FORTRA

DATENBLATT *(Cybersicherheit)*

Sandbox

Optimieren Sie Ihr bestehendes Clearswift Secure E-Mail Gateway mit der Next-Gen Cloud-Sandbox von Sophos. Die Netzwerk-Sandbox bietet durch modernstes maschinelles Lernen eine zusätzliche Sicherheitsebene gegen Ransomware und gezielte Angriffe, ohne dass Sie weitere Systeme verwalten müssen.

Der Schutz auf Enterprise-Niveau ist in wenigen Minuten einsatzbereit und lässt sich nahtlos in das EMail-Gateway integrieren.

Tiefgehende Absicherung

Der Einsatz mehrerer AV-Engines in EMail-Gateways ist üblich, und das Clearswift SEG bildet hier keine Ausnahme, da es die AV Engines von Sophos, Avira und Kaspersky parallel nutzen kann. Ergänzend dazu haben wir unsere eigene Erkennungsfunktion entwickelt, um aktiven Code in Dokumenten zu erkennen und optional zu entfernen. Für alle Kunden, die sicher verhindern wollen, dass ausführbare Inhalte per Email in ihr Unternehmen eindringen und Schaden anrichten, ist die Sandbox-Technologie als weitere Sicherheitsebene unbedingt empfohlen.

So Funktioniert Es

Wenn Nachrichten am Gateway ankommen, werden sie einem AV-Scan unterzogen, der anhand von Signaturen und Heuristiken prüft. Dateien mit bekannter Malware werden automatisch blockiert/gelöscht1, ausführbare Dateien oder solche mit ausführbarem Inhalt, die Sophos AV Engine als verdächtig einstuft, werden weiter untersucht.

Zunächst wird der Hash der Datei in der Sandbox überprüft, um festzustellen, ob die Datei von der Sandbox gesehen wurde. Wenn dies der Fall ist, wird die Datei gemäß der Policy blockiert/gelöscht, wenn nicht, wird sie zur Überprüfung vorgelegt. Wenn die Datei von der Sandbox gescannt wird, wird ihr Verhalten sorgfältig auf Anzeichen von bösartiger Software überwacht.

Sobald die Datei gescannt wurde, gibt die Sandbox die Scan-Ergebnisse zurück an das Gateway, wo die Datei blockiert, gelöscht oder weiteren Prüfungen unterzogen wird, wie z. B. einer Stichwortsuche.

PRODUKTÜBERSICHT

KEY FEATURES

- Untersucht mehrere Inhaltstypen mit einer Reihe von Methoden, um zu erkennen, ob die Datei gefährliche Inhalte enthält, wobei statische Analyse und Modelle für maschinelles Lernen die Erkennung unterstützen.
- Scannt ausführbare Dateien und Skripteo
  - o Ausführbare Windows PE-Dateien
  - o DLL
  - o VBscript & Javascript
- Scans Documents
  - o MS Office
  - o RTF
  - o PDF
- Scans Archive files
  - o Zip, BZip, Gzip
  - o RAR, TAR, 7z
  - o LHA, LZH, Cabinet

HIGHLIGHTS

- In der Cloud gehostet - keine zusätzlichen Systeme, die der Kunde verwalten muss
- Sichere und private Detonation von Inhalten
- Unterstützung für On-Premises und Hosted Gateways
- Auswahl des Sandbox-Standorts durch den Kunden (USA, Großbritannien, Deutschland, Japan)
- Hochgradig skalierbarer AWS-Cloud-Service (SOC2)
- Niedrige Latenzzeit der gescannten Dateien, typischerweise <5min
- Umfassende Analyse der gescannten Datei

[1] Abhängig von Ihrer Policy

Umfassendes Reporting

Wenn die Sandbox die Datei als gefährlich einstuft, wird ein umfassender Bericht erstellt, in dem die Detonation der Datei für das Admin-Team einsehbar ist. Der Bericht zeigt

- Datei-Details
- Datei-Hashes
- Aufgerufene Prozesse
- Auf die Festplatte geschriebene Dateien
- Netzwerk-Aktivität
- Bösartige Aktivität
- Aktivitätsbaum
- Screenshots