Implementierung der Endpoint Protection Plattformen Apex One und Deep Security

Studiengang: MAS Cyber Security

Cyberkriminalität ist heutzutage ein sehr lukratives Geschäft. Mittels verschiedenen Methoden werden schätzungsweise Milliarden an Umsatz generiert. Gemäss dem NCSC gehört Ransomware immer noch zu den Top-Cyberbedrohungen. Um die Endpoint Security zu erhöhen, will die Kliniken Valens die zwei Endpoint Protection Plattformen Apex One und Deep Security von Trend Micro implementieren.

Blerand Mehukaj

Ausgangslage

Die Bedrohung durch eine Cyberattacke steigt stetig an. Dabei sieht man die Endpoints eines Unternehmens gerne als Eingangstor ins Unternehmensnetzwerk an. Die Angriffstechniken gegen die Endpoints werden immer ausgefeilter. Vor allem Ransomware Attacken, früher einfacher und automatisierter, haben sich zu hoch organisierten und von Menschen gesteuerten Kampagnen entwickelt. Ziel ist es das Maximum an Lösegeld von den Opfern zu erpressen. Hinzu kommt der Faktor Mensch. Ob Stress, Arbeitslast oder Gutgläubigkeit, es braucht nur einen Klick um dem Angreifer Zutritt zu gewähren. Eine reine Anti-Malware Lösung bietet nur minimalen Schutz und ist für die aktuelle Bedrohungslage ungenügend.

Zielsetzung

Das Ziel der Master-Thesis ist die Konzeptionierung und Implementierung der zwei EPP's Deep Security für die Server und Apex One für die Virtuelle Desktop Infrastruktur (VDI), Notebooks und Desktop-PC's. In einem PoC werden die zwei Lösungen überprüft und getestet. Ein weiteres Ziel ist ein funktionierendes Alerting & Reporting zu konfigurieren. Die IT der Kliniken Valens soll immer eine aktuelle Übersicht über die Bedrohungslage auf den Endpoints erhalten.

Vorgehensweise

Ein Projektzeitplan wird erstellt, welcher die Vorgehensweise festhält, sowie die Milestones, den erwarteten und effektiv geleisteten Aufwand. Die Knowledge Base, das E-Learning und die Guides sind die Basis für den Aufbau des Konzeptes. Basierend auf dem Konzept, folg die technische Umsetzung.
In einem PoC liefern die beiden Produkte die ersten Ergebnisse.

Ergebnis

Bei den Testungen vor dem PoC stich die Performance im negativen heraus, dies hatte zwei Gründe. Einerseits brauchen die zusätzlichen Security Features mehr CPU Leistung, andererseits wurden noch keine Exclusions hinterlegt. Bis effektiv gearbeitet werden konnte, dauerte es bis zu drei Minuten. Des Weiteren starteten Applikationen, Explorer uvm. bedeutend langsamer. Damit eine stabile Performance für den PoC gewährleistet werden konnte, wurden Exclusions für Behavior Monitoring, Predictive Machine Learning und Application Control hinterlegt. Folglich war das Arbeiten in der VDI wieder möglich. Im PoC bemerkten die Teilnehmenden eine wenig längere Anmeldezeit, aber das Arbeiten war ohne weitere Herausforderungen möglich. Währen dem PoC alarmierte Deep Security diverse Verstösse. Ein Lieferant der Kliniken Valens hat auf einem Server versucht, eine von der IT nicht autorisierte Software zu installieren. Application Control hat die Ausführung blockiert. Dieser Verstoss wäre mit der jetzigen Lösung nicht aufgefallen. Das Alerting und Reporting funktionierten einwandfrei.

Fazit: Die neuen Endpoint Protection Plattformen bringen eine enorme Steigerung der Endpoint Security. Die zahlreichen neuen Security Features (Abb. 1) helfen den Kliniken Valens sich gegen die steigende Bedrohung einer Cyberattacke zu verteidigen. Die neuen EPP's bieten zudem noch weitere Funktionen an wie Data Leak Prevention, Endpoint Detection and Respons und Advanced Detection and Respons.

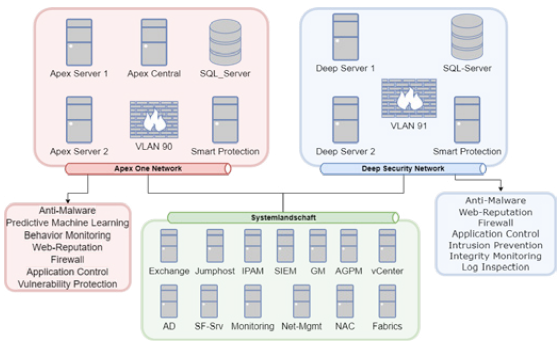

Abbildung 1: EPP's Gesamtübersicht