TRIOVEGA
SECURELY SHAPING YOUR FUTURE

edge.SHIELDOR
Technische Daten

Schützen Sie Ihre Industrie-maschinen vor Angriffen von innen und außen

Mit dem edge.SHIELDOR verhindern Sie den unkontrollierten Informationsaustausch von Industriemaschinen. Durch den Einsatz von ausschließlich benötigten Diensten und der Segmentierung sowie Überwachung dieser Dienste wird das Anlagen-Netzwerk (OT-Netzwerk) von dem übergeordneten IT-Netzwerk getrennt. Möglichen Angreifern wird zusätzlich die gesamte Netzwerktopologie verschleiert, so dass bei einer Kompromittierung eines Teilnetzwerkes nicht auf weitere Teilnehmer hinter dem Gateway zugegriffen werden kann.

Zusätzlichen Schutz bietet die Funktionalität, veraltete und unsichere Protokolle in (nach heutigem Kenntnisstand) sichere Protokolle umzuwandeln. Dadurch können die im OT-Netzwerk zu schützenden Einheiten unterbrechungsfrei betrieben werden und die Sicherheit ist durch den edge.SHIELDOR durchgehend gewährleistet. Unterstützt werden hierbei gängige administrative Dienste und deren Protokolle. Nutze Sie zudem die individualisierbare Konfigurationsoberfläche: Web-Dienste, Logging und Nutzer-Authentifikation sind von außen mit Zugriffsberechtigung abrufbar.

Firewall und Gateway

- Einfache Inbetriebnahme über zentrale Management-Oberfläche
- IP-Konfiguration des Steuerrechners
- Gesicherte webbasierte Konfiguration über HTTPS-Verschlüsselung
- Positive und negative Filterregeln (IP-, Port-, Zeitgesteuert)
- Host- und Netzwerkbasiertes Intrusion Detection System (IDS) und Intrusion Prevention System (IPS) – Identifizierung und Blockierung unerwünschter Kommunikationsversuche
- Abwehr von DoS-Angriffen
- Betriebsart: Kein Routing
- Betriebsart: Standard-Router
- Betriebsart: NAT-Router
- Integration der Insel über eine einzige Intranet-IP
- Static NAT für 1:1-Mapping von Intranet-IPs auf Insel Hosts

Unterstützte Protokolle

- IPv4 / IPv6, TCP/UDP/ICMP/SCTP
- IEEE 802.1X Ethernet Authentifizierung
- VLAN (IEEE 802.1Q)
- DHCP Server, Client
- DNS-Server
- Transfer zu Azure/IoT-Hub, AWS/IoT-Core und weiteren

Weitere Schnittstellen auf Anfrage

edge.SHIELDOR
Technische Daten

Gesicherter Zugriff und Bedienung

- Eigene Benutzerverwaltung
- Tokenbasierte Authentifizierung
- LDAP-Integration eines firmenweiten LDAP
- Zwei-Faktor Authentifizierung
- Server: Sichere VPN-Einwahl in die Insel mit Windows-, Linux-, MacOS-, Android-, IOS-Clients
- Firewall-Zugriffsteuerung der VPN-Clients (IP-, Port-, zeitgesteuert)
- VPN-Fernzugriff von externen Netzwerk-Teilnehmern wie Hersteller und Service-Anbieter
- Verschlüsselung: SSL / TLS v1.3 (Firmenzertifikate importierbar)
- Zwei-Faktor Authentifizierung: Zertifikatsauthentifizierung
- Alle Service-/Management-Dienste deaktivierbar
- Alle Dienste durch REST-API konfigurierbar (OpenAPI-Definition)
- Seamless Update (wenn möglich), sonst automatisches Update im Service-Fenster
- Interaktion über / Kollaboration von mehreren Produktinstanzen
- Vereinfachte Konfiguration und Analyse durch Machine-Learning

Unterstützte Ports

- HTTP/S-Server (Port 80, 443)
- FTP-Server (Port 21)
- SMB-Server (Port 139, 445)
- SMTP-Sever (Port 25, 587)
- LDAP-Server (Port 389, 636)
- FTP(S)-Server (Port 21, 30000-30009)
- Benutzerdefinierte Portweiterleitungen aus dem OT-Netzwerk (optional zus. Verschlüsselung)
- Benutzerdefinierte Portweiterleitungen aus dem IT-Netzwerk

Logging / Protokollierung von Informationen

- Aus Transferarten, Diensten, Authentifikationen, Nutzeraktionen, Konfigurationsänderungen, Firewall, IP-Weiterleitungen
- Weiterleitung an zentrales Firmen Logging-System
- Automatische Analyse der Log-Daten und Informierung der Nutzer:innen

Backup, Wiederherstellung und Datensicherung

- 120 Stunden Datenhaltung
- Automatisches Backup und Wiederherstellung auf externes System

Transfervarianten

File-Transfer / -Synchronisierung

- Filterung durch Positiv- und Negativ-Listen (Dateinamen, Dateitypen, SHA512-Checksummen)
- Virenscan inkl. Abwehr von Viren, Ransomware, Botnet und Spyware
- Unterstützte Betriebssysteme: Windows 10 oder neuer (nur IT-Netzwerk), Windows 7, Windows XP, Windows NT (Protokoll: SMB NTLM v1)

Remote-Transfer

Protokolle: RDP, VNC, SSH, Telnet

Prozessdatentransfer

- Protokolle: OPC-UA Server/Client,
- Modbus/TCP, S7 Protokoll (RFC 1006)

Support Plan

Basis Support und Premium Support auf Anfrage verfügbar.

Sie möchten mehr über den edge.SHIELDOR erfahren?

Schreiben Sie uns gerne direkt an: **sales@triovega.com**

TRIOVEGA GmbH
Isaac-Newton-Straße 8
23562 Lübeck, Deutschland
T: +49 451 39771 0
E: info@triovega.com

MKTD-v007-20240201 -Öffentlich