secorvo
security consulting

EnBW Energie Baden-Württemberg AG

Sicherheitsüberprüfung der Leittechnik-IT konventioneller Kraftwerke der EnBW

Secorvo prüfte 2018 innerhalb eines halben Jahres an fünf KRITIS-relevanten Kraftwerksstandorten der EnBW die IT-Sicherheit der eingesetzten Leittechnik. Detaillierte Planung, enge Einbindung der Kraftwerksleitungen, eine hohe Awareness der EnBW-Mitarbeiter und standardisierte Prüfprozesse sorgten für die reibungslose Durchführung der technischen Audits im laufenden Betrieb.

Um den Anforderungen des IT-Sicherheitsgesetzes gerecht zu werden, etablierte die EnBW als eines der großen Energieversorgungsunternehmen in Deutschland ein ISO/IEC 27001-konformes Informationssicherheitsmanagementsystem (ISMS). In diesem Zusammenhang erhielt Secorvo den Auftrag, die Informationssicherheit der konventionellen Kraftwerke der EnBW zu auditieren mit dem Ziel, das etablierte Sicherheitsniveau festzustellen und die bereits ergriffenen Maßnahmen auf ihre Wirksamkeit hin zu überprüfen. Weiterhin galt es, die hierbei identifizierten Schwachstellen und Angriffspunkte in der IT-Infrastruktur zu bewerten und geeignete Gegenmaßnahmen zu empfehlen.

In den Kraftwerken kommen zahlreiche IT-Komponenten im Bereich der Leittechnik zum Einsatz, denn häufig werden elektronische Komponenten durch neue, mit IT ausgestattete Generationen ersetzt. Leittechniker betrachten diese Komponenten in der Regel nicht aus „IT-Perspektive". Daher kann es vorkommen, dass Maßnahmen der IT-Sicherheit nicht ausreichend berücksichtigt werden.

In den vergangenen Jahren bekannt gewordene Angriffe auf Kraftwerke haben gezeigt, dass gerade diese weniger gut geschützten Komponenten Ziel von Angreifern sind. Deshalb wurden im Rahmen der IT-Sicherheitsüberprüfung insbesondere diese Komponenten untersucht.

Diese Leittechniksysteme werden von den Herstellern in einer vorgegebenen Konfiguration implementiert und können vom Betreiber nicht ohne weiteres verändert oder aktualisiert werden. Typische IT-Sicherheitsmaßnahmen, wie sie seit Jahren in der Bürokommunikation angewendet werden, sind daher oft nicht umsetzbar. Es müssen alternative Wege der Absicherung gefunden werden, um beispielsweise Systeme, bei denen Hersteller keine Aktualisierungen liefern, vor Angriffen zu schützen.

„Die Firma Secorvo hat sehr zielorientiert und klar strukturiert mit großem Fachwissen diesen Security Check zu meiner vollsten Zufriedenheit durchgeführt."

Klaus Holzwarth
Projektleiter E-& Leittechnik, EnBW

Stand: 15.04.2019

Auch stehen oft keine Test-Systeme zur Verfügung und die technischen Audits müssen an den produktiven Anlagen erfolgen.

Zu Projektbeginn wurde der Prüfungsumfang abgestimmt und dokumentiert. Secorvo erarbeitete daraufhin eine einheitliche Methodik zur Prüfung der Kraftwerksstandorte auf Basis gängiger Best-Practices und den eigenen Erfahrungswerten.

Das technische Audit wurde in sechs Prüfbereiche gegliedert:

- physische Sicherheitsmaßnahmen
- kritische Leittechnik-Systeme (z. B. SPS-Systeme, Server, Netzwerkkomponenten, Aktoren/Sensoren, Bus-Systeme)
- Sicherheit der Netzzugänge (Netzwerkports in der Leittechnik)
- kabellose Netzzugänge (WLAN), sonstige kabellose Zugangsmöglichkeiten (Bluetooth)
- Fernwartungs- und Remote-Netzwerkzugänge
- exemplarische Client-Systeme (z. B. Bedienstationen, Engineering-Stationen)

Jeder Standort konnte außerdem zwei weitere Prüfbereiche selbst bestimmen, um standortspezifische Infrastrukturen untersuchen zu lassen.

Für jeden Prüfbereich wurden definierte Prüfpunkte festgelegt und den Betreibern zur Vorbereitung der Termine vor Ort zur Verfügung gestellt. Zusätzlich wurden im Dokumentationswerkzeug von Secorvo für die Prüfpunkte einzelne Prüfschritte hinterlegt. Hierdurch konnte sichergestellt werden, dass auch bei unterschiedlichen Prüfern für jeden Standort vergleichbare Ergebnisse erzielt wurden.

Vorab fanden an jedem Standort umfangreiche Klärungen statt: Die externen Prüfer mussten Zugang zu den Kraftwerksbereichen und Dokumentationen erhalten, zum Arbeitsschutz belehrt werden, und es mussten Interviewtermine mit den Verantwortlichen abgestimmt werden. Schichtleiter mussten über Begehungen und Prüfungen informiert werden, Notfallmaßnahmen mussten besprochen und als Vorsichtsmaßnahme Rufnummern zu den Herstellern bekannt sein.

Durch diese systematische Vorbereitung konnte an allen Standorten der Betrieb der Kraftwerke während aller Prüfphasen des Projektes störungsfrei weitergeführt werden. Außerdem konnte der Aufwand für die Vor-Ort-Audits auf Seiten der Betreiber jeweils auf wenige Projekttage begrenzt werden, ohne die Vergleichbarkeit oder Aussagekraft der Testergebnisse zu beeinträchtigen.

Schwachstellen wurden sowohl auf Seiten des Betreibers als auch bei einzelnen Produkten gefunden. Auf Grundlage der Prüfergebnisse erarbeitete Secorvo pragmatische Vorschläge, wie die EnBW das etablierte Sicherheitsniveau mit überschaubarem Aufwand anheben kann, indem Angriffsflächen reduziert oder komplett unterbunden werden.

Die Leitungsebene der Standorte war von Anfang an eingebunden und garantierte die erforderliche Rückendeckung. Die beteiligten Mitarbeiter der EnBW zeigten ein hohes Maß an Sensibilität für die Belange der Informationssicherheit und starkes Interesse an einer wirksamen Steigerung des bereits etablierten Sicherheitsniveaus.

EnBW Energie Baden-Württemberg AG – Energiewende. Sicher. Machen.

Mit über 21.000 Mitarbeitern ist die EnBW eines der größten Energieversorgungsunternehmen in Deutschland und Europa und versorgt rund 5,5 Millionen Kunden mit Strom, Gas und Wasser sowie mit Energielösungen und energiewirtschaftlichen Dienstleistungen.

Über Secorvo

Die Secorvo Security Consulting GmbH ist ein auf Informationssicherheit und Datenschutz spezialisiertes und bereits mehrfach ausgezeichnetes Beratungsunternehmen. Alle Mitarbeiter sind ausgewiesene Experten mit vieljähriger Erfahrung.

Telefon +49 721 255171-0 · info@secorvo.de · www.secorvo.de

Weil Sicherheit Erfahrung braucht.

Stand: 15.04.2019