SUCCESS STORY

NETCLOUD

SCHWEIZERISCHE RHEINHÄFEN

ALL-IN-ONE SECURITY LÖSUNG VON CISCO

- **Next Generation Firewall**
- **E-Mail Security Appliance**
- **Umbrella – Web Security**
- **Advanced Malware Protection**

© Patrik Weigt Photography

„**Muss denn immer erst etwas gravierendes passieren?** Nein, das war für uns definitiv keine Option. Als einziger Hafen in der Schweiz tragen wir eine grosse Verantwortung gegenüber unseren Mitarbeitenden und Kunden. Die bisherige Security Lösung war in die Jahre gekommen. Nun galt es, diese abzulösen. Nach umfangreichem Benchmark haben wir uns für eine Security Infrastruktur entschieden, die unseren Anforderungen voll und ganz entspricht – ein All-in-One Paket von Cisco, welches von unserem zuverlässigen Partner Netcloud implementiert wurde. Und das optimale Zusammenspiel aller Sicherheitskomponenten, bietet uns in sämtlichen Teilbereichen den Rundumschutz, den wir benötigen."

PORT OF SWITZERLAND

Matthias Frech
IT System Specialist, SRH

Der Rhein als Tor zur Welt

Die Schweizerischen Rheinhäfen sind die nationale Drehscheibe im Güterverkehr zwischen Rotterdam, Basel und Genua. In den drei Hafenteilen Basel, Birsfelden und Muttenz werden jährlich 6 Millionen Tonnen Güter und 100'000 Container umgeschlagen. Dies entspricht zwölf Prozent aller Schweizer Importe. Jeder dritte Liter Mineralöl und jeder vierte Container werden über die Rheinterminals abgewickelt. Eine exzellente Anbindung an die Schiene und Strasse gewährleisten den Weitertransport von Gütern aller Art. Gegen 100 Hafenfirmen ermöglichen damit einen wichtigen Teil des Schweizer Aussenhandels.

Sicherheit geht vor

Lotsen haben die Aufgabe, Schiffe durch Untiefen, Strömungen oder Nebel zu navigieren. Dabei stehen sie dem Kapitän des Schiffes beratend zur Seite. Eine funktionierende Security Infrastruktur der Schweizerischen Rheinhäfen (SRH) ist ebenso verpflichtend wie das sichere Umschiffen von Hindernissen durch genaueste Kenntnisse der Umgebung. Die Anforderungen an eine adäquate Security Lösung konnten mit der vorhanden Infrastruktur nicht mehr gewährleistet werden. Somit fiel die Entscheidung für eine neue, moderne Security Infrastruktur. Netcloud hat nun die Funktion des Lotsen übernommen und ein Konzept für eine komplett neue Security Infrastruktur erstellt. Dabei gab es verschiedene Klippen zu umschiffen, die vorgängig in einem Workshop zusammen mit der SRH erarbeitet und definiert wurden. Aspekte wie Wirtschaftlichkeit und Preis-/Leistungsverhältnis waren ebenso wichtig wie Erfahrungswerte aus bereits umgesetzten Projekten ähnlicher Art. Auch die Skalierbarkeit im Bezug auf Erweiterung und Ausbau an zukünftige Anforderungen waren gesetzt. Gesamthaft wünschte sich die SRH ein optimales Zusammenspiel der verschiedenen Security Komponenten, um einen umfassenden Schutz über alle Teilbereiche hinweg zu erlangen.

All-in-One

Nach Abwägung aller möglichen Varianten hat sich die SRH für eine All-in-One Lösung von Cisco entschieden. Der IT System Specialist der SRH, Matthias Frech, erklärt dies so: „Wir legen grossen Wert auf Sicherheit und dafür ist die Trennung aller Services notwendig. Denn sollte doch ein Hackerangriff passieren, so wird nur ein System kompromittiert. Und da sehen wir auch ganz klar den Vorteil mit der Cisco Lösung."

Sicherheitslösung der neuesten Generation

Bevor die Security Lösung implementiert werden konnte, musste vorgängig das WLAN Netz aus der bestehenden Umgebung herausgelöst werden. Dann konnte es losgehen. Die folgenden Sicherheitskomponenten wurden migriert:

Die **Next Generation Firewall** basiert auf der Cisco Firepower 2100 Serie und entspricht den State-of-the-Art Anforderungen für Security. Mit der Multicore Architektur bietet sie gegenüber herkömmlichen Firewall Systemen den Vorteil, dass der Durchsatz mit Service Stacking nicht einbricht. Selbst wenn die SRH zu einem späteren Zeitpunkt einen weiteren Security Service auf der Firewall aktivieren möchte, wie z.B. Malware Checks oder SSL Decryption, schlägt sich das nicht auf die Performance nieder. Dazu kommt, dass die SRH als „Early Adopter" in der Schweiz mit dieser Lösung ausgestattet wurden.

Als Schutz für den Email Verkehr kommt die **Cisco Email Security Appliance** zum Einsatz. Das Cisco ESA Netzwerk umfasst 35% des weltweiten Mail Traffics. Diese globale Sicht ermöglicht jeder ESA Instanz, innert kürzester Zeit auf bekannte und neue Bedrohungen zu reagieren. Befinden sich innerhalb einer Email schadhafte URLs, Malware Anhänge oder andere Bedrohungen, werden diese umgehend detektiert und blockiert, über einen Webproxy umgeleitet und in Quarantäne gelegt. Alle vier Stunden wird automatisch die Cisco Threat Intelligence abgefragt, ob es Neuerungen aus den Untersuchungen gibt. Handelt es sich tatsächlich um einen neuen Outbreak, wird die Email endgültig blockiert. Die Lösung besteht hier aus der ESA als Mail Transfer Agent und der SMA als Manager Appliance, welche als zentrale Spam Quarantäne dient. Das Message Tracking ist sehr detailliert. Somit kann man stets nachvollziehen, warum eine Nachricht abgelehnt wurde.

Dank dem **cloudbasierten Cisco Umbrella** Service wird auf den Einsatz eines klassischen Webproxys verzichtet. Bereits beim Verbindungsaufbau wird via DNS eine erste Prüfung durchgeführt. Dies hat den Vorteil, dass Traffic im Falle von Malware oder geblockten Kategorien erst gar nicht entsteht und entlastet somit die Geräte. Ein weiterer Vorteil der Umbrella Lösung ist, dass sie auch Schutz für Firmengeräte bietet, die sich nicht im Netzwerk befinden oder per VPN verbunden sind. Die letzte Komponente dieser All-in-One Lösung widmet sich der Endpoint Protection.

Die Cisco **Advanced Malware Protection (AMP)** besteht aus zwei Teilen, dem Schutz am Endpoint sowie dem Schutz durch die Integration in bestehende Netzwerk Komponenten, wie z.B. der Firewall. Von Vorteil ist, dass beide Teile dieselbe Cloud für Updates sowie dieselbe Logik benutzen. Damit ist die Erkennung von Threats, beispielsweise durch die Firewall, auch für die Endpoints ersichtlich. Cisco setzt hierbei auf diverse Technologien, die dazu beitragen, Dateien als sicher oder als Malware zu klassifizieren. Dank der AMP Cloud sind auch hier Remote User geschützt, ohne dass sie sich mittels VPN auf das Firmennetzwerk einwählen müssen.

Die heutige IT Welt ist sehr komplex. Einen Hersteller für die Gesamtlösung zu nutzen, birgt viele Vorteile und hilft, die Komplexität zu reduzieren. Somit können bereits im Vorfeld Reibungspunkte vermieden werden. Matthias Frech ergänzt: „Eine Single Vendor Strategie hat uns insofern überzeugt, dass die einzelnen Komponenten miteinander verzahnt sind und unablässig kommuzieren. So werden Angriffe, egal über welchen Bereich diese in unser System eindringen, erkannt, nachverfolgt und eliminiert. Wir sind bestens aufgestellt für die Zukunft."

Technische Umsetzung: Die bei den Schweizerischen Rheinhäfen eingesetzte Lösung basiert auf einer redundant ausgelegten Firepower 2100 Plattform. Diese läuft im Unified Image (FTD) als Next Generation Firewall (NGFW) und verbindet somit Anti-Malware, NGIPS und klassisches Firewalling am Internet Edge. Dank der Multicore Architektur stehen auch für zukünftige Ausbauten genügend Ressourcen zur Verfügung. Als Verwaltungs- und Reporting Appliance wird das Cisco Firepower Management Center (FMC) eingesetzt. Policies werden hier zentral gesteuert und auf die einzelnen Geräte verteilt. Ähnlich verhält es sich bei der Email Security Appliance (ESA), welche ebenfalls redundant ausgelegt ist und dank Clustering ein zentrales Management bietet. Reporting und Message Tracking findet zentral auf der Security Management Appliance (SMA) statt. Sämtliche Appliances der Email Security Lösung sind virtuell und bieten somit einen kleinen Footprint. Auf den Clients und Servern sorgt Advanced Malware Protection for Endpoints (AMP4E) für Schutz. AMP for Networks läuft als Service innerhalb der NGFW und der ESA und erkennt und blockiert somit frühzeitig Threats, so dass diese nach Möglichkeit nicht bis zum Endpoint gelangen. Um Infektionen ausserhalb des Firmennetzwerkes zu vermeiden, schützen die beiden Cloud-Dienste AMP4E und Umbrella. Dank der Cloud ist eine einheitliche Policy in- und ausserhalb der Firmenumgebung gewährleistet.

Vorteile der All-in-One Lösung mit Netcloud im Überblick

Informationsaustausch und Zusammenspiel der einzelnen Security Services
Rückverfolgbarkeit bei Security Incidents vom Internet Edge bis hin zum Client, sowohl North-South wie auch East-West
On- und Off-Network Protection mit einheitlichen Policies
Automatisches **Sandboxing** von unbekannten und potentiell schädlichen Dateien
Zentralisiertes Management und Reporting
Hohe Skalierbarkeit und Verfügbarkeit
Automatisches **Update der Cloud Infrastruktur** durch den Hersteller
Transparenter **Schutz** der gesamten DNS Infrastruktur
Minimaler Footprint dank **Virtualisierung**

Mehr über unsere Success Stories erfahren Sie
unter +41 58 344 12 12, sales@netcloud.ch, www.netcloud.ch

Netcloud AG in **Winterthur**: Gewerbehaus Nägelsee, Schlachthofstrasse 19, 8406 Winterthur
Netcloud AG in **Bern**: Carba Center, Waldeggstrasse 37, 3097 Liebefeld
Netcloud AG in **Basel**: Schützengraben 21,4051 Basel

NETCLOUD BERN WINTERTHUR
ICT PROFESSIONALS BASEL