Netz-Basisinfrastruktur für Berufs- und Mittelschulen des Kantons Zürich

Grobarchitektur

5. Mai 2015

Dokumentinformationen

Dokument / Ausgabe / Datum / Status

MBA_Grobarchitektur_10.docx / 1.0 / 05.05.2015 / Final

Autor(en)

Basile Bluntschli

Änderungsverzeichnis

Datum	Version	Autor	Änderung
16.01.2015	0.1	B. Bluntschli	Dokument erstellt
20.02.2015	0.6	B. Bluntschli	Rückmeldungen eingepflegt
09.03.2015	0.7	B. Bluntschli	Rückmeldungen eingepflegt
13.03.2015	0.8	.ch	Kleinere Korrekturen
08.04.2015	0.9	B. Bluntschli	Eingefügt Vorwort
05.05.2015	1.0	F. Keller	Lektorat

Inhalt

Abbildungen

Vorwort

Von Beat Stettler, Professor für Computernetze und Internet-Applikationen an der Hochschule für Technik in Rapperswil

Die Schule der Zukunft

Wenn man die Arbeitsweise der heute aktiven Generation von „Wissensarbeitern“ mit den Lernmethoden vergleicht, mit denen diese Generation aufgewachsen ist, stellt man fest, dass sich viele damals gelernte Arbeitsmethoden auf fast dramatische Weise verändert haben. Die Art und Weise der Informationsbeschaffung, die Auswertung und Bewertung von Informationen und die Art der Zusammenarbeit mit Arbeitskollegen, aber auch mit Kunden und Lieferanten hat sich in den letzten 20–30 Jahren völlig verändert und wird sich auch in Zukunft weiter entwickeln. Das Internet ist dabei fester Bestandteil der täglichen Wissensarbeit geworden und nicht mehr aus dem Alltag wegzudenken. Um heutzutage noch konkurrenzfähige Wissensarbeit leisten zu können, spielt das „lebenslange Lernen“ eine zentrale Rolle. Diese findet zu einem grossen Teil mit Hilfe des Internets statt. Die folgenden Beispiele sollen illustrieren, wie sich wichtige Tätigkeiten im Lernprozess verändert haben und wie sich diese Veränderungen auf die Infrastrukturen der Schulen auswirken.

Informationsbeschaffung

Informationen werden nicht mehr alleine von wenigen „allwissenden“ Autoritäten wie Lehrern und Büchern bezogen, sondern aus Millionen von mehr oder weniger fundierten Quellen im Internet ergänzt. Bereits im Vorschulalter lernen Kinder, mit allerlei Geräten wie Handys, Tablets und Computern umzugehen und diese immer automatisch zu verwenden, wenn sie etwas suchen oder Neues lernen wollen. Standen dabei über lange Zeit vor allem Suchmaschinen wie Google oder Online-Lexika wie Wikipedia im Vordergrund, ist es heute vor allem Youtube, das über fast jedes erdenkliche Thema ein „How-to“-Video anbietet. Und vom Zuschauen lernt es sich bekanntlich schneller als vom Lesen alleine. Zudem kann man jederzeit zurückspulen und knifflige Schritte mehrfach wiederholt anschauen. Aber auch wichtige Fähigkeiten wie Konzentrationsfähigkeit, Reaktionsfähigkeit und räumliches Vorstellungsvermögen werden dank immer realistischeren grafischen Interfaces früh geübt.

Wenn man also die Kunst des Lernens vor 20–30 Jahren mit heute vergleicht, ging es früher mehr darum, durch eine Lehrperson strukturierte Informationen aufzunehmen, anzuwenden und wiedergeben zu können. Heutzutage zeichnet sich intelligentes Vorgehen eher dadurch aus, aus einer möglichst vielfältigen Masse von unstrukturierten Informationen das Wesentliche herauszukristallisieren, zu strukturieren, auszuwerten, anzuwenden und vielleicht auch in einen breiteren Kontext zu stellen. Eine effiziente Nutzung des Internets im Kontext des Lernens muss aber auch per se gelernt sein. Hier

hat die Schule die wichtige Aufgabe, dass sie die jungen Menschen bei der Suche nach Informationen im Internet begleitet und ihnen zeigt, wie mit der unendlichen Flut von verfügbaren Informationen umzugehen ist. Um die effiziente Nutzung des Internets gewährleisten zu können, müssen die notwendigen Infrastrukturen wie Geräte (PCs, Notebooks, Tablets usw.) in genügender Menge vorhanden und mit guter Internetverbindung (z.B. über WLAN) ausgerüstet sein.

Kollaboration

Während sich die Kollaboration früher auf die Gruppenarbeit im Klassenverband beschränkte, wird heute auch ausserhalb der Schule intensiv zusammengearbeitet und kollaboriert. Hausaufgaben und offene Fragen werden in Klassenchats besprochen und Resultate geteilt. Dabei helfen meist auch die älteren Schüler mit, indem sie die Jüngeren mit Erklärungen, Hilfestellungen und früheren Prüfungsaufgaben / Lösungen versorgen (was ihnen den heutzutage wichtigen Ruhm des „Teilens“ einbringt). Das heisst, die elektronische Kollaboration im direkten Umfeld einer einzelnen Schule wird bereits intensiv gelebt und findet (auch ohne Zutun der Lehrerschaft) statt. In einer zunehmend globalisierten Welt sollte aber auch der Austausch mit Gleichaltrigen aus anderen Landesteilen oder Kulturkreisen gefördert werden, da in der globalisierten Welt nicht nur die Kollaboration mit dem näheren Umfeld wichtig ist. Vielmehr wird zum Erhalt der Konkurrenzfähigkeit die Fähigkeit benötigt, mit den unterschiedlichsten Menschen aus verschiedenen Kulturkreisen effizient über elektronische Kanäle zusammenarbeiten zu können. Dabei stehen schon heute Kollaborationsmethoden wie Team-Chats, Videokonferenzen und Workplace-Sharing, das heisst das gemeinsame Bearbeiten von Texten, Tabellen, Bildern, Präsentationen usw., im Vordergrund. Diese Technologien werden sich weiter verbessern und damit die Produktivität der Lernenden weiter steigern. Wie sich führende Technologiefirmen die produktive Kollaboration von morgen vorstellen, zeigt sehr eindrücklich das folgende Video: https://www.youtube.com/watch?v=w-tFdreZB94

Das Klassenzimmer von morgen

Unbestritten bleibt, dass sich die Arbeitsmethoden zukünftiger Jobs weiter digitalisieren und verändern werden. Der Konkurrenzkampf zwischen Wissensarbeitern aller Länder wird härter werden, da die Informationsasymmetrie zwischen armen und reichen Ländern zunehmend verschwindet. Klar ist damit auch, dass die zukünftigen Wissensarbeiter (das heisst, die Kinder von heute) über neuartige Kompetenzen verfügen müssen, die wir heute vielleicht noch gar nicht so genau kennen. Deshalb ist auch die Suche der richtigen didaktischen Ansätze für die Schule von morgen auch immer noch Gegenstand der aktuellen Forschung. Klar ist aber, dass wir traditionelle Lehrmethoden durch neuartige Formen ergänzen müssen – insbesondere, dass wir den Nachwuchs darauf ausbilden müssen, effizient und effektiv mit der stetigen Vernetzung und der unmittelbaren Verfügbarkeit unendlicher Mengen von Informationen umzugehen. Eine Verbannung der

neuen Kommunikationsmöglichkeiten aus den Klassenzimmern wäre eine verlorene Chance, der produktiven Gesellschaft von morgen eine möglichst optimale Vorbereitung auf deren Arbeitsalltag mitzugeben, und würde schlussendlich auch den zukünftigen Wohlstand unseres Landes gefährden. Dabei stellen die folgenden Technologien die Hauptpfeiler des modernen Lernens dar:

- **Kollaborations-Technologien:** Lösungen, die das Zusammenarbeiten in Teams vereinfachen, die es erlauben, auch externe Personen kurzzeitig miteinzubeziehen, die es unabhängig von geografischen Distanzen erlauben, Probleme und Lösungen einfach darzustellen und zu erklären, sei es durch Video-Elemente oder grafische Visualisierungen. Kurzum alles, was hilft, komplexe Problemstellungen im Team gemeinsam bearbeiten zu können.

- **Virtualisierungs-Technologien:** Mögliche Lösungen müssen ausprobiert werden können – am besten durch kurzfristiges Erstellen von virtuellen Umgebungen, in denen dann praktisch gearbeitet und experimentiert werden kann. Dabei können grafische Zeichnungen verwendet werden, die dreidimensional betrachtet und verändert werden können, oder aber es werden 3D-Drucker verwendet, um Modelle noch realistischer „darstellen“ und untersuchen zu können. Im Bereich der Informatik können kurzfristig virtuelle Maschinen erzeugt werden, die mit der nötigen Software zur Bearbeitung eines spezifischen Problems ausgestattet sind. Dieses können die Lernenden zur weiteren Bearbeitung auf ihr eigenes Gerät „ziehen“, mit nach Hause nehmen und dort (wie früher die Schulhefte) ablegen.

- **Allgegenwärtige Vernetzung:** Um all diese neuen Lernmethoden Realität werden zu lassen, braucht es eine nicht spürbare, sichere und genügend performante Vernetzung der Schulhäuser, die nicht zu stark einschränkt und stets auch erlaubt, Neues auszuprobieren. Selbstverständlich gehören auch Massnahmen zum Schutz der jungen Menschen vor unpassenden oder illegalen Inhalten des Internets dazu.

All dies soll nicht heissen, dass stilles und konzentriertes Arbeiten in Zukunft nicht mehr nötig wäre. Die Wichtigkeit des „in Ruhe reflektieren“ wird im Gegenteil eher zunehmen, da all die aus verschiedenen Quellen beschafften Informationen ja auch verarbeitet, strukturiert und aussortiert werden müssen. Es werden sich also Phasen mit intensiver Kommunikation mit ruhigen Phasen ablösen. Das heisst, es kann durchaus sinnvoll sein, die Vernetzung zwischendurch bewusst auszuschalten. Die Funktion der Lehrperson entwickelt sich dabei zum „Coach“ der Lernenden, der diese im Umgang mit diesen Medien unterstützt und auch die nicht technischen Aspekte wie z.B. die kritische Hinterfragung der Informationen, die zwischenmenschlichen Aspekte wie z.B. kulturelle Unterschiede usw. anspricht und damit auch die Sozialkompetenz fördert und stärkt.

1. Einführung

Um eine von den Schulen mitgetragene Lösung zu erarbeiten, hat das Mittelschul- und Berufsbildungsamt (MBA) im Zuge der Weiterentwicklung vom heutigen LEUnet zum künftigen LEUnet2 vom Kantonalen IT-Team (KITT) die Ausnahmebewilligung für den Betrieb eines dezentralen Netzes für die Sekundarstufe II erhalten (Protokoll KITT-Sitzung vom 4. April 2014, Geschäft K277-4).

In diesem Dokument wird die Basisnetzwerk-Architektur für die höheren Fach-, Berufs- und Mittelschulen des Kantons Zürich definiert. Eingeflossen in die Überlegungen sind die Erfahrungen mit bestehenden Netzwerken an den Schulen sowie der Betrieb mit dem Angebot „Schulen ans Internet“ der Swisscom. Die Architektur sieht vor, die Bedürfnisse und Technologieentwicklungen in einem Zeithorizont von 2015 bis 2025 zu erfassen

Die Nutzer des Netzwerks, das heisst Schülerinnen und Schüler, Lernende, Lehrpersonen, Ausbildner, Schulleitungen, administrative Mitarbeitende usw. sollen das Netzwerk als verlässliche Dienstleistung empfinden und die Infrastruktur im Rahmen der berechtigten Zugriffe überall performant und sicher nutzen können.

Technologietrends und neue Kommunikationsarten werden von jungen Menschen schnell aufgenommen und vollumfänglich in den Alltag integriert. Dies stellt eine permanente Herausforderung an das bisher bekannte IT-Infrastruktur-Management dar, welches mit solchen Neuerungen versucht, Schritt zu halten. In neuerer Zeit hat sich in der Arbeitswelt das Konzept des „Bring your own Device“ (BYOD) etabliert. Damit ist gemeint, dass die Mitarbeitenden ihre eigenen Geräte zunehmend selbst auswählen und auch selbst verwalten. Die Aufgabe der Informatikabteilung fokussiert sich in diesem Fall vor allem darauf, jedem User resp. jedem Gerät einen gesicherten Zugriff auf die berechtigten internen und externen Ressourcen zu gewährleisten. Technisch ist dazu eine dynamische Netzzugangskontrolle (Network Access Control) zu implementieren, welche sowohl drahtgebundene wie auch drahtlose Anschlüsse sichert.

Im schulischen Umfeld kann dieses Konzept wie folgt illustriert werden: Zu jedem Zeitpunkt an jedem Schulstandort ist der Zugriff auf die notwendigen Infrastrukturmittel sicher und sinnvoll möglich. Dies kann beispielsweise bedeuten, dass der Wireless Beamer in einem Schulzimmer auch von den Lernenden mit ihren eigenen mobilen Geräten für Präsentationen genutzt werden kann. Das Ansteuern soll intuitiv möglich sein. Gleichzeitig sollen nur die Beamer in der Nähe überhaupt ansprechbar sein und eine Lehrperson geniesst immer die Priorität beim Zugriff auf einen Wireless Beamer.

1.1. Eckwerte

1. Chancengleichheit – Netzwerkstandards
Im Kontext der Chancengleichheit sollen alle Schulstandorte den gleichen oder zumindest einen ähnlichen Ausbaustandard bezüglich Netz-Basisinfrastruktur aufweisen.

2. Arbeits-, Lehr- und Lernwelt
Die Netz-Basisinfrastruktur soll ein analoges Arbeiten, Lernen und Lehren ermöglichen, wie das am Arbeitsplatz, im Hochschul- oder im privaten Bereich möglich ist.

3. Zugang zu den Schulorganisationsdiensten und kantonalen Services
Den Bildungsinstitutionen sollen zwei Anschlussvarianten zur Verfügung gestellt werden:

1. WEB: Zugang via VDI-Plattform (Virtual Desktop Infrastructure), bisherige Lösung Mittelschulen oder Citrix, bisherige Lösung für Teile der Berufsschulen. Internet, LAN, WLAN usw. sollen durch die Bildungsinstitutionen selber organisiert werden unter Einhaltung gewisser Vorgaben: Netzwerkstandards Berufs- und Mittelschulen Kanton Zürich, Datenschutz, GATT/WTO-konforme Ausschreibungen usw.
2. WAN-Anschluss: Vollservicepaket Netz-Basisinfrastruktur: gemanagter Internet-Anschluss, LAN, WLAN, Firewall, URL-Filter, Anbindung DataCenter, Authentifizierung, Eduroaming, VOIP usw. Netzwerkbedürfnisse der Schulen, die über die Netz-Basisinfrastruktur hinausgehen, sollen diese selber planen und betreiben im Rahmen von Labor- und Fachschaftseinrichtungen.

4. WAN-Anschluss
Mit dem WAN-Anschluss übergibt die Schule den Betrieb des Netzwerks an einen Dienstleister (NOC). Dieser zeichnet verantwortlich für Zugang zum Netz (Authentifizierung), Betrieb Internetanbindung, LAN, WLAN, Betrieb Firewall, URL Filter, Anbindung DataCenter. Für alle Netzbelange gibt es einen Single Point of Contact.

5. Konsolidierte Netz-Basisinfrastruktur
Mittelfristig wird der Betrieb von zwei DataCentern (evtl. Zürich und Winterthur) vorgesehen. Der Anschluss einzelner Bildungsinstitutionen oder einzelner Standortverbünde erfolgt ebenfalls redundant.

6. Organisation NOC
Für den Betrieb einzelner Dienste, Authentifizierungs-Services, Internetanbindung, Firewall, Content filter, LAN, WLAN, Betrieb DataCenter sollen die IT-Services einzelner Schulen gemäss ihren Fachkompetenzen involviert werden. An jeder beteiligten Schule übernimmt das IT-Team Fieldforce-Aufgaben.

7. Migration
Die Migration erfolgt generisch innerhalb der normalen Hardwareerneuerungszyklen.

8. Finanzen
Die Kosten für den Betrieb der Netzwerk-Basisinfrastruktur werden nach einem zu bestimmenden Schlüssel zwischen den Schulen und der Verwaltung aufgeteilt.

2. Ausgangslage

Durch die schnelle Entwicklung im Umfeld der Informations- und Kommunikationstechnologie entstand an den meisten Schulen ein sehr hoher Entwicklungsbedarf in der pädagogischen Informatik bezüglich Ausbau der Basisinfrastruktur (WLAN, LAN und Internetanbindung mittels Glasfaser). Einer der Haupttreiber dieser Entwicklung sind die vielen verfügbaren persönlichen mobilen Geräte (Notebooks, Tablets und Smartphones) der Lehrpersonen und der Lernenden. Ein weiterer Treiber sind die zunehmend im Internet verfügbaren Bildungsinhalte wie Online-Lernplattformen, Lexika, TV- und Videoprovider. Aber auch Cloud-Dienste und Web-Services bieten zunehmend pädagogisch wertvolle Inhalte für den Schulalltag an.

Die zunehmende Automatisierung von Prozessen sowie die Verknüpfung verschiedener Datenquellen zeigen zudem, dass die physische Trennung des Netzwerks der Schulverwaltung und des „pädagogischen Netzes“ überholt ist. Viele Services und Inhalte müssen je nach Benutzergruppe in beiden „Welten“ verfügbar sein, wie nachfolgende Beispiele zeigen:

- Lernplattform basiert auf den Schulverwaltungsdaten der Lehrpersonen, der Lernenden, der Klassen, der Freifachkurse usw.
- Spezialdrucker für Broschürendruck
- Zugang zu netzgebundenen Bildungsinhalten sollte im pädagogischen und im Schulverwaltungsnetz verfügbar sein.
- Weitere übergreifende Services sind: Noteneingabe, Klassen- und Schülerlisten, Stundenkonto Lehrpersonen, Finanzen, Budget, Personalverfügungen, Adressdaten von Mitgliedern der Schulkommissionen usw.
- Die Ablösung der Schulverwaltung Eco Open durch eine neue Software wird erhöhte Anforderungen an das Netz stellen.

Die Schulen stehen dabei alle vor identischen Entwicklungsaufgaben. Wie wird der grosse Netzbedarf der Lehrpersonen und der Lernenden gedeckt? Wie sieht die Netzarchitektur aus? Welche logischen Netze werden benötigt? Wie wird die Zugangskontrolle resp. Authentifizierung gelöst? Wie implementiert man die neuen Zugänge zu den kantonalen Services unter Berücksichtigung der Vorgaben des KITT bezüglich Datensicherheit und Datenschutz?

Alle diese Aufgaben lassen sich am besten durch ein gemeinsames koordiniertes Planen und Entwickeln von standardisierten und allseits genutzten Netzdiensten lösen. Durch die Bündelung aller Kräfte lassen sich erhebliche Ressourcen einsparen.

Das Netzwerkkonzept baut auf den Erkenntnissen aus der Umfrage zur Basisinfrastruktur (2013) und den Vorarbeiten und Erkenntnissen aus dem Projekt “Basisinfrastruktur (2012)“ auf.

2.1. Vorgaben

Für die Grobarchitektur gelten folgende Vorgaben:

- AGB SIK, Ausgabe 2015
- Gesetz über die Information und den Datenschutz (IDG) vom 12. Februar 2007
- Verordnung über die Information und den Datenschutz (IDV) vom 28. Mai 2008
- Informatiksicherheitsverordnung (ISV) vom 17. Dezember 1997 (in Revision)
- Allgemeine Geschäftsbedingungen über die Geheimhaltung, den Datenschutz und die Daten- und Informationssicherheit bei der Erbringung von Informatikdienstleistungen (AGB Sicherheit des Kantons Zürich, 2011)
- Gesetz über die Auslagerung von Informatikdienstleistungen vom 23. August 1999
- Informatikstrategie und -eckwerte für die Sekundarstufe II
- Netzwerkstrategie des Kantons Zürich vom 16. August 2013
- Konzept LEUnet2, 20. Dezember 2013
- Network Security Policy KITT

2.2. Mehrwert angeschlossene Schulen

Für die angeschlossenen Schulen bildet der gemeinsame Betrieb einer konsolidierten Netzwerk-Basisinfrastruktur folgende Vorteile:

- Kantonale Richtlinien DSG, IDG, GATT müssen nur einmal berücksichtig und überprüft werden. Bei Audits des Datenschutzbeauftragten kann auf den gemeinsamen Betreiber verwiesen werden.
- Die Netzwerk-Basisinfrastruktur deckt 80% des Bedarfs der Schulen ab und stellt so den Betrieb sicher.
- Zusätzliche schulspezifische IT- und Netzbedürfnisse kann die Schule individuell entwickeln und betreiben.
- Der redundante Betrieb verschiedener Dienste ist wirtschaftlich und technisch möglich.
- Mit dem redundanten Setting ist nicht nur auf dem Papier, sondern auch technisch eine hohe Performance und Verfügbarkeit gewährleistet.
- Mittels Bildung von Clustern (Schulen auf dem gleichen Campus oder benachbarte Institutionen) lassen sich wirtschaftlich sinnvolle Grössen bilden. Durch die gemeinsame Nutzung lassen sich Dienste und Dienstqualitäten finanzieren, die alleine nicht tragbar wären.

3. Anforderungen an ein modernes Netzwerk

Es wurden unterschiedliche Dokumente zur Arbeitsweise und zu den Anforderungen heutiger Schulen der Sekundarstufe II erstellt.

- Dossier „Bildung im Netz 2010–2015“
- Dossier ICT-Basisinfrastruktur
- Persönliche Geräte ans Schulnetz, Pegasus, Kanton Luzern

Kurz zusammengefasst sind folgende Anforderungen zentral:

- einfacher Zugriff auf die benötigten Dienste
- performanter Zugriff auf die benötigten Dienste
- eindeutige Identifizierung des Benutzers
- hohe Verfügbarkeit des Netzwerks
- nutzbar mit eigenem, selbstgewählten Gerät
- Folgende Dienste haben dabei eine sehr hohe Priorität:
    - Zugriff auf Unterrichtssysteme wie: Beamer, Audiosysteme, interaktive Wandtafeln und Drucker
    - Zugriff auf das Internet für Lerninhalte wie: Moodle, Olat, Educanet2, Nanoo.tv, Youtube, Khan Academy, Dateiaustauschsysteme usw.
    - Zugriff auf Verwaltungssysteme wie Mitarbeiterverwaltung, interne Dokumente für die Schulverwaltung
    - Kommunikation mittels Telefonie, Video und Chat-Systemen

3.1. Nutzungsverhalten

Aus den Erfahrungen des MBA besteht der Netzwerkverkehr zu einem überragenden Anteil aus Internet-Zugriffen (80%). Die restlichen Prozente sind aber nicht zu vernachlässigen, da es sich dabei um administrative Arbeiten wie Zugriff auf die Dienste SAP und Pulse handelt, die für die Verwaltung und Organisation einer Schule existenziell sind.

3.2. Sicherheit beim Zugriff auf schulinterne Systeme

Die Sicherheit auf applikatorischer Ebene wird durch Usernamen und Passwort oder sinngemässe Sicherheitsvorkehrungen geschützt. Mit dem Netzzugang wird durch die Identifikation der Benutzer der Zugriff auf Login-Portale von Applikationen ermöglicht. Damit sind unbekannte Login-Versuche auf die schulinternen Systeme zum grossen Teil ausgeschlossen.

3.3. Benutzergruppen

Bei der Definition der Benutzergruppen wurden die grösstmöglichen Gemeinsamkeiten zusammengefasst. Daraus haben sich die drei wesentlichen Benutzergruppen Lehrpersonen, administratives Personal, Lernende und Gäste herauskristallisiert. Dabei

haben Lehrpersonen, lernende Personen und das administrative Personal einen direkten Bezug zu der Schule, das heisst, sie sind angestellt oder in der Schule eingeschrieben, dadurch sind die persönlichen Daten bekannt. Gäste hingegen sind Personen, die nicht bekannt sind und die keine direkte Beziehung zur Schule haben müssen. In der Gruppe Lehrpersonen sind auch administrative Angestellte mit eingeschlossen, die keinen Lehrauftrag besitzen. Die Gruppe der Lehrpersonen wird weiter unterteilt in eine Gruppe mit selbstverwalteten Geräten und eine Gruppe mit Geräten, die durch die Informatik-Dienste verwaltet werden.

3.3.1. Lehrpersonen und administratives Personal

In dieser Gruppe sind alle Personen zusammengefasst, die eine Anstellung resp. einen Lehrauftrag an einer Schule inne haben, das heisst Lehrpersonen, Fachlehrer, Mitglieder der Schulorganisation, Rektoren, Prorektoren, Adjunkte, Sekretariatsmitarbeiter, administrative Angestellte, Mitarbeitende der Aufsichtskommission usw. Im Kanton Zürich beinhaltet dies die folgende Anzahl an Benutzern:

- 3074 Lehrpersonen Mittelschulen
- 3228 Lehrpersonen Berufsschulen
- 75 Schulsekretariate, Rektorate, Haus- und Informatikdienste
- 12 000 Mitarbeitende Qualifikationsverfahren
- 18 000 Total

Die Daten, die dieser Personenkreis benötigt resp. produziert, sind zum Teil persönlich und darum mit einem starken Schutz vor Fremdeinflüssen und unerwünschten Zugriffen zu versehen. Mit dem Netzzugang wird sichergestellt, dass eine sich einloggende Person eindeutig identifiziert werden kann.

Diese Gruppe wird unterteilt in selbstverwaltete Geräte und in Geräte die durch die Informatik-Dienste verwaltet werden. Durch diese Unterteilung, kann eine stärkere Sicherheit bei den verwalteten Geräten sichergestellt werden. Bei den verwalteten Geräten können Sicherheitsvorgaben wie Anti-Virus- und Malware-Erkennungsprogramme mit aktuellen Signaturen durchgesetzt werden.

3.3.1.1. Lehrpersonen und Mitarbeiter am Standort Schule

Typische Dienste: Webservices, Lernplattform, Schulverwaltung, Intranet2, Citrix, Virtual Desktop Infrastructure (VDI)

Verwendete Geräte durch die Lehrpersonen: in der Regel persönliche, selbstverwaltete Geräte, Smartphones, Tablets, Computer (ausgenommen davon sind die administrativen Mitarbeitenden die hauptsächlich schuleigene Systeme verwenden).

3.3.1.2. Lehrpersonen mit Standort ausserhalb der Schule

Lehrpersonen bereiten sich auch ausserhalb der Schulgebäude auf ihren Unterricht vor. Dabei ist der gleiche Zugriff auf die Infrastruktur notwendig, wie er auch vor Ort an der Schule möglich ist. Davon ausgenommen sind der Zugriff auf Drucker und Wireless Beamer oder anderweitige nur lokal sinnvolle Infrastruktur.

Die verwendeten Dienste umfassen Webservices, Lernplattformen, Schulverwaltung, Intranet2, Virtual Desktop Infrastructure (VDI)

3.3.1.3. Administratives Personal am Standort Schule

Typische Dienste, die dabei an der Schule genutzt werden, umfassen die Schulverwaltung, Intranet2, Citrix, Virtual Desktop Infrastructure (VDI), Fat Client SAP.

Verwendete Geräte werden in der Regel durch die Informatik-Dienste verwaltet.

3.3.1.4. Administratives Personal ausserhalb der Schule

Typische Dienste, die ausserhalb der Schule genutzt werden: Schulverwaltung, Intranet2, Citrix, Virtual Desktop Infrastructure (VDI).

Verwendete Geräte werden in der Regel durch die Informatik-Dienste verwaltet.

3.3.2. Lernende

In dieser Gruppe sind alle Lernenden zusammengefasst: Schüler, Lernende, Besucherinnen und Besucher von Weiterbildungskursen, Mitglieder höherer Fachschulen usw. Im Kanton Zürich beträgt die Anzahl der Benutzer gemäss Publikation „Die Schulen im Kanton Zürich 2013/2014“:

- 6716 Gymnasium 7., 8. und 9. Schuljahr
- 9128 Gymnasium ab 10. Schuljahr
- 42 354 Personen berufliche Grundbildung
- 60 000 Total

3.3.2.1. Lernende am Standort Schule

Typische Dienste, die dabei an der Schule genutzt werden, umfassen Webservices, Lernplattformen, Dateiablage der Schule via Schulgeräte, Zugriff auf Wireless Beamer, Drucker. Je nach Schule haben Lernende oft keinen Zugang zu Diensten innerhalb der Schule mit persönlichen, selbstverwalteten Geräten.

Geräte: persönliche, selbstverwaltete Geräte, Smartphones, Tablets und Computer.

3.3.2.2. Lernende mit Standort ausserhalb der Schule

Typische Dienste, die dabei genutzt werden, umfassen Webservices, Lernplattformen.

Geräte: persönliche, selbstverwaltete Geräte, Smartphones, Tablets und Computer.

3.3.3. Gäste

Gäste umfassen alle weiteren Personen, die nicht mit den beiden Gruppen Lehrpersonen und Lernende erfasst sind. Dabei ist die Identität der Personen oftmals unbekannt.

3.3.3.1. Gäste am Standort Schule

Der Zugriff beschränkt sich auf das Internet. Weitere schulinterne Dienste sind nicht notwendig. Bei den Geräten handelt es sich ausschliesslich um selbstverwaltete Geräte der Gäste. Der Zugriff der Gäste soll einfach, selbsterklärend und selbstverwaltbar sein. Die Randdaten der Benutzung sollen für 6 Monate aufgezeichnet werden. Die Registrierung soll ohne weitere Kontakte mit Personal der Schulen möglich sein. Als gültige Identifikation wird eine Mobile-Nummer vorausgesetzt, welche bei der Registrierung angegeben wird. An diese Mobile-Nummer wird der Zugangstoken via SMS versandt. Durch die Mobile-Nummer kann bei einer Straftat von den Untersuchungsbehörden auf die Person geschlossen werden.

3.3.4. Weitere Systeme

Geräte wie Drucker, Beamer, Überwachungskameras und Steuergeräte der Haustechnik müssen ebenfalls in das Netzwerk integriert werden. Die Geräte müssen auch integriert werden können, wenn keine Authentifizierung von den Geräten unterstützt wird.

3.4. Verwendete Geräte

Die Gerätevielfalt an den Schulen ist sehr hoch. Mehrheitlich werden mobile Geräte wie Notebooks, Tablets und Smartphones verwendet. Die Netzwerkinfrastruktur muss aber mit allen möglichen Geräten umgehen können, die kabelgebunden oder kabellos via Ethernet das IPv4- und zukünftig das IPv6-Protokoll verwenden.

Der Wireless-Zugang wird jetzt und in Zukunft der hauptsächliche Zugang für Geräte der Benutzer sein.

Neben den Geräten der Benutzer ist eine Vielzahl an unterschiedlichen Geräten in einem Netzwerk vorhanden. Dies umfasst Geräte wie Drucker, Kameras, Gebäudeautomationsgeräte, Serversysteme usw. Weiter ist festzuhalten, dass auch Geräte wie Beamer, Kameras, Drucker vermehrt die Möglichkeit haben, kabellos auf das Netzwerk zuzugreifen. Bei vorhandener Gebäudeverkabelung ist die kabelgebundene Anbindung für Geräte, die keine Mobilität erfordern, weiter zu bevorzugen.

Infrastrukturgeräte, die sich mittels Multicast DNS selber als lokalen Dienst im Netzwerk bekannt machen, sind zu berücksichtigen und so zu integrieren, dass ein sinnvolles Erkennen und Nutzen durch die Benutzer gewährleistet ist.

3.5. Verfügbarkeit

Die Verfügbarkeit beschreibt den Prozentsatz, mit welcher ein System oder ein Netzwerk korrekt funktioniert (z.B. 99.9% der Zeit über ein Jahr). In der Telekommunikation hat sich bewährt, Systeme mit hoher verlangter Verfügbarkeit redundant auszulegen. Das heisst, es wird ein zweites sekundäres System installiert, das die Funktionen des primären Systems bei dessen Ausfall vollumfänglich erfüllen kann. Technisch gibt es die Möglichkeit, die Systeme aktiv/passiv oder aktiv/aktiv zu betreiben.

Wichtig ist, dass die erwartete Verfügbarkeit der Kunden mit der technischen Verfügbarkeit der Systeme korreliert.

Bei einem Netzwerkdesign wird oft das gesamte Netzwerk redundant aufgebaut und Single Point of Failures vermieden. Davon ausgenommen werden aus Kostengründen meist die Access-Zugänge in das Netzwerk (das heisst die Access Switches oder WLAN Access Points). Ein Computer wird demnach normalerweise nicht mit zwei Kabeln an unterschiedliche Switches an das Netzwerk angebunden. Die Endgeräte werden als Single-Systeme betrachtet. Der Ausfall einzelner Endgeräte wird normalerweise in Kauf genommen.

Die Redundanz eines Netzwerks ist mit Mehrkosten und einer höheren Komplexität verbunden. Bei tieferen Verfügbarkeitsanforderungen an das Netzwerk kann häufig auch auf Redundanzen verzichtet werden. Dabei ist wichtig zu verstehen, dass ein einzelner Fehler das gesamte Netzwerk ausser Betrieb setzen kann. Die Wiederherstellung des Betriebs in einem solchen Fall kann bei fehlendem Ersatzmaterial oder entsprechenden Supportverträgen bis zu mehreren Tagen dauern.

4. Netzwerk-Basisinfrastruktur

Im Wandel der Zeit haben sich Wasser- und Stromversorgung zu Basisdiensten entwickelt, die überall selbstverständlich verfügbar sind. Mit der Informatik verhält es sich in vielen Bereichen ähnlich, sind doch die Basisdienste wie Internet und Telekommunikationsdienste nicht mehr wegzudenken.
Das MBA möchte den Schulen eine solche konsolidierte Informatik-Basisinfrastruktur als Dienst zur Verfügung stellen. Die Synergieeffekte, die dabei erzielt werden können, sind hoch einzuschätzen:

- Erhöhte Wirtschaftlichkeit bei Preisverhandlungen durch grösseres Volumen
- Erhöhte Wirtschaftlichkeit bei Personalkosten durch Konsolidierung des Know-hows
- Homogenität in Bezug auf Hersteller und Produktewahl
- Homogenität in Bezug auf Design und Aufbau der Netzwerke
- Homogenität in Bezug auf den Betrieb durch identische Prozesse und Nutzerzugänge
- Synergienutzung von zentralen Komponenten wie z.B. der WLAN Controller, Management Tools

Folgende Dienste sollen durch einen externen Anbieter zur Verfügung gestellt werden:

- Modul Managed LAN und WLAN
- Modul Managed WAN
- Modul Firewall
- Modul Content Filter
- Modul Userverwaltung
- Modul Mail
- Modul VoIP
- Modul Cloud / Compute Ressources
- Modul IPAM, DNS, DHCP
- Modul Internet

Mit diesen Diensten kann die Basisinfrastruktur Telekommunikation, Vernetzung und Internet aus einer Hand bereitgestellt werden. Die Schulen können sich auf das eigentliche Unterrichten und Verwalten konzentrieren. Darüber hinausgehende Bedürfnisse bezüglich IT und Netzwerk kann die Schule im Rahmen von Laboraufbauten selber betreiben.

4.1. Externe Einflüsse

Einige dieser Basisdienste sind externen Einflüssen ausgesetzt resp. von den Diensten weiterer Drittanbieter abhängig.

4.1.1. Schwierigkeit Lufthoheit

Das Frequenzspektrum des Wireless LAN befindet sich in unlizenzierten Bereichen. Dadurch wird das Band auch von Modellflug, drahtlosen Telefonen, Bluetooth, Mikrowellen und vielen weiteren Geräten verwendet. Dies stellt eine besondere Herausforderung an

Wireless LAN dar. Es muss daher immer von Störeinflüssen ausgegangen werden. Diesen Einflüssen kann zum Teil mit sinnvollen Automatismen begegnet werden. Zusätzlich können Störeinflüsse eingegrenzt werden, wenn das Medium Luft an den Standorten durch Messungen ausgewertet und beim Aufbau der Infrastruktur mit einbezogen wird.

Wichtig bei einem Wireless LAN ist, dass der Zugriff einfach, sicher und flächendeckend möglich ist. Wenn das Wireless LAN für die Benutzer nicht zufriedenstellend funktioniert, werden häufig nicht konforme eigene Lösungen eingesetzt. Dies wirkt sich störend auf die Frequenzspektrum-Belegung und die Performanz und die Stabilität des Wireless-Signals aus. So werden meist auch die Sicherheitsmechanismen ausgehebelt oder stark beeinträchtigt. Aus diesem Grund muss ein von der Schule unterhaltenes Wireless LAN grundsätzlich sehr gut funktionieren. Eigenständige Wireless-Installationen sind zu unterbinden.

4.1.2. Standortvernetzung

Bei den durch das MBA vertretenen Schulen handelt es sich um ca. 40 Standorte, die über den Kanton Zürich verteilt sind. Die folgende Karte gibt einen Überblick über die Verteilung auf dem Kantonsgebiet:

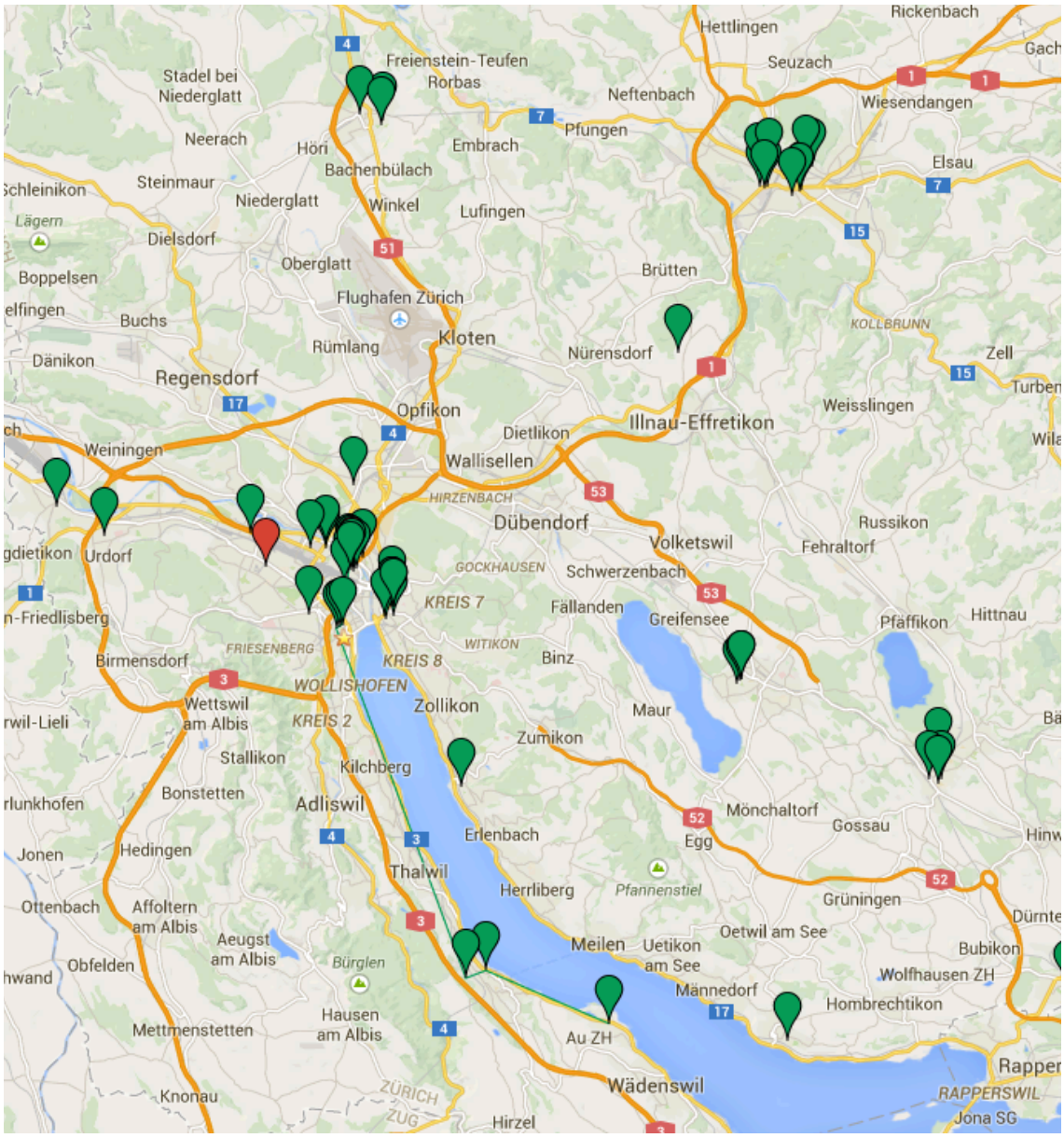

Abbildung 1: Geografische Übersicht über die beteiligten Schulen des MBA

Die Standorte müssen vor allem auf Internetdienste zugreifen können. Zudem müssen die Zugänge für kantonale Services sicher und hochverfügbar bereit stehen. Der Vorteil der

geografischen Nähe der Schulen ermöglicht, verschiedene Arten der Standortvernetzung in Betracht zu ziehen. Die Distanzen zwischen den Schulen befinden sich in einem Rahmen, der mittels üblicher Netzwerkhardware abdeckbar ist.

5. Architektur

Eine Architektur eines Netzwerks wird mittels spezifischen Building Blocks dargestellt. Ein Building Block basiert auf ähnlichen Anforderungen an das Netzwerk, die sich an bestimmten Standorten ergeben und wird meist durch eine oder mehrere Netzwerkkomponenten umgesetzt. Durch diese Abstrahierung kann auf Grund der detaillierten Anforderungen ein Netzwerkdesign basierend auf verschiedenen Building Blocks abgeleitet werden. Die folgenden Building Blocks wurden während der Anforderungsanalyse der verschiedenen Schulen identifiziert.

Access	Zugang der Benutzer auf das Netzwerk, basierend auf kabelgebundenen LAN oder Wireless LAN
Authentifizierung	Eindeutige und sichere Identifikation des Benutzers inklusive der Authorisierung der notwendigen Zugriffsmöglichkeiten
Infrastruktur Schulen	Schulinterne Infrastruktur wie Beamer, Drucker, Haussteuerung, LAN usw.
WAN	Verbinden der Schulen mit dem Internet und standortübergreifenden Diensten
Konsolidierte Infrastruktur	Dienste, die schulübergreifend durch das MBA zur Verfügung gestellt werden
Netzübergang LEUnet2	Zentrale Dienste für kantonale Angestellte (SAP und Pulse, Eco Open, Compass)
Netzübergang Internet	Zugang zum Internet

Die Building blocks sind nachfolgend grafisch dargestellt. Die Pfeile stellen die hauptsächlichen Kommunikationsrichtungen dar.

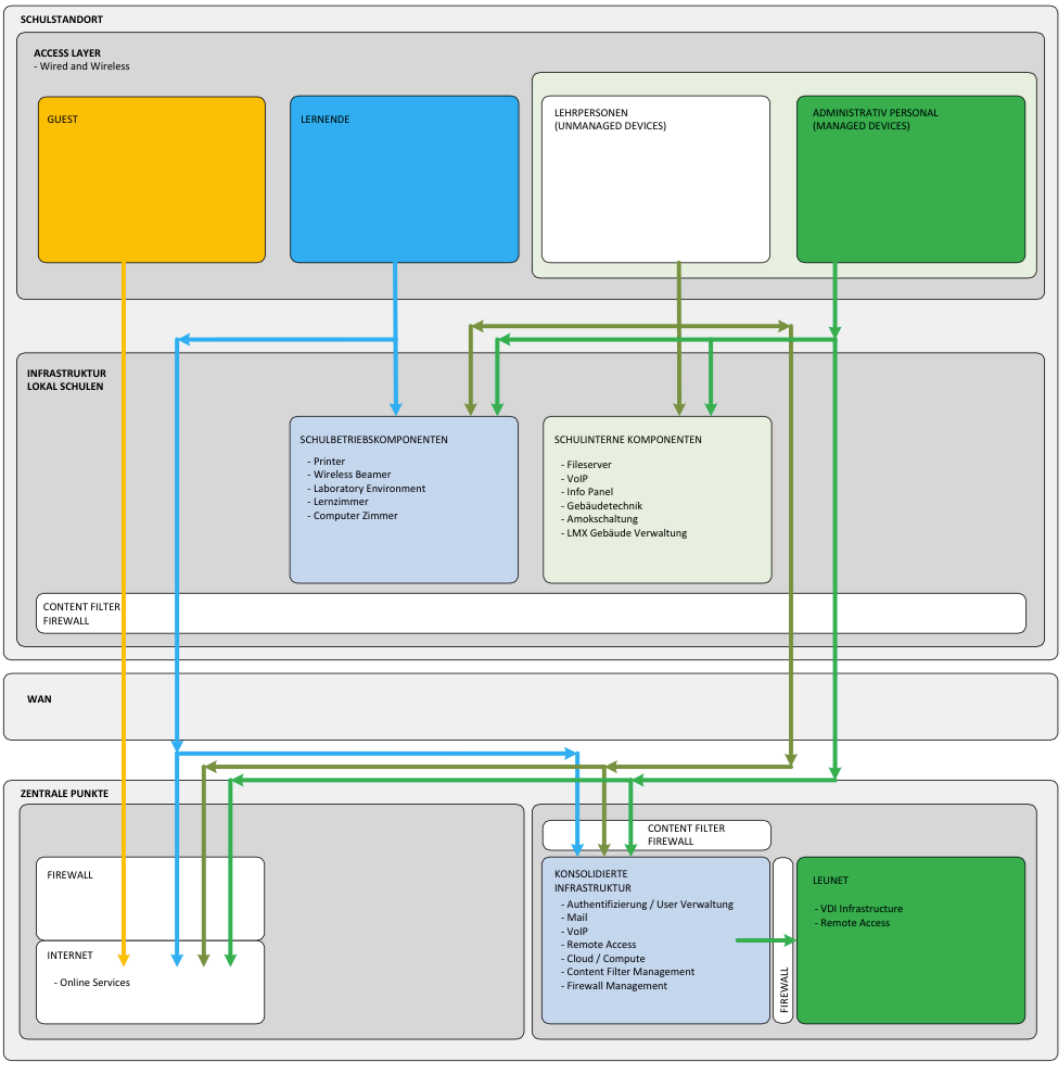

Abbildung 2: Grobarchitektur Building blocks

5.1. Access

Der Netzzugriff durch Endgeräte wird als Building block Access bezeichnet. Dabei handelt es sich um Wireless- und Wired-Zugang. Der Zugriff auf das Netzwerk stellt die erste Möglichkeit dar, User anhand ihrer notwendigen Zugriffsrechte zu unterscheiden und logisch getrennten Zugriff auf das Netzwerk zu erteilen. Folgende Use Cases sind dabei definiert worden:

5.1.1. Lehrpersonen (unmanaged devices)

- Geräte: selbstverwaltet
- Zugriff: wireless und wired
- Sicherheit: hohe Sicherheit, Verschlüsselung mittels WPA2, Authentifizierung mittels PEAP
- Zugriff: Shared Infrastruture Schule, Internal Infrastructure Schule, MBA-Dienste, Internet
- Unterrichtsunterstützende Geräte (Beamer, Apple TV, Drucker)
- Problemstellen: Selbstverwaltung der Geräte ermöglicht kein Erzwingen von Sicherheitsparametern

Wireless: Die Lehrperson verbindet sich mit der verschlüsselten SSID SECURE. Dabei wird sie aufgefordert, ihren Usernamen und ihr Passwort einzugeben. Auf Grund von Gruppenzugehörigkeiten innerhalb eines Directory Services werden dynamische Attribute zurückgeliefert, welche es den Wireless-Komponenten erlauben, die Lehrperson in die korrekte Zone innerhalb des Building block Access zuzuweisen. Technisch wird während der Anmeldung am Wireless durch die Wireless-Komponenten eine Authentifizierungsanfrage an den Radius Server gestellt, welcher bei erfolgreicher Authentifizierung einen Wert für eine VLAN ID zurückliefert. Die Authentifizierungstechnologie ist dabei 802.1x PEAP (Protected EAP), welche mit Usernamen und Passwort authentifiziert.

Wired: Der Zugriff funktioniert prinzipiell gleich wie bei der Wireless-Infrastruktur. Die Lehrperson verbindet sich aber anstatt mit einer SSID mittels eines Kabels mit der Netzwerkinfrastruktur. In diesem Fall mit einem Switch, welcher die Technologie 802.1x und PEAP unterstützt und dabei auch dynamische Attribute verarbeiten kann.

Nach der erfolgreichen Authentifizierung befindet sich die Lehrperson in der Zone LEHRPERSONEN und hat die notwendigen Zugriffsrechte innerhalb des Netzwerks.

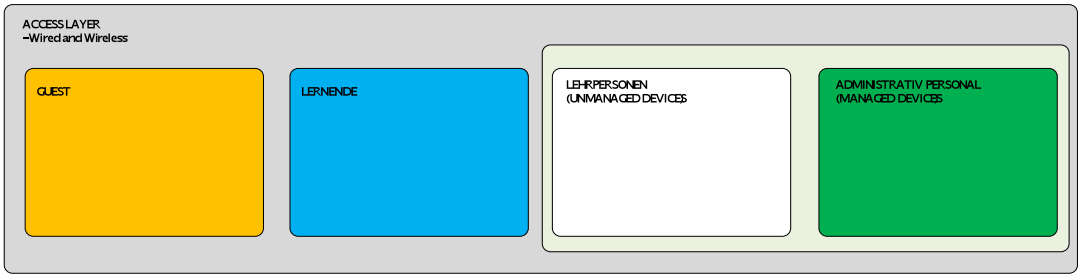

Abbildung 3: Building block Access

5.1.2. Verwaltungsmitarbeitende (managed devices)

- Geräte: verwaltet durch Informatik-Dienste
- Zugriff: wireless und wired
- Sicherheit: höchste Sicherheit, Verschlüsselung mittels WPA2, Authentifizierung mittels X.509-Zertifikaten

- Zugriff: Shared Infrastructure Schule, Internal Infrastructure Schule, MBA-Dienste, LEUnet, Internet
- Problemstellen: Sicherheit muss gewährleistet sein, damit der Zugriff auf das SAP via LEUnet mit der nativen Applikation möglich ist (Kein VDI- oder VPN-Client-Start notwendig).

Wireless: Der Verwaltungsmitarbeitende verbindet sich mit der verschlüsselten SSID SECURE, dabei erfolgt die Anmeldung automatisch. Die Authentifizierung basiert auf einem Client-Zertifikat, das von einer internen Certificate Authority für nur diesen User und dessen Notebook ausgestellt wurde. Auf Grund von Gruppenzugehörigkeiten innerhalb eines Directory Services werden dynamische Attribute zurückgeliefert, welche es den Wireless-Komponenten erlaubt, den Verwaltungsmitarbeitenden in die korrekte Zone innerhalb des Building block Access zuzuweisen. Technisch wird während der Anmeldung am Wireless durch die Wireless-Komponenten eine Authentifizierungsanfrage an den Radius Server gestellt, welcher bei erfolgreicher Authentifizierung einen Wert für eine VLAN ID zurückliefert. Die Authentifizierungstechnologie ist dabei 802.1x EAP-TLS, welche mit Client-basierten Zertifikaten (x.509) authentifiziert. Diese Technologie gilt als aktuell sicherste Methode, auf ein Netzwerk zuzugreifen. Banken setzen dieses Verfahren im Wireless-Umfeld ebenfalls ein.

Wired: Der Zugriff funktioniert prinzipiell gleich wie bei der Wireless-Infrastruktur. Der Verwaltungsmitarbeitende verbindet sich aber anstatt mit einer SSID mittels eines Kabels mit der Netzwerkinfrastruktur. In diesem Fall mit einem Switch, welcher die Technologie 802.1x und EAP-TLS unterstützt und dabei auch dynamische Attribute verarbeiten kann.

Nach der erfolgreichen Authentifizierung befindet sich der Verwaltungsmitarbeitende in der Zone VERWALTUNG und hat die notwendigen Zugriffsrechte innerhalb des Netzwerks. Mit dieser sicheren Authentifizierung kann auch mittels Fat Clients direkt auf Verwaltungssoftware bei LEUnet zugegriffen werden.

5.1.3. Lernende

- Geräte: selbstverwaltet
- Zugriff: wireless und wired
- Sicherheit: hohe Sicherheit Verschlüsselung mittels WPA2, Authentifizierung mittees PEAP
- Zugriff: Shared Infrastruture Schule, Intranet2, Internet
- Problemstellen: Selbstverwaltung der Geräte ermöglicht kein Erzwingen von Sicherheitsparametern

Wireless: Der Lernende verbindet sich mit der verschlüsselten SSID SECURE. Dabei wird er aufgefordert, seinen Usernamen und sein Passwort einzugeben. Auf Grund von Gruppenzugehörigkeiten innerhalb eines Directory Services werden dynamische Attribute zurückgeliefert, welche es den Wireless-Komponenten erlauben, den Lernenden in die korrekte Zone innerhalb des Building block Access zuzuweisen. Technisch wird während der Anmeldung am Wireless durch die Wireless-Komponenten eine Authentifizierungsanfrage an den Radius Server gestellt, welcher bei erfolgreicher Authentifizierung einen Wert für eine VLAN ID zurückliefert. Die

Authentifizierungstechnologie ist dabei 802.1x PEAP (Protected EAP), welche den Lernenden anhand seines Usernamens und und seines Passworts authentifiziert.

Wired: Der Zugriff funktioniert prinzipiell gleich wie bei der Wireless-Infrastruktur. Der Lernende verbindet sich mittels eines Kabels mit der Netzwerkinfrastruktur. In diesem Fall mit einem Switch, welcher die Technologie 802.1x und PEAP unterstützt und dabei auch dynamische Attribute verarbeiten kann.

Nach der erfolgreichen Authentifizierung befindet sich der Lernende in der Zone LERNENDE und hat die notwendigen Zugriffsrechte innerhalb des Netzwerks.

5.1.4. Gäste

- Geräte: selbstverwaltet
- Zugriff: wireless
- Sicherheit: keine Sicherheit, Aufzeichnen von Randdaten
- Zugriff: Internet
- Problemstellen: SSID muss unverschlüsselt sein, prinzipbedingt bei öffentlichen Guest-Wireless-Netzen

Wireless: Der Gast verbindet sich mit der unverschlüsselten SSID GUEST. Mittels eines Captive-Portals wird der Zugriff auf das Internet unterbunden. Jeglicher Webzugriff auf das Internet wird auf die Landing Page des Captive-Portals redirected.

Nach erfolgreicher Registrierung mit der Mobile-Nummer auf dem Captive Portal und der Eingabe des via SMS zugesendeten Tokens wird dem Gast der Internet-Zugriff gewährt. Interne Dienste sind für den Gast nicht zu erreichen. Die Zugriffdauer wird beschränkt.

5.1.5. Geräte

Geräte wie Drucker, Beamer, Überwachungskameras und Steuergeräte der Haustechnik müssen ebenfalls in das Netzwerk integriert werden. Die Integration solcher Geräte wird durch die IT-Technik vorgenommen. Falls die Geräte ebenfalls moderne Lösungen unterstützen, können auch diese mittels Authentifizierung eingebunden werden. Wenn dies nicht möglich ist, sollen die Geräte manuell oder mittels MAC-Adresse eingebunden werden.

5.2. Netzwerkstruktur

Der Access-Bereich des Netzwerks, in diesem Fall das LAN (Local Area Network) der jeweiligen Schule, soll sich an den gängigen hierarchischen und skalierbaren LAN-Architekturen orientieren. Dabei wird die Redundanz der Netzwerkkomponenten auf allen sinnvollen Ebenen ausgeführt.

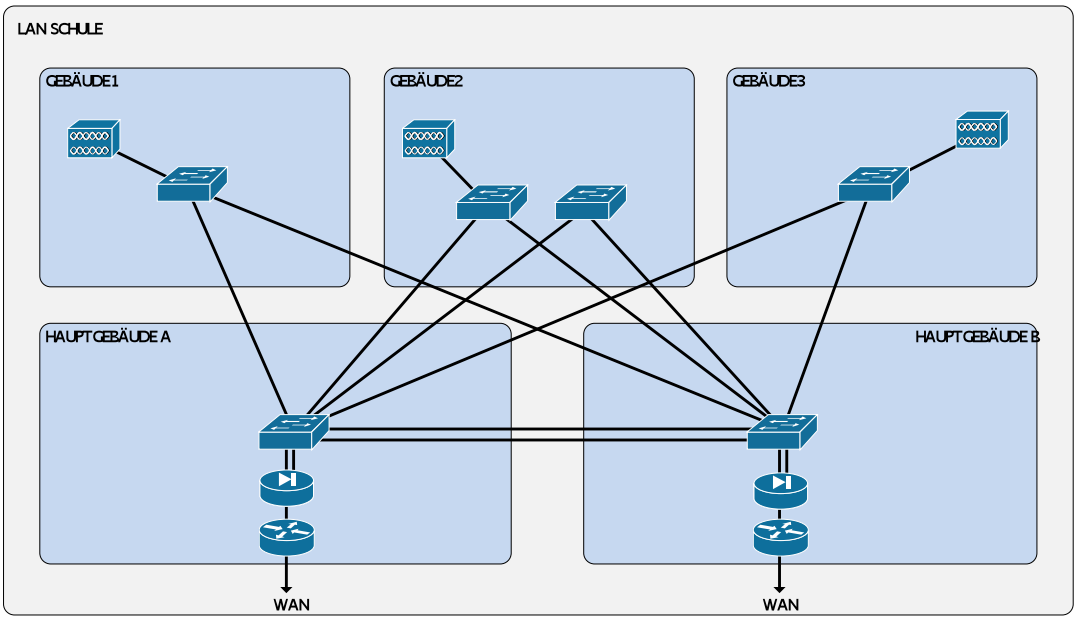

Abbildung 4: Bespiel Netzwerkstruktur an der Schule

5.2.1. Infrastruktur lokal

An jeder Schule befinden sich Geräte und Systeme, die lokal verfügbar sein müssen, so zum Beispiel Drucker, Beamer und Gebäudesteuerung. Die lokale Infrastruktur wird unterteilt in einen Bereich, der auch für die Lernenden zugänglich ist, und einen Bereich, der nur für Lehrpersonen und Verwaltungsmitarbeitende erreichbar ist.

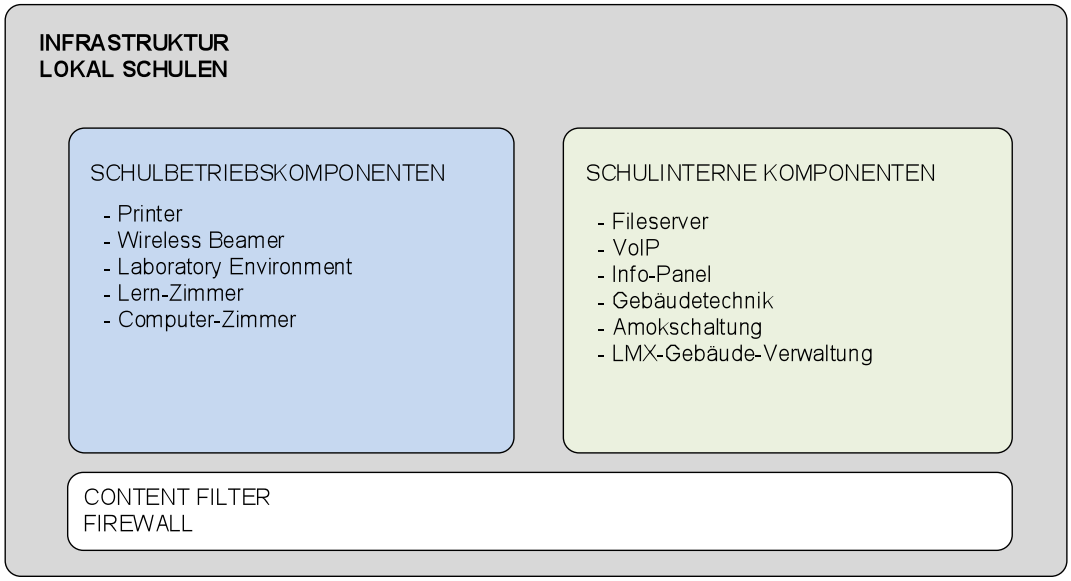

Abbildung 5: Infrastruktur Schulen lokal

5.2.2. Schulbetriebskomponenten

Nachfolgend sind einige mögliche Geräte aufgeführt, die den Lehrpersonen und Lernenden zur Verfügung stehen sollen:

- Wireless Beamer
- Drucker
- Apple TV
- Lab-Umgebungen für Informatikunterricht
- CAD-Stationen
- Labor Computer-Zimmer
- Lern-Zimmer

Wichtig ist die gesicherte und sinnvolle Integration von eigenständigen, selbstmitteilenden Geräten mittels Multicast DNS wie zum Beispiel Apple TV. Dabei sollen die Geräte einfach in das Netzwerk integriert werden können. Die erste Priorität des Zugriffs soll den Lehrpersonen vorbehalten sein. Auf Grund des Standorts der Lehrpersonen und Lernenden sollen nur einzelne, sich in sinnvoller Distanz befindende Geräte ansprechbar sein.

5.2.3. Lehrpersonen und Verwaltungsmitarbeitende

Die lokalen Komponenten, die nur durch Lehrpersonen und Verwaltungsmitarbeitende zu bedienen sind, befinden sich in einem eigenen, abgetrennten Teil innerhalb des lokalen Netzwerks. Darin sind folgende Systeme zu finden:

- Gebäudeautomationskomponenten
- Informationsbildschirme
- Serversysteme

5.3. WAN (Wide Area Network)

Die verteilten Schulstandorte im Kanton Zürich sollen zu einem gemeinsamen Netzwerk zusammengefasst werden. Dabei sind verschiedene Möglichkeiten vorhanden, um eine Vernetzung zu ermöglichen:

- Zentrale Zusammenführung mittels Ringstruktur an zwei Standorten im Kanton Zürich
- Zentrale Zusammenführung mittels Sternstruktur an zwei Standorten im Kanton Zürich
- Bildung von Verbünden an geografisch günstigen Standorten (z.B. Bildungsmeile Zürich)
- Logische Netzbildung, dezentrale Anbindung einzelner Schulen direkt an das Internet

Idealerweise werden maximal zwei Strukturen angeboten, um Schulen gemeinsam zusammenzuschliessen. Aufgrund der Anforderungen an die Verfügbarkeit des Netzwerks wird eine redundante Anbindung an den Building Block WAN notwendig sein.

Ringstrukturen sind in der Skalierung begrenzt. Wenn zum Beispiel in einer Ringstruktur die Kapazität erhöht werden muss, sind davon alle transitiven Standorte, Services und Komponenten betroffen, auch wenn die transitiven Standorte gar keine Erweiterung oder ein Vergrössern der Bandbreite erfordern.

Sternstrukturen haben die höchste Flexibilität und Skalierungsmöglichkeiten. Der Nachteil besteht darin, dass ungenutzte Ressourcen nicht ausgelastet werden können.

Ein guter Kompromiss zwischen Ringstruktur und Sternstruktur bildet das Zusammenfassen von regionalen Schulen, die dabei sternförmig an die zentralen Punkte angeschlossen werden. Dabei wird der eigentliche Übergang in das Internet an den zwei zentralen Punkten erstellt. Die zwei zentralen Punkte sollen geografisch so gewählt werden, dass auch die Dienste des MBA als Building Block Datacenter genutzt werden können. Idealerweise haben die zwei zentralen Standorte auch eine grosse Auswahl an Internetdienstanbieter, welche es ermöglichen, zu Marktpreisen Internetzugänge einzukaufen.

Die dezentrale Anbindung einzelner Schule an das Internet stellt eine Möglichkeit dar, um kleine Schulen, die geografisch ungünstig gelegen sind, ohne WAN-Anbindung zu integrieren. Dabei gehen jedoch die Synergieeffekte aus einem gemeinsamen Zusammenschluss verloren. Diese umfassen den Verlust der einfachen Vernetzung von Diensten über das eigene Netzwerk. Den Verlust der gemeinsamen Kostenoptimierungen bei den Standortvernetzungen. Die technische Komplexität wird zudem erhöht, um die Redundanz des Internetzugangs zu lösen.

Aus Sicht der Wirtschaftlichkeit ist es nicht einfach abzuschätzen, welche Lösung einen kostengünstigeren Building Block WAN ermöglicht. Damit eine sinnvolle Abschätzung möglich ist, müssen Offerten zu den konkreten Verbindungen eingeholt werden. Generell gilt, umso mehr Schulen konsolidiert und koordiniert durch das MBA Offerten einholen, desto kostengünstiger werden die Lösungen ausfallen.

5.3.1. Zentrale Zusammenführung, Sternstruktur und Clusterbildung

Als Beispiel für eine Zusammenführung verschiedener Schulen wurde im nachfolgenden Schema der Standort Winterthur gewählt.

Vorteile:	**Nachteile:**
Synergie Standortvernetzung und Internet	Standortverbindungen Preise
Redundantes Design	
Kontrolle des Netzwerk bis in Datacenter	

Abbildung 6: Zentrale Anbindung am Beispiel der Region Winterthur

5.3.2. Dezentrale Anbindung einzelner Schulen direkt an das Internet

Als Beispiel für eine dezentrale Anbindung einer Schule wurde im nachfolgenden Schema der Standort Küsnacht gewählt.

Vorteile	Nachteile
Evtl. günstige Internetanbindung	Downtime hoch bei Fehlerfall

	Keine Netzwerkkontrolle im Internet
	Tunnel-Anbindung an Data center via IPSec, GRE oder ähnlich
	Komplexität erhöht, wenn Services von extern erreichbar sein müssen.

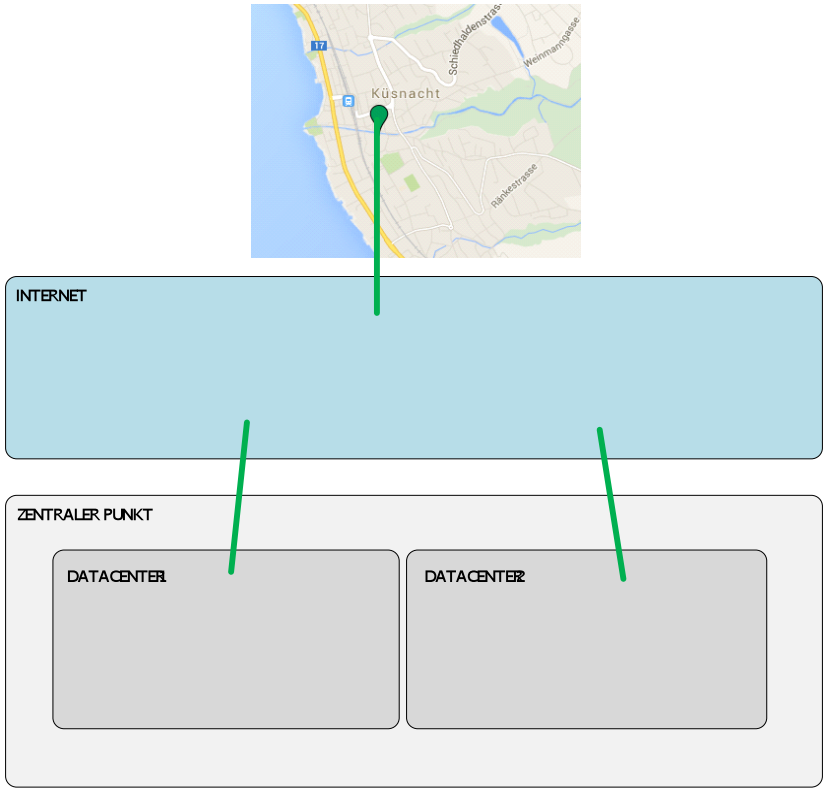

Abbildung 7: Dezentrale Anbindung am Beispiel der Schule Küsnacht

5.4. Konsolidierte Infrastruktur

Ein grosser Teil der unten aufgeführten Module benötigt eine zentrale Infrastruktur, um die Dienste zu produzieren oder den Schulen zur Verfügung zu stellen. Diese konsolidierte Infrastruktur wird mittels einem Building Block Data Center abgebildet. Dies beinhaltet, dass die Infrastruktur an zwei geografisch getrennten Standorten aufgebaut wird. Die Data-Center-Infrastruktur ist so aufgebaut, dass ein einzelner Standort vollumfänglich die Services von beiden Standorten betreiben kann. Der Aufbau folgt dabei der Vorgabe, dass ein einzelner Fehler keinen Service ausser Betrieb setzen kann. Die folgenden Module sollen als Basisdienste zur Verfügung stehen:

1. Modul Managed LAN und WLAN
2. Modul Managed WAN
3. Modul Firewall
4. Modul Content Filter
5. Modul Userverwaltung
6. Modul Mail
7. Modul VoIP
8. Modul Cloud / Compute Ressources
9. Modul Internet
10. Modul IPAM, DNS, DHCP

Durch die Konsolidierung der Services bietet sich die Möglichkeit an, den verschiedenen Schulen Kompetenzzentren zu gründen, welche sich um einzelne oder mehrere Dienste kümmern. Durch die Verwaltung bestimmter Dienste durch einzelne Kompetenzzenter können die Effizienz und die Kompetenz für bestimmte Arbeiten gesteigert werden.

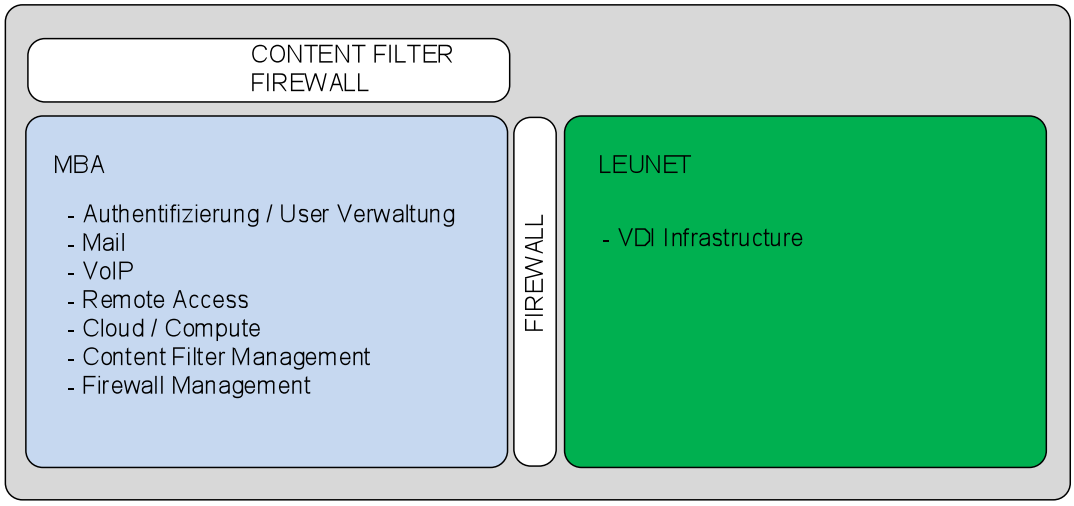

Abbildung 8: Konsolidierte Infrastruktur

5.4.1.1. Modul Managed LAN und WLAN

Das Basismodul Managed LAN und WLAN stellt den Schulen die LAN-Basisinfrastruktur zur Verfügung. Dabei werden die notwendigen Komponenten wie Switches, Access Points, Router und WLAN Controller durch zu definierende Kompetenzzentren betrieben und gewartet. Die Beschaffung, Preisgestaltung und Herstellerwahl wird durch das MBA unterstützt und gefördert. Aus Sicht der Schule wird ein Service eingekauft, der die notwendigen Bedürfnisse sinnvoll und kosteneffizient abbildet und einen Ansprechpartner für alle Belange bietet.

5.4.1.2. Modul Managed WAN

Das Modul Managed WAN stellt den Schulen die Standortvernetzung zwischen den Schulen, den zentralen Diensten des MBA und des Internets sicher. Dabei werden die eingesetzten Standortverbindungen betrieben, überwacht und gewartet. Die Kapazität wird mit genügend grosser Bandbreite zur Verfügung gestellt. Aus Sicht der Schule wird ein Service eingekauft, der die notwendigen Bedürfnisse sinnvoll und kosteneffizient abbildet und einen Ansprechpartner für alle Belange bietet.

5.4.1.3. Modul Firewall

Das Modul Firewall stellt die Sicherheit für die einzelnen Schulen her. Es sollen pro Schule eigenständige Filterregeln möglich sein. Durch ein zentrales Management und eine Logauswertung im MBA können Vorfälle korreliert werden. Die Lösung soll mandantenfähig sein, das heisst, bei Bedarf kann die Schule einen Teilbereich der Firewall selber managen. Idealerweise wird ein Prozess etabliert, der die Sicherheitsanpassungen auditiert und dokumentiert. Regelmässige Überprüfung der Sicherheitseinstellungen sollen durchgeführt werden. Aus der Sicht der Schule wird ein Service eingekauft, der die notwendigen Bedürfnisse sinnvoll und kosteneffizient abbildet und einen Ansprechpartner für alle Belange bietet.

5.4.1.4. Modul Content Filter

Das Modul Content Filter ermöglicht es, unangemessenen Inhalt zu unterdrücken. Als Basis soll ein DNS-URL-Filter eingesetzt werden. Die Filterung mittels DNS ermöglicht auch Inhalte, die via SSL gesichert werden, zu filtern. Dies stellt einen erheblichen Vorteil gegenüber Proxy Lösungen dar. Ein DNS-URL-Filter befindet sich nicht im Fluss des Verkehrs und hat keinen direkten Einfluss auf die Performance. Die Skalierung mittels DNS-URL-Filter ist sehr hoch. Es können eigenständige Cloud-Lösungen in Betracht gezogen werden. Der Schule soll ein Standard-Filterset angeboten werden. Dabei werden sinnvolle Filterregeln für alle Schulen erstellt. Die Schulen sollen die Möglichkeit haben, eigene White Lists und Black Lists zu pflegen. Da es sich bei Filterung von Inhalten um ein schwierigen Eingriff in die Meinungsfreiheit handelt, ist es wichtig, einen Prozess zu etablieren, der die Anpassungen dokumentiert und auditiert.

5.4.1.5. Modul Userverwaltung

Das Modul Userverwaltung ermöglicht es, die Verwaltung der User zentral zu administrieren und zu verwalten. Das MBA stellt einen mandantenfähigen, hochverfügbaren Directory Service zur Verfügung. In diesem Directory Service werden alle User und Berechtigungen der verschiedenen Nutzer und Schulen abgebildet. User, die an verschiedenen Schulen unterrichten oder unterrichtet werden, können mit einem einheitlichen Benutzeraccount arbeiten. Der Zugriff auf die notwendigen Ressourcen an den unterschiedlichen Schulen soll zentral verwaltet werden können. Dies soll in einem eigenen Projekt ausgearbeitet werden.

5.4.1.6. Modul Mail

Das Modul Mail stellt den Schulen eine sinnvolle Mail-Infrastruktur zur Verfügung. Dabei werden die gängigen Mail Clients und Kalender-Clients unterstützt. Zudem werden Antivirus und Spamfilter schon serverseitig umgesetzt. Dies soll in einem eigenen Projekt ausgearbeitet werden. Die jetzige bestehende Lösung deckt diese Bedürfnisse weitgehend ab.

5.4.1.7. Modul VoIP

Das Modul VoIP stellt die Telefoniekommunikation der Schulen sicher. Wichtig dabei ist, dass für die Telefonienutzer die gewohnte Qualität beibehalten wird. Im Zuge einer VoIP-Integration macht es Sinn, anstatt nur VoIP anzubieten, gleich eine vollumfängliche Kollaborations-Softwarelösung (ähnlich Skype) zu integrieren. Damit würde Telefonie, Chat, Video und Desktopsharing verschmelzen. Dies soll in einem eigenen Projekt ausgearbeitet werden.

5.4.1.8. Modul Cloud / Compute Ressources

Das Modul Cloud / Compute Ressources stellt eine mandantenfähige Cloud zur Verfügung, welche den Schulen die notwendigen Ressourcen für den Betrieb von Server- oder auch Lab-Aufbauten zur Verfügung stellt. Durch die zentrale Platzierung ist eine hohe Synergienutzung der Ressourcen möglich. Dies würde einerseits die Möglichkeit bieten, die Serversysteme der Schulen zu betreiben. Andererseits bietet eine moderne Cloud-Lösung die Möglichkeit, dass komplette Infrastrukturen schnell und einfach genutzt werden können. Man kann sich vorstellen, dass in einem Informatik-Projekt die Lernenden ihre „eigene“ Infrastruktur zur Verfügung gestellt bekommen. So zum Beispiel 4 CPU Cores, 16GB RAM und 250GB Diskplatz. Die Lehrpersonen können dann bestimmte Aufgaben stellen, welche die Lernenden selbständig umsetzen können. Nach Abschluss des Projekts oder der Klasse werden die Ressourcen wieder für andere Projekte verwendet. Dies soll in einem eigenen Projekt ausgearbeitet werden.

5.4.1.9. Netzübergang LEUnet2

Die kantonalen Dienste SAP und Pulse werden im Netzwerk des Kantons, genannt LEUnet2, zur Verfügung gestellt. Die Anforderungen an die Sicherheit und den Zugangsschutz, um Zugriff auf das LEUnet zu erhalten, sind erhöht. Damit für die notwendigen Benutzer ein nativer Zugriff mit Fat Clients auf die LEUnet-gehosteten Applikationen möglich ist, werden die Geräte durch die Informatik-Dienste verwaltet und der Netzwerkzugang entspricht höchsten Sicherheitsanforderungen.

Der Netzübergang zwischen LEUnet und dem MBA-Netzwerk soll an zwei zentralen Standorten stattfinden. Dadurch kann die Verfügbarkeit hoch gehalten werden und im Fehlerfall ist ein zweiter Übergang verfügbar. Im Konzept LEUnet 2 wird explizit erwähnt, dass den am MBA beteiligten Schulen via Remote Access der Zugriff auf die notwendigen Applikationen gewährt werden kann. Das heisst, es sind grundsätzlich zwei Möglichkeiten denkbar. Als Grundlage für den LEUnet2-Netzübergang wird auch die Network Security Policy des KITT angewandt.

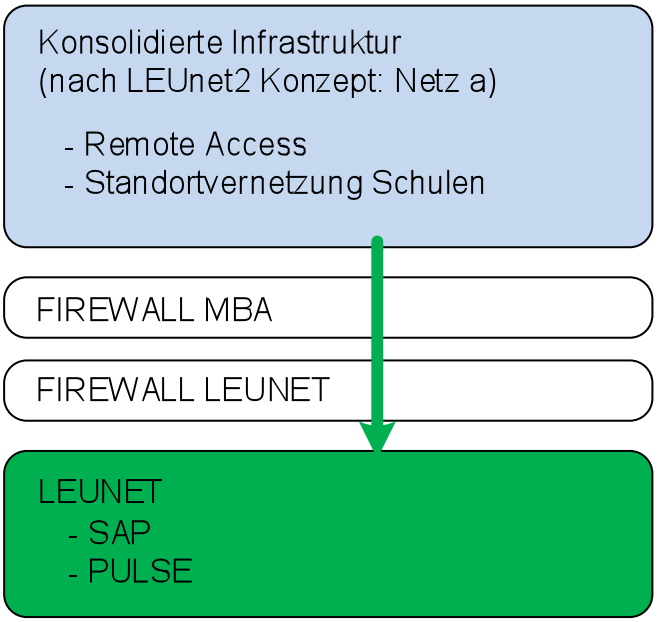

Abbildung 9: Schema Firewall Übergänge MBA – LEUnet2

- Variante 1: Anbindung als kantonales dezentrales Netzwerk (a-Netz) mit zentralen Zonenübergängen
- Variante 2: Zugriff via Remote-Access-Lösung

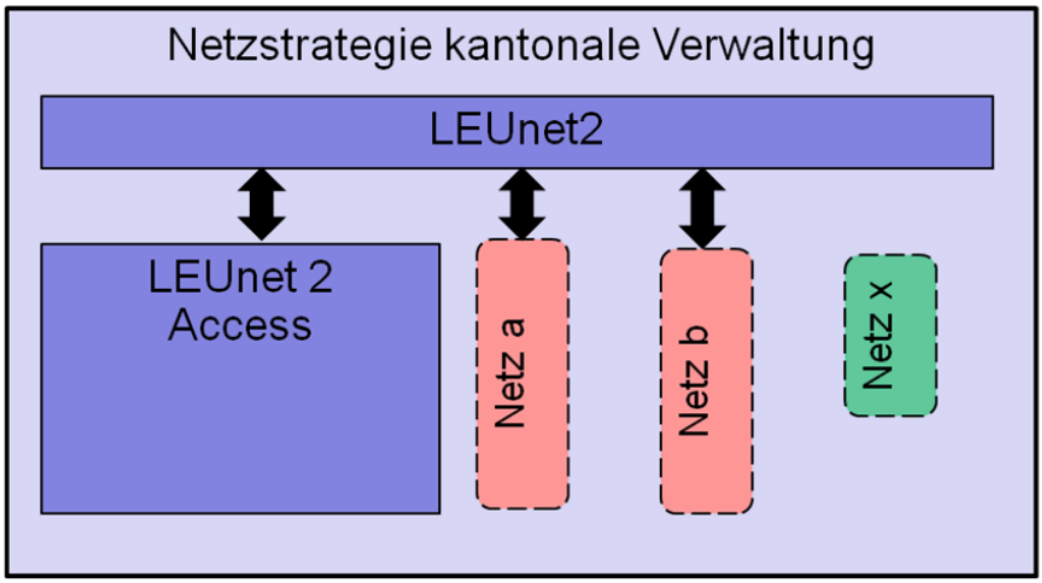

Abbildung 10: Schema Anbindung dezentrale Netze an LEUnet2

5.4.1.10. Modul IPAM, DHCP, DNS

Zu den Basisdiensten in einem Netzwerk gehört die IP IP-Adressverwaltung, die IP-Adressvergabe und das Pflegen der Domainnamen-Einträge. Mittels des Moduls IPAM, DHCP, DNS soll den Schulen eine Lösung angeboten werden, die durch die Schulen selbständig gepflegt und genutzt werden kann.

5.4.1.11. Internet

Der Internetzugang ist der Lebensnerv für die unterschiedlichsten pädagogischen Lerninhalte. Die meisten Inhalte und Services werden über das Internet bezogen. Der Ausgangslage, dass 80% des Verkehrs Zugriffe auf das Internet sind, muss ein hoher Stellenwert beigemessen werden. Durch eine konsolidierte Netz-Basisinfrastruktur und die Zentralisierung an zwei zentralen Standorten bietet es sich an, den Internetverkehr auch an diesen Standorten einzukaufen. Ein grosses Volumen und ein grosser Bandbreitenbedarf helfen, um gute Preise für Internetverkehr zu bekommen. Dementsprechend ist der zentralisierte Ansatz vor allem dann interessant, wenn möglichst alle Schulen für die gemeinsame Netzwerkinfrastruktur zu gewinnen sind.

5.4.1.12. Remote Access

Für Lehrpersonen und Verwaltungsmitarbeiter soll eine Remote-Access-Lösung via sicherer Authentifizierung und starker Verschlüsselung eingerichtet werden. Die Authentifizierung soll mindestens mit Usernamen und Passwort erfolgen, allenfalls sind stärkere Methoden wie zertifikatsbasierter Zugriff und / oder ein Zwei-Faktor-Authentifizierung in Betracht zu ziehen.

Bei einer zentralen Zusammenführung, einer Sternstruktur und Clusterbildung des Netzwerks werden die VPN-Remote-Access-Endpunkte an den zentralen Punkten der MBA-Infrastruktur aufgebaut.

Die Zugriffsrechte via Remote Access sollen den Möglichkeiten aus den Zonen des Building Blocks Access folgen. Wenn gewisse Zugriffe oder Dienste via Remote Access eingeschränkt werden sollen, muss die Lösung dies abbilden können.

5.4.1.13. IPv4 und IPv6

Das IPv4-Protokoll umfasst einen Adressraum von 32bit, dies entspricht ungefähr 4,3 Milliarden Adressen. Dieser Adressbereich ist ausgeschöpft und kann mit dem aktuellen Wachstum an mobilen Geräten und der Vernetzung aller möglichen Geräte nicht mehr genügend Adressen zur Verfügung stellen. Mit dem IPv6-Protokoll steht ein ungleich grösserer Adressraum zur Verfügung, dieser umfasst 128 Bit (eine unvorstellbar grosse Zahl). Die Problematik dabei besteht darin, dass IPv6 nicht rückwärtskompatibel ist. IPv4 und IPv6 können nicht miteinander kommunizieren. Aktuell hat sich der Trend durchgesetzt, dass Netzwerke im sogenannten Dual-Stack-Modus betrieben werden. Das heisst, es werden IPv4 und IPv6 parallel betrieben. Wann dieser Dual-Stack-Betrieb nicht mehr nötig sein wird, ist aktuell nicht vorhersehbar. Einige Studien gehen von wenigen Jahren aus, andere sprechen von 20 bis 30 Jahren.

Das Wichtigste besteht aktuell darin, dass bei Neubeschaffungen die IPv6-Funktionalität durch die Hersteller gewährleistet wird. Bei Infrastruktur-Projekten ist dringend vorzusehen, dass auch immer IPv6-Funktionalität integriert wird. Mittels der Integration von IPv6 in aktuelle Projekte kann der Aufwand für die Integration von IPv6 tief gehalten werden. Ein nachträgliches Integrieren von IPv6 ist mit ungleich höherem Aufwand verbunden.