DiMaBBS – 2. Qualitätszirkel

Aus der Praxis:

Konzept für IT-Sicherheit

an den berufsbildenden Schulen

im Landkreis Ravensburg

Amt für Kreisschulen

Sachgebiet IT-Koordination Schulen (ITKS)

Claudia Roßmann M.A., Leitung Sachgebiet ITKS

15.06.2026

Zahlen – Daten – Fakten

- Der Landkreis Ravensburg ist Schulträger für:
  - 5 berufsbildende Schulen
  - 2 Sonderpädagogische Bildungs- und Beratungszentren
  - 1 Fachschule für Landwirtschaft
  - 1 Krankenpflegeschule
  - rd. 10.000 Schülerinnen und Schüler
- seit 2019: Digitalisierungsschub durch den DigitalPakt
- 2022: Konzept für „Betrieb, Wartung und Support“, (Gremienbeschluss)

Grundlegendes zum IT-Sicherheitskonzept

- baut auf dem Konzept „Betrieb, Wartung, Support“ aus dem Jahr 2022 auf
- Grundlage:
  - **IT-Grundschutz-Kompendium** des Bundesamts für Sicherheit in der Informationstechnik (BSI)
  - **Handlungsempfehlungen der Cybersicherheitsagentur Baden-Württemberg** (CSBW)
- Charakter:
  Leitfaden für eine kontinuierliche Überprüfung und Anpassung der IT-Infrastruktur-parameter und schulischen Betriebsprozesse
- Umsetzung des IT-Sicherheitsprozesses erfolgt gemeinsam mit den Schulen –
  - d.h. individuell mit jeder einzelnen Schule (Start mit Pilotschule ab SJ 2026/27)

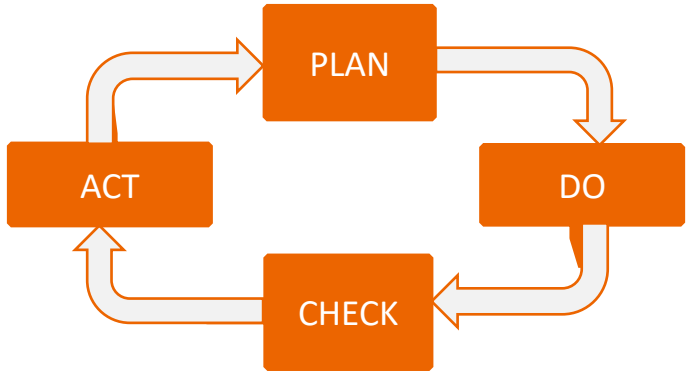
Inhalt

Inhalt

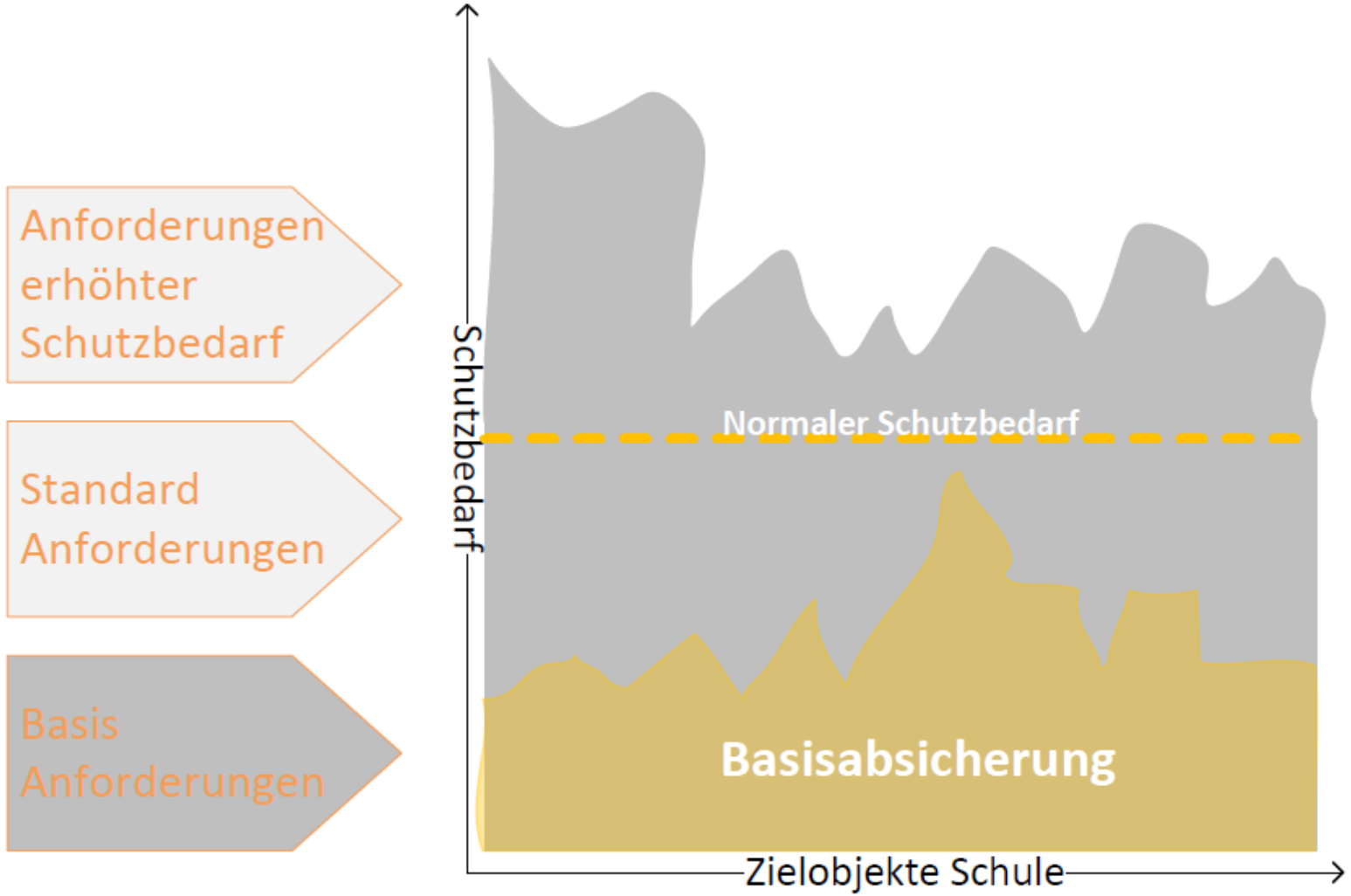
Inhalt

Zielsetzung und Vorgehen

- **Basisabsicherung** → breite Absicherung aller IT-Bereiche auf geringem Niveau
  - grundlegende Anforderungen an IT-Sicherheit nach BSI-Standard
- **Kernabsicherung** → punktuell hohe Absicherung der wichtigsten Systeme und Prozesse
  - z.B. Schutz personen-, leistungs- und gesundheitsbezogener Informationen und kritischer IT-Infrastrukturen (Serverräume, Verwaltungsnetzwerke, Datenbanken usw.)
- **IT-Grundschutz-Kompendium:** Umfangreicher Baustein-Katalog mit Anforderungen und Empfehlungen für
  - Einzelkomponenten der IT-Landschaft
  - (schulischen) Geschäftsprozessen
- **PDCA Zyklus:** Fortlaufender Überprüfungs- und Optimierungsprozess



1. Schritt: Basisabsicherung



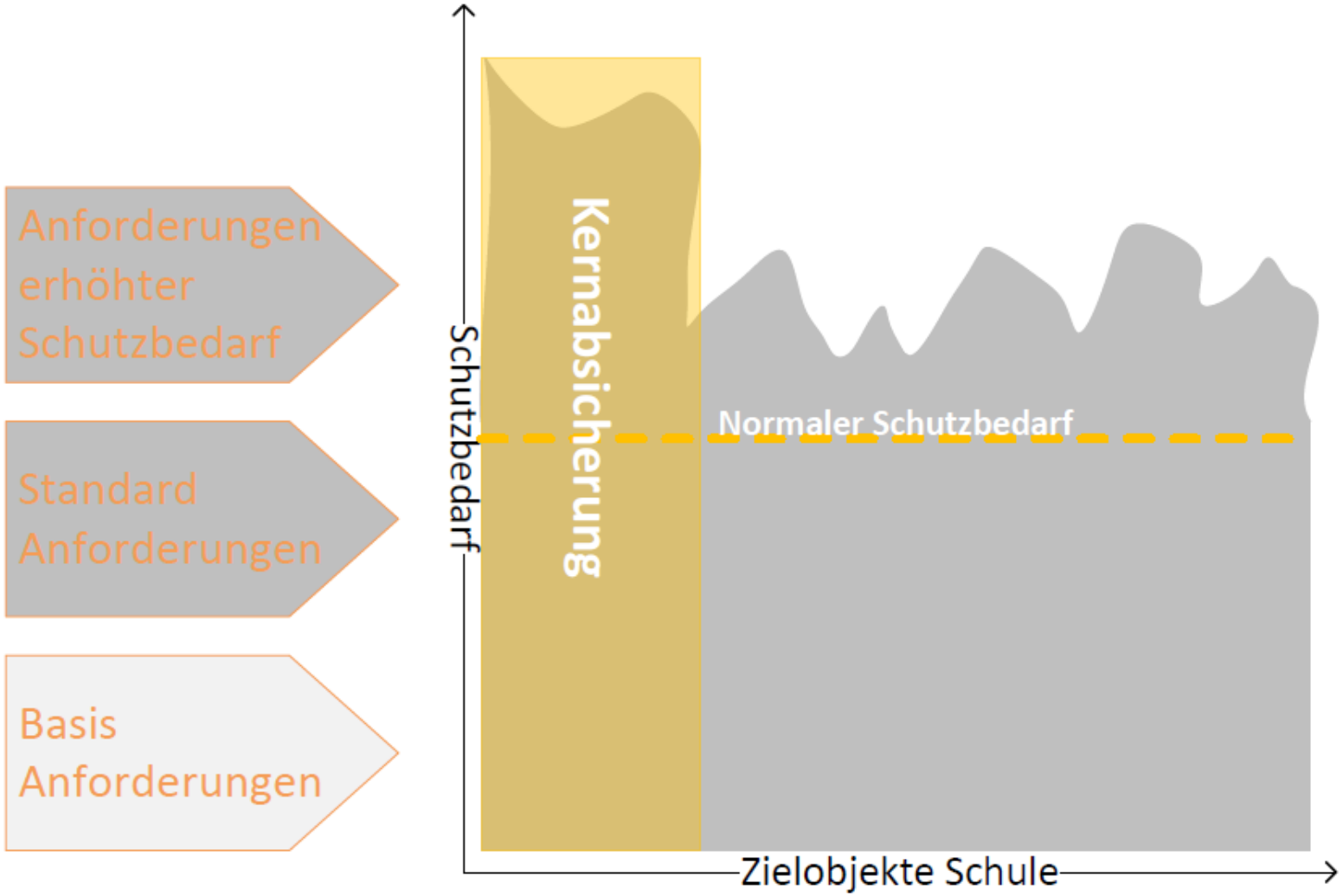
Beispiele für Maßnahmen bei Clients:

Erhöhter-Schutzbedarf-Maßnahmen, z.B.
- Systemüberwachungskonzept
- Verschlüsselung
- Referenzinstallation erstellen für die Grundkonfiguration, Updates, Patches …
- Mehrfaktor-Authentifizierung

Standard-Maßnahmen, z.B.
- Installationen und Konfigurationen nur durch Admins oder Dienstleister
- restriktive Vorgaben für Nutzung von Wechseldatenträgern

Basis-Maßnahmen, z.B.
- sichere Authentisierung des Users
- regelmäßige automatische Updates
- Schutzprogramme vor Schadsoftware
- Schwachstellenanalyse / Awareness-Tests

2. Schritt: Kernabsicherung (nach Schutzbedarfsanalyse)



Beispiele für Maßnahmen bei Clients:

Erhöhter-Schutzbedarf-Maßnahmen, z.B.
- Systemüberwachungskonzept
- Verschlüsselung
- Referenzinstallation erstellen für die Grundkonfiguration, Updates, Patches …
- Mehrfaktor-Authentifizierung

Standard-Maßnahmen, z.B.
- Installationen und Konfigurationen nur durch Admins oder Dienstleister
- restriktive Vorgaben für Nutzung von Wechseldatenträgern

Basis-Maßnahmen, z.B.
- sichere Authentisierung des Users
- regelmäßige automatische Updates
- Schutzprogramme vor Schadsoftware
- Schwachstellenanalyse / Awareness-Tests

„Checkliste“ Basisabsicherung

(aus dem Baustein-Katalog des IT-Grundschutz-Kompendiums)

- Technische Bausteine - beispielhaft „SYS.1.1“:

Baustein-ID	Basis-Anforderung	Zuständigkeit	Beschreibung Basis-Anforderung
SYS.1.1 Allgemeiner Server	SYS.1.1.A1 Zugriffsschutz und Nutzung (B)	KR + IKP (TIG & BPM)	Physische Server MÜSSEN an Orten betrieben werden, zu denen nur berechtigte Personen Zutritt haben. Physische Server MÜSSEN daher in Rechenzentren, Serverräumen oder abschließbaren Serverschränken aufgestellt beziehungsweise eingebaut werden (siehe hierzu die entsprechenden Bausteine der Schicht INF Infrastruktur). Bei virtualisierten Servern MUSS der Zugriff auf die Ressourcen der Instanz und deren Konfiguration ebenfalls auf die berechtigten Personen begrenzt werden. Server DÜRFEN NICHT als Arbeitsplatzrechner genutzt werden. Server DÜRFEN NICHT zur Erledigung von Aufgaben und Tätigkeiten verwendet werden, die grundsätzlich auf einem Client-System aus- und durchgeführt werden können. Insbesondere DÜRFEN vorhandene Anwendungen, wie Webbrowser, auf dem Server NICHT für das Abrufen vo Informationen aus dem Internet oder das Herunterladen von Software, Treibern und Updates verwendet werden. Als Arbeitsplatz genutzte IT-Systeme DÜRFEN NICHT als Server genutzt werden.
	SYS.1.1.A2 Authentisierung an Servern (B)	KR + Schule	Für die Anmeldung von Benutzenden und Diensten am Server MÜSSEN Authentisierungsverfahren eingesetzt werden, die dem Schutzbedarf der Server angemessen sind. Dies SOLLTE in besonderem Maße für administrative Zugänge berücksichtigt werden. Soweit möglich, SOLLTE dabei auf zentrale, netzbasierte Authentisierungsdienste zurückgegriffen werden.

„Checkliste“ Basisabsicherung

- Technische Bausteine - beispielhaft „ORP.4“:

Baustein-ID	Basis-Anforderung	Zuständigkeit	Beschreibung Basis-Anforderung
ORP.4 Identitäts- und Berechtigungsmanagement	ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzenden und Benutzendengruppen (B) [IT-Betrieb]	KR + Schule	Es MUSS geregelt werden, wie Benutzendenkennungen und -gruppen einzurichten und zu löschen sind. Jede Benutzendenkennung MUSS eindeutig einer Person zugeordnet werden können. Benutzendenkennungen, die längere Zeit inaktiv sind, SOLLTEN deaktiviert werden. Alle Benutzenden und Benutzendengruppen DÜRFEN NUR über separate administrative Rollen eingerichtet und gelöscht werden. Nicht benötigte Benutzendenkennungen, wie z. B. standardmäßig eingerichtete Gastkonten oder Standard-Administrierendenkennungen, MÜSSEN geeignet deaktiviert oder gelöscht werden.
	ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen (B) [IT Betrieb]	KR + TIG + Schule	Benutzendenkennungen und Berechtigungen DÜRFEN NUR aufgrund des tatsächlichen Bedarfs und der Notwendigkeit zur Aufgabenerfüllung vergeben werden (Prinzip der geringsten Berechtigungen, englisch Least Privileges und Erforderlichkeitsprinzip, englisch Need-to-know). Bei personellen Veränderungen MÜSSEN die nicht mehr benötigten Benutzendenkennungen und Berechtigungen entfernt werden. Beantragen Mitarbeitende Berechtigungen, die über den Standard hinausgehen, DÜRFEN diese NUR nach zusätzlicher Begründung und Prüfung vergeben werden. Zugriffsberechtigungen auf Systemverzeichnisse und -dateien SOLLTEN restriktiv eingeschränkt werden. Alle Berechtigungen MÜSSEN über separate administrative Rollen eingerichtet werden.
	ORP.4.A3 Dokumentation der Benutzendenkennungen und Rechteprofile (B) [IT-Betrieb]	KR + TIG + Schule	Es MUSS dokumentiert werden, welche Benutzendenkennungen, angelegte Benutzendengruppen und Rechteprofile zugelassen und angelegt wurden. Die Dokumentation der zugelassenen Benutzendenkennungen, angelegten Benutzendengruppen und Rechteprofile MUSS regelmäßig daraufhin überprüft werden, ob sie den tatsächlichen Stand der Rechtevergabe widerspiegelt. Dabei MUSS auch geprüft werden, ob die Rechtevergabe noch den Sicherheitsanforderungen und den aktuellen Aufgaben der Benutzenden entspricht. Die Dokumentation MUSS vor unberechtigtem Zugriff geschützt werden. Sofern sie in elektronischer Form erfolgt, SOLLTE sie in das Datensicherungsverfahren einbezogen werden.
	ORP.4.A4 Aufgabenverteilung und Funktionstrennung (B) [IT-Betrieb]	KR + TIG + Schule	Die von der Institution definierten unvereinbaren Aufgaben und Funktionen (siehe Baustein ORP.1 Organisation) MÜSSEN durch das Identitäts- und Berechtigungsmanagement getrennt werden.
	ORP.4.A5 Vergabe von Zutrittsberechtigungen (B) [IT-Betrieb]	KR + TIG + Schule	Es MUSS festgelegt werden, welche Zutrittsberechtigungen an welche Personen im Rahmen ihrer Funktion vergeben bzw. ihnen entzogen werden. Die Ausgabe bzw. der Entzug von verwendeten Zutrittsmittel wie Chipkarten MUSS dokumentiert werden. Wenn Zutrittsmittel kompromittiert wurden, MÜSSEN sie ausgewechselt werden. Die Zutrittsberechtigten SOLLTEN für den korrekten Umgang mit den Zutrittsmitteln geschult werden. Bei längeren Abwesenheiten SOLLTEN berechtigte Personen vorübergehend gesperrt werden.

Danke für Ihre Aufmerksamkeit!

Wo der Süden am schönsten ist.