Palo Alto Networks

Besserer Schutz vor Cyber-Angriffen

[05.09.2016] Schwachstellen auf Endpoints in Behörden waren oft der Grund für erfolgreiche Cyber-Angriffe. Antivirus-Lösungen sind an dieser Stelle unwirksam. Das Unternehmen Palo Alto Networks empfiehlt stattdessen intelligente Lösungen, die Malware frühzeitig erkennen.

Bei den jüngsten größeren Cyber-Angriffen auf Behörden waren stets bestimmte Konstanten gegeben, wie das Unternehmen Palo Alto Networks aufzeigt: Es gab
Schwachstellen im Betriebssystem oder in einer Anwendung auf dem Endpunkt und es wurde versäumt, die neuesten Patches aufzuspielen. Die Angreifer konnten sich so die Schwachstellen auf dem Endpunkt zunutze machen, um ungehinderten Netzwerkzugang zu erhalten. Antivirus?Lösungen auf den Endpunkten haben sich laut dem Unternehmen für den Schutz vor heutigen Sicherheitsbedrohungen als unwirksam erwiesen. Eine empfehlenswerte Gegenmaßnahme sei daher zunächst das regelmäßige Patchen, um Sicherheitslücken zu schließen. Ebenfalls sollte eine Schwachstellenanalyse durchgeführt werden. „Um Angriffe zu stoppen oder die seitliche Bewegung der Angreifer im Netzwerk zu verhindern, ist Netzwerksegmentierung wichtig“, erklärt Martin Zeitler, Senior Manager Systems Engineering bei Palo Alto Networks weitere Empfehlungen. „Eine moderne Next?Generation?Sicherheitsplattform liefert eine verbesserte Transparenz zur Netzwerknutzung. Zudem ist eine solche integrierte Sicherheitslösung den heutigen Bedrohungen besser gewachsen, als punktuelle Produkte, die separat und unkoordiniert agieren.“ Das Unternehmen empfiehlt außerdem eine intelligente Lösung wie Traps von Palo Alto Networks für Endpunkte, die Malware an deren Verhalten frühzeitig erkennt. Hierbei komme eine Kombination hocheffektiver Methoden zum Schutz der Endpunkte zum Einsatz: Eine statistische Analyse über maschinelles Lesen beurteile jede unbekannte Datei, bevor diese ausgeführt werden darf. Bösartige ausführbare Dateien werden in Quarantäne gestellt.

Sicherheitsmaßnahmen für Behörden

Um zu bestimmen, ob eine ausführbare Datei gutartig oder bösartig ist, arbeite der Endpunktschutz Traps von Palo Alto Networks mit einer Bedrohungsanalyse?Cloud zusammen. Sie könne eine unbekannte Bedrohung in etwa fünf Minuten in eine bekannte Bedrohung verwandeln. Eine Trusted?Publisher?Identifizierung ermögliche es Behörden, unbekannte gutartige Dateien, die als seriöse Software-Hersteller eingestuft worden sind, zu identifizieren. Auch eine regelbasierte Einschränkung der Ausführung sei eine Schutzmethode. Sie könne die Angriffsfläche jeder Umgebung reduzieren. Darüber hinaus sei die Definition von Richtlinien durch die Organisationen eine Schutzlösung. So lasse sich kontrollieren, was in einer Umgebung ausgeführt werden darf. Um Schad-Software vorzubeugen, umfasst das Produkt Traps laut dem Anbieter eine Prävention gegen Speicherbeschädigung oder ?manipulation, eine Logic?Flaw?Prävention und eine Prävention gegen die Ausführung eines bösartigen Codes. Auch ermögliche ein moderner Endpunktschutz, nicht?bösartige, aber anderweitig unerwünschte Software an der Ausführung zu hindern. Traps könne auch installiert werden, um Altsysteme vor Exploits sowie bekannten und unbekannten Sicherheitslücken zu schützen. Nicht zuletzt empfiehlt Palo Alto Networks, dass Sicherheitsteams und -produkte nicht in isolierten Strukturen agieren. Die Endgeräte? und Netzwerksicherheitsfunktionen sollten sich gegenseitig ergänzen und Informationen austauschen. Gleiches gelte für den globalen Austausch von Bedrohungsdaten in Sicherheitsallianzen sowie für die Interaktion mit Interessengemeinschaften oder staatlichen Stellen.

(ve)

Stichwörter: IT-Sicherheit, Palo Alto Networks, Traps