FUJITSU

Sicherheit für Energieversorger

Mit Fujitsus Cyber Security Services for Operational Technology systemkritische Anlagen überwachen

Sicherheit für Ihre Operational Technology

Wie schaffen Sie es als Energieversorger, Ihren Kund*innen Produkte und Services in gleichbleibend hoher Qualität und Zuverlässig bereitzustellen? Das gelingt nur, wenn Ihre Operational Technology (OT) samt aller Erzeugungsanlagen und Versorgungsinfrastruktur inklusive der Geräte und Komponenten sowie der darauf laufenden Prozesse unterbrechungsfrei funktioniert.
Mit einer Digitalisierungs- und Konnektivitätsstrategie lassen sich Anlagen und Assets vernetzen, Daten austauschen und die Gesamtanlageneffizienz (OEE) sowie der Kundennutzen steigern. Mit zunehmender Konnektivität erhöht sich jedoch das Risiko für Cyberangriffe. Gefahren drohen nicht nur von kriminellen externen Akteuren, sondern auch von böswilligen Insidern oder durch Industriespionage. Je digitaler Ihre OT, desto stärker müssen Sie diese überwachen.

Als Energieversorger unterliegen Sie in Sachen Sicherheit zusätzlich den besonderen Auflagen der KRITIS-Verordnung zum Schutz kritischer Infrastrukturen. Das bedeutet, Sie müssen Zertifizierungen nachweisen – zum Beispiel ISO/IEC 27001 und 27019 – und damit energieversorgungsspezifische erweiterte Sicherheitsmaßnahmen und Zusatzanforderungen des IT-Sicherheitskatalogs erfüllen. Hinzu kommen möglicherweise noch internationale Normenreihen wie die IEC 62443, die Sie einhalten müssen. Doch wie dabei vorgehen?

Zunächst sollten Sie Ihre bestehenden Anlagen (Brownfield-Anlagen) neu auf den Prüfstand stellen, da sich Design und Implementierung von Konnektivitätsnetzwerken ständig weiterentwickeln. Gefragt ist ein kontinuierliches Monitoring der internen Assets, Ressourcen und Prozesse – optimalerweise in enger Zusammenarbeit zwischen Security- und Betriebstechnologieexperten. Fehlt die systematische Transparenz über Ihre digitalen Assets, müssen Sie diese herstellen. Nur dann können Sie Ihre Infrastruktur schützen und die Daten sicher nutzen. Nutzen Sie dazu unsere Fujitsu Cyber Sercurity Services for Operational Technology. Diese bestehen aus drei Elementen:

OT Asset Discovery – Entdecken Sie Ihre vernetzten, digitalen Assets als Basis für technologische und organisatorische Transformationen.

OT Assessment – Bewerten Sie die Einhaltung gesetzlicher Standards und finden Sie heraus, wo Defizite liegen. Nur dann können Sie Ihre Ressourcen dorthin organisieren, wo sie am dringendsten
benötigt werden.

OT Managed Monitoring – Überwachen Sie Ihre OT-Assets sämtlicher Anlagen und Standorte zentral und permanent rund um die Uhr (24/7), um anomale Verhaltensweisen schnell zu erkennen.

Die OT Cyber Security Services von Fujitsu in der Übersicht

OT Asset Discovery

Mit dem Service **OT Asset Discovery** stellen Sie eine vollständige Transparenz über Ihre OT-Umgebung her – als Grundlage für Optimierungen der Anlageneffizienz sowie für Innovation und Cybersicherheit. OT Asset Discovery lässt sich auf zwei Arten durchführen:

1. Fujitsu Mitarbeitende installieren vorübergehend ein physisches Gerät über SPAN-Ports, das Asset-Discovery-Aufgaben innerhalb Ihres OT-Netzwerks durchführt.
2. Sie machen selbstständig Aufnahmen Ihres OT-Stands – unter virtueller Anleitung von Fujitsu Mitarbeitenden.

Die erfassten Netzwerkinformationen werden anschließend verarbeitet und detaillierte Informationen über Ihre OT-Assets und den Netzwerkverkehr extrahiert. Sobald die Netzwerke vollständig erfasst sind, erhalten Sie eine Asset-Liste inklusive eines High-Level-Berichts über die entdeckten Assets. Optional können wir die Daten auch in einem Format bereitstellen, das sie für eine ServiceNow-Integration nutzen können.

Ihr Nutzen:

Sie erhalten die optimale Transparenzbasis für weitere Services sowie die Optimierung und Modernisierung Ihrer Anlagen.

OT Assessment

Beim OT Assessment evaluieren wir Ihre bestehende Umgebung unter dem Gesichtspunkt der Cybersicherheit in Bezug auf Menschen, Prozesse und Technologie. Sie erhalten Empfehlungen auf Basis einer Roadmap, die technische und ggf. organisatorische Aspekte sowie die damit verbundenen Compliance-Anforderungen berücksichtigen. In die Bewertung kann auch eine Offline-Datenanalyse sowie Interviews mit Betriebsexperten einfließen. Ebenso können wir Ihre Werksdokumentation oder eine Proof-of-Value-Testphase inkludieren, die von der laufenden Produktion isoliert ist. Je nach Umfang und Umfeld arbeiten wir beim Assessment mit spezialisierten Partnern zusammen. Die Liste der passiven Asset Discovery kann in eine Configuration Management Database (CMDB) importiert werden, um weitere Digitalisierungsschritte zu unterstützen.

Ihr Nutzen:

Sie lernen den aktuellen Stand Ihrer OT aus der Perspektive der Cybersicherheit kennen. Gewonnene Empfehlungen und eine Roadmap bilden die Grundlage für weitere Digitalisierungsinitiativen, die jeweils Ihr Risikoprofil und Compliance-Prioritäten berücksichtigen.

OT Managed Monitoring

Dieser Service wird vom Fujitsu Security Operations Center (SOC) erbracht. In der Einrichtungsphase arbeitet Fujitsu eng mit Ihrem Security Operations Team zusammen und etabliert das Arbeitsmodell sowie den Datenaustausch. Wir definieren gemeinsam das normale Cyber-verhalten Ihrer OT-Umgebung und proben die Kommunikation zwischen Fujitsu und Ihren Teams. In der operativen Phase erfolgen das Monitoring und Reporting nach vereinbarten Verfahren. Das Fujitsu SOC überwacht kontinuierlich den Cybersicherheitszustand Ihrer OT (z. B. SCADA-Systeme) ebenso wie den Datenverkehr auf Anomalien. Die am Service Desk erfassten Ereignisse werden klassifiziert, mit Tickets versehen, priorisiert und dann an die entsprechende Schnittstelle in Ihrem Unternehmen weitergeleitet. Dies ermöglicht Ihren Teams eine schnelle Erkenntnis und Entscheidungsfindung. Der Service erkennt dem Netzwerk neu hinzugefügte Assets automatisch und erlaubt optional Aktualisierungen der CMDB. Weitere Optionen wie Vulnerability Management und Privileged Access Management können Sie in Kombination mit diesem Service nutzen.

Ihr Nutzen:

Sie erhalten ein stets aktuelles Bild der Bedrohungslage Ihrer Anlagen und erkennen und verhindern Gefahren schnell und zuverlässig.

Warum Fujitsu?

Fujitsu verfügt über eigene Security Operations Centers, Security Consultancy Practice und Implementierungskapazitäten und bringt Erfahrung und Fachwissen in alle Projekte ein. Wir bieten Best Practices und Referenzen in der Energie- und Versorgungsbranche, bei der Einhaltung von ISO/IEC 27019, 27001 und 22301 sowie anderen internationalen oder branchenspezifischen Standards, zum Beispiel der IEC 62443. Darüber hinaus profitieren Unternehmen von unserer langjährigen Expertise im Rahmen der Datenverarbeitung, der strategischen Beratung sowie der praktischen Umsetzung.

Sie möchten mehr erfahren?

Kontaktieren Sie uns jetzt, um mehr zu den konkreten Vorteilen unserer OT Cyber Security Services für Energieversorger zu erfahren.

Kontakt: Fujitsu Enterprise & Cyber Security CE
E-Mail: OT-Security-CE@Fujitsu.com
Website: www.fujitsu.com/de/