Projektinformation zu

VLAN Security

Nutzen und Motivation einer VLAN Security

- **Configuration Management Database (CMDB)**
- **Secure VLAN**
- **RADUIS Server**
- **MAC-Autentifizierung**
- **Netzwerksicherheit**

Situation: Bei den Stadtwerken Düsseldorf werden zur Erhöhung von Sicherheit und Leistung in den Netzen einzelne Bereiche durch VLANs (Virtual Local Area Networks) nach IEEE 802.1q, in thematisch abgegrenzte, virtuelle Netzsegmente unterteilt.

„Wilde"- also nicht dokumentierte Umzüge oder das undokumentierte Umstecken eines PCs von der einen Dose in die andere („Es funktioniert ja") führten u.a. auch zu Sicherheitsproblemen, da ein User, der seinen Laptop an einen andere Dose anschließt, evtl. in einem VLAN landet, wo er nichts zu suchen hat. Auch ein fremder User, der seinen Rechner an eine Dose anschließt, hat Zugriff auf die Ressourcen innerhalb des VLANs. Es wird also ein Mechanismus benötigt, der geräteabhängig das richtige VLAN ermittelt und unbekannte Geräte einem sicheren VLAN zuordnet, in dem die Geräte keine anderen Ressourcen erreichen.

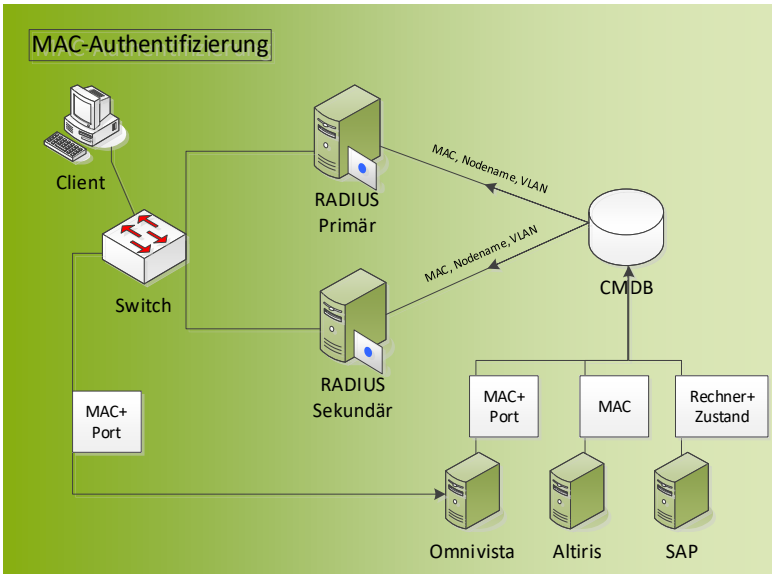
Motivation

- ***Sicherheit im Netzwerk***
- ***Flexible Umzugsmöglichkeiten***
- ***Bessere Unterstützung von Notebooks***
- ***Erhöhung der Leistung im Netz***
- ***Kein Netzzugriff durch nicht authorisierte Geräte***

Ursache für dieses Problem ist, dass die VLANs den Ports auf dem Switch statisch zugeordnet waren. Es musste hier also eine Lösung gefunden werden, in der die Ports abhängig vom Gerät anderen VLANs zugeordnet werden. Voraussetzung hierfür ist, dass man die eigenen Geräte kennt.

In der hochintegrierten Umgebung der Stadtwerke Düsseldorf wird der gesamte Lebenszyklus (Bestellung, Lieferung, Aufbau,..) von Endgeräten in der CMDB abgebildet. Im SAP erfolgt die Erfassung der Geräte bei Wareneingang. Diese werden über eine Schnittstelle automatisch an die CMDB geliefert. In der CMDB werden die Umzüge der Geräte verwaltet und die neuen Standorte wiederum vollautomatisch an SAP zurückgeliefert. Eine Schnittstelle zum Inventorysystem Altiris liefert die Hard- und Softwarekonfiguration der Clients für automatisierte Soll- / Ist-Vergleiche und die Netzwerkkonfiguration (IP-Adresse / MAC-Adresse / Interfaces). Dadurch stehen für alle Endgeräte die Konfiguration und die Netzwerkinformationen (MAC-Adresse, Node-name und VLAN-ID) in der CMDB zur Verfügung.

Diese Informationen kann man nun nutzen, um einem Switch mitzuteilen, welches VLAN einem Endgerät, das sich am Switch „anmeldet", zugeordnet werden soll. Besitzt man einen Switch, der eine RADIUS-Authentifizierung (Remote Authentication Dial-In User Service) erlaubt, steht dem nichts mehr im Wege. Auch im Hinblick auf Voice-Over-IP (VoIP) wurden neue Switches von Alcatel eingeführt, die auf den Ports eine Radius-Authentifizierung nach RFC 2138 / 2865 /2868 / 3575 / 2618 ermöglichen.



RADIUS Server liefern das VLAN

Die Radiusserver erlauben eine unternehmensweite, zentrale Administration der Zugriffsrechte. Betankt werden die Radiusserver mit Informationen aus der CMDB, welche MAC-Adresse des Clients, den Nodename und die VLANID an den Radiusserver übermitteln. Durch diese Technik ist es nun unerheblich, an welchem Port ein Client angeschlossen ist. Anhand seines Nodenames und der MAC-Adresse wird er automatisch in das richtige VLAN geschaltet. Nicht im Radiusserver bekannte Geräte erhalten keinen Zugriff auf das Netz.

Ein **RADIUS-Server** ist ein zentraler Authentifizierungsserver, an den sich Services für die Authorisierung von Clients in einem Netzwerk, ja nach Konfiguration auch über einen RADIUS-Proxy-Server, wenden.
Der RADIUS-Server übernimmt dabei für den Service die Authentifizierung, das heißt die Überprüfung von Benutzername und Kennwort. Des Weiteren werden Parameter für die Verbindung zum Client bereitgestellt. Die dabei verwendeten Daten entnimmt der RADIUS-Server eigenen Konfigurationsdateien, eigenen Datenbanken oder ermittelt diese durch Anfragen an weitere Datenbanken oder Verzeichnisdienste, in denen die Zugangsdaten wie Benutzername und Kennwort gespeichert sind.

Auch aus Dokumentationssicht bietet die Einführung der Radiusauthentifizierung einen entscheidenden Vorteil: Alle Clients müssen korrekt in der CMDB dokumentiert sein. Es gibt keine Clients im Netz ohne dokumentierte MAC-Adresse.

Die Konfiguration der Clients und die VLAN-Zuordnung werden zentral in der CMDB vorgenommen und über eine Schnittstelle an die Radiusserver (Primär und Sekundär) weitergeleitet.

Wenn sich ein Client über den Switch verbindet, übergibt der Switch die MAC-Adresse des Clients an den Radiusserver und fragt die zugeordneten VLANs ab. Nur wenn die MAC-Adresse im RADIUS-Server bekannt ist, bekommt der Client Zugriff auf das Netz und den hinterlegten VLANs.

info@agineo.de

www.agineo.de