Network Access Protection

Ausgangslage

Das Unternehmen KMU IT Management AG sucht ein Produkt, welches infizierte Computer isoliert und somit keine Gefahr für andere Geräte darstellt. Vor ein paar Jahren wurde das Produkt FreeNAC evaluiert, jedoch entsprach dies nicht den Vorstellungen des Unternehmens.

Ziel der Arbeit

Dieses Projekt soll das Network Access Protection von Microsoft analysieren. Es soll die Stärken und Schwächen aufzeigen. Als Resultat wird eine Empfehlung erwartet, ob Network Access Protection implementiert werden soll oder nicht.

Network Access Protection

Network Access Protection ist ein Produkt von Microsoft. Es verhindert, dass Clients, die ungenügend geschützt sind, das Firmennetz beschädigen können. Ungenügend geschützten Clients wird limitierter Zugriff ins Firmennetzwerk gewährt. Clients mit limitiertem Zugriff können nur Server kontaktieren, die sie aktualisieren und mögliche Sicherheitslücken schliessen können. Falls dieser Vorgang erfolgreich abläuft erhält der Client dadurch vollen Zugriff. Der limitierte Zugriff kann durch fünf verschiedene Methoden implementiert werden.

- DHCP NAP Enforcement
- IPSec NAP Enforcement
- 802.1x NAP Enforcement
- VPN NAP Enforcement
- TS Gateway NAP Enforcement

Die DHCP, IPSec und 802.1x NAP Enforcement Methoden verwalten den direkten Zugriff ins LAN. Die VPN und TS Gateway NAP Enforcement Methoden verwalten den Zugriff von aussen ins LAN. Die Methoden lassen sich miteinander verknüpfen.

Empfehlung

Ich empfehle dem Unternehmen die 802.1x NAP Enforcement Methode zu implementieren. Diese Methode ist sehr sicher und einfach zu implementieren. Für die Implementation dieser Methode werden 802.1x Switches benötigt. Die KMU IT Management AG besitzt solche Switches. Die IPSec Variante ist ebenfalls empfehlenswert, jedoch ist die Implementation sehr komplex. Meiner Meinung nach ist die IPSec NAP Enforcement Methode vom Aufwand her nicht geeignet für kleinere Firmen.