Evaluation und PoC einer Threat Protection Lösung

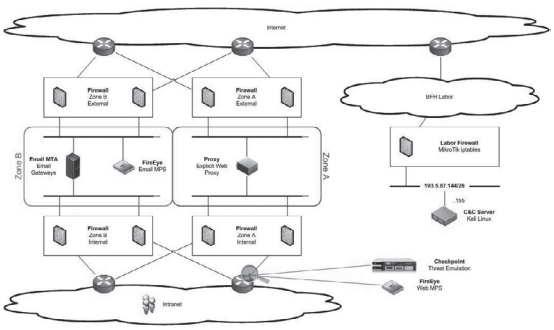
Fachgebiet: Informatik / IT-Security
Betreuer: Prof. Hansjürg Wenger
Experte: Dr. Igor Metz (Gluesoft AG)
Industriepartner: T-Systems Schweiz AG, Zollikofen

Die Bedrohung und das Risiko durch das Internet nimmt für Unternehmen stetig zu. Herkömmliche Schutzmechanismen werden den immer komplexeren, persistenten und gezielten Angriffen nicht mehr gerecht. Threat Protection Lösungen bieten einen neuartigen Ansatz, solche Gefahren zu erkennen und entsprechende Gegenmassnahmen einzuleiten.

Der IT-Provider T-Systems Schweiz AG hat uns die beiden Threat Protection Lösungen von FireEye und Checkpoint zur Verfügung gestellt, um diese bei einem ihrer Kunden zu evaluieren. Mit dieser Arbeit haben wir gezeigt, wie einfach herkömmliche Sicherheitsmechanismen umgangen werden können. Nach den heutigen Standards gesicherte IT-Umgebungen, wie diese des Kunden, waren von unseren Angriffen nicht geschützt. Der Ansatz der Threat Protection Lösung stellt aus unserer Sicht ein effektives Mittel gegen fortgeschrittene Angriffe (APT, Cybercrime, etc.) dar. Diverse Angriffe konnten damit erkannt und protokoliert werden. Gerne werden Threat Protection Lösungen als Wundermittel gegen Zero-days und APT Angriffe angepriesen. Wir haben jedoch bewiesen, dass Threat Protection Lösungen nicht alle Angriffe erkennen und Probleme lösen können. Wir verstehen Threat Protection deshalb als effektive Ergänzung zu den bereits bestehenden herkömmlichen Sicherheitselementen. Die Erkennung von Angriffen alleine reicht als Schutz nicht aus. Zusätzlich zur Threat Protection müssen erkannte Threats auf den Endgeräten analysiert und gegebenfalls isoliert und entfernt werden.

Durch den Einsatz von eigenentwickelter und fremd Malware wurden die beiden Lösungen detailiert analysiert. In den von uns bewerteten Lösungen hat FireEye besser abgeschnitten. Das Produkt ist deutlich ausgereifter und darf nicht nur als eine reine Sandbox Lösung bezeichnet werden. FireEye unterstützt eine grosse Auswahl an Dateitypen und prüft diese in enorm vielen Kombinationen von Betriebssystemen und Applikationsversionen. Zusätzlich wird zum Teil der gesamte Netzwerkverkehr in den virtuellen Umgebungen analysiert. Durch unsere Arbeit wurden einige Mängel festgestellt, die daraufhin vom Hersteller zum Teil behoben wurden. Während der Arbeit hat FireEye die bekannte Sicherheitsfirma Mandiant aufgekauft. Mandiant ist spezialisiert auf das Erkennen und Bereinigen von Threats auf Endsystemen. In Kombination mit FireEye soll in Zukunft eine einheitliche Lösung zwischen der der Threat Protection Erkennung und dem direkten Bereinigen auf den Endgeräten erreicht werden. Dadurch würde sich der Aufwand für die Endsystemanalyse stark verringern. Da die Threat Emulation von Checkpoint erst seit einem halben Jahr auf dem Markt verfügbar ist, war im Vergleich zu FireEye eine Diskrepanz zu erwarten. Bis zum Abschluss der Arbeit war Checkpoint, wider erwarten, nicht in der Lage Executables zu analysieren. Dadurch schliesst das Produkt in unseren Tests verhältnismässig schlecht ab. Erst mit den angekündigten Erweiterungen kann die Lösung von Checkpoint sinnvoll eingesetzt werden. Die Resultate aus unserem Test würden sich damit wahrscheinlich deutlich verbessern.

Die Frage nach dem Nutzen einer Threat Protection Lösung gilt es für jedes Unternehmen individuell abzuschätzen. Die Wahrscheinlichkeit einer Datenentwendung, sowie einer möglichen Manipulation gilt es dem möglichen Schadenausmass gegenüberzustellen. Grundsätzlich dürfte sich der Einsatz einer Threat Protection Lösung für Unternehmen mit sensitiven Daten in den meisten Fällen lohnen.



Netzwerk Übersicht POC

Philipp Langenegger

Lukas Rothacher