MICROSENS

WHITE PAPER

Safety first - Sichere Gebäudenetze durch dezentrale Infrastrukturlösungen

Safety first - Sichere Gebäudenetze durch dezentrale Infrastrukturlösungen

Es steht außer Frage, dass die IT-Infrastruktur sicher und zuverlässig arbeiten muss – schließlich ist sie das Fundament, auf dem zahlreiche Geschäftsprozesse und damit der Unternehmenserfolg aufbauen. Wie beim Gebäude selbst gilt auch hier: Wenn es beim Fundament Probleme gibt, zieht sich das durch das gesamte Gebilde.

Während Anwender auf die Zuverlässigkeit und die Performance ihrer Verkabelung achten, wird der Sicherheit oft nicht genügend Beachtung geschenkt. Entwicklungen wie BYOD, immer mehr mobile Geräte, die eingebunden werden müssen und immer raffiniertere Angriffe auf das Unternehmensnetzwerk erfordern ein höheres Sicherheitsniveau als bislang.

Gleichzeitig unterliegen Infrastruktur-Projekte einem immer größer werdenden Kostendruck. Eine verteilte Infrastruktur mit dezentralen Switches kann all diese Forderungen optimal erfüllen.

Längst hat sich die Verkabelung mit dezentraler Switching-Architektur wie beispielsweise das von MICROSENS entwickelte Fiber To The Office (FTTO) als kosteneffiziente Inhouse-Vernetzung in zahlreichen Projekten bewährt. Unabhängige Studien wie die der WIK-Consult und zahlreiche erfolgreiche Projekte weisen die wirtschaftlichen Vorteile dieser Lösung immer wieder nach. Dabei ist das dezentrale Konzept nicht auf Glasfaserleitungen beschränkt, sondern kann seine spezifischen Vorteile auch bei einer Verkabelung mit Kupferleitungen voll zur Geltung bringen. Bei beiden Medien werden leistungsfähige Leitungen bis in den Anwenderbereich verlegt, wo Installations- oder Micro-Switches als aktive Elemente zum Einsatz kommen, die flexible Kupferanschlüsse für die Endgeräte wie beispielsweise Arbeitsplatz-PCs, VoIP-Telefone, Drucker, Laptops, Wireless LAN Access Points oder IP-Kameras bereitstellen. Als Technologieführer für dezentrale Switching-Konzepte für Glasfaser und Kupfer implementiert der Technologiespezialist MICROSENS neue und umfangreiche Sicherheits-Features in seine Produkte, um den Anwendern ein Höchstmaß an Sicherheit beim Netzwerkzugang zu gewährleisten.

Dezentrale Switches bieten Vorteile

Dezentrale Switches der neuesten Gerätegeneration bieten eine Fülle von Funktionen, die bislang Core-Switches vorbehalten waren. Über sichere Protokolle wie SNMP V3 oder HTTPS kann jeder Parameter in den Switches konfiguriert, geändert und an andere Software-Instanzen übermittelt werden. Die vollständige IPv6-Implementierung ist eine wichtige Voraussetzung für zukunftssichere Netze.
Das dezentrale Konzept bietet jedoch weit mehr. Seine anwenderorientierte Struktur bringt die Switch-Intelligenz und damit überwachte, managebare Geräte dort hin, wo sie gebraucht werden, nämlich vor Ort beim Anwender.

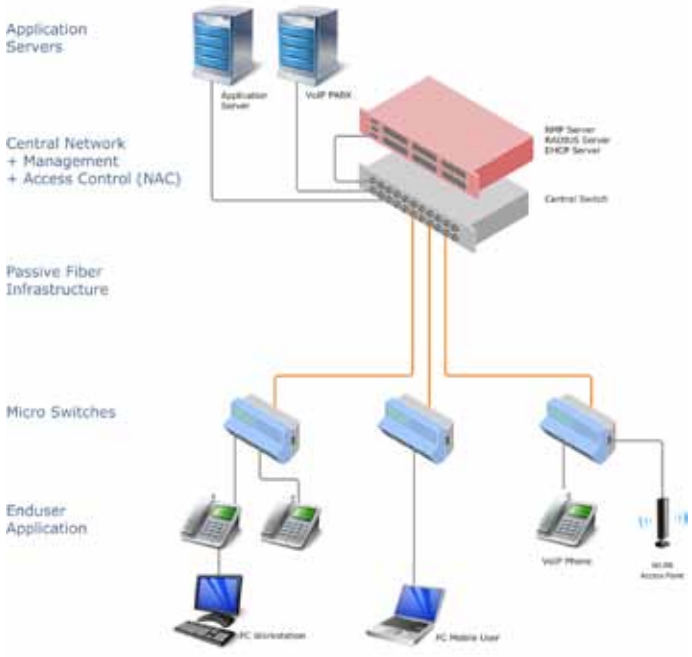
Ein weiteres Plus am Rande: Das Verkabelungskonzept mit dezentralen Switches ermöglicht deutlich kleinere Kabelbündel, was gerade bei Sanierungen von Altbauten ins Gewicht fällt. Und kleinere Kabelbündel führen zu kleineren Brandlasten, was wiederum die Sicherheit erhöht und die Kosten senkt. Darüber hinaus lassen sich bestehende Kupfernetze schnell und ohne aufwendige Nachverkabelung erweitern und bleiben ohne Neuverkabelung up to date.

Zugriffssicherheit

Die Authentifizierung des Users am Micro-Switch am Arbeitsplatz sorgt dafür, dass ein Anwender ohne die notwendige Berechtigung gar nicht erst ins Netz gelangt. Vollständig normkonform nach IEEE 802.1X geht es jedoch weit über die Forderungen der Norm hinaus und bietet umfassende Sicherheit durch Port-Security. Meldet sich ein Endgerät am Micro-Switch an, so schickt dieser die Anfrage an den RADIUS-Server und entscheidet abhängig von dessen Antwort. Je nach Entscheidung kommt der Anwender dann in ein sicheres VLAN oder wird bereits direkt am Arbeitsplatz-Anschluss geblockt.
Moderne Büroumgebungen mit Voice over IP (VoIP) fordern jedoch mehr. Verbindet ein Anwender seinen PC oder Laptop über ein VoIP-Telefon mit dem Netzwerk, kann das herkömmlichen Switch-Lösungen Sicherheitsprobleme bereiten, da sich am authentifizierten Telefon noch ein vom Switch nicht zu authentifizierender Netzwerkport befindet. Mit der Multi-User-Authentifizierung von MICROSENS kann der Switch geräteweise unterscheiden: Das VoIP-Telefon kann beispielsweise manipulationssicher über das Maschinenzertifikat authentifiziert werden, der daran angeschlossene Laptop oder Arbeitsplatzrechner über die MAC-Adresse. Je nach Switch-Konfiguration werden weitere Geräte abgelehnt.
Meldet sich ein nicht autorisiertes Endgerät an, wird es in ein Gast- oder Quarantäne-VLAN geschaltet, statt den Switchport komplett zu sperren. Dadurch bleiben bereits authentifizierte Endgeräte, die an das IP-Telefon angeschlossen sind wie auch das Telefon selbst weiterhin im Netz und damit voll funktionsfähig.
Der Zugriff auf das Switch-Management ist ebenfalls über einen RADIUS-Server authentifizierbar, was ein zusätzliches Plus an Sicherheit bietet.
Wer's einfacher mag: Natürlich kann der Zugang auch auf eine einzige MAC-Adresse pro Port beschränkt werden. Wird der Switchport einem Endgerät fest zugeordnet, bietet das einen zusätzlichen Schutz. Andere Geräte werden abgewiesen, wodurch ein Eindringen durch Kaskadierung einfach und wirkungsvoll verhindert wird. Ein RADIUS-Server wird dazu nicht benötigt.

Ausfallsicherheit

Durch die Kaskadierung von Micro-Switches kann eine zusätzliche Redundanz geschaffen werden. Dabei genügt es, die Switches untereinander über Glasfasern oder Kupferleitungen – im einfachsten Fall durch ein Patchkabel – miteinander zu verbinden.
Noch mehr Redundanz kann mit Dual Homing erreicht werden, bei dem jeder Micro-Switch gleich über zwei Links mit einem – oder zwei – Core-Switches verbunden wird. Rapid Spanning Tree (RSTP) sorgt dabei für einen sicheren Betrieb und kürzest mögliche Umschaltzeiten, falls der Hauptlink einmal ausfallen sollte.



Netzwerk mit dezentraler Switcharchitektur und zentraler Netzzugangskontrolle

Wirksamer Diebstahlschutz durch Disconnect Monitoring

Die Disconnect-Monitor-Funktion der Micro-Switches erkennt, ob ein an den Switch angeschlossenes Endgerät entfernt wird. Über eine zyklische Impedanzmessung der Verbindung über das Twisted-Pair-Kabel überwacht der Switch permanent, ob ein Endgerät physikalisch angeschlossen ist – auch wenn dieses ausgeschaltet ist. Damit kann beispielsweise der Diebstahl eines über Nacht ausgeschalteten Endgerätes zuverlässig festgestellt werden und zu einer sofortigen Alarmierung führen. Herkömmliche Switches können nur über den Linkstatus erkennen, ob ein Endgerät angeschlossen ist. Bei ausgeschaltetem Endgerät kann ein Entfernen des Gerätes so nicht festgestellt werden.
Alarmmeldungen des Disconnect Monitors können als SNMP Traps oder Syslog erfasst und über einen geeigneten externen Dienst beispielsweise als SMS oder E-Mail weitergeleitet werden. Administrator und Sicherheitsdienst können so einfach, schnell und zuverlässig informiert werden.

Einfach sicherer

Ob Verkabelungen mit Glasfasern oder Kupferleitungen – Gebäudeinfrastrukturen mit dezentraler Switch-Architektur bieten zahlreiche Vorteile.
Geringerer Verkabelungsaufwand und eine einfache Erweiterbarkeit bestehender Netze ohne Betriebsunterbrechung führen zu niedrigen Installations- und Betriebskosten.
Die am Arbeitsplatz zum Einsatz kommenden Micro-Switches bieten alle Sicherheits- und Management-Features, die bis dato Core-Switches vorbehalten waren. Mit überwachten, managebaren Geräten in Anwendernähe können unberechtigte Zugriffe abgewiesen werden, noch bevor sie sich mit dem Netz verbinden. Richtungsweisende Funktionen wie der Disconnect Monitor können feststellen, ob Endgeräte entfernt werden – selbst wenn das Endgerät ausgeschaltet ist. Die Möglichkeit zur einfachen Kaskadierung und Dual Homing sorgen für eine erhöhte Ausfallsicherheit bei nur minimalem Aufwand.
Dabei bieten dezentrale Infrastrukturlösungen nicht nur technische, sondern auch wirtschaftliche Vorteile, wie einschlägige Studien nachweisen.

GBE Desktop Switch von MICROSENS mit Disconnect Monitor überwacht auch ausgeschaltete Endgeräte und sorgt somit für wirksamen Diebstahlschutz.