Technische Berufsschule Zürich TBZ

Höhere Fachschule
Sihlquai 101
8090 Zürich

Evaluation und Implementation einer neuen Virenschutzlösung (PoC)

Diplomand: Fabienne Wenger
Klasse: ITSE18a
Schulexperte: Hans Rudolf Kramer
Firmenexperte: Roman Koller
Firma: Nexpert AG

Fabienne Wenger

Firmenportrait

Die Firma Nexpert AG unterstützt Unternehmen und Informatik-Organisationen mit massgeschneiderten Lösungen über das gesamte IT-Spektrum; von der Bedürfnisanalyse und der Prozessoptimierungsberatung über das Design und die Implementation von Infrastrukturlösungen bis zur Evaluation und Einführung von betriebswirtschaftlichen Lösungen und dem professionellen Outsourcing-Betrieb.

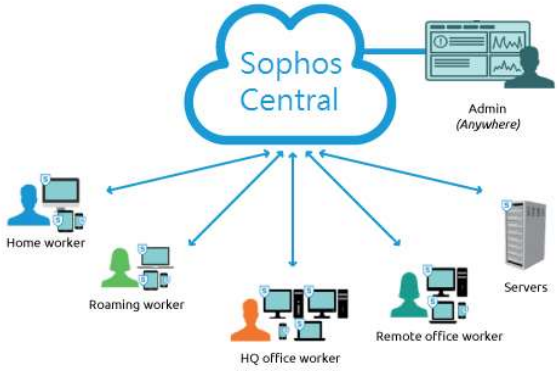
Zu den über 150 Kunden gehören Grossunternehmen und mittelständische Firmen aus Industrie, Handel und dem Dienstleistungssektor, Versicherungen, Finanzdienstleister, Anwaltskanzleien sowie Organisationen der öffentlichen Hand.

Ausgangslage

Einige Bestandeskunden der Nexpert AG nutzen aktuell noch den serverbasierten Virenschutz Sophos Endpoint Protection mit eXploit Prevention. Diese Lösung entspricht nicht mehr den eingesetzten Nexpert-Standards und wird spätestens im Juni 2Q23 End-of-Life sein. Deshalb soll in dieser Projektarbeit der PoC bestehend aus Evaluation, Planung und Test-Implementation durchgeführt werden. Das wesentliche Ziel der Arbeit besteht darin, aus dem PoC eine geeignete Virenschutzlösung für die Ablösung der Systeme zu finden.

Technische Berufsschule Zürich TBZ

Höhere Fachschule
Sihlquai 101
8090 Zürich



Evaluation

Virenschutzhersteller gibt es mittlerweile wie Sand am Meer. Einige der zur Auswahl gestandenen Produkte mussten auf Grund von fehlenden Komponenten, nicht erreichen der Muss-Ziele sowie ungenügender Schutzleistung für Business-Umgebungen bereits aus dem Rennen genommen werden. Die drei Produkte Sophos Central, McAfee MVISION und Trend Micro Worry-Free erfüllen jedoch alle Anforderungen und wurden deshalb getestet Die durchgeführte Wirtschaftlichkeitsanalyse (mit SWOT-Analyse, Präferenzmatrix und Produkt- & Nutzwertanalyse) zeigte zum Schluss einen klaren Produktsieger: Sophos Central. In Bezug zu den aktuell eingesetzten on-premises Kundenumgebungen erfüllt diese Lösung alle Anforderungen, Kriterien und Ziele.

Hauptstudie

In der Hauptstudie wurde Sophos Central genauer unter die Lupe genommen. Dabei hat sich herausgestellt, dass die Lösung weitaus mehr als nur einen herkömmlichen Virenschutz bietet. Über die zentrale Plattform können alle cloud-fähigen Produkte von Sophos verwaltet werden.

Realisierung

Die Inbetriebnahme von Sophos Central ist sehr intuitiv aufgebaut. Alle lizenzierten Komponenten sind über einen separaten Menü-Punkt im Portal ersichtlich.

Für die Realisierung wurden drei virtuelle Systeme (2x Server, 1x Win10 Client) und drei physische Geräte (1x Notebook, 1x Tablet, 1x Mobile) mit dem Virenschutz ausgestattet und entsprechend dazu passende Richtlinien erstellt. Beim Notebook wurde zusätzlich die Verschlüsselung implementiert. Alle mit dem Produkt durchgeführten Tests verliefen erfolgreich.

Fazit

Alle definierten Ziele konnten im Laufe der Arbeit erfüllt werden. Sophos bietet mit der Central-Lösung eine einfache, zentrale Plattform für die Verwaltung der eigenen Next-Gen-Security-Lösungen.

Alle Vorbereitungen für mögliche Kunden-Migrationen nach Abschluss dieser Diplomarbeit sind abgeschlossen. Die Resultate der Arbeit werden abschliessend intern vorgestellt, um weitere Entscheidungen für die Schritte in Richtung Sophos Central vorzunehmen.