Informationssicherheit für moderne Leitsysteme - Umsetzung der BDEW-Anforderungen

Kisters PraxisForum Energie – 18.05.2011

Dr. Stephan Beirer
s.beirer@gai-netconsult.de

Am Borsigturm 58, 13507 Berlin
Tel / Fax: +49 30 417898-0/-300
E-Mail: info@gai-netconsult.de
Web: www.gai-netconsult.de

GAI NetConsult GmbH

- Gegründet 1994
- 30 Mitarbeiter (Stand 05/2011)
- Standort Berlin
- Bundesweiter Kundenstamm vom Mittelstand bis zu Großkonzernen
- Bereich „Informationssicherheit" mit den Schwerpunkten Sicherheitsprüfung und Consulting / Konzeption
- Bereich „Entwicklung & Integration" mit der Erstellung sicherer eBusiness-Anwendungen
- Wichtige Branchenschwerpunkte…
  - Energieversorger, Finanzdienstleister
  - Gesundheitswesen, Chemie, Pharma, …
- PR-Aktivitäten…
  - Kostenfreies Periodical: Security *Journal*

Überblick Dienstleistungen der GAI NetConsult im Leittechnik-Umfeld

- Sicherheitsorganisation
  - Aufbau von Sicherheits-Managementsystemen (ISMS)
  - Konzepte zur Betriebsorganisation
  - Erstellung von Sicherheitsrichtlinien und Standards
  - IT-Notfallplanung
- Sicherheitskonzeption
  - Beratung zu Sicherheitsfragen beim Systemdesign
  - Unterstützung bei Ausschreibungen und Lasten/Pflichtenhefterstellung
  - Technische Sicherheitsmaßnahmen auf Systemebene
  - Konzeption sicherer Netzwerke und Schnittstellen
  - Evaluierung, Auswahl und Einführung von Sicherheitsprodukten
- Audits und Sicherheits-Reviews
  - Technische Überprüfungen von Systemen und Komponenten, z.B. Abnahmeprüfungen
  - Organisatorische Audits auf Basis anerkannter Standards wie ISO 27001/27002

bdew Whitepaper – Hintergründe und Zielsetzung

Hintergrund

- Moderne Steuerungs- und Regelungstechnik im Prozessbereich von Energieversorgern basiert inzwischen auf **Standard-IT-Technologien**.
- Die betrifft sowohl die zentrale Leittechnik, aber auch Stations- und Kraftwerksautomatisierung
- Ursprünglich wurden die Systeme für den Einsatz in isolierten, gut geschützten Bereichen konzipiert

- Dieses Inselprinzip lässt sich heute nicht mehr aufrechterhalten – moderne Leittechnikumgebungen verfügen i.d.R. über eine Vielzahl von Schnittstellen zu weiteren Systemen:
  - TCP/IP-basierte Fernwirkanbindungen
  - Fernwartungsschnittstellen zu Herstellern und Dienstleistern
  - Automatisiertes Dispatchnig per Mail oder Web-Services
  - Daten-Import/Export von und zur Büroumgebung
  - Dateneingabe und Parametrierungen von Büro-Arbeitsplätzen

- **Folge:** die Systeme sind in zunehmenden Maße **klassischen IT-Sicherheitsbedrohungen** ausgesetzt.

bdew Whitepaper

- 2008 wurde durch den bdew das Whitepaper *„Anforderungen an sichere Steuerungs- und Telekommunikationssysteme"* veröffentlicht.
- Das Whitepaper ist ein Best-Practice-Anforderungskatalog und wird für alle neuen Steuerungs- und TK-Systeme empfohlen.
- Es verpflichtet Lieferanten und Anlagenintegratoren auf die Einhaltung von grundlegenden **Regeln zur IT-Sicherheit**.

- Die Zielsetzung des Whitepapers ist dabei:
  - Angemessener Schutz gegen Sicherheitsbedrohungen im täglichen Betrieb
  - Gewährleistung einer Grundsicherheit der Systeme „ab Werk"
  - Sichere Integration in die vorhandene Prozessumgebungen
  - Ermöglichung eines langfristig sicheren Betriebs
  - Positive Beeinflussung der Produktentwicklung

- Das bdew-Whitepaper schreibt **nicht** vor, wie der sichere Betrieb durch den Betreiber erfolgt!
- Organisatorische Sicherheitsmaßnahmen auf Betreiberseite sind ebenfalls nicht im Fokus des Whitepapers.

Struktur des Whitepaper und abgedeckte Themenbereiche

- Allgemeines und Organisation
  - z.B. sichere Systemarchitektur, Patchfähigkeit, Support, Ansprechpartner für Sicherheitsfragen, Dokumentation
- Basis- und Betriebssysteme
  - z.B. Systemhärtung, Schadsoftware-Schutzkonzept, Benutzerverwaltung
- Netze und Kommunikation
  - z.B. Verwendung sicherer Protokolle, sichere Netzwerkstruktur, Absicherung von Wartungszugängen, Einsatz von Funknetzen
- Anwendungs-Software
  - z.B. Passwortsicherheit, Benutzeranmeldung, Autorisierung kritischer Aktionen, Protokollierung, Integritätsprüfung
- Entwicklung, Test und Rollout
  - z.B. Qualitätsmanagement, sichere Entwicklungssysteme, sichere Übertragung vertraulicher Daten, Behandlung von Sicherheitslücken
- Backup, Recovery, Notfallplanung
  - Test von Backup- und Recoverykonzepten, Notfallkonzeption, Wiederanlaufplan

Empfohlene Vorgehensweise

- Bestimmung des erforderlichen Sicherheitsniveaus:
  - Durchführung einer *Schutzbedarfsfeststellung,* z.B. nach BSI-Methodik
- Schutzbedarf „normal" → Anforderungen des WP ausreichend
- Erhöhter Schutzbedarf:
  - Individuelle Risikoanalyse
  - Ggf. Ableitung weiterer, spezifisch angepasster Maßnahmen
- In Ausschreibungen sind zu spezifizieren:
  - konkretisierte Anforderungen
  - zusätzliche Maßnahmen und Umsetzungsvorgaben aus der Risikoanalyse
  - zulässige Ausnahmen oder Workarounds
- Ermittelte endgültige Anforderungen werden in Lastenheft integriert und ihre Realisierung im Pflichtenheft spezifiziert.

Ausgewählte Umsetzungsbeispiele

Systemhärtung Betriebssystem/Firmware
(2.2.1: Grundsicherung und Systemhärtung)

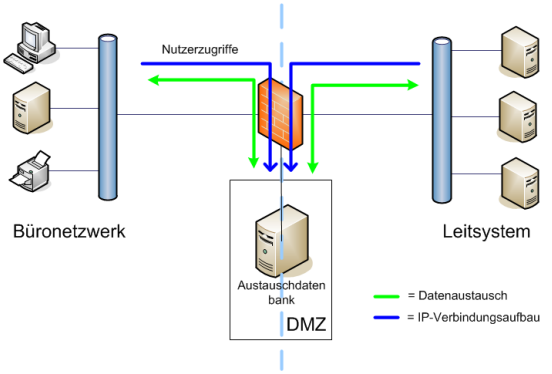
- Ausreichende Härtung der Betriebssysteme und Basiskomponenten, z.B. Applikationsserver, Datenbanken, X-Server, Hilfsapplikationen
- Keine Standardinstallation, sondern angepasstes Minimalsystem
  - Reduzierung installierter Programmpakete auf das notwendige Minimum
  - Deaktivierung unnötiger Netzwerkdienste
  - Sichere Dateirechte, Nutzer nur mit minimal notwendigen Rechten
- Deaktivierung aller Standardnutzer, Änderung von Auslieferungs-Passworten
- Aktivierung verfügbarer sicherheitserhöhender Optionen, z.B.
  - verschlüsselte Übertragung von Passworten/Nutzdaten in Netzwerkdiensten
  - Adressraum-Randomisierung *(Address Space Layout Randomization)*
  - Aktivierung des erweiterten Speicherschutzes *(NX, Data Execution Prevention)*

Sichere Netzwerke und Schnittstellen
(2.3.1 Sichere Netzwerkkonzeption und Kommunikationsverfahren)

- Nutzung sicherer Netzwerkprotokolle
  - Telnet → SSH
  - FTP → SFTP/SCP/FTPS
  - HTTP → HTTPS
- Absicherung aller Schnittstellen durch Firewall-Struktur, mehrstufiger Aufbau über Gatewaysysteme in DMZ
  - Prozessankopplung
  - Anbindung kaufmännische IT
  - Fernwartung
- Schutz der Datenübertragung in öffentlichen Netzen durch VPNs
  - Prozessankopplung und Fernwirkanbindung
  - Anbindung an Partnerunternehmen, z.B. TASE.2
  - Auch innerhalb des VPN-Tunnels sollte Firewalling/Port-Filterung aktiviert werden!

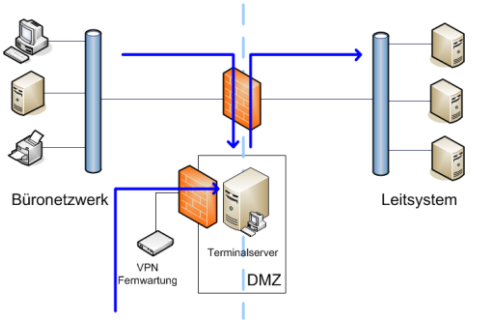
Beispiel:
Datenbank-Ankopplung Leitsystem-Büronetz

- Austauschdatenbank in separater DMZ-Zone
- Mechanismen zur Überprüfung aller (importierten) Daten auf Schadsoftware
- Verifizierung der Import/Export-Aufträge und -Daten
- Bei erhöhtem Schutzbedarf: zweistufige DMZ



Sichere Fernwartung
(2.3.2 Sichere Wartungsprozesse und RAS-Zugänge)

- Schutz der Fernwartungsverbindung durch VPN
- 2-Faktor Authentisierung für Zugriffe aus externen Netzen
- Entkopplung durch gehärteten Zugriffserver (z.B. Terminalserver)
  – keine transparente Netzwerkkopplung!
- Nutzung Terminalserver auch für interne Zugriffe möglich
- Platzierung in separaten Fernwartungs-DMZ
- Vertragliche Regelungen zur Absicherung der Wartungssysteme des Dienstleisters



Patchmanagement/Wartungsvertrag
(2.1.1.3 Patchfähigkeit, Patchmanagement)

- Regelungen zur Prüfung und Freigabe von Sicherheitsupdates
  - Basis-/Betriebssystem
  - Anwendungs-Software
  - Vom Hersteller gelieferte Drittsoftware
- Abstimmung von Testprozessen:
  - Auf Seiten des Herstellers
  - Durch den Betreiber
  - Klärung der Notwendigkeit einer Testumgebung
- Definition von Funktionen und Prozessen zur Patchinstallation
  - Installation im laufenden Betrieb (Nutzung Redundanzsystem)
  - Rollback-Verfahren

Backup und Notfallplanung
(2.6 Datensicherung/-wiederherstellung und Notfallplanung)

- Definition von Backup- und Restore-Verfahren
  - Anwendungsdaten
  - Systemdaten (Systeminstallation und Konfiguration)
  - Durchführung von Rücksicherungstests notwendig
- Unterstützung einer hinreichenden Notfallplanung des Betreibers
  - Sicherstellung eines Notbetriebs
  - Systemwiederaufbau bei schwerwiegenden Fehlern
  - Abhängig von den Nutzer-Anforderungen
  - Eine reine Hardware-Redundanz ist i.d.R. nicht ausreichend!

Sicherheits-Abnahmetests

Sicherheitstests
(2.1.1.8 Interne/externe Sicherheits- und Anforderungstests)

- Korrekte Umsetzung der Sicherheitsanforderungen sollte durch dedizierte Sicherheitstests geprüft werden, z.B. Abnahmetests.
- Prüfziele:
  - Verifikation der korrekten und effektiven Umsetzung der Sicherheitsmaßnahmen
  - Identifizierung konkreter, ggf. bisher nicht berücksichtigter Sicherheitslücken
- Zweistufiger Ansatz sinnvoll:
  - Scan- und Penetrationstests:
    - Netzwerkseitige Überprüfung
    - Identifikation konkreter Schwachstellen
    - Ggf. Ausnutzung zu Demonstrationszwecken
  - Detaillierter System- und Konfigurationsreview
    - Sichtung der Basisinstallation und der Konfiguration
    - Prüfung Firewallkonfigurationen
    - Inaugenscheinnahme der Applikation

Prüfungsumfang Sicherheitstests

- Prüfumfang
  - Alle Kernkomponenten
    - z.B. Leitrechner, Wartenplatz, abgesetzter Arbeitsplatz, Koppelrechner, Datenbankrechner,
  - Alle relevanten Schnittstellen(-komponenten)
    - Bürozugriff, Web- und Datenbankschnittstelle, Prozessanbindung, Fernwartung,
- Audit nur an einem vom Prozess isolierten Testsystem
  - im Rahmen der Werksprüfung/ Inbetriebnahmephase
  - Alternativ: Testsystem beim Systemhersteller
  - für Produktivumgebung typische Konfiguration und Parametrierung

Fragen & Antworten