Progressiver Schutz für Endgeräte

Wirksame Abwehr bekannter und unbekannter Angriffe

Bestehende Antiviren-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 … Endgeräte wie PCs, Notebooks, Tablets und Smartphones sind zahlreichen Gefahren ausgesetzt. Doch bisherige Endpoint-Security- beziehungsweise Antiviren-Lösungen sind trotz zeitnaher Signatur-Updates nicht in der Lage, unbekannten Schadcode zu erkennen und das Einschleusen von Malware in die Firmen-IT zu verhindern.

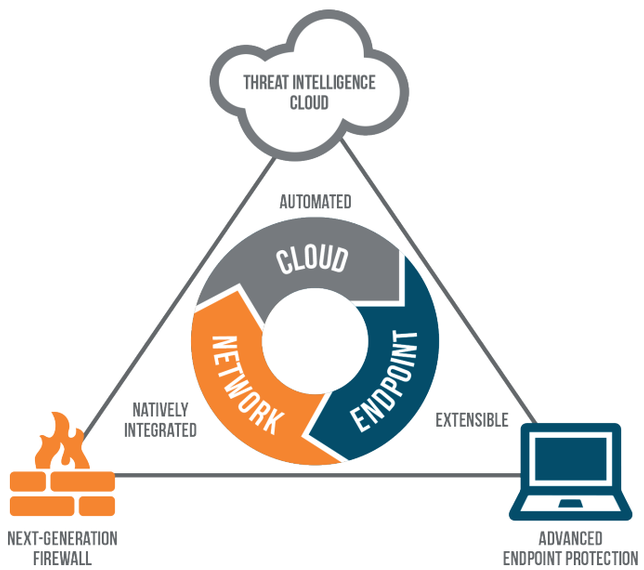
Um Sicherheitslücken bei Endgeräten zu schliessen und unbekannte Angriffe wirksam abzuwehren, hat Palo Alto Networks die wegweisende Endpoint-Security-Software TRAPS (Targeted Remote Attack Prevention System) lanciert. Diese hochwirksame, ressourcenschonende Plattform erkennt sowohl bekannte als auch unbekannte Angriffe, ohne sich dabei klassischer Signatur-Erkennungsmethoden oder Verhaltensanalysen zu bedienen. Vielmehr erkennt TRAPS Techniken zur Ausnutzung von Schwachstellen und schützt die Malware-Einfallstore mittels hocheffizienter Fallen (Traps).

Abwehr von Exploits

Bei der Abwehr von Exploits macht sich TRAPS die Tatsache zunutze, dass ein Hacker für einen erfolgreichen Angriff eine Reihe von Exploit-Techniken ausführen muss. TRAPS ist in der Lage, diese Angriffstechniken zu identifizieren und umgehend abzuwehren – ohne Kenntnisse über vorhandene Schwachstellen, unabhängig von Patches, losgelöst von notwendigen Signaturen oder Software-Updates. Die Einbindung von TRAPS ist effizient und ressourcenschonend. Wird ein neuer Benutzerprozess gestartet, klinken sich die Sicherheitsmodule automatisch ein, um gefährliche Manipulationen zu verhindern. Wird ein Angriff lanciert, erkennt TRAPS die verwendeten Techniken, blockiert die Attacke, beendet den entsprechenden Prozess und informiert User und Administrator über den Vorfall. Zusätzlich sammelt TRAPS detaillierte Forensikdaten und übermittelt diese umgehend an den jeweiligen Endpoint Security Manager.

Schutz vor Malware

Um auch unbekannte Malware-Angriffe zu vereiteln und so einen wirksamen Rund-um-Schutz der Endgeräte zu gewährleisten, unterstützt TRAPS zudem vorab definierte Richtlinien. Dank auf Policy basierenden Beschränkungen lässt sich beispielsweise steuern, über welche externe Medien und Verzeichnisse ausführbarer Code gestartet werden darf oder welche Prozesse eine Kopie von sich selbst erzeugen dürfen. Mithilfe weiterer von TRAPS unterstützter Mechanismen zur Abwehr von Malware lässt sich zudem verhindern, dass potenziell bösartiger Java-Code im Browser ausgeführt wird. Ferner besteht die Möglichkeit, «Speicherkorruption» zu erkennen und den Austausch von schadcodebehafteten dynamischen Programmbibliotheken (DLL Hijacking) sowie Code-Injektionen zu unterbinden.



Die Endpoint-Security-Software TRAPS ist integraler Teil der «Next Generation Security Platform» von Palo Alto Networks.

Leistungsmerkmale – ein Auszug

TRAPS, das «Targeted Remote Attack Prevention System» von Palo Alto Networks, darf als revolutionärste ATP-Lösung (Advanced Threat Prevention) bezeichnet werden. Es

- verhindert Exploits für sämtliche Schwachstellen,
- wehrt malwarebasierte Angriffe ab,
- liefert umgehend Forensikdaten über abgewehrte Angriffe,
- ermöglicht eine nahtlose Einbindung in bestehende Netzwerk- und Cloud-Security-Infrastrukturen,
- ist frei skalierbar,
- überzeugt durch seine Benutzerfreundlichkeit und
- 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