- Erweiterter Bedrohungsschutz – als Ergänzung zu JEDER Firewall
- SSL-Inspektion mit mehreren integrierten Antiviren-Scan-Engines
- Keine Beeinträchtigung der bestehenden Firewall-Leistung
- Virtuell, als Hardware Appliance oder als Service in der Cloud

Clavister NetEye

Überprüfen und neutralisieren Sie eingebettete SSL-Bedrohungen

Verschlüsselung - die Möglichkeit, Daten auf der einen Seite in unlesbaren Inhalt zu verwandeln, der nur von einem Empfänger mit zugelassenen Schlüsseln gelesen werden kann - ist ein Segen für den Datenschutz ... und ein wachsendes Sicherheitsproblem. Verschlüsselter SSL-Datenverkehr, in der Regel von HTTPS-Webseiten und anderen Websites, durchläuft herkömmliche Firewalls, für die der Inhalt nicht identifizierbar ist. Hacker betten zunehmend mehr bösartige Codes und Datei-Downloads in diese Websitzungen ein, welche die Sicherheit umgehen. Führende Analysten schätzen, dass bereits heute mehr als die Hälfte der Netzwerkangriffe auf Unternehmen mit verschlüsseltem Datenverkehr durchgeführt werden, um Sicherheitskontrollen zu umgehen. Die traditionelle Art der Entschlüsselung und SSL-Inspektion auf der Firewall reduziert den Durchsatz und die Leistung um bis zu 80% und führt somit zu einer drastischen Verringerung der Servicequalität. Mit der Zunahme des verschlüsselten Datenverkehrs, der in den nächsten Jahren fast 100% betragen wird, suchen IT-Administratoren, CIOs und CSOs nach einem Weg, ihre Endbenutzer zu schützen, die Daten in Echtzeit überprüfen zu lassen, und dies ohne Beeinträchtigung der Firewall-Performance. Was sie gesucht haben, ist die Lösung “Clavister NetEye”, die als On-Premise Appliance oder als Cloud Service angeboten wird.

Clavister NetEye ist der ideale Weg, Advanced Threat Protection zu implementieren, um eingebettete SSL-Bedrohungen zu identifizieren und den Administrator über das InCenter-Verwaltungstool von Clavister zu alarmieren, damit dieser Maßnahmen ergreifen kann. Darüber hinaus ermöglichen die Detonationsfunktionen von Clavister Sandbox Cloud, verdächtige Dateien und Pakete an eine sichere Cloud-Umgebung zu senden, in Quarantäne zu stellen und nach bösartigem Verhalten zu untersuchen, welche versuchen, die Sicherheit des Netzwerks zu umgehen. Sobald dies geschehen ist, benachrichtigt die Sandbox-Cloud Clavister InCenter über die Aktivität und warnt die Netzwerkadministratoren vor der Malware, um Maßnahmen im Netzwerk ergreifen.

Clavister NetEye ist für jede Firewall (Clavister oder Drittanbieter) einfach und mit minimalem Aufwand zu implementieren. Es hat keinen wesentlichen Einfluss auf den Durchsatz der eigentlichen Firewall und bietet eine einfache Möglichkeit, die Skalierung über mehrere Standorte mit einem zentralen System vorzunehmen. Der IT-Manager kann nun die Kosten einfach verwalten und gleichzeitig sicherstellen, dass der gesamte Datenverkehr auf Bedrohungen überprüft wird.

Herausforderungen, die wir lösen

Die beste Antiviren-Engine, um Bedrohungen zu stoppen

Clavister NetEye verwendet aktuelle Antivirensignaturen, um Malware und bösartige Inhalte zu erkennen. Es kann auch mit einer Artificial Intelligence Engine erweitert werden, die polymorphe Viren sofort erkennt. Diese Engine scannt und erkennt bösartiges Verhalten innerhalb der Dateieigenschaften. Es verzögert den Download in Echtzeit, scannt in wenigen hundert Millisekunden und wenn OK, lässt es die Datei passieren. Mit diesem Ansatz benötigt nur ein winziger Teil der Dateien Sandboxing.

Clavister NetEye arbeitet mit allen gut zusammen

Obwohl Clavister NetEye natürlich im Optimalfall gemeinsam mit Clavister NetWall genutzt wird, unterstützt es alle Anbieter und kann daher als Ergänzung in jeder Sicherheitsinfrastruktur eingesetzt werden.

Vor Ort oder in der Cloud ... wählen Sie

Clavister NetEye ist entweder als hochkarätige und extrem performante On-Premise Hardware-Appliance für Kunden mit Compliance- oder anderen Anforderungen oder als Cloud-Produkt erhältlich. Was auch immer Sie benötigen, Clavister NetEye ist die richtige Lösung für Sie.

Inspektion verschlüsselter Datenverkehr

Sandboxing

Antivirus Scanning

Clavister NetEye Models

Rack-mounted	NE-8000	NE-8500	NE-8900
SSL Inspection performance	500 Mbps	1 Gbps	2 Gbps
Approx nr of users	600	1200	2500

Virtual	NE-50V	NE-100V	NE-250V	NE-500V
SSL Inspection performance	50 Mbps	100 Mbps	250 Mbps	500 Mbps
Approx nr of users	50	100	300	600

Cloud	NE-50C	NE-100C	NE-250C	NE-500C
SSL Inspection performance	50 Mbps	100 Mbps	250 Mbps	500 Mbps
Approx nr of users	50	100	300	600

SECURITY BY SWEDEN

#NoBackDoors und Zugangsbeschränkung für Dritte

Clavister bestätigt hiermit, dass Clavister-Produkte keine "Hintertüren" enthalten, was bedeutet, dass es keine bewusst eingebauten Mechanismen gibt, die es einem Unternehmen oder einer Organisation ermöglichen würden, ohne vorherige Zustimmung des Administrators des betreffenden Produkts auf ein Clavister-Produkt zuzugreifen oder es zu kontrollieren.

John Vestberg, CEO, Clavister

www.clavister.com/SecurityBySweden

clavister®
CONNECT • PROTECT

Clavister GmbH • Kirchstr.23a • 31595 Steyerberg • Germany
Phone: +49 (0)89 21 09-3400 • Mail: info@clavister.de • Web: www.clavister.com