HERAUSFORDERUNG

- Einrichtung von Traffic-Shaping/QoS für die verschiedenen Netzwerke
- Unterbringung von Arbeitsgruppen bei Ausschluss von Zugriffsmöglichkeiten auf andere Netze
- möglichst sparsamer Hardwareeinsatz
- Einrichtung von persönlichen Netzwerken pro Bewohnerzimmer

KUNDE

ÖJAB

AUFGABENSTELLEUNG

Planung und Umsetzung einer LAN- und WLAN-Infrastruktur mit eigenem, abgegrenztem Netzwerk pro Zimmer

UNSERE LEISTUNGEN

Netzwerk-Konzeptionierung, Subnetting, Routing, Authentication

BRANCHE

Gemeinnützige Jugendarbeit, Seniorinnen- und Seniorenarbeit, europäische Bildungsarbeit und Entwicklungszusammenarbeit

RAHMENBEDINGUNGEN

Da das betroffene Objekt primär als Studierendenheim genutzt wird, hatte für den Kunden die **Trennung des Netzwerkverkehrs** besondere Priorität. Die Beeinflussung der Internetgeschwindigkeit durch einzelne Bewohner sollte ebenso ausgeschlossen werden wie die Sichtbarkeit von Endgeräten, die nicht im Besitz des jeweiligen Zimmerbewohners stehen.

Zusätzlich galt es, Verwaltung und ausgewählten Arbeitsgruppen im Haus eine **garantierte Mindestbrandbreite** einzurichten, um vom Surfverhalten der Studierenden unbeeinflusst arbeiten zu können. Die diesbezügliche Trennung der Netzwerke war im Umsetzungsprozess natürlich inbegriffen.

Alle Anforderungen im Überblick:

- ein eigenes Netzwerk pro Zimmer
- priorisierte Bandbreite für Verwaltung und ausgewählten Arbeitsgruppen im Haus (darunter auch ein Coworking Space)
- faire und durchdachte Aufteilung der WAN-Bandbreite
- persönlicher Zugriff auf seine privaten LAN-Geräte im Zimmer über WLAN im ganzen Gebäude
- Zugriffsmöglichkeiten auf ausgewählte Steuerdienste (z.B. RFID-Türen) für den Verwaltungsbereich
- möglichst geringer Hardwareeinsatz

LÖSUNG

Um die Zahl der eingesetzten Hardwarekomponenten gering zu halten und dennoch die erforderliche Anzahl an benötigten Netzwerken zu erreichen, war der **Einsatz von VLANs** unabdingbar. Dabei wurde jedem Zimmer ein eigenes virtuelles Netzwerk mit einer /24er Subnetmask zugeteilt. Für die kabelgebundenen Clients konfigurierten wir die benötigten Dosen fix auf die jeweiligen VLANs.

Im Bereich **WLAN** gestaltete sich die Situation allerdings komplexer: Um einem WiFi-Client ein VLAN zuweisen zu können, bedarf es entweder einer SSID pro Zimmer oder eines Benutzers, der an einem Server authentifiziert werden muss. Da wir aus Erfahrung wissen, dass eine Häufung von SSIDs an einem Standort zu einer schlechteren Performance pro WLAN führt, fiel unsere Wahl auf die **User-Authentifizierung**. Um Lizenzkosten vorzubeugen und den Administrationsaufwand gering und nachvollziehbar zu halten, entschieden wir uns dabei bewusst gegen ein Microsoft Active Directory und für einen **Radius-Server mit Web-Frontend**. Damit wird Verwaltenden mit wenig IT-Kenntnissen die Möglichkeit gegeben, in einer übersichtlichen Weboberfläche User und Passwörter anzulegen und sie einem bestimmten VLAN zuzuordnen.

Auf den Accesspoints, die ein flächendeckendes WLAN am Standort ausstrahlen, wurde in einem weiteren Schritt eine SSID mit WPA2-Enterprise angelegt, wobei wir den Radiusserver als Authentifizierungsstelle angaben. Meldet sich ein Client im WLAN an, erfolgt eine Abfrage der Credentials (Benutzername + Passwort). Tippt sie der Anwender ein, leiten die Accesspoints den Request an den Radiusserver weiter, der die angegebenen Credentials mit seiner Datenbank abgleicht. Sind die Logindaten korrekt, sendet dieser eine Anfrage zum Start einer Usersession an den Accounting-Server (in diesem Fall die Firewall). Dem Client wird nun mitgeteilt, in welchem VLAN er sich befindet. Anschließend wird via DHCP nach einer IP-Adresse gefragt. Dabei ist firewallseitig definiert, dass kein Internet-Traffic aus den Zimmernetzen erlaubt ist, solange keine aktive Useranmeldung besteht. Somit wird eine Umgehung der Authentifizierung ausgeschlossen.

Gästen im Haus steht eine eigene SSID mit PSK (Passwort) zur Verfügung, über die Benutzer in ein eigenes Gästenetzwerk verbunden werden.

Durch die Aufteilung der Netzwerkinfrastruktur in VLANs ist eine klare Abtrennung der einzelnen Zimmer und Dienstleister gegeben. Damit lässt sich ein **durchdachtes Trafficshaping mit Bandbreitenpriorisierung für bestimmte Netze** – wie Verwaltung und eingemietete Arbeitsgruppen – einrichten. Über Firewallregeln kann der Netzwerkverkehr letztlich sogar so weit eingeschränkt werden, dass jedes Unternehmen ausschließlich auf die von ihm benötigten Dienste Zugriff erhält, die Netzwerke sonst aber keinen Einfluss aufeinander nehmen.

ERGEBNIS

Mit der etablierten Lösung konnte GEKKO it-solutions den Anforderungen des Kunden in allen Aspekten gerecht werden. Das Ergebnis spricht für sich:

- Kostenersparnis durch reduzierten Hardwareeinsatz
- Schaffung klar abgetrennter Netzwerke
- Zugriff auf stationäre Geräte im eigenen Bewohnerzimmer über WLAN
- Brandbreitengarantie/-priorisierung über Trafficshaping/QoS
- Einschränkbarkeit einzelner Netzwerke über Firewall

Jens Tersteegen

Spezialist für Netzwerk-Konzeptionierung

> *Die Planung einer Netzwerkinfrastruktur ist stark von den Anforderungen eines Kunden abhängig. Auch komplexe Systeme lassen sich durch eine gute Konzeption und unter Einsatz der richtigen Technologien effizient umsetzen.*