FiReS V2

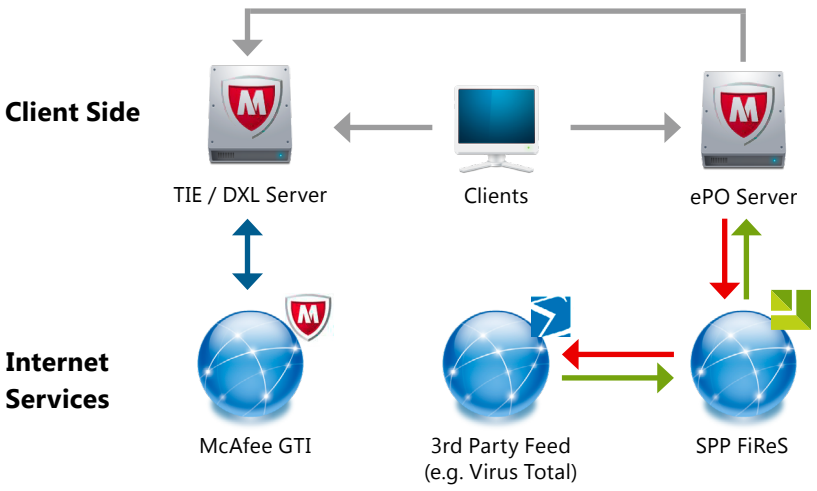
File Intelligence Reputation Exchange Service

Allgemeine Beschreibung

Die grundsätzliche Idee unseres Services ist es, Dateireputationen, neben der GTI-Cloud (Global Threat Intelligence) von McAfee auch auf 3rd Party Feeds, wie z.B. VirusTotal (prüft über 50 Security Hersteller), NSRL oder MHR zu bewerten und zu überprüfen.

Erweiterter Schutz auf Endpoints und Gateways

Filehashes, die von McAfee Security Produkten nicht erkannt werden, jedoch von Herstellern wie Symantec oder Sophos, können am Endpoint durch das Verändern der File-Reputation geblockt werden. Dadurch ist das signaturbasierte Scannen von über 50 AV-Herstellern am Endpoint bzw. Gateway in Real-Time möglich.



VirusTotal Anbindung

VirusTotal - seit 2012 ein Tochter-unternehmen von Google - bietet ein freies Online Service, das Dateien und URLs analysiert, um Viren, Würmer, Trojaner und andere Schadsoftware mit Hilfe von einer Vielzahl an Antiviren- und Website Scannern zu identifizieren. Virustotal bietet dieses Service grundsätzlich gratis an, jedoch ist die Nutzung auf 4 Abfragen pro Minute eingeschränkt.

SPP bietet für Großunternehmen deshalb eine Virustotal-Private-API(SPP FiReS) an, um automatisiert tausende von Dateireputations-Abfragen pro Sekunde zu tätigen. SPP-FiReS wird auf einem ePolicy Orchestrator Server installiert und alle verwalteten Systeme können transparent auf Dateireputationsinformationen von Virustotal und zusätzlich auf NSRL und MHR zugreifen.

Wichtige Funktionen

Datei Reputationsdienst zur Bestimmung der Reputationswerte von unbekannten Dateien oder sich verdächtig verhaltenden ausführbaren Codes.

Erweiterung des vorhandenen McAfee Threat Intelligence Exchange Dienstes um die Erkennungsraten von mehr als 50 AV Herstellern zu steigern.

Die **Gewichtung** der Erkennungsrate kann pro Hersteller selbst eingestellt werden.

Die **Abfrage** in Richtung Virus-Total erfolgt über SPP.

Der Kunde ist **transparent** gegenüber Virus-Total.

Die zurückgelieferte Reputationsinformationen können **nach Belieben weiterverwertet** werden.

Sowohl **Endpoints als auch Gateways** können die umfangreichen Hashdatenbank von Virustotal.com oder NIST über das FiReS nutzen.

Mittels „Data Exchange Layer-Integration“ und einer „ePolicy Orchestratator Anbindung“ ist ein **aktiver Schutz in Real-Time** möglich.