AKAMAI-LÖSUNGSÜBERBLICK

Spotlight zur Angriffserkennung mit mehreren Methoden: mit Segmentierungsrichtlinien Attacken auf Rechenzentren erkennen

Da es nicht danach aussieht, als würden Angriffe auf Rechenzentren zurückgehen, ist es an der Zeit, dass sich Sicherheitsteams stärker auf das Herzstück des Rechenzentrums konzentrieren – wo Anwendungen miteinander kommunizieren und unternehmenskritische Funktionen ausführen. Da immer mehr Unternehmen Rechenzentrums-Assets über mehrere virtualisierte Umgebungen verteilen, ist der klassische Schutz des Unternehmensnetzwerks vor außerhalb nicht mehr ausreichend. Sicherheitsadministratoren benötigen ein effizientes Mittel, um den internen East-West-Traffic vor Angriffen zu schützen, die bereits erfolgreich gegen die externe Abwehr verstoßen haben.

Firewalls stoßen an ihre Grenzen

Firewalls werden traditionell verwendet, um die Kommunikation zu schützen, die in Rechenzentren ein- und ausgeht. Allerdings ist es problematisch, Firewalls im Kern des Rechenzentrums einzusetzen. Da sie nicht in der Lage sind, sich an die enormen Mengen des East-West-Traffics anzupassen, werden sie zu einem Engpass für die Performance. Firewalls auf Serverebene verbrauchen große Mengen an Rechenressourcen vom Host, der ohnehin schon stark belastet ist. Außerdem müssen mehrere Lösungen bereitgestellt werden, die die verschiedenen Betriebssystemtypen und -marken im Rechenzentrum abdecken, was die Verwaltung zusätzlich erschwert.

Bis vor Kurzem war auch die Implementierung von Sicherheitsrichtlinien auf L7-Prozessebene eine Herausforderung. Grund dafür ist, dass Transparenz in allen Anwendungen und Prozessen erforderlich ist, die in Ihrer Umgebung kommunizieren. Darüber hinaus müssen Teams genau verstehen, wie Prozesse innerhalb der Anwendung und des Rechenzentrums zusammenarbeiten sollten. Ohne diese Erkenntnisse kann die Implementierung von Sicherheitsrichtlinien auf Prozessebene ein Risiko darstellen, und die Wahrscheinlichkeit, dass etwas beschädigt wird, ist enorm hoch.

Um kritische Assets im Rechenzentrum zu schützen und gleichzeitig die Angriffserkennung und -reaktion zu verbessern, benötigen Sicherheitsteams folgende Möglichkeiten:

- Echtzeit-Visualisierung aller Anwendungen und Prozesse, die in ihren Rechenzentren ausgeführt werden
- Implementierung detaillierter Sicherheitsrichtlinien, ohne kritische Prozesse zu behindern
- Erkennung nicht autorisierter Kommunikation, die auf einen Angriff hinweisen könnte

Angriff ist die beste Verteidigung: richtlinienbasierte Erkennung mit Akamai Guardicore Segmentation

Richtlinienbasierte Erkennung kann Sicherheitsteams dabei unterstützen, Bedrohungen schneller zu erkennen, zu bestätigen und einzudämmen, um Schäden zu vermeiden und Verluste zu minimieren. Diese präzisen Sicherheitskontrollen kämpfen an zwei Fronten: Sie verhindern, dass ein Angreifer Zugriff auf eine Anwendung oder einen Prozess erhält, und informieren gleichzeitig Administratoren über die Anwesenheit des Eindringlings.

Die Funktionen der Segmentierungsrichtlinien in Akamai Guardicore Segmentation ermöglichen Sicherheitsexperten Folgendes:

- Sie können eine umfassende visuelle Übersicht aller Anwendungen und Aktivitäten im Rechenzentrum erstellen, um sich einen Überblick über alle Workloads zu verschaffen und die Kommunikation auf Anwendungsebene genau zu untersuchen.

Durch die Kombination mehrerer Erkennungsmethoden lassen sich Angriffe schneller erkennen

Dynamische Täuschung

Eine Umleitungsarchitektur und dynamisch generierte Live-Umgebungen beschäftigen Angreifer und identifizieren ihre Methoden, ohne die Performance des Rechenzentrums zu beeinträchtigen.

Richtlinienbasierte Erkennung

Sicherheitsrichtlinien auf Layer-4-Netzwerk- und Layer-7-Prozessebenen ermöglichen die sofortige Erkennung nicht autorisierter Kommunikation und nicht konformen Traffics.

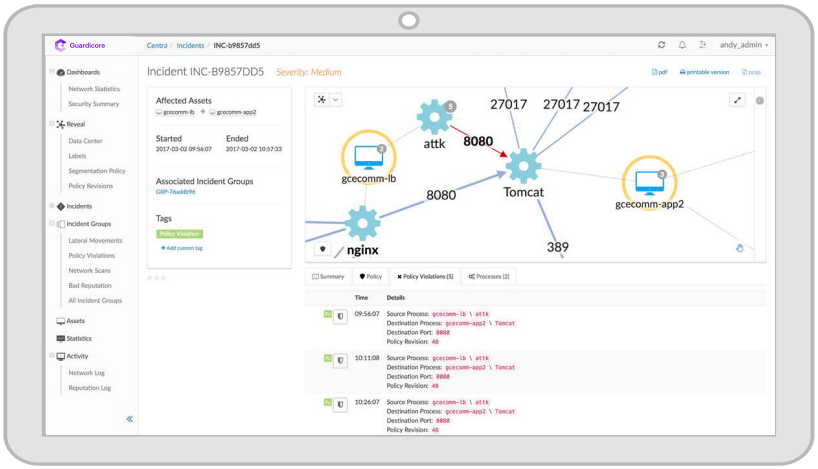
Reputationsanalyse

Erkennt verdächtige Domainnamen, IP-Adressen und Datei-Hashes im Traffic und ermöglicht so umfassende Angriffserkennung.

Akamai

- Sie können Anwendungen in Gruppen filtern und organisieren und sie benennen, um gemeinsame Sicherheitsrichtlinien festzulegen, z. B. alle Anwendungen, die sich auf einen bestimmten Workflow oder eine bestimmte Geschäftsfunktion beziehen.
- Sie können Regeln für die autorisierte Kommunikation zwischen Anwendungen definieren und erstellen.
- Sie können Regeln testen und optimieren, um zu gewährleisten, dass sie den normalen autorisierten Traffic nicht stören.

Jeder nicht konforme Traffic, jede nicht autorisierte Kommunikation und jeder andere Richtlinienverstoß löst automatisch eine Warnung aus, die darauf hinweist, dass ein Eindringling anwesend sein könnte. Hierdurch wird wiederum der Untersuchungsprozess eingeleitet, um die Bedrohung zu bestätigen und einzudämmen.



Akamai Guardicore Segmentation erkennt potenzielle Angriffe, indem es Verstöße gegen Segmentierungsrichtlinien erkennt, bei denen nicht autorisierte Prozesse versuchen, über autorisierte Ports zwischen zwei zulässigen Hosts zu kommunizieren. Wird etwas erkannt, werden entsprechende Warnmeldungen ausgegeben.

Treiben Sie Angreifer mit verschiedenen Erkennungsmethoden in die Ecke

Die richtlinienbasierte Erkennung ist nur eine von mehreren Methoden, die unsere Lösung verwendet, um die Echtzeit-Angriffserkennung und -reaktion zu verbessern. Diese beiden Methoden arbeiten Hand in Hand und umfassen außerdem Folgendes:

- **dynamische Täuschung**, bei der echte Server, IP-Adressen, Betriebssysteme und Dienste in Rechenzentren als Köder eingesetzt werden, die beim ersten Anzeichen verdächtiger Aktivitäten den Eindringling aufspüren, mit ihm in Kontakt treten und ihn zur Bestätigung und Untersuchung von Bedrohungen in einen Sicherheitsbereich umleiten
- **Reputationsanalyse**, die das globale Akamai-Netzwerk von Bedrohungssensoren und Intelligence-Feeds nutzt, um negative Prozesse und verdächtige IP-Adressen, Domainnamen oder Datei-Hashes im Zusammenhang mit Bedrohungen zu identifizieren

Durch die gleichzeitige Implementierung dieser drei Methoden entsteht ein starkes Sicherheitsnetz, das gewährleistet, dass jeder aktuelle Angriff im Rechenzentrum erkannt, abgewehrt und für eine gründliche Untersuchung eingedämmt wird.

Weitere Informationen zu den umfassenden Funktionen zur Angriffserkennung und -reaktion von Akamai Guardicore Segmentation finden Sie unter akamai.com/guardicore.

 | Support | Veröffentlicht: 06/23