OHP

IT-Security in der Fernwirktechnik

mit den neuen IT-Security Fernwirk-Steuerungen der @120- und Micro-Baureihe

Artikel 06/2020

Die Sicherheitslage in der Informationstechnik ist angespannter denn je

Im Jahresbericht (2019) zur IT-Sicherheit berichtet das Bundesamt für Sicherheit in der Informationstechnik (BSI) weiterhin von einer angespannten IT-Sicherheitslage sowie Zunahme der Qualität vieler Cyber-Angriffe.

Die Fernwirk-Steuerungen von OHP erfahren daher eine kontinuierliche Weiterentwicklung der IT-Sicherheits-maßnahmen, um die teils systemkritischen Daten auf den Geräten sowie bei der Übertragung zu schützen.

Besonders OHP reagiert mit den neuen Steuerungen ALU315, -316 und 317 der @120-Baureihe sowie ALU030 der Micro-Baureihe auf diese Anforderungen. Die Steuerungen werden diesen Forderungen in vielerlei Hinsicht gerecht und unterstützen Sie dank vielfältig konfigurierbarer IT-Sicherheits-Setups dabei Cyber-Angriffe abzuwehren. Bei entsprechender Konfiguration erfüllen die Steuerungen die **Anforderung für geschlossene Benutzergruppen zur Erbringung von Regelreserve.**

Darüber hinaus ist das Sicherheitskonzept und die OHP Dienstleistungen an das **BDEW Whitepaper 2.0** angelehnt.

Unser „Whitepaper IT-Security von OHP Fernwirkstationen“ unterstützt Sie bei der Implementierung mit ausführlichen Setups und Checklisten.

Die neuen IT- Security Fernwirk-Steuerungen der @120- und Micro-Baureihe

Die essentiellen Sicherheits-Features auf einen Blick

- ✓ Hochgradig verschlüsselte Datenablage
- ✓ Verschlüsseltes Root-Filesystem mit encrypted Container
- ✓ Speziell gesicherte Schlüssel
- ✓ Individuell gesicherte SD-Karte, Ablehnung von Fremd-SD Karten oder genereller Verzicht auf SD-Karte
- ✓ Schutz gegen Wiedereinspielen alter Daten
- ✓ Kontinuierliche Firmwarepflege zur Einhaltung neuester Sicherheits-standards
- ✓ Kontinuierliche Pflege und Updates der IT-Sicherheitsumgebung auf dem neuesten technischen Stand
- ✓ Firmwareupdate über Package Management
- ✓ Symmetrisches Verschlüsselungsverfahren
- ✓ Authentisierung der Kommunikations-partner per Zertifikat
- ✓ Schutz der Integrität von Nachrichten
- ✓ Perfect Forward Secrecy entsprechend IKEv2
- ✓ Dynamische Auffrischung von Schlüsselmaterial (Re-Keying)
- ✓ Verschlüsselungsoptionen mit OpenVPN oder strongSwan nach neuestem Stand der Technik
- ✓ IT-Sicherheitskonzept der OHP Fernwirkstationen getestet durch das Security Analysis & Incident Response Team (CSIRT) eines großen Energieversorgers

Die essentiellen Sicherheits-Features im Detail

Linux-Echtzeitbetriebssystem

Die Steuerungen setzen Embedded Linux als Betriebssystem ein. Dieses erlaubt eine stetige Weiterentwicklung der Firmware um die Anforderungen nach aktuellem Stand der Technik abzubilden.

Das Dateisystem des Embedded Linux (bestehend aus einer EXT4-Partition) ist dabei verschlüsselt. Der Schlüssel für das Dateisystem wird auf der Steuerung generiert und verlässt diese niemals.

- Cipher: aes-xts-plain64
- Key-Size: 512bit
- Hash: SHA256

Firewall auf der Steuerung

Auf den Steuerungen kommt eine Firewall zum Einsatz, welche nach dem Whitelist-Verfahren („Es ist alles verboten was nicht explizit erlaubt ist“) arbeitet.

Das heißt für jeden Dienst oder jedes Paket, dass auf der Steuerung arbeitet und per Netzwerk kommuniziert, muss eine entsprechende Regel innerhalb der Firewall-Konfiguration gesetzt werden.

Um diese Konfiguration möglichst einfach zu gestalten, können die Firewall-Regeln per MULTIPROG in einer einfachen Konfigurationsmatrix aktiviert werden. Innerhalb dieser Konfigurationsmatrix befinden sich die Firewall-Zonen, sowie die Regeln.

VPN mittels IPSec und strongSwan

Die Steuerungen unterstützen die Absicherung der VPN-Verbindung per IPSec. Dies erlaubt es der Steuerung verschlüsselte und authentifizierte Kanäle zur sicheren Kommunikation aufzubauen.

Für den Aufbau der IPSec Verbindungen kommt das strongSwan Software Paket zum Einsatz, welches aktiv weiterentwickelt und supportet wird. Ein bestechender Vorteil von strongSwan ist die schnelle Adaption neuer Konfigurationsmöglichkeiten.

Die wichtigsten Eckdaten der Konfigurationsmöglichkeiten:

- IKEv2 (IKEv1 auch möglich)
- Authentifizierung per:
  - x509 Zertifikate
  - PreSharedKey
  - EAP
- Verschlüsselungs- und Authentifizierungsverfahren nach dem aktuellen Stand der Technik und darüber hinaus mit Post Quantum Cryptography.

Sichere Übertragung der Konfigurationsdaten via TLS

Die Daten sowie die Anmeldung sind per TLS geschützt. Der Server auf der Steuerung lässt nur verschlüsselte Verbindungen zu, die dem TLS 1.2 Standard entsprechen.

Speicherung der Konfigurationsdaten im verschlüsselten Container auf der Steuerung

Dieser Container wird durch den Einsatz einer hybriden Verschlüsselung gesichert. Das kryptographische Verfahren RSA kommt für den asymmetrischen Teil zum Einsatz wobei AES für den symmetrischen Teil genutzt wird. Somit lassen sich die Systemressourcen (CPU und RAM) bei der Ver- bzw. Entschlüsselung optimal nutzen.

Doorman

Einsatz eines „Doormans“ als digitaler Türsteher für Firewall-Berechtigungen und Festlegung des Timeouts bis ein Dienst durch die Firewall wieder gesperrt wird, sobald keine weitere Übertragung stattfindet.

SSH Text Konsole

Es wird nun eine Konfigurationskonsole, die per SSH erreichbar ist, angeboten. SSH bietet den Vorteil gegenüber der Telnet Variante, dass diese nun nach dem aktuellen Stand der Technik abgesichert werden kann. Mit SSH wird ein marktübliches Werkzeug zum sicheren Fernzugriff bereitgestellt.

Anwendungsbeispiel

LEW Lechwerke

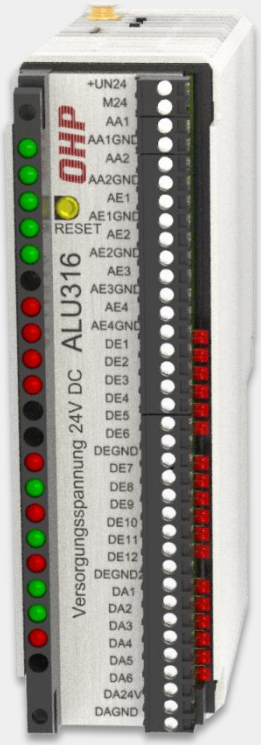
Für das virtuelle Kraftwerk ist bei der Lechwerke AG das Leitsystem ProWin mit dem Smart Grid Assistent ProSGA-VKW im Einsatz.

Die fernwirktechnische Datenerfassung im Bereich des virtuellen Kraftwerks erfolgt dabei über das Fernwirksystem @120 mit integrierten LTE-Modems.

Zur Steuerung und Überwachung der EEG-Anlagen sind mehr als 2.000 Micro-Fernwirksysteme im Einsatz.

IHRE VORTEILE AUF EINEN BLICK:

- IPSec VPN sowie Firewall direkt auf der Steuerung
- strongSwan für aktuellste Umsetzung des IKE-Protokolls
- Programmierung nach genormtem Standard IEC 61131-3
- modulare Erweiterbarkeit der Steuerung bis 32 EA-Module bei der Micro-Baureihe und 19 EA-Module bei der @120-Baureihe



@120 ALU316
Alles drin bei nur 4 cm Baubreite

- ✓ Linux Realtime OS mit extended IT-Security
- ✓ IEC 61131-3
- ✓ Ethernet
- ✓ RS485/232
- ✓ OnBoard-Modem
- ✓ 12 DE, 6 DA, 4 AE, 2 AA on board
- ✓ modular erweiterbar

stronSwan	TLS 1.2 SSH	Embedded Linux	IKEv2