Factsheet

cyber security

Energieversorgungsnetze vor Cyber-Angriffen sichern

Wie Sie kritische Informationsinfrastrukturen schützen können

IT-Sicherheit hat hohe Priorität. Ganz besonders für Unternehmen, die Netzsteuerungssysteme für Transport- und Verteilnetze im Strom-, Gas und Telekommunikationsbereich bereitstellen und unterhalten.

Die Bundesnetzagentur (BNetzA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) haben nach §11 Absatz 1a EnWG einen Katalog von Sicherheitsanforderungen zum Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme erstellt, die der Netzsteuerung dienen. Betreiber von Energieversorgungsnetzen sind verpflichtet, anhand dieser Grundlage für die Umsetzung eines Informationssicherheits-Managementsystems (ISMS) zu sorgen. Ein ISMS bildet generell die spezifischen Verantwortlichkeiten, Maßnahmen und Regelprozesse ab, die umgesetzt, dokumentiert und geprüft werden müssen, um die notwendigen Sicherheitsstandards zu erfüllen.

Was bedeutet das konkret für Ihr Unternehmen, wenn Sie ein ISMS einführen oder weiterentwickeln möchten, welches den aktuellen Sicherheitsstandards entspricht? Wie kann die erforderliche Zertifizierung zum Schutz von Netzleit- und Automationssystemen erreicht werden?

Die Dienstleistung von Atos

Atos unterstützt Sie dabei, Ihre Netzleitsysteme auf die Vorgaben des IT-Sicherheitskatalogs auszulegen und die Zertifizierung durch eine akkreditierte Zertifizierungsstelle zu erhalten.

In vier Schritten zur erfolgreichen ISMS-Zertifizierung: von der Entwicklung einer Sicherheitsstrategie bis zur Zertifizierung Ihres ISMS

Schritt 1: ISMS-Workshop

Die ISMS-Experten von Atos verfügen über jahrelange Erfahrung im Zertifizierungsprozess nach ISO/IEC 27001 Norm und führen den Kunden gezielt durch den Anforderungskatalog. Unternehmen im Energiesektor verfügen meist schon über explizite Sicherheitsprozesse und Know-how im IT-Security-Umfeld. Der Workshop wird das vorhandene ISMS analysieren und benchmarken. Auf Basis der gewonnenen Erkenntnisse werden die Zielvorstellung und das weitere Vorgehen definiert und festgelegt.

Schritt 2: Security Maturity Assessment (SMA)

Atos überprüft die Qualität und Effektivität der ISMS-Anpassung anhand eines spezifisch entwickelten Vorgehensmodells, das die Ergebnisse einer Ist-Aufnahme dem vom Kunden definierten Reifegrad (Soll-Zustand) gegenüberstellt. Das Modell stützt sich auf den führenden Standard ISO/IEC 27001 in Kombination mit dem Reifegrad-Modell (CMM) und ermittelt den Reifegrad des ISMS, der für den weiteren Handlungsbedarf maßgeblich ist. Da alle Kapitel der ISO/IEC 27002 im Rahmen des SMA behandelt werden, kann ein vollständiger Umsetzungsplan aus den Reifegradermittlungen abgeleitet werden.

Schritt 3: Implementierung

Atos prüft und vervollständigt die IT-sicherheitstechnischen Vorgaben und Richtlinien in Hinblick auf die ISO-Anforderungen. Der abgeleitete Umsetzungsplan umfasst infrastrukturelle, technische, personelle sowie organisatorische Aufgaben und beziffert die für die Umsetzung notwendigen Aufwände sowie Personalressourcen. Atos unterstützt die Umsetzung mit qualifiziertem Fachpersonal im erforderlichen Umfang.

Schritt 4: Zertifizierung

Atos ist mit der Zertifizierungsmethodik bereits nach ISO/IEC 27001 bestens vertraut und hat zahlreiche Kunden routiniert und erfolgreich auf die Zertifizierung vorbereitet. Die ISO 27001-Lead Auditoren von Atos betreuen bei den Audit-Vorbereitungen sowie bei den Vor-Ort-Prüfungen der Zertifizierungsstelle. Nach einer erfolgreichen Prüfung kann der Kunde die Sicherheit seiner Netzleitsysteme durch ein anerkanntes Zertifikat garantieren. Ein echter Wettbewerbsvorteil, denn mit einem hohen Sicherheitsstandard schaffen Sie Vertrauen bei Ihren Privat- wie Geschäftskunden.

Warum Atos?

- Das Bundesamt für Sicherheit in der Informationstechnik hat Atos als IT-Sicherheitsdienstleister für IS-Revision und IS-Beratung zertifiziert.
- Seit 2002 ist Atos offizieller IT-Dienstleister der Olympischen Spiele sowie der Paralympics. Cyber Security spielt insbesondere während der Olympischen Spiele eine zentrale Rolle. So konnte Atos bei den Spielen in London 2012 im Schnitt mehr als 14 Millionen tägliche Cyber Attacks erfolgreich abwehren.
- Atos verfügt über ein ETSI zertifiziertes Trust Center (über 100 Millionen ausgestellte Zertifikate).
- Für das BSI entwickelte Atos den IT-Grundschutz-Baustein „Cloud Management" zum sicheren Betrieb von Cloud-Diensten.
- Atos prüft SCADA-Systeme und kooperiert mit renommierten Herstellern wie beispielsweise Siemens.
- Atos setzt eigene zertifizierte IT-Produkte aus Deutschland ein (CardOS, DirX).
- Atos ist Partner der Allianz für Cyber-Sicherheit des BSI und der BITKOM.
- Langjährige Expertise von Atos im Aufbau von ISMS und in der Umsetzung von branchenspezifischen Sicherheits-anforderungen.

Allianz für Cyber-Sicherheit
Partner

Powering your success

Atos begleitet Sie von der Entwicklung einer Sicherheitsstrategie bis zur Zertifizierung Ihres Informationssicherheits-Managementsystems (ISMS)

Atos-Referenzen

Bundeseisenbahnvermögen
Bundesministerium für Arbeit und Soziales
Bundesverwaltungsamt
dpa
Open Grid Europe The Gas Wheel
GOETHE INSTITUT
DB SCHENKER
Landwirtschaftskammer Nordrhein-Westfalen
SIEMENS
gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
E-PLUS GRUPPE
NLWKN Niedersächsischer Landesbetrieb für Wasserwirtschaft, Küsten- und Naturschutz

Inject agility back in your business, call on your Business Technologist

Weitere Informationen erhalten Sie unter: de-info@atos.net

de.atos.net