Progressiver Schutz für Endgeräte

Wirksame Abwehr bekannter und unbekannter Angriffe

Bestehende Anti-Malware-Lösungen sind mit ihrem reaktiven Verhalten nicht in der Lage, unbekannten Schadcode bei Endgeräten zu erkennen und das Einschleusen von Malware zu verhindern. TRAPS, die Advanced-Endpoint-Protection-Lösung von Palo Alto Networks, schafft Abhilfe.

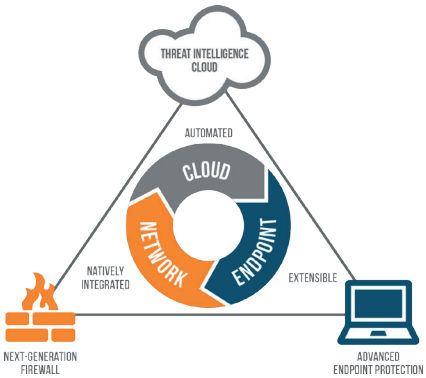
Hochentwickelte Cyberangriffe, «Modern Malware», Exploits, Zero-Day-Attacken, Ransomware … Endgeräte sind zahlreichen Gefahren ausgesetzt. Doch bisherige Anti-Malware-Lösungen sind trotz zeitnaher Signatur-Updates nicht in der Lage, unbekannten Schadcode zu erkennen und das Einschleusen von Malware zu verhindern.

Um Sicherheitslücken bei Endgeräten zu schliessen und unbekannte Angriffe wirksam abzuwehren, hat Palo Alto Networks die wegweisende Endpoint-Security-Software TRAPS lanciert (Targeted Remote Attack Prevention System). Sie steht bei vielen Schweizer Unternehmen bereits erfolgreich im Einsatz, etwa im Finanzsektor, in der Industrie und im Gesundheitswesen.

Die hochwirksame, ressourcenschonende Lösung erkennt bekannte und unbekannte Angriffe, ohne sich dabei klassischer Signatur-Erkennungsmethoden oder Verhaltensanalysen zu bedienen. Vielmehr erkennt TRAPS Techniken zur Ausnutzung von Schwachstellen und schützt so auch vor der Ausführung intelligentester Malware.

Abwehr von Exploits

TRAPS nutzt die Tatsache, dass ein Hacker für einen erfolgreichen Angriff eine Reihe von bekannten Exploit-Techniken ausführen muss. TRAPS identifiziert diese Techniken und wehrt Angriffe umgehend ab – ohne Kenntnisse über Schwachstellen, unabhängig von Patches, losgelöst von Signaturen. TRAPS ist effizient einzubinden und benötigt sehr wenig Systemressourcen. Erfolgt ein Angriff, erkennt TRAPS die verwendeten Techniken, blockiert die Attacke, beendet den Prozess und informiert Benutzer und Administrator über den Vorfall. Zusätzlich sammelt TRAPS detaillierte Forensikdaten und übermittelt diese an den Endpoint-Security-Manager.



TRAPS ist Bestandteil der Palo-Alto-Next-Generation-Security-Plattform und revolutioniert die Abwehr bekannter und unbekannter Angriffe.

Schutz vor Malware

Um auch unbekannte Malware-Angriffe zu vereiteln und so einen wirksamen Rundum-Schutz der Endgeräte zu gewährleisten, nutzt TRAPS die Intelligenz der WildFire-Cloud und der gesamten Palo-Alto-Networks-Plattform. In der neuen Version 3.4 stehen dafür fünf zusätzliche Methoden zur Verfügung:

- Static Analysis untersucht ausführbare Dateien noch vor der Ausführung, indem hunderte von Charakteristiken analysiert werden. Dazu kommt ein Machine-Learning-Modell auf Basis der WildFire-Intelligenz zum Einsatz. Diese Methode ist besonders effektiv bei unbekannter Malware und in Umgebungen, wo Workstations nicht am Netzwerk angeschlossen sind.
- Execution Restrictions ermöglichen Regeln, basierend auf allen Objekten in einem Active Directory, seien es Benutzer- oder Maschineninformationen.
- Trusted Publisher Identification identifiziert ohne Verzögerung digital signierte Dateien, die von einem vertrauenswürdigen Softwareanbieter stammen. Eine neue Version von Outlook.exe, die von Microsoft signiert ist, gilt zum Beispiel als gutartig.
- Admin Override Policies ermöglichen black- oder whitelisting, hilfreich etwa für den Umgang mit selbst entwickelten Programmen.
- Neu ist auch eine Quarantäne verfügbar. Dorthin wird erkannte Malware verschoben, damit diese nicht weiter verteilt wird und dort Schaden anrichten kann, wo TRAPS nicht installiert ist.

Mit den neuen Funktionen ergänzt Palo Alto die bewährte Advanced-Endpoint-Protection-Lösung TRAPS um weitere wirksame Methoden. Moderne Angriffe auf Geräte und Daten werden so noch effektiver verhindert.

TRAPS: DIE HIGHLIGHTS

TRAPS, die revolutionäre ATP-Lösung (Advanced Threat Prevention) von Palo Alto Networks

- verhindert Exploits für sämtliche Schwachstellen
- wehrt malwarebasierte Angriffe ab
- liefert umgehend Forensikdaten über abgewehrte Angriffe
- ist frei skalierbar
- überzeugt durch seine Benutzerfreundlichkeit
- besticht durch einen äusserst niedrigen Ressourcenverbrauch (ca. 25 MB Memory, 0,1 % CPU)

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen

Tel. 056 437 60 60
info@boll.ch
www.boll.ch