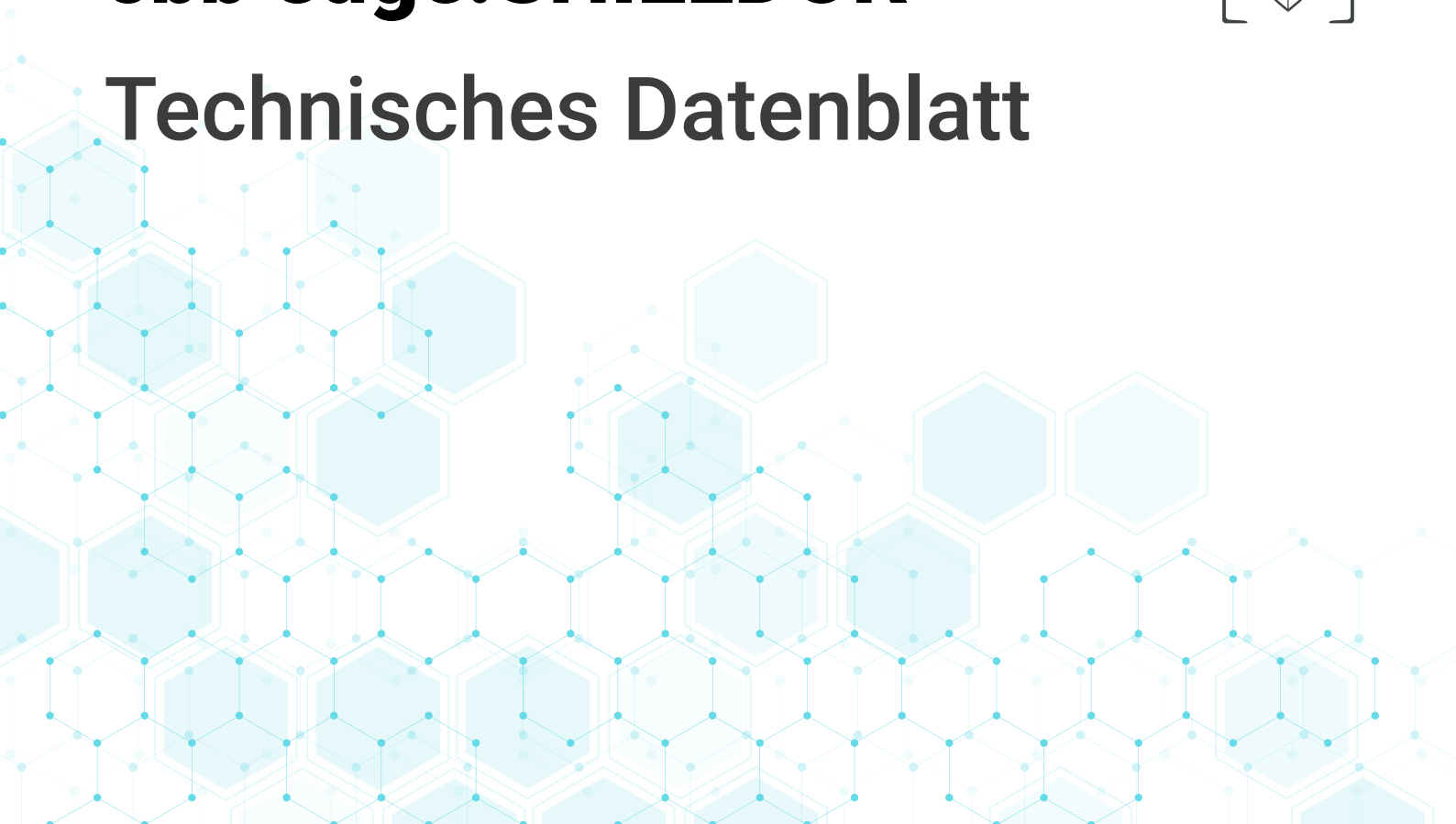




cbb edge.SHIELDOR



Technisches Datenblatt



Schützen Sie Ihre Industriemaschinen vor Angriffen von innen und außen

Mit dem cbb 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 Maschinen / Anlagen-Netzwerk (OT-Netzwerk) von dem übergeordneten IT-Netzwerk getrennt. Möglichen Angriffen 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 cbb edge.SHIELDOR durchgehend gewährleistet. Unterstützt werden dabei nicht nur gängige Industrieprotokolle, sondern auch administrative Dienste und Protokolle. Nutzen Sie zudem die individualisierbare Konfigurationsoberfläche: Web-Dienste, Maschinen-Status, Logging und Nutzer-Authentifizierung sind von außen mit Zugriffsberechtigung abrufbar.

Technische Daten cbb edge.SHIELDOR

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 netzwerkbasierendes 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
- DHCP Server, Client
- SNMP-Server
- NTP-Server
- DNS-Server
- Modbus-TCP-Client, Modbus-RTU-Client (mit Zusatzadapter)
- Siemens-SPS-Client
- OPC-UA-Client
- ProfiNet
- REST-Client
- MQTT-Client
- Transfer zu Azure/IoT-Hub, AWS/IoT-Core und weiteren

Unterstützte Protokolle

- IPv4 / IPv6, TCP/UDP/ICMP/SCTP
- IEEE 802.1X Ethernet Authentifizierung
- VLAN (IEEE 802.1Q)

Gesicherter Zugriff und Bedienung

- Eigene Benutzerverwaltung
- 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: TOTP / Zertifikats-authentifizierung
- 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)
- OPC-UA-Server (Port 4840)
- 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)
- SMB-Server (Port 139, 445)
- 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

- Filterung durch Positiv- und Negativ-Listen (Dateinamen, Dateitypen, SHA512-Checksummen)
- Virenskan 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

Data-Transfer

- Erfassung von Prozessdaten durch den Einsatz einer Middleware Architektur
- Aufbereitung von Daten (Verrechnung oder Überwachung)
- Weiterleitung der Daten in gewünschtem Zielprotokoll

Support Plan

Basis Support und Premium Support auf Anfrage verfügbar.



cbb software GmbH

Isaac-Newton-Straße 8, 23562 Lübeck

T: +49 451 / 39 77 1 - 10 E: sales@cbb.de

www.cbb.de