Mit Traps eine neue Sicherheitsstufe im Client einbeziehen – keine Sorgen mehr wegen veralteter Antivirussignaturen

Die steigende Frequenz von APT (Advanced Persistent Threat)-Vorfällen ruft neue Sicherheitsbedrohungen vor. Der Ursprung dieser Bedrohungslandschaft liegt in Schwachstellen auf den Endgeräten der Benutzer. Selbst aktuellste Lösungen sind nicht in der Lage, einen vollkommenen Schutz zu bieten. Konzentrieren Sie sich bei Ihrer IT-Sicherheit auf die Erkennung von Angriffen und die Sanierung Ihrer IT-Landschaft anstatt ausschließlich auf Prävention.

Funktionsweise

Zero-Day-Attacken, die Software-Schwachstellen ausnutzen, zu verhindern ist nur eine der Herausforderungen mit denen Unternehmen heutzutage konfrontiert werden. Bereits bekannte Angriffe werden durch Sicherheitsanalysten untersucht und dank Reverse Enineering deren Angriffsweise analysiert. Auf diesen Erkenntnissen werden Signaturen aufgebaut, wodurch Antivirus-Lösungen diesen Angriff in Zukunft erkennen. Für unbekannte Angriffe gibt es allerdings keine Analyse.

Damit ein Angriff erfolgreich verläuft, muss der Angreifer eine Reihe von aufeinander folgenden Exploit-Techniken ausführen. Dies erfolgt unabhängig von der Komplexität des Angriffs. Attacken benötigen mal mehr, mal weniger Schritte bis zum Erfolg. In allen Fällen werden jedoch mindestens zwei bis drei verschiedene Techniken eingesetzt. Palo Alto Networks Traps benutzt eine Reihe von Exploit Prevention-Modulen, um die einzelnen Schritte des Angreifers zu erkennen und zu blockieren. Der Angriff wird dadurch unterbunden. Die betroffene Applikation ist somit nicht mehr verwundbar.

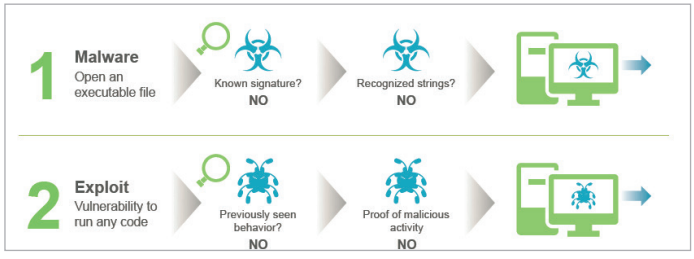

Abbildung 1: Funktionsweise

Der lokal installierte Agent injiziert sich bei jedem Aufruf einer Applikation (die durch TRAPS geschützt werden soll) selbst in den neuen Prozess. Versucht dieser nun etwas Ungewöhnliches zu machen, wie z. B. einen Kind-Prozess zu starten oder auf Speicheradressen zuzugreifen, die nicht zum Prozess gehören, wird der Agent aktiv und blockiert dieses Verhalten. Das Verhalten wird automatisch terminiert, ohne die ursprüngliche Applikation in Mitleidenschaft zu ziehen. Anschließend wird der User informiert. Durch die kettenartige Natur eines Exploits wird durch die Terminierung von einer Exploit-Technik diese komplett unterbunden.

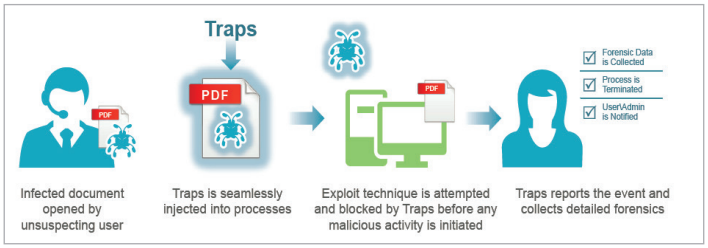

Abbildung 2: Erkennung von Malware

Architekturmodell

Endpoint Security Manager (ESM) - Console

Die Traps-Infrastruktur unterstützt verschiedene architektonische Möglichkeiten und ermöglicht eine Skalierbarkeit selbst auf großen, verteilten Umgebungen. Die Installation des ESM erstellt eine Datenbank auf einem Microsoft SQL-Server und installiert die Verwaltungskonsole in IIS. Microsoft SQL 2008 und 2012 werden hierbei unterstützt. Ebenso kann der SQL-Server für ESM bereitgestellt werden. Andernfalls kann eine Datenbank auf einem vorhandenen SQL-Server erstellt werden.

Endpoint Security Manager - Server

ESM-Server agieren im Wesentlichen als Proxy zwischen Traps und der ESM-Datenbank. Dadurch läuft die Kommunikation verschlüsselt ab. ESM-Server speichern keine Daten und können daher leicht zu einer Umgebung hinzugefügt oder entfernt werden, um eine ausreichende geographische Abdeckung und Redundanz zu gewährleisten.

Traps-Agent

Das Traps Agent-Installationsprogramm ist ein ~9MB MSI-Paket, das mit einem Software-Deployment-Tool Ihrer Wahl verteilt werden kann. Spätere Aktualisierungen an den Agenten können über die ESM verteilt werden. Der Agent verbraucht weniger als 25MB auf der Festplatte und weniger als 40MB, während er im Speicher ausgeführt wird. Die CPU-Auslastung ist dabei geringer als 0,1%. Der Agent verwendet verschiedene Manipulationsprüfverfahren, um zu verhindern, dass Benutzer oder schadhafter Code den Schutz deaktivieren oder die Agentenkonfiguration manipulieren.

Die Leichtbauweise ermöglicht der Traps-Umgebung eine horizontale Skalierung und unterstützt große Bereitstellungen von bis zu 50.000 Agenten pro ESM während immer noch eine zentrale Konfiguration und Datenbank für das Regelwerk existiert. Traps Agents können mit den meisten großen Endpunkt-Sicherheitslösungen koexistieren. Dabei bleibt die CPU-Auslastung und I/O unglaublich niedrig. Diese nur minimalen Unterbrechungen macht Traps optimal für kritische Infrastrukturen, spezialisierte Systeme und VDI-Umgebungen.

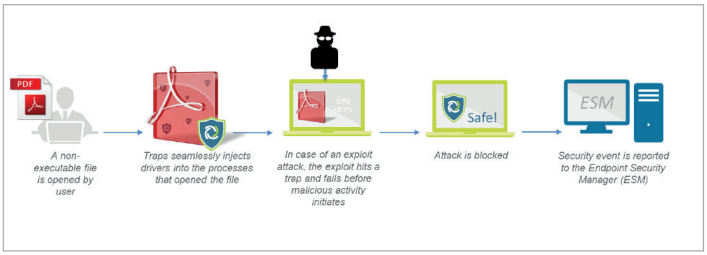

Abbildung 3: Funktionsweise des Endpoint Security Manager (Advanced Endpoint Protection)

Externe Protokollierung

Der ESM kann Protokolle zu einer externen Protokollierungsplattform wie zum Beispiel einem SIEM (Security Information & Event Management), Security Operation Center (SOC) oder Syslog, zusätzlich zur Speicherung Ihrer Protokolle intern schreiben. Für eine Organisation, die mehrere ESM einsetzt, ermöglicht eine externe Protokollierung eine aggregierte Sicht dieser Protokolldatenbanken.

Leistungen

Die Experten von iT-CUBE SYSTEMS planen die Installation von Palo Alto Netwotks Traps und führen diese durch. Die Lösung integrieren wir darüber hinaus in bereits bestehende SIEM (Security Information & Event Management) und Log Management-Systeme. Darüber hinaus kümmern wir uns stets um eine Erweiterung und Auditierung des Regelwerks.

iT-CUBE unterstützt Sie dabei, die Anforderungen an einem sicheren Zugang zum Internet in einem bestehenden IT-Security Konzept auf den neuesten Stand zu bringen und zu integrieren oder ein neues IT-Security Konzept zu erstellen.

Nutzen

Die iT-CUBE besitzt den Status des offiziellen **Palo Alto Networks Traps ASC (Authorized Support Center)** und die Auszeichnung **„NEXTWAVE TRAPS SPECIALIZED"**. Unsere Mitarbeiter sind zertifizierte **Palo Alto Networks Accredited Sales Experts** und **Certified Network Security Engineers**. Damit sind wir ein kompetenter Partner mit einem kompletten Leistungsspektrum von Planung, PoC/PoV, Realisierung, Implementierung bis hin zur Wartung und dem Support der Palo Alto Networks NGFW sowie den dazugehörigen Endpoint-Security-Lösungen.

Die Experten der iT-CUBE haben bereits viele Projekte mit unterschiedlichsten Produkten erfolgreich umgesetzt. Wir nutzen diese jahrelange Erfahrung, um Palo Alto Networks Traps perfekt in Ihre bestehende Infrastruktur zu integrieren. Dank des engen Kontakts mit dem Hersteller können technische sowie organisatorische Probleme schnell und reibungslos gelöst werden. Schon kurz nachdem Palo Alto Networks den europäischen Markt betrat, starteten wir bereits mit gemeinsamen Projekten durch.

Um Sie besser auf Sicherheitsvorfälle und den Umgang mit der Lösung zu schulen, bietet iT-CUBE speziell auf Ihre Bedürfnisse zugeschnittene Workshops für Ihre Mitarbeiter an.

paloalto NETWORKS ASC

paloalto NETWORKS NEXTWAVE TRAPS SPECIALIZED

pcnse 6 PALO ALTO NETWORKS CERTIFIED NETWORK SECURITY ENGINEER

Beispiel

Ein größeres Unternehmen verkündet einen Personalabbau. Daraufhin bekommt ein Mitarbeiter eine E-Mail von einem vermeintlichen Kollegen mit dem Betreff „geplante Personalabbauliste" und einer angehängten Excel-Datei. Im Text steht noch „Schau mal was ich zufällig bekommen habe, zum Glück stehe ich nicht drauf". Der Mitarbeiter wird nun mit sehr großer Wahrscheinlichkeit diese Datei öffnen und führt dabei eine Malware mit aus, die auf einer noch nicht bekannten Schwachstelle in Excel beruht. Ohne Traps würde diese jetzt komplett ausgeführt werden, eventuell stürzt Excel dabei ab und der Mitarbeiter schickt die Liste an seine Kollegen, damit die mal schauen können, ob sie die Datei öffnen können.

Mit Traps wird nun die Ausführung des Exploits unterbunden und der Mitarbeiter informiert. Der Rechner ist weiterhin nicht kompromittiert. Gleichzeitig wird diese Datei an Palo Alto Networks Wildfire zur genaueren Analyse weitergeleitet und die Wildfire-Datenbank um den Hashwert erweitert. Durch die automatische Verteilung der neuen Signatur wird beim nächsten Mal die Datei auf jeden Traps-Agent automatisch geblockt und die Kommunikation an der NGFW zusätzlich unterbunden. Wird diese Information nun mit einem SIEM geteilt, kann dieses zusätzliche Aktionen wie den Antivirus-Schutz des Mail-Servers ansteuern, ausführen und eine Bereinigung von E-Mails mit gleichem Anhang veranlassen. Ebenso ist es möglich, verschiedene Logs von Geräten zu korrelieren und so dem Administrator eine Übersicht zu verschaffen, auf welchen Geräten die Datei ausgeführt wurde. Anschließend kann hier genauer untersucht werden, ob es weitere Schad-Codes gibt. Die Mitarbeiter können anschließend im Umgang mit unbekannten Anhängen geschult werden.

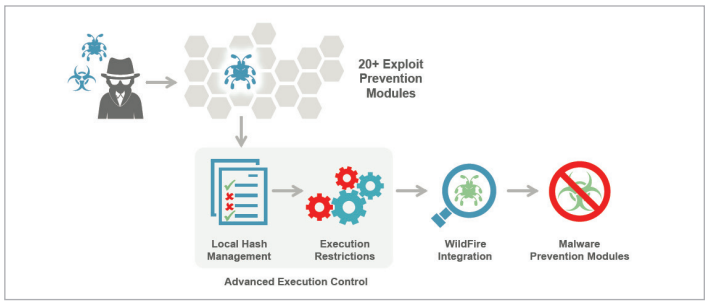

Abbildung 4: Advanced Execution Control

iT-CUBE SYSTEMS AG

Paul-Gerhardt-Allee 24
81245 München, Germany

T: +49 89 2000 148 00
F: +49 89 2000 148 29

info@it-cube.de
www.it-cube.de