ICS Managed Traps

Im letzten Jahr wurden über 142 Millionen neue Malware-Programme kreiert. Das sind über 390.000 Malware-Varianten am Tag. Zusätzlich gibt es täglich 25 neue Schwachstellen in Programmen. Ist der klassische Antivirenschutz vor bekannten Bedrohungen der richtige Ansatz?

Changing the game

Trotz der enormen Produktvielfalt für Endpoint Security werden Endpoints nach wie vor erschreckend häufig infiziert. Die gewöhnlichen Schutzmethoden für Endpoints können mit der schnellen Entwicklung der Bedrohungslage kaum mithalten. Daher bieten wir Ihnen mit unserem Partnerunternehmen Palo Alto Networks einen einzigartigen Ansatz zum Thema Endpoint Security an. Traps wurde dazu entwickelt Endpoints vollständig zu schützen, inklusive der Abwehr von bekannten, sowie hochentwickelten und neuartigen Angriffen, vor denen herkömmliche Lösungen keinen Schutz bieten können.

Umfassender Schutz für verschiedene Angriffsarten

Angriffe erfolgen auf unterschiedliche Art und Weise, beispielsweise über Webseiten, E-Mail und externe Speicher. Die meisten herkömmlichen Sicherheitsprodukte für Endpoints schützen Sie an dieser Stelle vor schädlichen, ausführbaren Dateien (Malware), welche die häufigste Form von Angriffen darstellen. Aber wie schützen Sie sich vor der Ausnutzung von Schwachstellen (Exploits)? Traps sichert Sie mit seiner einzigartigen Kombination von Malware und Exploit Schutzmethoden sowohl vor bekannten als auch unbekannten Bedrohungen.

Indem sich Traps auf die Kerntechniken zur Ausnutzung von Schwachstellen konzentriert, kann ein Angriff abgewehrt werden, ohne Millionen von Schwachstellen oder das explizite Verhalten einzelner Exploits vorher zu kennen. Dabei ist es egal, ob entsprechende Patches, Signaturen oder Software-Updates vorhanden sind, da sich Traps nahtlos in jeden Anwendungsprozess integriert. Durch das Erkennen dieser Kerntechniken ist Traps in der Lage, den Angriff sofort abzuwehren, bevor irgendeine schädliche Aktivität erfolgreich ausgeführt werden kann.

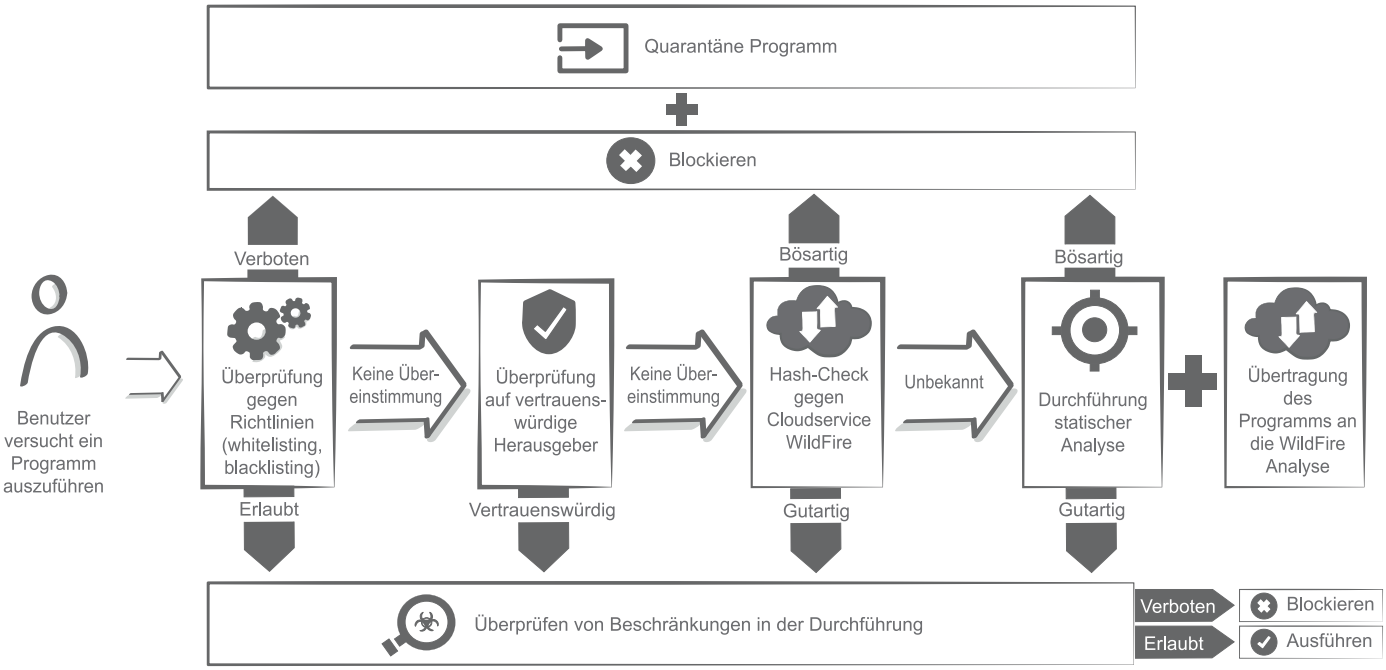
Next-Generation Endpoint Security

Traps bietet zusätzlich zu dem Exploit Modul ein umfangreiches Malware Prevention Module an, welches als weitere Technologie zur effektiven Bedrohungsabwehr dient. Hierzu zählt unter anderem das Erstellen von Richtlinien. So kann beispielsweise das Starten von ausführbaren Dateien aus lokalen Ordnern, Netzwerkpfaden oder von Wechselmedien verhindert werden. Weiterhin kann über entsprechende Richtlinien ein Application Whitelisting durchgeführt werden. Darüber hinaus gehört neben der Analyse von unbekannten Dateien durch den Cloudservice WildFire ebenfalls die statische Analyse. Dieses Modul wertet ausführbare Dateien aufgrund von vielen verschiedenen Eigenschaften aus, auch wenn Sie Offline sind. Mit diesen Maßnahmen können Sie den Angriffsvektor deutlich reduzieren.

Wir bieten Ihnen die Lösung als ICS Managed Traps an. Die Bereitstellung des Dienstes erfolgt aus dem Datacenter. Dies beinhaltet die Pflege der Plattform sowie das regelmäßige Einspielen von Updates und Patches. Des Weiteren werden die hoch skalierbaren, ressourcenschonenden Agenten für verschiedene Betriebssysteme bereitgestellt.

First- and Second-Level-Support

Als Mitglied der DTS-Gruppe übernehmen wir für Palo Alto Networks den First- and Second-Level-Support in Form eines 5x9 Next Business Day Telefon Supports. Sie profitieren bei allen Anliegen von der Unterstützung unserer Fachexperten über unseren Helpdesk. Auf Wunsch stellen wir Ihnen auch einen 7x24 Telefon Support zur Verfügung.



Traps bietet Ihnen eine einzigartige sowie leistungsfähige Lösung zum Schutz von Endpoints vor praktisch allen zielgerichteten Angriffen.

Traps geht den Schutz vor Malware und Exploits im Hinblick auf die Architektur komplett anders als herkömmliche Ansätze zur Abwehr von Schadsoftware an. Dies ist ein enormer Vorteil für die Skalierbarkeit, da die CPU-Auslastung und der Speicherplatzbedarf extrem gering sind.

Eine wesentliche Stärke von Traps ist die nahtlose Integration in die Next Generation Security Plattform von Palo Alto Networks. Angriffsversuche werden beispielsweise am Endpoint erkannt und über die Threat Intelligence Cloud an die Firewall Gateways weitergegeben, um für vollständige Transparenz und Kontrolle bei der Erkennung und Verhinderung von Angriffen sowie Bedrohungen zu sorgen.

ICS Managed Traps

Traps setzt sich aus den Endpoint Agenten und dem Endpoint Security Manager (ESM) zusammen. Letzterer bildet das Zentrum einer Traps Infrastruktur. Der ESM ist für das Logging und die Datenabfrage sowie für die forensischen Daten verantwortlich. Darüber hinaus befindet sich hier das administrative Dashboard.

Traps bietet folgende Vorteile:

- Schutz vor Exploits, einschließlich solcher, die unbekannte Zero-Day-Sicherheitslücken ausnutzen
- Schutz auch vor bisher unbekannter Malware
- Detaillierte forensische Daten zu verhinderten Angriffen
- Integration in die Netzwerk- und Cloud-Security Lösungen von Palo Alto Networks
- Auch ohne Palo Alto Networks Firewall einsetzbar
- Hohe Skalierbarkeit, einfacher Aufbau, nahtlose Integration und intuitive Bedienung
- Schutz für nicht mehr supportete Betriebssysteme (z.B. Windows XP, Windows Server 2003)
- Ressourcenschonende Agenten (ca. 0,1% CPU/ 50 MB RAM)

ICSmedia GmbH Soester Straße 13 48155 Münster +49 251 / 60 60 0 www.icsmedia.de