Informationssicherheit Schule im IT-Betrieb

Handreichung 2: Erste Schritte

Berlin, 23.05.2023

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Urheberschaft

Herausgeberin: PD – Berater der öffentlichen Hand GmbH, Friedrichstraße 149, 10117 Berlin
Web: https://www.pd-g.de

Haftungsausschluss

Zielgruppe

Die vorliegende Handreichung richtet sich primär an die umsetzenden Personen im Bereich der Informationssicherheit für Schulen und Schulträger. Dieser Personenkreis inkludiert Fachpersonal im IT-Bereich der Schulträger und Schulen. Konkret können das Personen aus Rechenzentren oder der IT-Abteilung eines Schulträgers sowie Lehrkräfte in Schulen sein, die für die Umsetzung der IT in den Schulen verantwortlich sind.

Darüber hinaus sollen auch Verantwortliche für die Informationssicherheit angesprochen werden, da die Fragen zur Informationssicherheit und IT-Sicherheit (siehe Seite 10 Definition der Begriffe) stets auch Fragen zum Personaleinsatz und Personalressourcen betreffen.

Zielsetzung

Die Handreichung „Einführung in die Informationssicherheit für Schulen: Handreichung für Schulträger und Schulen“ (im Folgenden HR 1 genannt) und die vorliegende Handreichung bieten den Umsetzungsverantwortlichen in den Schulen und bei den Schulträgern umfassendes Wissen, um eine Basisabsicherung gemäß dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu erlangen. Während die HR1 die Umsetzung der Basisabsicherung entlang der BSI Bausteine des Grundschutzkompendiums fokussiert, hat die HR2 den Lebenszyklus der einzelnen Komponenten von der Planung bis zur Entsorgung zum Gegenstand.

Ziel ist es, die Umsetzungsverantwortlichen über die notwendigen Maßnahmen zur IT-Sicherheit – von der Planung über die Beschaffung bis hin zum Betrieb der Komponenten – zu informieren und sie zur Umsetzung zu befähigen.

Des Weiteren sollen sich IT-Verantwortliche einen Eindruck darüber verschaffen können, welche Ressourcen personeller Art notwendig sind, um eine sichere IT in den Schulen und beim Schulträger aufzubauen.

1 Einleitung

Der „DigitalPakt Schule“ hat bei vielen Schulen zu einer signifikanten Zunahme an Endgeräten und pädagogischen Anwendungen geführt. In den letzten Jahren erhöhte sich die Anzahl der Organisationen, die zu Opfern von Cyberattacken wurden. Waren es bis vor wenigen Jahren noch Großunternehmen mit hohen Bilanzsummen, werden zunehmend auch Schulen Opfer derartiger Attacken.[1] Aus diesen quantitativen und qualitativen Entwicklungen leiten sich für die Verantwortlichen für den Schulbetrieb neue Herausforderung ab.

Behördenleitungen auf Schulträgerseite und Schulleitungen sind grundsätzlich für die Gewährleistung der Informationssicherheit zuständig. Die (einzelnen) Verantwortungsbereiche ergeben sich aus den jeweiligen gesetzlichen Regelungen der Bundesländer[2] in Verbindung mit weiteren geltenden, gesetzlichen Regelungen.

Darüber hinaus empfiehlt sich die Nutzung der Angebote des BSI für die Schulträger und Schulen, um sich mit der Informationssicherheit zu befassen und eine Orientierung über entsprechende Standards zu erhalten.

[1] Süddeutsche Zeitung (13. Februar 2023): Cyberattacke auf Karlsruher Schulen, https://www.sueddeutsche.de/wirtschaft/internet-karlsruhe-cyberattacke-auf-karlsruher-schulen-hacker-fordern-bitcoin-dpa.urn-newsml-dpa-com-20090101-230213-99-579615, abgerufen am 13.02.2023.

[2] Ausnahme: Die Stadtstaaten Bremen und Hamburg, bei denen das Schulgesetz keine Trennung zwischen inneren und äußeren Schulangelegenheiten vorsieht. Die Bildungsverwaltung beider Städte ist daher für alle schulischen Belange (curriculare, personelle und infrastrukturelle) verantwortlich.

1.1 Drei Einflussgrößen als Veränderungsparameter für die IT in den Schulen

Abbildung 1: Zusammenhang zwischen Raumgestaltung, Medienkonzepten und IT-Komponenten

Die **Einflussgröße 1** ist die fortschreitende Digitalisierung.

Sie stellt eine kontinuierliche Herausforderung für die Schulen dar und bedarf einer intensiven Schulentwicklungsarbeit. Die strategischen Planken setzte 2016 die Kultusministerkonferenz (KMK)[3], die „die Kompetenzen in der digitalen Welt“ in sechs Kompetenzbereiche unterteilt hat. Bei der Umsetzung dieser Strategie stellt die KMK in ihrem Jahresbericht 2022 heraus, dass „die digitale Bildungsinfrastruktur investiv aufwendige technische Maßnahmen erfordert. Verschiedene Maßnahmen konnten im Berichtszeitraum mit Mitteln aus dem DigitalPakt Schule realisiert werden. Alle Länder verfügen nun sowohl für allgemeinbildende als auch für berufliche Schulen über leistungsfähige, dynamische Cloud-Infrastrukturen in Form von Online-Lehr-Lernumgebungen, die virtuelle und hybride Unterrichtsformen ermöglichen.“[4]

Dieser Fortschritt dokumentiert sich in einer veränderten IT-Infrastruktur, zum Beispiel in der Zunahme von IT-Komponenten im Schulbereich, dem nun erweiterte und angepasste IT-Betriebs-, Support- und IT-Sicherheitskonzepte folgen müssen.

Die **Einflussgröße 2** bilden die geeigneten Lehr- und Lernräume.

Unter den Gegebenheiten heutiger Schulcampus sind regelmäßig die Raumgestaltungs- und Raumausstattungskonzepte zu überprüfen, die die Schulträger mit ihren Schulen planen, um digitale Lern- und Erlebnisräume zu schaffen. Ob Schulhof, Sporthalle oder Klassenraum – die Nutzung von IT-Komponenten setzt

[3] Kultusministerkonferenz (2016): Bildung in der digitalen Welt. Strategie der Kultusministerkonferenz, https://www.kmk.org/, Seite 16, abgerufen am 23.11.2022.

[4] Kultusministerkonferenz (08.12.2022): Jahresbericht der Kultusministerkonferenz zur Bildung in der digitalen Welt, Seite 4.

einerseits passende Betriebs- und Supportkonzepte für einen stabilen und sicheren IT-Betrieb voraus. Andererseits ist jede IT-technische Raumausstattung unter Informationssicherheitsaspekten zu beleuchten.

Der Raumansatz wird im Weiteren bei den beispielhaften Netzwerkplänen aufgegriffen, da sich dieser Ansatz eignet, um Entscheidungen bezüglich fest installierter oder mobiler IT-Komponenten im Schulbetrieb vorzunehmen.

Die **Einflussgröße 3** bezieht sich auf die Medienentwicklungspläne.

In den letzten zwei Jahren haben Schulen bedingt durch den „DigitalPakt Schule“ verstärkt Medienentwicklungspläne mit unterschiedlichen Schwerpunkten erarbeitet. Art und Umfang der damit einhergehenden IT-Komponenten sind keineswegs (bundes- oder landes-) einheitlich, sodass (auch an dieser Stelle) kaum allgemeingültige Aussagen über eine angemessene Ausstattung getroffen werden können. Vielmehr werden von den Beteiligten vor Ort (Schulen, Schulträger, medienpädagogische Beraterinnen und Berater, Medienzentren) Ausstattungskonzepte entwickelt, die schulspezifische Ansätze, regionale Besonderheiten und den finanziellen Rahmen berücksichtigen.

Die Medienentwicklungspläne werden übergreifend als das „Anforderungsmanagement“ interpretiert, in dem die Lehrkräfte die „fachlichen/pädagogischen“ Anforderungen gegenüber der Schul-IT formulieren.

1.2 Ansätze und Empfehlungen der PD-Handreichungen zur Informationssicherheit für Schulträger und Schulen

Abbildung 2: Handlungsfelder der Handreichungen

Die vorliegende (zweite) Handreichung greift über die drei Einflüsse hinausgehend die ausgewählten Handlungsfelder und Herausforderungen aus der ersten Handreichung „Einführung in die Informationssicherheit für Schulen" auf und bricht diese auf den Lebenszyklus von IT-Komponenten und die zugehörigen Entscheidungspunkte im schulischen Alltag herunter.

IT-Sicherheit ist ein Teilgebiet der *Informationssicherheit*. Im weiteren Verlauf der Handreichung wird der Fokus nur auf die IT-Sicherheit gelegt.

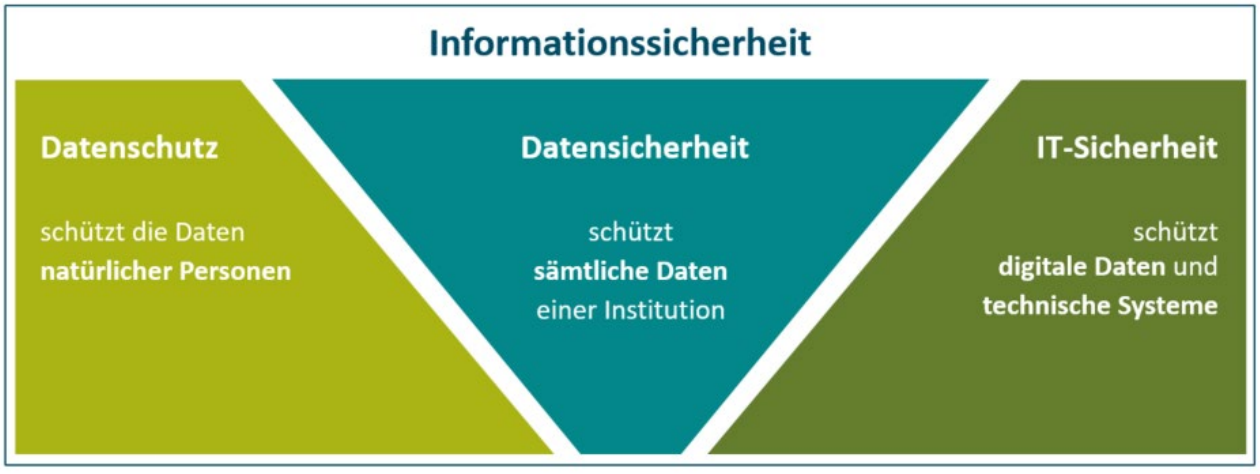

Abbildung 3: Abgrenzung der IT-Sicherheit zur Informationssicherheit (Quelle: Muster-IT-Konzept-Handreichung 1)

In der vorliegenden Handreichung werden die folgenden drei Aspekte vertiefend betrachtet:

1. **Beschaffung:** Komponenten und IT-Dienstleistung auf Basis eines Lebenszyklus von IT-Komponenten
2. **IT-Betrieb:** Netzwerk, Internetzugang, Serverbetrieb, Endgeräte als Zielobjekte in einer Schichtengrafik
3. **Notfallmanagement:** Fokus auf zentralen IT-Sicherheitsrisiken und Maßnahmen

2 Phasen des Lebenszyklus von IT-Komponenten

In diesem Kapitel wird der Lebenszyklus von IT-Komponenten dargestellt. Er gliedert sich in die fünf Phasen Planung, Beschaffung, Inbetriebnahme, regulärer Betrieb und Rückbau. Es wird dargestellt, welche Schritte notwendig sind, um IT-Komponenten über den gesamten Lebenszyklus hinweg sicher im Bereich der Schul-IT einzusetzen.

Die Inhalte der einzelnen Phasen können auch unabhängig voneinander betrachtet werden. Das bedeutet, dass Schulträger oder Schulen die folgenden Handlungsempfehlungen auch auf eine IT-Komponente beziehen können, die schon vorhanden ist, und die Phase Planung überspringen können.

Es wurde durchgehend ein Beispiel dargestellt, das zum gleichen Sachverhalt die notwendigen Sicherheitsmaßnahmen je Phase aufzeigt.

2.1 Phase 1 – Planung (IT-Strategie)

In der Planungsphase werden mittel- bis langfristige Entscheidungen für die Schul-IT getroffen. Impulsgeber für die Entscheidungen sind innere und äußere Veränderungen. Diese Anforderungen durch Änderungen in der Lernkultur und/oder in den technischen Ausstattungen werden identifiziert, bewertet und – sofern relevant – schriftlich in einer Schul-IT-Strategie fixiert. Innere Impulse können zum Beispiel die weitere Zunahme an mobilen Endgeräten bei den Schülerinnen und Schülern sein sowie die fortschreitende Digitalisierung von Lehrmaterialien für den Unterricht. Äußere Impulse können gesetzliche Auflagen zur Nutzung von Schul-Clouds und zentral gehosteten, pädagogischen Anwendungen sowie konkrete Aussagen zum Datenschutz darstellen.

Im Ergebnis sollte die Schul-IT-Strategie zeitlich auf einem Horizont von zwei bis fünf Jahren Leitplanken für das Handeln setzen. Eine Schul-IT-Strategie kann dabei die Adaption einer kommunalen IT-Strategie sein.

In dieser ersten Phase sollte bereits das Thema Personalressourcen in die Strategieplanung einfließen: Ohne ausreichendes Personal lassen sich die nötigen Strukturen nur schwer umsetzen. Nicht nur das Mehr an IT-Komponenten, sondern auch das zwingend höhere IT-Sicherheitsniveau sollte in Personalkapazitäten umgerechnet werden.

Für die Zukunft wird es immer wichtiger, dass strategische Aussagen für den Einsatz von IT-Komponenten standardisierten Prinzipien und Rahmenwerken folgen, wie dem des Designkonzeptes „Security by Design“[5].

> „Security by Design“ ist ein in der Hard- und Softwareentwicklung angewandtes Designkonzept.
>
> Die Sicherheit der Hard- oder Software wird schon im Entwicklungsprozess berücksichtigt und in den kompletten Lebenszyklus einer IT-Komponente integriert. Zu den sicheren Designkriterien zählen beispielsweise die Minimierung der Angriffsfläche, der Einsatz von Verschlüsselung, die Authentifizierung und Isolation sicherheitsrelevanter Bereiche sowie die Möglichkeit zur Installation von (z.B. Firmware-, Sicherheits-)Updates.

[5] Bundesamt für Sicherheit in der Informationstechnik (2011): Security Assessments und Security-by-Design, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/PIA_01-Bernd_Kowalski.pdf?__blob=publicationFile&v=1, abgerufen am 11.11.2022.

„Security by Design“ sollte zur Maßgabe für alle strategischen Erwägungen erklärt werden. Geräte, die nicht diesem Prinzip entsprechen, sollten möglichst keine Berücksichtigung bei der Entscheidungsfindung für die zukünftige Schul-IT finden.

Beispiel Schule:

Ein Schulträger möchte Accesspoints für die Schulen der Kommune beschaffen. Bevor sie die Beschaffung anstößt, werden alle strategischen Entscheidungen für die Beschaffung von IT-Komponenten zurate gezogen. Dies beinhaltet auch die Planung der personellen Ressourcen in allen weiteren Phasen des Lebenszyklus.

2.2 Phase 2 – Beschaffung

Sollte aus einer Strategieentscheidung heraus oder aufgrund von zyklischen Bedarfen an neuen IT-Komponenten die Notwendigkeit einer Beschaffung entstehen, empfiehlt sich die gezielte Aufnahme von Kriterien zur IT-Sicherheit in die Beschaffungsunterlagen. Hierzu zählen zum Beispiel eine Bewertungsmatrix oder ein Kriterienkatalog.

Das unter „Planung“ benannte Prinzip des „Security by Design“ sollte zum Ausschlusskriterium im Bewertungskatalog erklärt werden. Ist dieses Kriterium nicht zu halten, sollte mindestens unter der Abfrage des Herstellerlandes eine gedankliche Auseinandersetzung erfolgen, sodass bewusste Entscheidungen daraus resultieren, wie sicher eine gelieferte IT-Komponente sein kann. In jedem Fall sollten diese Komponenten in einem separaten Netzwerksegment betrieben werden.

Darüber hinaus sollte bei einer Leistungserbringung durch einen Dienstleister ein IT-Sicherheitskonzept angefordert und bewertet werden.

Der Bezug zu den einzelnen IT-Komponenten kann exemplarisch wie folgt hergestellt werden:

Tabelle 1: Fragen zur IT-Sicherheit in der Beschaffungsphase

Phase des Lebenszyklus (Auszug)	Kernfragen	Verantwortliche Person / Rolle	Empfehlungen und Erläuterungen
Beschaffung	Ist die IT-Komponente eng an vorhandenen Standards und Erfahrungen funktional beschrieben?	Beschaffung / IT-Leitung	Wenn möglich, sollten sich die neuen Endgeräte in bestehende Management-Plattformen leicht integrieren lassen. Insgesamt sollte bei der Beschaffung auf eine Standardisierung der IT-Komponenten geachtet werden.
	Ist „Security by Design” belegt?	Beschaffung / IT-Leitung	Lässt sich bei der IT-Komponente belegen, dass bei der Entwicklung Prinzipien des „Security by Design“ angewendet wurden und nachgewiesen werden können.
	Besteht ein nutzbarer Rahmenvertrag (RV), der den Einsatz bekannter und schon validierter IT-Komponenten ermöglicht?	Beschaffung	Durch den Bezug über einen RV wird die Prüfung von IT-Sicherheitsaspekten an den RV-Halter delegiert. Es sollten nur IT-Komponenten zum Einsatz kommen, die hohen IT-Sicherheitsanforderungen genügen.

Die vollständige Übersicht über die Kernfragen ist den Checklisten aus den Anlagen zu entnehmen.

Beispiel Schule:

Nachdem alle strategischen Vorgaben verifiziert und in die Überlegungen zur Beschaffung einbezogen wurden, wird zunächst geprüft, ob es einen Rahmenvertrag mit Anbietern gibt. Der Halter des Rahmenvertrages muss die IT-Sicherheitsaspekte prüfen. Müssen die IT-Komponenten auf dem freien Markt beschafft werden, sollten schon alle Sicherheitsaspekte in die Ausschreibung für die Accesspoints als Bedingungen einbezogen werden.

Die Anforderung „Security by Design“ garantiert sichere Geräte und verhindert, dass im Nachgang weitere virtuelle Netze aufgelegt werden müssen, um bei nicht so sicheren Geräten zu garantieren, dass die Sicherheitsrichtlinien für das gesamte Netzwerk eingehalten werden können. Dies spart auch Personalressourcen im späteren Betrieb.

2.3 Phase 3 – Inbetriebnahme

Mit der Inbetriebnahme von neuen IT-Komponenten erfolgt eine Erweiterung der bestehenden IT-Infrastruktur um neue Hard- und Software. Damit wird die IT-Infrastruktur komplexer und potenziell um mögliche Schwachstellen erweitert. Der Fokus vor der Inbetriebnahme liegt auf der Prüfung, welche Software oder Hardware zum Einsatz kommen soll. Eine Empfehlung hierbei lautet, dass alle Sicherheitspatches geladen und diese entsprechend konfiguriert sind (Netzwerkports sind geschlossen, USB-Ports abgeschaltet etc.) und dass alle Komponenten in einem Monitoring-Werkzeug erfasst sind.

Zur Sicherheit bieten sich schon in der Installationsphase Penetrationstest von außen und Sicherheitsscans von innen an, um die IT-Komponenten auf bekannte und gegebenenfalls noch nicht geschlossene Schwachstellen zu prüfen. Derartige Leistungen lassen sich über zertifizierte Dienstleister einkaufen.

Tabelle 2: Fragen zur IT-Sicherheit in der Phase der Inbetriebnahme

Phase des Lebenszyklus (Auszug)	Kernfragen	Verantwortliche Person / Rolle	Empfehlungen und Erläuterungen
Inbetriebnahme	Ist die Inbetriebnahme von neuen, mobilen Endgeräten beschrieben?	IT-Leitung	Es werden Standards beschrieben, die im Moment der Bereitstellung an einem festen Endgerät umgesetzt werden, um die IT-Sicherheit zu gewährleisten.
	Gibt es klare Abnahmekriterien zur IT-Sicherheit?	IT-Leitung	Es werden die beschriebenen Standards und Richtlinien für IT-Sicherheit überwacht.
	Erfolgt eine Registrierung des Endgeräts in einer Asset-, Management- und Monitoring-Software?	IT-Leitung	Es wird die Einbindung in eine Überwachungs-, Geräte- oder Assetlösung angestrebt.

Die vollständige Übersicht über die Kernfragen ist den Checklisten in den Anlagen zu entnehmen.

Beispiel Schule:

Sobald die Accesspoints beim Schulträger angekommen sind, müssen diese gemäß den bestehenden Sicherheitsrichtlinien geprüft und inventarisiert werden. Es ist notwendig, alle Updates und Sicherheitspatches auf dem neuesten Stand zu installieren, bevor sie in das Netzwerk eingebunden werden.

Darüber hinaus sollten keine Standardeinstellungen verwendet und zumindest die Passwörter neu vergeben werden. Wenn eine Software zum Monitoring vorhanden ist, müssen die neuen Komponenten auch in diese integriert werden.

2.4 Phase 4 – Regulärer Betrieb

Im regulären Schul-IT-Betrieb sollen die IT-Komponenten sicher, verfügbar und performant genutzt werden können. Dazu wird jede IT-Komponente regelmäßig gepatcht und über ein Monitoring überwacht. Technische Störungen und Veränderungen werden genauso wie Auffälligkeiten im Monitoring an einen Service Desk gemeldet und dort bearbeitet.

Für die Prüfung der IT-Sicherheit wird empfohlen, in größeren Abständen (z. B. einmal jährlich) Penetrationstest in Auftrag zu geben (siehe auch Phase 3 – Inbetriebnahme). Da die aktuell größten Gefahren von außen durch Angriffe auf die IT-Infrastruktur und durch manipulierte Dateianhänge beziehungsweise Downloads von innen ausgehen, ist es sinnvoll, den Penetrationstest dementsprechend durch simulierte Angriffe von außen und durch einen Schwachstellenscan von innen durchführen zu lassen.

Mithilfe eines (automatisierten) Schwachstellenscans wird das IT-System proaktiv auf vorhandene Schwachstellen untersucht, neue Schwachstellen werden umgehend erkannt und können passgenau gepatcht werden. Der Schwachstellenscan liefert einen grundlegenden Einblick in potenziell vorhandene Schwachstellen und dient häufig als Basis für weitergehende Sicherheitsüberprüfungen wie einen Penetrationstest. Dieser stellt eine gezielte und individuell durchgeführte IT-Sicherheitsüberprüfung dar. Hierbei wird analysiert, inwieweit die IT- beziehungsweise Informationssicherheit durch externe oder interne Angriffe gefährdet ist und ob die bereits getroffenen Maßnahmen ausreichenden Schutz bieten.

Die Überprüfung der IT-Komponenten, bezogen auf die durch den Schulträger beziehungsweise die Schule festgelegten IT-Sicherheitsstandards, sollte wiederholt im regulären Betrieb durchgeführt werden.

Tabelle 3: Kernfragen zum sicheren IT-Betrieb

Phase des Lebenszyklus (Auszug)	Kernfragen	Verantwortliche Person / Rolle	Empfehlungen und Erläuterungen
Regulärer Betrieb	Wird das Gerät regelmäßig gemonitort?	Schul-IT-Admin	Alle Komponenten, die durch die IT gestellt werden, sollten über ein Monitoring überwacht werden. Wenn ein Monitoring nicht möglich ist, sollte eine Abgrenzung durch separate Services, wie einen Internetzugriff über ein getrenntes WLAN, realisiert werden.
	Wird das Gerät systemseitig regelmäßig aktualisiert?	Schul-IT-Admin	Es ist wichtig, dass alle von der IT verantworteten Geräte regelmäßig gepatcht werden. Dabei sollten die Patches zunächst in einer Testphase auf korrekte Funktionen geprüft werden.
	Regelung bei Störungen (Defekt, Verlust etc.)	Schul-IT-Admin	Es sind Regeln für Störungen in der Strategie aufgestellt worden.

Zum regulären IT-Betrieb zählen sowohl die geplanten als auch vorhersehbaren Unterbrechungen. Diese können in einer zyklisch durchzuführenden Wartung und Systemaktualisierung begründet liegen. Konzeptionell werden die regulären IT-Betriebsunterbrechungen in einem IT-Betriebs- und Servicekonzept niedergeschrieben. Dieses inkludiert den Aufbau von IT-Services, deren Betrieb sowie die notwendigen Wartungen und stellt einen Bezug zum IT-Support her.

Für die Verknüpfung von IT-Betrieb/IT-Service und IT-Sicherheit sollte ein Ticketsystem eingeführt werden. Die Ticketsoftware im erweiterten Sinne wird als Software-Unterstützung für die Bearbeitung von Störungen (incidents) und Änderungsanträgen (changes) genutzt. Diese Tickets werden in den ersten Phasen der Software-Einführung meist von „menschlichen“ Nutzenden ausgelöst. In einer späteren Phase lohnt es sich, die „menschlichen“ Nutzenden um „maschinelle“ Komponenten zu erweitern. Diese können dann auch Störungen melden, mit dem speziellen Ziel, auch Anomalien zu melden.

Beispiel Schule:

Der Server meldet in der Nacht eine erhöhte Auslastung der CPU. Da eine übermäßige Nutzung des Servers in der Nacht zumeist ausgeschlossen werden kann, ist hier zu prüfen, ob ein Angriff auf das System erfolgt. Wenn die neuen Accesspoints überwacht werden, kann sofort erkannt werden, ob eine Person Zugriff auf diese hatte und sie für einen Angriff genutzt hat.

Eine Empfehlung der Phase 4 ist folglich, sich mit einer werkzeuggestützten Ticketverarbeitung auseinanderzusetzen und zügig über den Ausbau dieses Werkzeugs zu einem Security Information and Event Management (SIEM) nachzudenken.

2.5 Phase 5 – Rückbau

IT-Komponenten, die für eine Aussonderung oder Rückgabe (z. B. beim Leasing) vorgesehen sind, müssen bereinigt werden. Es dürfen keine Informationen der Organisation mehr auf dem Gerät vorhanden sein.

Mit Blick auf die IT-Sicherheit ist es darüber hinaus wichtig, die IT-Komponenten aus Asset-, Inventar- und Monitoringsystemen zu entfernen, sodass das Ausbleiben von Monitoringmeldungen nicht als vermeintlicher Sicherheitsvorfall eingestuft wird.

Tabelle 4: Kernfragen zum sicheren Rückbau von IT-Komponenten

Phase des Lebenszyklus	Kernfragen	Verantwortliche Person / Rolle	Empfehlungen und Erläuterungen
Rückbau	Rücklieferung des Geräts	Schul-IT-Admin	Das Gerät ist aus dem Monitoring und anderen Assetdatenbanken zu entfernen.
	Vernichtung von Speichermedien	Schul-IT-Admin	Um den Missbrauch von auf den Speichermedien noch befindlichen Informationen zu verhindern, sind die Medien fachgerecht (mit Zertifikat) zu entsorgen.

Die vollständige Übersicht über die Kernfragen ist den Anlagen zu entnehmen.

Beispiel Schule:

Accesspoints, die ausgemustert werden, sind kaum mehr nutzbar, da die Schule (aus meist finanziellen Gründen) nicht immer aktuelle Gerätegenerationen vorhält. Beim Rückbau ist es notwendig, alle Informationen, die Möglichkeiten bieten, auf den schulischen Betrieb zuzugreifen, zu löschen, bevor die Geräte entsorgt werden. Trotz des Alters oder einer Beschädigung ist davon auszugehen, dass diese von möglichen Angreifenden repariert oder in Teilen weitergenutzt werden können. Aus diesem Grunde muss eine sachgerechte Entsorgung durchgeführt werden.

3 Handlungsfelder

Das folgende Kapitel beschreibt die Handlungsfelder Planung und Beschaffung, IT-Betrieb sowie Notfallmanagement. Für jedes Handlungsfeld werden die Methodik und die zu beleuchtenden Aspekte dargestellt, die primär für dieses wichtig sind. Ein Fokus wird vor allem auf den Betrieb gelegt. Hier werden verschiedene Netzwerktypen dargestellt und deren Vor- und Nachteile erklärt.

Der Abschnitt Notfallmanagement geht intensiv auf die Reaktion auf einen Notfall sowie die vorzubereitenden Dokumente und Organisationsstrukturen ein, die die schnelle Beseitigung eines Sicherheitsvorfalls unterstützen, um zügig den normalen Betrieb wiederherzustellen.

3.1 Planung und Beschaffung: Komponenten und IT-Dienstleistungen

Die Planung und Beschaffung sind die ersten Schritte des Lebenszyklus von IT-Komponenten. Aus diesem Grunde sind diese beiden Phasen besonders wichtig im Hinblick auf die sicherheitsrelevanten Aspekte der Schul-IT. Wurden diese schon in der Planung berücksichtigt, wirkt sich dies auf den gesamten weiteren Prozess aus und bedingt eine sichere IT-Infrastruktur. Im folgenden Abschnitt werden die identifizierten IT-Komponenten dargestellt und zu beleuchtende Aspekte in Fragen formuliert.

3.1.1 Methodik

Aufbauend auf einem generischen Lebenszyklus von IT-Komponenten werden fünf Phasen definiert, in denen Verantwortliche Entscheidungen zu treffen und Handlungen durchzuführen haben. Kernaufgabe des regulären IT-Betriebs mit Bezug zur IT-Sicherheit sind die Prävention und die Detektion von Störungen und Vorfällen. Die Vorfälle werden im weiteren Verlauf auch als Cybervorfälle oder IT-Sicherheitsvorfälle konkretisiert.

Die Reaktion, als drittes Element der Dreiteilung gemäß dem Leitbild des BSI[6], kommt erst im Falle eines erfolgreichen Angriffs zum Tragen (siehe hierzu Abschnitt 3.3.5 zum Notfallhandbuch).

[6] https://www.bsi.bund.de/DE/Das-BSI/Leitbild/leitbild_node.html abgerufen am 23.12.2022.

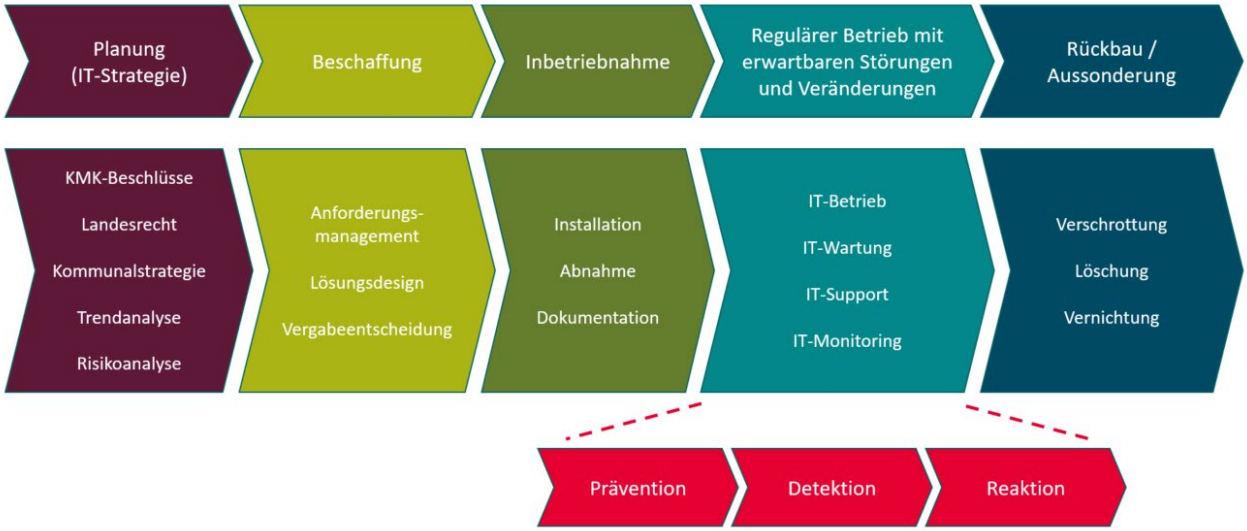

Abbildung 4: Generischer Lebenszyklus von IT-Komponenten

Jede Phase des Lebenszyklus dient der Einbettung von Sicherheitsmaßnahmen in den Lebenszyklus der IT-Komponenten.

3.1.2 Relevante Aspekte

Um Schulen für die IT-Sicherheit souverän und handlungsfähig aufzustellen, sollten folgende Aspekte beleuchtet werden:

1. Welche Handlungen und Prüfpunkte gibt es bei der Planung und Einführung von IT-Komponenten, inklusive Beschaffung und Abnahme?
2. Wie kann das Aufrechterhalten eines sicheren Betriebs der IT-Komponenten gewährleistet werden?
3. Wie werden geplante Unterbrechungen (z. B. Wartung, Systempflege) im regulären IT-Betrieb organisiert?
4. Werden die technischen Störungen über ein Ticketsystem verwaltet, stellt sich die Frage nach dem Ausbau des Ticketsystems für die IT-sicherheitsrelevanten Meldungen im Sinne eines SIEM.

Mit den zu untersuchenden Aspekten soll es verantwortlichen Personen möglich sein, frühzeitig innerhalb des Lebenszyklus einer IT-Komponente auf den Aspekt der IT-Sicherheit zu achten. Unter präventiven sowie detektierenden Gesichtspunkten ist jede Phase des Lebenszyklus ein Baustein, der dabei helfen soll, die Wahrscheinlichkeit eines erfolgreichen Cyberangriffs zu minimieren.

3.1.3 Identifizierte IT-Komponenten

Der Lebenszyklus findet Anwendung auf jede IT-Komponente. Für die Auswahl der IT-Komponenten greift die Handreichung auf die Empfehlungen der DigitalAgentur Brandenburg[7] zurück. Die folgenden IT-Komponenten wurden für den schulischen IT-Betrieb abweichend identifiziert:

1. Strom / Strom-Verkabelung / Steckdosen
2. Breitbandanschluss / DSL / 5G
3. WLAN
4. Netzwerkverkabelung
5. Etagenverteiler
6. Servertechnik / Firewalls / Router
7. Präsentationstechnik (Beamer, Großbildmonitore, elektronische Displays, Kameras etc.), Audio und Video
8. Endgeräte (Handy, Tablet, Notebook/PCs etc.)
9. Anwendungen (pädagogische / Schulverwaltung)

3.2 IT-Betrieb: Netzwerke, Internetzugang, Serverbetrieb, Endgeräte

Der IT-Betrieb bezieht sich auf die Netzwerke, den Internetzugang, den Serverbetreib und die Endgeräte. Alle genannten IT-Komponenten sollten den Sicherheitsrichtlinien der Schulträger und Schulen entsprechen. Im folgenden Abschnitt wird ein besonderer Fokus auf die Netzwerkstrukturen gelegt. Es werden drei verschiedene Varianten dargestellt und deren Vor- und Nachteile diskutiert.

3.2.1 Methodik

Bei der Bereitstellung von IT-Komponenten für den Schulverwaltungs- als auch den pädagogischen Bereich ist das Hosting von Anwendungen eine zentrale Entscheidungsgröße. Es darf aufgrund jüngster Entwicklungen davon ausgegangen werden, dass Schulen immer weniger ausschließliche Betreiber von Anwendungen sind. So ist nachvollziehbar, dass die Anwendungen für die Schulverwaltung meist durch die kommunale IT bereitgestellt werden.

Durch die Corona-Pandemie haben wiederum viele Cloud-Anwendungen (gehostet in kommunalen oder privat-wirtschaftlich organisierten Rechenzentren[8]) Einzug in die pädagogische Arbeit gehalten. Der Zugriff aus dem Schulcampus auf die extern bereitgestellten Anwendungen läuft über eine WAN-Infrastruktur.

[7] DigitalAgentur Brandenburg (2021): Orientierungshilfe zur IT-Basis-Ausstattung an Schulen im Land Brandenburg, https://www.digital-agentur.de/fileadmin/06_Bilddatenbank/Digitale_Bildung/DigitalPakt_Orientierungshilfe/DABB_Orientierungshilfe-IT-Basis-Ausstattung-an-Schulen_V1.2.pdf, Seiten 3-10, abgerufen am 20.11.2022.

[8] eGovernment, Susanne Ehneß (15.06.2020): Schul-Cloud des HPI. Die deutschen Schulen gehen in die Cloud, https://www.egovernment.de/die-deutschen-schulen-gehen-in-die-cloud-a-939742/, abgerufen am 23.12.2022.

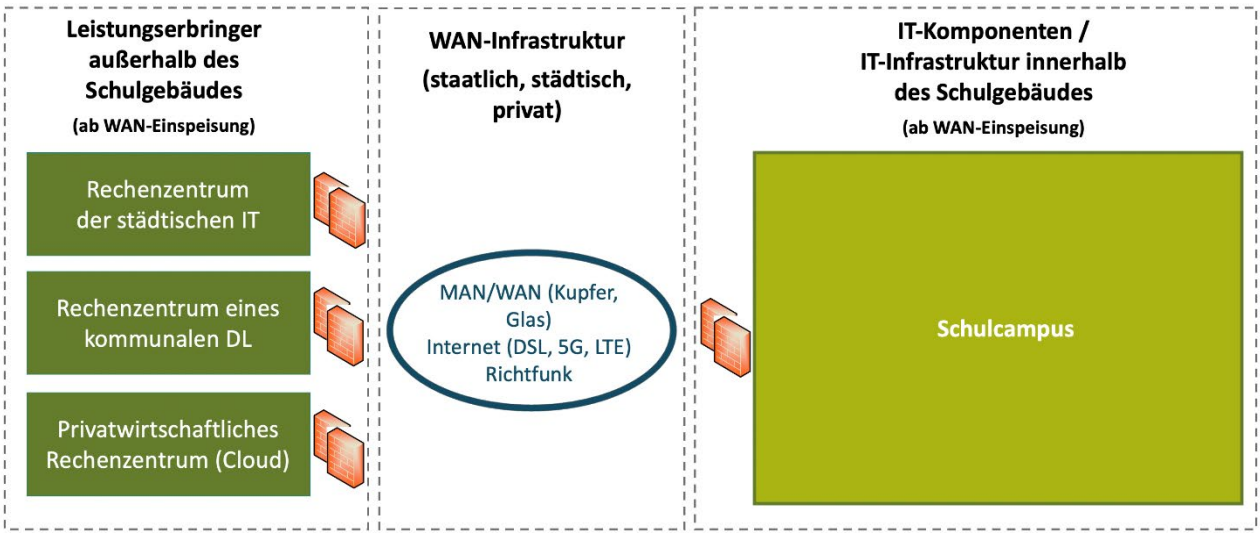

Abbildung 5: Schematische Darstellung des Zusammenwirkens von Dienstleistern, WAN-Infrastruktur und IT-Infrastruktur im Schulgebäude

Bei der Vertiefung der Frage, wie der IT-Betrieb mittels Netzwerks, Serverbetrieb und Endgeräte sicher erfolgen kann, wird der Fokus auf den Schulcampus gelegt. In einer beispielhaften Abstufung werden Netzwerk, Server und Endgeräte in drei Varianten projiziert, um auf mögliche Standardvorgehensweisen zu verweisen:

- eine Schule mit alleinstehendem Netzwerk (Variante 1),
- eine Schule mit Anbindung an ein kommunales Netzwerk und Rechenzentrum (Variante 2) und
- eine Schule mit Anbindung an ein regionales oder überregionales Netzwerk und Rechenzentrum (Variante 3) (siehe Abbildung 7).

Der klassische Aufbau einer IT-Infrastruktur ist seit Anfang der 1980er-Jahre in Schichten schematisiert worden.[9] Dieses Modell aufgreifend dient die folgende Darstellung dem Zusammenspiel verschiedener IT-Komponenten und der Betonung ausgewählter Zielobjekte. Dabei wird in erster Instanz zwischen dem Schulcampus, der Weitverkehrsvernetzung (WAN) und der IT-Infrastruktur der IT-Dienstleister unterschieden.

[9] International Organization for Standardization: OSI Referenzmodell: http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip, aufgerufen am 22.03.2023.

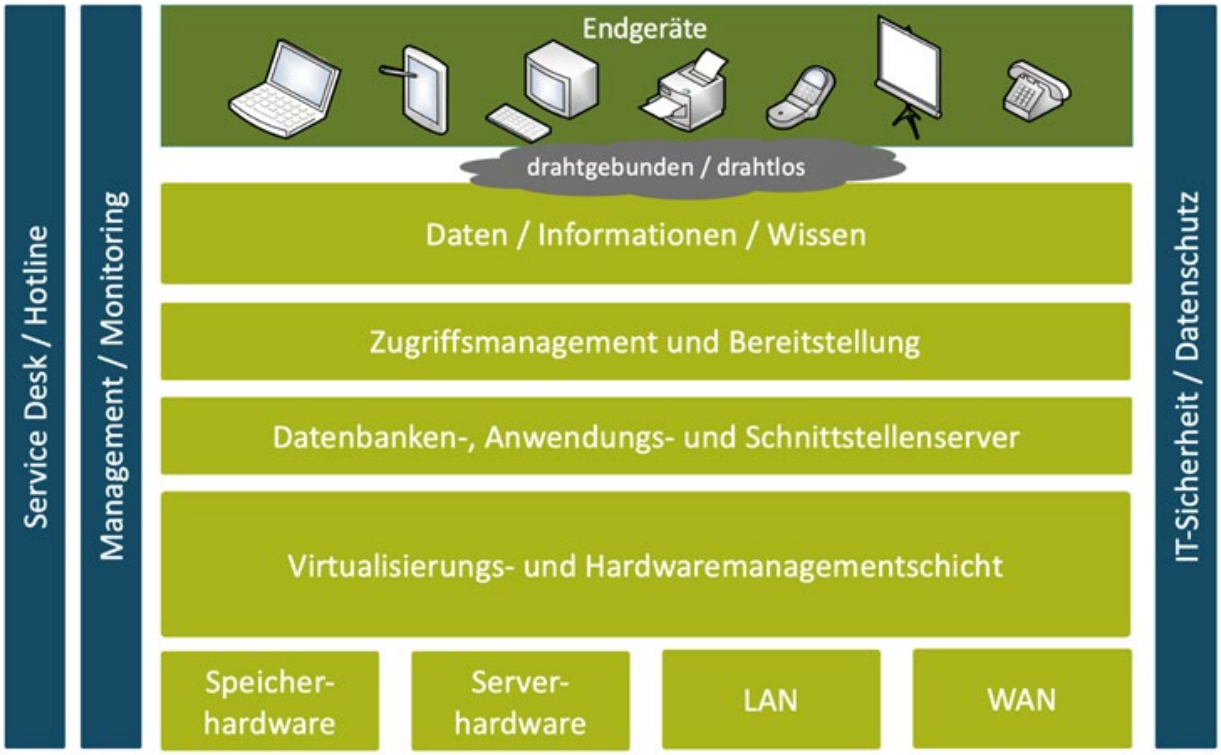

Abbildung 6: Schichtenmodell der im Schulcampus zum Einsatz kommenden IT-Komponenten

3.2.2 Relevante Aspekte

Um die Schulen für die IT-Sicherheit souverän und handlungsfähig aufzustellen, sollten folgende Aspekte beleuchtet werden:

1. Welche Varianten eines IT-Betriebs in Schulen gibt es?
2. Wie können die Bereitstellung von und der Zugriff auf externe IT-Services erfolgen?
3. Wie kann ein erfolgreiches Endgerätemanagement erfolgen?
4. Wie kann der Zugriff auf das Internet optimal gestaltet werden, um sowohl IT-Sicherheitsanforderungen als auch den Ansprüchen der Nutzenden zu entsprechen?
5. Wie werden geplante Unterbrechungen im regulären IT-Betrieb organisiert? (Werden die technischen Störungen über ein Ticketsystem einem Support zugeführt, empfiehlt sich perspektivisch der Einsatz einer äquivalenten Lösung für die Aufzeichnung von Anomalien in der IT-Infrastruktur.)

Kernfrage eines jeden schulischen IT-Betriebs (und IT-Supports) ist die Frage des Hostings. Hier wird unterschieden, inwieweit IT-Services, einschließlich der dazugehörigen IT-Komponenten, intern auf dem Schulcampus und/oder extern bei einem (Cloud-)Dienstleister gehostet werden. Es kann von einer MAKE-or-BUY-Entscheidung gesprochen werden. Um diese Entscheidung in IT-sicherheitsbezogene Überlegungen zu übersetzen, werden im Folgenden beispielhaft drei Varianten eines idealtypischen Schulnetzwerkes vorgestellt.

3.2.3 Typisierung der Schulvarianten

Diese Typisierung erfolgt durch Zuordnung von Merkmalen mit dem Schwerpunkt IT-Betrieb und IT-Support. Die Typisierung führt gezielt zu drei schematischen IT-Architekturskizzen, die in diesem Abschnitt dargelegt werden.

Die an dieser Stelle herausgearbeiteten Varianten stellen Idealtypen dar, die in dieser Eindeutigkeit nicht der Realität entsprechen.

Tabelle 5: Merkmal für die drei IT-Betriebs- und Supportvarianten

Merkmal	Variante 1 „Schule mit alleinstehendem NW (Netzwerk)“	Variante 2 „Schule mit Anbindung an kommunales NW & RZ (Rechenzentrum)“	Variante 3 „Schule mit Anbindung an regionales oder überregionales NW & RZ“
Kriterium	Keine Anbindung an kommunales Netzwerk	Netzwerkanbindung an kommunale IT zur Nutzung kommunaler RZ-Ressourcen (Regiebetrieb)	Anbindung an ein von einem externen IT-Dienstleister betriebenes Netzwerk zur Nutzung von weiteren RZ-Ressourcen
Netzwerkinfrastruktur	LAN-Infrastruktur: Typischerweise DSL-Router für Internetzugang	MAN-Infrastruktur: Teilweise über kommunales Netz; teilweise über eigenen Glasfaseranschluss	WAN-Infrastruktur: Meist durch landes- oder interkommunales Netz gegeben, was Voraussetzung für den Bezug der IT-Services des kommunalen oder privatwirtschaftlichen Dienstleisters ist
IT-Steuerung	Schulleitungen in Fragen IT-Betrieb und IT-Sicherheit größtenteils auf sich gestellt; einzelne Lehrkräfte sind mit Kontingentstunden für IT-Aufgaben zuständig	Schulleitungen in Fragen IT-Betrieb und IT-Sicherheit mit kommunaler IT im Kontakt – meist über Schul-IT; Lehrkräfte verfügen über Kontingentstunden für IT-Aufgaben	Schulleitung steht mit kommunalem Dienstleister in Kontakt; Lehrkräfte verfügen über Kontingentstunden und sind für IT-Aufgaben zuständig: teilweise erfolgt eine Zusammenarbeit mit der Schul-IT der Stadt
IT-Betrieb	Typischerweise allein auf dem Schulcampus	Teilweise eigenständig auf dem Schulcampus, teilweise in kommunaler IT-Hoheit (z. B. für Schulverwaltungsanwendungen)	Größtenteils über den kommunalen oder privatwirtschaftlichen Dienstleister; in Abstimmung mit der Schulverwaltung; teilweise in Abstimmung mit der Schul-IT (städtisch)
IT-Support	Meist nur schuleigener Administrator und nur situativ und reaktiv vorhanden	Vorhanden, aber nicht immer mit ausreichend Personal ausgestattet, um Support auch im Ernstfall umsetzen zu können	Vorhanden und meist umsetzbar
IT-Sicherheit	Kaum gegeben und kaum dokumentiert	In Ansätzen durch die kommunale IT gegeben; teilweise dokumentiert; teilweise durch externen ISB überwacht	Meist durch die DL gegeben und auch eingefordert; gut dokumentiert; durch ISB oder SoC/CERT des DL gut überwacht (einschließlich regelmäßiger Pen-Tests)

Variante 1

Dieser Variante liegt die Annahme zugrunde, dass es Schulen gerade in der Trägerschaft von Kleinstkommunen gibt, bei denen die Verantwortung für den IT-Betrieb allein in der Schule liegt und die IT-Sicherheit von Schulleitung, IT-Mitarbeitenden und/oder IT-affinem Lehrpersonal übernommen wird.

Unter dieser Annahme besteht netzwerkseitig zumeist eine einfache und nicht redundant betriebene Kabel-/DSL-Anbindung in das Internet – meist über herkömmliche Privatverbrauchertechnik (z. B. eine FritzBox oder einen Router). Alle weiteren IT-Komponenten und Anwendungen werden auf einem oder mehreren Servern an einem mehr oder weniger geeigneten Platz innerhalb des Schulcampus betrieben.

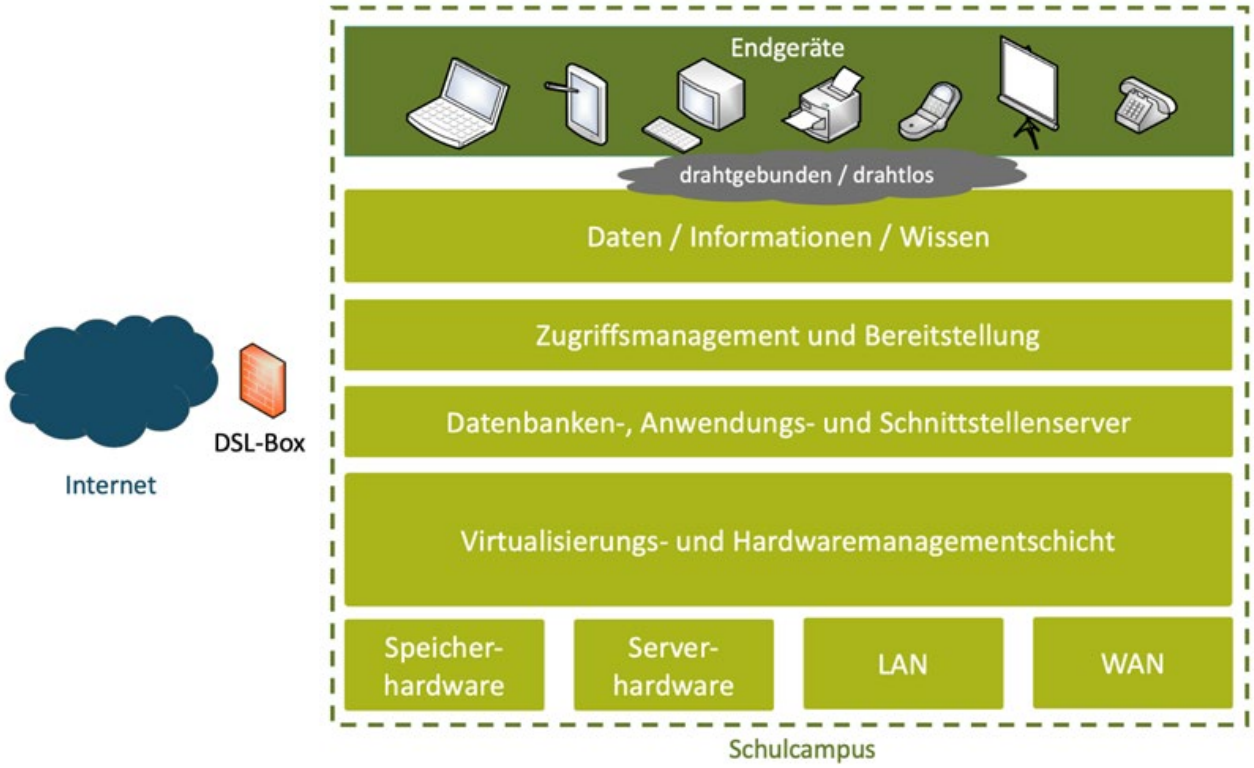

Abbildung 7: Schichtenmodell mit IT-Betrieb auf dem Schulcampus-Typ Variante 1 „Schule mit alleinstehendem NW (Netzwerk)“

Im Wissen um die Komplexität und Anforderungen bei der Aufrechterhaltung des IT-Betriebs und der damit einhergehenden Absicherung von Schwachstellen beginnen viele Kleinstkommunen, ihre Technik an privatwirtschaftlich organisierte IT-Dienstleister zu vergeben. Die Herausforderungen bestehen darin, alle IT-Komponenten auf dem Schulcampus (und beim Dienstleister) zu verwalten, deren Betrieb ausfallsicher aufrechtzuerhalten und potenzielle Schwachstellen schnellstmöglich zu schließen. Ein Ausfall des wenigen, qualifizierten IT-Personals führt immer wieder zu kritischen Zuständen. Deshalb wird auch für den Schultypus der Variante 1 empfohlen, perspektivisch in weiteres Personal und eine verstärkte Dienstleisterorientierung zu investieren.

Eine wesentliche Schwachstelle ist die Verbindung zum Internet. Für diesen Zugriff sollte mindestens eine logische, wenn möglich physische, Netztrennung von Verwaltungs- und pädagogischem Netz konfiguriert sein. Zum Schutz der jeweiligen Netzwerksegmente ist es wichtig, dass die zum Einsatz kommenden IT-Komponenten, die die verschiedenen Netzwerksegmente miteinander verbinden besonders zu schützen:

- DSL-Modem oder Kabelmodem
- Router / Multiprotokoll-Router
- Managed Switch (mit der Möglichkeit, mehrere VLANs einzurichten)
- Accesspoint für WLAN (mit der Möglichkeit, mehrere SSIDs einzurichten)

Gängige „DSL-Boxen“ für den Heimanwenderbereich, wie in Abbildung 7, skizziert, bieten den geforderten Funktionsumfang nur sehr eingeschränkt. Sollten diese dennoch beispielsweise aus wirtschaftlichen Gründen eingesetzt werden, sollte der notwendige Funktionsumfang durch weitere Komponenten sichergestellt werden. Um nicht zwingend auf teure Produkte von Markenanbietern angewiesen zu sein, wird ein Blick auf den Open-Source-Markt empfohlen.

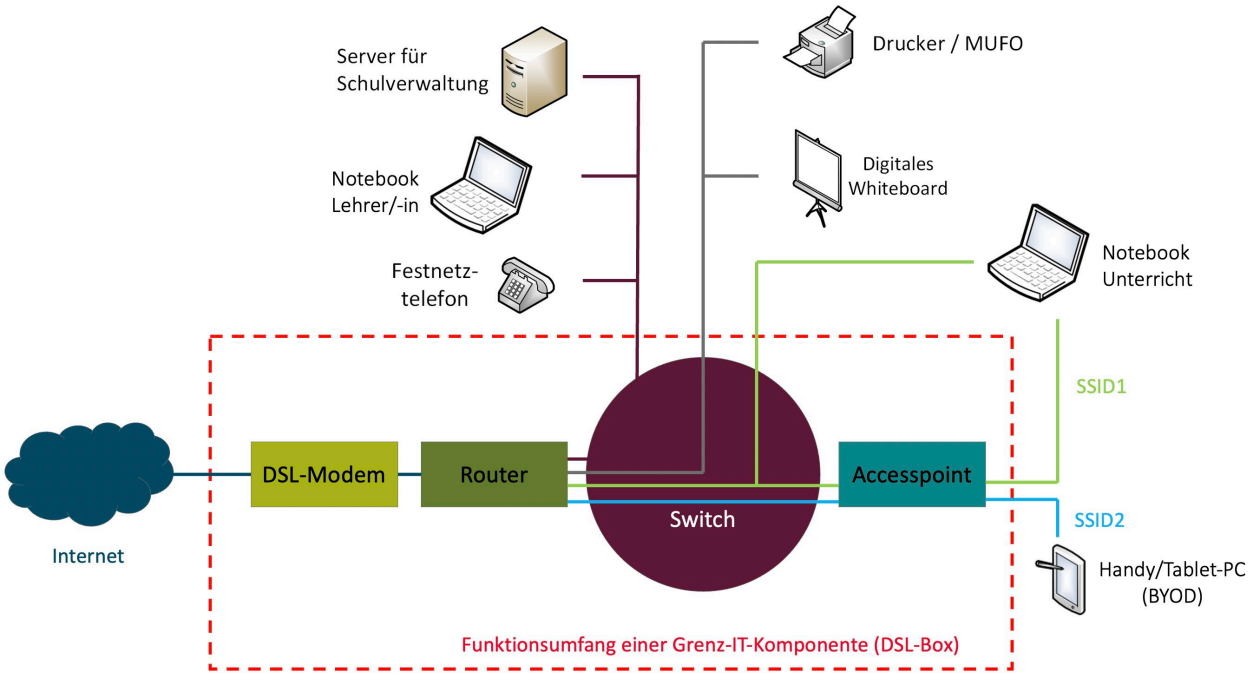

Abbildung 8: Funktionsumfang der Abgrenzung zum WAN mit vier VLANs

In Abbildung 8 ist der beispielhaft dargestellte Router (DSL-Box) mit vier VLANs konfiguriert. Dazu werden zwei SSIDs ausgestrahlt. Einzig das Unterrichts-Notebook kann drahtlos und drahtgebunden an das schulische Netzwerk angeschlossen werden. Das BYOD-Gerät wird nur mit dem Internet verbunden.

In der Fortführung der Konfigurationsmöglichkeiten wird folgende Soll-Netzwerkarchitektur für den Schultyp der Variante 1 empfohlen:

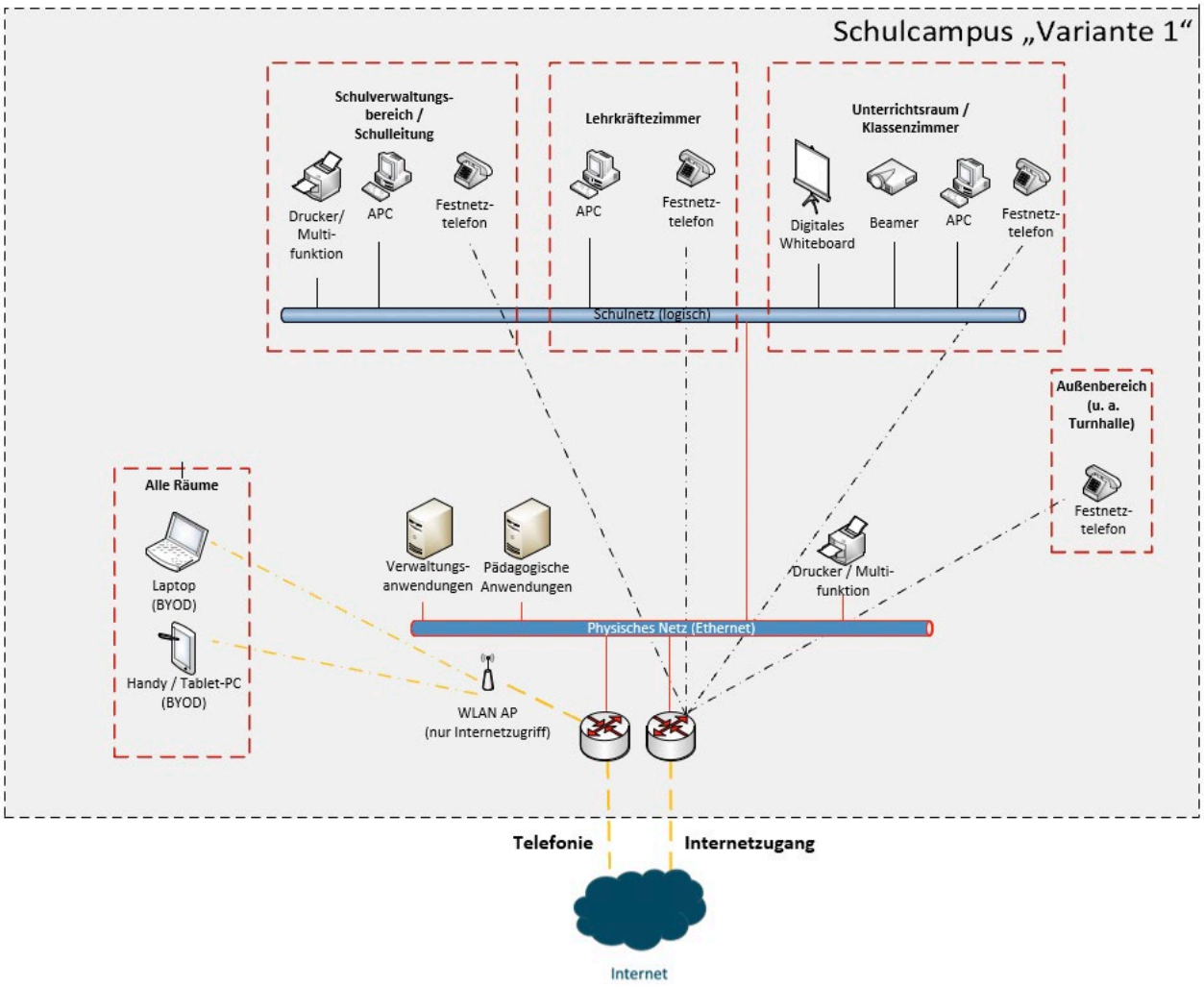

Abbildung 9: Netzwerkplan Schulcampus-Typ Variante 1

Abweichend von Abbildung 7 wird in Abbildung 9 für die Abgrenzung zum WAN eine redundante Auslegung empfohlen. Demnach sind die redundanten Komponenten identisch zu den Produktivsystemen zu konfigurieren, sodass diese im Notfall die Produktivsysteme sofort ersetzen können. Schematisch ist in Abbildung 9 die Telefonie auf der redundanten Abgrenzung zum WAN (hier: Router) realisiert worden. Alle Anwendungen des pädagogischen sowie des Verwaltungsnetzes werden drahtgebunden bereitgestellt.

Der WLAN-Access-Point ist nur für BYOD-Geräte der Schülerinnen und Schüler, der Lehrkräfte und der Schulleitung eingebunden. Für den Unterrichtsbetrieb wurden in der Grafik exemplarisch nur Arbeitsplatz-PCs dargestellt.

Variante 2

Diese Variante beschreibt Schulträger mit einer hohen Integration in die kommunale IT. Hier werden beispielsweise Schulverwaltungsanwendungen, der zentrale Helpdesk oder ein zentrales Mobile Device Management vom kommunalen Rechenzentrum bereitgestellt. Häufig ist durch die Anbindung an die kommunale IT auch der Internetzugang realisiert. Ungeachtet dessen werden häufig auch auf dem Schulcampus pädagogische und weitere Anwendungen durch die Schule bereitgestellt.

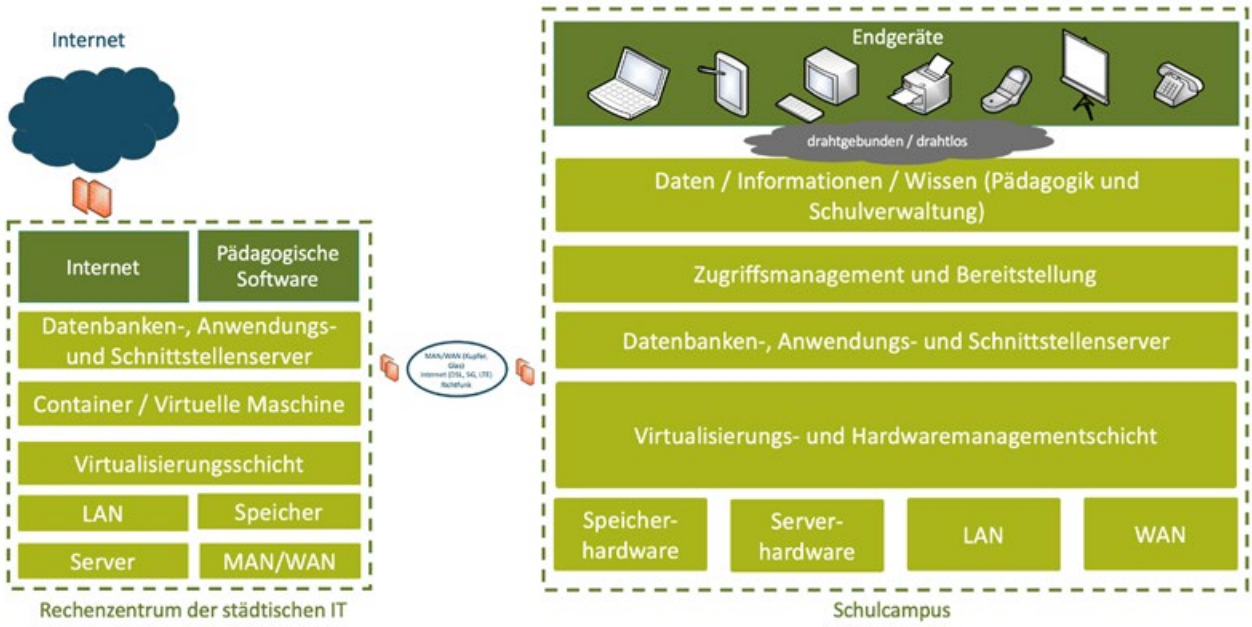

Abbildung 10: Schichtenmodell mit IT-Verantwortlichkeit beim Schulcampus-Typ Variante 2 „Schule mit Anbindung an kommunales NW & RZ (Rechenzentrum)“

In dieser Variante ist es notwendig, dass die Schule über Netzwerktechnik zum Anschluss von beispielsweise Glasfaser, Richtfunk, 5G verfügt, um über das kommunale MAN (Metropolitan Area Network) zu kommunizieren. Zu „kommunizieren“ bedeutet in diesem Fall, auf zentrale Services der städtischen IT, wie E-Mail, Internet und Telefonie, zuzugreifen beziehungsweise für pädagogische Anwendungen auf die Cloud zuzugreifen.

Unter Berücksichtigung der Gesichtspunkte Störung und/oder Vorfall sollte ein redundanter (Glasfaser-) Ring beziehungsweise eine getrennte Einspeisung durch einen weiteren Provider abgewogen werden. Klassisch werden die Anforderungen an die Schul-IT nicht die zu vermutenden Kosten begründen, aber es empfiehlt sich, dass sich die IT-Teams mit dem Thema auseinandersetzen.

Abbildung 11 zeigt eine Netzwerkdarstellung, bei der per VLAN getrennte Netze über einen Glasfaser-Backbone mit einem städtischen Rechenzentrum verbunden sind und der Backbone auch genutzt wird, um einen Zugriff auf das Internet zu haben.

Schematisch skizziert wird folgende Netzwerkarchitektur mit kommunaler Anbindung empfohlen:

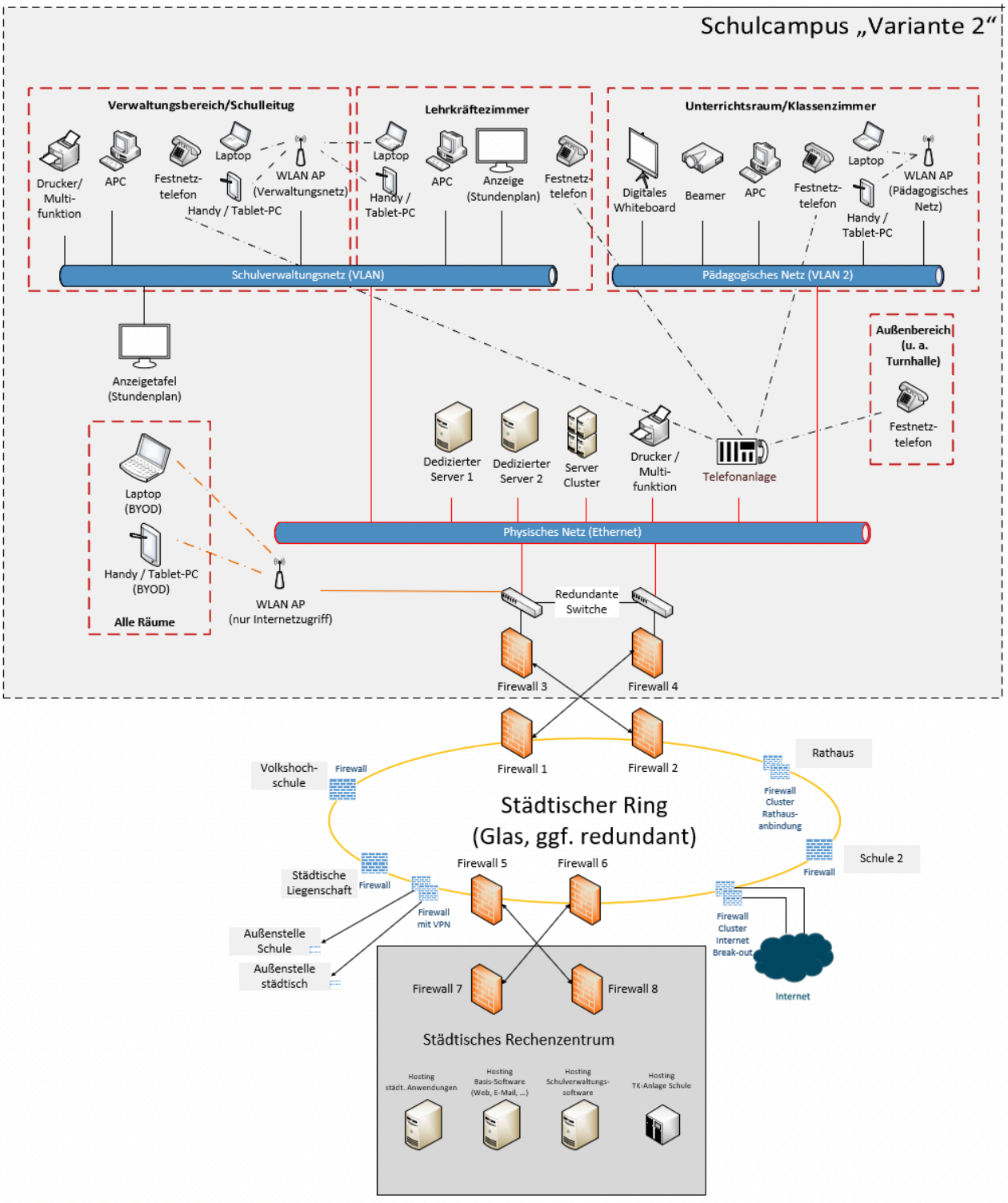

Abbildung 11: Schulcampus-Typ Variante 2 „Schule mit Anbindung an kommunales NW & RZ (Rechenzentrum)“

In Abbildung 11 werden IT-Services der kommunalen IT genutzt, deren IT-Komponenten in einem Rechenzentrum verbaut sind. Über eine hoch redundante WAN-Anbindung, auch als Grenz-IT-Komponente bezeichnet, wird das Ausfallrisiko für den Zugriff auf das kommunale Rechenzentrum minimiert.

Variante 3

Diese Variante beschreibt die Anbindung der Schulen an ein von einem externen IT-Dienstleister betriebenes Netzwerk (Rechenzentrum). Neben der Möglichkeit, eine zentrale IT des Kreises und deren Rechenzentrumskapazitäten zu nutzen, bieten sich sowohl kommunale als auch privatwirtschaftlich organisierte Rechenzentrumsdienstleister an.

Selbst die Schulcampus-Verkabelung, die Accesspoints und die WAN-Einspeisung können in der Verantwortung des externen Dienstleisters liegen. Damit reduziert sich der Aufwand für eine interne Schul-IT.

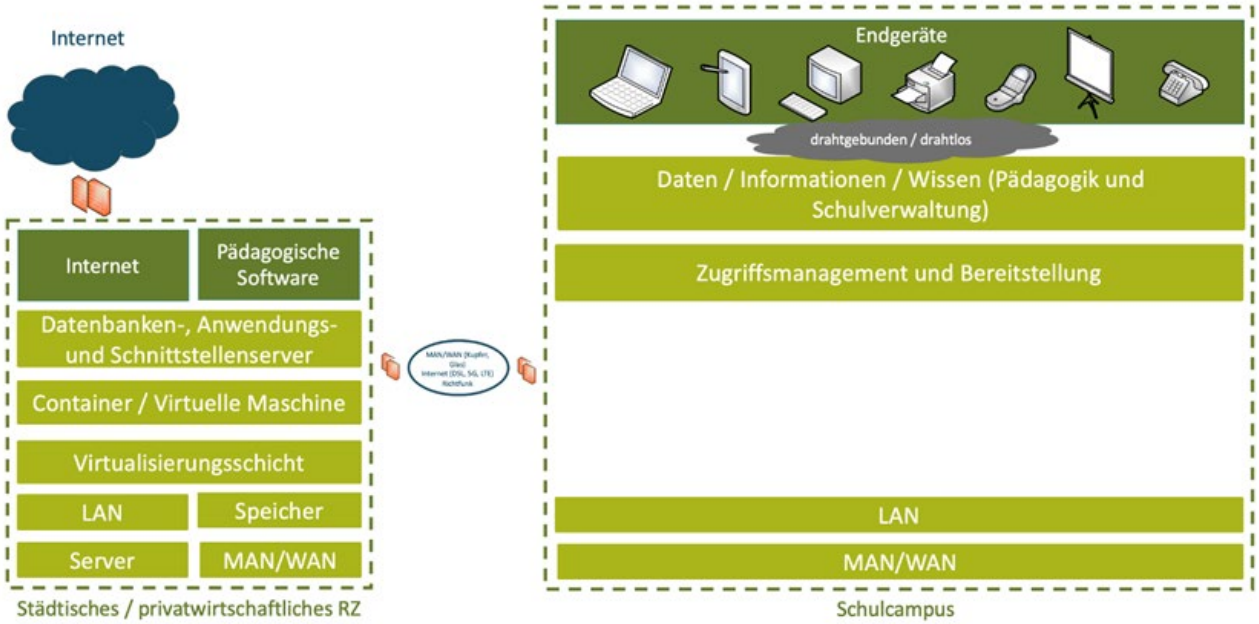

Abbildung 12: Schulcampus mit Anbindung an ein regionales oder überregionales Netzwerk und Rechenzentrum

Damit die im Rechenzentrum betriebene IT-Infrastruktur im Schulcampus genutzt werden kann, ist es zwingend erforderlich, einige IT-Komponenten dennoch im Schulcampus zu verwalten. Dazu gehört vor allem die Netzwerktechnik.

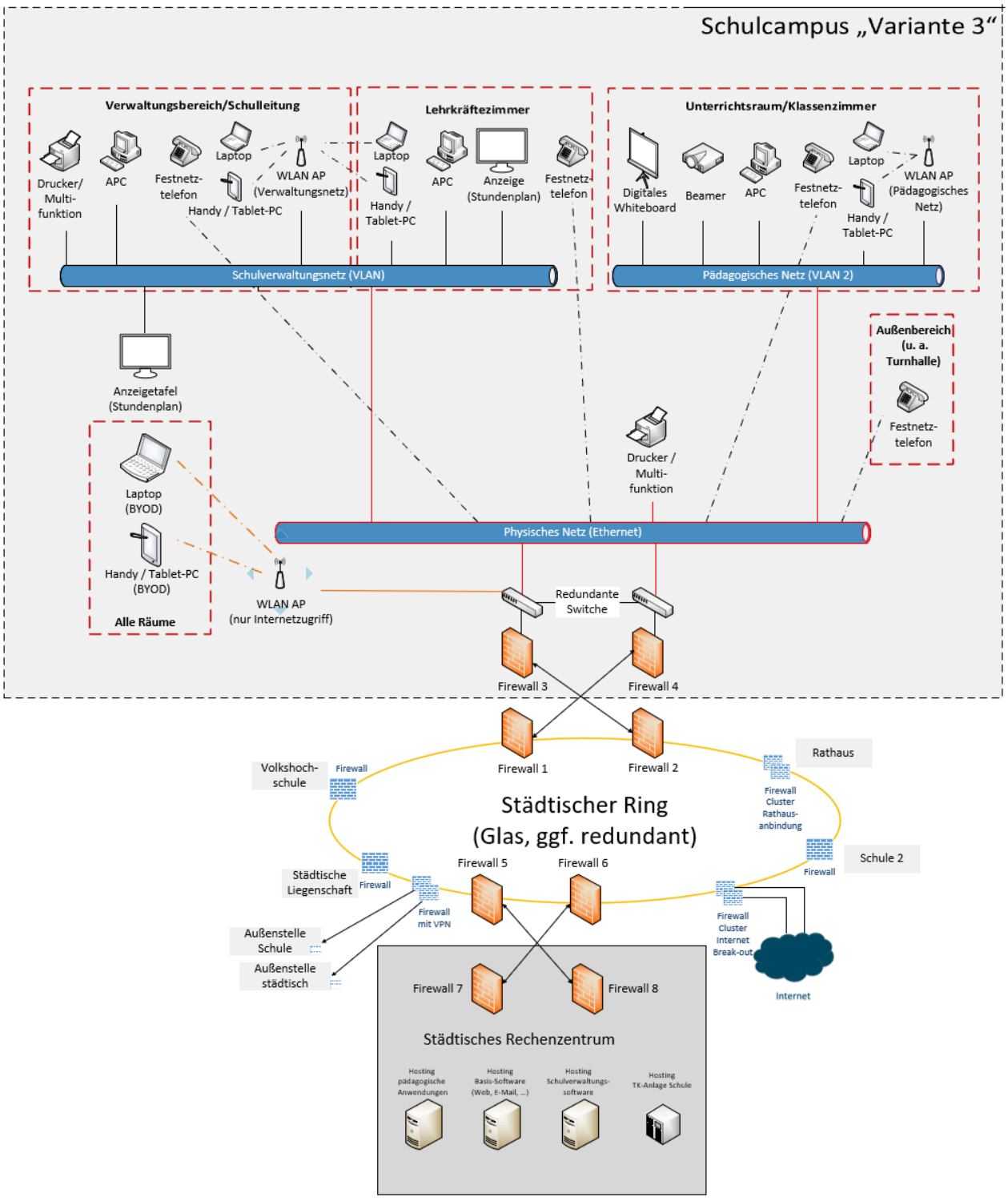

Abbildung 13: Schulcampus-Typ Variante 3 „Schule mit Anbindung an regionales oder überregionales NW & RZ“

VLAN als Teil der IT-Infrastruktur

Bei einem VLAN handelt es sich um ein logisches Netzwerksegment eines physischen Netzwerks (LAN). Diese Technik wird eingesetzt, um beispielsweise Datenverkehr zu priorisieren oder Datenströme logisch zu trennen. Über ein einziges Netzwerkkabel lassen sich mehrere logisch separierte VLANs gleichzeitig übertragen und können sich auch über mehrere Switche hinweg erstrecken.

Mithilfe von konfigurierbaren (managed) Switches lassen sich einzelne Ports fest einem VLAN zuordnen. Ebenso können sich diese logischen Netzwerksegmente auf ein oder mehrere WLANs erstrecken. Sofern Multi-SSID-fähige Accesspoints eingesetzt werden, können mehrere WLANs gleichzeitig angeboten werden und eine Trennung der einzelnen Segmente ist weiterhin gegeben.

Im Fall der drei vorgestellten Varianten könnten VLANs wie folgt umgesetzt werden:

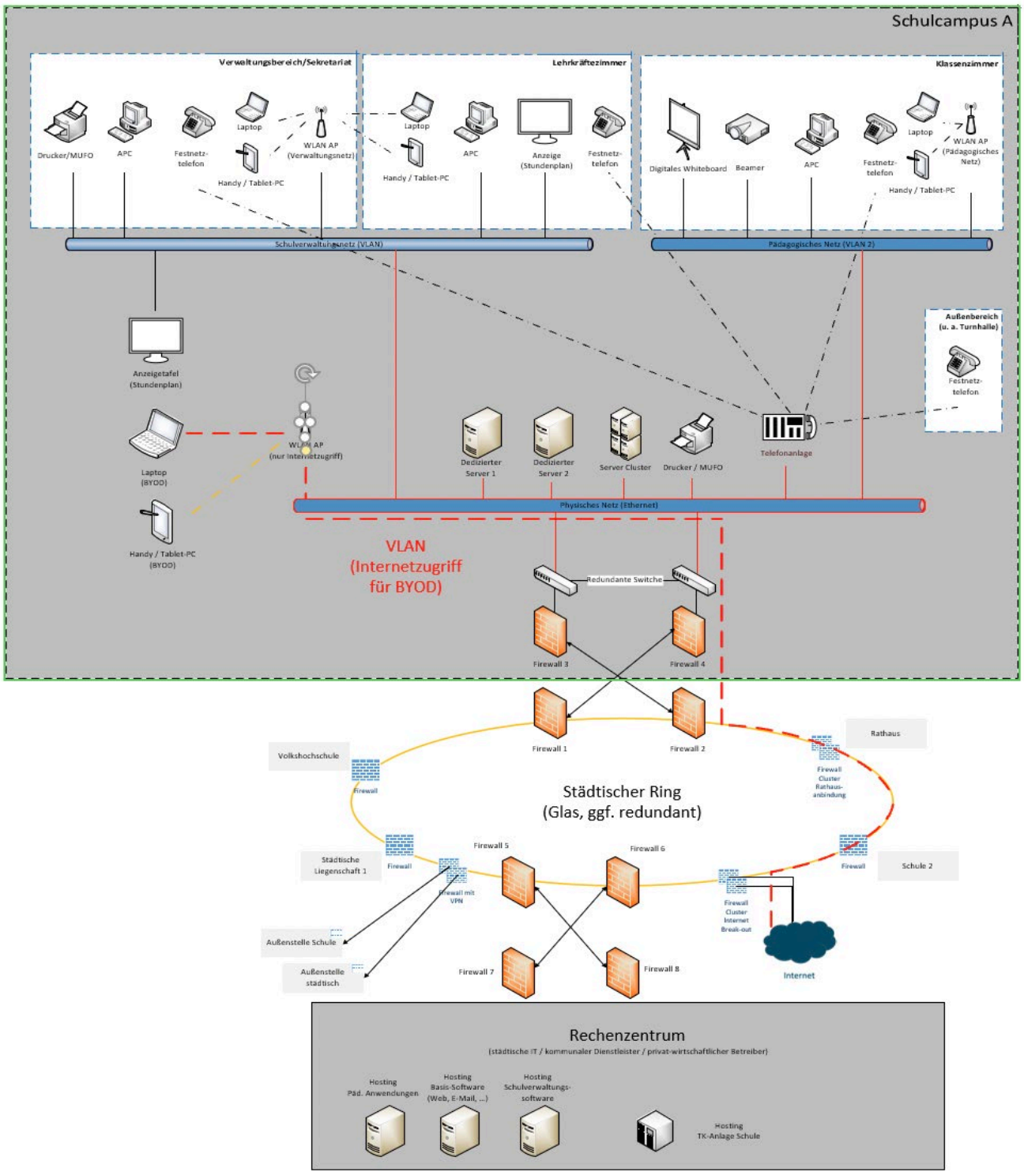

Abbildung 14: Mögliche VLAN-Konstellation (1)

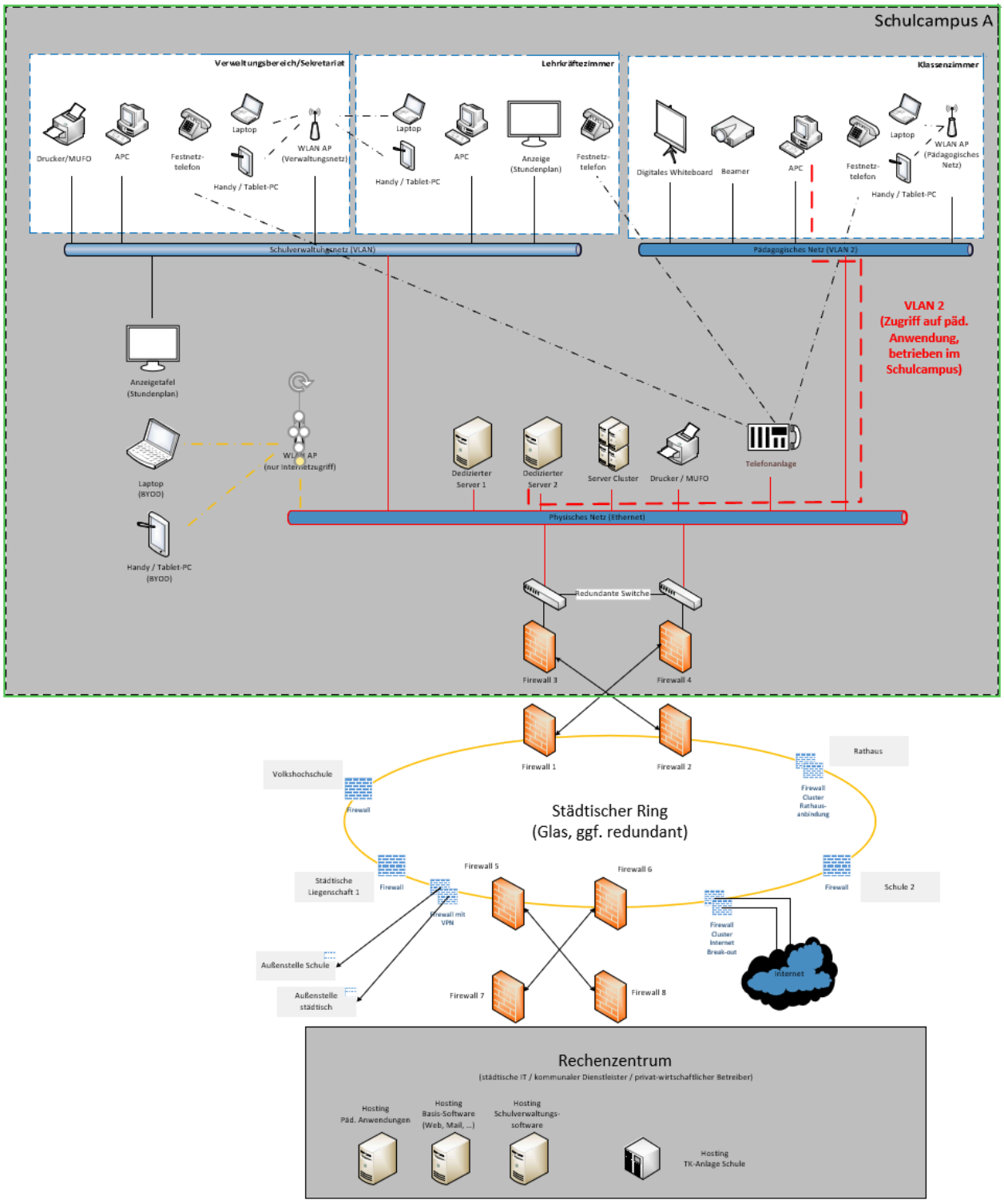

Abbildung 15: Mögliche VLAN-Konstellation (2)

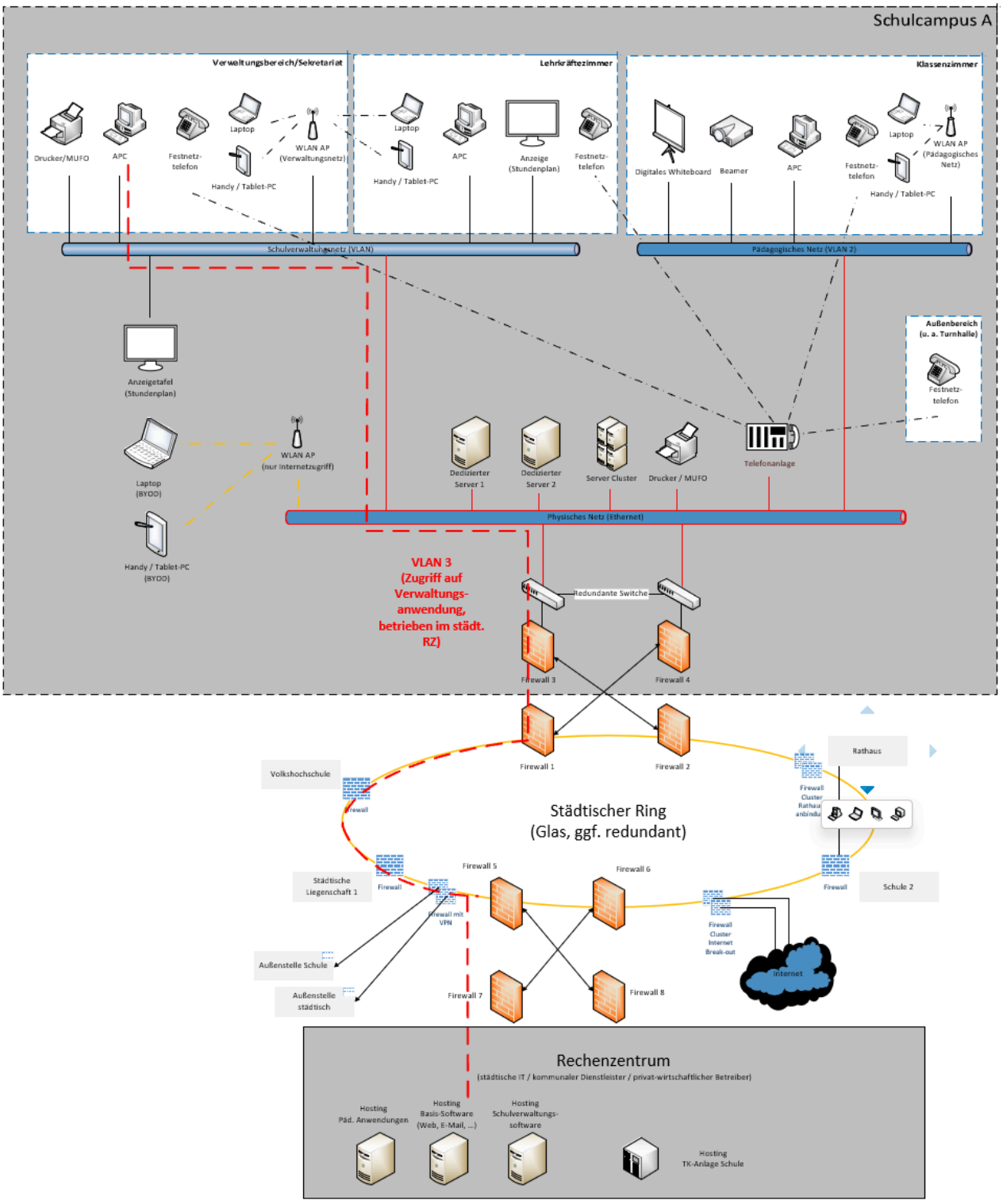

Abbildung 16: Mögliche VLAN-Konstellation (3)

3.3 Notfallmanagement

Das (klassische) Notfallmanagement wird im BSI-Standard 100-4 beschrieben. Notfallmanagement ist der (komplexe) Prozess, der sowohl die Notfallvorsorge, die Notfallbewältigung als auch die kontinuierliche Verbesserung des Notfallmanagementprozesses umfasst. Um einen solchen Prozess etablieren und aufrechterhalten zu können, ist ein effizientes Managementsystem notwendig.[10]

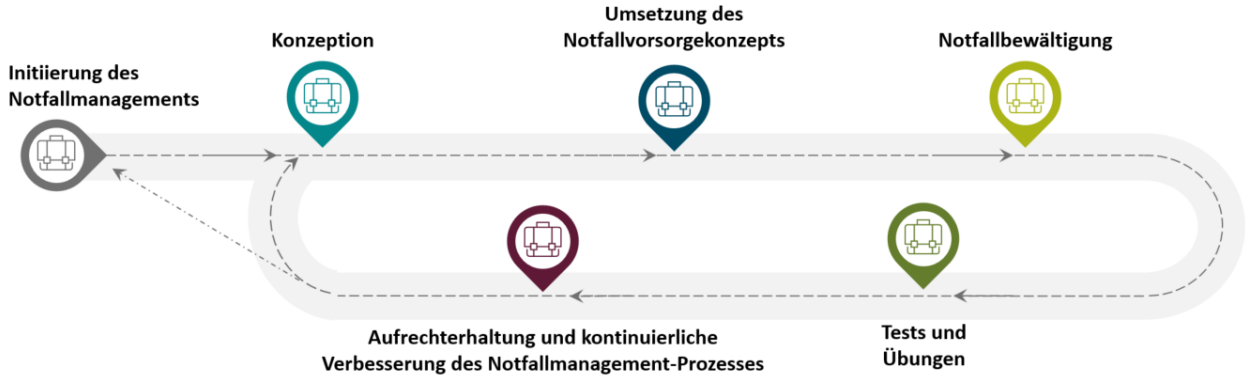

Abbildung 17: Notfallmanagement – Prozess gemäß BSI-Standard 100-4 Notfallmanagement

Mit den im Frühjahr 2023 zu erwartenden Neuerungen des BSI wird der BSI-Standard 100-4 Notfallmanagement vom BSI-Standard 200-4 Business Continuity Management (BCM) abgelöst. Dies ist eine Weiterentwicklung des Notfallmanagements, das damit vor allem eine ganzheitliche Betrachtung des Notfallmanagements mit dem Fokus auf die Resilienz erfährt.

Darüber hinaus werden ergänzende Prozessschritte in diesem Dokument enthalten sein. Da an dieser Stelle zunächst grundlegend auf das Notfallmanagement eingegangen werden soll und die Neukonzeption noch nicht final veröffentlicht wurde, wird hier zunächst auf die Version 100-4 referenziert.

Die Ziele eines Notfallmanagements sind die Aufrechterhaltung der notwendigen Geschäftsprozesse sowie die Minimierung der Auswirkungen eines Schadensereignisses.

3.3.1 Methodik

Die Behandlung von IT-Sicherheitsrisiken ist dem IT-Risiko- und IT-Notfallmanagement zuzuordnen. Wird ein Information Security Management System (ISMS) gemäß ISO 27001 umgesetzt, steht die Risikoanalyse am Beginn des Prozesses.

Im IT-Grundschutz gemäß BSI folgt das Risikomanagement den Standards 100-3 beziehungsweise 200-3. Die Grundschutzsystematik orientiert sich an den Zielobjekten, die in Bausteine untergliedert und mit Maßnahmen verknüpft werden.

Die sich daraus ergebende Kaskade von Zuordnungen soll helfen, IT-Sicherheitsanforderungen bezogen auf Zielobjekte (IT-Komponenten) zu strukturieren und umzusetzen. In dieser Kaskade werden Bausteine, Maßnahmen und handelnde Personen miteinander verknüpft. Je nach Umfang der Zielobjekte wird diese um Zielobjektgruppen erweitert. Zielobjekte beziehungsweise Zielobjektgruppen gehören wiederum zu einem Informationsverbund (siehe HR 1).

[10] BSI-Standard 100-4, 2008, Seite 10.

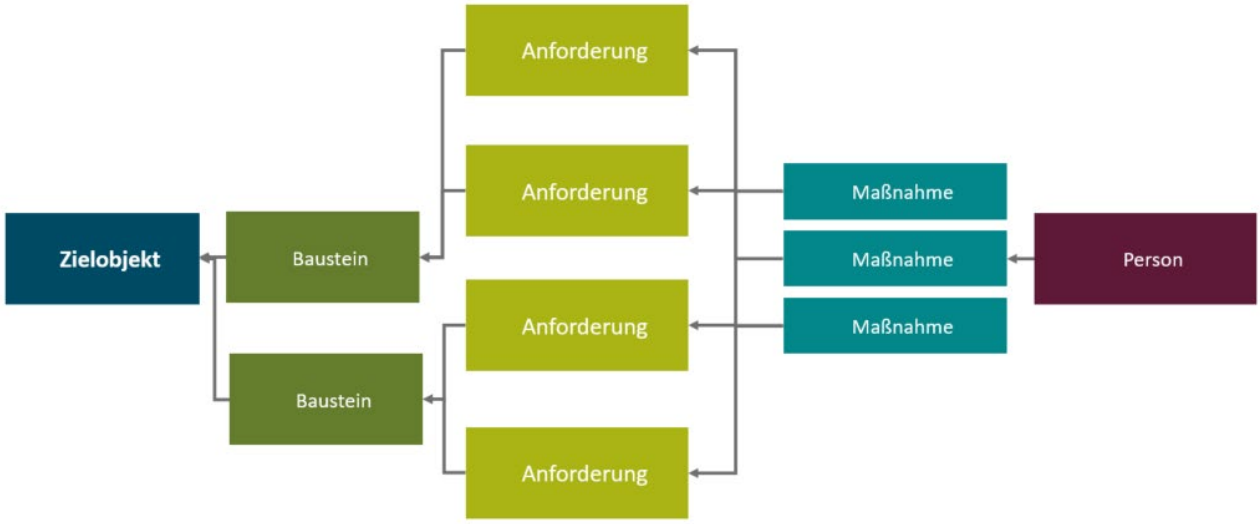

Abbildung 18: Datenmodell in der Perspektive des modernisierten BSI-Grundschutzes

3.3.2 Relevante Aspekte

Um Schulleitungen, Schulverwaltungen und IT-Verantwortliche zur Vorsorge und im Falle eines erfolgreichen Cyberangriffs bei der Wiederherstellung des normalen IT-Betriebszustands zu unterstützen, gilt es, einige zentrale Punkte zu beachten, die an dieser Stelle als Fragen formuliert sind:

1. Was ist Notfallmanagement?
2. Was beinhaltet ein Notfallmanagement?
3. Was sind die ersten Schritte nach dem Entdecken eines erfolgten Cyberangriffs?
4. Welche Organisationsstrukturen haben sich bewährt?
5. Wer steht außerhalb der erweiterten Schulorganisation als Unterstützung zur Seite?

3.3.3 Notfallleitlinie

Um ein Notfallmanagement beim Schulträger und den Schulen zu etablieren, ist es sinnvoll, eine Notfallleitlinie zu schreiben. Diese fokussiert neben der Zielsetzung und Definition des Notfallmanagements vor allem auf:

— die Notfallstrategie,
— die wichtigsten Rollen und Zuständigkeiten,
— die regelmäßige Überprüfung der Notfallstrategie durch Tests und Übungen,
— relevante Gesetze, die zu beachten sind.

Diese Notfallleitlinie sollte allen Mitarbeitenden bekannt gemacht werden.

Ein professionelles Notfallmanagement bedingt organisatorische Strukturen. Schulen und Schulverwaltungen stehen beim Aufbau dieser Strukturen noch am Anfang. Folglich müssen die empfohlenen Rollen und Verantwortungen für ein solches Management durch wenige, schon im Schulalltag eingebundene Kolleginnen und Kollegen übernommen werden.

Der an dieser Stelle empfohlene Ansatz ist auf Schulen anwendbar und soll einen Einstieg in ein Notfallmanagement ermöglichen. Für den Aufbau eines Notfallmanagements werden die folgenden Entscheidungen und Umsetzungsschritte als zwingend notwendig eingestuft:

- Beziehen Sie Position, dass ein Notfallmanagement notwendig ist, und verankern Sie dessen Aufbau in der (Kommunal-)Strategie.
- Planen und kalkulieren Sie personelle und finanzielle Ressourcen ein.
- Spielen Sie den Notfall durch. Legen Sie feste Zeitpunkte fest, an denen Sie den Notfall eintreten lassen.
- Planen und führen Sie regelmäßig Penetrations- und Angriffstests gesteuert durch.
- Erstellen Sie Notfalldokumente in Papier und stellen Sie sicher, dass alle Beteiligten die Ablageorte kennen.
- Statten Sie die Führungs- und Expertenebene mit autarken Kommunikationskomponenten aus, sodass beim Ausfall der Telefonie durch den Cybervorfall eine Kommunikation möglich ist.

3.3.4 Notfallvorsorgekonzept

Um ein Notfallvorsorgekonzept zu erstellen, ist es notwendig, eine Analyse der Prozesse durchzuführen, die zwingend für die Aufrechterhaltung des IT-Betriebs notwendig sind. Dies bedeutet, dass Schulen und Schulträger zunächst festlegen müssen, welche Prozesse einzuhalten sind, um den Schulbetrieb permanent aufrechterhalten zu können.

In einem zweiten Schritt ist die Kritikalität der Prozesse für den Schulbetrieb einschließlich der zugehörigen IT festzulegen. Um bei der Bestimmung der Kritikalität einen Anhaltspunkt zu haben, helfen Szenarien (BSI-Szenario-Technik), wie diese immer häufiger in der realen Welt zu erleben sind. Die folgenden zwei Szenarien sollen als Beispiele dienen.

Beispiel 1: Schule ohne Internetzugriff

Das Internet fällt in einer Schule am Morgen der Einschulung aus. Die Namen der Schülerinnen und Schüler sowie die Klassenzuordnungen können nicht vom zentralen Verwaltungsserver abgerufen werden.

Beispiel 2: Schule ohne Zugriff auf die internen Anwendungen

Die IT einer Schule wird durch den Angriff mit einer Schadsoftware „lahmgelegt“. Es ist kein digital unterstützter Unterricht mehr möglich.

Mittels solcher Szenarien können mögliche Auswirkungen eines Angriffs durchgespielt und geeignete Wiederherstellungsmaßnahmen definiert werden.

In einem weiteren Schritt können zusätzliche Parameter, wie die höchste tolerierbare Ausfallzeit und die Abhängigkeit der Prozesse voneinander, analysiert werden.

Im Ergebnis ist das Notfallvorsorgekonzept die Grundlage zur Aufrechterhaltung des IT-Betriebs (BSI-Kontinuitätsstrategie), das auch alle „organisatorischen und konzeptuellen Aspekte sowie alle Maßnahmen und Tätigkeiten des Notfallmanagements, die nicht zur direkten Bewältigung des Notfalls beitragen“[11], enthält. Damit fällt das Notfallkonzept in den Bereich der Prävention (siehe auch Abschnitt 3.2.1 zur Methodik).

Warum Vorsorgemaßnahmen notwendig sind?

[11] Bundesamt für Sicherheit in der Informationstechnik (2008): BSI-Standard 100-4 – Notfallmanagement, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=2, Seite 57, abgerufen am 31.01.2023.

Auch Behörden und Verwaltungen werden immer öfter das Ziel von Cyberattacken. Laut BSI stieg die Qualität und Anzahl von Schadprogramm-Varianten in den letzten Jahren rasant an – mit bis zu 553.000 neuen Varianten pro Tag als dem höchsten jemals gemessenen Wert.[12]

Die Arten der Cyberattacken sind vielfältig und finden sowohl von außen als auch von innen statt. Häufige Formen von Cyberattacken sind (Distributed-)Denial-of-Service- (DoS), Man-in-the-Middle-Angriffe (MitM), Kennwort- und Accountangriffe, Abhören, Malware, Ransomware, aber auch Phishing-Angriffe als eine Form des Social Engineering (Beeinflussen von Personen). In allen Fällen kann eine nur rudimentär umgesetzte oder gar vernachlässigte Vorsorge schnell zu einem Totalausfall aller IT-Systeme führen, wie aus den Medien in letzter Zeit immer wieder zu entnehmen war: Beispiele sind unter anderem die Stadtverwaltung Potsdam[13], die Universität Duisburg-Essen[14], die Technische Universität Freiberg [15].

In den genannten Fällen wurden die IT-Systeme vom Netz genommen und waren über mehrere Wochen nicht erreichbar. Somit konnte in den Universitäten keine Online-Lehre stattfinden, Behörden waren online nicht erreichbar, sodass Anträge und dringende Meldungen online nicht möglich waren. Häufig ist in solchen Fällen nicht einmal der E-Mail-Server nutzbar, sodass darüber keine Kommunikation stattfinden kann und alle E-Mails aus diesem Zeitraum gegebenenfalls neu versendet werden müssen.

Um den Schaden eines erfolgreichen Cyberangriffs zu minimieren, ist es daher absolut notwendig, sich auf den Ernstfall mithilfe einer gründlichen Vorsorge und eines Notfallplans vorzubereiten. In Abbildung 19 wird deutlich, dass die Vorbereitungen und die eigentlichen Attacken im Netzwerk in den meisten Fällen unentdeckt bleiben. Häufig ahmen die Angreifenden einen autorisierten Benutzer nach, da die Angreifenden unzählige leicht verfügbare Tools, aber auch legitime Zugangsberechtigungen nutzen.

Meistens fällt der Schaden erst in der letzten Phase (oder noch später) auf: Daten sind verschlüsselt, die Freigabe erfolgt erst nach einer Lösegeldzahlung, die Daten oder ganze Datenbanken sind im Internet veröffentlicht etc.

---

[12] Bundesamt für Sicherheit in der Informationstechnik (2022): Die Lage der IT-Sicherheit in Deutschland 2022, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6, abgerufen am 31.10.2022.

[13] Heise Medien (2023): Stadt Potsdam ist schon wieder offline, https://www.heise.de/hintergrund/Stadt-Potsdam-ist-schon-wieder-offline-7470006.html, abgerufen am 02.02.2023.

[14] Heise Medien (2023): Ransomware – Daten von Uni-Essen im Darknet, Uni Innsbruck attackiert, https://www.heise.de/news/Ransomware-Daten-von-Uni-Duisburg-Essen-im-Darknet-Uni-Innsbruck-attackiert-7461603.html, abgerufen am 02.02.2023.

[15] Heise Medien (2023): Cyber-Angriff: IT der TU Freiberg weitreichend lahmgelegt, https://www.heise.de/news/Cyber-Angriff-IT-der-TU-Freiberg-weitreichend-lahmgelegt-7469937.html, abgerufen am 02.02.2023.

Abbildung 19: Eine Cyberattacke aus der Sichtweise eines Angreifenden

Die erste Phase einer Cyberattacke geschieht schon Monate vor dem Erkennen. Sie dient der Identifikation lohnenswerter Ziele. Große Unternehmen mit einem hohen Budget sind eher in der Lage, ihre Systeme abzusichern und permanent zu überwachen. Kleinere Unternehmen, öffentliche Institutionen (Schulträger und Schulen) verfügen nicht über dieses Budget. Den Angreifenden stehen hier „schneller und einfacher“ verwertbare Informationen zur Verfügung, der Aufwand ist geringer. Im Normalfall hat diese Phase auf die Organisation keine oder nur minimale Auswirkungen, die in den meisten Fällen nicht bemerkt werden.

In der zweiten Phase wird der Angriff auf das Ziel vorbereitet. Die Angreifenden versuchen mithilfe ihrer gesammelten Informationen in das Netzwerk einzudringen. Unter Umständen werden valide Zugangsdaten verwendet, um in die Netzwerkstruktur einzudringen und anschließend mit weiteren Tools die Umgebung zu infiltrieren. Auch an dieser Stelle ist weiterhin ein Angriff auf die IT-Infrastruktur praktisch nicht erkennbar. Die Angreifenden haben nun die Möglichkeit, einen langfristigen Remote-Access einzurichten. Auch dies geschieht in den meisten Fällen bereits Monate vor der Detektion des Angriffs.

Während der dritten Phase werden weitere Systeme und Accounts kompromittiert und Zielsysteme mit den Zieldaten detektiert. Auf Fileservern werden Passwortdateien und andere sensible Daten gesucht und das gesamte Netzwerk wird kartographiert, um einen Überblick über die Netzwerkstruktur und alle potenziellen Ziele zu erhalten. In dieser Phase ist es sehr schwierig, die Angreifenden zu erkennen, da hier häufig autorisierte Accounts verwendet werden.

In Phase vier testen die Angreifenden (wenige Wochen oder Tage vor der Erkennung), welche Level an Sicherheitsfreigaben erreicht werden müssen, um an die Ziele zu gelangen. In dieser Phase haben die Angreifenden bereits die Kontrolle über die Zugangskanäle und die Zugangsberechtigungen. Darüber erhalten sie den Zugriff auf die Zieldaten. Die Folge ist, dass E-Mail-Server, Dokumentenmanagementsysteme, Kundendaten, Personalmanagementsysteme etc. nun kompromittiert sind.

Die Phase fünf ist die finale Phase. Frühestens hier wird der Angriff als solcher erkannt, in den meisten Fällen erst nach Abschluss dieser Phase. Hier werden (Kunden-)Daten kopiert, verschlüsselt, kritische Systeme korrumpiert und operative Systeme unterbrochen.

Anschließend werden Beweise mithilfe von Ransomware zerstört. Sofern nicht an dieser Stelle die Attacke abgewehrt wird, steigen die Kosten für das Unternehmen exponentiell.

Nach der Phase können die Angreifenden die Daten an den Besitzer verkaufen beziehungsweise von diesem freipressen lassen, veröffentlichen oder löschen. Hier fallen für den Angegriffenen hohe Kosten an, da entweder vom Angreifenden finanzielle Mittel gefordert werden, damit das System wieder nutzbar und die Daten wieder sicher sind oder das System mithilfe von professioneller IT-Unterstützung wieder nutzbar gemacht werden muss. Die Wiederherstellung der Systeme bedingt in den meisten Fällen einen hohen finanziellen Aufwand.

Zusammenfassend lässt sich festhalten: Jede Organisation, die über veräußerbare Daten verfügt, ist ein potenzielles Angriffsziel für Cyberattacken. Um das eigene System zu schützen, ist eine permanente Überwachung aller Systeme von grundlegender Bedeutung. Aufmerksamkeit und Vorsicht sollten immer gelten. Das BSI stellt hierfür unter anderem hilfreiche Informationen zur Verfügung.[16] Um systematisch das Thema Cybersicherheit anzugehen, sollte sich jede Organisation mit dem übergreifenden Thema Informationssicherheit auseinandersetzen und zumindest eine Basisabsicherung gemäß BSI anstreben. Ein Umsetzungsmodell und entsprechende Informationen dazu lassen sich in der Handreichung 1 finden.

Im Rahmen der Schul-IT sind nicht nur die Mitarbeitenden in der Schulverwaltung, sondern die Gesamtheit des pädagogischen Personals, Hausmeister und Hausmeisterinnen und alle anderen Personen mit Zugang zu den Schulbehörden und Schulgebäuden unter dem Aspekt der Wachsamkeit und Aufmerksamkeit zu sensibilisieren. Daneben sind auch Eltern und – mit zunehmendem Alter – auch die Schülerinnen und Schüler für den Erfolg des Informationssicherheitsmanagements relevant. Gerade der verstärkte Einsatz von mobilen Endgeräten, die einen Zugriff auf sensible Server und Netzwerke zulassen, erfordert einen verantwortlichen Umgang mit den Zugangsdaten und die Achtsamkeit aller Beteiligten. Zentrale Anforderungen zur Sensibilisierung der Mitarbeitenden und Nutzenden lassen sich in den Bausteinen des BSI finden (siehe HR 1).

3.3.5 Notfallhandbuch

Bei einer erfolgreichen Cyberattacke kommt es auf die Reaktion an. Je schneller es gelingt, die Situation zu beherrschen, desto geringer fällt der Schaden aus. Aus der Erfahrung heraus kann festgehalten werden, dass einerseits die „Reaktionsfähigkeit“ mit der Entscheidungsgeschwindigkeit korreliert. Das heißt, hier kommen die oben beschriebenen (Entscheidungs-)Befugnisse zum Tragen.

Zum anderen muss transparent sein, wer benötigt wird. Es hilft wenig oder ist gar kontraproduktiv, sehr viele Experten und Expertinnen mit einem Mal zu kontaktieren und diese den eingetretenen Vorfall behandeln zu lassen. Ein spezielles Management der Notfallansprechpersonen ist gefragt. Für Schulen und Schulträger sollte daher ein Notfallhandbuch erstellt werden. Dieses beinhaltet alle notwendigen Maßnahmen zur Vorbeugung von Notfällen und zur Reaktion auf Notfälle. Zur Erstellung einen solchen kann die Vorlage des BSI (Notfallhandbuch[17]) herangezogen werden.

---

[16] Bundesamt für Sicherheit in der Informationstechnik (2022): Problembewusstsein und sicheres Verhalten, https://www.bsi.bund.de/dok/13768350, abgerufen am 02.02.2023.

[17] Bundesministerium für Sicherheit in der Informationstechnik (2021): BSI-Standard 200-4 Hilfsmittel – Dokumentvorlage für ein Notfallhandbuch, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_Vorlage_Notfallhandbuch.html, abgerufen am 26.01.2023.

Das BSI bietet darüber hinaus eine Vorlage für eine Notfallkarte[18] an. Die Notfallkarte ist ein Dokument, in dem komprimiert das Vorgehen im Notfall sowie die Ansprechpersonen festgeschrieben sind. Diese sollte an exponierten Stellen in allen Gebäuden verfügbar sein.

In der folgenden Abbildung wird der Notfall plastisch und auf die Phasen des Lebenszyklus bezogen dargestellt.

Abbildung 20: Unterbrechung der vierten Phase des Lebenszyklus von IT-Komponenten durch eine erfolgreiche Cyberattacke

Im Lebenszyklusmodell wurde in zwei Phasen die Empfehlung ausgesprochen, Penetrationstests durchführen zu lassen. Dies hat einen weiteren Hintergrund: Auch die potenziellen Angreifenden gehen häufig diesen aufwendigen Weg und scannen das Zielsystem. Folglich können häufig schon diese selbst initiierten Scans als erste Indikation wahrgenommen werden.

Ein eingetretener Vorfall unterbricht dabei nicht nur den normalen Betrieb, sondern bringt unter Umständen das ganze System in Gefahr und enthält das Risiko des Datenabflusses an unbefugte Dritte. Gerade im Bereich der Schul-IT, in dem eine Vielzahl sensibler Daten Minderjähriger verarbeitet werden, stellt die Publikation dieser Daten ein hohes Risiko dar. Es wird deshalb empfohlen, sich mit dieser Situation theoretisch im Vorfeld (BSI-Szenarien-Theorie) auseinanderzusetzen und eine Grundsatzhaltung zu erarbeiten.

Eine Notfallplanung sollte folgende Aspekte beleuchten und in einer Notfallkonzeption fixieren:

- regelmäßige Informationsbeschaffung über neu aufgedeckte Schwachstellen (z. B. durch Bezug der Meldungen des BSI oder OpenCVE),
- Backup-Strategie prüfen und sicherstellen,
- Notfallplan mit Schwerpunkt Kommunikation erstellen,
- Personen benennen, die im Notfall zu kontaktieren sind,

[18] Bundesministerium für Sicherheit in der Informationstechnik (unbekannt): IT-Notfallkarte „Verhalten bei IT-Notfällen“, https://www.bsi.bund.de/dok/13035680, abgerufen am 26.01.2023.

- Verantwortungsbereiche klären, Entscheidende benennen,
- regelmäßige Prüfung der Sicherheit aller als kritisch eingestuften IT-Komponenten,
- Lebenszyklusmodell im Notfallplan berücksichtigen.

Kommt es zum beschriebenen Cyber-Vorfall, ist „Zeit“ eine wesentliche Stellgröße für das Ausmaß des Schadens. Die Verantwortung für die Reaktion (Terminologie BSI) liegt bei der Schulleitung. Um zügig mit der Reaktionsphase zu beginnen, werden folgende konkrete, über die oben allgemein aufgezählten Aspekte hinausgehende Empfehlungen ausgesprochen:

Empfehlung 1: Externe Unterstützung.

Auch wenn mit dieser Empfehlung unter Umständen die Expertise der operativen Schuladministratoren infrage gestellt wird, sind Angriffe auf die IT-Infrastruktur einer Schule kaum durch eine Einzelperson zu behandeln. Expertinnen und Experten aus dem „näheren“ Umfeld, wie kommunale Dienstleistungszentren, spezialisierte Dienstleistende oder gelistete Freelancer und Freelancerinnen, sollten umgehend eingebunden werden. Ansprechpersonen, Rufnummern und weitere Kontaktdaten sollten Bestandteil des Notfallplans sein.

Empfehlung 2: **Bestimmen von Notfallansprechpersonen, die mit Eintreten eines Notfalls wichtige Entscheidungen treffen dürfen.**

Sind IT-Komponenten vom Cybervorfall betroffen, muss gehandelt werden. Um eine ungehinderte Ausbreitung des Schadens oder den Abfluss von Daten zu stoppen, kann es ein gängiger Ansatz sein, sofort „die Stecker“ zu ziehen. Diese Entscheidung ist bewusst und gezielt zu treffen. Dafür braucht es einen mit dieser *Befugnis* ausgestatteten Personenkreis.

Für die weitere Steuerung des Notfalls ist es darüber hinaus essenziell, auf Expertise und Erfahrungen im Umgang mit derartigen Situationen zurückgreifen zu können.

Des Weiteren kann es sinnvoll sein, eine IT-Cyberversicherung abzuschließen. Sollte für den Schulcampus eine IT-Cyberversicherung abgeschlossen worden sein, sind die entsprechenden Ansprechpersonen auch dem Notfallhandbuch zu entnehmen. Anderenfalls ist auf eine (in Papier ausgefertigte) Notfallansprechpartnerliste zurückzugreifen oder diese sollte auch auf der Notfallkarte notiert sein.

Empfehlung 3: **Den Angriff beim BSI melden.**

Durch eine Meldung des Vorfalls beim BSI kann die nationale Wissensdatenbank zu IT-Sicherheitsvorfällen kontinuierlich weiter aufgebaut werden. Dies versetzt langfristig alle Betroffenen in die Lage, bessere Vorkehrungen zu treffen und national notwendige Entscheidungen zu unterstützen.

Da ein Sicherheitsvorfall eine besondere Situation für den Schulträger darstellt, wurden in Tabelle 6 weitere zentrale Handlungsempfehlungen aufgeführt.

Tabelle 6: Besondere Checkliste für den Notfall

Phase des Lebenszyklus	Kernfragen	Verantwortliche Rolle	Empfehlungen und Erläuterungen
IT-Sicherheitsnotfall	Gibt es eine schriftlich fixierte Regelung zum IT-Notfallmanagement?	Schulleitung	Es sollte einen Notfallplan geben, der beschreibt, was durch wen wann wie zu erfolgen hat. Der Notfallplan sollte nicht (nur) elektronisch vorliegen.
	Ist das Regelungsdokument kommuniziert worden und ist es im Zugriff?	Schulleitung	Ein Regelungsdokument muss in einer Organisation bekannt sein und es muss im Zugriff sein, falls der Inhalt für Entscheidungen herangezogen werden muss. Drucken Sie das Dokument aus! Im Notfall haben Sie mit großer Wahrscheinlichkeit keinen geordneten Zugriff auf ihre IT. Das betrifft auch Regelungsdokumente.
	Ist bekannt, wer die Ansprechpersonen im Notfall sind und sind die Kontaktdaten (außerhalb einer Datenbank auf der IT-Technik, ggf. in Papierform) hinterlegt?	Schulleitung	Der Empfehlung folgend, den Vorfall nicht nur mit eigenem Personal zu begegnen, ist eine Ansprechpersonenliste in Papierform vorzuhalten, um Experten und Expertinnen sowie Dienstleistende zu erreichen. Gegebenenfalls sind Telefonnummern von Entscheidenden vorzuhalten, um wichtige Entscheidungen herbeizuführen.
	Können die Ansprechpersonen auch beim Ausfall der Telefonanlage erreicht werden?	Schul-IT-Admin	Es ist davon auszugehen, dass gerade VoIP-Telefonanlagen bei Verschlüsselungsattacken nicht einsatzbereit sind. Eine Backup-Telefoninfrastruktur (z. B. über Mobiltelefone) wird dringend empfohlen.
	Ist ein Kommunikationsplan vorhanden?	Schulleitung	Es zeigt einen kompetenten Umgang mit Krisenmanagement, wenn die angegriffene Schule selbst oder die verantwortliche Kommune aktiv über den Vorfall berichtet. Erreicht der Vorfall einen Schweregrad, der eine Fortführung des Schulbetriebs nicht mehr gewährleistet, ist eine umgehende, breitflächige Kommunikation angeraten.
	Ist es möglich, schnell externe Expertise hinzuzuziehen?	Schulleitung	Sie werden schnell merken, dass die Notfallsituation bei aller Vorplanung kaum allein zu beherrschen ist. Externe Expertise hilft, um die richtigen Schritte schnell und kompetent einzuleiten.

4 Fazit

Die IT-Sicherheit muss entlang des Lebenszyklus jeglicher IT-Komponenten mitgedacht werden. Schon bei der Planung der Schul-IT sollte eine Leitlinie erstellt werden, die alle sicherheitsrelevanten Aspekte berücksichtigt. Bei der Beschaffung, der Inbetriebnahme, dem regulären Betrieb und dem Rückbau muss diese Leitlinie als Grundlage der Entscheidungen dienen. Die Leitlinie sollte einem ständigen Verbesserungsprozess unterliegen und zumindest jährlich überarbeitet werden, um neue Risiken mit zu berücksichtigen.

Die Schul-IT befindet sich in einem permanenten Veränderungsprozess, da neue IT-Komponenten ergänzt und überalterte zurückgebaut werden müssen. Vor allem die Umsetzung des „DigitalPakts Schule“ führte in vielen Schulen zu einer enormen Erweiterung der IT-Komponenten. Die Notwendigkeit, diese in kurzer Zeit anzuschaffen, kann zur Folge haben, dass nicht immer alle Sicherheitsaspekte berücksichtigt wurden. An dieser Stelle ist es im Hinblick auf die IT-Sicherheit erforderlich, diese Komponenten in gesonderten Netzen zu betreiben, um die Gesamtheit der Schul-IT zu schützen.

Ein Notfall, wie zum Beispiel ein Cyberangriff, kann jederzeit in jedem Netz erfolgen. Aus diesem Grund ist es wichtig, sich auf eine solche Möglichkeit im Sinne eines Notfallmanagements vorzubereiten. Darüber hinaus sollte jede Schule und jeder Schulträger ein Notfallhandbuch erstellen.

Folglich ist es wichtig, dass Schulträger und Schulen gemeinsam Sicherheitsrichtlinien für die Schul-IT erstellen, um sich vor Cyberangriffen zu schützen sowie ein Notfallmanagement zu etablieren. Ziel ist es, Notfällen vorzubeugen oder bei deren Eintritt diese bewältigen zu können.

5 Glossar

Asset Management	Allgemein bezeichnet man mit *Asset* Vermögenswerte in einer Organisation. In der IT bedeutet ein IT-Asset sowohl die Hardwarekomponenten als auch die eingesetzte Software in einer Organisation. Das Assetmanagement ist für den Prozess verantwortlich, dass die Assets einer Organisation dokumentiert, bereitgestellt, gewartet, aktualisiert und stillgelegt werden, wenn der Zeitpunkt dafür gekommen ist.
Change	Handlung, um die IT-Infrastruktur zu verbessern und Ausfälle zu minimieren.
Change Management	Es behandelt jede Art von Veränderung (Change) an einer IT-Infrastruktur und seinen Services. Es steuert jede Anpassung an der IT-Infrastruktur kontrolliert effizient und unter Minimierung von Risiken für den Betrieb.
Einflussgrößen	Das sind die Trends und Entwicklungen, die zu einem veränderten Aufgabenumfang der IT-Infrastruktur führen.
Handlungsfelder und Herausforderungen	Das sind die thematischen Überschriften, unter denen Umsetzungsempfehlungen zur IT-Sicherheit mit Bezug zu den IT-Komponenten ausgesprochen werden.
Informationssicherheit	Durch die Informationssicherheit sollen Daten geschützt werden. Es soll sichergestellt werden können, dass nur autorisierte Benutzer Zugriff auf diese Daten haben und ein unbefugter und unkontrollierbarer Zugriff nicht erfolgen kann. Um das gewährleisten zu können, müssen die Schutzziele der Informationssicherheit erreicht werden. Bei der Vertraulichkeit dürfen Daten lediglich von autorisierten und befugten Benutzern eingesehen und verwaltet werden. Durch die Integrität soll verhindert werden, dass Daten unbemerkt verändert und manipuliert werden können. Die Verfügbarkeit dient der Verhinderung von Systemausfällen. Weitere Schutzziele der Informationssicherheit sind die Authentizität und die Verbindlichkeit. Authentizität bezeichnet die Echtheit und Überprüfbarkeit von Daten. Durch die Verbindlichkeit wird gewährleistet, dass jeder Zugriff auf Daten nachvollziehbar ist. In jeder Organisation sollten entsprechende Maßnahmen implementiert werden, damit die Schutzziele eingehalten werden können und die Sicherheit der Informationen gewährleistet werden kann.
Incident	Bei einem Incident handelt es sich um eine (kurze) Unterbrechung/Störung eines IT-Services.

Incident Management	Das IT-Incident- beziehungsweise IT-Störungsmanagement umfasst typischerweise den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle beziehungsweise Betriebsstörungen in IT-Bereichen sowie hierzu vorbereitende Maßnahmen und Prozesse. Ein gutes Störungsmanagement stellt den Prozess, die Werkzeuge und das Konzept für eine schnelle Störungsbehebung zu einem vereinbarten Service bereit.
IT-Architektur	Unter IT-Architektur werden die gesamte IT-Infrastruktur, das IT-Management und die IT-Schnittstellen zusammengefasst. Sie beschreibt die jeweiligen Anwendungs-, Infrastruktur-, Informations- und Datenarchitekturen und deren Beziehungen untereinander.
IT-Beauftragte	Teilweise wird der/die Medienbeauftragte auch als IT-Beauftragte/-r geführt. Davon soll im Sinne einer möglichst scharfen Trennung von Rollen und Begrifflichkeiten Abstand genommen werden. Die Begrifflichkeit des/der IT-Beauftragten wird aus dem Vokabular dieses Dokuments gestrichen.
IT-Governance	In der Regel besteht die IT-Governance aus einer klaren Führungsebene, Organisationsstrukturen und Prozessen beziehungsweise definierten Abläufen. Diese tragen gemeinsam die Verantwortung dafür, dass die gesamte Informationstechnik (IT) und Infrastruktur die Organisationsziele unterstützt.
IT-Komponenten	Dies sind Zielobjekte (gemäß BSI), für die eine Schutzbedarfsfeststellung zu erfolgen hat. Zum Beispiel Endgeräte, Server, Drucker und Access-Points.
IT-Störungen	Auslöser für IT-Störungen sind technische Defekte oder unbeabsichtigtes (menschliches) Fehlverhalten. Es findet keine Einwirkung Dritter (z. B. Angreifende) statt (Beispiele: Maus oder Tastatur funktioniert nicht, Probleme mit dem Netzwerk, Bildschirm zeigt kein Bild). Die Beeinträchtigung beschränkt sich auf eine kurzzeitige Nichtverfügbarkeit. Der Behandlungsaufwand ist niedrig.
IT-Sicherheitsvorfall	Auslöser für IT-Vorfälle sind in der Regel Angriffe durch Cyberkriminelle (Beispiele: Verschlüsselung von Dateien durch Ransomware, Identitätsdiebstahl, Manipulationen von Dateien). Die Beeinträchtigung lässt sich als langwierige Nichtverfügbarkeit beschreiben. Der Behandlungsaufwand ist hoch.
Make or Buy	Das beschreibt die Entscheidung, Produkte selbst herzustellen (Make) oder sie einzukaufen (Buy).
Penetrationtest	Simulierte Cyberangriffe, bei denen Sicherheitsexperten und Sicherheitsexpertinnen IT-Systeme auf Sicherheitslücken untersuchen und analysieren.
Problem-Management	Innerhalb des IT-Services steuert das Problem-Management die Behebung von IT-Störungen sowie Vorfällen und untersucht deren Ursache. Es führt standardisierte Vorgehensweisen ein, um die Abläufe der IT-Prozesse zu analysieren und eine schnelle Herstellung bei einem Ausfall zu gewährleisten.

Service Desk	Unter Service Desk versteht man in der Regel den IT-Service, der als Ansprechpartner Lösungen findet und für alle Beteiligten einer Organisation erreichbar ist, wenn etwas bei der IT nicht funktioniert.
Vorfall	Siehe IT-Sicherheitsvorfall.

6 Abkürzungen

AKV	Aufgaben, Kompetenzen und Verantwortung
BCM	Business Continuity Management
BIA	Business Impact Analysis
BYOD	Bring your own device
DL	Dienstleister
GYOD	Get your own device
HR 1	Handreichung 1: Einführung in die Informationssicherheit für Schulen
IDM	Identity Management
ISMS	Information Security Management System
LAN	Local Area Network
MAN	Metropolitan Area Network
RV	Rahmenvertrag
SbD	Security by Design
SIEM	Security Information and Event Management
SSID	Service Set Identifier
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network

7 Autorinnen und Autoren

Uta Fiedler
Mathias Ragnow
Antje Reuter

Für ihre Unterstützung bedanken wir uns bei der SONOXO.AI-GmbH & Co. KG:

Astrid Aha
Alexander Gutendorf

Kontakt:

PD – Berater der öffentlichen Hand GmbH
Friedrichstraße 149
10117 Berlin
www.pd-g.de/
E-Mail: SchuleDigital@pd-g.de

Die vorliegende Handreichung im Modul „IT-Steuerung und Kooperation“ wurde im Rahmen einer Ressortforschung des Bundesministeriums der Finanzen (BMF), finanziert aus Mitteln des Deutschen Aufbau- und Resilienzplans (DARP), erstellt.

Finanziert von der Europäischen Union
NextGenerationEU

8 Literaturverzeichnis

Arbeitsgruppe Kommunale Basis-Absicherung (AG KOBA) (2022): IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung (31.03.2022), https://www.landkreistag.de/images/stories/themen/egovernment/220331_IT-Grundschutz-Profil.pdf, abgerufen am 14.09.2022.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2022): IT-Grundschutz-Kompendium, Bonn: Reguvis Fachmedien GmbH, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2022.pdf?__blob=publicationFile&v=3, abgerufen am 14.09.2022.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2022a): Gefährdungslage im Cyber-Raum hoch wie nie, https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/221025_Lagebericht.html, abgerufen am 22.03.2023.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2022b): Awareness, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/Awareness/awareness_node.html, abgerufen am 14.09.2022.

Der Spiegel (24.02.2021): Cyberangriff auf Schulplattform. 14-Jähriger soll Unterricht lahmgelegt haben, https://www.spiegel.de/netzwelt/web/rheinland-pfalz-14-jaehriger-stoerte-von-schulen-genutztes-konferenzsystem-a-664fa36a-c962-42a8-bca6-529342b81c79, abgerufen am 14.09.2022.

International Standard ISO/IEC 7498-1, Open Systems Interconnection – Basic Reference Model, Second Edition: http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip, abgerufen am 22.03.2023.

NDR (08.03.2022): Computer-Hacker erpressen Berufsbildende Schulen in Goslar, https://www.ndr.de/nachrichten/niedersachsen/braunschweig_harz_goettingen/Computer-Hacker-erpressen-Berufsbildende-Schulen-in-Goslar,hacker408.html, abgerufen am 14.09.2022.

Nieder-Entgelmeier (01.08.2019): Cyberangriffe auf Schulen gefährden Schülerdaten, https://www.lz.de/lippe/kreis_lippe/22523333_Cyberangriffe-auf-Schulen-gefaehrden-Schuelerdaten.html, abgerufen am 14.09.2022.

Anhang: Checkliste für Schulen und Schulträger