Absicherung

Kritischer Infrastrukturen

durch Clavister

Kritische Infrastrukturen

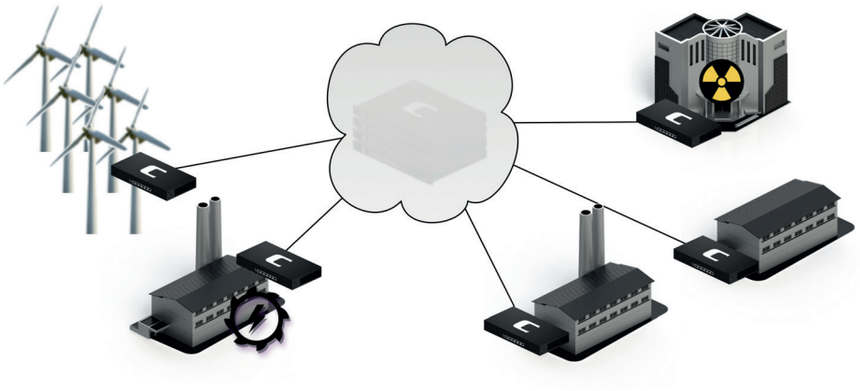
Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das (staatliche) Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

> **Auszug IT-Sicherheitsgesetz**
>
> II.1.1 Einhaltung von Mindestanforderungen an die IT-Sicherheit
>
> „Betreiber kritischer Infrastrukturen sollen verpflichtet werden, spätestens zwei Jahre nach Erlass […] organisatorische und technische Mindestanforderungen zur Vermeidung von Beeinträchtigungen ihrer informationstechnischen Systeme und Prozesse zu erfüllen, soweit diese für den Betrieb ihrer kritischen Infrastrukturen erforderlich sind.“

In Deutschland werden u.a. folgende Sektoren den Kritischen Infrastrukturen zugeordnet:

- Behörden, Verwaltung und Justiz (staatliche Einrichtungen)
- Energie (Elektrizität, Kernkraftwerke, Mineralöl, Gas)
- Versorgung (Lebensmittel- und Wasserversorgung, Gesundheits-, Notfall- und Rettungswesen, Katastrophenschutz, Entsorgung)
- Informationstechnik und Telekommunikation (Telekommunikation, Informationstechnologie)

clavister-sol-protecting-critical-infrastructures_2018.indd 1 2017-12-27 19:10:23



Schematische Darstellung eines Kommunikationsnetzes / Smart-Grid

Europäische Sicherheit für Infrastrukturbetreiber

Energieversorger, Stadtwerke und Netzbetreiber haben daher vieles gemeinsam. Durch das IT-Sicherheitsgesetz sind sie verpflichtet, sowohl die Kommunikations- wie auch die Prozessnetze vor unbefugten Zugriffen zu schützen.

Dies beinhaltet nach dem heutigen Stand der Technik nicht nur klassische Firewalling-Funktionalitäten, sondern auch sogenannte Next-Generation-Firewall-Funktionen, die es erlauben die Kommunikation zwischen herkömmlichen Netzen wie etwa in Büros und Verwaltungen und den SCADA-(Supervisory Control and Data Acquisition) Netzen für die Prozesssteuerung und Überwachung auf der einen Seite zu ermöglichen, auf der anderen Seite diesen Datenverkehr aber auch separieren und kontrollieren zu können.

An dieser Stelle kommen Lösungen von Clavister zum Einsatz, die beispielsweise das 104-Protokoll (IEC 60870-5-104) nicht nur erkennen können, sondern es vollumfänglich innerhalb des Netzwerkes reglementieren können.

Alle Clavister Appliances werden mit dem von Clavister selbst entwickelten Betriebssystem cOS Core ausgeliefert.

Durch diese komplette Eigenentwicklung der Software in Schweden inklusive des Verzichts auf OpenSource-Komponenten sind Clavister Firewalls 100% Backdoor-frei. Ebenfalls sind auch Schwachstellen wie „Heartbleed“, „Shellshock/Bash“, „Ghost“ oder „FREAK“, aber auch noch zu entdeckende OpenSource-Bugs in Clavister-Lösungen nicht möglich.

Eine einheitliche Software auf allen Systemen stellt sicher, dass es keine Funktionsunterschiede zwischen den Plattformen gibt.

Nicht nur Next-Generation-Firewall

Im Gegensatz zu den meisten anderen auf dem Markt erhältlichen Securitysystemen ist Clavister keine reine Applikationskontrolllösung. Stattdessen bietet Clavister bewährte Funktionalität von UTM-Firewalls in perfekter Kombination mit modernster Next-Generation-Firewall-Technologie in einer einzigen hochperformanten Appliance.

Der Vorteil davon liegt klar auf der Hand. NGFW-Systeme heute verfügen nicht über die Funktionalitäten, die eine UTM bietet und müssten daher als zusätzliches Gerät im Netzwerk betrieben werden. Dies bedeutet jedoch doppelten Aufwand in Bezug auf Planung und Konfiguration, doppelte Kosten bei Anschaffung und Wartung sowie doppelte mögliche Fehlerquellen.

Gerade im Bereich Prozessnetze und Fernwartungszugriffe werden jedoch nicht nur sichere, sondern auch kostengünstige Lösungen benötigt, was dazu führt, dass aus Gründen der Kostenersparnis häufig eine ineffiziente Lösung beschafft wird. Dies lässt sich mit den Lösungen von Clavister wirkungsvoll vermeiden, denn hier erhält man alles aus einer Hand und innerhalb einer Appliance.

Lang erprobte und bewährte Funktionen, sowie neueste Sicherheitstechnologien, die auch den Angriffen von morgen gewachsen sind. Die Clavister Appliances unterscheiden sich lediglich in Bezug auf die Hardware sowie die dadurch zu erreichende maximale Leistung und stellen so die perfekte Wahl für eine Sicherheitslösung dar, die in den unterschiedlichsten Bereiche des Netzwerkes eingesetzt werden kann.

clavister-sol-protecting-critical-infrastructures_2018.indd 2 2017-12-27 19:10:23

Traffic Management

Alle Clavister Appliances bieten die Möglichkeit, sowohl Bandbreitenmanagement wie auch Load-Balancing zu nutzen.

So können etwa mehrere Internetverbindungen zeitgleich genutzt und der Datenverkehr auf diese aufgeteilt werden.

Auch eine Priorisierung oder Zuweisung von bestimmten Bandbreiten einer Anwendung ist darüber zu realisieren.

VPN

Alle Clavister Appliances bieten die Möglichkeit, verschiedene Formen von VPN zu nutzen.

Es werden unter anderem IPsec, L2TP und SSL unterstützt.

Die in der Lizenz angegebene maximale Anzahl an Tunneln legt hierbei nur die gleichzeitig möglichen Verbindungen fest, nicht aber die Art oder Anzahl der konfigurierbaren.

True Application Control

Alle Clavister Appliances bieten die Möglichkeit, True Application Control zu nutzen.

Darüber lassen sich Anwendungen innerhalb des Netzwerkes und zwischen Netzwerk und Internet sowohl analysieren wie auch steuern, wie etwa das 104-Protokoll, aber auch Skype, SQL queries, Facebook Chat oder VoIP.

VLAN

Alle Clavister Appliances bieten die Möglichkeit, VLAN zu nutzen.

Diese Funktion ermöglicht es, in einem einzigen physikalischen Netzwerk mehrere virtuelle Netzwerke zu erstellen und zu verwalten.

So kann ohne gesonderte Verkabelung mit verschiedenen Segmenten gearbeitet werden, die auch vom Datenverkehr voneinander getrennt sind, obwohl sie die gleiche Infrastruktur nutzen.

User Identity Awareness

Alle Clavister Appliances bieten die Möglichkeit, User Identity Awareness (UIA) zu nutzen.

Diese Funktion ermöglicht sowohl auf einzelnen Arbeitsplätzen wie auch in Terminalserverumgebungen das Erstellen und Nutzen von benutzerbasierten Regelwerken, ohne dass hierzu Software auf einem Domaincontroller installiert werden muss.

Vorteile von Clavister-Lösungen

Hohe Performance
Kein Risiko von Durchsatzeinbußen und langsamen Diensten mehr.

Volles UTM Paket
Alle UTM-Funktionen sind immer verfügbar (Antivirus, WebContent-Filter, IDP).

Next-Generation-Firewall
Application Control ist immer verfügbar.

Skalierbare Lizenzen
Zukunftssicheres Lizenzieren nach dem Pay-as-you-grow-Prinzip, ohne Hardwaretausch.

Flexible Interfacemodule
Kosten sparen und die Lebensdauer der Hardware verlängern, durch das Austauschen von Modulen anstelle der kompletten Appliance.

Eine Software für alle Systeme
Identische und umfangreiche Funktionen auf allen Clavister Appliances, ohne Einschränkungen oder Kompromisse.

Zentrales Management & Reporting
Das zentrale Management-Tool „Clavister InControl“ ist immer verfügbar.

Sicher – Ohne Backdoors oder OpenSource
Schwedische Technologie ohne Hintertüren oder Open-Source. Kein PRISM, kein CALEA, kein Heartbleed, kein Ghost oder ähnliches.

Zwei-Faktor-Authentifizierung

Alle Clavister Appliances bieten die Möglichkeit, Zwei-Faktor-Authentifizierung zu nutzen.

Dadurch können etwa Hardwaretoken oder Smart-Cards zusätzlich zu der Verwendung von Benutzernamen und Passwort für die Anmeldung am System verwendet werden, um die Sicherheit zu erhöhen.

IP Reputation

Eines der besten Werkzeuge für eine starke IT-Sicherheit ist ein IP Reputation Service, der von Minute zu Minute immer die aktuellsten Daten über schädliche IP-Adressen bereithält. Bei über vier Milliarden IP-Adressen und darunter mehr als zwölf Millionen Malware und Viren verbreitende, bleibt die Netzwerksicherheit so immer auf dem neuesten Stand.

clavister-sol-protecting-critical-infrastructures_2018.indd 3 2017-12-27 19:10:23

Zentrale Verwaltung aller Security Gateways

Für einen reibungslosen Betrieb ist es wichtig, die vorhandenen Security-Lösungen auch vollumfänglich und einfach administrieren und überwachen zu können.

Alle Clavister Appliances können daher nicht nur einzeln über eine Weboberfläche administriert werden, in dem für die Appliances verfügbaren Service ist auch immer gleichzeitig eine Lizenz für die Nutzung des zentralen Managements „Clavister InControl“ mit enthalten. Die Clavister-Technologie ermöglicht es dem Betreiber hierbei, auch während des laufenden Betriebes Änderungen vorzunehmen, ohne dass Verbindungen unterbrochen werden. Ein zusätzlicher Schutzmechanismus verhindert außerdem ein versehentliches „Aussperren“ des Administrators und erlaubt so wirklich sichere Fernwartung der Systeme.

Neben der revisionssicheren und rollenbasierten Verwaltung von allen Clavister-Lösungen in einer einheitlichen Oberfläche, bietet das System zentrale Logging- und Auswertungsmöglichkeiten ohne weitere Kosten. Die generierbaren Reports sind komplett individuell anpassbar und können die gewünschten Informationen auch grafisch darstellen. Ebenso ist ein fein skalierbares Live-Monitoring über ein anpassbares Dashboard enthalten und stellt sicher, dass etwa VPN-Tunnel oder Internetverbindungen dauerhaft überwacht werden können.

Natürlich können Clavister-Lösungen auch in ein bereits vorhandenes Monitoring, wie etwa Nagios-basierte Systeme, integriert werden. Auch die Logs können auf alternativen Plattformen wie syslog oder SPLUNK zur weiteren Auswertung genutzt werden Die dafür notwendigen Einstellungen können einfach und komfortabel genau wie die restliche Konfiguration über das zentrale Management vorgenommen werden.

Über Clavister

Gegründet im Jahr 1997, ist das schwedische Unternehmen Clavister mittlerweile ein führender Network-Security-Anbieter.

Die preisgekrönten Lösungen bieten ein extrem gutes Verhältnis von Preis zu Performance und Funktionalität, um sicherzustellen, dass Unternehmen den bestmöglichen Schutz gegen die digitalen Bedrohungen von heute und morgen erhalten.

Um bei der Entwicklung der Systeme Leistungsfähigkeit, Sicherheit und Wirtschaftlichkeit zu erreichen, wird ein eigens entwickelter Kernel eingesetzt. Auf der Firewall kommt somit kein Betriebssystem wie Unix, Linux oder Windows zum Einsatz.

Durch diese komplette Eigenentwicklung der Software in Schweden inklusive des Verzichts auf OpenSource-Komponenten sind Clavister Firewalls 100% Backdoor-frei, dies bestätigt Clavister seinen Kunden schriftlich bereits seit 2003.

Ein weiterer Effekt ist, dass Bugs wie „Heartbleed“, „Shellshock/Bash“ und „Ghost“, aber auch zukünftige, noch zu entdeckende Schwachstellen in OpenSource-Software Clavister-Lösungen dadurch nicht betreffen.

Eine einheitliche Software auf allen Systemen stellt sicher, dass es keine Funktionsunterschiede zwischen den Plattformen gibt. Außerdem hat Clavister ein sehr übersichtliches Lizenzmodell und verzichtet auf Userlizenzen, Feature-Bundles, Pakete o.ä. Ebenso wird das zentrale Management immer kostenfrei mitgeliefert und gewährleistet so minimalen Wartungsaufwand und flexible Konfigurationsmöglichkeiten.

Dadurch ist es möglich, kleine wie auch große Unternehmen mit einem schlüsselfertigen, hocheffizienten Next-Generation-Firewall-System auszustatten, ohne auf die bewährten UTM-Funktionalitäten zu verzichten oder eine weitere Appliace dafür einsetzen zu müssen.

Für weitere Informationen über Clavister-Lösungen und Services besuchen Sie bitte: www.clavister.com.

Kontaktieren Sie Ihren Clavister-Ansprechpartner für weitere Informationen oder finden Sie einen Clavister-Partner in Ihrer Nähe: www.clavister.com/about-us/contact-us.

ICSA labs CERTIFIED FIREWALL - CORPORATE

EAL4+

Ihr Clavister-Ansprechpartner

clavister
CONNECT . PROTECT

Clavister DACH, Paul-Dessau-Str. 8, D-22761 Hamburg, Germany
Phone: +49 40 411259-0 **Fax:** +49 40 411259-299 **Web:** www.clavister.com

Copyright © 2016 Clavister AB. All rights reserved. The Clavister logo and all Clavister product names and slogans are trademarks or registered trademarks of Clavister AB. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. Information in this document is subject to change without prior notification.