
clavister
SECURITY BY
SWEDEN
CONNECT
PROTECT
PREVENT
ENTERPRISE SECURITY
USE - CASE GUIDE

Eine alles kommunizierende Welt, basierend auf Vertrauen und Sicherheit.
Clavister's Vision

SECURING BUSINESS CONTINUITY

Clavister sichert und schützt Netzwerke von Unternehmen und Dienstleistern und ermöglicht Geschäftskontinuität mit einer Produktreihe für verschiedene Anwendungsfälle

Die Cybersicherheit wird heute als eine der größten Bedrohungen für die Weltwirtschaft angesehen und wird im Jahr 2021 jährlich schätzungsweise 6 Billionen US-Dollar kosten (Quelle: Cybersecurity ventures). Clavister beliefert dezentrale Unternehmen mit Sicherheitslösungen, die ihre Geschäfte sicher schützen und vernetzen. Die Produkte wurden in Schweden entwickelt – garantiert frei von Backdoors und nicht auf Standard-Betriebssystemen basiert.

Die Lösungen bieten mehrere Anwendungsfälle im selben Setup, sichere Konnektivität, Schutz vor Bedrohungen und ermöglichen das Ergreifen von vorbeugenden Maßnahmen, die unangemessene Nutzung innerhalb von Netzwerken einzuschränken. Die Lösungen laufen auf Geräten, die sich für kleine bis große Büros eignen, aber auch zum Schutz der Cloud-Ressourcen virtualisiert sind. Clavisters Lösungen können von IT-Abteilungen intern verwaltet oder von lokalen spezialisierten Managed-Services-Partnern betrieben werden.

Clavisters Hauptsitz befindet sich in Örnsköldsvik, Schweden, mit Niederlassungen in Deutschland, Japan, Südostasien und den nordischen Ländern. Clavister hat mehr als 200 000 Installationen bei Kunden in 154 Ländern. Die Lösungen werden auf OEM-Basis durch unter anderem Nokia und D-Link vertrieben.

Das Clavister-Paket

Clavisters Next Generation Firewall verfügt über ein sehr einfaches Lizenzmodell, das auf Benutzerlizenzen, Software-Blades, Add-on-Pakete oder ähnliches verzichtet. Stattdessen stehen zwei Abonnementmodelle zur Verfügung, die Basic- oder erweiterte Funktionalitäten ermöglichen, um Anwendungsfälle erstellen zu können. Das zentrale Management, das minimale Wartung und flexible Konfigurationsmöglichkeiten gewährleistet, wird ebenfalls in beiden Paketen bereitgestellt.

Diese Pakete ermöglichen es, sowohl kleine als auch große Unternehmen mit einer schlüsselfertigen, hocheffizienten „Next Generation Firewall"-Lösung auszustatten, ohne auf die bewährte Funktion des Universal Threat Management zu verzichten oder ein anderes Instrument zu diesem Zweck einsetzen zu müssen. Mit Clavister setzen Sie eine Sicherheitslösung ein, die Ihnen Sicherheit bei geringeren Kosten bietet.

Ökosystem

Clavister arbeitet mit in ihrem jeweiligen Segment führenden Lieferanten zusammen und integriert deren Technologien. Das Clavister-Ökosystem konzentriert sich auf die Einbeziehung von Spitzenlösungen und umfasst:

- **McAfee (Intel Security) für Intrusion Prevention System**
- **Kaspersky Lab für Antivirus**
- **Webroot für IP Reputation Feeds**
- **ContentKeeper für die Filterung von Webinhalten**
- **Qosmos von ENEA für Application Control mit Deep Packet Inspection**
- **Bitdefender für Endpoint Protection**

McAfee · KASPERSKY lab · WEBROOT · ContentKeeper · ENEA · Bitdefender

Die beiden verfügbaren Abonnementpakete sind:

Clavister Product Subscription – CPS
Das Grundabonnement mit 24/7-Support und Hardware-Ersatz am nächsten Werktag.

Firewall-Upgrades sind enthalten und die Software kann die wichtigsten Anwendungsfälle unterstützen.

Clavister Security Subscription — CSS
Ebenso wie CPS plus Abonnementdienste, die folgende Anwendungsfälle ermöglichen: Network/Server Attack Protection, Advanced Threat Protection, Web Content Blocking und Application Visibility & Control.

Die Produkte von Clavister werden in einer breiten Palette von Sicherheitslösungen und Anwendungsfällen eingesetzt. In diesem Buch stellen wir Beispiele der beliebtesten Lösungen vor und erläutern deren Vorteile.

CONNECT

Die Verbindung von Geschäftsstandorten miteinander und mit dem Internet, unter dem Aspekt von Sicherheit und Zuverlässigkeit, gewährleisten die Kontinuität von Geschäftsvorgängen.

PROTECT

Anwendungsfälle zur Überprüfung des Verkehrs und des Verkehrs-verhaltens bei Bedrohungen, um Ihre digitalen Assets zu schützen.

PREVENT

Diese Anwendungsfälle reduzieren mithilfe von präventiven Sicherheitsmaßnahmen und -regeln das Risiko auf Benutzerfehler, die das digitale Umfeld Ihres Unternehmens bedrohen oder gefährden könnten.

„Bis 2020 werden mehr als 50 % der Aktualisierungsinitiativen für WAN-Edge-Infrastrukturen auf SD-WAN im Vergleich zu herkömmlichen Routern basieren. (eine Steigerung von den aktuellen 2 %).“
- Gartner

Zuverlässiges und sicheres Virtual Private Networking

Niederlassungen und entfernte Standorte sicher und kostengünstig verbinden

Unternehmen hängen von ihrer Konnektivität zwischen den Niederlassungen ab und benötigen daher eine robuste, zuverlässige und sichere Lösung. In einer dezentra-lisierten Geschäftsumgebung ist Kommunikation in Echtzeit zwischen Systemen der Schlüssel zu Business-Intelligence und -Enablement. In der Vergangenheit haben Unternehmen private Leasingleitungen gemietet oder MPLS-Lösungen verwendet. Diese Lösungen erwiesen sich als einschränkend und teuer und brachten oft eine Abhängigkeit zu einem einzigen Telekommunikationsanbieter mit sich. Der Bedarf an Flexibilität und Kostenreduzierung führte zur Nutzung von Virtual Private Networking statt gemeinsamen Internetverbindungen an jedem Standort. Fortschritte bei der Cloud-Enablement haben zu Lösungen mit dem Namen Software Defined – Wide Area Networks – oder SD-WAN geführt.

Lösung

Die Secure SD-WAN-Lösung von Clavister kombiniert den Reliable Secure VPN-Anwendungsfall und andere Anwendungsfälle wie Perimeterschutz und Routing – Redundanz und Lastverteilung. Dies wird in einer virtualisierten Nur-Software-Lösung für die Bereitstellung in der Cloud oder auf einer Reihe von Hardware-Appliances angeboten. Ein virtuelles Netzwerk zwischen Ihren Standorten lässt sich mit Verwaltungstools, die eine sichere Kommunikation zwischen den Standorten und der Cloud ermöglichen, einfach einrichten.

Die kleinste Einrichtung von Clavister liegt nur zwischen zwei Standorten, während die größte Installation 3 000 verschiedene Standorte mit fast 10 000 eindeutigen VPN-Tunneln umfasst. Mit ganzheitlichen Managementfunktionen und richtlinienbasiertem Routing ist die Lösung flexibel und skalierbar sowie einfach zu verwalten.

Ergebnisse

Unternehmen, die SD-WAN-VPN-Lösungen einsetzen, verringern die Betriebskosten im Vergleich zu gemieteten Leitungen oder MPLS-Lösungen erheblich. Ebenfalls im Gegensatz zu MPLS kann der Anbieter von Internetdiensten an jedem Standort ein anderer sein. Eine große Auswahl an Internet-Transportmethoden (wie Kabel, DSL, Faser und 4G) steht zur Verfügung, um Flexibilität und Kostensenkungen zu ermöglichen.

Hier erfahren Sie mehr über die SD-WAN-Lösung von Clavister:

www.clavister.com/sd-wan (Auf Englisch)

Routing – Redundanz und Lastverteilung

Ausfallzeiten vermeiden und Kontinuität von Geschäften gewährleisten

Unternehmen sind auf ihre Kommunikationsinfrastruktur angewiesen, um Geschäftsvorgänge effizient durchführen zu können. Selbst die kürzeste Ausfallzeit einer Verbindung kann die Produktivität beeinträchtigen – oder einen wichtigen entfernten Standort unerreichbar machen. Da das gesamte Unternehmen immer stärker von Konnektivität abhängig ist, läuft die gesamte Belegschaft Gefahr, unproduktiv zu werden.

Clavisters Routing-Funktionalität wurde in jeder nach 1997 durchgeführten Kundenbefragung als Vorreiter bezeichnet und es wurde hervorgehoben, wie einfach es einzurichten und zu verwenden ist.

Lösung

Mit der richtigen Infrastruktur können Unternehmen kostengünstigere Zweitverbindungen (wie Kabel, DSL und 3G) nutzen, um bei Bedarf als Backup-Route zu dienen. In größeren Einrichtungen kann die Firewall als Traffic-Router fungieren und mit einfacher Einrichtung komplexe Entscheidungen treffen.

Ergebnisse

Integrierte fortschrittliche Routing- und Lastverteilungsfunktionen gewährleisten die Geschäftskontinuität, indem kosteneffiziente Möglichkeiten genutzt werden. Es vereinfacht auch Wartung und Migration für IT-Techniker – was zusätzliche Ausrüstung von Drittanbietern überflüssig macht.

Hier erfahren Sie mehr über die Routing- und Lastverteilungsfunktionen von Clavister:

www.clavister.com/routing (Auf Englisch)

„Nur 3 % der von Gartner befragten Unternehmen verfügen über einen Anti-Malware-Schutz auf mobilen Android-Geräten und nur 1 % auf iOS-Geräten.” – Gartner

Secure Network Zones

Netzwerksegmentierung zum Schutz der digitalen Unternehmenswerte

Mitarbeiter gehen davon aus, eigene Geräte ins Büro bringen und an die Infrastruktur anschließen zu dürfen. Oft werden diese Geräte jedoch nicht vom Administrator verwaltet und unterliegen daher nicht dem gleichen Schutz wie die von Unternehmen ausgegebenen Geräte. Dies stellt ein Risiko für interne Systeme dar, das von innerhalb des sicheren Bereichs ausgeht.

Lösung

Die Lösung besteht darin, Ihr Netzwerk in mehrere Zonen zu segmentieren und den zwischen ihnen erlaubten Verkehr sorgfältig zu kontrollieren. Eine ergänzende Möglichkeit besteht darin, vor den wichtigsten Geschäftsanwendungen wie Datenbanken, Dateiservern und Collaboration-Servern eine interne Sicherheitsumgebung einzurichten.

Ergebnisse

Durch den Schutz Ihrer digitalen Assets mit einer virtualisierten dedizierten Firewall erhalten Sie die volle Kontrolle über den Datenverkehr, auch von innerhalb Ihres Netzwerks. Aufgrund des geringen Platzbedarfs von Clavister benötigt dies minimale zusätzliche Ressourcen und kann auf derselben Virtualisierungs-Hypervisor-Infrastruktur betrieben werden.

Hier erfahren Sie mehr über die Secure Network Zones von Clavister:

www.clavister.com/zones (Auf Englisch)

Server-Lastverteilung

Vereinfachung von Skalierung und Möglichkeit der vorbeugenden Wartung

Jede IT-Infrastruktur verfügt über Komponenten, die unerlässlich sind und ein Hochverfügbarkeits-Setup benötigen, um Redundanz bereitzustellen. Dies gewährleistet sowohl die Serviceverfügbarkeit, falls in einem der Server etwas Unerwartetes vorfällt, als auch die Möglichkeit einer proaktiven Wartung auf einfache Weise. Redundanz kann in die Applikationsebene eingebaut werden oder mit DNS-Round-Robin eingerichtet werden, aber dies erhöht die Komplexität und bietet für den Service-Besitzer nicht immer Kontrollmöglichkeiten.

Lösung

Eine Server-Lastverteilung-Funktion, die in die Firewall, die den gehosteten Dienst schützt, eingebaut ist, kann Hochverfügbarkeit und Kontrolle bereitstellen. Die Lösung kann ohne das Umschreiben von Paketinhalten die Lasten des Protokollverkehrs einschließlich HTTP(S), DNS und LDAP verteilen und Strategien zu Verbindungsraten und Ressourcennutzung einsetzen.
Sie kann Informationen über eine API empfangen, um dynamisch das Verhältnis der Lastverteilung zu den Servern zu ändern, sodass dies mittels externer Prozesse von Drittanbietern entschieden werden kann. Dabei kann es sich um mail.que, Plattenspeicher, CPU-Nutzung usw. handeln.

Ergebniss

Mit einer integrierten Server-Lastverteilung benötigt der IT-Administrator keine speziellen Lösungen, um die hohen Verfügbarkeitsanforderungen zu erfüllen. Auch die Möglichkeit einer proaktiven Wartung während der normalen Arbeitszeit erleichtert die Arbeit und ermöglicht eine kosteneffiziente Skalierung der Serviceinfrastruktur.

Die Firewall-Lösung von Clavister bietet mehrere Möglichkeiten, die Verfügbarkeit des Servers zu überprüfen.
Eine einfache Ping-ICMP-Nachricht überprüft, ob der Server antwortet. TCP-Überwachung validiert, ob bestimmte Dienste auf ihren Ports reagieren, und HTTP-Überwachung kann darauf konfiguriert werden, eine bestimmte URL abzufragen und damit eine erwartete Antwort zu validieren. In Kombination mit Skripten auf dem Server kann dies auch überprüfen, ob eine Backend-Datenbank funktioniert und, basierend auf den Ergebnissen, ein Failover auslösen.

Hier erfahren Sie mehr über die Lastverteilungs-funktionen von Clavister:
www.clavister.com/slb (Auf Englisch)

Flexibler Remote Access

Remote-Mitarbeit sicher ermöglichen

Unsere Arbeitsweise hat sich drastisch verändert: Wir sind jetzt mobiler und globaler, wir verwenden unsere eigenen Geräte, wir greifen über komplexe und nicht gesicherte Verbindungen wie WLAN-Hotspots und andere Zugangsmöglichkeiten auf unsere Arbeit zu. Unabhängig von Standort oder Verbindung ist eine einfach zu verwaltende und zu konfigurierende sichere Remote-Arbeitslösung, die eine Vielzahl von verschiedenen Geräten unterstützt, ein unerlässlicher Faktor für den Erfolg und den Datenschutz eines Unternehmens.

Lösung

Eine flexible Fernzugriffslösung unterstützt eine Reihe von Technologien, einschließlich IPsec, SSL, L2TP oder PPTP und ermöglicht eine sichere Konnektivität auch in den am meisten eingeschränkten Remote-Umgebungen. Die Kompatibilität mit VPN-Clients, die in Windows-, Mac- und mobilen Betriebssystemen integriert sind, ermöglicht es allen Geräten, eine Verbindung herzustellen und einen integrierten SSL-VPN-Client von Clavister zu verwenden, der sowohl für den Endbenutzer als auch für den IT-Administrator einfach zu nutzen ist.

Ergebnisse

Remote-Access-VPN-Lösungen von Clavister lassen sich schnell auf allen Ihren Geräten einrichten, ohne dass IT-Administratoren benötigt werden. Sie können darauf vertrauen, dass alle Daten vertraulich und ohne böswillige Codes versandt werden, wenn sie durch Ihr Netzwerk geschickt werden. Clavisters Lösung führt dies alles ohne Latenz durch, um so Ihrem Netzwerk (und Ihren Mitarbeitern) die bestmögliche Leistung zu ermöglichen und funktioniert sowohl in Appliance- als auch in virtualisierten Installationen.

Hier erfahren Sie mehr über die VPN-Lösungen von Clavister:

www.clavister.com/vpn (Auf Englisch)

Perimeterschutz

Netzwerk-Firewall zur Sicherung von IT-Ressourcen und Benutzern

Hacker, Viren, Ransomware, Datendiebstahl, Industriespionage und sogar von Regierungen unterstützte Angriffe. Die Liste der Cyber-Bedrohungen, die Ihr Unternehmen gefährden könnten, wird immer länger. Das Weltwirtschaftsforum hat Cyber-Angriffe auf den dritten Platz bei der Wahrscheinlichkeit und auf den sechsten Platz der Bedrohungen mit den größten Auswirkungen gesetzt. Aber die Herausforderung besteht nicht nur darin, das Netzwerk sicher zu machen, sondern es gleichzeitig auch effizient und produktiv zu gestalten.

Lösung

Notwendig ist eine Firewall, die eingehenden und ausgehenden Netzwerkverkehr anhand intelligenter Sicherheitsregeln überwacht und kontrolliert. Für einen optimalen Schutz ist es entscheidend, sehr spezifisch festzulegen, welche Art von Verkehr zugelassen wird und alles andere zu blockieren. Obwohl die Grenze zwischen dem Internet und Ihrem Netzwerk die offensichtliche Stelle für eine Firewall ist, kann die Einrichtung innerhalb des Unternehmensnetzwerks auch die Sicherheitsstufen für bestimmte Segmente erhöhen.

Ergebnisse

Mit sowohl virtualisierten als auch Appliance-basierten Versionen bietet Clavister Sicherheit für jede Nische Ihres Netzwerks. Alle Unternehmensversionen enthalten Optionen, die im Hochverfügbarkeitsmodus ausgeführt werden können, um die Kontinuität von Geschäftsvorgängen auch während der Wartungszeiten zu gewährleisten.

Clavisters Firewalls der nächsten Generation werden in Schweden hergestellt und basieren auf einem urheberrechtlich geschützten Betriebssystem. Dadurch sind sie garantiert frei von Backdoors und nicht für die in Betriebssystemen wie Windows und Linux regelmäßig auftretenden Mängel anfällig. Die Firewalls umfassen eine Reihe von Netzwerkdiensten, einschließlich Netzwerkadressenübersetzung, dynamische Adresszuweisung und Nutzersensibilisierung durch Integration mit Microsoft Active Directory.

Hier erfahren Sie mehr über den Perimeter-schutz von Clavister:

www.clavister.com/firewall (Auf Englisch)

Netzwerk/Server Attack Protection

Systeme zur Erkennung von und Schutz vor Eindringen plus Schutz vor Denial of Service

Distributed Denial of Services (DDoS)-Angriffe gehören zu den einfachsten und zugänglichsten Möglichkeiten selbst für einen Hacker-Anfänger, Probleme zu verursachen. Mit einem der vielen vorgefertigten Tools ist es einfach, einen Angriff auf Hunderte oder sogar Tausende von Computern auszuführen, der nahezu jedes System oder jede Firewall überfordert und sie dazu bringt, sich abzuschalten oder im Schneckentempo zu arbeiten. Nicht nur Web-Shops fallen dem zum Opfer, sondern ganze Unternehmen auf Carrier Grade.
Sicherheitssysteme werden zum Gegenstand von Lösegeldforderungen. Die meisten Szenarien enden damit, dass Unternehmen das verlangte Lösegeld zahlen, um die Bedrohung abzuweisen. Ganz und gar nicht optimal, aber immer noch viel günstiger als tagelange Ausfallzeiten, die irreversible Schäden für den Markennamen verursachen

Lösung

Clavister bietet einen auf Ihr Unternehmen zugeschnittenen Schutz. Dieser Schutz bildet eine Verteidigung, die nicht nur den Verkehr stoppt, sondern evasiv und flexibel bleibt. Selbst während eines massiven DoS-Angriffs, der alles abschaltet, stellt die Clavister Next Generation Firewall sicher, dass das interne Netzwerk und die Backup-Internetverbindungen funktionsfähig bleiben. DoS-Angriffe auf Serverdienste hinter der Firewall können durch Verkehrsmanagement und Ratenbegrenzung abgeschwächt werden.

Ergebnisse

Die Clavister Next Generation Firewall ermöglicht nicht nur eine Vielzahl von Strategien, um die Auswirkungen eines DoS-Angriffs auf einen Server, der hinter der Firewall gehostet wird, zu mildern und zu reduzieren. Die Lösung stellt auch sicher, dass die internen Betriebsabläufe während eines DoS-Angriffs nicht beeinträchtigt werden und sich Ihre Mitarbeiter auf die Kontinuität des Geschäfts konzentrieren können.

Hier erfahren Sie mehr über die DoS-Schutzfunktionen von Clavister:

www.clavister.com/server-protection (Auf Englisch)

„4 % aller Personen klicken auf jede beliebige Phishing-Kampagne."
- Verizon's 2018 Data Breach Investigations Report (DBIR)

Das AV-TEST Institut registriert über 250 000 neue Malware-Programme täglich.

Advanced Threat Protection

Integriertes System zum Schutz vor unbefugtem Eindringen mit Antivirus- und Malware-Screening

Hacker mit böswilligen Absichten werden versuchen, Codeteile oder Links durch die Firewall zu senden, um Nutzer dazu zu bringen, von innen eine Schwachstelle zu erzeugen. Dies ermöglicht es den Hackern oft, die Kontrolle über ein Gerät des Benutzers zu erlangen und bietet ihnen eine Plattform, um die digitalen Assets in Ihrem Unternehmen zu erkunden. Angriffe sind oft sehr gut abgeschirmt und selbst der vorsichtigste Benutzer kann den Fehler machen, einem Hacker unbeabsichtigt zu helfen.

Lösung

Firewalls der nächsten Generation bieten integrierten Schutz vor mehreren Formen von Bedrohungen. Nicht vertrauenswürdiger Datenverkehr kann auf Viren und Malware gescannt werden, basierend auf mehreren Signaturdatenbanken, künstlicher Intelligenz und Verhaltenserkennung. Jeglicher E-Mail- und Web-Verkehr wird speziell auf bekannte Bedrohungen oder verdächtiges Verhalten hin gründlich überprüft. Beispielsweise müssen in E-Mails auch Anhänge sowie Links daraufhin überprüft werden, ob ihr Ziel mit der Domain übereinstimmt, von der die E-Mail gesendet wurde.

IP-Adressen sind eindeutig und Informationen darüber, wie vertrauenswürdig sie sind, werden zentral gesammelt. Basierend auf diesem Ruf kann die Next Generation Firewall Richtlinien hinzufügen, um den Datenverkehr zu weniger renommierten Websites zu blockieren – oder zusätzliches Screening für Inhalte in riskanten Bereichen des Internets bereitzustellen.

Clavister-Firewalls umfassen Virenschutz- und Malware-Scans mit Signaturdatenbanken von Kaspersky und McAfee/Intel Security, die Web-, FTP- und E-Mail-Inhalte in Echtzeit scannen. Darüber hinaus werden Verbindungen durch eine IP-Reputationsdatenbank von Webroot gescreent. Alle Anbieter sind Weltmarktführer in ihren jeweiligen Bereichen.

Ergebnisse

Mit einer Next Generation Firewall von Clavister schützen Sie Ihr Netzwerk und Ihre Benutzer vor Hackern und Eindringlingen. Bösartige Inhalte werden verhindert und der Verkehr von Websites mit fragwürdigem Ruf kann vermieden werden. Benutzer können damit aufhören, sich Sorgen über verdächtig aussehende E-Mails und Webinhalte zu machen und sich darauf konzentrieren, Mehrwert für das Unternehmen zu erzeugen.

Hier erfahren Sie mehr über die Advanced Threat Protection-Funktionen von Clavister:

www.clavister.com/threat-protection (Auf Englisch)

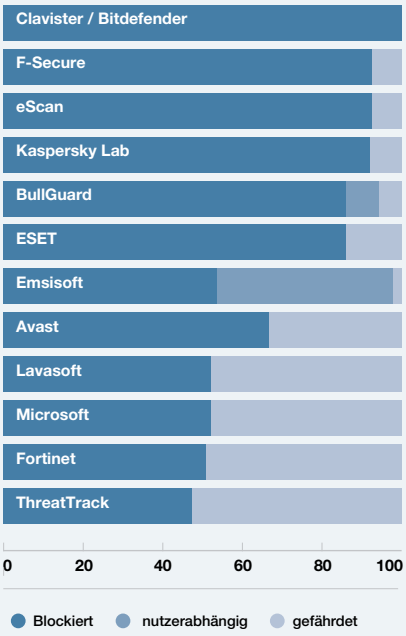
Endbenutzerschutz

Blockierung von Bedrohungen und Erkennung von Datenverlusten an Endgeräten

Wenn sich Laptop-Geräte außerhalb Ihres sicheren Perimeters bewegen, sind sie gefährdet, während sie mit anderen offenen Netzwerken verbunden werden. Wenn sie unterwegs sind, laufen diese Laptops Gefahr, infiziert zu werden – und im schlimmsten Fall bleibt dies unerkannt, bis der Laptop wieder in das Unternehmensnetzwerk zurückkehrt. Der Virus oder die Malware wird uneingeschränkten Zugriff auf die interne Umgebung haben, was für eine sehr unerwünschte und gefährliche Situation sorgt.

Lösung

Clavisters Endpunktlösung basiert auf dem Branchenführer Bitdefender, der künstliche Intelligenz und Verhaltenserkennungssoftware in Kombination mit Signaturdatenbanken bereitstellt, um Viren und Malware zu erkennen. Die Software verfügt darüber hinaus über eine integrierte Datenleck-Prävention (DLP), die Einhaltung der DSGVO-Richtlinien gewährleistet und sensible Daten nicht gefährdet. Die Lösung ist Cloud-verwaltet, einfach bereitzustellen und hat sich Jahr für Jahr in unabhängigen Tests als die beste Lösung auf dem Markt herausgestellt.



Source: AV-Comparatives, Heuristic/Behavior Test

Hier erfahren Sie mehr über den Endbenutzerschutz von Clavister:
www.clavister.com/endpoint (Auf Englisch)

Blockierung von Webinhalten

Zugriff auf unangemessene Inhalte einschränken und Vorschriften einhalten

Spezifische Standorte in öffentlichen Netzwerken, Unternehmensrichtlinien für private Netzwerke oder staatliche Vorschriften: Es gibt viele Gründe dafür, warum bestimmte Arten von Websites möglicherweise eingeschränkt werden müssen.

Wenn 100 Mitarbeiter pro Woche eine Stunde sparen, indem der Zugang zu nicht-geschäftsbezogenem Web-Browsing eingeschränkt wird, resultiert dies in Einsparungs-möglichkeiten von mehr als 100.000 EUR pro Jahr.

Lösung

Eine Webinhalt-Klassifizierungs-Engine gleicht die URL und den Hostnamen des Servers in Echtzeit mit einer Datenbank mit Inhaltskategorien ab und kennzeichnet den Verkehrsfluss entsprechend des Inhalts. Richtlinien in der Engine können dann entweder geeignete Maßnahmen ergreifen oder diese Informationen lediglich für statistische Zwecke protokollieren. Auf diese Weise können Administratoren den Zugriff auf als jugendgefährdendes Material leicht einschränken oder Social-Media-Websites während bestimmter Tageszeiten blockieren. Die Datenbank wird mehrmals täglich aktualisiert, um sicherzustellen, dass neue Websites kontinuierlich hinzugefügt und die entsprechenden Maßnahmen ergriffen werden.

Ergebnisse

Wenn dies eingesetzt wird, werden nicht nur peinliche Situationen vermieden, sondern es trägt auch zu einer Erhöhung der Produktivität bei und stellt sicher, dass Geschäftsressourcen für die richtigen Zwecke eingesetzt werden.

Hier erfahren Sie mehr über den Filter von Webinhalten von Clavister:

www.clavister.com/filtering (Auf Englisch)

Marktführer von ENEA/Qosmos

Clavister integriert Qosmos ixEngine von ENEA, den Marktführer für die Klassifizierung von IP-Verkehr und Netzwerkintelligenz-Technologie. Genau so, wie man anhand der Baummerkmale eine Birke in einem Kiefernwald findet, identifiziert Qosmos mehr als 3 000 einzigartige Anwendungen außerhalb des Netzwerkverkehrs. Die Definitionen werden kontinuierlich aktualisiert und unsere Software-Freigabe ist monatlich eingeplant. Weitere Informationen finden Sie auf www.qosmos.com

Anwendungssichtbarkeit und -kontrolle

Kontrolle von Anwendungen und Benutzerverhalten

IT-Administratoren von Unternehmen müssen die Nutzung ihres Netzwerks kontrollieren, um sicherzustellen, dass es für Geschäftsanwendungen verwendet wird. Einige dieser Anwendungen könnten sogar Vorrang bekommen, während andere proaktiv blockiert werden sollten, da sie bekannt dafür sind, höhere Risiken mit sich zu bringen und die Sicherheit zu gefährden. Beispiele sind BitTorrent-Clients für Peer-to-Peer-Datei-Download oder Tor, eine Anwendung zum Browsen im Dark Web und häufig von Malware verwendet, um Daten aus Ihrem Netzwerk zu exfiltrieren. Ein weiteres Beispiel ist die nicht autorisierte, übermäßige Nutzung von Serverressourcen für Bitcoin-Mining, die die Stromrechnung von Unternehmen erhöht.

Diese Anwendungen sollten blockiert werden. Nicht der gesamte Verkehr ist Web-Verkehr – eine Menge Verkehr läuft auf getrennten Ports und verwendet benutzerdefinierte Protokolle, um mit seinen Servern und Peers zu kommunizieren. Dazu ist eine Anwendungsidentifikations-Engine (auch Deep Packet Inspection/DPI genannt) erforderlich, um die Anwendung bzw. den Dienst präzise zu erkennen. Eine Anwendung wie WebEx und Skype kann identifiziert und der Datenverkehr priorisiert werden, um die Qualität der Gespräche zu unterstützen. Anwendungskontrolle ist unerlässlich, um die Benutzerfreundlichkeit zu verbessern.

Um den Datenverkehr Ihrer Benutzer auf kontrollierte Weise zu verwalten, bietet Clavisters Next Generation Firewall die weltweit beste Deep Packet Inspection-Technologie an, um eine Anwendungsidentifizierung durchzuführen. Darüber hinaus stuft Clavister jeden Antrag mit einem Risikoniveau von sehr niedrig bis sehr hoch ein, wodurch die Konfiguration der Blockierung riskanter Anwendungen ein Kinderspiel ist.

JA! Verschlüsselter Verkehr kann klassifiziert werden.

Der Großteil des Verkehrs wird heute verschlüsselt. Doch durch das Lesen der Servernamenanzeige (SNI) im SSL/TLS-Zertifikat, die Durchführung der Statistischen Protokollidentifizierung (SPID) oder die Suche nach binären Mustern im Datenverkehr kann die Deep Packet Inspection Engine in Clavisters Next Generation Firewall noch mit 90 bis 100 % Genauigkeit erkennen, um welche Anwendung es sich handelt.

Internet der Dinge (IoT)

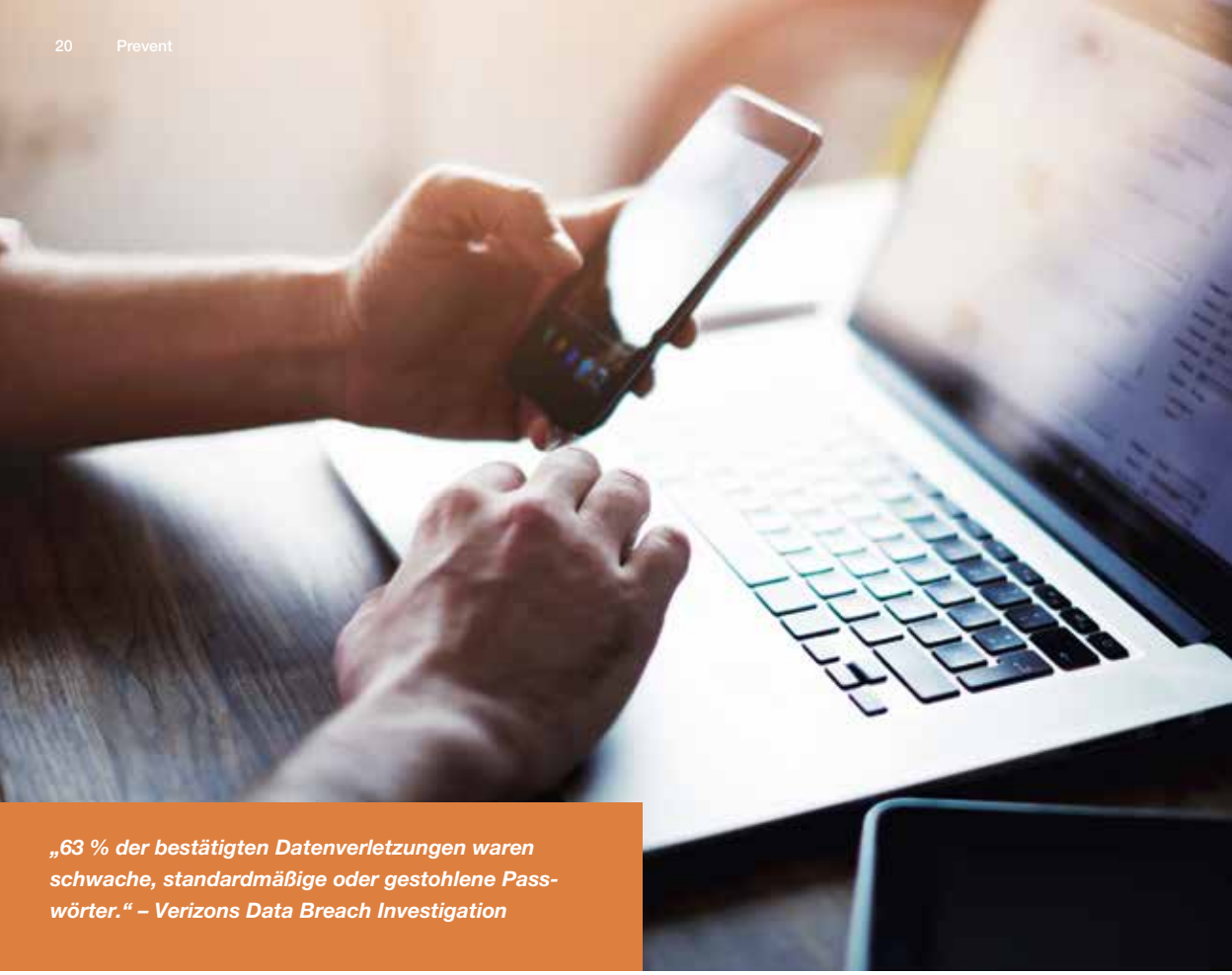
Speziell für IoT-Geräte bietet Anwendungssichtbarkeit die perfekte Möglichkeit zur Kontrolle der Geräteaktivitäten. Mit erweiterten Richtlinien können Sie sie auf dem Netzwerk nur auf die Aktivitäten einschränken, die sie ausführen sollten. Auf diese Weise kann ein gehacktes IoT-Gerät nicht als Sprungbrett verwendet werden, um andere Ressourcen zu erreichen.

Ergebnisse

Anwendungskontrolle bietet Mittel, sehr spezifisch angeben zu können, was Sie auf Ihrem Netzwerk zulassen möchten. Dies erhöht die Sicherheitsstufen und ermöglicht es Ihnen, frühzeitig neue Technologien einzusetzen, ohne unnötige Risiken einzugehen.

Hier erfahren Sie mehr über den Anwendungsfall von Clavisters Anwendungssichtbarkeit und -kontrolle:

www.clavister.com/dpi (Auf Englisch)



„63 % der bestätigten Datenverletzungen waren schwache, standardmäßige oder gestohlene Passwörter.“ – Verizons Data Breach Investigation

Multi-Faktor-Authentifizierung

Sicherstellung der Authentizität von Endnutzern

Benutzer sind in der Regel nicht vorsichtig genug mit Passwörtern und verwenden häufig einfache Passwörter. Dies ermöglicht Hackern einen einfachen Weg, einen Account zu gefährden. Auch wenn Ihr System sicher ist: Wenn die Kontoinformationen der Nutzer anderswo erhältlich sind, ist es wahrscheinlich, dass Ihre Infrastruktur ebenfalls in Gefahr ist. Dies liegt daran, dass Benutzer in vielen Fällen dasselbe Passwort in verschiedenen Diensten wiederverwenden. Eine zweite Sicherheitsschicht sollte erstellt werden, um die Identität des Benutzers zu identifizieren und zu autorisieren.

Lösung

Multi-Faktor-Authentifizierung oder 2-Faktor-Authentifizierung bietet eine einfache und sichere Möglichkeit für Ihre Benutzer, sich anzumelden. Zur Bestätigung der Identität des Benutzers können mehrere Out-of-Band-Methoden verwendet werden. Dazu können Einmal-Passwort-Lösungen über SMS, mobile App oder HW-Token bzw. Zertifikate gehören.

Multi-Faktor-Authentifizierung (MFA) von Clavister wird von den wichtigsten Regierungsinstitutionen in Schweden verwendet. Das Produkt umfasst mehrere und flexible MFA-Liefermethoden wie ein Einmal-Passwort über SMS, E-Mail, mobile App, One-Touch-Bestätigung und Hardware-Token, x.509 Zertifikate usw. Es ist redundant und skalierbar für hohe Verfügbarkeit und bietet mit seiner Benutzerfreundlichkeit das zusätzliche Maß an Sicherheitsschutz, das Ihr Unternehmen benötigt.

Ergebnisse

Mit einer Multi-Faktor-Authentifizierungslösung wird die Sicherheit verbessert und ein Administrator kann einfach feststellen, ob derjenige, der angemeldet ist, tatsächlich als der beabsichtigte Benutzer authentifiziert ist. Mit der Integration in den Anwendungsfall des flexiblen Remote Access können Benutzer von überall sicher arbeiten.

Hier erfahren Sie mehr über die Multi-Faktor-Authentifizierungslösungen von Clavister:

www.clavister.com/mfa (Auf Englisch)

Aktive Verkehrsoptimierung

Verkehrspriorisierung zur Sicherung der gewünschten Ressourcennutzung

Es kommt häufig vor, dass Netzwerkverbindungen ihre Grenzen erreichen und aufgrund der Art und Weise, wie Anwendungen entwickelt werden, um die verfügbare Bandbreite zu nutzen, überlastet werden. Typischerweise geschieht dies mit Dateifreigabe/-Synchronisierung oder durch die Verwendung anderer Anwendungen, die mehrere TCP-Sitzungen parallel erstellen und auf eine maximale Bandbreitennutzung abzielen.

Das Ergebnis ist, dass Kapazitäten nicht angemessen an andere Benutzer zugewiesen werden können, was zu einer Verschlechterung des Dienstes führt und normalerweise Auswirkungen auf gefährdete Anwendungen wie VoIP und Konferenz-Anwendungen hat. Dies führt zu einer schlechten Gesprächsqualität, und durch das Netzwerk induzierte Unterbrechungen beeinträchtigen die Produktivität.

Lösung

Am Rande des Netzwerks fungiert die Next Generation Firewall als Richtlinien-Gatekeeper, um verschiedene Arten von Datenverkehr – oder Datenverkehr von verschiedenen Benutzern – mit unterschiedlicher Priorität zu behandeln. Dienstleistungsvereinbarungen können eingerichtet werden, um einen Teil der verfügbaren Bandbreite für bestimmte Anwendungen oder Benutzer zu garantieren.

Clavisters Next Generation Firewalls sind umfassend konfigurierbar, um den Datenverkehr zu unterscheiden. Verschiedene virtuelle Leitungen können erstellt werden, um Verkehrsmengen innerhalb von Sets zu verwalten und können sowohl Anwendungserkennung als auch Benutzeridentifizierung einsetzen, um zu entscheiden, zu welcher Verkehrsleitung eine bestimmte Sitzung gehört.

Ergebnisse

Die Implementierung intelligenter Verkehrsoptimierung und -priorisierung hat erhebliche Auswirkungen auf den Verkehr, wenn Kapazitätsgrenzen erreicht werden. Die Qualität von Sprach- und Videokonferenzanrufen verbessert sich und wird weniger oft unterbrochen, während Dateisynchronisierungsanwendungen wie Dropbox nur eine Sekunde länger dauern, um die Dateien im Hintergrund zu synchronisieren, aber weiterhin normal funktionieren.

Um mehr darüber zu erfahren, wie verschiedene Verkehrsarten voneinander unterschieden werden können, lesen Sie bitte dieses Whitepaper:

www.clavister.com/optimisation (Auf Englisch)

Die Bedeutung von Proaktivität

Erweiterter Perimeterschutz und sichere Verbindungen zwischen Standorten bilden die Grundlage einer soliden Sicherheitsinfrastruktur. Aber oft spielt der Nutzer eine unbeabsichtigte wichtige Rolle dabei, wenn Hacker den Zugang zu den digitalen Vermögenswerten und Ressourcen der Unternehmen erhalten.

Die Multi-Faktor-Authentifizierung hilft beim Problem schlechter Passwörter auf eine Weise, die auch eine verbesserte Benutzerfreundlichkeit bei der Verbindung mit Unternehmenssystemen bieten kann. Aber für IT-Administratoren gibt es eine weitere wichtige Möglichkeit, die Nutzer von falschen Entscheidungen abzuhalten, indem der Zugriff auf sichere Anwendungen und Websites kontrolliert wird. Die Beschränkung böswilliger Websites aufgrund ihres weltweiten Rufs und Blockierung von Dark Web, Bitcoin-Mining und anderen spezifischen Anwendungen reduzieren das Risiko und stellen sicher, dass die Unternehmensressourcen bestimmungsgemäß eingesetzt werden. Die Kontrolle der Verkehrsströme kann auch ein verbessertes Kundenerlebnis bieten, indem wichtige Echtzeitanwendungen vom Hintergrundverkehr unterschieden werden und damit die Qualität von beispielsweise Webkonferenzanwendungen erhöht wird.

Es ist an der Zeit, proaktiv zu denken und vorbeugende Maßnahmen zu implementieren, um Sicherheitsvorfälle zu vermeiden. Clavister bietet die fortschrittlichen Technologien für vorbeugende Anwendungsfälle, für die Sie kein Experte sein müssen, um sie zu implementieren und sofortige Ergebnisse zu sehen.

Netzwerkauto-matisierungs-möglichkeit

In einer sich schnell bewegenden Welt, in der neue Bedrohungen stündlich oder sogar häufiger auftreten, müssen IT-Administratoren ständig auf der Hut sein, um die digitalen Vermögenswerte des Unternehmens zu schützen.

Die Zunahme bei den Geräten, die auch in Unternehmensnetzwerken mit dem Internet der Dinge verbunden sind, macht es notwendig, schnell zu reagieren.

Um diese Kosten effizient zu verringern, sind fortschrittliche Technologien wie maschinelles Lernen und künstliche Intelligenz erforderlich, um Muster zu sehen, Abweichungen zu erkennen und auf Anomalien aufmerksam zu machen. Clavister geht noch weiter: Die Lösung ergreift gegebenenfalls automatisierte Maßnahmen, um eine Bedrohung auszuschalten, bevor sie Ihr Unternehmen beeinträchtigt.

Sie müssen kein Sicherheitsexperte werden – die selbstlernende Lösung von Clavister schützt Sie rund um die Uhr.

clavister

SECURITY BY SWEDEN

Brancheninformationen und weltweite Cyber-Sicherheitstrends

ENTERPRISE SECURITY
USE-CASE GUIDE

#NoBackDoors

Alle Clavister-Geräte werden mit dem von Clavister entwickelten Betriebssystem cOS Core ausgeliefert. Diese komplett in Schweden in Eigenregie entwickelte Software baut auf urheberrechtlich geschützten Betriebssystemen auf. Diese vollständige Kontrolle ermöglicht Clavister die Garantie, dass seine Next Generation Firewalls zu 100 % Backdoor-frei sind.

Ebenso sind Schwachstellen wie „Heartbleed“, „Shellshock/Bash“, „Ghost” oder „FREAK” sowie zukünftige Open-Source-Fehler aufgrund der Verwendung des proprietären Betriebssystems in Clavister-Lösungen nicht möglich. Viele alternative Sicherheitslösungen wurden in der Vergangenheit beeinträchtigt (siehe Tabelle unten).

Einheitliche Software auf allen Systemen stellt sicher, dass es keine funktionalen Unterschiede zwischen den Plattformen gibt – sowohl gerätebasiert als auch virtualisiert.

	Heartbleed	Shellshock/Bash	Ghost	Freak
Barracuda	🟠	🟠	🟠	🔵
Checkpoint	🟠	⚫	⚫	🔵
Cisco	🟠	🟠	🟠	🟠
Clavister	🔵	🔵	🔵	🔵
Cyberoam	🟠	⚪	–	🔵
Fortinet	🟠	🟠	🟠	🟠
Juniper	🟠	⚫	🔵	🟠
Palo Alto Networks	🔵	🟠	🟠	🔵
Securepoint	🟠	🟠	⚫	–
Sophos	🟠	⚪	🟠	🟠
Watchguard	🟠	🔵	🟠	🔵

🔵 **Keine Firewall betroffen** 🟠 **Alle Firewalls betroffen** ⚫ **Einige Firewalls betroffen**
⚪ **Alle Firewalls sind betroffen, können aber laut Lieferant nicht angegriffen werden**
– Keine Angaben

Haftungsausschluss: Erklärung zum Zeitpunkt der Veröffentlichung des Angriffs gültig. Anbieter könnten ihre Produkte seitdem gepatcht haben.

Kontakt Clavister - Hauptsitz: Sjögatan 6J, SE-891 60, Örnsköldsvik, Schweden. Telefon: +46 660 299200
Weitere Informationen finden Sie auf www.clavister.com oder folgen Sie uns auf Twitter @Clavister

Weltweite Cyber-Sicherheitstrends

Viele Sicherheitsthemen werden gegenwärtig in der Tagespresse behandelt. Im Global Risks Report 2018 des Weltwirtschaftsforums erscheinen Cyber-Angriffe auf dem dritten Platz bei der Wahrscheinlichkeit und auf dem sechsten Platz der Bedrohungen mit den größten Auswirkungen. Cyber-Angriffe stehen hier im Vergleich mit anderen Katastrophen wie extremen Wetterereignissen und Terroranschlägen!

Top 10 Gefahren in Bezug auf **Wahrscheinlichkeit**

1. Extreme Wetterereignisse
2. Naturkatastrophen
3. **Cyber-Angriffe**
4. **Betrug mit oder Diebstahl von Daten**
5. Scheitern beim Abschwächen des Klimawandels und Anpassungen
6. Unfreiwillige Migration in großem Umfang
7. Durch Menschen verursachte Umweltkatastrophen
8. Terroristische Angriffe
9. Illegaler Handel
10. Vermögensblasen in einer großen Volkswirtschaft

Top 10 Gefahren in Bezug auf **Auswirkung**

1. Massenvernichtungswaffen
2. Extreme Wetterereignisse
3. Naturkatastrophen
4. Scheitern beim Klimawandel
5. Minderung und Anpassung Wasserkrisen
6. **Cyber-Angriffe**
7. Nahrungsmittelkrisen
8. Verlust der biologischen Vielfalt und Zusammenbruch des Ökosystems
9. Unfreiwillige Migration in großem Umfang
10. Verbreitung von Infektionskrankheiten

Quelle: Global Competitiveness Report des Weltwirtschaftsforums
www.weforum.org/reports/the-global-risks-report-2018

Um mehr über bestimmte Sicherheitsthemen zu erfahren, lesen Sie bitte die folgenden Seiten

Brancheninformationen

Jede Branche ist anders und spezifische Anforderungen und Vorschriften müssen mithilfe von Lösungen erfüllt werden. In einer Zusammenfassung der gemeinsamen Anforderungen werden in diesem Anwendungsfall-Buch die folgenden spezifischen Branchen erläutert:

Ransomware

Malware encrypting systems causing them to malfunction

Ransomware is the newest cyber threat whereby a cybercriminal takes control of your files by encrypting them and forcing you to pay to get them back.

First the computer gets infected through a virus or malware installed on the system. Often these get installed because a users is tricked to click an unsecured link or add unauthorized software on their system outside the security perimeter.

If infected, the cybercriminal will display a message on your computer like “Your computer files have been encrypted and are inaccessible. Your photos, videos, documents etc. are under our control. But don’t worry, we have not deleted them yet. You have 24 hours to pay 500 USD in bitcoins”. Just to show you he/she can do it, he destroys a few files and then starts exponentially destroying more and more, by the hour. Try to restart your computer and he’ll destroy the hard drive; not paying within 72 hours, the same.

Experts have been working on a fix, using anti-ransomware protection through your firewall and keeping backups is preventative. Once you are hit, you can only pay up or destroy your drive and recover from an off-line backup.

Hier erfahren Sie mehr über Ransomware:

www.clavister.com/ransomware (Auf Englisch)

Botnets, Zero-Days-Bedrohungen

Bösartiger Code auf Ihrem Gerät, der Dritten Zugriff und Kontrolle gibt

Ein Botnet ist eine Anzahl internetverbundener Systeme, von denen jedes einen oder mehrere Bots ausführt.

Ein Bot ist ein kleines Programm, das ferngesteuert werden kann, um bestimmte Aufgaben vorzubereiten – es stammt von dem Wort „Roboter". Botnets werden in der Regel in einem negativen Kontext genannt und können verwendet werden, um dezentralisierte Denial-of-Service-Angriffe (DDoS-Angriffe), Datendiebstahl oder Spamversand auszuführen und ermöglichen es dem Angreifer, auf das Gerät und seine Verbindung zuzugreifen. Für den Hacker ist der Bot ein Werkzeug, um böswillige Aufgaben auszuführen und dazu entweder lokale Ressourcen zu verwenden oder als Sprungbrett zu fungieren, um so ein Netzwerk oder IT-System tiefer zu durchdringen.

Ein Zero-Day-Exploit (auch als 0-Day-Exploit bekannt) ist ein Cyber-Angriff, der am selben Tag auftritt, an dem die Schwachstelle in der Software entdeckt wird. An diesem Punkt wird es genutzt, bevor sein Ersteller eine Reparatur zur Verfügung stellt. Zero-Day-Exploits werden oft von Hackern verwendet, um schlafende Bots auf Systemen zu installieren, die
ein anderes Mal bei einem Angriff verwendet werden

Hier erfahren Sie mehr über den Schutz vor Botnets und Zero-Day-Bedrohungen:
www.clavister.com/ipreputation (Auf Englisch)

Dezentralisierte Denial-of-Service-Angriffe

Internationale gezielte Überlastung von Server- oder Netzwerkressourcen

Ein Denial-of-Service-Angriff (DoS-Angriff) ist ein Cyber-Angriff, bei dem der Anstifter versucht, einen Dienst oder ein Netzwerk für seine entsprechenden Benutzer unzugänglich zu machen. Dies geschieht entweder durch Überschwemmung des Dienstes mit Anforderungen, die die Dienst- oder Netzwerkkapazität überlasten, oder durch Ausnutzung von Schwachstellen in den Dienstanwendungen.

Ein dezentralisierter DoS-Angriff nutzt eine Vielzahl von Quellen für diese Anfragen, um eine Flut aus allen Richtungen gleichzeitig einzuleiten.

DDoS-Angriffe sind in vielen Ländern illegal, aber es kann schwer festzustellen sein, wer den Angriff eingeleitet hat. Da Angriffswerkzeuge immer weiter verbreitet und einfach zu bedienen sind, hat sich die Zahl der angegriffenen Organisationen drastisch erhöht.

Es gibt Angriffe in vielen Variationen und daher ist eine Kombination verschiedener Merkmale erforderlich, um einen guten Schutz zu bieten. Verteidigungstechniken beinhalten Ratenbegrenzung, Verkehrsformung und Zugangskontrolle. Wichtig für die Sicherheitsinfrastruktur ist das Arbeiten in einem segmentierten Modus, was bedeutet, dass die Überlastung einer Schnittstelle nicht zu einer Beeinträchtigung der anderen Schnittstellen führt. Auf diese Weise können Unternehmen ihre interne Infrastruktur weiter betreiben und Backup-Links nutzen, auch während eines laufenden DDoS-Angriffs, indem die primäre Internetverbindung vollständig genutzt wird.

Langsamer DDoS

Nicht alle Systemüberlastungen werden absichtlich durch Hacker oder Cyber-Terroristen erzeugt. Fehlerhafte Geräte wie Mobiltelefone mit älteren Betriebssystemen oder Geräte mit schlechter Konnektivität, die mit dem Internet of Things verbunden sind, können wiederholte Anfragen an denselben Dienst senden – oft in sehr kurzen Abständen. Dies beginnt möglicherweise unbemerkt mit zehn oder sogar Hunderten dieser Geräte, aber wenn Tausende das gleiche Verhalten zeigen, wird dies Probleme bei der Serverkapazität verursachen. In diesem Szenario müssen Muster im Verkehr erkannt werden, um fehlerhafte Geräte zu identifizieren und sie vom Rest des Verkehrs zu isolieren, um eine Serviceverschlechterung zu vermeiden..

Schutz und Geschäftskontinuität

Die Produkte von Clavister bieten umfassenden Schutz vor DoS- und DDoS-Angriffen und können entweder als zentraler Schutz eingesetzt werden,
oder nachträglich als separate Ebene in ein bestehendes Netz eingebaut werden. Anstelle teurer Nischenprodukte bietet Clavister einen guten Schutz, ohne Verwaltungsaufwand und Kosten erheblich zu erhöhen. Selbst während eines massiven DDoS-Angriffs, der auf Ihre öffentlichen Web-Services abzielt, stellen die Multi-Wan-Link-Technologien von Clavister sicher, dass das interne Geschäft nicht beeinträchtigt wird.

Hier erfahren Sie mehr über DDoS und die Lösungen von Clavister:
www.clavister.com/ddos (Auf Englisch)

„Die EU-Datenschutz-Grundverordnung (DSGVO) hat ein erneutes Interesse geschaffen und wird bis 2018 65 Prozent der Kaufentscheidungen zur Vermeidung von Datenverlust vorantreiben." – Gartner Inc.

Datenschutz-Grundverordnung (DSGVO)
Das EU-Recht zum Datenschutz und zur Privatsphäre

Die DSGVO ist eine Verordnung des EU-Rechts zum Datenschutz und zur Privatsphäre aller Personen innerhalb der Europäischen Union. Sie trat am 25. Mai 2018 in Kraft; weil es sich um eine Verordnung und nicht um eine Richtlinie handelt, ist es nicht erforderlich, dass die nationalen Regierungen entsprechende Gesetze verabschieden, und die Verordnung ist somit direkt verbindlich und anwendbar.
Die DSGVO erfordert die Einführung verbesserter Datenschutzpraktiken, -technologien und -richtlinien für die meisten Unternehmen. Sie klassifiziert personen-bezogene Daten weitgehend als alle Informationen, die direkt oder indirekt einer Einzelperson zugeschrieben werden können. Die DSGVO beauftragt Unternehmen, neue Verfahren und Prozesse, Berichterstattung und Kommunikation sowie eine verbesserte Netzwerksicherheit bei den neuesten Technologien aufzunehmen, die „Situationsbewusstsein für Risiken" bietet und „präventive, korrigierende und abschwächende Maßnahmen ermöglicht".

Der Begriff „Situationsbewusstsein" steht bei den DSGVO-Richtlinien zentral und bezieht sich auf die Anforderungen von Routinen und Fähigkeiten, um zu erkennen, ob ein Verstoß vorliegt, bei dem sensible Informationen gefährdet sein könnten.
Datenverantwortliche sind verpflichtet, einen Verstoß und Datenverlust innerhalb von 72 Stunden zu melden. Sollte entweder kein angemessenes Situationsbewusstsein gezeigt oder innerhalb einer Frist von 72 Stunden kein Bericht erstattet werden, kann dies zu erheblichen Geldbußen führen.

Wichtige Komponenten, die dies ermöglichen, sind Technologien zur Vermeidung von Datenverlusten und die Multi-Faktor-Authentifizierungsstrategien, um sicherzustellen, dass der angemeldete Benutzer authentifiziert und autorisiert ist, sodass Versuche, Daten aus dem sicheren Perimeter zu entfernen, erkannt werden und ein Alarm ausgelöst wird.

Hier erfahren Sie mehr über die DSGVO und die Lösungen von Clavister:
www.clavister.com/gdpr (Auf Englisch)

NIS-Richtlinie

Die EU-Richtlinie über die Sicherheit von Netzwerk- und Informationssystemen

Die NIS-Richtlinie ist der erste Teil der EU-weiten Gesetzgebung zur Cybersicherheit. Sie sieht rechtliche Maßnahmen zur Steigerung des Gesamtniveaus der Cybersicherheit in der EU vor und ist speziell für die Betreiber bedeutender Infrastrukturen gedacht. Dazu gehören digitale Dienstleister und Betreiber unverzichtbarer Dienstleistungen, einschließlich Strom-, Wasser- und Abfallwirtschaft.

Lösung

TDer Vorschlag wurde Mitte 2016 angenommen und bis Ende 2018 müssen alle Mitgliedstaaten Betreiber wesentlicher Dienstleistungen identifiziert haben. Sie sind dann für die Meldung wichtiger Sicherheitsvorfälle an die Einsatzteams verantwortlich. Betreiber, die nicht in der EU ansässig, aber weiterhin in der EU tätig sind, unterliegen trotzdem den Vorschriften. Auch beim Auslagern der Wartung ihrer Informationssysteme an Dritte sind sie gemäß der NIS-Richtlinie weiterhin für alle Sicherheitsvorfälle verantwortlich.

Ergebnisse

Sicherheitsanforderungen umfassen technische Maßnahmen, die die Risiken von Cybersecurity-Verstößen präventiv steuern. Die Richtlinie wird die Sicherheit von Netzwerk- und Informationssystemen in der EU erhöhen und den Schutz unserer Gesellschaft vor Hackern und Cyberterroristen gewährleisten.

Hier erfahren Sie mehr über die NIS-Richtlinie und die Lösungen von Clavister für wichtige Infrastrukturen:

www.clavister.com/nis (Auf Englisch)

„Finanz und Einzelhandel sind die zwei großen Branchen, die unter DDoS-Angriffen leiden."
– Verizon 2017 Data Breach Investigations Report

Sicherheit für Filialinfrastrukturen

Einzelhandel & dezentrale Büros

Ein moderner Einzelhändler ist stark auf IT angewiesen, um seine Ziele bei betrieblicher Effizienz, niedrigeren Kosten und besserer Kundenerfahrung zu erreichen. Unternehmen mit vielen kleinen Filialen oder Geschäften stehen oft vor der Herausforderung, ohne lokale Administratoren ununterbrochene Verbindungen in den Feldbüros gewährleisten zu müssen, damit das Warenwirtschaftssystem, SAP oder das Kassensystem ordnungsgemäß funktionieren. Mit mehr Geschäfts-Technologie wie WiFi-basierten Point-of-Sale-Terminals, kostenlosem WiFi-Zugang für Kunden, intelligenten Beacons, Selbstbedienungskassen, Reklame-Bildschirmen im Geschäft und internen Verwaltungsnetzwerken wird die Komplexität stets größer. Obwohl IT an allen diesen Punkten eine fantastische Arbeit leistet, lässt sie die Unternehmen auch für Sicherheitsverletzungen anfällig werden, die ihre Geschäftskontinuität und damit ihren Gewinn gefährden.

Unternehmen mit vielen kleinen Filialen oder Geschäften, aber auch Unternehmen mit mehreren Filialen haben viel gemeinsam. Sie benötigen eine zentral verwaltbare und gleichzeitig kostengünstige Lösung für den Anschluss der Filialniederlassungen, ohne dabei Kompromisse bei Funktionalität und Sicherheit machen zu müssen. Dazu gehören nicht nur klassische Firewall-Funktionen wie Perimetererkennung, sondern auch sogenannte Next Generation Firewall-Funktionen, die es ermöglichen, die Kommunikation auf Basis von Protokollen und Anwendungen mit fortgeschritteneren Anwendungsfällen zu regulieren.

Lösungen von Clavister bieten die neuesten Technologien und Funktionen, auch für kleinste Geräte. Diese bieten einen effektiven und kostengünstigen Schutz und optimale Lösungen für die IT-Sicherheit in dezentralen Netzwerken, immer einschließlich zentralisierter Verwaltung.

Wichtige Komponenten und Anwendungsfälle, die Clavister zur idealen Wahl für Einzelhandels-unternehmen und Unternehmen mit dezentralen Niederlassungen machen:

• Zuverlässiges und sicheres Virtual Private Networking stellt sicher, dass vertrauliche Daten privat bleiben und Zweigstellen sicher miteinander und mit dem Hauptsitz kommunizieren können.

• Routing – Redundanz und Lastverteilung ermöglichen den Aufbau einer zuverlässigen und fehlertoleranten Infrastruktur, mit kostengünstigen Breitbanddiensten anstelle von teuren gemieteten Verbindungen.

• Netzwerk/Server Attack Protection – integrierte Systeme zur Erkennung von und zum Schutz vor unbefugtem Eindringen und DDoS, um Schutz für digitale Frontends zu ermöglichen – aber auch mit einem Schutzmechanismus, um die Geschäftskontinuität während solcher Überlastsituationen zu gewährleisten.

• Berichte, die vollständig anpassbar sind und auch die gewünschten Informationen grafisch darstellen können. Auch ist eine feinskalierbare Live-Überwachung über ein anpassbares Dashboard
enthalten, die gewährleistet, dass z. B. VPN-Tunnel oder Internetverbindungen permanent überwacht werden können.

Hier erfahren Sie mehr über die Lösungen für Einzelhandel und dezentrale Büros von Clavister:
www.clavister.com/retail (Auf Englisch)

Securing business continuity

Industrie-Internet der Dinge (IoT) & Transport

Fast alle Maschinen und Industriesysteme bieten heute die bequeme Möglichkeit der Fernwartung sowie der zentralen Analyse von gesammelten statistischen Messdaten. Dies erfordert einen gesicherten Zugang von außen, der wiederum von Unbefugten missbraucht werden könnte. Zugänge müssen auch an Orten mit wechselnden Umwelteinflüssen, in industriellen Umgebungen oder für bewegte Maschinen solide geschützt werden.

Netzwerke sollten in Zonen segmentiert werden, um verschiedene Sicherheits- und Verkehrsmanagementrichtlinien zu ermöglichen, die gewährleisten, dass der Zugang zu industriellen Sensoren sorgfältig kontrolliert und der externe Zugang begrenzt wird. Weitere Richtlinien müssen eingeführt werden, um eine bestimmte garantierte Bandbreite bereitzustellen und so eine hohe Verfügbarkeit, beispielsweise für Industrieroboter, zu gewährleisten.

Fallstudie: Sicherung des Fernwartungsnetzes in Maschinen und Anlagen

Ob der Schiffsdieselmotor auf einem Kreuzfahrtschiff vom Hersteller überwacht und gewartet wird oder ein Fertigungsroboter ein Softwareupdate erhält: Fernzugriff ist heutzutage bei großen Maschinen unverzichtbar. Da hierfür oft nur ein kleines Zeitfenster zur Verfügung steht und der Schutz vor Missbrauch durch Unbefugte notwendig ist, ist die Geschwindigkeit und die hohe Verfügbarkeit wichtiger Punkte unverzichtbar. Mit Lösungen von Clavister lässt sich dies einfach und kostengünstig erreichen und gleichzeitig das IT-Sicherheitsniveau insgesamt deutlich erhöhen.

Wichtige Komponenten und Anwendungsfälle, die Clavister zur idealen Wahl für Industrie-IoT und Transport machen:

• Zuverlässiges und sicheres Virtual Private Networking stellt sicher, dass vertrauliche Daten privat bleiben und Zweigstellen sicher miteinander und mit dem Hauptsitz kommunizieren können.

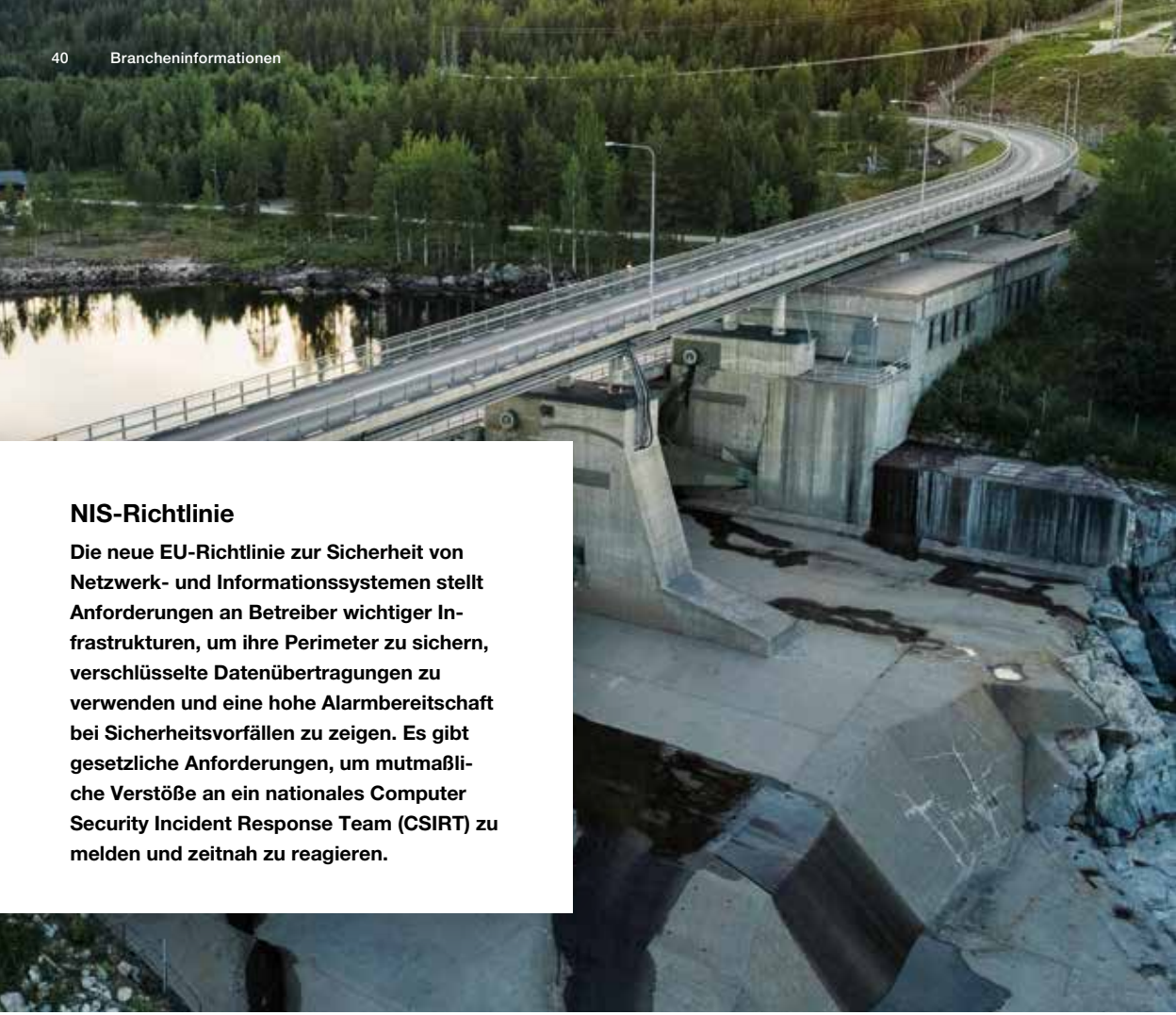
• Routing – Redundanz und Lastverteilung ermöglichen den Aufbau einer zuverlässigen und fehlertoleranten Infrastruktur, mit kostengünstigen Breitbanddiensten anstelle von teuren gemieteten Verbindungen.

• Sichere Netzwerkzonen, um Netzwerksegmentierung zu ermöglichen und verschiedene Sicherheits- und Qualitätsrichtlinien anzuwenden, um die richtigen Maschinen mit guten Netzwerkressourcen zu versorgen.

• Zentralisiertes Remote-Management, das den IT-Administrator in die Lage versetzt, alles kontrollieren und sehen zu können und in Echtzeit Maßnahmen zu ergreifen.

• Die virtualisierte Next Generation Firewall von Clavister bietet alle Anwendungsfälle und Funktionen mit einem extrem niedrigen Platzbedarf, die in praktisch jeder Hypervisor-Umgebung installiert werden kann.

Hier erfahren Sie mehr über die Lösungen für Industrie-IoT und Transport von Clavister:
www.clavister.com/iot (Auf Englisch)



NIS-Richtlinie

Die neue EU-Richtlinie zur Sicherheit von Netzwerk- und Informationssystemen stellt Anforderungen an Betreiber wichtiger Infrastrukturen, um ihre Perimeter zu sichern, verschlüsselte Datenübertragungen zu verwenden und eine hohe Alarmbereitschaft bei Sicherheitsvorfällen zu zeigen. Es gibt gesetzliche Anforderungen, um mutmaßliche Verstöße an ein nationales Computer Security Incident Response Team (CSIRT) zu melden und zeitnah zu reagieren.

Vollständige Einhaltung mit einer Lösung mit geringem Platzbedarf

Wichtige Infrastrukturen

Energieversorger, kommunale Versorgungsunternehmen und Netzbetreiber haben viel gemeinsam – sie alle betreiben eine wichtige Infrastruktur, um normales Leben gewährleisten zu können. Diese Infrastruktur benötigt wiederum eine robuste Sicherheitsinfrastruktur, die volle Kontrolle vom Hauptquartier aus bietet, Echtzeit-Datenerfassung zu Analysezwecken ermöglicht und sicheren Fernzugriff zur Steuerung bietet. Das Besondere bei wichtigen Infrastrukturen ist, dass physischer Raum knapp sein kann und eine Lösung zusammen mit anderen Funktionen wie Prozessen zur Erfassung von Sensordaten gehostet werden muss.

Fallstudie: Anbindung von Solar- und Windparks

Eine Next Generation Firewall, die als Komponente für die direkte Wartung, beispielsweise in der Turbine einer Windturbine, eingesetzt wird, bietet Perimeter-Sicherheit und kann den externen Zugriff auf ein spezielles Remote-Netzwerk begrenzen. Sie kann sogar so konfiguriert werden, dass der Zugriff nur zu bestimmten Zeiten oder für ein spezielles Wartungsprogramm möglich ist.
Darüber hinaus kann sie die Datenübertragung eines kompletten Windparks sicherstellen und verschlüsseln, um zu gewährleisten, dass die Daten über die erzeugte Strommenge leicht das zentrale Rechenzentrum erreichen können. Um physischen Speicherplatz zu sparen, kann die Next Generation Firewall praktisch auf der gleichen Infrastruktur wie andere Komponenten ausgeführt werden – in jeder gängigen Hypervisor-Umgebung.

Wichtige Komponenten und Anwendungsfälle, die Clavister zur idealen Wahl für wichtige Infrastrukturen machen:

- Voll ausgestattete Firewall mit Anwendungsfällen der nächsten Generation, die einen soliden Schutz des Netzwerkperimeters bieten.
- VPN mit starker Verschlüsselung garantiert, dass Ihre sensiblen Informationen vertraulich bleiben.
- Zentralisiertes Management und Betrieb sorgen dafür, dass die IT-Sicherheitsadministratoren zeitnah über Vorfälle und mögliche Verstöße informiert werden.
- Als virtualisierte Next Generation Firewall bietet sie alle Anwendungsfälle und Funktionen mit einem extrem niedrigen Platzbedarf, die in praktisch jeder Hypervisor-Umgebung installiert werden kann.

Hier erfahren Sie mehr über die Lösungen für wichtige infrastrukturen von Clavister:
www.clavister.com/critical (Auf Englisch)

Zentrale Individualkontrolle mit sicherer Identifizierung

Bildung & öffentlicher Bereich

Neue Netzwerktechnologien wie eLearning, Online-Zusammenarbeit und Geräte haben in vielen Bildungseinrichtungen die Lernerfahrung verbessert. Aber mit diesen neuen Technologien und der ständig steigenden Anzahl von Geräten besteht die Notwendigkeit, Netzwerke für den Zugriff zu skalieren und gleichzeitig zusätzliche Sicherheit zum Schutz sensibler Systeme und Informationen bereitzustellen. Darüber hinaus arbeitet der öffentliche Sektor mit besonders sensiblen und kostbaren Daten sowie mit empfindlichen und teuren Geräten, die einen besonderen Schutz erfordern.

An öffentlichen Orten wie im Schulgelände sind strenge Vorschriften erforderlich, damit kontrolliert wird, welche Inhalte angezeigt werden und welche Internetdienste genutzt werden können.

Bildungsinstitute und lokale Regierungen benötigen eine flexible Sicherheitslösung, die ihnen die Befugnis gibt, den Zugang auf einer sehr granularen Ebene zu kontrollieren, während sie gleichzeitig volle Einsicht in alle Vorgänge haben, um Vorfälle überprüfen und zurückverfolgen zu können.

Fallstudie: WiFi in Klassenzimmern mit Lehrerkontrolle

Alle Schüler und Lehrer sind mit dem WLAN-Netzwerk der Schule verbunden und authentifiziert. Studenten, die keinen Unterricht haben, haben Zugang zum Internet, während Lehrer in der Klasse die Macht haben, den Zugang zum Internet vorübergehend zu blockieren, um die Aufmerksamkeit der Schüler auf den Unterricht zu richten. Ein temporärer Zugriff kann bereitgestellt werden, damit die Schüler Informationen zu einem Thema finden können. Oder es kann eine Anwendungsfilterung verwendet werden, um nicht-pädagogische Nutzung – wie soziale Medien – eine Zeit lang zu blockieren. Die Firewall sichert das Netzwerk und bietet Filterrichtlinien für Webinhalte, um sicherzustellen, dass auf dem Schulhof kein unerwünschtes Material eingesehen wird.

Wichtige Komponenten und Anwendungsfälle, die Clavister zur idealen Wahl für Schulen und den öffentlichen Sektor machen:

• Identifizierung durch einen Sensibilisierungsagenten mit Integration in WLAN-Netzwerke, der die Identifizierung einzelner Endbenutzer ermöglicht und spezifische Richtlinien anwendet.

• Web-Inhalte und Anwendungsidentifikation und -kontrolle ermöglichen Lehrern die Kontrolle darüber, wie die Zeit genutzt wird.

• Zentralisiertes Management und funktionsbasierter Zugang, der Lehrern die Werkzeuge zur Kontrolle des Internetzugangs im Klassenzimmer bietet..

Hier erfahren Sie mehr über die Lösungen für Bildung und öffentliche Bereiche von Clavister:
www.clavister.com/schools (Auf Englisch)

Sichere Cloud mit minimalen Ressourcen

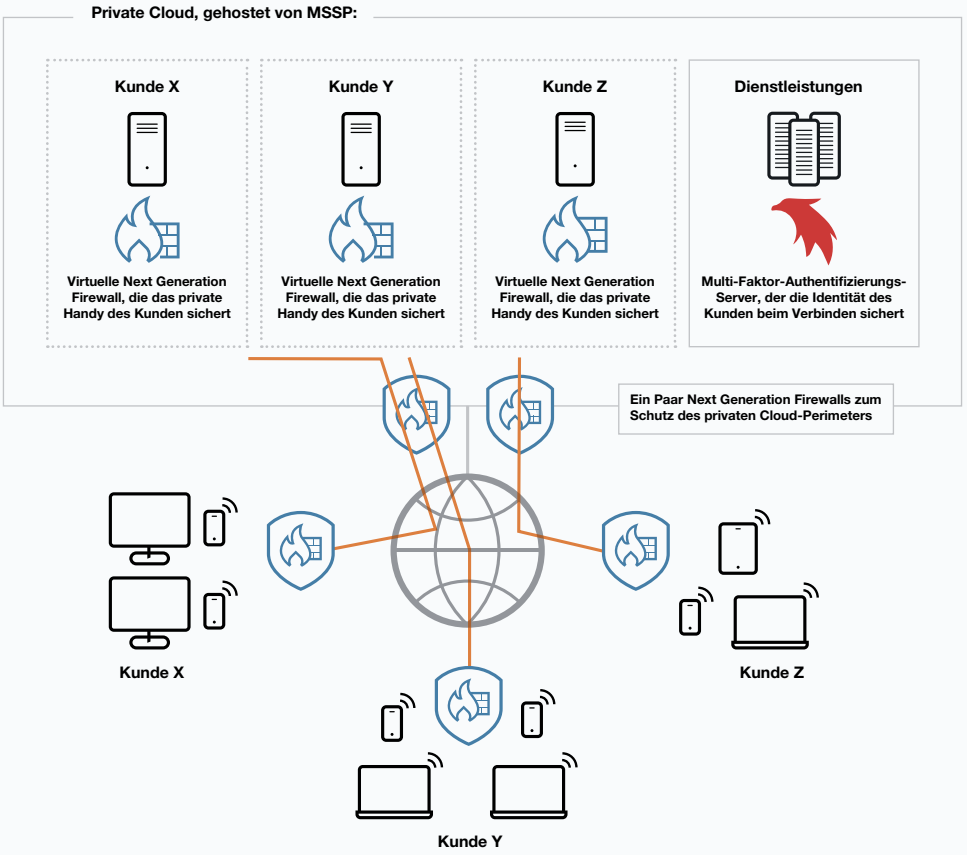
Anbieter von Managed Security Service

Aufgrund der Bedeutung und der erhöhten Komplexität der Sicherheitsinfrastruktur steigt die Zahl der Unternehmen, die sich dafür entscheiden, Betrieb und Wartung an eine Drittpartei auszulagern. Systemintegratoren und lokale Wiederverkäufer erweitern ihr Angebot, um Sicherheit als Managed Service bieten zu können.

Clavisters Lösungen sind ideal für den Einsatz durch Anbieter von Managed Security Services (MSSP) und können in Kombination mit anderen gehosteten Diensten angeboten werden. Denn die Software ist im Appliance- und auch im virtualisierten Format verfügbar und kann sowohl im Rechenzentrum zum Schutz der Cloud-Ressourcen als auch vor Ort eingesetzt werden.

Fallstudie: Sichere virtuelle Zellen

IT-Dienste wie Remote Desktop, Backup und Fileserver werden vom Dienstleister an kleine und mittlere Unternehmen angeboten. Die Dienste werden in dedizierten virtuellen Maschinen erstellt, die in einer privaten Cloud-Umgebung gehostet werden. Die Cloud-Infrastruktur wird durch ein dediziertes Paar von Next Generation Firewalls geschützt, die Perimeterschutz bieten, während die virtuellen Maschinen des Kunden jeweils durch dedizierte virtualisierte Next Generation Firewalls geschützt sind. Ein sicheres SD-WAN wird eingerichtet, um das Kundennetzwerk direkt mit den virtuellen Maschinen zu verbinden und so eine virtuelle sichere Zelle mit End-to-End-Sicherheit und vollständigem Datenschutz zu bieten.



Wichtige Komponenten, die Clavister zur idealen Wahl für Anbieter von Managed Security Service machen:

- Die virtualisierte Next Generation Firewall bietet alle Anwendungsfälle und Funktionen mit einem extrem niedrigen Platzbedarf, die in praktisch jeder Hypervisor-Umgebung installiert werden kann.
- Zentralisiertes Management mit Mandantenfähigkeits-Unterstützung, die es ermöglicht, große Bereitstellungen für mehrere Kunden ganzheitlich und effizient zu verwalten (Tausende von virtuellen Bildern).

Hier erfahren Sie mehr über die MSSP-Lösungen von Clavister:

www.clavister.com/mssp (Auf Englisch)

Next Generation Firewalls – Geräte und Virtuelles für die Cloud

Produktportfolio

Clavister bietet eine große Auswahl an Geräten, von Desktop-Modellen für kleine Büros bis hin zu Rack-montierbaren Modellen
für Serverräume in mittelgroßen Unternehmen. Rechenzentrumsmodelle für größere Unternehmen und Dienstleister umfassen redundante und Hot-Swap-fähige Stromversorgungen und unterstützen eine Reihe von Schnittstellenmodulen, mit denen Sie die Portkonfiguration anpassen können. Die Anwendungsfälle sind auf allen Plattformen verfügbar, einschließlich der virtualisierten Software, die auf allen modernen Hypervisoren läuft und auch zur Sicherung des Perimeters Ihrer virtuellen Maschinen verwendet werden kann.

clavister		 Desktop	 Server Room	 Data Center	 Virtual – Cloud
Modell		E10 – E80	W20 – W30	W40 – W50	V2 – V10
Kapazität	**Firewall**	1 – 4 Gbps	4 – 10 Gbps	10 – 55 Gbps	300 Mbps – 10 Gbps*
	VPN	100 Mbps – 1 Gbps	1 – 2 Gbps	2 – 8 Gbps	150 Mbps – 5 Gbps*
Schnittstellen		4-6 x 1GbE	6 – 9 1GigE W30 unterstützt ein Schnittstellenmodul	8 GigE or 4 x 10GbE pro Schnittstellenmodul	3 – 10 Schnittstellen unterstützt
Unterstützte Hypervisoren		n/a			VMware vSphere, KVM, Microsoft Hyper-V, OpenStack
Anforderungen an Ressourcen		n/a			256 MB – 4 GB oder RAM, 256 MB Speicher, 1 vCPU
Hochverfügbarkeit		Optional	Active-Passive, Active-Active und Active-Passive-Active		Ja
Geschätzte Anzahl der Benutzer		10 - 25	100 - 200	n/a	n/a
Technologien		All platforms include support for Universal Treat Management (UTM) and Next Generation Firewall (NGFW) technologies including IDS/IPS, Antivirus, Anti-Spam, IP Reputation, Geo Fencing, Application Control/DPI and Web Content Filtering – depending on support subscription type.			
Anwendungsfälle		Alle	Alle	Alle	Alle

** Die tatsächliche Leistung hängt von Host/Server-Hardware, Hypervisor usw. ab.*

Konfigurationsmanagement und Betriebssoftware

Ganzheitliche End-to-End-Steuerung

Die Next Generation Firewalls von Clavister bieten mehrere Schnittstellen für die Konfiguration und Verwaltung. Eine moderne Web-GUI mit Assistenten für die schnelle Einrichtung ist enthalten, aber auch direkter CLI-Zugriff und APIs für die Konfigurationsautomatisierung sind verfügbar.

Im Lieferumfang der Softwarelizenz ist eine zentrale Verwaltungssoftware enthalten, die für alle installierten Sicherheitsgateways verwendet werden kann. Diese Software heißt InControl und ermöglicht es dem Administrator, während des Betriebs Änderungen vorzunehmen, ohne die Verbindungen zu unterbrechen. Die generierten Berichte sind vollständig anpassbar und können die gewünschten Informationen auch grafisch darstellen. Auch ist eine feinskalierbare Live-Überwachung über ein anpassbares Dashboard enthalten, die gewährleistet, dass z. B. VPN-Tunnel oder Internetverbindungen permanent überwacht werden können.

Selbstverständlich können Clavister-Lösungen auch in bestehende Überwachungssysteme wie Nagios-basierte Systeme integriert werden. Die Protokolle können auch für die weitere Auswertung auf alternativen Plattformen wie syslog oder Splunk verwendet werden. Die notwendigen Einstellungen können einfach und bequem vorgenommen werden.

Hier erfahren Sie mehr über die Produktpalette von Clavister:

www.clavister.com/product-models (Auf Englisch)

SECURITY BY SWEDEN

Die Wikinger sind hier, um uns zu beschützen

Clavister ist ein schwedisches Cybersecurity-Unternehmen, das glaubt, dass robuste Netzwerksicherheit in jedermanns Interesse liegt. Mit einem sowohl virtuellen als auch physischen Systemansatz schützen wir die Geschäftskontinuität und stellen sicher, dass unsere Kunden die bestmögliche Sicherheit haben, um vor den wachsenden Bedrohungen geschützt zu sein. Wir haben vielleicht Schwerter gegen Codes eingetauscht, haben aber immer noch unseren Wikingergeist, der uns glauben läßt, dass die beste Cyber-Verteidigung ein starker Angriff mit Sicherheit ist.

Clavisters Schwedischsein hebt uns hervor

Schweden gelten als innovativ und aufmerksam, hören den Kunden zu und bieten Kundendienst der Spitzenklasse. Clavister beschäftigt qualifizierte Mitarbeiter mit über 50 verschiedenen Nationalitäten. Dennoch befinden sich alle Entwicklungs- und Support-Einrichtungen in Schweden. Auf diese Weise können wir sehr beweglich sein und hervorragenden Kundenservice bieten, der Jahr für Jahr hoch bewertet wird. Security By Sweden bedeutet vertrauenswürdige, seriöse und flexible Produkte, um Ihr Unternehmen zu schützen.