Informationssicherheit

Absicherung von Prozesskontroll- und Automatisierungssystemen

Durch die zunehmende Nutzung von modernen IT-Technologien in Automatisierungs- und Prozesssteuerungsumgebungen sind diese nun auch vermehrt konventionellen IT-Sicherheitsbedrohungen ausgesetzt. Da die genannten Systeme in der Regel zentrale Produktions- oder Versorgungsprozesse überwachen und steuern, können IT-Sicherheitsprobleme hier schnell weitreichende Folgen haben – von kostspieligen Produktionsausfällen in der herstellenden Industrie bis zu nachhaltig wirkenden Versorgungsengpässen und Störungen der öffentlichen Sicherheit bei kritischen Infrastrukturen.

Unabhängig von Industriebranche oder Anwendungsumfeld werden in heutigen Steuerungsumgebungen überall Softwaresysteme und Technologien aus der klassischen IT eingesetzt, wie z.B. Industrial Ethernet, TCP/IP und Betriebsysteme wie Linux, Unix oder Microsoft Windows. Aufgrund hoher Verfügbarkeitsanforderungen und der notwendigen, umfangreichen Tests ist es hier aber meist nicht möglich, die zahlreichen in den Systemen auftretenden Sicherheitslücken zeitnah durch Security-Patches zu schließen. Ein zusätzliches Problem ist, dass Industrieprotokolle und Hardware-Komponenten wie SPSen oder Kommunikations-Gateways über keine Sicherheitsfunktionen verfügen, die wirksam vor unberechtigten Zugriffen oder anderen Angriffen schützen könnten. Während Prozessdatennetze bis vor wenigen Jahren komplett isoliert betrieben werden konnten, besteht heute in allen Branchen der Bedarf, zeitnah auf Daten aus der Automatisierungs- und Prozesswelt zuzugreifen und Fernwartung zu betreiben. Deswegen entstehen immer mehr Schnittstellen zu Büronetzwerken, aber auch an externe Systeme, z.B. von Dienstleistern oder Lieferanten.



Durch die Kombination der oben genannten Probleme sind die Systeme mittlerweile durch vielfältige Sicherheitsbedrohungen gefährdet, wie z.B. Eindringen von Schadsoftware, Unachtsamkeit von Angestellten oder Zugriffe von Unbefugten.

Die Absicherung von kritischen Kontroll- und Automatisierungssystemen erfordert durchdachte und individuelle, auf die jeweilige Umgebung angepasste Konzepte und Strategien. Die GAI NetConsult verfügt hier über langjährige Erfahrung aus verschiedenen Industrie-Branchen und dem Versorgerumfeld und unterstützt Sie gerne in allen Projekt-Phasen.

Unser Leistungsangebot auf dem Gebiet der Absicherung von kritischen Automatisierungs-, Leit- und Steuerungssystemen deckt das gesamte Spektrum von Analyse, Test und Audit über Sicherheitskonzeption bis zur Sicherheitsorganisation ab.

☞ Analyse

- ☑ Erfassung der vorhandenen Systemarchitektur
- ☑ Durchführung von Schutzbedarfsfestellungen und Risikoanalysen
- ☑ Erstellung von Maßnahmenkatalogen
- ☑ Entwurf von Sicherheitskonzepten

☞ Test und Audit

- ☑ Technische Sicherheitsüberprüfung von Systemen, Komponenten und Netzwerken
- ☑ Schwachstellensuche mit Scan- und Penetrationstests im Prozesskontroll- und Automatisierungsumfeld
- ☑ Organisatorische Audits auf Basis anerkannter Standards wie ISO 27001/27002

☞ Sicherheitskonzeption

- ☑ Technische Sicherheitsmaßnahmen
- ☑ Sichere Fernwartungs- und Datenkopplungs-Lösungen
- ☑ Evaluierung, Auswahl und Einführung von Sicherheitsprodukten unter besonderer Berücksichtigung industrieller Anforderungen
- ☑ Beratung zu Sicherheitsfragen beim Systemdesign

☞ Sicherheitsorganisation

- ☑ Aufbau von Information Security Managementsystemen (ISMS) im Prozess- und Produktionsumfeld
- ☑ Konzepte zur Betriebsorganisation
- ☑ Erstellung von Sicherheitsrichtlinien und Standards unter Beachtung branchenspezifischer Besonderheiten
- ☑ IT-Notfallplanung

GAI NetConsult GmbH, Am Borsigturm 58, D-13507 Berlin, Tel: 030-417 898-0, Fax: 030-417 898-300
E-Mail: info@gai-netconsult.de Internet: http://www.gai-netconsult.de