Cyber-resiliente Netze für Energieversorger

Mit zunehmender Automatisierung wachsen die Anforderungen an die IT- und OT-Infrastruktur bei Energieversorgen. Ein hochverfügbares und sicheres Kommunikationsnetz wird zur zwingenden Voraussetzung für den zuverlässigen Betrieb. Die hohe wirtschaftliche und gesellschaftliche Bedeutung der Energieversorger macht diese Netze allerdings auch zu einem bevorzugten Ziel von Cyberangriffen. Mit neuen regulatorischen Anforderungen wie der NIS2- und RCE-Direktive hat die Europäische Gemeinschaft auf eine verschärfte Bedrohungslage reagiert. Im Folgenden werden die Anforderungen an die Kommunikationsnetze beschrieben und Lösungen für eine vorteilhafte Implementierung dargestellt.

Neue Anforderungen an die IT- und OT-Infrastruktur

Verschärfte Bedrohungslage

Wachsende Gefährdung: Betreiber kritischer Anlagen, Unternehmen mit Sicherheits-anforderungen und Regierungen digitalisieren ihre Prozesse und sind damit durch Cyber-Angriffe auf ihre Netze und IT-/OT-Infrastruktur gefährdet. Der aktuelle "Threat Landscape Report 2023" der ENISA und der "Stand der IT-Sicherheit in Deutschland im Jahr 2023" des BSI berichten von einer deutlichen Zunahme böswilliger Aktivitäten. Hinzu kommt, dass künstliche Intelligenz (KI) das Waffenarsenal von Cyber-Kriminellen erweitert hat.

Massive Angriffe: Im Mai 2023 wurde das dänische Energieversorgungsnetz durch koordinierte Angriffe auf 22 Unternehmen bedroht. Die Angreifer konnten sich Zugang zu einigen der industriellen Kontrollsysteme verschaffen. Einige Unternehmen mussten ihre operativen Systeme vom Netzverbund trennen. Dies war der größte Cyberangriff auf kritische Einrichtungen in Dänemark und kann als Warnung für Netze in anderen EU-Ländern verstanden werden.[1]

Quantencomputer: Viele Sicherheitsmechanismen basieren auf Algorithmen, die durch Quantencomputer kompromittiert werden können. Mit Post-Quanten Kryptographie (PQC) und Quanten-Schlüssel-austausch stehen Möglichkeiten für einen quantensicheren Schutz zur Verfügung. Die Implementierung dieser neuen Verfahren ist allerdings ein zeitaufwändiger Prozess und sollte daher zeitnah begonnen werden, um die kritischen Komponenten und Funktionen zuverlässig vor zukünftigen Angriffen durch Quantencomputer zu schützen.

[1] SectorCERT, The attack against Danish critical infrastructure, November 2023

Regulatorische Vorgaben

Kritische Infrastrukturen: Die Energieversorger gehören zu den kritischen Infrastrukturen und müssen Vorgaben zur Sicherstellung ihres Betriebs erfüllen. Die Einführung von Management-Systemen zur Informationssicherheit und zur Sicherstellung der Geschäftskontinuität ist vorgeschrieben. Schutzmaßnahmen müssen dem Stand der Technik entsprechen und Systeme zur Angriffserkennung sind erforderlich. Die Anforderungen ergeben sich aus dem BSI-Gesetz, der BSI-KritisV, dem IT-Sicherheitsgesetz 2.0 und dem Energiewirtschaftsgesetz.

Neue Gesetze: Im Jahr 2022 wurden zwei Direktiven zur Stärkung der Sicherheit von Kritischer Infrastruktur verabschiedet. Die Umsetzung dieser Vorgaben wird bis Oktober 2024 durch das NIS2-Umsetzungsgesetz und das KRITS-Dachgesetz erfolgen. NIS2 senkt die Schwellenwerte für die Einstufung von Unternehmen. Zukünftig muss die Supply Chain beim Schutz des Netzes einbezogen werden. Verschlüsselung wird ebenfalls vorgeschrieben. Das KRITIS-Dachgesetz stärkt die Widerstandskraft gegen physische Störungen.

Stand der Technik: Bei Maßnahmen zur Informationssicherheit sind die gesetzlichen Bestimmungen an den aktuellen „Stand der Technik“ angelehnt. Es sollte daher ein besonderes Augenmerk auf die Bereiche gelegt werden, in denen sich neue Schutz-Technologien etablieren und damit der Stand der Technik fortgeschrieben wird. In der Kryptografie werden traditionelle Algorithmen durch quantensichere Methoden ersetzt. Neuere Timing-Architekturen schützen vor Angriffen auf die Satelliten-basierte Zeitversorgung. Virtualisierung von Netzfunktionen ermöglicht eine agile und flexible Anpassung an sich verändernde Bedrohungslagen.

Digitale Transformation

IP/Ethernet Verbindungsnetz: Die Einführung neuer operativer Technologien sowie der Übergang zu Cloud-gehosteten Daten und Applikationen wirkst sich auf die im Verbindungsnetz verwendete Technologien aus. IP in Verbindung mit Ethernet schaffen einen Konvergenz-Layer, der von allen zukünftigen IT und OT-Anwendungen genutzt wird. Teilweise noch verwendete PDH- und SDH-Systeme verlieren weiter an Bedeutung.

Präzises Timing: Die Automatisierung stellt höhere Anforderungen an die Zeitverteilung im Netz. Nach IEC 61850 wird zukünftig eine Genauigkeit im µs Bereich an Umspannwerken notwendig sein. Ähnliche Anforderungen sind für eine effiziente Replikationen von Daten in der Cloud notwendig. Das Netz muss also in der Lage sein, hochpräzise Zeitinformation bereitzustellen.

Edge Cloud: Vielen Anwendungen können zentral in der Cloud gehostet werden. Zeitkritischen Funktionen und bestimmte Schutzfunktionen müssen allerdings am entfernten Standort eingesetzt werden. Hierfür kommen innovative Edge Cloud Lösungen zum Einsatz, die besondere Anforderungen an die Cybersicherheit stellen.

Lösungsportfolio für Cyber-resiliente Weitverkehrsnetze

Implementierung von Cyber-resilienten Netzen

Quantensichere optische Übertragung: Optische DWDM-Mehrkanaltechnik liefert die notwendige Bandbreite für den gesamten Verkehr eines Betreibers. Flexible Add-Drop-Multiplexer ermöglichen eine automatisierte Anpassung auf neue Anforderungen. Die Kapazität lässt sich durch Hinzufügen von optischen Kanälen einfach erweitern. Durch Redundanz können einzelne Schnittstellen und Wellenlängen oder komplette Glasfaser-Strecken und Netzelemente geschützt werden. Unsere ConnectGuard™ Sicherheitstechnologie bietet schon heute einen quantensicheren Schutz. Die FSP 3000 Lösung ist die einzige vom BSI zugelassene Verschlüsselungstechnik für optische Verbindungen auf der Netzschicht 1 (Layer 1).

BSI-Zulassung

FSP 3000 optischer Transport

- Flexibler, optischer Layer
- Quantensichere Verschlüsselung
- Hohe Verfügbarkeit

Geschützter Netzzugang und Edge Cloud: Ethernet-Technik ist die dominierende Schnittstellentechnologie für die Anbindung von Standorten und Liegenschaften. Unsere hochsichere Netzzugangstechnik kombiniert umfassende Überwachungsfunktionen mit quantensicherer ConnectGuard™-Verschlüsselung und lokalem Hosting von virtualisierten Netzfunktionen. Die vom BSI zugelassene Verschlüsselung sichert den Datenverkehr und schützt die integrierte Edge Cloud vor Cyber-Angriffen. Virtualisierte Netzfunktionen übernehmen das Routing, die Überwachung von SCADA-Verkehr aber auch die effiziente Nutzung des Verbindungsnetzes durch SD-WAN Funktionalität. Unsere FSP 150-XG118Pro (CSH) bietet einzigartige Flexibilität, Geschwindigkeit und Schutz.

BSI-Zulassung

FSP 150 IP/Ethernet und NFV

- 1/10Gbit/s geschützter Netzzugang
- Integrierter Server für Edge Hosting
- Virtuelle Router, SCADA-Monitoring

Robuste Synchronisierung, präzises Timing: Die heutigen Anforderungen an Präzision, Zuverlässigkeit und Management lassen sich mit etablierten Zeitprotokollen wie NTP, IRIG-B nicht mehr erfüllen. Die Verwendung von GNSS-Empfängern ist eine beliebte Methode, um von Satelliten eine präzise Zeitinformation zu erhalten. Diese Systeme sind durch Jamming und Spoofing sehr leicht angreifbar. Sie sollten nicht als primäre Quelle für die Synchronisation und das Timing in den Netzen von Energieversorgern eingesetzt werden. Unser Partner Adtran Oscilloquartz bietet ein umfassendes Lösungs-Portfolio für Energieversorger, das sowohl Cäsium-Atomuhren als auch skalierbare Grandmaster und optimierte Timing-Komponenten umfasst.

Oszilloquartz Timing Portfolio

- Skalierbare PTP-Grandmaster
- Cäsium Atomuhren
- Multi-Protokoll: BITS, IRIG-B, PTP, NTP

Fasermonitoring in Echtzeit: Glasfaserbrüche sind in einem Land, das hohe Bautätigkeiten hat, unvermeidlich. Eine schnelle und zielgerichtete Reparatur ist von entscheidender Bedeutung. Durch die Verwendung von Adtran ALM Fasermonitoring können Störungen auf der Glasfaser in Echtzeit erkannt und lokalisiert werden. Eine zeitintensive Fehlersuche wird vermieden. Dies ermöglicht eine schnellere Wiederinbetriebnahme von Verbindungen und damit eine hohe Verfügbarkeit. ALM erkennt auch, wenn die Faserverbindung abgehört wird, da durch die Ankopplung eine Dämpfung erzeugt wird.

ALM Glasfaser Monitoring

- Echtzeit Überwachung
- Lokalisierung von Faserbrüchen
- Erkennen von Abhörversuchen