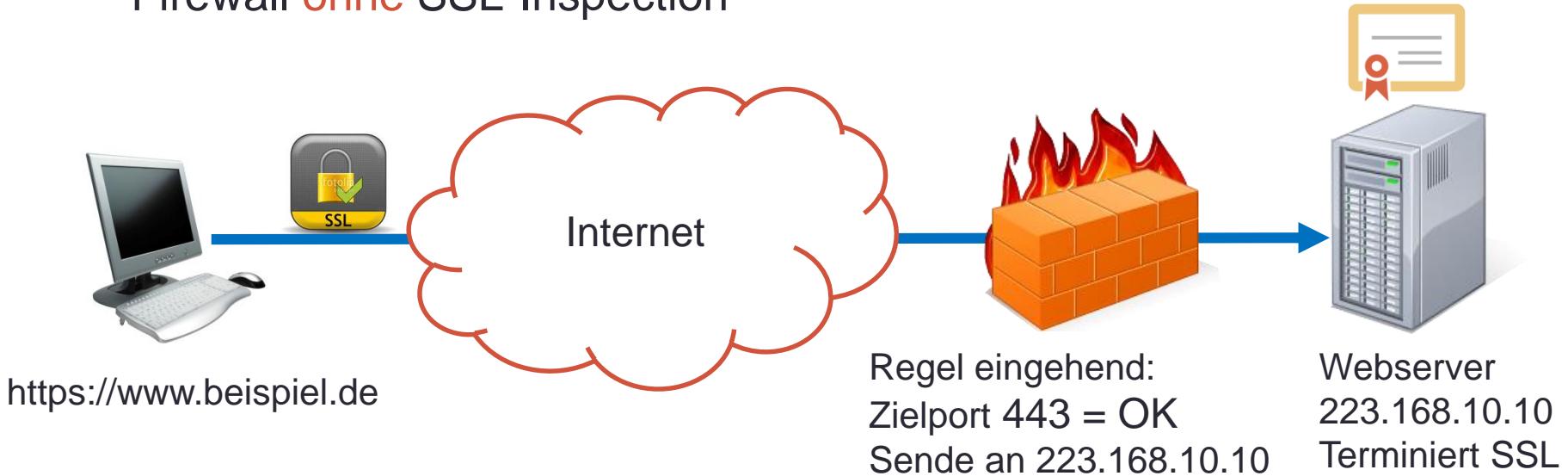
- Firewall – Firewall-Typen
- Nach Schutzfunktionen und Funktionsumfang – Application Level Firewall
 - Führt Deep Packet Inspection durch, auf den Schichten 5-7 des OSI-Modells
 - Analysiert Inhalte, Kommandos usw. im Datenpaket und vergleicht diese mit vordefinierten Regeln.
 - Verwirft Datenpakete, die nicht ausschließlich und genau die zulässigen Inhalte und Kommandos enthalten
- ... und was ist mit verschlüsselten Datenpaketen?

IT-Sicherheit

- Firewall – Firewall-Typen
- Nach Schutzfunktionen und Funktionsumfang – Application Level Firewall
 - Ohne besondere Konfiguration könnte auch eine Application Level Firewall verschlüsselte Datenpakete nicht prüfen
 - Lösung: **SSL-Inspection**, SSL-Verschlüsselung terminiert an der Firewall und nicht am Server, auf den zugegriffen wird
 - Firewall entschlüsselt, prüft Inhalte und leitet zulässige Anfragen (ggf. unverschlüsselt) an Webserver (in der DMZ) weiter.
 - Firewall verschlüsselt Antworten an Client

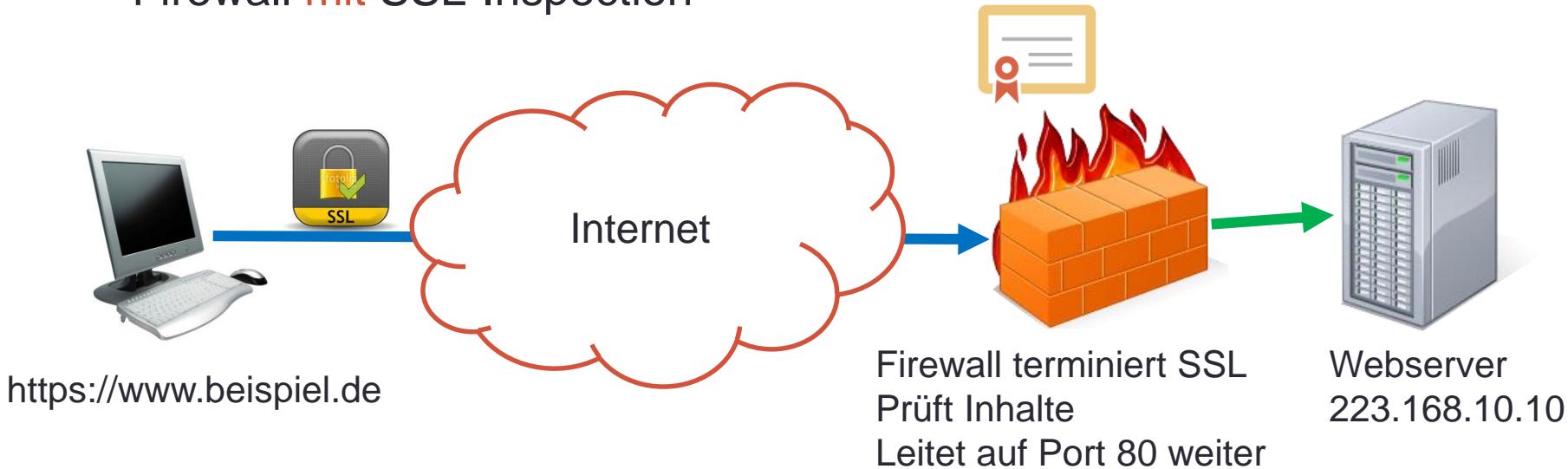
IT-Sicherheit

- Firewall – Firewall-Typen
- Nach Schutzfunktionen und Funktionsumfang – Application Level Firewall **ohne** SSL-Inspection



IT-Sicherheit

- Firewall – Firewall-Typen
- Nach Schutzfunktionen und Funktionsumfang – Application Level Firewall mit SSL-Inspection



IT-Sicherheit

- Firewall – Firewall-Typen
- Nach Schutzfunktionen und Funktionsumfang – Next Generation Firewall und Unified Threat Management Firewalls
 - Next Generation Firewalls ergänzen die Application Level Prüfung um Angriffserkennung (Intrusion Detection Systems) und Angriffsschutz (Intrusion Protection Systems)
 - IDS erkennt Angriffe anhand von Mustern, z.B. eine DDOS-Attacke anhand vieler synchroner Anfragen auf einen Host oder Aktivitäten von Schadsoftware durch Kontaktaufnahme mit IP-Adressen von bekannten Bot-Netz-Controllern. Das IDS warnt z.B. Admins vor erkannten Angriffen.
 - Das IPS unterbindet ggf. erkannte Angriffe auch

IT-Sicherheit

- Firewall – Firewall-Typen
- Nach Schutzfunktionen und Funktionsumfang – Next Generation Firewall und Unified Threat Management Firewalls
 - Unified Threat Management-Systeme fügen Firewall und IDS/IPS noch Antiviren- und Antispam-Funktionen hinzu
 - Diese Funktionen können mit Anti-Malware-Lösungen für Clients und Server zusammenarbeiten
 - Hersteller versprechen damit nahezu vollständigen Netzwerkschutz
- Gegenargument: Höhere Sicherheit durch verschiedene Systeme

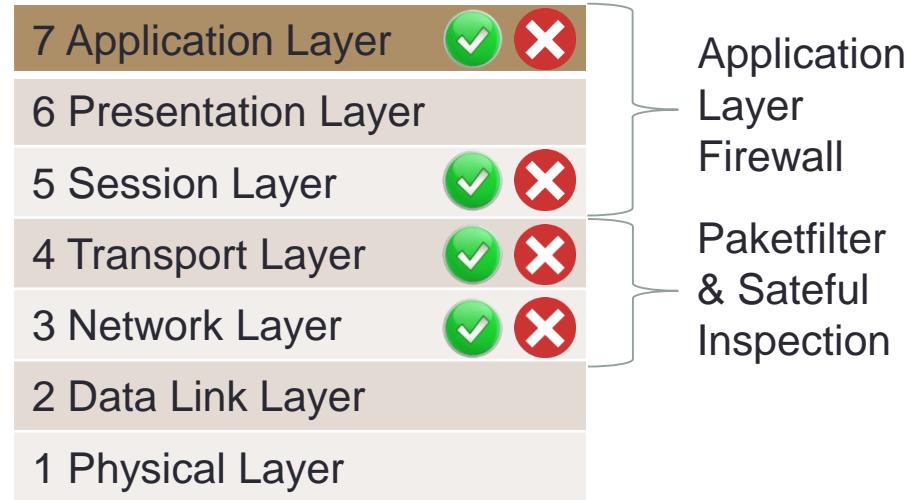
IT-Sicherheit

- Firewall – Empfehlungen des BSI
- Baustein NET 3.2 Firewall legt v.a. folgendes fest:
 - Firewall-Filterregeln festlegen und Paketfilter konfigurieren **bevor die Firewall eingesetzt wird**
 - Deny-All-Regel aktiviert, nur unbedingt benötigte Dienste sind erlaubt
 - Administration nur durch festgelegten Personenkreis und über separate Schnittstellen, insbesondere nicht vom Internet aus
 - Regelung für Sicherheitsvorfälle treffen
 - SSL-Inspection, mindestens temporär
 - Kaskadierte Firewalls mit **DMZ** und ggf. **Hochverfügbarkeit** einsetzen

IT-Sicherheit

- **Firewall – Zusammenfassung**

- Firewalls filtern unerwünschte Kommunikationsversuche und schützen so Netzwerke und Systeme
- Je nach Typ arbeiten sie als Paketfilter nur auf OSI-Schichten 3 und 4 oder als Application Layer Firewalls zusätzlich auf Schicht 5 und 7
- Jeder Zugang vom LAN zum Internet benötigt eine Firewall, die nur erwünschte Kommunikation passieren lässt
- Bei erhöhten Sicherheitsanforderungen ist eine DMZ einzusetzen
- Firewalls sollten auch SSL-verschlüsselte Kommunikation untersuchen



IT-Sicherheit

Fragen zum Selbststudium

- Nennen Sie die Aufgaben eines IT-Sicherheitsbeauftragten. Darf ein ITSB gleichzeitig IT-Leiter oder Datenschutzbeauftragter sein?
- Welche Form Nutzen Sie für die Darstellung der IT-System-Struktur der Organisation im Rahmen der Erstellung eines IT-Sicherheitskonzeptes?
- Welche Aufgabe hat eine Firewall und wo wird sie im Netzwerk (mindestens) platziert?
- Welcher Firewall-Typ wird mindestens benötigt, um den Inhalt übermittelner Datenpakete analysieren zu können?

Quellen: Dieses Skript, BSI-Grundschutz-Kompendium unter

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.html