IT-Sicherheit in der Praxis

Sicherheitsrichtlinie der KBV und Hinweise zur Umsetzung

Stefan Troschke
IT-Service der KV Sachsen-Anhalt

1 **IT Sicherheitsrichtlinie der KBV**

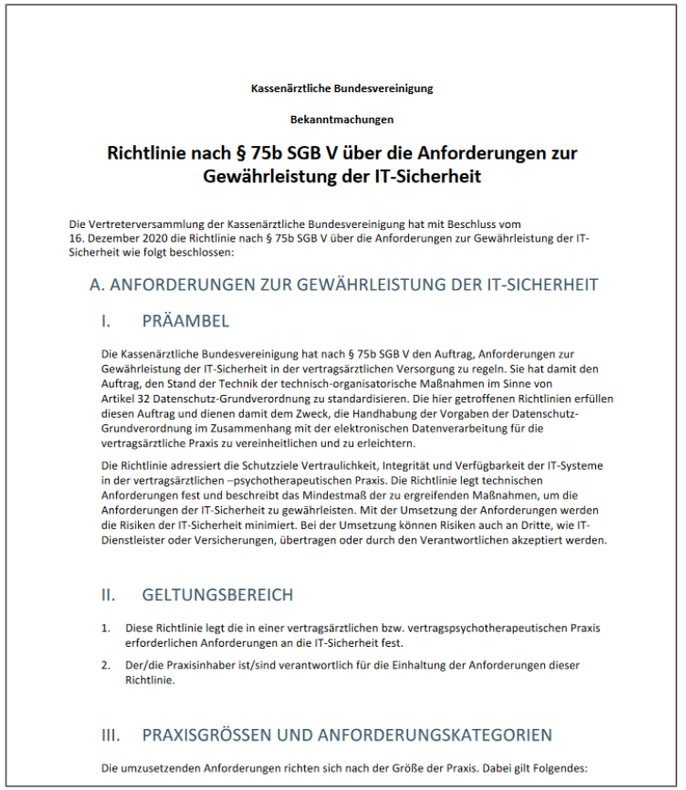
2 Hinweise zur Umsetzung

IT-Sicherheitsrichtline der KBV – Übersicht

Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung - (Artikel 1 des Gesetzes v. 20. Dezember 1988, BGBl. I S. 2477)
§ 75b Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung

(1) Die Kassenärztlichen Bundesvereinigungen legen bis zum 30. Juni 2020 in einer Richtlinie die Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung fest. Die Richtlinie umfasst auch Anforderungen an die sichere Installation und Wartung von Komponenten und Diensten der Telematikinfrastruktur, die in der vertragsärztlichen und vertragszahnärztlichen Versorgung genutzt werden.
(2) Die in der Richtlinie festzulegenden Anforderungen müssen geeignet sein, abgestuft im Verhältnis zum Gefährdungspotential und dem Schutzbedarf der verarbeiteten Informationen, Störungen der informationstechnischen Systeme, Komponenten oder Prozesse der vertragsärztlichen Leistungserbringer in Bezug auf Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele zu vermeiden.
(3) Die in der Richtlinie festzulegenden Anforderungen müssen dem Stand der Technik entsprechen und sind jährlich an den Stand der Technik und an das Gefährdungspotential anzupassen. Die in der Richtlinie festzulegenden Anforderungen sowie deren Anpassungen erfolgen im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik sowie im Benehmen mit dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, der Bundesärztekammer, der Bundeszahnärztekammer, der Deutschen Krankenhausgesellschaft und den für die Wahrnehmung der Interessen der Industrie maßgeblichen Bundesverbänden aus dem Bereich der Informationstechnologie im Gesundheitswesen. Die Anforderungen nach Absatz 1 Satz 2 legen die Kassenärztlichen Bundesvereinigungen zusätzlich im Benehmen mit der Gesellschaft für Telematik fest.
(4) Die Richtlinie ist für die an der vertragsärztlichen und vertragszahnärztlichen Versorgung teilnehmenden Leistungserbringer verbindlich. Die Richtlinie ist nicht anzuwenden für die vertragsärztliche und vertragszahnärztliche Versorgung im Krankenhaus, soweit dort bereits angemessene Vorkehrungen getroffen werden. Angemessene Vorkehrungen im Sinne von Satz 2 gelten als getroffen, wenn die organisatorischen und technischen Vorkehrungen nach § 8a Absatz 1 des BSI-Gesetzes oder entsprechende branchenspezifische Sicherheitsstandards umgesetzt wurden.
(5) Die Kassenärztlichen Bundesvereinigungen müssen ab dem 30. Juni 2020 die Mitarbeiterinnen und Mitarbeiter der Anbieter im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik auf deren Antrag zertifizieren, wenn diese Personen über die notwendige Eignung verfügen, um die an der vertragsärztlichen und vertragszahnärztlichen Versorgung teilnehmenden Leistungserbringer bei der Umsetzung der Richtlinie sowie deren Anpassungen zu unterstützen. Die Vorgaben für die Zertifizierung werden von den Kassenärztlichen Bundesvereinigungen im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik sowie im Benehmen mit den für die Wahrnehmung der Interessen der Industrie maßgeblichen Bundesverbänden aus dem Bereich der Informationstechnologie im Gesundheitswesen bis zum 31. März 2020 erstellt. In Bezug auf die Anforderungen nach Absatz 1 Satz 2 legen die Kassenärztlichen Bundesvereinigungen die Vorgaben für die Zertifizierung der Mitarbeiterinnen und Mitarbeiter der Anbieter nach Satz 1 im Benehmen mit der Gesellschaft für Telematik fest.

- gesetzliche Grundlage § 75b SGB V
- beschlossen am 16.12.2020 durch die Vertreterversammlung der KBV
- Umsetzung ist für alle Praxen verbindlich
  - erste Anforderungen ab 01.04.2021
  - alle Anforderungen seit 01.07.2022



Kassenärztliche Bundesvereinigung

Bekanntmachungen

Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit

Die Vertreterversammlung der Kassenärztliche Bundesvereinigung hat mit Beschluss vom 16. Dezember 2020 die Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit wie folgt beschlossen:

A. ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT

I. PRÄAMBEL

Die Kassenärztliche Bundesvereinigung hat nach § 75b SGB V den Auftrag, Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen Versorgung zu regeln. Sie hat damit den Auftrag, den Stand der Technik der technisch-organisatorische Maßnahmen im Sinne von Artikel 32 Datenschutz-Grundverordnung zu standardisieren. Die hier getroffenen Richtlinien erfüllen diesen Auftrag und dienen damit dem Zweck, die Handhabung der Vorgaben der Datenschutz-Grundverordnung im Zusammenhang mit der elektronischen Datenverarbeitung für die vertragsärztliche Praxis zu vereinheitlichen und zu erleichtern.

Die Richtlinie adressiert die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme in der vertragsärztlichen –psychotherapeutischen Praxis. Die Richtlinie legt technischen Anforderungen fest und beschreibt das Mindestmaß der zu ergreifenden Maßnahmen, um die Anforderungen der IT-Sicherheit zu gewährleisten. Mit der Umsetzung der Anforderungen werden die Risiken der IT-Sicherheit minimiert. Bei der Umsetzung können Risiken auch an Dritte, wie IT-Dienstleister oder Versicherungen, übertragen oder durch den Verantwortlichen akzeptiert werden.

II. GELTUNGSBEREICH

1. Diese Richtlinie legt die in einer vertragsärztlichen bzw. vertragspsychotherapeutischen Praxis erforderlichen Anforderungen an die IT-Sicherheit fest.
2. Der/die Praxisinhaber ist/sind verantwortlich für die Einhaltung der Anforderungen dieser Richtlinie.

III. PRAXISGRÖSSEN UND ANFORDERUNGSKATEGORIEN

Die umzusetzenden Anforderungen richten sich nach der Größe der Praxis. Dabei gilt Folgendes:

IT-Sicherheitsrichtlinie der KBV – Struktur

- „Richtline nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit“

  - Festlegung des Geltungsbereichs, der Praxisgrößen sowie die Zuordnung der Anlagen zu den Praxisgrößen

  - Anlagen 1 bis 5 mit den Anforderungen für die verschiedenen Praxisgrößen, den Umgang mit medizinischen Großgeräten sowie den Umgang mit den Komponenten für die Telematik-Infrastruktur

IT-Sicherheitsrichtlinie der KBV – Praxisgrößen

- **Praxis** mit bis zu fünf ständig mit der Datenverarbeitung betraute Personen
- **Mittlere Praxis** mit 6 bis 20 ständig mit der Datenverarbeitung betraute Personen
- **Großpraxis** oder Praxis mit Datenverarbeitung im erheblichen Umfang mit über 20 ständig mit der Datenverarbeitung betrauten Personen oder großem Umfang der Datenverarbeitung

- Zählung aller Personen, die routinemäßig in der Praxis mit Daten arbeiten, d.h. Ärzte, MFA aber auch Verwaltungspersonal

  → d.h. auch eine Einzelpraxis kann als mittlere Praxis gelten

IT-Sicherheitsrichtlinie der KBV – Zuordnung der Anlagen

- (kleine) Praxis Anlagen 1 und 5
- Mittlere Praxis Anlagen 1, 2 und 5
- Großpraxis Anlagen 1, 2, 3 und 5
- bei Einsatz medizinischer Großgeräte wie CT oder MRT zusätzlich Anlage 4

IT-Sicherheitsrichtlinie der KBV – Inhalte

- allgemeine Unterscheidung nach Software und Hardware
  - Software: Apps, Office-Produkte, Internet-Anwendungen
  - Hardware: PCs, Smartphones, Tablets, Wechseldatenträger, Netzwerk
- separate Regelungen für TI-Komponenten und medizinische Großgeräte

IT-Sicherheitsrichtlinie der KBV – Beispiel Software

- Anlage 1 Nr. 5 – Verzicht auf Cloud-Speicherung bei Office-Produkten „Keine Nutzung der in Office-Produkte integrierte Cloud-Speicher zur Speicherung personenbezogener Informationen“

- Anlage 1 Nr. 16 – Konfiguration von Synchronisationsmechanismen „Die Synchronisierung von Nutzerdaten mit Microsoft-Cloud-Diensten sollte vollständig deaktiviert werden“

→ OneDrive deaktivieren, Microsoft Office ohne Anmeldung nutzen

IT-Sicherheitsrichtlinie der KBV – Beispiel Hardware

- Anlage 1 Nr. 32 – Absicherung der Netzübergangspunkte
  „Der Übergang zu anderen Netzen insbesondere das Internet muss durch eine Firewall geschützt werden.“

  → Empfehlung eine Hardware-Firewall einzusetzen und diese nach den eigenen Anforderungen zu konfigurieren und zu warten

- Anlage 1 Nr. 33 – Dokumentation des Netzwerks
  „Das interne Netz ist inklusive eines Netzplans zu dokumentieren.“

  → Dokumentation der logischen Struktur des Netzes und von Änderungen

1 IT Sicherheitsrichtlinie der KBV

2 **Hinweise zur Umsetzung**

Exkurs Risikoeinschätzung

Risiken für schützenswerte Informationen

- Vertraulichkeit — Informationen sind nur berechtigten Personen zugänglich
- Integrität — Informationen sind unbeschädigt oder unverändert
- Verfügbarkeit — Zugriff auf die Informationen besteht

Risikoeinschätzung

- Wie hoch ist die Wahrscheinlichkeit, dass ein bestimmter Schaden eintritt?
  - z.B. sehr gering → gering → mittel → hoch → sehr hoch
- Wie hoch ist der mögliche Schaden?
  - z.B. sehr gering → gering → mittel → hoch → sehr hoch
- Mit dieser Einschätzung kann eine Risikobewertung vorgenommen werden.

Risikobewertung

Eintrittswahrscheinlichkeit

Schadenspotenzial	sehr gering	gering	mittel	hoch	sehr hoch
sehr gering	sehr niedrig	sehr niedrig	niedrig	niedrig	mittel
gering	sehr niedrig	niedrig	niedrig	mittel	hoch
mittel	niedrig	niedrig	mittel	hoch	hoch
hoch	niedrig	mittel	hoch	hoch	sehr hoch
sehr hoch	mittel	hoch	hoch	sehr hoch	sehr hoch

Beispiele für eine Risikoeinschätzung

Verlust einer **unverschlüsselten** USB-Festplatte mit der Datensicherung der Praxis – Risiko für die Vertraulichkeit der Patientendaten!

- Eintrittswahrscheinlichkeit mittel
- Schadenspotenzial sehr hoch
- → **Risikobewertung** **hoch**

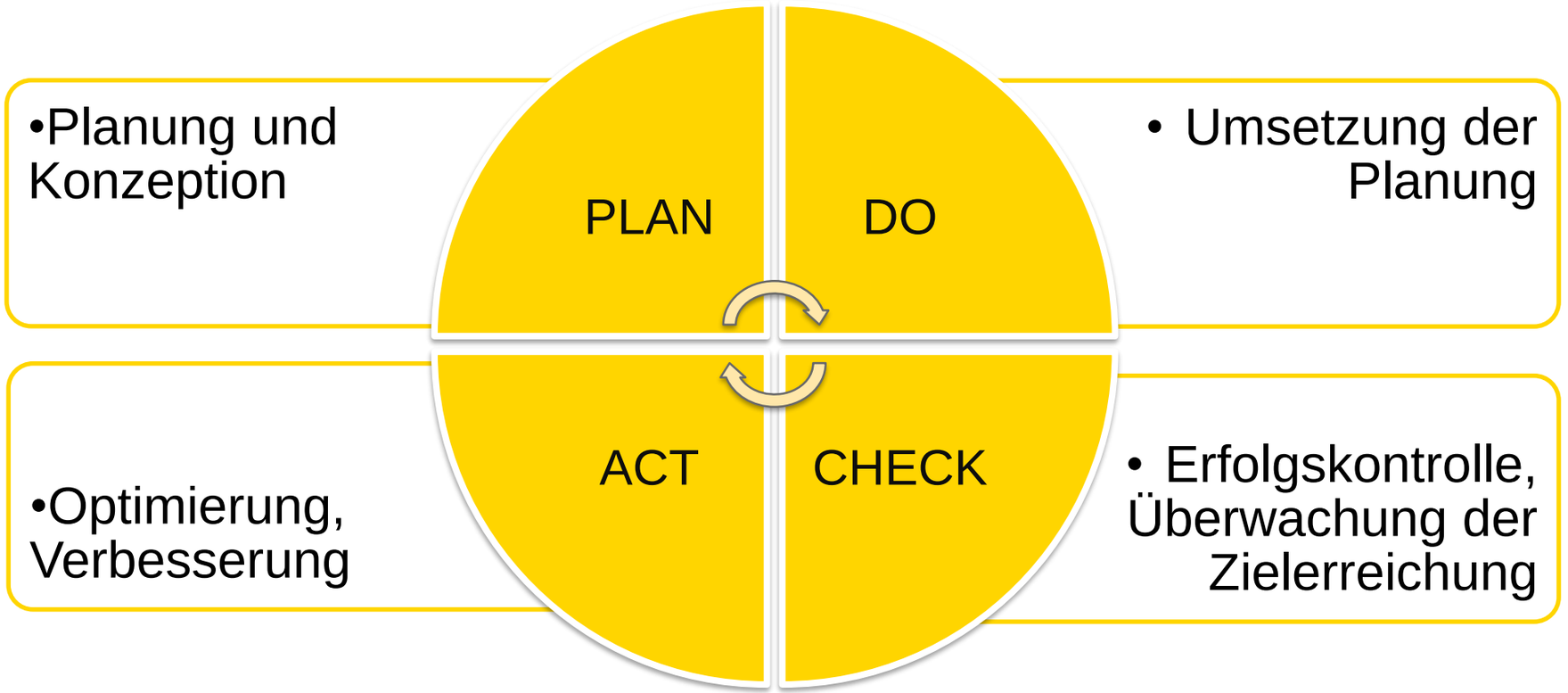
Verlust einer **verschlüsselten** USB-Festplatte mit der Datensicherung der Praxis – Risiko für die Vertraulichkeit der Patientendaten?

- Eintrittswahrscheinlichkeit mittel
- Schadenspotenzial sehr gering
- → **Risikobewertung** **niedrig**

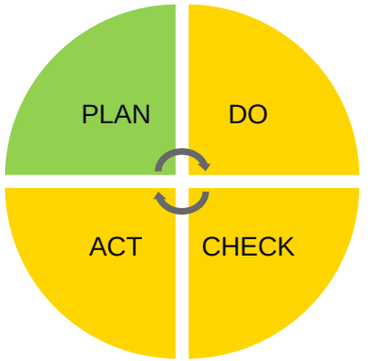
Verbesserung der IT-Sicherheit – allgemeiner Ablauf

- Bestandsaufnahme
- kurzfristige Umsetzung der „einfachen“ Maßnahmen
- Planung weiterer Maßnahmen, ggf. externe Beratung
- Umsetzung weiterer Maßnahmen
- kontinuierliche Überprüfung der umgesetzten Maßnahmen sowie Prüfung, ob zusätzliche Maßnahmen notwendig sind

PDCA-Zyklus als Planungshilfe

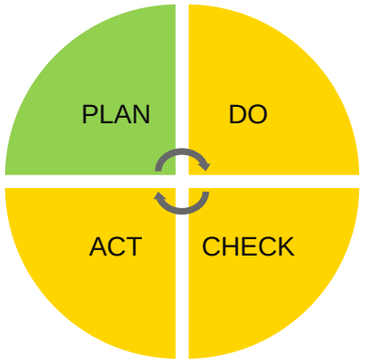


Informationen zusammentragen



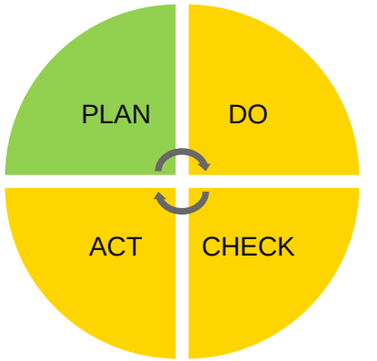
- Richtlinie und Anlagen
- Zusatzinformationen der KV (u.a. Checklisten, Infoletter)
- Informationen der KBV
- praxisintern bereits bekannte Themen
- ggf. Hinweise externer Personen, z.B. Softwarebetreuer

Bestandsaufnahme durchführen



- Welche Anforderungen aus der Richtlinie sind für die eigene Praxis relevant?
  - Wie groß ist die eigene Praxis einzustufen?
  - Werden z.B. Smartphones für den Praxisbetrieb genutzt?
- Welche Probleme oder Mängel sind bereits bekannt?
- Welche Maßnahmen wurden in der Vergangenheit umgesetzt?
  - Wurden z.B. Standardpasswörter geändert?
  - Wurde z.B. der Virenscanner umkonfiguriert?

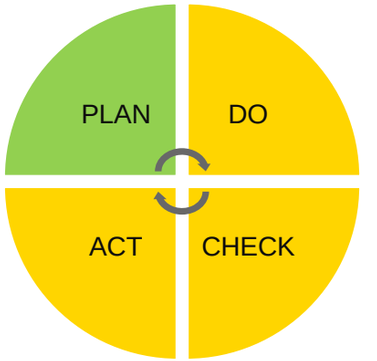
Umzusetzende Maßnahmen identifizieren I



- Welche Anforderungen aus der Richtlinie müssen zwingend umgesetzt werden?
  - z.B. Anlage 1 Nr. 32, 33, 34 – Netzwerksicherheit „Das interne Netz ist inklusive eines Netzplanes zu dokumentieren.“

- Welche Anforderungen aus der Richtlinie sollten umgesetzt werden?
  - z.B. Anlage 1 Nr. 12 – „Mikrofon und Kamera am Rechner sollten grundsätzlich deaktiviert sein und nur bei Bedarf temporär direkt am Gerät aktiviert und danach wieder deaktiviert werden.“

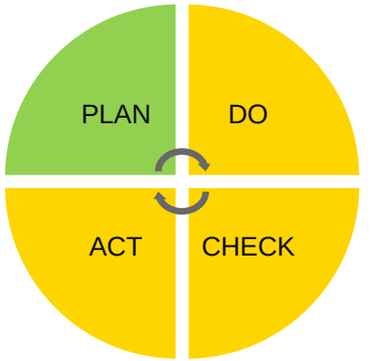
Umzusetzende Maßnahmen identifizieren II



- Welche zusätzlichen Anforderungen aus der Richtlinie können sinnvoll umgesetzt werden?
  - z.B. Anforderungen, die für größere Praxen gelten
    Anlage 3 Nr. 10 – Verschlüsselung externer Datenträger

- Welche Maßnahmen aus anderen Informationsquellen sollten umgesetzt werden?
  - z.B. Hinweise des Systembetreuers, Informationen der KV oder KBV, individuelle Beratung durch die KV, externe Sicherheitsberatung …

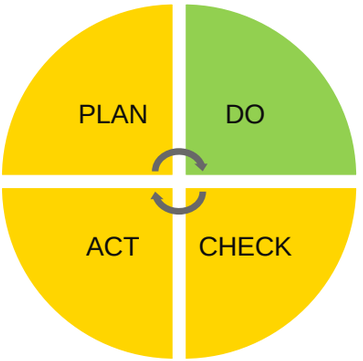
Priorisierung und Planung der Umsetzung



- Welche Maßnahmen sollten zuerst umgesetzt werden?
  - Behebung der größten Sicherheitsprobleme
  - Lösung von Problemen, die einfach und mit wenig Aufwand gelöst werden können

- Zeitplanung für die Umsetzung aufwändiger Maßnahmen
  - ggf. Beschaffung von Hardware (Firewall)
  - Terminvereinbarung mit externen Fachleuten

Umsetzung der Planung

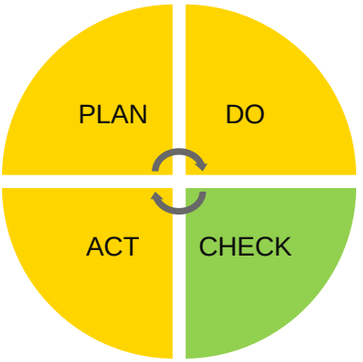


- Durchführung der geplanten Maßnahmen zur Verbesserung der TI-Sicherheit anhand der Priorisierung

- Dokumentation der durchgeführten Maßnahmen
  - z.B. anhand der Checklisten
  - komplexere Maßnahmen erfordern ggf. eine detaillierte Dokumentation, z.B. Einbau und Konfiguration einer Firewall

- falls bei der Umsetzung geplanter Maßnahmen weitere Probleme erkannt werden, Priorisierung und Aufnahme in die weitere Planung

Überprüfung der Wirksamkeit der Maßnahmen

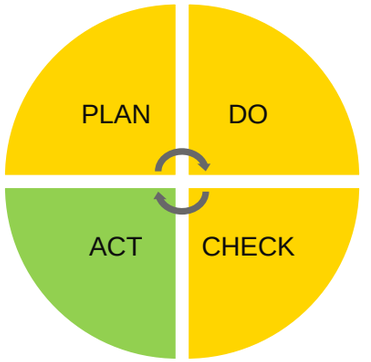


- Erfolgskontrolle und Überwachung der Wirksamkeit

- erste Überprüfung direkt nach bzw. kurz nach der Umsetzung
  - Werden die festgelegten Ziele erreicht?
  - Ist die Maßnahme wirksam?
  - Gibt es Anpassungen, die umgesetzt werden sollten?

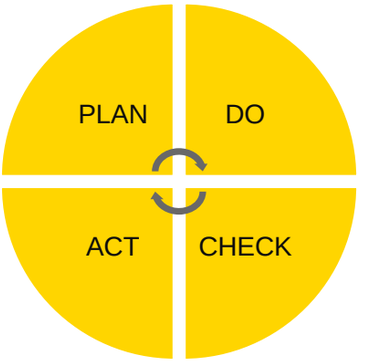
- Regelmäßige Überprüfung der umgesetzten Maßnahmen
  - Ist die Maßnahme weiterhin wirksam?
  - Gibt es neue Geräte, Erkenntnisse oder Bedrohungen, die berücksichtigt werden müssen?

Optimierung und Verbesserung



- kleinere Anpassungen, die bestehende Umsetzungen betreffen
- Beispiele für Optimierung und Verbesserung
  - Anpassung des
  - Anpassung der Firewall-Konfiguration
  - Überarbeitung der Dokumentation
  - Verbesserung von Personalschulungen
- große Änderungen erhalten einen eigenen Umsetzungszyklus

IT-Sicherheit als Daueraufgabe

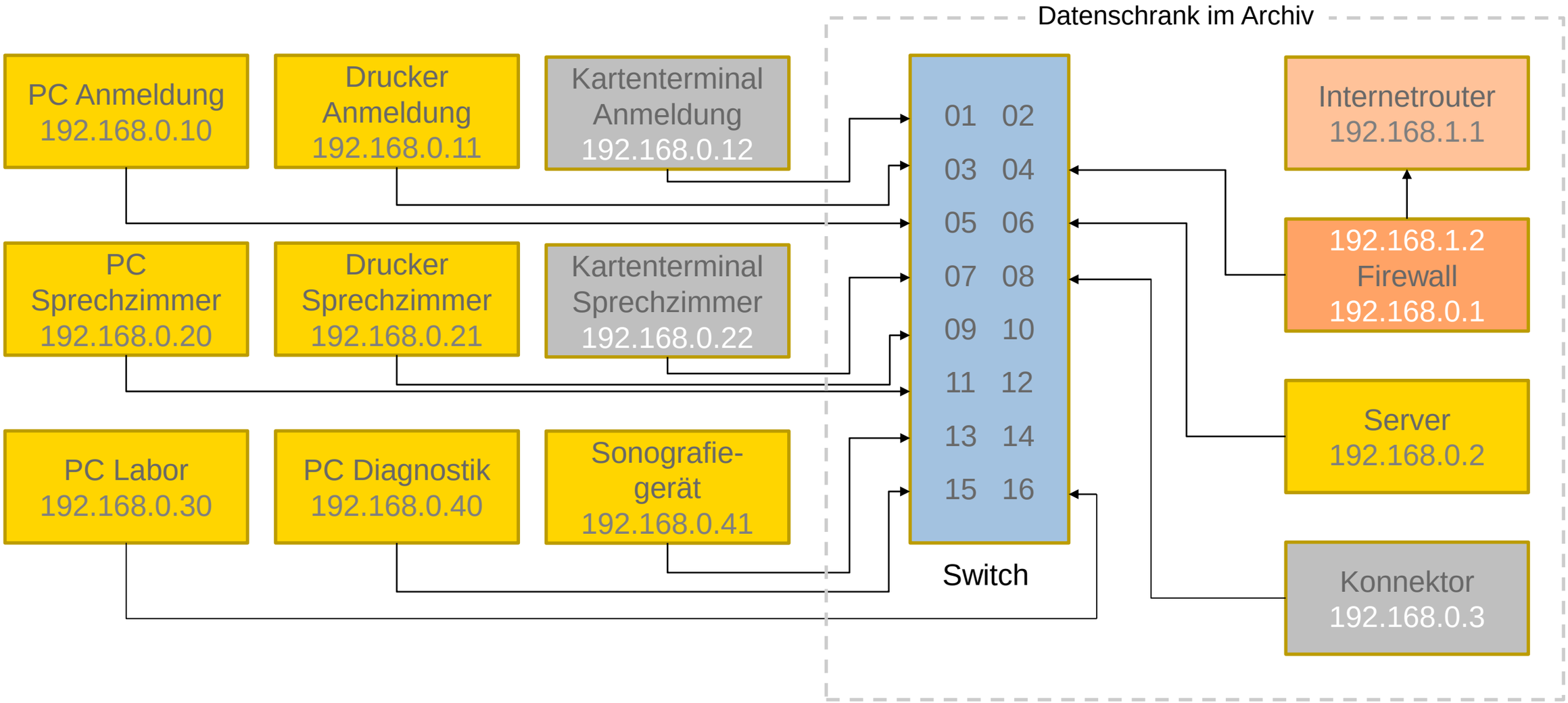


- IT-Sicherheit muss kontinuierlich sichergestellt werden, der Zyklus aus Planen, Umsetzen, Prüfen, Verbessern ist niemals abgeschlossen
- ständig werden neue Bedrohungen entdeckt und Angriffsszenarien entwickelt, die meist neue Schutzmechanismen erfordern
- neues Personal muss geschult werden, Wissen des vorhandenen Personals muss aufgefrischt werden
- Verantwortung liegt bei den Praxisinhabern
  Umsetzung, Prüfung, usw. können delegiert werden

Schnell umsetzbare, konkrete Empfehlungen

- Dokumentieren Sie Ihr Netzwerk und die Sicherheitsmaßnahmen!
  - Zeichnung auf Papier, Zeichenfunktion in Word oder PowerPoint, …
- Verbessern Sie die Sicherheit der verwendeten Passwörter!
  - PC-Anmeldung, PVS-Anmeldung, Drucker, Konnektor, Onlinedienste, …
- Aktivieren Sie die automatischen Updates auf allen Geräten!
- Nutzen Sie separate Geräte im Gäste-WLAN für den Internetzugang!
  - Tablet oder Laptop zur flexiblen Nutzung in den Praxisräumen

Beispiel für einen einfachen Netzwerkplan



Informationsquellen

- KBV: Übersichtsseite zur IT-Sicherheitsrichtline
  https://www.kbv.de/html/it-sicherheit.php
- KBV: Praxishinweise zur IT-Sicherheitsrichtlinie
  https://hub.kbv.de/display/itsrl/Praxishinweise
- KBV: Verzeichnis zertifizierter Dienstleister
  https://www.kbv.de/media/sp/KBV_ISAP_Dienstleister_ZERT_P75b_SGBV.pdf
- KVSA: Checklisten zur Umsetzung
  https://www.kvsa.de/praxis/it_in_der_praxis/it_sicherheit.html

Vielen Dank für Ihre Aufmerksamkeit!

Stefan Troschke
IT-Service der KV Sachsen-Anhalt

Telefon: 0391 627 7000
E-Mail: it-service@kvsa.de
KIM: it-service@kvsa.kim.telematik