Progressive Endpoint-Security

Klassische Antiviren-Lösungen sind mit ihrem reaktiven Verhalten trotz täglich mehrfacher Signatur-Updates nicht in der Lage, unbekannten Schadcode zu erkennen und das Einschleusen von Malware zu verhindern. Die Zeit ist reif für einen neuen Ansatz: «Next Generation Endpoint Protection». Autor: Patrick Michel

DER AUTOR

Patrick Michel
Sicherheitsexperte und Product Manager bei Boll Engineering, Wettingen

Ob «Modern Malware», hochentwickelte Cyberangriffe oder Zero-Day-Attacken: Endgeräte wie PCs, Notebooks, Smartphones und Tablets sind einer stark wachsenden Zahl an Gefahren ausgesetzt und bilden beim Einschleusen von Schadcode ins Firmennetz oft ein ungeschütztes Einfallstor – dies trotz installierter und kontinuierlich aktualisierter Antiviren-Software. Vor diesem Hintergrund sind neue Ansätze nötig, um Sicherheitslücken bei Endgeräten zu schliessen und Angriffe wirksam abzuwehren.

Diese Erkenntnis hat einen führenden AV-Anbieter zur Aussage bewogen: «Antivirus is dead.» Dieses Statement mag zwar etwas gar radikal erscheinen, trifft jedoch den wunden Punkt bisheriger Antiviren-Lösungen. Diese sind mit ihrem reaktiven Verhalten trotz täglich mehrfacher Signatur-Updates nicht in der Lage, unbekannten Schadcode zu erkennen und das Einschleusen von Malware in die Firmen-IT zu verhindern, beziehungsweise Endpunkte zu schützen. Sie benötigen «Vorkenntnisse» über jegliche Bedrohungen, um diese zu verhindern. Folglich sind beispielsweise gezielte Attacken oder sogenannte Zero-Day-Exploits – Attacken, die noch unbekannt sind und für deren Erkennen und Abwehr noch keine Signaturen zur Verfügung stehen – durch klassische AV-Lösungen schlicht nicht zu erkennen, beziehungsweise abzuwehren.

Um diesen Schwachstellen zu begegnen, sind neue Mechanismen erforderlich, die sich weder klassischer Signatur-Erkennungsmethoden noch Verhaltensanalysen bedienen. Sie müssen vielmehr in der Lage sein, Techniken zur Ausnutzung von Schwachstellen zu erkennen. Entsprechende Lösungen wie etwa die «Advanced Endpoint Protection»-Plattform TRAPS (Targeted Remote Attack Prevention System) von Palo Alto Networks setzen exakt an diesem Punkt an. Sie sorgen dafür, dass Gefahren nicht nur reaktiv begegnet werden kann, sondern dass unbekannte Malware, intelligente Angriffe und Zero-Day-Exploits erkannt und gestoppt werden, bevor sie Schaden anrichten.

In die Falle gelockt

Lösungen wie TRAPS locken Angreifer in eine Falle. Wird ein neuer Benutzerprozess gestartet, klinken sich Sicherheitsmodule ein – dies mit dem Ziel, gefährliche Manipulationen zu erkennen und abzuwehren. Bei einem Exploit-Versuch beispielsweise blockt die «Falle» den Angriff und informiert User und Administrator über den Zugriff.

Um unbekannte Malware-Angriffe und Schwachstellen-Exploits progressiv zu vereiteln und so einen wirksamen Schutz der Endgeräte zu gewährleisten, bedienen sich «Advanced Endpoint Protection»-Plattformen vorab definierter Richtlinien. Dadurch lässt sich beispielsweise 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. Mithilfe von Richtlinien lässt sich zudem steuern, über welche externe Medien und Verzeichnisse ausführbarer Code gestartet werden darf und welche Prozesse eine Kopie von sich selbst erzeugen dürfen.

Damit die Abwehr unbekannter Malware und Exploits auch in grossen und verteilten Unternehmen wirksam erfolgen kann, sollten Lösungen, die eine progressive Endpoint-Security ermöglichen, enterprisetauglich sein und ein zentrales und umfassendes Management bieten. Von Bedeutung ist ferner, dass die eingesetzte Plattform keine oder eine ausgesprochen geringe False-Positive-Rate aufweist, beziehungsweise ausschliesslich schlechten Code blockiert und unkritische Daten passieren lässt.

Plattformen der beschriebenen Art sind drauf und dran, die Endpoint Security auf eine neue Basis zu stellen. Angesichts der zunehmenden Intelligenz und Zerstörungskraft moderner Malware eine dringende Notwendigkeit.

Bild: Fotolia