Informationssicherheitsleitlinie der Thyssengas GmbH

Inhaltsverzeichnis

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht.

1 Einleitung

Die Geschäftsführung der Thyssengas GmbH verabschiedet hiermit folgende Leitlinie zur Informationssicherheit als Bestandteil ihrer Unternehmensstrategie.

Aufgrund der Weiterentwicklung der Informationstechnik unterliegen diese Informationssicherheitsleitlinie und die darauf aufbauenden Richtlinien einer ständigen Anpassung und Weiterentwicklung. Die Informationssicherheitsleitlinie ist allen interessierten Parteien der Thyssengas GmbH in der jeweils aktuell gültigen Fassung zur Verfügung gestellt.

2 Geltungsbereich

Der Gültigkeitsbereich dieser Informationssicherheitsleitlinie umfasst das gesamte Unternehmen und alle internen und externen Mitarbeiter (im folgenden Mitarbeiter genannt), sowie unter der Steuerung von Thyssengas GmbH arbeitende Dienstleister.

3 Informationen und Sicherheit

3.1 Stellenwert der Informationssicherheit

Die Thyssengas GmbH ist ein mittelständisches, reguliertes, deutsches und deutschsprachiges Unternehmen.

Informationen sind grundlegende Faktoren für den Geschäftsbetrieb und für die Erreichung der Unternehmensziele. Diese stellen Unternehmenswerte der Thyssengas GmbH dar.

Alle wesentlichen, strategischen und operativen Funktionen und Aufgaben werden durch informationsverarbeitende Systeme maßgeblich unterstützt. Die Definition und Umsetzung der Ziele und Grundsätze der Informationssicherheit erfolgt daher anhand der strategischen Ausrichtung der Thyssengas GmbH, mit Integration der Anforderungen des ISMS in die Geschäftsprozesse.

Alle Beteiligten (Kunden, Geschäftspartner, Gesellschafter, Regulierungsbehörden etc.) müssen sich darauf verlassen können, dass die Thyssengas GmbH die Sicherheitsverantwortung für die von ihr verarbeiteten Informationen gewissenhaft wahrnimmt und Informationen vor missbräuchlicher Verwendung schützt.

3.2 Zielsetzung der Informationssicherheit

Informationsverarbeitung spielt eine Schlüsselrolle für die Aufgabenerfüllung bei der Thyssengas GmbH. Informationen kommen in verschiedenster Form (elektronische Daten, Papierform, mündliche Informationen etc.) vor und sind auf die Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität der Informationen angewiesen.

Die Trennung der Schutzziele Authentizität und Integrität ist in der Praxis nur schwer durchzuführen und wurde daher aus Sicht des BSI in der Aufzählung des Sicherheitskatalogs im Schutzziel Integrität subsummiert.

Zur Wahrung der Informationssicherheit dienen deshalb die folgenden Schutzziele:

- **Vertraulichkeit**
  Vertraulichkeit bedeutet Schutz vor Offenlegung von Informationen.
- **Integrität**
  Integrität bedeutet Schutz vor Änderung von Informationen durch nicht berechtigte Personen und stellt die Richtigkeit, Konsistenz und Vollständigkeit von Informationen dar.
- **Verfügbarkeit**
  Verfügbarkeit bedeutet, dass Prozesse, Informationen, Funktionen und Informationssysteme immer dann verfügbar sind, wenn sie bearbeitet bzw. in Anspruch genommen werden müssen.

Der Thyssengas GmbH ist dabei bewusst, dass Sicherheit nur in einem ausgewogenen Verhältnis der vorgenannten Schutzziele sinnvoll möglich ist, so ist Vertraulichkeit ohne Integrität ebenso wenig sinnvoll, wie ohne Verfügbarkeit. Diese Schutzziele müssen für jedes Thema ggf. spezifisch in Ihrer Priorität festgelegt werden, um sinnvolle Maßnahmen ergreifen zu können. Da wir als reguliertes Unternehmen im Vergleich zu anderen Unternehmen ein hohes Maß an Markttransparenz haben, ist für uns das Schutzziel Verfügbarkeit von höchster Priorität. Jedoch müssen die drei Schutzziele in den jeweiligen Geschäftsprozessen analysiert und festgestellt werden.

Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informations- und Kommunikationstechnik (IKT) maßgeblich unterstützt. Ein Ausfall von IKT-Systemen muss insgesamt kurzfristig kompensiert werden können. Auch in Teilbereichen dürfen unsere Prozesse und Systeme nicht ausfallen. Da unsere Kernprozesse auf die sichere Verarbeitung und Verbreitung von Informationen angewiesen sind, ist der Schutz dieser Informationen vor unberechtigtem Zugriff und vor unerlaubter Änderung von existenzieller Bedeutung.

3.3 Grundsätze der Informationssicherheit

Verspätete oder fehlerhafte Managemententscheidungen können weitreichende Folgen nach sich ziehen. Daher ist für das Management bei wichtigen Entscheidungen der Zugriff auf aktuelle Steuerungsdaten wichtig. Für diese Informationen ist ein hohes Sicherheitsniveau in Bezug auf Verfügbarkeit und Integrität sicher zu stellen.

IKT-Systeme werden sowohl für die Netzsteuerung, als auch für die Bürokommunikation eingesetzt. Die historisch bedingte Trennung wird zunehmend durch die Konvergenz der technischen Entwicklung aufgeweicht. Entsprechend ist eine enge Abstimmung bzgl. der Ziele, Herausforderungen, Bedrohungen, und Maßnahmen wichtig.

Die Netzsteuerung hat hohe Anforderungen an Verfügbarkeit, Vertraulichkeit und Integrität. Wir beteiligen uns an relevanten Kommunikationsinfrastrukturen für Lageberichte und Warnmeldungen sowie zur Bewältigung großflächiger IKT-Krisen.

Für uns ist die Aufrechterhaltung der Kommunikation nach außen zu den Kunden, Geschäftspartnern und Regulierungsbehörden elementar. Die Geschäftsabwicklung darf nicht verzögert oder gar gefährdet werden. Wenn vertraglich festgelegte Liefermengen und ggf. Lieferfristen nicht eingehalten werden können, kann dies weitreichende negative Folgen haben. Insbesondere eine mangelhafte Verfügbarkeit der IKT-Systeme und der Daten, aber auch Fehlfunktionen können zu Erlösminderungen führen. Die Aufrechterhaltung der Kommunikation und der ständige Zugriff auf korrekte Daten für die Mitarbeiter haben einen hohen Schutzbedarf.

Die Daten einiger Prozesse und einiger Bereiche haben sehr hohe Vertraulichkeitsanforderungen. Durch technische Maßnahmen und die hohe Aufmerksamkeit der Mitarbeiter wird die Vertraulichkeit geschützt und Manipulationen vorgebeugt.

Innerhalb der Leittechnik werden die Verfügbarkeit und die Funktionstüchtigkeit der Systeme sichergestellt. Stillstandzeiten sind nur in einem sehr geringen Maße akzeptabel. Die Thyssengas GmbH orientiert sich bezüglich der Akzeptanz von Stillstandzeiten und deren Auswirkungen an der DVGW G1001 M (Merkblatt Risikomanagement) vom März 2015.

Die Nutzung des Internets zur Informationsbeschaffung und zur Kommunikation ist für uns selbstverständlich. E-Mail dient als Ersatz oder als Ergänzung von anderen Bürokommunikationswegen. Durch entsprechende Maßnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.

Des Weiteren verlangen die Datenschutzgesetze und die Interessen unserer Mitarbeiter eine Sicherstellung der Vertraulichkeit der Mitarbeiterdaten.

3.4 Ziele der Informationssicherheit

Das Fundament dieser Informationssicherheitsleitlinie bilden die folgenden Grundsätze, an denen sich sämtliche Sicherheitsmaßnahmen und -vorgaben ausrichten und die für alle im Geltungsbereich tätigen Personen verbindlich sind.

1. Für Unternehmenswerte wie Informationen, IT-Systeme und IT-Anwendungen sind Eigentümer benannt, die für die Sicherheit der jeweiligen Unternehmenswerte verantwortlich sind.
2. Risiken aus der Nutzung der Informationen und Informationssysteme sind frühzeitig zu identifizieren und auf ein akzeptiertes Restrisiko zu minimieren.
3. Kosten und Nutzen von Informationssicherheitsmaßnahmen stehen in einem angemessenen wirtschaftlichen Verhältnis.
4. Vorgaben und Maßnahmen orientieren sich an anerkannten Standards und Best Practices zur Informationssicherheit.
5. Gesetzliche, regulatorische, vertragliche und sonstige Vorgaben für die Informationssicherheit sind zu identifizieren und durch angemessene Maßnahmen umzusetzen.
6. Zugriff, Zugang und Zutritt zu den Informationswerten sind auf das notwendige Maß zu beschränken.
7. Alle wesentlichen Aktivitäten und Ereignisse im Bereich Informationssicherheit müssen transparent und im erforderlichen Umfang nachvollziehbar sein. Verfahren für den Betrieb bzw. die Wiederherstellung des Betriebes der wesentlichen Informationssysteme sind zu dokumentieren. Sofern erforderlich, ist ein Notfallplan und ein Wiederanlaufplan zu erstellen und in das Notfallmanagement der Thyssengas GmbH zu integrieren.
8. Für die an der Verarbeitung von Informationen beteiligten Mitarbeiter müssen angemessene Vorkehrungen zur Gewährleistung der Vertrauenswürdigkeit getroffen werden.
9. Die Mitarbeiter werden hinsichtlich des sicheren Umgangs mit Informationswerten informiert, geschult und sensibilisiert. Sie sind angehalten, die entsprechenden Vorgaben umzusetzen.

4 Gesamtgesellschaftliche Verantwortung

Wir stellen uns unserer gesamtgesellschaftlichen Verantwortung als Betreiber einer kritischen Infrastruktur KRITIS[1] und sind immer darauf bedacht den Betrieb unseres Gastransportnetzes stets sicher aufrecht zu erhalten.

Thyssengas GmbH ist ein eigenständiges Unternehmen, wir erfüllen alle Aufgaben als vollfunktionsfähiger Transmission System Operator (TSO). Wir haben die Hoheit sowohl über das Asset als auch über die technischen und kommerziellen Aufgaben eines Independent Transport Operator (ITO).

Unsere Unternehmenswerte bzw. Assets sind:

- Menschen, mit Ihren Qualifikationen, Erfahrungen und Fähigkeiten
- Leitungen, GDRM- und Verdichteranlagen
- Unsere Prozesse, Verfahren und Abläufe
- Informationen als Ergebnisse unserer Prozesse
- Hardware und Software
- Reputation und Ansehen
- Dienste

Unsere Informationen und unsere IKT-Systeme in allen Bereichen werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandzeiten toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten und IKT-Systemen sollen nur in geringem Umfang und so selten wie möglich vorkommen.

5 Informationssicherheitsmanagementsystem (ISMS)

Um die dauerhafte Wirksamkeit der Informationssicherheit und ihrer Maßnahmen sicherzustellen und ihrer Gesamtverantwortung für die Informationssicherheit nachzukommen, führt die Thyssengas GmbH in 2017 ein ISMS nach DIN ISO/IEC 27001, in der aktuell gültigen Version, ein und verankert dieses als einen zentralen Führungsprozess in der Organisation, um es in Teilbereichen zertifizieren zu lassen. Der Informationssicherheitsbeauftragte (ISB) steuert, kontrolliert und entwickelt das ISMS im Auftrag der Geschäftsführung kontinuierlich weiter. Die Aufgaben aller Beteiligten im Rahmen des ISMS sind detailliert im ISMS-Handbuch der Thyssengas GmbH beschrieben.

Die Umsetzung des ISMS bei der Thyssengas GmbH entspricht den formulierten Anforderungen und Vorgaben des IT-Sicherheitskataloges der Bundesnetzagentur gemäß §11 Absatz 1a des Energiewirtschaftsgesetzes.

5.1 Methodik für das Informationssicherheitsmanagementsystem

Das ISMS der Thyssengas GmbH wird auf Basis dieser Informationssicherheitsleitlinie, Richtlinien und Sicherheitskonzepten geführt. Diese sind innerhalb der relevanten Geschäftsprozesse umzusetzen.

Die in Kapitel 3.4 definierten Informationssicherheitsgrundsätze werden in Richtlinien und Sicherheitskonzepten konkretisiert. Die detaillierte und aktuelle Übersicht der Dokumente befindet sich in der Anlage zur Informationssicherheitsleitlinie.

Die Anlage zur Informationssicherheitsleitlinie ist als intern klassifiziert.

[1] Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden [www.kritis.bund.de]

6 Verbesserung der Sicherheit

Die Leitlinie zur Informationssicherheit, sowie nachgelagerte Dokumente, wie Richtlinien und Konzepte werden regelmäßig auf ihre Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeitern bekannt sind, ob sie umsetzbar und in den Betriebsablauf integrierbar sind.

Die Geschäftsführung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben, z.B. durch Hinweise oder Verbesserungsvorschläge.

Zur kontinuierlichen Bewertung und Verbesserung des ISMS und seiner Prozesse ist die Einführung eines Auditprogramms zur Informationssicherheit erforderlich. Dieses bietet die Möglichkeit, Abweichungen von den Zielen des ISMS zu identifizieren und zeitnah zu bewerten.