Aktuelles

Cisco Stealthwatch Cloud – Anomalieerkennung in der Hybrid Cloud

19.10.2018

IT-Verantwortliche müssen heute davon ausgehen, dass bestimmte Malware-Varianten die Unternehmensgrenzen mühelos passieren. Angriffe dieser Kategorie sind in der Regel „unsichtbar“ und „lautlos“ und sie werden meistens erst im Nachhinein anhand ihrer Auswirkungen entdeckt. Dies erfordert eine lückenlose Überwachung aller internen Infrastrukturen – inklusive der Public Clouds.

Moderne Verteidigungssysteme, wie Cisco Stealthwatch Cloud, sind kein Selbstzweck, sondern das Ergebnis einer sich stetig verschärfenden Sicherheitsbedrohung. Die Erkennung von Anomalien findet dabei üblicherweise im Netzwerk statt. Mittels Auswertung der Flow Protokolle ist es möglich, ungewöhnliches Verhalten im Netzwerk zu identifizieren. Das funktioniert auch dann, wenn der Schadcode Verschlüsselung verwendet, um sich zu verstecken.

Cisco Stealthwatch Cloud untersucht jedes IP-Paket, das innerhalb eines Netzwerks weitergeleitet wird, nach gewissen Attributen, Diese Attribute stellen die Identität des IP-Pakets oder den Fingerabdruck dar. Somit lässt sich ermitteln, ob das Paket einzigartig oder ähnlich zu anderen Paketen ist. Mit Cisco Stealthwatch Cloud werden Bedrohungen in Echtzeit erkannt und die Anzahl von "false positives" reduziert.

Funktionen und Vorteile

- Automatisches Aufspüren von Bedrohungen
- Erkennen von ersten Anzeichen einer Kompromittierung
- Identifizierung von Richtlinienverstößen, falsch konfigurierten Cloud-Ressourcen, Benutzerfehlern und Missbrauchsversuchen.

Aussagekräftige Warnungen

- Cisco Stealthwatch Cloud empfängt umfangreiche Netzwerk-Telemetrie und Netzwerkprotokolle. Anhand dieser Informationen identifiziert die Lösung die Rolle jeder Netzkomponente.
- Verhält sich eine Komponente ungewöhnlich oder zeigt Anzeichen schädlichen Verhaltens, erhalten Sie eine Warnung und können umgehend eine Untersuchung einleiten.
- Anwender bewerten 96 % aller Stealthwatch Cloud-Warnungen als "hilfreich."

Einfaches Management und unkomplizierte Skalierbarkeit

Stealthwatch Cloud wird als Software-as-a-Service-Produkt (SaaS-Produkt) bereitgestellt. Evaluierung, Kauf und Nutzung sind also vollkommen unkompliziert. Sie müssen weder besondere Hardware kaufen noch Softwareagenten bereitstellen, und auch besonderes Know-how ist nicht erforderlich.

Um bereits ein positives User-Erlebnis bei der Bestellung zu ermöglichen, unterstützt BT Stemmer seine Kunden von der Planung bis hin zur Umsetzung. Selbstverständlich können die Cloud Services auch nachträglich an sich verändernde Umgebungen angepasst werden. Unter dem Motto „Hybrid Everything“ kombinieren wir Private Cloud, Public Cloud und On Premise Bausteine zu flexiblen, effizienten und sicheren Infrastruktur-Lösungen. Für Fragen, Anregungen und Angebote steht Ihnen unser Cisco Goldpartner Team gerne zur Verfügung.