Architekturbeispiel: Videokonferenzsystem für den Distanzunterricht

Dieses Beispiel wendet die Methode „Enterprise Architecture Management“ an, um technisch-infrastrukturelle Voraussetzungen für den digital gestützten Distanzunterricht zu ermitteln. Als Grundlage dienen die ermittelten Fähigkeiten für digitale Schule und konkrete Anwendungsbereiche, in denen die Fähigkeiten eingesetzt werden, um die erforderlichen technischen Bedarfe zu klären.

1 | Digitale Fähigkeiten – Klärung des Was?

Das Beispiel Videokonferenzsystem konzentriert sich auf die Kernfähigkeit aller Schulen im Kontext der Digitalisierung: die digital gestützte Vermittlung von Wissen.

Abbildung 1 – Beispiel für digitale Fähigkeiten

2 | Anwendungsbereich und Funktionsumfang – Klärung des Wofür?

Konkret benötigen Schulen digitale Fähigkeiten zur Wissensvermittlung in mehreren Anwendungsfällen. Dazu gehören in erster Linie die digitale Kommunikation und der Informationsaustausch, die gleichzeitig die Basis für den Distanzunterricht darstellen. Auch das digital gestützte Lernen sowie die Lernfortschrittskontrolle sind Anwendungsbereiche der digitalen Wissensvermittlung, weshalb Lernplattformen in einem separaten Architekturbeispiel betrachtet werden. Ihre Relevanz wird sich auch im Präsenzunterricht stetig erhöhen.

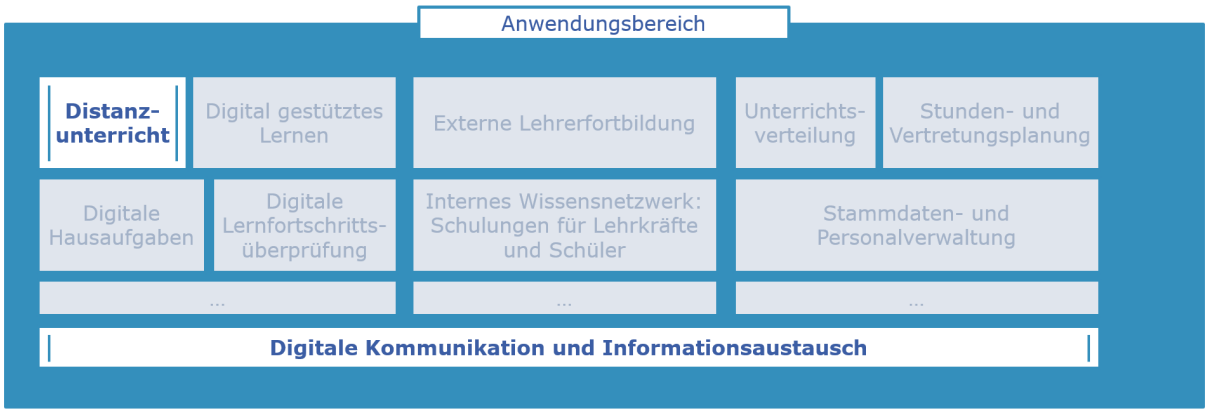


Abbildung 2 – Beispiel für Anwendungsbereich

Cross-Business-Architecture Lab e. V., info@cba-lab.de
Autoren: Mirjam Bayatloo, Olaf Reimann

3 | Technisch-infrastruktureller Bereich – Klärung des Womit?

Unabhängig der Schulform bedarf es einer Kommunikationsplattform, damit der Informationsaustausch zwischen Lehrkräften und Schülerinnen und Schülern gewährleistet wird. Diese technische Plattform bildet die Basis für den digital gestützten Distanzunterricht.

Die didaktische und methodische Konzeption des Präsenzunterrichts sollte in geeigneter Art und Weise auf den Distanzunterricht übertragen werden, sind doch gewählte Arbeitsmaterialien, Interaktions- und Kommunikationsansätze bisher auf die physische Präsenz in einem Klassenraum zugeschnitten.

Zentrale Aspekte der Unterrichtsgestaltung lassen sich trotz weitreichender Unterschiede, wie in Abbildung 3 ersichtlich, auf den digital gestützten Distanzunterricht übertragen.

	PRÄSENZ-UNTERRICHT	DISTANZ-UNTERRICHT
Kommuni-kation	Unterrichtsteilnehmer sehen sich im Klassenraum	Videokonferenz & Webcam
	Unterrichtsteilnehmer reden miteinander	Telefonat oder Videokonferenz
Vermittlung von Lerninhalten	Tafelanschrieb/ Whiteboardanschrieb	• Textfunktion virtuelles Whiteboard • Text- und Bildversand per Messenger
	Arbeitsmaterialien zeigen *(Overhead-Projektor, Beamer, Smartboard)*	• Bildschirmfreigabe in der Videokonferenz • Upload des Arbeitsmaterials
	Arbeitsmaterialien verteilen und einsammeln	• Upload auf ein Dokumentenverwaltungssystem / Lernplattform • Interaktive Arbeitsmaterialien in eLearning Apps • *Nicht digital: Verweis auf Schulbücher*
Arbeitsphasen	Arbeitsmaterialien bearbeiten	• Nutzung von Produktivitätssoftware (Schreib-/Präsentationsprogramm) • Bearbeitung auf Lernplattformen oder in der eLearning App • *Nicht digital: handschriftliche Bearbeitung im Schulheft*
	Gruppenarbeiten durchführen	• Virtuelle Räume in einer Videokonferenz
Feedback	Gemeinsame Besprechung der Aufgaben	• Telefon-/Videokonferenz • Bildschirmfreigabe oder virtuelles Whiteboard
	Individuelles Feedback	• Textuelles Feedback (Messenger) • Telefonat/Videokonferenz • Direkte Rückmeldung auf Lernplattformen / eLeaning Apps / Dokumentenverwaltungssystem

Abbildung 3 – Übertragung verschiedener Aspekte des Präsenzunterrichts auf den Distanzunterricht

Die in der Tabelle abgebildeten Funktionen werden von verschiedenen Computerprogrammen (auch Software, Anwendung oder [mobile] Applikation) zur Verfügung gestellt. Deutlich wird auch, dass sich viele Aspekte bereits mit einem Videokonferenzsystem abdecken lassen. Für unseren Anwendungsfall „Distanzunterricht“ ist das Videokonferenzsystem die erste Antwort auf die Frage des „Womit?“.

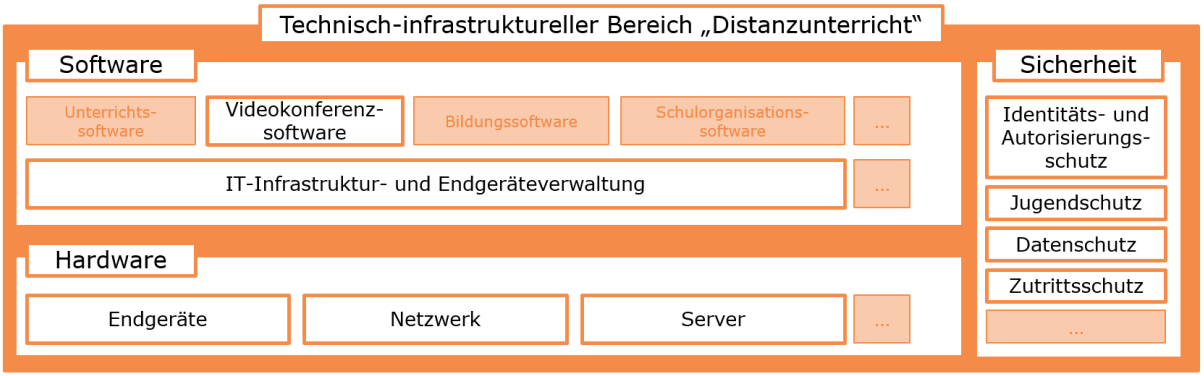


Abbildung 4 – Beispiel für den technisch-infrastrukturellen Bereich

Lernplattformen und E-Learning-Apps können den Distanzunterricht ergänzen, decken aber gleichzeitig auch die Anwendungsbereiche „Lernen mit digitalen Medien“ und „Lernfortschrittskontrolle“ ab, die nicht im Fokus dieses Beispiels stehen.

Der nachfolgende Abschnitt beschreibt die erforderliche technisch-infrastrukturelle Architektur für ein konkretes Videokonferenzsystem.

Beispiel Videokonferenzsoftware BigBlueButton, Hilfssoftware und Endgeräte

Die Software BigBlueButton ist ein Beispiel für eine Videokonferenzplattform. Sie bietet den Nutzern außer der Videokonferenzfunktion weitere Möglichkeiten, wie die Nutzung eines Whiteboards, virtuelle Räume oder Nachrichtenfunktionen. Damit sowohl Lehrkräfte als auch Schülerinnen und Schüler BigBlueButton nutzen können, benötigen sie weitere Software-, Netzwerk- und Hardwarekomponenten sowie Prozesse für die Einrichtung, den sicheren Betrieb und die Wartung der Komponenten. Eine strukturierte Übersicht erforderlicher Komponenten zeigt ein IT-Architekturbild (Beispiel siehe Abbildung 5). Die Anschaffung von Tablets für Schülerinnen und Schüler ist in diesem Kontext also nur einer von vielen Aspekten.

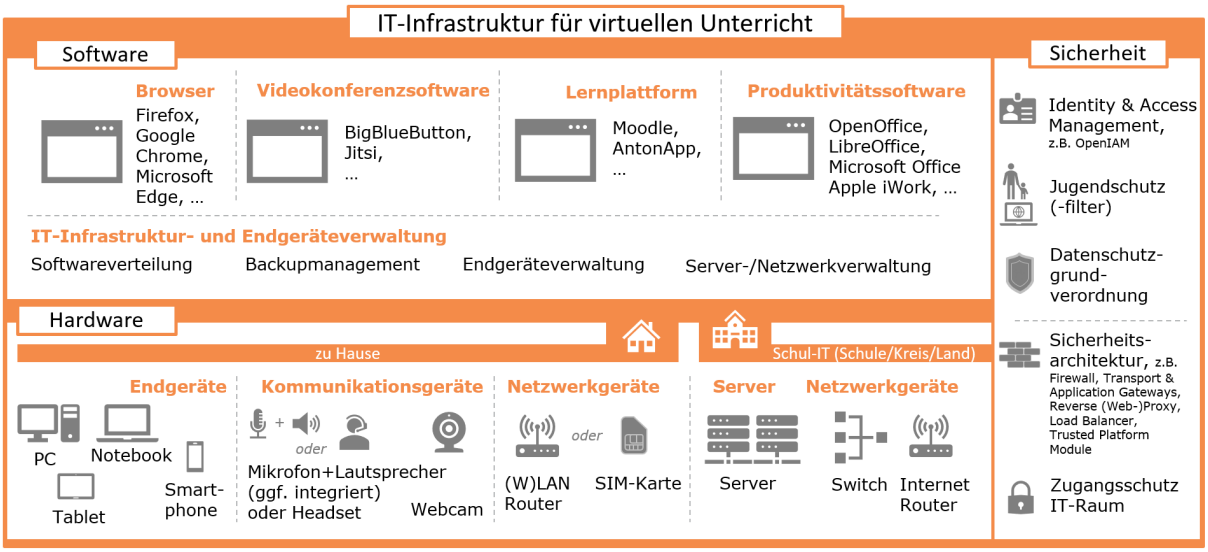


Abbildung 5 – Beispielarchitektur für den Distanzunterricht mit einer Videokonferenzsoftware.

BigBlueButton ist eine Webanwendung, d. h., sie muss über einen Browser geöffnet werden. Empfohlen werden Firefox und Google Chrome. Auch ein Browser ist eine Software. Browser werden auf den Endgeräten installiert. Abhängig vom Betriebssystem der (mobilen) Endgeräte (z. B. Microsoft Windows, Mac OS, Linux, iOS, Android) sind Browser vorinstalliert. Zu den üblichen Endgeräten zählen PC, Notebook, Tablet oder Smartphone. Aufgrund der Displaygröße und Bedienbarkeit empfiehlt sich für den digitalen Unterricht mindestens ein Notebook. Ohne externe Tastatur fällt es auf Dauer schwer, mit einem Tablet alle Aufgaben während des Distanzunterrichts durchzuführen. Spezielle Stifte erleichtern zumindest das Schreiben per Hand auf dem Tablet. Hinzu kommen eine Webcam und ein Headset, falls das Endgerät diese nicht integriert hat, damit Schülerinnen und Schüler

Für die Nutzung eines Videokonferenzsystems im Distanzunterricht müssen zahlreiche Software-, Hardware- und Sicherheitskomponenten aufeinander abgestimmt werden.

Viele Komponenten der Beispielarchitektur sind nicht ausschließlich für den Distanzunterricht erforderlich, sondern **finden ihren Einsatz auch in anderen Anwendungsbereichen** der Fähigkeiten digitaler Schule (vgl. Abbildung 2).

aktiv am Unterricht teilnehmen können. Falls vorhanden ist ein Headset dem im Endgerät integrierten Mikrofon und Lautsprecher vorzuziehen, da es zu unangenehmen Echos kommen kann. Das passiert immer dann, wenn mindestens ein Gerät die Audioausgabe wieder zurückleitet.

Netzwerk- und Serverinfrastruktur

Eine ausreichend schnelle und stabile Internetverbindung ist ebenfalls Voraussetzung für den digitalen Unterricht über eine Videokonferenzsoftware wie BigBlueButton. Lehrkräfte sowie Schülerinnern und Schüler benötigen dafür zu Hause einen Internetanschluss und einen Router. Der Router ermöglicht den Endgeräten per Kabel (LAN) oder ohne Kabel (WLAN) den Zugriff auf das Internet. Alternativ kann auch das Mobilfunknetz verwendet werden. Dafür muss das Endgerät SIM-fähig sein. Über die SIM-Karte und entsprechendes Datenvolumen kann man sich dann mit dem Internet verbinden.

> Die **erforderliche Bandbreite** der Internetverbindung für eine stabile Videokonferenz **hängt maßgeblich von** der Wahl der **Software**, der **Anzahl der Teilnehmer** und der **geteilten Inhalte**, z. B. Webcam-Bild oder Screensharing, **ab**.

Videokonferenzsysteme unterscheiden sich auch in der Verarbeitung von Video- und Tonsignalen der Konferenzteilnehmenden. Während andere Software beide Signale zusammenführt, komprimiert, runterskaliert und dadurch Bandbreite und Rechenleistung spart, wird bei BigBlueButton lediglich mit dem Tonsignal so verfahren. Das bedeutet, je mehr Personen mit Ton und Bild an einer BigBlueButton-Videokonferenz teilnehmen, desto mehr Bandbreite und Rechenleistung aller teilnehmenden Geräte, also Übertragung einer Datenmenge pro Sekunde und Prozessorauslastung, wird benötigt, um eine ausreichende Qualität der Konferenz aufrecht zu erhalten (vgl. Abbildung 6). Dadurch ergibt sich in der Regel eine begrenzte Anzahl von Benutzern pro Videokonferenz von weniger als 20 Teilnehmern.

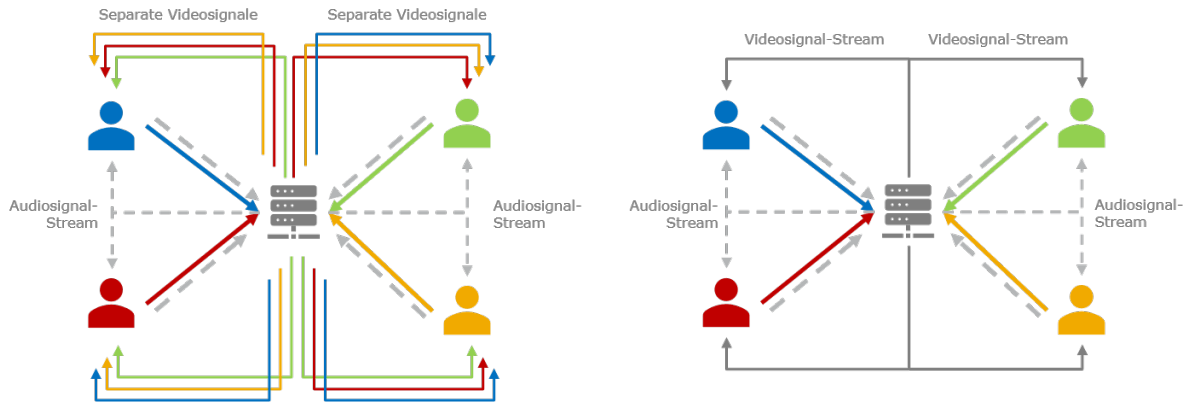


*Abbildung 6 – Veranschaulichung der Audio- und Videosignale, die vom Server und den Endgeräten der Teilnehmenden verarbeitet werden müssen für BigBlueButton (links) und andere Videokonferenzsysteme (rechts). Bei n Teilnehmenden erzeugt BigBlueButton n*n Videostreams*[1]

[1] BigBlueButton Inc., Zugriff März 2021, https://docs.bigbluebutton.org/support/faq.html#how-many-simultaneous-users-can-bigbluebutton-support

Den größten Einfluss auf die zu übertragende Datenmenge hat auf der Seite der Endbenutzenden die Anzahl der Konferenzteilnehmenden mit jeweils eingeschaltetem Mikrofon und eingeschalteter Kamera sowie die Bildschirmfreigabe. BigBlueButton empfiehlt den Nutzern eine Mindestbandbreite von 0,5 Mbit/s im Upload und 1 Mbit/s im Download. Wesentlich mehr leisten müssen die Server, auf denen BigBlueButton für die Lehrkräfte sowie Schülerinnen und Schüler installiert ist. Netzwerk-Switches leiten die über das Internet übertragenen Daten an die Server.

Ein Beispiel in Zahlen

Mithilfe der Anzahl der Teilnehmer T einer Videokonferenz, der Webcamnutzer W, die ihre Webcam eingeschaltet haben und der von BigBlueButton unterstützten Webcamauflösung bzw. deren benötigter Datenmenge D (0,25 Mbit/s bei kleiner Auflösung, 0,4 Mbit/s bei mittlerer Auflösung, 0,6 Mbit/s bei großer Auflösung), lässt sich die erforderliche eingehende Bandbreite $B_in = W * D$ sowie die ausgehende Bandbreite $B_out = W * (T - 1) * D$ für die Server ermitteln. Hinzu kommen zu übertragende Datenmengen für geteilte Bildschirme und Audioinformationen der Mikrofone. Das Teilen von Bildschirmen fällt mit 0,2 Mbit/s bis 1 Mbit/s stark ins Gewicht.[2]

Für eine Schule mit 40 Klassen á 28 Schülerinnen und Schüler, also 1120 Schülerinnen und Schüler insgesamt, bedeutet das bei parallelem Unterricht:

$T_{Schule} = 1160$, nämlich 1120 Schülerinnen und Schüler und 40 Lehrkräfte
$T_{Klasse} = 29$, nämlich 28 Schülerinnen und Schüler und eine Lehrkraft

Bestenfalls nutzen nur die Lehrkräfte ihre Webcam in schlechter Auflösung und teilen den Bildschirm mit geringstmöglicher Datenübertragung. Dann gilt für jeweils eine der 40 parallelen Videokonferenzen:

$W = 1$
$D_{webcam} = 0{,}25\ Mbit/s$
$D_{screensharing} = 0{,}2\ Mbit/s$
$B_{in} = W * D = 1 * D_{webcam} + 1 * D_{screensharing} = 0{,}45\ Mbit/s$
oder für alle Klassen insgesamt $40 * 0{,}45\ Mbit/s = 18\ Mbit/s$
$B_{out} = W * (T_{Klasse} - 1) * D = 1 * 28 * 0{,}45\ Mbit/s = 12{,}6\ Mbit/s$
oder für alle Klassen insgesamt $40 * 12{,}6\ Mbit/s = 504\ Mbit/s \approx 0{,}5\ Gbit/s$

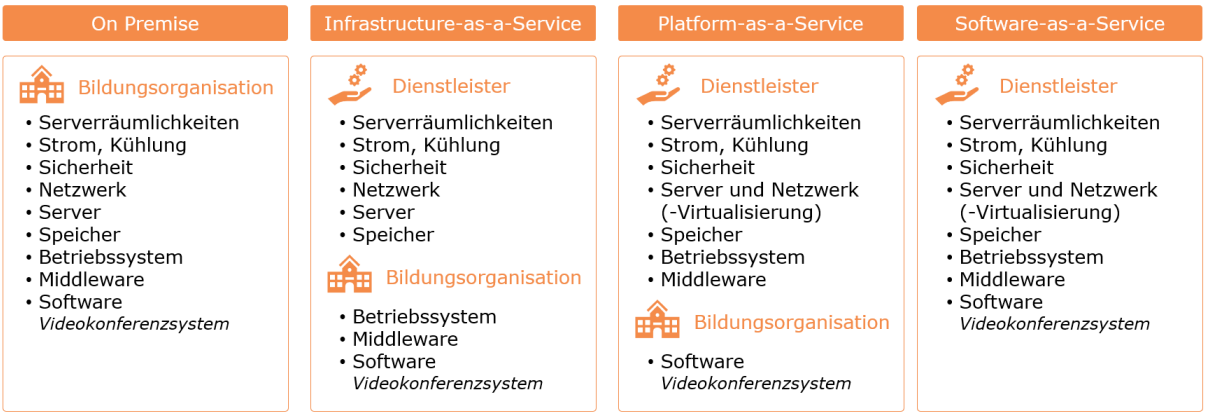
Im Extremfall sind alle Teilnehmer per hochauflösender Webcam zugeschaltet und jeweils eine Person teilt ihren Bildschirm mit höchstmöglicher Datenübertragung. Dann gilt für jeweils eine der 40 parallelen Videokonferenzen:

$W = 29$
$D_{webcam} = 0{,}6\ Mbit/s$
$D_{screensharing} = 1\ Mbit/s$
$B_{in} = W * D = 29 * D_{webcam} + 1 * D_{screensharing} = 18{,}4\ Mbit/s$
oder für alle Klassen insgesamt $40 * 18{,}4\ Mbit/s = 736\ Mbit/s$
$B_{out} = W * (T_{Klasse} - 1) * D = 29 * 28 * 1{,}6\ Mbit/s = 1.299{,}2\ Mbit/s \approx 1{,}3\ Gbit/s$
oder für alle Klassen insgesamt $40 * 1{,}3\ Gbit/s = 52\ Gbit/s$

Zum Vergleich: Ein 16.000er DSL-Anschluss ermöglicht als eingehende Bandbreite (Download) maximal 16 Mbit/s, als ausgehende Bandbreite (Upload) nur maximal 2 Mbit/s. Die Beispielrechnung für nur eine Schule zeigt, dass eine stabile und insbesondere skalierbare Infrastruktur unerlässlich ist und professionell umgesetzt werden muss. Während der Kernunterrichtszeiten, zu der alle Schulformen auf die Infrastruktur zugreifen müssen, besteht eine erheblich größere Last der Bandbreite und Rechenleistung als zu Randzeiten am späten Nachmittag oder am Wochenende.

[2] BigBlueButton Inc., Zugriff Februar 2021, https://docs.bigbluebutton.org/support/faq.html#bandwidth-requirements

Um die Fragen „Wer kann die Infrastruktur bereitstellen?“ und „Wie muss die Infrastruktur für einen sicheren Betrieb aussehen?“ beantworten zu können, findet sich nachfolgend eine Übersicht verschiedener Betriebsmodelle für eine Videokonferenzplattform:



Um den Fokus auf dem Bildungsauftrag der Schulen zu behalten, ist es zielführend, IT-Expertinnen und Experten in den Aufbau und Betrieb einer solchen erforderlichen Infrastruktur einzubinden. Ein einheitlicher und übergreifender Ansatz und dessen Umsetzung sind wesentlich effizienter. Der Einkauf von Software- oder Infrastrukturdiensten bietet zudem immer die Möglichkeit eines Wechsels zu einem anderen Anbieter. Eigene Rechenzentren bzw. eigene Hardware erschweren hingegen flexible Anpassungen an den Diensten, die für die Schulen bereitgestellt werden.

Entscheidet man sich für den eigenen Betrieb der Infrastruktur, ergeben sich viele Aspekte, die im Rahmen der Architektur zu beachten sind. Wie auf den physischen Endgeräten der Nutzer (Notebook, Tablet etc.) müssen auch auf den Servern entsprechende Betriebssysteme installiert sein. Der BigBlueButton-Server erfordert das Linux-Betriebssystem Ubuntu. Auch die Minimalanforderungen an die Hardware werden von BigBlueButton beschrieben, um eine stabile Nutzung der Videokonferenzplattform zu gewährleisten. Dazu gehört beispielsweise die Rechenleistung, die ein Server erbringt (Central Processing Unit, kurz CPU). Zur Verarbeitung der Audiodaten ist es beispielsweise die Aufgabe des Servers mit seiner Rechenleistung alle Audiokanäle der Konferenzteilnehmer zu mischen und dieses gemischte Signal an jeden Teilnehmenden zu verteilen.

Weiterhin sind umfassende technische, aber auch organisatorische Maßnahmen erforderlich, um

Für den Betrieb der IT-Infrastruktur gibt es unterschiedliche Modelle, ähnlich wie beim Essen von Pizza:

- **On Premise**: Alles wird selbst gemacht. Teig, Belag, Zubereitung im eigenen Ofen und gegessen wird am eigenen Esstisch
- **Infrastructure-as-a-Service**: Wir essen Tiefkühlpizza, müssen uns nur noch um die Zubereitung kümmern und können sie dann essen.
- **Platform-as-a-Service**: Die zubereitete Pizza wird geliefert. Wir müssen sie nur noch am eigenen Tisch essen.
- **Software-as-a-Service**: Wir essen Pizza im Restaurant und müssen uns um nichts kümmern. Sogar der Tisch ist gedeckt.

den Zugriff auf die Server zu schützen. Sicherheitsarchitekturen beschreiben zahlreiche Komponenten, die weit über Firewalls hinausgehen und sowohl auf Softwareebene als auch auf Netzwerk- und Hardwareebene umgesetzt werden müssen. Hinzu kommen Sicherheitsmaßnahmen für das Rechenzentrum und den Zugriff auf die physischen Server selbst.

Endgerätemanagement und Zugriffsschutz

Nach wie vor arbeiten viele Lehrkräfte, Schülerinnen und Schüler mit ihren privaten Endgeräten. Bei individuell auftretenden technischen Problemen kann daher nur schwer geholfen werden. Die Digitalisierungsstrategie für Schulen sieht in vielen Bundesländern vor, die Lehrkräfte aber z. T. auch Schülerinnen und Schüler mit einheitlichen Endgeräten auszustatten.

Eine **zentrale Endgeräteverwaltung** mit strukturierten Prozessen ist dabei unerlässlich, da veraltete Geräte zurückgenommen, durch neue ersetzt, eingerichtet und ausgegeben werden müssen. Hinzu kommt die zeitweise Ausgabe und Rücknahme von Geräten, z. B. für Vertretungskräfte.

Softwareverteilungssysteme stellen sicher, dass nur genehmigte Software installiert ist. Gleichzeitig können (sicherheits-)relevante Updates und neue, standardisierte Software auf Endgeräte aufgespielt werden, ohne dass Lehrkräfte, Schülerinnen und Schüler vor Ort auf Hilfe angewiesen sind.

So genannte **Identity und Access Management Systeme** (IAM) verwalten Nutzeraccounts, stellen die Identität sicher und autorisieren Lehrkräfte, Schülerinnen und Schüler mit ihrem Account an den Endgeräten und der Software.

Ein **Single-Sign-On Service** (SSO) erleichtert den Nutzenden das Arbeiten. Mithilfe von SSO können sich Lehrkräfte, Schülerinnen und Schüler sowohl an Endgeräten als auch in verschiedener Software mit ein und demselben Account authentisieren. Ist das Passwort einmal eingegeben, so erfolgt der Login in alle verknüpften Programme automatisch, ohne dass es erneut eingegeben werden muss.

Bekanntlich ist die Fluktuation an Schulen weitaus höher als in einem typischen Unternehmen. Ein IAM-System erhöht zusammen mit einem organisierten Vorgehen die Informationssicherheit an den Schulen und standardisiert das sogenannte User-Lifecycle-Management. Abbildung 7 illustriert, dass Accounts der Vertretungskräfte oder Schülerinnen und Schüler bereits beim Erstellen mit einem Ablaufdatum versehen werden können, um einen unberechtigten Zugriff auf Systeme und Daten zu verhindern.

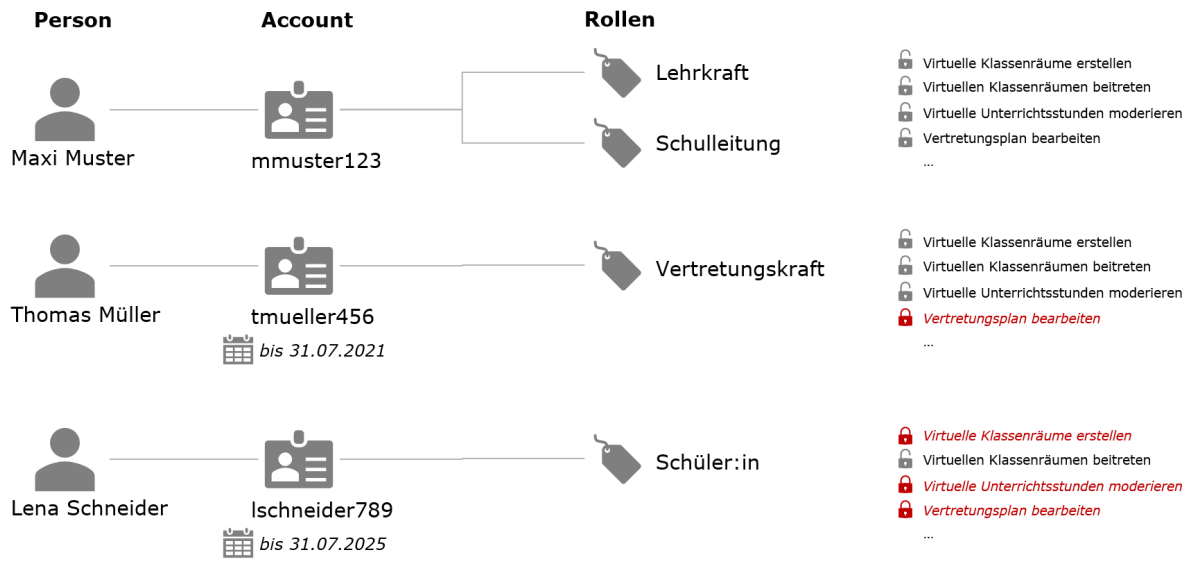


Abbildung 7 – Illustrative Abbildung der Einträge in einem IAM-System

Daten- und Jugendschutz

Insbesondere bei minderjährigen Schülerinnen und Schülern müssen Schulen bei der Auswahl der zur benutzenden Software für den virtuellen Unterricht sowohl den Datenschutz als auch den Jugendschutz als weitere Sicherheitsaspekte berücksichtigen.

Im Fokus steht dabei einerseits die Verarbeitung personenbezogener Daten, also alle Informationen, die sich laut **Datenschutzgrundverordnung** (DSGVO) „auf eine identifizierte oder identifizierbare natürliche Person beziehen". Schulen müssen daher für den digitalen Unterricht Software auswählen, die nur zwingend notwendige personenbezogene Daten verarbeitet, diese Daten aber keinen Dritten zugänglich macht und löscht, sobald der Zweck der Verarbeitung erfüllt ist. BigBlueButton ist in der Hinsicht – mit Installation auf entsprechender Infrastruktur und geeigneten Organisationsprozessen – eine DSGVO-konforme Lösung. Rechtsunsicherheit besteht unterdessen bei kommerziellen Lösungen wie Microsoft Teams, die als Service eingekauft und von einigen Schulen als stabile Alternative genutzt werden, um ihren Bildungsauftrag bestmöglich ausführen zu können. Dieser Unsicherheit steuern nun Unternehmen wie Microsoft entgegen und setzen zusätzliche Maßnahmen für den Datenschutz um.[3] In jedem

Sichere Nutzung der Software ist **mehr als die Einhaltung der DSGVO**. Installierbare Software muss und kann nur auf Leihgeräten zentral gesteuert werden. Starke Passwörter, **Multi-Faktor-Authentifizierung** und die **geschulte** Konfiguration und **Nutzung** von Software spielen eine sehr große Rolle.

Schülerinnen und Schüler sowie (Vertretungs-) Lehrkräfte dürfen nur während ihrer aktiven Zeit an der Schule **Zugriff auf Systeme und Daten** erhalten. Ganz wichtig ist dabei der **Jugendschutz** für Endgeräte und das Schulnetzwerk.

[3] Julie Brill, Microsoft, Zugriff Februar 2021, https://news.microsoft.com/de-de/neue-massnahmen-zum-schutz-von-daten/

Fall bedarf es bei Nutzung eines Videokonferenzsystems der freiwilligen Zustimmung der Schülerinnen und Schüler bzw. ihrer gesetzlichen Vertreter.

Andererseits sind Maßnahmen für den **Jugendschutz** für die Schülerinnen und Schüler umzusetzen. Endgeräte, die an Schülerinnen und Schüler von Bildungsorganisationen herausgegeben werden, sind mit geeigneten Jugendschutzfiltern zu versehen. Bei privaten Geräten sind die Eltern angehalten, entsprechende Vorkehrungen zu treffen. Sowohl für die Endgeräte als auch für verschiedene Browser und andere Software bieten Hersteller sowie unabhängige Anbieter größtenteils kostenlose Jugendschutzvorkehrungen an. Diese umfassen beispielsweise Einschränkungen von Downloads und Installationen ungeeigneter oder nicht-kostenfreier Apps, die Einstellung der Nutzungsdauer und -zeiten, Filter für Werbung, Webzugriffe und Websuchen oder auch inhaltsbasiertes Filtern von Webseiten. Auch für die Notbetreuung in der Schule vor Ort ist darauf zu achten, die Nutzung des WLANs über vorkonfigurierte und mit Jugendschutzfiltern ausgestattete Zugangsprofile des Internet-Routers zu steuern. Das reine Sperren (Blacklist) oder Zulassen (Whitelist) von Internetseiten ist ein Anfang, aber nicht so sicher wie Inhaltsfilter, die den Zugriff auf Webseiten basierend auf deren Inhalt erlauben oder verweigern.

Die sichere Nutzung von IT-Systemen hängt selbstverständlich nicht unerheblich von den **Nutzenden selbst** ab. Schulungen für Lehrkräfte sowie Schülerinnen und Schüler sind so durchzuführen, dass aus organisatorischer Sicht ein reibungsloser Distanzunterricht stattfinden kann.

Ein sicheres Passwort bildet die Grundlage. Zusätzliche Sicherheit bietet die so genannte Multi-Faktor-Authentifizierung (MFA). Standardmäßig identifizieren sich Nutzer mit ihrem Wissen, indem sie das geheime Passwort nutzen. Für die MFA werden weitere Faktoren hinzugezogen, z. B. der Besitz eines Gerätes (Versand eines Tokens per SMS) oder biometrische Merkmale (Fingerabdruck). Ein Identitätsdiebstahl und missbräuchliche Nutzung von Systemen werden durch MFA enorm erschwert.

Allein die Betrachtung einer Beispielarchitektur für den sicheren Betrieb einer Videokonferenzsoftware zeigt unabhängig von organisatorischen und gesellschaftlichen Aspekten die Vielfältigkeit der zu berücksichtigenden technischen Komponenten. Auch nach der Zeit des digital gestützten Distanzunterrichts wird das Lernen gestützt durch digitale Medien mittels geeigneter Lernsoftware zunehmen. Analog zur Ermittlung der Architektur für Videokonferenzsysteme verfährt man für Lernplattformen, deren Relevanz insbesondere nach dem Distanzunterricht weiter zunehmen wird.

Die Integration unterschiedlicher und vielfältiger Software in eine einheitlich-integrative Bildungsarchitektur wird dann umso wichtiger und als gemeinsame Basis für viele Schulen auch weitaus effizienter. Man darf von den Schulen nicht erwarten, dass sie Definition und Umsetzung solch komplexer Strukturen allein leisten können. Dies kann nur mit einem gemeinsamen Ansatz gelingen, bei dem die Schulen das digitale Lernen fachlich und methodisch gestalten, während die „Digitalen Bildungsarchitekten“ den technischen Rahmen dafür bereitstellen.