TRAPS

Advanced Endpoint Protection

Palo Alto Networks Traps ersetzt herkömmliche Antivirensoftware durch multimethodischen Schutz. Diese proprietäre Kombination aus speziell entwickelten Methoden zur Abwehr vor Malware und Exploits schützt Benutzer und Endpunkte vor bekannten und unbekannten Bedrohungen. Mit Traps werden Sicherheitsverletzungen von vorne herein vermieden und nicht erst erkannt und behoben, nachdem bereits wichtige Ressourcen beschädigt wurden.

Vorteile von Traps Advanced Endpoint Protection:

- **Verhindert Cyberangriffe** durch die vorbeugende Blockade bekannter und unbekannter Malware, Exploits und Zero-Day-Bedrohungen.
- **Schützt und befähigt Benutzer**, ihre täglichen Aktivitäten unter Verwendung webbasierter Technologien auszuführen, ohne sich Gedanken um bekannte oder unbekannte Cyberbedrohungen machen zu müssen.
- **Automatisiert den Schutz**, indem sich die Anwendung anhand der von WildFire bezogenen Threat Intelligence selbstständig umprogrammiert.

Die meisten Unternehmen schützen ihre Endpunktsysteme mit einer Mischung aus Sicherheitslösungen, die meist eine oder mehrere herkömmliche Antivirenlösungen beinhalten. Angreifer sind heute durch die Verbreitung kostenloser bzw. kostengünstiger Tools in der Lage, neue und einzigartige Angriffe zu starten, bei denen die signaturbasierte Antivirensoftware umgangen wird. Derzeit auf dem Markt verfügbare Endpunkt-Sicherheitslösungen und Antivirensoftware bieten Benutzern und Systemen keinerlei Schutz vor ausweichenden, unbekannten oder Zero-Day-Angriffsmethoden.

Traps™ Advanced Endpoint Protection von Palo Alto Networks® bietet eine einzigartige Kombination aus speziell zum Schutz vor Malware und Exploits entwickelten Methoden. Diese verhindern bekannte und unbekannte Bedrohungen, bevor sie einen Endpunkt beschädigen können.

Multimethodischer Malware-Schutz durch Traps

Traps wehrt schadhafte ausführbare Dateien mit einem einzigartigen multimethodischen Schutzansatz ab, der für maximalen Schutz vor Malware sorgt. Dadurch reduziert sich auch die Angriffsoberfläche, und die Genauigkeit der Malware-Erkennung steigt. Dieser Ansatz vereint mehrere Schutzmethoden, um die Infektion eines Systems durch bekannte und unbekannte Malware unmittelbar zu verhindern (Abbildung 1).

Abbildung 1: Multimethodischer Malware-Schutz durch Traps

1. **Statische Analysen durch maschinelles Lernen:** Diese Methode liefert sofort ein Verdikt zu sämtlichen unbekannten ausführbaren Dateien, bevor deren Ausführung gestattet wird. Traps untersucht im Bruchteil einer Sekunde Hunderte von Dateieigenschaften, ohne sich rein auf Signaturen, Scans oder Verhaltensanalysen zu verlassen.
2. **WildFire-Inspektion und -Analyse:** Diese Methode nutzt die Fähigkeiten der cloudbasierten Malware-Analyseumgebung WildFire™ von Palo Alto Networks, um unbekannte Malware schnell zu erkennen. Traps wird daraufhin automatisch umprogrammiert, um die nun bekannte Malware abzuwehren. WildFire eliminiert unbekannte Bedrohungen, indem es diese innerhalb von etwa 300 Sekunden in bekannte Bedrohungen umwandelt.
3. **Ausführungsbeschränkungen auf vertrauenswürdige Anbieter:** Mit dieser Methode können Unternehmen ausführbare Dateien identifizieren, die sich unter den „unbekannten guten" Dateien befinden, da sie von vertrauenswürdigen Anbietern veröffentlicht und digital signiert wurden. Dabei handelt es sich um Anbieter, die Palo Alto Networks als seriöse Softwareanbieter einstuft.
4. **Richtlinienbasierte Ausführungsbeschränkungen:** Unternehmen können auf einfache Weise Richtlinien definieren, um bestimmte Ausführungsszenarien einzuschränken. Sie reduzieren dadurch die Angriffsoberfläche einer Umgebung. Traps kann beispielsweise verhindern, dass Dateien aus dem Temp-Verzeichnis von Outlook® oder mit einem bestimmten Dateityp von einem USB-Stick ausgeführt werden.
5. **Verwaltungsrichtlinien zur Außerkraftsetzung:** Mit dieser Methode können Unternehmen anhand des Hash-Werts einer ausführbaren Datei Richtlinien definieren um zu steuern, was in einer Umgebung ausgeführt werden darf. Diese detaillierte Positiv- und Negativlistenfunktion steuert die Ausführung sämtlicher Dateien anhand von benutzerdefinierten Bedingungen, die sich auf alle Objekte anwenden lassen, die mit Microsoft® Active Directory® definiert werden können.

Jegliche als schädlich erachtete ausführbare Datei, deren Ausführung auf dem Endpunkt verhindert wird, kommt in einem geschützten, nur für Systemadministratoren zugänglichen Depot in Quarantäne. Traps-Administratoren können in Quarantäne gestellte Dateien überprüfen, und je nach Bedarf löschen oder an ihrem ursprünglichen Speicherort auf dem jeweiligen Endpunkt wiederherstellen.

Multimethodischer Exploit-Schutz durch Traps

Traps verwendet einen völlig neuen Ansatz des Exploit-Schutzes. Anstatt sich auf die Millionen von individuellen Angriffen oder deren zugrundeliegenden Sicherheitslücken zu konzentrieren, fokussiert sich Traps auf die Kerntechniken von Exploits, die bei allen derartigen Angriffen genutzt werden. Um eine Anwendung erfolgreich zu untergraben, muss ein Exploit stets eine Reihe dieser Exploit-Techniken verwenden. Traps macht diese Techniken unwirksam, indem es ihre Anwendung von Beginn an blockiert. Unternehmen, die Traps einsetzen, können beliebige Anwendungen ausführen – einschließlich intern entwickelter oder solcher, die keinen Sicherheitssupport mehr erhalten – ohne ihre Umgebung zu gefährden.

Traps implementiert einen multimethodischen Ansatz für den Exploit-Schutz. Dabei werden mehrere Schutzschichten kombiniert, um Exploit-Techniken zu blockieren (Abbildung 2):

Abbildung 2: Multimethodischer Malware-Schutz durch Traps

1. **Schutz vor Speicherfehlern:** Traps wehrt Exploit-Techniken ab, die reguläre Speicherverwaltungsmechanismen für die Anwendung manipulieren, die zum Öffnen der schädlichen Datei mit dem Exploit dient.
2. **Schutz vor Logikfehlern:** Traps erkennt und blockiert die Exploit-Techniken, die es einem Exploit ermöglichen, die regulären Anwendungsprozesse und Ausführungsmechanismen des Betriebssystems zu manipulieren.
3. **Schutz vor der Ausführung von Schadcode:** Exploits dienen meist dem Ziel, die in die Exploit-Datei eingebetteten Befehle des Angreifers auszuführen. Diese Schutzmethode erkennt die Exploit-Techniken, mit denen Schadcode von Angreifern ausgeführt werden kann, und blockiert diese, noch bevor sie wirksam werden.

Sicherheitsplattform der nächsten Generation

Infolge der beständig sinkenden Kosten für Rechenleistung können Angreifer leichter den je immer zahlreichere und raffiniertere Angriffe starten. Unzusammenhängende Sicherheitsschichten und Punktlösungen, die auf veralteten Technologien basieren oder Eingriffe von Benutzern erfordern (nachdem diese benachrichtigt wurden) reichen nicht mehr aus, um den heutigen Umfang an Bedrohungen zu bewältigen. Sicherer Schutz vor fortschrittlichen, gezielten und ausweichenden Angriffen ist nur mit einer Plattform möglich, die mehrere vorbeugende Technologien konsolidiert, automatisiert und nativ integriert.

Die native Integration von Traps in die Sicherheitsplattform der nächsten Generation von Palo Alto Networks ermöglicht es Unternehmen, die wachsende, von Tausenden Unternehmenskunden erfasste Threat Intelligence kontinuierlich an Netzwerke und Endpunkte weiterzuleiten, um vorbeugende und reaktive Maßnahmen zu koordinieren. Die automatische Umprogrammierung und Konvertierung von Threat Intelligence in Schutzmaßnahmen entzieht Angreifern die Grundlage, um ein System mit unbekannter und fortschrittlicher Malware zu infizieren. Ein Angreifer kann jede Art von Malware weltweit maximal einmal verwenden, und es bleiben ihm nur wenige Sekunden für einen Angriff, bevor dieser von WildFire unwirksam gemacht wird.

Systemanforderungen und Plattformunterstützung

Traps schützt ungepatchte Systeme auf beliebigen Plattformen, auf denen Windows® ausgeführt wird: Desktops, Server, Industriesteuerungssysteme (Industrial Control Systems, ICS), Komponenten virtueller Desktop-Infrastrukturen (VDI), virtuelle Maschinen und eingebettete Systeme (Abbildung 3).

Betriebssysteme	
Windows XP (32-bit, SP3 oder höher) Windows Vista (32-bit, 64-bit, SP1 oder höher; FIPS-Modus) Windows 7 (32-bit, 64-bit, RTM und SP1; FIPS-Modus; alle Ausgaben, außer Home) Windows Embedded 7 (Standard und POSReady) Windows 8 (32-bit und 64-bit) Windows 8.1 (32-bit, 64-bit; FIPS-Modus) Windows Embedded 8.1 Pro Windows 10 Pro (32-bit und 64-bit) Windows 10 Enterprise LTSB Windows Server 2003 (32-bit, SP2 oder höher) Windows Server 2003 R2 (32-bit, SP2 oder höher) Windows Server 2008 (32-bit, 64-bit; FIPS-Modus) Windows Server 2008 R2 (32-bit, 64-bit; FIPS-Modus) Windows Server 2012 (alle Ausgaben; FIPS-Modus) Windows Server 2012 R2 (alle Ausgaben; FIPS-Modus)	
Virtuelle Umgebungen	
VMware ESX Citrix XenServer	Oracle Virtualbox Microsoft Hyper-V
Virtuelle Desktop-Infrastruktur	
VMware Horizon View	Citrix XenDesktop
Physische Plattformen	
SCADA Windows Tablets	ATM POS
Laufzeit-Speicherbedarf	
0,1 % CPU-Auslastung 50 MB RAM	250 MB Festplattenspeicher

Abbildung 3: Traps-Systemanforderungen und -Plattformunterstützung

4401 Great America Parkway
Santa Clara, CA 95054

Zentrale: +1/408/75 34 000
Vertrieb: +1/866/320/4788
Support: +1/866/89 89 087

www.paloaltonetworks.com

pan-traps-ds-071416