Best-Practices für ein sicheres Stromnetz

Erweiterte Sicherheits-anforderungen für Prozessteuerungstechnik der Energieversorgung

Dr. Stephan Beirer, Teamleiter Informationssicherheit in Prozesssteuerungsumgebungen, GAI NetConsult GmbH; Dipl.-Ing. Erwin Bosin, MSc, Teamleiter Prozessrechner und USV, TIWAG-Netz AG; Rolf-Dieter Kasper, Telekommunikation und Sicherheit, RWE Deutschland AG

Ein angemessenes IT-Sicherheitsniveau zu gewährleisten, ist inzwischen ein wichtiger Aspekt von moderner Prozessleittechnik in der Energieversorgung geworden. Basierend auf einem 2008 erschienenen BDEW-Whitepaper haben Oesterreichs Energie und BDEW gemeinsam erweiterte Ausführungshinweise und Anwendungsbeispiele zur Umsetzung der Whitepaper-Anforderungen veröffentlicht.

Die Nutzung von standardisierten IT-Komponenten ist heute im Bereich der Prozesssteuerung der Energieversorgung und der zugehörigen Nachrichten- und Telekommunikationstechnik üblich. Durch den Trend zu Smart-Grid-Szenarien ist eine weitere Zunahme der Vernetzung von Systemen und Komponenten absehbar. Bereits in einigen Jahren ist damit zu rechnen, dass die Anzahl der IP-vernetzten Komponenten im Bereich der Prozesssteuerung die Zahl der Systeme im klassischen Büroumfeld überholen wird.

Vom BDEW Bundesverband für Energie- und Wasserwirtschaft wurde bereits im Jahr 2008 mit dem Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ ein Dokument mit grundsätzlichen Sicherheitsmaßnahmen für Steuerungs- und Telekommunikationssysteme für die Prozesssteuerung in der Energieversorgung entwickelt. Ziel dieses BDEW-Whitepaper ist es, unter Verweis auf Sicherheitsstandards wie die ISO/IEC 27000 Normenreihe generische Anforderungen an die Systemtechnik und die zugehörigen Wartungs- und Entwicklungsprozesse festzuschreiben. Auf Grund des breiten Anwendungsbereichs werden im BDEW-Whitepaper allgemeine Anforderungen gestellt, die im Rahmen von Projektierung und Ausschreibungen konkretisiert werden sollen. In der Praxis kam es allerdings nicht selten zu Interpretationsschwierigkeiten und unterschiedlicher

Auslegung zwischen Betreibern und Planern auf der einen Seite sowie Anbietern und Herstellern auf der anderen Seite.

Auf Initiative von Oesterreichs Energie wurde deshalb von der IT-Sicherheits-Arbeitsgruppe des österreichischen Verbands gemeinsam mit dem BDEW ein Best-Practice-Papier mit Ausführungshinweisen zur Anwendung des BDEW-Whitepapers erarbeitet. Das Best-Practice-Papier enthält zu den einzelnen Anforderungen des BDEW-Whitepapers Umsetzungsbeispiele und Anwendungshinweise für die unterschiedlichen Technologiebereiche der Prozessautomatisierung in der Energieversorgung. Eingeflossen sind die praktischen Erfahrungen von Experten aus vielen konkreten Automatisierungs- und Leittechnik-Projekten sowie Ergebnisse aus den Diskussionen mit verschiedenen Systemherstellern.

Mindestens ebenso wichtig sind aber auch die organisatorischen Sicherheitsmaßnahmen im Unternehmen, wie der Aufbau einer Sicherheitsorganisation oder die Schaffung eines umfassenden Sicherheitsbewusstseins bei den Mitarbeitern. Hierzu sei insbesondere auf die Normenreihe ISO/IEC 27000 und die ergänzenden, branchenspezifischen Normen und Frameworks verwiesen. Der DIN hat im April 2012 die Sicherheitsnorm DIN SPEC 27009 „Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002“ veröffentlicht.

Struktur und Inhalte

Das Best-Practice-Papier ist entsprechend den Anforderungskapiteln des BDEW-Whitepaper gegliedert. Zu Beginn jedes Kapitels wird das darauf verweisende Anforderungskapitel des BDEW-Whitepaper zitiert und ein Verweis zum entsprechenden Kapitel der ISO/IEC 27002 angeführt. In der folgenden Tabelle werden im Abschnitt „Ergänzungen und Anmerkungen“ zunächst allgemeingültige Hinweise gegeben, die alle Technologiebereiche der Prozesssteuerung in der Automatisierung der Energieversorgung betreffen. Anschließend werden für die drei im EVU-Prozessumfeld anzutreffenden Haupttechnologiebereiche „Betriebsführungs-/Leitsysteme und Systembetrieb“, „Übertragungstechnik/Sprachkommunikation“ und „Sekundär, Automatisierungs- und Fernwirktechnik“ spezifische Ausführungshinweise aufgeführt.

Wenn es um die Härtung von Standardsoftware wie PC-Betriebssysteme oder Datenbankserver geht, verweist das Papier beispielsweise auf die Dokumentation der jeweiligen Hersteller oder auf die Anleitungen des Center for Internet Security. Bei Embedded Systems wie Steuerungs- und Schutzkomponenten sollten zur Härtung alle nicht für den Betrieb notwendigen Kommunikationsdienste und Parametrierzugänge deaktiviert, Standardpassworte geändert sowie nicht benötigte Nutzeraccounts deaktiviert werden.

Der Schutz vor Schadsoftware ist bei Prozessdatensystemen häufig schwierig zu realisieren. Weil auf den wenigsten Embedded Systemen Schutzsoftware installiert werden kann, wird auf die Absicherung und Härtung der Schnittstellen und ein sicheres Netzwerkdesign verwiesen. Hierdurch sollen neben dem Schadsoftwarebefall auch Auswirkungen von Störungen wie Netzwerküberlast reduziert werden, die zu den Nebeneffekten von Schadsoftware gehören können. Für PC-basierte Systeme wird als Alternative zu traditionellen Schadsoftware-Scannern auf Schutzmethoden wie das Application-Whitelisting hingewiesen. Im Best-Practice-Papier wird auch explizit hervorgehoben, dass das Schutzkonzept für Schadsoftware auch mobile Arbeitsplätze, Parametriernotebooks und Programmiergeräte sowie die Schnittstellen für Fernzugriff und Fernwartung abdecken muss.

Anwendung im Projekt

Die vorliegenden Ausführungshinweise richten sich sowohl an Hersteller, Systemintegratoren und externe Planer auf Auftragnehmerseite als auch an unternehmensinterne Planer, Realisierer und Betreiber auf der Auftraggeberseite. Bei Lieferanten und Herstellern sind die Ausführungshinweise bereits für die Produkt- und Systementwicklung hilfreich und sollten deshalb frühzeitig berücksichtigt werden. Dies betrifft insbesondere die Weiterentwicklung von Systemen und Produkten.

Der Auftraggeberseite wird empfohlen, frühzeitig in der Planungsphase eine Schutzbedarfsfeststellung durchzuführen. Wenn ein erhöhter Schutzbedarf festgestellt wird, sollte sich daran eine individuelle Risikoanalyse anschließen. Auf den Ergebnissen aufbauend, muss für das geplante System detailliert spezifiziert werden, wie die einzelnen Anforderungen erfüllt werden sollen. Insbesondere in dieser Phase sollen die vorliegenden Umsetzungshinweise unterstützend wirken. Ist das geplante Projekt zur Ausschreibung vorgesehen, werden nach Ende der planerischen Phase die ermittelten Sicherheitsanforderungen in das Lastenheft übernommen. In der Ausschreibung sollten dann eine Kopie des Best-Practice-Papiers, konkretisierte Anforderungen, zusätzliche

Links zum Artikel

http://www.bdew.de/internet.nsf/id/it-sicherheitsempfehlunge
http://oesterreichsenergie.at/sichere-steuerungs-und-telekommunikationssysteme.html

Maßnahmen, Umsetzungsvorgaben sowie die zulässigen Abweichungen und Ausnahmen definiert werden.

Die Anbieter müssen im Angebot detailliert Stellung zur Umsetzung der technischen und organisatorischen Sicherheitsanforderungen nehmen. Auch eventuell notwendige Abweichungen und Alternativvorschläge sind zu dokumentieren. Der Ausschreibende muss die Vorschläge bewerten und bei der Zuschlagserteilung berücksichtigen. Falls Maßnahmen nicht angewendet werden sollen, sind die Gründe dafür durch die Planer, Realisierer oder Betreiber im Rahmen einer Risikoanalyse zu begründen. Nach der Vergabe müssen im Rahmen der Detailkonzeption und für das gegebenenfalls zu erstellenden Pflichtenheft eine ausreichende Berücksichtigung und die korrekte Umsetzung der definierten Sicherheitsanforderungen gewährleistet werden.

Sicherheitsanforderungen lassen sich bei Bestandssystemen nachträglich aufgrund technologischer Beschränkungen oft nur mit Einschränkungen umsetzen. Vereinzelt stellen Upgrades oder Erweiterungen eine Möglichkeit dar, um das Sicherheitsniveau zu erhöhen.

Wartung und Service

Die Sicherheitsbetrachtung ist nicht allein auf die Planungsphase und die Projektumsetzung begrenzt, sie hat auch Auswirkungen auf den gesamten Lebenszyklus der Systeme. Dies betrifft insbesondere die Wartung, Fehlerkorrekturen und die kontinuierliche Weiterentwicklung. Das Best-Practice-Papier gibt auch hier zu den relevanten organisatorischen Aspekten entsprechende Empfehlungen. So sollten mit den Systemlieferanten oder Dienstleistern bereits zum Zeitpunkt der Ausschreibung oder zur Projektumsetzung die relevanten Details zu Wartungsprozessen und sicherheitsspezifischen Dienstleistungen wie dem Patchmanagement und Schadsoftwareschutz geregelt sein. Alle IT-Komponenten, die zur Wartung genutzt werden, müssen ebenfalls den Sicherheitsanforderungen des Gesamtsystems entsprechen, unabhängig davon, ob sie dem Betreiber oder einem IT-Dienstleister gehören. Zur Überprüfung der korrekten Umsetzung der Anforderungen wird die Vereinbarung eines Auditrechts empfohlen.

Die von Oesterreichs Energie und BDEW gemeinsam erarbeiteten Ausführungshinweise zur Anwendung des BDEW-Whitepaper unterstützen Energieversorger und Hersteller dabei, Sicherheitsmaßnahmen für moderne EVU-Prozesssteuerungssysteme zu konkretisieren. So können die stetig wachsenden IT-Sicherheitsanforderungen bereits in der Projektplanung und bei der Beschaffung berücksichtigt werden.