Verteilnetzbetreiber Rhein-Main-Neckar

Prüfung und Zertifizierung der IT-Sicherheit der Querverbundleitstelle

Leitstellen und die dort installierten Leittechnikprodukte (Leitsysteme) werden zur Überwachung und Steuerung unterschiedlicher Industrieanlagen und Netze eingesetzt. Durch Veränderungen in der Leittechnik und die zunehmende Integration in die IT-Landschaft der Unternehmen verlieren Leitstellen ihren bisherigen Schutz. Mittlerweile ist eine Vielzahl von Vorfällen und Störungen bekannt, die durch vorsätzliche Angriffe gegen Netz- und Prozessleitstellen oder versehentliche Fehlbedienungen ausgelöst wurden. So entsteht die Notwendigkeit, Leitsysteme und Leitstellen durch zusätzliche Maßnahmen zu schützen.

Dipl.-Ing. ***Christian Freckmann***, Tüv Informationstechnik GmbH, Essen, Dipl.-Ing. ***Detlef Timmermann***, Consulectra Unternehmensberatung GmbH, Hamburg, Dipl.-Ing. ***Gerhard Regenbogen***, Dipl.-Ing. ***Detlef Thoma***, Verteilnetzbetreiber (VNB) Rhein-Main-Neckar GmbH & Co. KG, Darmstadt.

Typische Anwendungsbereiche für leittechnische Produkte gibt es beispielsweise in den Branchen der Energie- und Wasserversorgung, des Transports, der Ölindustrie, der chemischen und pharmazeutischen Industrie und der Papierindustrie.

Seit geraumer Zeit sind folgende Trends für die IT der Leittechnik erkennbar (*Bild 1*):

- zunehmende Verwendung von Standardsoftwareprodukten oder auch Open-Source-Produkten,
- Vernetzung der Leitsysteme mit anderen Netzwerken,
- Verwendung von Modemverbindungen und standardisierten Internetprotokollen,
- Import von technischen Informationen in die Leitsysteme.

Durch diesen Wandel in der Leittechnik und die zunehmende Integration in die IT-Landschaft der Unternehmen verlieren Leitstellen ihren bisherigen Schutz (Entkopplung, Isolierung). Mittlerweile ist eine Vielzahl von Vorfällen und Störungen bekannt, die durch vorsätzliche Angriffe gegen Netz- und Prozessleitstellen oder versehentliche Fehlbedienungen – begünstigt durch die genannten Trends – ausgelöst wurden. So entsteht die Notwendigkeit, Leitsysteme und Leitstellen durch zusätzliche Maßnahmen zu schützen.

Divergierende Schutzziele

Bestehende Sicherheitskonzepte der klassischen IT – z. B. der Unternehmenskommunikation – auf die Leittechnik zu übertragen, ist aufgrund der divergierenden Schutzziele nur bedingt möglich. So hat die klassische IT in Bezug auf Vertraulichkeit im überwiegenden Fall einen hohen Schutzbedarf, während der Schutz der Vertraulichkeit im Leittechnikbereich bei normalem Niveau einzustufen ist. Anders sieht es für die Schutzziele Integrität und Verfügbarkeit aus. Hier haben Leitsysteme einen hohen Schutzbedarf, während die klassische IT i. d. R. mit einem normalen Schutzbedarf auskommt (*Tafel 1*).

Risikofaktoren

Die Risikofaktoren im Bereich der Leittechnik sind vielfältig und in ihren Auswirkungen gravierend. Laut dem Basisschutzkonzept für kritische Infrastrukturen des Bundesministeriums des Innern werden die folgenden vier Risikofaktoren angenommen:

1. Risikofaktor Mensch, z. B. mangelndes Sicherheitsbewusstsein oder kriminelles Verhalten,
2. Risikofaktor Organisation, etwa Konzentration unverzichtbarer Ressourcen oder Outsourcing unternehmenskritischer Infrastrukturen,
3. Risikofaktor Natur und Umwelt, beispielsweise Naturkatastrophen oder Seuchen,
4. Risikofaktor IT mit:
   - Komplexität der Systeme,
   - zunehmender IT-Abhängigkeit,
   - umfangreicher, weltweiter Vernetzung von IT-Systemen,
   - kurzen Innovationszyklen der IT,
   - Standardisierung der Technik und Komponenten,

Schutzziele

	klassische IT	Leittechnik
Vertraulichkeit der Daten	hoch	normal
Integrität der Daten	normal	hoch
Verfügbarkeit des Systems	normal	hoch
Nichtabstreitbarkeit von Aktionen	normal	hoch

Tafel 1. Divergierende Schutzziele

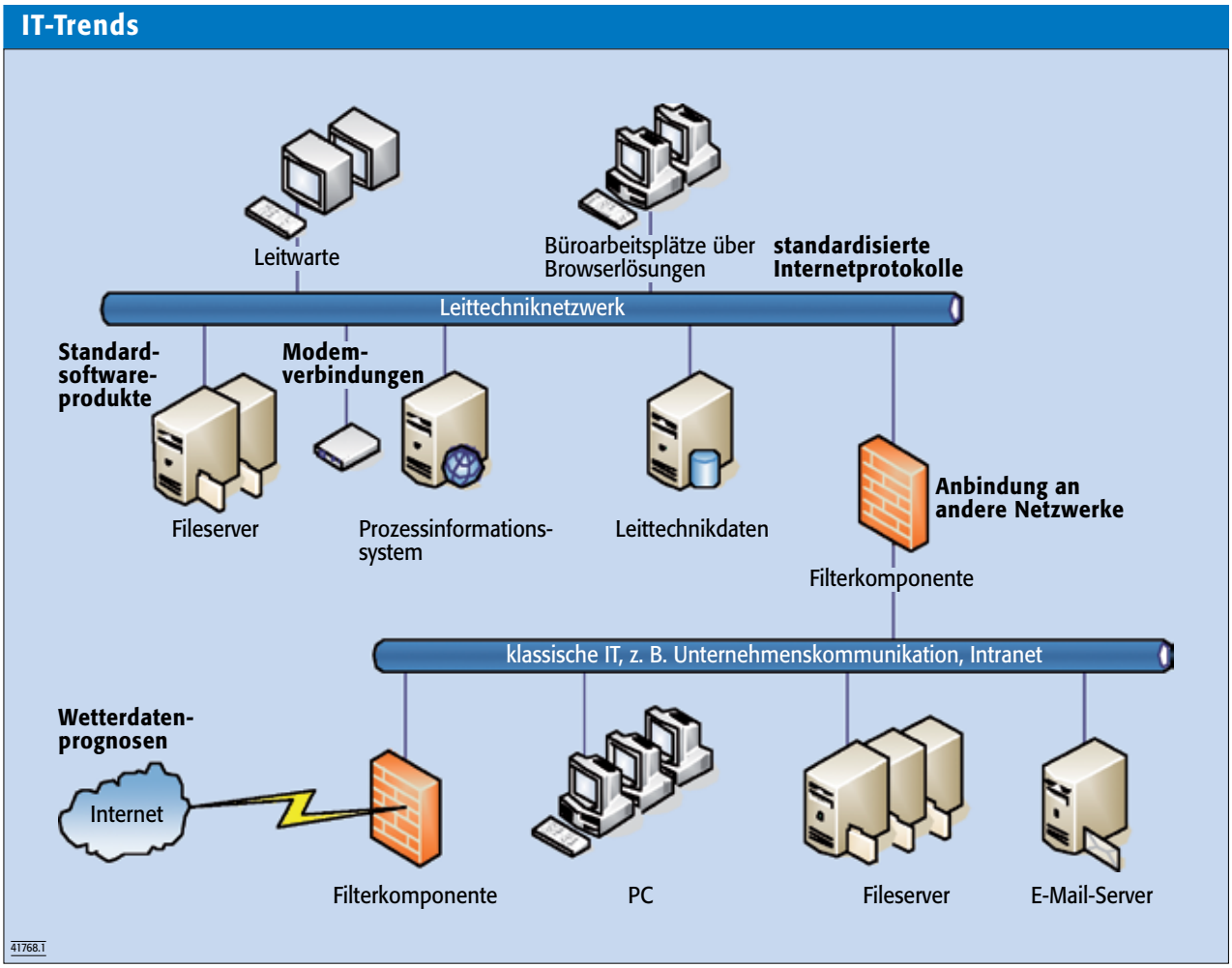

Bild 1. IT-Trends für Leitsysteme

- Vernetzung und Interdependenzen von kritischen Infrastrukturen
- und öffentliche Netze und Internet als Übertragungsmedium.

Zertifizierungsziele

Die verantwortungsvolle Wahrnehmung der Betriebsführungsaufgaben sollte zum Ziel haben, für Leitstellen und Leittechnikprodukte eine objektive Identifikation aller Sicherheitsrisiken und deren angemessene Reduzierung zu ermöglichen. Der implementierte Sicherheitsstatus sollte von einem unabhängigen Dritten geprüft und kann gegenüber allen Nutzern durch Ausstellung eines Zertifikats bestätigt werden.

Verteilnetzbetreiber Rhein-Main-Neckar

Aus der Fusion der Heag Versorgungs-AG und der Südhessischen Gas und Wasser AG entstand 2003 die Heag Südhessische Energie AG (HSE). Die HSE ist der größte eigenständige Energie- und Infrastrukturdienstleister in Südhessen. Im Netzgebiet der HSE leben rd. 1 Mio. Menschen in mehr als 70 Städten und Gemeinden.

Die zentrale Führung aller Versorgungsnetze obliegt der Verteilnetzbetreiber Rhein-Main-Neckar GmbH & Co. KG (VNB RMN), einer Tochtergesellschaft der HSE Netz AG. Dazu betreibt das Unternehmen eine Querverbundleitstelle (QVL) am Dornheimer Weg in Darmstadt und eine Notnetzleitstelle in der Frankfurter Straße in Darmstadt. Diese Leitstelle ist u. a. für die Betriebsführung der 28 Umspannanlagen (110/20 kV), 43 Schalthäuser und rd. 4 000 Transformatorenstationen im Strombereich zuständig. Das Stromleitungsnetz umfasst rd. 3 000 km Mittelspannungs- und rd. 7 500 km Niederspannungsleitungen. Im Gasbereich werden neben den 15 Übernahme- und Übergabestationen rd. 3 000 km Leitungsnetz im Hoch-, Mittel- und Niederdruckbereich betrieben. Weiterhin werden die Wasser- und Fernwärmenetze der HSE überwacht.

Zur Unterstützung des Betriebsführungspersonals in der Leitstelle hat VNB RMN ein Querverbundleitsystem vom Typ PSI-Control der PSI AG aufgebaut, das seit 2008 in Betrieb ist und in dem die Sparten Strom, Gas, Wasser und Fernwärme geführt werden. Daneben haben die Mitarbeiter Zugriff auf weitere IT-Systeme (z. B. GIS, Office-Anwendungen) sowie die erforderlichen Telekommunikationseinrichtungen. VNB RMN übernimmt werktags nach Dienstschluss sowie an Wochenenden und Feiertagen die Tätigkeiten der Netzleitstelle der Aschaffenburger Versorgungs-

Vorgehen	
Inhalte	Ergebnisse
1. Vorprüfung	
• Organisation/Prozesse • technisches Konzept • Dokumentation	• zentrale Defizite • Maßnahmen VNB RMN
2. technische Untersuchung	
• technische Tests und Inspektionen	• Defizite Systemtechnik • Maßnahmen PSI
3. Vorbereitung Zertifizierung	
• Vervollständigung Istaufnahme • Regelwerk/ISMS	• internes Regelwerk mit allen notwendigen Festlegungen • technische Sicherheit
4. Zertifizierung	
• Prüfung der Voraussetzungen im notwendigen Umfang	• Qualifizierungsbericht • Zertifikat

Tafel 2. Vorgehensmodell

GmbH (AVG). Das Leitsystem von AVG ist hiermit ein Mandant im Querverbundleitsystem von VNB RMN. Die QVL mit ihren Einrichtungen der Netzleit-, Informations-, Kommunikations- und Übertragungstechnik spielt für die Versorgungsqualität in den Netzen von VNB RMN eine Schlüsselrolle. Es bedarf deshalb besonderer technischer und organisatorischer Vorkehrungen, um die Arbeitsfähigkeit der Leitstelle jederzeit sicherzustellen. Dabei bilden die aktuellen Normen und Vorschriften zur IT-Sicherheit den entsprechenden Rahmen.

Vor diesem Hintergrund hat VNB RMN entschieden, die IT-Sicherheit der QVL durch ein unabhängiges, externes Beratungsunternehmen überprüfen und zertifizieren zu lassen. Der Auftrag zur Beratung wurde an die Consulectra Unternehmensberatung GmbH, und der Auftrag zur Prüfung und Zertifizierung an die Tüv Informationstechnik GmbH (Tüv IT) erteilt.

Betrachtungsgegenstand ist die Informations- und Kommunikationssicherheit aller Arbeitsprozesse innerhalb der spartenübergreifenden Netzführung. Neben den rein technischen Risiken müssen hierbei auch die Risikofaktoren Mensch, Organisation, Natur und Umwelt in die Gesamtbetrachtung einbezogen werden.

Projektablauf

Basis der Prüfung und Zertifizierung war das Whitepaper des BDEW. Es wurde untersucht, ob die relevanten Anforderungen durch die QVL erfüllt werden.

Zielstellung des Projektes
Folgende Schwerpunkte wurden als Zielstellung formuliert:

- Prüfung der IT-Sicherheit der neuen QVL von VNB RMN,
- Umsetzung des Sicherheitskonzepts durch ein Regelwerk,
- Regelwerk als Grundlage einer späteren Zertifizierung,
- Optimierung des Aufwands zur Erreichung der erforderlichen IT-Sicherheit und der anschließenden Zertifizierung,
- Einbeziehung der AVG-Anbindung in ein Mandantensystem.

Vorgehensweise
Als erster Schritt der Bearbeitung (*Tafel 2*) auf dem Weg zum Zertifikat sollte eine Vorprüfung die bestehenden Defizite und erforderlichen Umsetzungsmaßnahmen ermitteln. Dazu diente ein Kriterienkatalog, der die Anforderungen des BDEW-Whitepapers enthielt. Der aktuelle Stand bei VNB RMN und der relevanten Dienstleister wurde festgestellt durch:

- Interviews mit den Systemadministratoren und den Betriebsführern,
- Vor-Ort-Aufnahmen in den Warten- und Rechnerräumen sowie repräsentativen Anlagentypen mit Anbindung an das Querverbundleitsystem,
- Sichtung der vorhandenen Dokumentation und Bedienungshandbücher für Administration und betriebliche Nutzung,
- Schnittstellen- und Netzwerkanalyse mit Penetrationstest an den Außenschnittstellen des Querverbundleitsystems.

Ein Bericht dokumentierte die Ergebnisse, wobei der Schwerpunkt auf den erforderlichen Maßnahmen zur Erhöhung der IT-Sicherheit bzw. zur Umsetzung der ermittelten Maßnahmen lag.

Ein Ergebnis der Vorprüfung war z. B., dass die eingesetzten Router im Fernwirknetz ausgetauscht werden mussten. Bereits Ende der 1990er Jahre ging ein umfangreiches Routernetz zur Anbindung der Fernwirktechnik in Betrieb. Diese Router funktionieren nach wie vor. Jedoch waren mit den mehr als zehn Jahre alten Geräten die aktuellen Sicherheitsanforderungen (z. B. Nutzung von sicheren Protokollen) nicht mehr einzuhalten. Die Erkenntnisse aus der Vorprüfung führten zu einem Ersatz der Router durch eine aktuelle Gerätegeneration.

Parallel zur Umsetzung der technischen Maßnahmen erarbeitete die Consulectra Unternehmensberatung federführend das IT-Sicherheitskonzept der Rechnersysteme im Bereich der QVL.

Dieses IT-Sicherheitskonzept regelt die Festlegungen zu:

- Geltungsbereich,
- Richtlinien zur Informationssicherheit (Information Security Policy),
- Regeln für die Benutzung der Rechnersysteme,
- Kontinuitäts- und Notfallplanung,
- Zugriffs- und Berechtigungssteuerung,
- Systementwicklung und -pflege.

Die sich häufig ändernden Angaben und Festlegungen – wie die zugelassenen Benutzer mit ihren Rechten – sind in Anlagen zum Sicherheitskonzept dokumentiert. Das gesamte IT-Sicherheitskonzept einschließlich der Anlagen wird in einem Wiki »IT-Sicherheit« innerhalb des Intranets verwaltet, auf das der relevante Benutzerkreis Zugriff hat. Über die Standardfunktionen des Wikis können Änderungen dokumentiert und als Grundlage für spätere Rezertifizierungen verwendet werden.

Das IT-Sicherheitskonzept gilt auch für Mandanten, die das QVL nutzen, und alle Dienstleiter (z. B. Systemhersteller, Betreiber des Informationsnetzwerkes, Stations- und Fernwirktechnikbereich), die zur Einhaltung des Sicherheitskonzepts verpflichtet wurden. Nach Inkraftsetzung des Regelwerks und dem Abschluss der Umsetzungsmaßnahmen konnte die letzte Phase – die eigentliche Prüfung und Zertifizierung – in Angriff genommen werden.

Zertifizierung

Die Funktionssicherheit von Leitsystemen kann nur durch ein

ganzheitliches Schutzkonzept optimiert werden. Die Sicherheitsaspekte auf dem Gebiet der Netzwerke, IT-Systeme und komplexen IT-Anwendungen sind ebenso wichtig wie die organisatorische und die physikalische Sicherheit. Für die beiden letztgenannten Sicherheitsaspekte gibt es zunehmend Verfahren und Lösungen, wogegen die IT-Sicherheit von Leitsystemen – abgesehen von den Ansätzen in den IT-Grundschutzkatalogen – bislang kaum systematisch untersucht wurde.

Das Regelwerk von Tüv IT setzt hier an und hilft, gezielt und vollständig die Gegebenheiten zu erfassen, zu beurteilen und zu bewerten. Zur Prüfung und Zertifizierung von komplexen IT-Systemen und IT-Produkten unter Berücksichtigung der genannten Maßnahmen hat Tüv IT die Prüfmethodik der sicherheitstechnischen Qualifizierung (SQ) entwickelt. Die SQ wurde als standardisiertes Verfahren in das Trusted-Zertifizierungsprogramm von Tüv IT aufgenommen als

- Trusted Site Security (TSS) für IT-Systeme und
- Trusted Product Security (TPS) für IT-Produkte.

Diese Prüfmethodik ermöglicht die Untersuchung von IT-Systemen und IT-Produkten unter Berücksichtigung der i. d. R. anzutreffenden Heterogenität, Komplexität und Dynamik. Sie orientiert sich dabei am CESG Tailored Assurance Service (CTAS) der britischen CESG.

Bei der Absicherung komplexer IT-Systeme und IT-Produkte sollen sowohl technische als auch infra-strukturelle, organisatorische und personelle Maßnahmen zum Einsatz kommen. Das Prüfverfahren TSS/TPS konzentriert sich auf die technische und prozedurale Sicherheit von Systemen und Produkten. Für die Überprüfung und Zertifizierung der übrigen Aspekte stehen ähnliche Verfahren aus dem Trusted-Zertifizierungsprogramm zur Verfügung.

Die SQ zeichnet sich durch ein systematisches, ingenieurmäßiges Vorgehen aus, das eine deutlich höhere Flexibilität bietet als beispielsweise das reine Abarbeiten von Checklisten. Dadurch kann sie vom relativ einfachen Einzelprodukt bis hin zu hochkomplexen Netzwerken für sehr unterschiedliche Anwendungsfälle zum Einsatz kommen.

Bild 2. Übergabe des Abschlussberichts und des Zertifikats

IT-Systeme und -Produkte, die auf Basis der Prüfmethodik der SQ erfolgreich geprüft wurden, können mit einem Zertifikat ausgezeichnet werden, das zur Nutzung der Prüfzeichen TSS oder TPS berechtigt. Dazu müssen die einzelnen Prüfkriterien der SQ erfüllt sein. Diese umfassen je nach Anwendungsfall und angestrebter Vertrauenswürdigkeit das Aufstellen technischer Sicherheitsanforderungen, Forderungen an Architektur und Design, eine Revision der Entwicklungsprozesse, Installations- und Betriebsvorgaben, die Durchführung von Schwachstellenanalysen und Penetrationstests, eine Prüfung des verwendeten Sourcecodes sowie Forderungen an ein geeignetes Änderungsmanagement.

Zertifikat und Prüfzeichen

Basierend auf den Prüfkriterien für TSS/TPS kann bei der Erfüllung aller Teilaspekte für das untersuchte Prüfobjekt ein Zertifikat erteilt werden, das zur Nutzung des Prüfzeichens TSS oder TPS berechtigt. Eine Zusammenfassung der Prüfkriterien ist auf der Rückseite des Zertifikats abgedruckt. Das Zertifikat gilt zwei Jahre und kann danach verlängert werden. Das Prüfzeichen steht sowohl für die Website als auch für Broschüren und Verpackungen des Auftraggebers zur Verfügung. Ebenso werden das Prüfzeichen und das Zertifikat auf der Internetseite von Tüv IT veröffentlicht. Der Auftraggeber hat das Recht, einer solchen Veröffentlichung zu widersprechen.

Am 6. September 2012 fand die Übergabe des Abschlussberichts und die Projektschlussbesprechung mit der Geschäftsführung von VNB RMN statt (*Bild 2*).

(41768)

c.freckmann@tuvit.de

detlef.timmermann@consulectra.de

gerhard.regenbogen@vnb-rmn.de

detlef.thoma@vnb-rmn.de

www.tuvit.de

www.consulectra.de

www.vnb-rmn.de