

IT-Sicherheit

IT-Sicherheit für prozessnahe Systeme der Energiebranche

Auch in den prozessnahen Bereichen der Energieversorgungsunternehmen ist die moderne Informations- und Kommunikationstechnologie heutzutage ein integraler Bestandteil nahezu aller Geschäfts- und Betriebsprozesse. Von zentralen Steuerungs- und Leitsystemen bis hin zur verteilten Automatisierungs-, Schutz- und Leittechnik in Stationen und Kraftwerken – in allen modernen Systemen werden IT-Standardtechnologien wie Ethernet, TCP/IP und konventionelle Software und Betriebssysteme genutzt. Gleichzeitig nimmt durch Marktliberalisierung und steigenden Kostendruck der Bedarf nach einer durchgehenden Vernetzung der Systeme untereinander, mit der Büro-IT aber auch mit Fremdunternehmen und Dienstleistern für Datenaustausch und Fernwartung stark zu.

Durch diese Entwicklung sind auch betriebsrelevante und kritische Systeme zunehmend IT-Sicherheitsbedrohungen ausgesetzt – wie dem Befall mit Schadsoftware, Unachtsamkeit von eigenen Mitarbeitern oder gar Zugriffen von Unbefugten.

Die Folgen können von kostspieligen Systemausfällen bis hin zur Gefährdung von Versorgungssicherheit, Anlagen oder gar Menschenleben reichen.



Die sich stetig ändernde Bedrohungslage verlangt sowohl von Betreibern als auch von den Herstellern neue Konzepte und angepasste Maßnahmen, um auch in Zukunft für einen ausreichenden Schutz ihrer Systeme zu sorgen.

Weitergehende Informationen zum Thema finden Sie in unserem SCADA Security Whitepaper unter http://www.gai-netconsult.de/WP_SCADA.pdf

Zur Absicherung prozessnaher IT-Systeme im EVU-Umfeld sind individuell angepasste Konzepte und Vorgehensweisen notwendig. Die GAI NetConsult verfügt hier über nachgewiesene langjährige Erfahrung und unterstützt sowohl Betreiber als auch System- und Komponentenhersteller aus der gesamten Energiebranche in allen Projektphasen. Unser Leistungsangebot umfasst unter anderem:

Analyse

- Erfassung der vorhandenen Systemarchitektur, Durchführung von Schutzbedarfsfeststellungen und Risikoanalysen
- Erstellung von angepassten Maßnahmenkatalogen und individuellen Sicherheitskonzepten

Test und Audit

- Technische Sicherheitsüberprüfung von Systemen, Komponenten und TCP/IP-basierter Kommunikation (z.B. IEC 60870-5-104, IEC 61850, OPC oder proprietäre Protokolle)
- Schwachstellensuche mit Scan- und Penetrationstests im Prozessbereich, z.B. in Leit- und Automatisierungssystemen, in der Nachrichtentechnik oder an sekundärtechnischen Komponenten
- Organisatorische Audits auf Basis anerkannter Standards wie ISO 27001 / 27002
- Reviews anhand von Richtlinien wie den KRITIS-Anforderungen des Bundesamts für Sicherheit in der Informationstechnik oder NERC CIP

Sicherheitskonzeption

- Technische Sicherheitsmaßnahmen, z.B. zur Absicherung von Fernwartungslösungen für sensitive Systeme wie zentraler Leittechnik, Stations- oder Kraftwerkautomatisierung
- Evaluierung, Auswahl und Einführung von Sicherheitsprodukten in prozessnahen Bereichen
- Beratung zu Sicherheitsfragen beim Systemdesign und zur Umsetzung von Sicherheitsanforderungen wie dem [BDEW-Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“](#), der VGB-Richtlinie R 175 „IT-Sicherheit für Erzeugungsanlagen“ oder den NERC CIP Cyber Security Standards für den nordamerikanischen Markt

Sicherheitsorganisation

- Aufbau von Information Security Managementsystemen (ISMS) im Prozessumfeld
- Erstellung von Betriebskonzepten, Sicherheitsrichtlinien und Standards für den prozessnahen Bereich
- Notfallplanung und Business Continuity Management für kritische IT-Systeme