Automated Moving Target Defense (AMTD): Wegweisend für moderne IT-Sicherheit

Durch die sich verschärfenden Cyberbedrohungen haben Sicherheitsteams mit einer steigenden Anzahl von Warnmeldungen und Fehlalarmen zu kämpfen. Das beeinträchtigt die Sicherheitseffizienz und bindet viele Ressourcen. Automated Moving Target Defense (AMTD), ein neues Konzept, das von Gartner entwickelt und gefördert wird, soll diese Dynamik durchbrechen und für Abhilfe sorgen. Sicherheitsprodukte und -dienste, die AMTD-Technologien einsetzen, erhöhen die Hürden für Angreifer. Die kontrollierte Orchestrierung von Veränderungen in IT-Umgebungen unterbricht Angriffe aktiv und vereitelt Einbruchsversuche.

AMTD auf dem Endpoint
Sophos setzt AMTD-Technologien am Endpoint ein und stellt damit den Angreifern Barrieren auf, um die Bedrohungen automatisch abzufangen beziehungsweise zu eliminieren. Neben der Reduzierung der Bedrohungsoberfläche, der Verhaltensanalyse und dem Einsatz von Deep-Learning- beziehungsweise AI-Modellen verbessert AMTD die Anwendungssicherheit durch das Erstellen von bedrohungsagnostischen Barrieren für jeden Prozess. Das Resultat: Für Software wird es schwieriger Code auszuführen, der nicht originärer Teil der Anwendung ist. Damit wird insbesondere Malware an ihrer Ausführung gehindert. Zu AMTD-Schutztechnologien gehören:

1. **Adaptive Attack Protection (AAP)**
   Adaptive Attack Protection (AAP) erkennt die Anwesenheit eines aktiven Angreifers auf zwei Arten: Erstens durch die Verwendung gängiger Angriffs-Toolkits und zweitens durch Kombinationen aktiver bösartiger Verhaltensweisen, die auf das Anfangsstadium eines Angriffs hindeuten. Sobald ein aktiver Angriff auf einem Endpoint erkannt wird, aktiviert AAP vorübergehende Einschränkungen. Ein Beispiel ist die Verhinderung eines Neustarts im abgesicherten Modus, welche Angreifer beispielsweise nutzen, um die Erkennung zu umgehen.

2. **Randomisierung**
   Wenn beispielsweise eine Dynamic Link Library (DLL) einer Anwendung stets vorhersehbar an derselben Speicheradresse geladen wird, ist es für Angreifer einfacher, Schwachstellen auszunutzen. Zwar können Entwickler während der Kompilierung die Adressraum-Layout-Randomisierung (ASLR) aktivieren, wodurch die Adressen einmal pro Neustart randomisiert werden, doch kann jede Software von Drittanbietern, die keine ASLR enthält, diese Strategie untergraben. Sophos verbessert die Sicherheit von Anwendungen, indem es sicherstellt, dass jedes Modul bei jedem Start der Anwendung an einer zufälligen Speicheradresse geladen wird und damit die Komplexität eines möglichen Angriffs erhöht.

3. **Täuschung**
   Angreifer versuchen oft, ihren schädlichen Code durch Verschleierung vor Datei- und Speicherscannern zu verbergen. Allerdings muss die Verschleierung von bösartigem Code fallen, bevor er auf dem Computer ausgeführt werden kann. Dieser Prozess ist in der Regel auf bestimmte Betriebssystem-APIs angewiesen. Sophos platziert strategisch Täuschungselemente, die speicherbezogene APIs imitieren, die von Angreifern häufig zur Initialisierung und Ausführung ihres schädlichen Codes

verwendet werden. Diese bedrohungs- und code-agnostische Verteidigung kann schädlichen Code unterbrechen, ohne gutartige Anwendungen zu behindern.

4. **Begrenzung**
   Um Abwehrmaßnahmen zu umgehen, wird bösartiger Code in der Regel verschleiert und oft über gutartige Anwendungen transportiert. Vor der Ausführung eines verdeckten Codes muss die Bedrohung ihre Verschleierung aufheben, was zur Schaffung eines für die Ausführung von Code geeigneten Speicherbereichs führt und somit eine CPU-Hardwareanforderung darstellt. Die zugrundeliegenden Befehle, die zur Erstellung eines codefähigen Speicherbereichs erforderlich sind, sind derart kurz, dass sie allein nicht ausreichen, um von Schutztechnologien als bösartig eingestuft zu werden. Bei einer Blockierung solcher Befehle würden zwangsläufig auch gutartige Anwendungen nicht mehr funktionieren. Sophos Endpoint führt eine eindeutige Historie, verfolgt die Eigentümerschaft und korreliert Zuweisungen von codefähigem Speicher über Anwendungen hinweg. Dadurch sind neuartige Schutzmaßnahmen auf solch niedriger Ebene möglich und sinnvoll einsetzbar.

5. **Härtung**
   Sophos verhindert die Manipulation von Prozessen, indem es Barrieren um die sicherheitssensiblen Speicherbereiche jeder Anwendung errichtet. Beispiele für sensible Speicherbereiche sind der Process Environment Block (PEB) oder der Adressraum von sicherheitsrelevanten Modulen wie dem Anti-Malware Scan Interface (AMSI). Angreifer, die darauf abzielen, die Identität eines gutartigen Prozesses anzunehmen, verstecken Befehlszeilenparameter, deaktivieren oder führen beliebigen Code im eigenen (oder im Adressraum eines anderen Prozesses) aus und manipulieren regelmäßig Code oder Daten innerhalb dieser sensiblen Bereiche. Durch die Abschirmung dieser Prozesse werden generisch eine Vielzahl bestehender und zukünftiger Angriffstechniken beendet und entlarvt.

6. **Leitplanken**
   Sophos installiert sogenannte Guardrails (Leitplanken) um eine Code-Ausführung herum. Dadurch wird verhindert, dass die Code-Ausführung zwischen einzelnen Code-Abschnitten fließt und in einen Adressraum eindringt, der zwar Teil der ursprünglichen Anwendung ist, aber nur Daten enthalten soll. Außerdem werden aktiv APC-Injektion und die Nutzung verschiedener anderer Systemfunktionen verhindert, die nicht von legitimen Anwendungen verwendet werden.

„Wenn AMTD richtig eingesetzt wird, stellt es eine unschätzbare Verteidigungsschicht gegen Advanced Persistent Threats (APTs), auf Exploits basierende Angriffe und Ransomware dar“, so Michael Veit, Cybersecurity-Experte bei Sophos. „AMTD-Technologien auf dem Endpoint verbessern die Widerstandsfähigkeit aller Anwendungen automatisch, ohne dass eine Konfiguration, Quellcode-Änderung oder Kompatibilitätsprüfung erforderlich sind. Automatisierte und orchestrierte Cybersecurity-Strategien setzen die Messlatte für Angreifer höher, da sie die Unklarheiten für die Angreifer erhöht und Attacken damit zeitaufwendiger geplant werden müssen.“

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de