Netzleittechnik

IT-Sicherheit und Penetrationstests an einem Netzleitsystem

Die Netzleitstelle der Stromnetz Hamburg GmbH ist zuständig für die Netzführung und das Störungsmanagement des Hoch- und Mittelspannungsnetzes im Verteilungsnetzgebiet der Freien und Hansestadt Hamburg sowie im Westmecklenburgischen Verteilungsnetzgebiet der Wemag Netz GmbH. Nach umfangreichem Upgrade und Erneuerung des Netzleitsystems sollte dessen IT-Sicherheit überprüft werden. Neben dem Erstellen eines Handbuchs zur IT-Sicherheit gehörten auch unterschiedliche Penetrationstests zu diesem Projekt.

Die Stromnetz Hamburg GmbH führt mit ihrem Netzleitsystem Versorgungsgebiete in Hamburg und in Westmecklenburg. In *Tafel 1* sind die Kennzahlen der Versorgungsnetze und in *Bild 1* und *2* ihre räumliche Ausdehnung und Struktur dargestellt.

Im Jahr 2012 wurde ein umfangreiches Upgrade- und Erneuerungsprojekt des Netzleitsystems IDS High Leit der Stromnetz Hamburg abgeschlossen. Nachdem das komplexe Netzleitsystem entsprechend der zum Projektabschluss bestehenden Anforderungen der geltenden Normen, des BDEW-Whitepapers sowie der Best-Practice-Erfahrungen ausgeprägt wurde, sollten die Prozesse des Netzbetriebs und des Betriebs des Netzleitsystems den Anforderungen der IT-Sicherheit gerecht werden.

Dazu beauftragte Stromnetz Hamburg die Consulectra Unternehmensberatung GmbH mit folgenden Leistungen:

- Erstellung eines Handbuchs für die IT-Sicherheit des Netzleitsystems
- Ermittlung der erforderlichen Prozesse zur Umsetzung des gesteckten Sicherheitsziels
- Durchführung eines Penetrationtests am Netzleitsystem.

Einen besonderen Schwerpunkt legte das Management dabei auf die prozessuale Sicht der Anforderungen der IT-Sicherheit. Das erarbeitete Handbuch wurde kurzfristig in das betriebliche Regelwerk aufgenommen. Die Vorgehensweise und Ergebnisse des Projekts sind Gegenstand dieses Aufsatzes. Ein ähnliches Projekt fand gleichzeitig für die Stromnetz Berlin GmbH statt.

Bild 1. Versorgungsgebiet Hamburg

Vorgehensweise

Als erster Schritt wurden die geltenden Richtlinien und Vorschriften des Konzerns auf Relevanz für die Netzführung und das Netzleitsystem beider Gesellschaften geprüft. Dabei wurde festgestellt, dass die bestehenden Regelungen nahezu ausschließlich für die Systeme der kommerziellen IT und der Bürowelt gelten. Für die kritischen IT-Systeme der Netzführung wird zu Recht auf separate Regelungen der Fachbereiche verwiesen. Dies sind Systeme der Zone 1 und 2. In *Bild 3* ist das allgemeine Zonenkonzept zu sehen.

Danach wurde ein Handbuch für die IT-Sicherheit des Netzleitsystems in einer Projektgruppe erarbeitet, in der Mitarbeiter der Systemadministration, die verantwortlichen Mitarbeiter der Netzführung beider Gesellschaften sowie der IT-Sicherheitsbeauftragte des Unternehmens vertreten waren. Dabei wurden besprechungsbegleitend Textentwürfe für das Regelwerk zu den folgenden Themen erstellt, in der Projektgruppe in Besprechungen diskutiert sowie anschließend entsprechend angepasst.

Nach Fertigstellung des Handbuchs wurden die resultierenden Prozesse zur Umsetzung des Regelwerks ermittelt und dokumentiert. Diese Prozesse zur Erreichung der definierten Sicherheitsziele erfordern einen integrierten Sicherheitsmanagementprozess (ISMS) nach IEC 27001. Der Ablauf ist in *Bild 4* dargestellt. Der integrierte Sicherheitsmanagementprozess ist eine zentrale Komponente im Entwurf des Sicherheitskatalogs der BNetzA gemäß § 11, Absatz 1a EnWG. Er gewährleistet die kontinuierliche Überwachung und Überprüfung, ob das Regelwerk eingehalten wird, und ermittelt erforderliche Maßnahmen zur Anpassung.

In den Prozess des Sicherheitsmanagements sind folgende Personen eingebunden:

- Leiter des Bereichs Netzbetrieb
- Leiter des Bereichs Netzführung
- Verantwortliche gemäß Zonenkonzept
- Administratoren.

Penetrationstest

Um die Sicherheit des Netzleitsystems zu überprüfen, entschloss sich Stromnetz Hamburg, einen Penetrationstest durchzuführen. Um den Betrieb nicht zu gefährden, wurde eine reale Testumgebung geschaffen. Zur Verfügung standen ein Bedienarbeitsplatz, ein Leitrechner und eine Fernwirkschnittstelle, die mit einem exakt nachgebildeten Netzwerk und der entsprechenden Übertragungstechnik miteinander verbunden waren.

Durchgeführt wurde der Penetrationstest durch Mitarbeiter der Tüv-IT, die keinerlei Informationen über Netzwerk und Konfiguration des Netzleitsystems oder Ähnliches erhielten. Zu unterscheiden waren zwei Szenarien:

- Szenario 1: innerer Penetrationstest
- Szenario 2: äußerer Penetrationstest.

Im Szenario 1 erhielt das Testteam Zugang zum internen Netzwerk des Leitsystems. Angenommen wurde dabei das erfolgreiche Eindringen in den Schutzbereich der Netzführung und das unbemerkte Infiltrieren des Netzwerks zwischen MMI und Leitsystem. Das Testteam hatte 8 h Zeit, um entsprechende Analysen und Zugriffe zu versuchen.

Im Szenario 2 wurde dem Testteam ein Zugang zu einer Unterstation der Stationsleittechnik gewährt. Hier wurde das erfolgreiche Eindringen in den Schutzbereich einer Unterstation unterstellt. Auch für dieses Szenario bekam das Testteam 8 h Zeit.

Zusammenfassend kann festgestellt werden, dass dem physikalischen und organisatorischen Schutz der zentralen Komponenten des Netzleitsystems und seiner unter- und überlagerten Systeme eine hohe Bedeutung zukommt.

Die Befunde zeigen, dass bereits heute ein hohes Sicherheitsniveau erreicht ist, einige Aufgaben jedoch noch umzusetzen sind.

Kennzahlen der Netze

Asset	Hamburg	Westmecklenburg	Summe
			
Umspannwerke	53	33	86
Netzstationen	7500	3200	10700
Freileitung	1372 km	7709 km	9081 km
Kabel	26073 km	6649 km	33122 km
Systemlänge gesamt	27445 km	14358 km	41803 km
Höchstlasten	2013 MW	429 MW	2442 MW
Anschlusspunkte	1124226	164207	1288000
Einwohner	1812709	292980	2106000
Versorgungsfläche	757 km^2	8683 km^2	9438 km^2

Tafel 1. Kennzahlen der beiden Versorgungsnetze; Stand: Hamburg 12/2012, Wemag 12/2009

Bild 2. Versorgungsgebiet Westmecklenburg

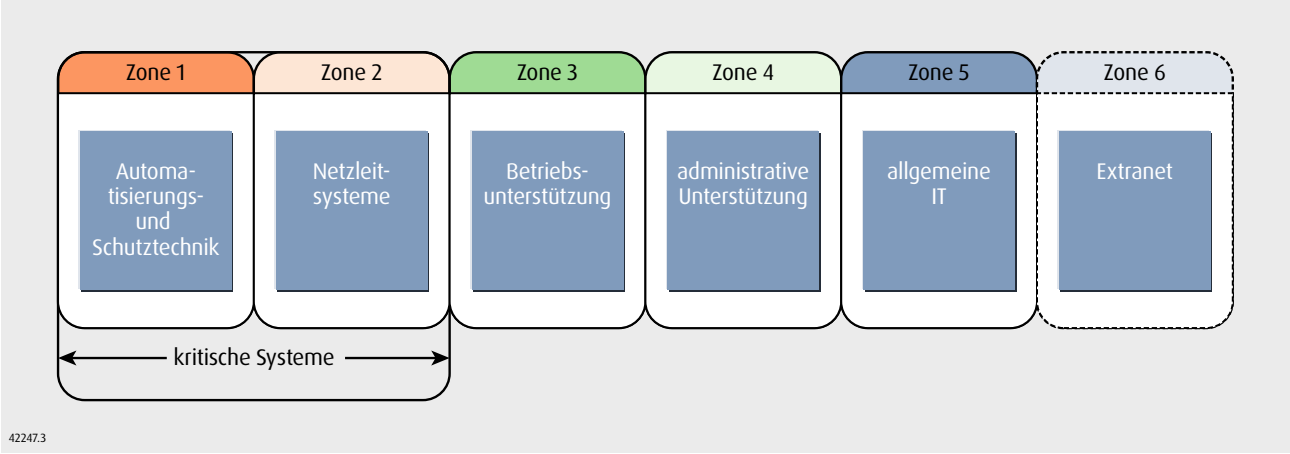

Bild 3. Kritische IT-Systeme in einem Zonenkonzept

Handbuch für die IT-Sicherheit des Netzleitsystems

Das Handbuch wurde in folgende Abschnitte gegliedert:

- Klassifizierung der Informationen und Anwendungen
- Abgrenzung der Verantwortungen, Rechte und Pflichten
- Systemdokumentation
- Betrieb und Administration des Gesamtsystems
- Maßnahmenplanung bei besonderen Ereignissen
- Zugriffs- und Berechtigungssteuerung
- Systementwicklung und -anpassung.

Bei der Erstellung des Handbuchs wurde großer Wert auf die nötige Umsetzbarkeit der bestehenden Richtlinien und Vorschriften im täglichen Netzführungsbetrieb gelegt. Das erfordert die enge Einbindung der verantwortlichen Mitarbeiter in die Diskussion und Ausprägung der Regeln. Nur so können die definierten Sicherheitsziele pragmatisch in realisierbare Verfahrensanweisungen umgesetzt werden.

Stromnetz Hamburg hat die ermittelten Prozesse mit den bereits praktizierten Prozessen verglichen und so den erforderlichen Aufwand zur Umsetzung abschätzen können. Ein Beispiel für einen solchen Prozess ist die Systemhärtung. Hierzu zählen unter anderem:

- Deinstallieren oder Deaktivieren unnötiger Softwarekomponenten, die häufig im Rahmen der Systemerstellung benötigt werden
- Deaktivieren unnötiger System- und Kommunikationsdienste
- Aktivieren sicherheitserhöhender Konfigurationsoptionen
- Deaktivieren unnötiger Kommunikations- und Datenträgerschnittstellen (zum Beispiel CD/DVD, USB, Bluetooth, WLAN)
- Entfernen von Standardusern und Standardpasswörtern
- Entfernen von Usern des Herstellers, die nicht zum After-Sale-Support gehören.

Im Rahmen des Wartungsvertrags wurden zwischen der Stromnetz Hamburg und dem Systemlieferanten zyklische Updates sowie regelmäßige Systemhärtungsmaßnahmen einschließlich Sicherheitspatches vereinbart. Die Sicherheitspatches enthalten Maßnahmen zum Virenschutz und zum Schutz vor Malware. Die unternehmensseitige

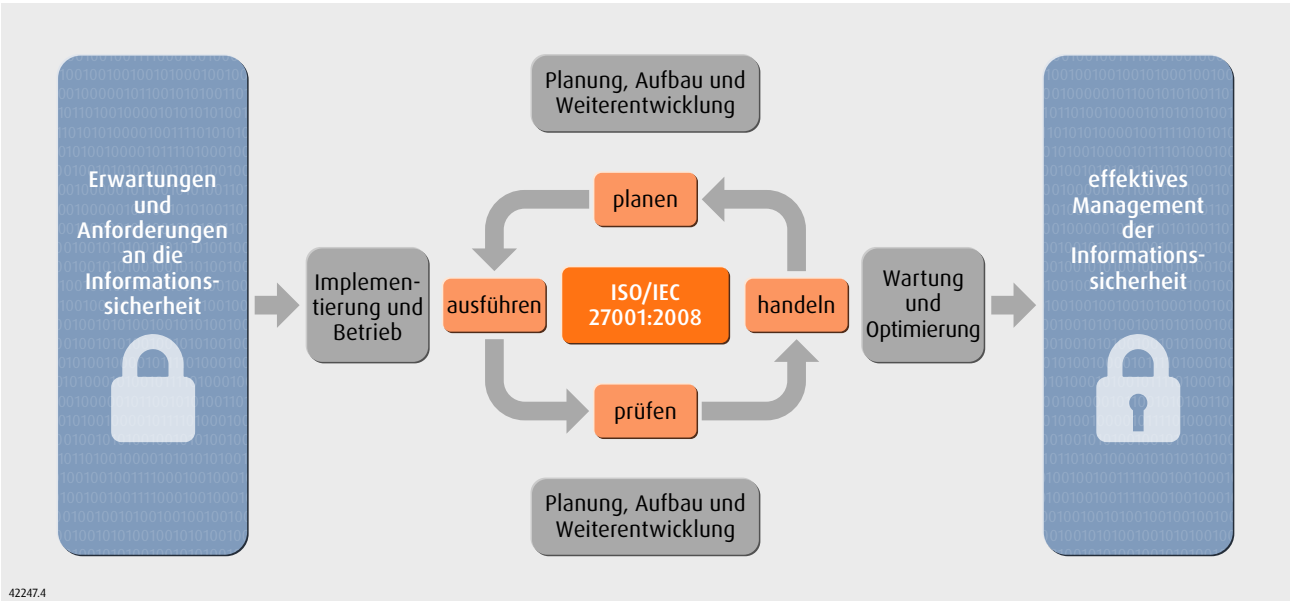

Bild 4. Integrierter Sicherheitsmanagementprozess nach IEC 27001

Bild 5. Netzleitwarte der Stromnetz Hamburg

Firewall wird jedoch vom Auftraggeber in eigener Verantwortung administriert.

Ein weiteres Beispiel ist die Maßnahmenplanung bei besonderen Ereignissen. Die erforderlichen Regelungen sind in detaillierten Verfahrensanweisungen beschrieben und dokumentiert. Die erforderliche Handlungssicherheit bei derartigen Ereignissen wird im Rahmen jährlich durchzuführender Übungen nachgewiesen.

An dieser Stelle sei darauf hingewiesen, dass in einem Handbuch zur IT-Sicherheit Doppelregelungen oder widersprüchliche Regelungen zu anderen Vorschriften zwingend zu vermeiden sind. Existieren Regeln, sollte auf diese verwiesen werden und nicht die Regelung verbal beschrieben werden. So können auch künftig entstehende Widersprüche vermieden werden.

Um eine permanente Überarbeitung des Handbuchs zu vermeiden, wurden dynamische Dokumentationen, wie Inventarlisten von Komponenten des Netzleitsystems oder Listen berechtigter Personen, in Anlagen zum Handbuch aufgenommen. Auf diese Weise können Anlagen auch kurzzyklisch ausgetauscht werden, ohne das Handbuch neu aufzulegen.

Es kann festgestellt werden, dass die zahlreichen Anforderungen bezüglich der IT-Sicherheit bereits in der Vergangenheit nach bestem Wissen und Gewissen gelebt wurden. Jedoch wurden die Verfahren nicht im erforderlichen Detailgrad dokumentiert beziehungsweise strukturiert behandelt. Das erarbeitete Handbuch führt nicht zu einer neuen Quantität, sondern eher zu einer besseren Qualität der Dokumentation der Maßnahmen zur Gewährleistung einer möglichst hohen und auch wirtschaftlichen IT-Sicherheit.

Ausblick

Das Handbuch für die IT-Sicherheit des Netzleitsystems wurde im Rahmen einer Abschlusspräsentation des Projekts in Kraft gesetzt. Es gilt, die darin dokumentierten Regelungen im Alltag des Leitstellenbetriebs mit Leben zu füllen. Einige der ermittelten Prozesse zur Umsetzung des Handbuchs sind detailliert zu dokumentieren und die bestehenden Dokumente aufzunehmen.

Für das Geschäftsjahr 2014/15 ist das Netzleitsystem bezüglich bestehender Schwachstellen weiter zu analysieren und für eine Zertifizierung vorzubereiten. Der Anforderungskatalog der BNetzA sieht in seinem ersten Entwurf eine entsprechende Zertifizierungspflicht für Netzbetreiber vor.

Zusammenfassend kann festgestellt werden, dass Stromnetz Hamburg im Bereich der Netzführung für die gegenwärtigen und künftigen Anforderungen bezüglich der IT-Sicherheit bestens gerüstet ist.

Dipl.-Ing. **Gero Boomgaarden**, Leiter Netzbetrieb, Stromnetz Hamburg GmbH, Hamburg

Dipl.-Ing. **Detlef Timmermann**, Projektleiter, Consulectra Unternehmensberatung GmbH, Hamburg

>> gero.boomgaarden@stromnetz-hamburg.de
d.timmermann@consulectra.de

>> www.stromnetz-hamburg.de
www.consulectra.de

42247