SDN im Data Center
Referenzbericht

«Der Ablösungsbedarf des Data Center-Netzwerks hat uns bewogen, die ganze IT-Sicherheitsarchitektur zu hinterfragen und zu überarbeiten. Mit Hilfe von Econis haben wir unsere Netzwerk- und Sicherheitskonzepte bereinigt und auf Basis eines Software Defined Networks (SDN) von Cisco umgesetzt.»

Martin Meier,
Senior Infrastructure Engineer, HTW Chur

HTW - Hochschule für Technik und Wirtschaft

Die Fachhochschule HTW Chur bildet Fach- und Führungskräfte aus. Sie ist regional verankert und mit rund 1700 Studierenden ein Anziehungspunkt über die Kantons- und Landesgrenzen hinaus. Die HTW Chur bietet Bachelor- und Masterstudiengänge sowie Weiterbildungen an. Sie trägt mit angewandter Forschung zu Innovationen und Lösungen für die Gesellschaft bei. Ab 1. Januar 2020 wird die HTW Chur die 8. öffentlich-rechtliche Fachhochschule der Schweiz sein.

HTW Chur
Hochschule für Technik und Wirtschaft
University of Applied Sciences

Schrittweiser Umbau der Core-Infrastruktur

Die HTW Chur hat die Econis AG mit der Konzeption und dem Parallelaufbau des neuen Netzwerks und der anschliessenden Migration beauftragt.

Interview mit Martin Meier, Senior Infrastructure Engineer, HTW Chur

Sie haben ein Redesign Ihrer Core-Infrastruktur vorgenommen. Wie ist es dazu gekommen?
Die HTW Chur befindet sich im Wachstum und es gilt auch künftig die Informatik effizient und sicher zu betreiben. Teile unserer Core-Infrastruktur aus den Jahren 2007/08 gelangten ans Ende ihres Life Cycles. Zudem war unser Securitykonzept mit 38 Firewalls über die Jahre höchst unübersichtlich geworden. Deshalb sollte das gesamte Policy Set bereinigt und nur noch über einige wenige Firewalls geregelt werden.

Sie haben Econis zum Migrationspartner gewählt. Warum?
Mit Econis verbindet uns seit über zehn Jahren eine eingespielte Zusammenarbeit. Sie kennen unsere Infrastruktur und unsere Bedürfnisse. Das gab uns bei diesem – für uns nicht alltäglichen Projekt – die Gewissheit, mit Econis den richtigen Ansprech- und Umsetzungspartner zu haben. In unserer Einschätzung wurden wir im Gesamtprojekt rundum bestätigt. Econis hat das Projekt mit vollem Einsatz zum Erfolg gebracht und das Budget sogar unterschritten.

Worin liegt der grosse Unterschied der heutigen Lösung zur alten Infrastruktur?
Das neue ACI zentriert sämtliche Anwendungen in einem Software Defined Network (SDN). Dabei werden alle Switches von einem zentralen Controller gesteuert. Sämtliche Regeln können über ein Web GUI bequem festgelegt und gesteuert werden. Früher mussten wir für 38 Zonen alle Regeln dezentral und auf mehreren Firewalls konfigurieren. Im Projekt haben wir die Struktur auf eine Handvoll Zonen heruntergebrochen. Dank der Microsegmentations-Möglichkeiten von Cisco ACI können wir bei Bedarf trotz der starken Vereinfachung erheblich granularer segmentieren als zuvor.

Wie haben Sie das Projekt in Angriff genommen und umgesetzt?
Wir haben das Projekt während zweier Jahre in den schulfreien Phasen realisiert. 2017 starteten wir mit Konzeptarbeiten und Workshops, haben dann mit dem Parallelaufbau von Cisco ACI begonnen und im Sommer die Data Center Switches durch Cisco ACI abgelöst. 2018 haben wir das Core-Redesign und den Firewallersatz in Angriff genommen, die Logik umgebaut und die Mikrosegmentierung eingeführt. Unsere Informatikfachleute haben eng mit den Econis Network Engineers zusammengearbeitet. Diese haben uns abschliessend so geschult, dass wir das System möglichst selbstständig betreiben und Fehler beheben können.
Der Support ist durch SLAs mit Econis gesichert. Für uns, intern, geht das Projekt noch weiter: Wir nehmen die neuen WLAN Controller in Betrieb und ersetzen danach den fast leergeräumten Campus Core durch eine schlankere Lösung. Ideal ist, dass wir nicht alle Funktionalitäten auf einmal umstellen müssen. Ein durchdachtes Migrationskonzept erlaubt es uns, alte Systeme vorerst zu integrieren und sie nach und nach abzulösen.

Mit welchen besonderen Herausforderungen wurden Sie im Projekt konfrontiert?
Das komplette Firewall-Regelset neu zu definieren war eine gewaltige Herausforderung. Mit internen Ressourcen haben wir in Zusammenarbeit mit Econis ein Script programmiert, welches die Regeln von rund 40 Firewalls unterschiedlicher Hersteller eingelesen, bereinigt und angepasst auf die neue Architektur ausgegeben hat. So konnten wir am Tag X auf Knopfdruck die konsistenten und bereinigten Regeln auf den neuen Firewalls importieren. Die effektive Migration (Routing, Firewalls, Microsegmentation) erbrachten wir mit Hilfe von Econis an einem Wochenende innert 44 Stunden; dank der sorgfältigen Vorbereitung und dem Sondereinsatz aller Beteiligten unterbruchsfrei und erfolgreich! Als herausfordernde Spezialfälle haben sich das Multicast Routing für die campusweite Alarmierung via IP Telefonie erwiesen sowie das vorhandene mDNS (Bonjour Gateway) für Applikationen wie Everyone Print usw. Doch auch das haben wir schliesslich gemeistert.

Martin Meier
HTW Chur, Senior Infrastructure Engineer

«Der bevorstehende End of Life-Status der Netzwerk-Infrastruktur im Data Center gab den Anstoss für das komplette Redesign. Für die Fachhochschule ist die gewählte neue Lösung ein Zukunftsschritt zu einem einfacheren, effizienteren und sichereren IT-Betrieb.»

Innovative, risikominimierte IT-Strategie basierend auf ACI

(Weiterführung des Interviews)

Worin liegt der objektive Nutzen des Redesigns für die HTW Chur?
Die Bereinigung der Logik, das Software Defined Networking und die Auftrennung der verschiedenen Building Blocks vereinfachen die gesamte Architektur. Und einfacher heisst auch sicherer: sowohl bei der Konfiguration als auch bei der Reduktion der Failure Domain Grösse. Eingriffe erfolgen an wenigen Stellen, wo es früher bis zu 40 waren. So müssen wir dank Hypervisor-Integration neue Netze nur noch an einer einzigen Stelle erfassen. Zum Vergleich: früher mussten wir ein neues Netz manuell auf allen Switches, der Firewall, dem Blade-System und im vCenter konfigurieren und waren dafür besorgt, dass die Änderungen umgebungsweit konsistent implementiert wurden. Das Gleiche gilt auch für das Troubleshooting, welches sich nun auf ein paar Firewalls mit zentralem Logging beschränkt, statt auf 38 Firewalls mit individuellen Logs wie zuvor. Snapshot & Restore Tools innerhalb des Netzwerks, wie man das zum Beispiel von VMware kennt, führen zu einer erheblichen Risikominimierung bei Anpassungen und falls nötig zu einem einfachen Rollback auf Knopfdruck. Der Backupverkehr (east-west) wird direkt in der Fabric geroutet und kontrolliert und entlastet die Firewall erheblich. Zudem konnten wir auch unsere neue Virtual Desktop Infrastructure (VDI) sinnvoll und gesichert ins Netzwerk einbinden. Insgesamt haben wir mit dieser State of the Art-Lösung die Grundlagen geschaffen, unseren IT-Betrieb langfristig sicherzustellen. Wir sind bereit für automatisierte Konfigurationen. Wir sind ready für Multi Cloud-Umgebungen. Und wir sind gerüstet für einen allfälligen weiteren Ausbau.

Umsetzung der neuen Lösung.

Ausgangslage
Das Core-Netzwerk und die Core-Firewall der HTW Chur waren am Ende des Life Cycle angelangt, das Securitykonzept über die Jahre unübersichtlich geworden und dessen Betrieb schwierig zu bewerkstelligen. Neben der Ablösung der Core-Infrastruktur war zentral, die bestehenden 38 Firewalls möglichst zu reduzieren. Für etliche, im Einsatz stehende, Geräte bestanden teilweise bereits keine Ersatzmöglichkeiten mehr.

Die Campus Core Switches (Catalyst 6500) dienten gleichzeitig als Data Center Cores und enthielten zudem mehrere Service Module (WLAN Controller, Firewall). Die daraus entstandenen Abhängigkeiten sollten reduziert und das Risiko durch die Unterteilung in Building Blocks minimiert werden.

Diese Situation wurde zum Anlass genommen, die gesamte IT-Infrastruktur zu überdenken und die IT-Strategie auf die Zukunft sowie das stetige Wachstum der Hochschule auszurichten.

Ziele und Anforderungen
Das junge, dynamische Team verfolgte einen innovativen und zukunftsorientierten Ansatz, der ihrer modernen Hochschule sicherheitstechnisch und wirtschaftlich eine State-of-the-Art-Lösung versprach. Früh hatte es erkannt, dass die gestellten Anforderungen mittels ACI-Technologie von Cisco erfüllt werden konnten.

Das Core-Netzwerk sollte Schritt für Schritt aufgebrochen werden, entsprechend den heutigen IT-Architekturen, die sich in den letzten zehn Jahren stark weiterentwickelt hatten.

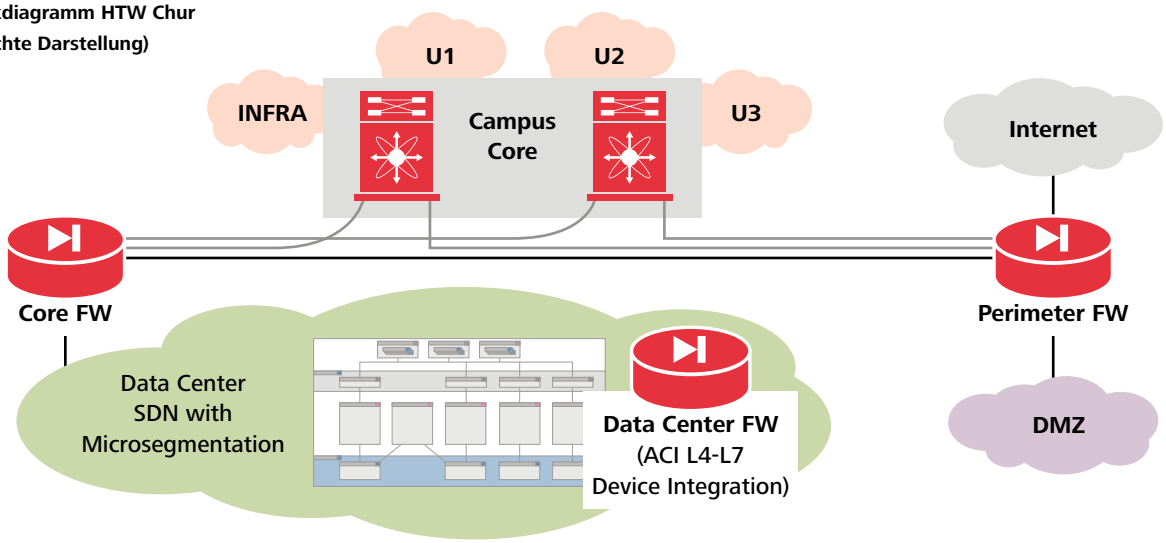
Umsetzung der neuen Lösung

Vorgehen und Lösung

Die traditionellen Nexus 5500 Data Center Switches wurden durch moderne SDN Switches (Nexus 9000) ersetzt. Der collapsed Network Core (Catalyst 6500 mit Service Modulen) wurde schrittweise abgelöst. Gleichzeitig wurden die schützenswerten Out-of-Band (OOB) Management Interfaces der Data Center Geräte in ein unabhängiges und sicheres OOB Netzwerk ausgelagert. Im Bereich Security wurden neben der Perimeter Firewall eine neue Core Firewall sowie eine neue Data Center Firewall mit zentralem Loggingsystem aufgebaut. Das brachte eine erhebliche Vereinfachung des Security-Zonen-Designs mit einer Reduktion von 38 auf 2 Firewalls.

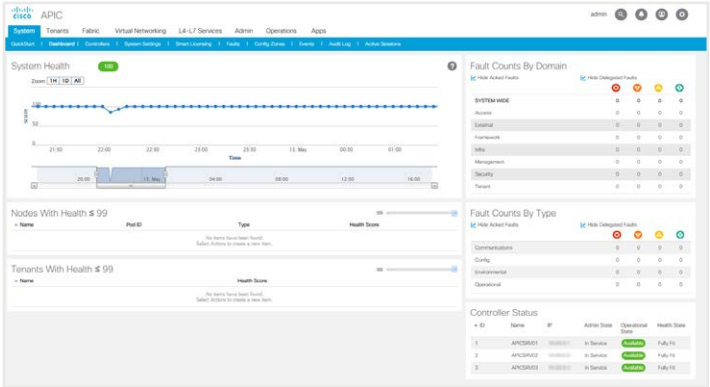
Eine Konsequenz daraus war es, die Security-Zonen neu zu definieren sowie die Security Policies zu bereinigen und zu vereinfachen. Für die Bereinigung und Migration der Firewallkonfigurationen wurde von einem Informatikspezialisten der HTW Chur eine eigens dafür entwickelte Software bereitgestellt. Dank minutiöser Vorbereitung und sorgfältigen Tests verlief die Migration reibungslos. Die Implementierung der Lösung erfolgte partnerschaftlich durch die Engineers der HTW Chur und Econis. Die Vorgehensweise der Umsetzung ist aus dem Interview mit Martin Meier ersichtlich, der sich bei der HTW Chur für das Projekt verantwortlich zeichnete.

Netzwerkdiagramm HTW Chur (vereinfachte Darstellung)



Projektziel: Abbau des monolithischen Netzwerk-Cores und Auftrennung in vier Building Blocks

ACI Dashboard



Beim Betrieb hilft der zentrale Einstiegspunkt über das Web GUI mit einem übersichtlichen Dashboard, wo zum Beispiel allfällige Probleme fabric-weit auf einen Blick angezeigt werden.

Ein Schritt in die Zukunft mit einfacherem, sicherem Betrieb

Meilensteine

- **Q2/2017**
  Start der Konzeptarbeiten und Workshops / Parallelaufbau von Cisco ACI
- **Sommer 2017**
  Ablösung der Data Center Switches (Nexus 5k/2k) durch Cisco ACI (im Layer 2 Modus)
- **Q2 2018**
  Konzeptarbeiten für Core Redesign und Firewall-Ersatz / Parallelaufbau der neuen Firewall-Infrastruktur
- **Sommer 2018**
  Migration
  – Migration Layer 3 in ACI
  – Microsegmentierung
  – Ersatz Core Firewall
- **Herbst 2018**
  Schulung und Projektabschluss

Nutzen für die HTW Chur
Das Projekt «Core and Data Center Redesign» brachte der HTW Chur mehrere Vorteile. Mit der Umsetzung der innovativen IT-Strategie wappnet sich die Hochschule für zukünftige Anforderungen und ist für die Weiterentwicklung der IT-Infrastruktur vorbereitet. Die Grundlagen für eine Infrastrukturautomatisierung wurden gelegt und die eingesetzte Technik ebnet den Zugang zu Multicloud-Umgebungen.

Über HTW Chur

Hauptsitz
Pulvermühlestrasse 57, 7004 Chur

Themenschwerpunkte
Die HTW Chur hat in ihrer Strategie drei Themenschwerpunkte definiert. Die Fachhochschule aus Graubünden betreibt in allen Themenschwerpunkten Lehre, Weiterbildung, angewandte Forschung und Dienstleistung.
– Angewandte Zukunftstechnologien
– Lebensraum
– Unternehmerisches Handeln

Anzahl Mitarbeitende
Stand 2018: 245
Zusätzlich sind 293 Lehrbeauftragte, Gastdozierende und Hilfskräfte befristet bei der HTW Chur tätig

Studierende
2017: 1447
2018: 1718

Econis

Das fördert die nutzbringende Zusammenarbeit

Werte und Qualität
In allen Handlungen orientiert sich Econis an den Zielen und Bedürfnissen der Kunden.

Partner
Für perfekte Outsourcing-Dienstleistungen, vorteilhafte Managed Services und komplette IT-Lösungen arbeitet Econis mit global führenden Technologiepartnern zusammen.

Service Desk
Garantierte Supportleistungen erbringt die Econis Service Desk und die Pikett-organisation bis 24/7/365 gemäss SLA.

Unternehmensführung
Die erfahrene Führungsmannschaft der Econis AG handelt kontinuierlich, konsequent und konsistent.

Erfahren Sie mehr unter: econis.ch

Smart. Innovativ. Persönlich.

Das führende Schweizer Technologie- und Dienstleistungsunternehmen Econis entwickelt und betreibt kundenspezifische IT-Infrastrukturlösungen und Services. Die interdisziplinäre Ausrichtung befähigt Econis, ihre Kunden umfassend zu betreuen. Die Outsourcing-Angebote bauen konsequent auf Modulen auf. Sie rationalisieren Geschäftsprozesse, reduzieren die Komplexität, setzen Management-kapazität frei und steigern dadurch die Agilität der Kunden.

econis.ch

Econis AG, Neumattstrasse 7, CH-8953 Dietikon
T +41 44 744 73 73, F +41 44 744 73 99

Econis AG, Werkstrasse 37, CH-3250 Lyss
T +41 32 387 93 87, F +41 32 387 93 88

Econis AG, Arsenalstrasse 4, 6005 Luzern
T +41 41 310 67 77