Thüringer Mess- und Zählerwesen

Leitlinie

Schutzklasse: öffentlich

Gültig ab: 01.07.2019

Informationssicherheit der TMZ

TMZ Thüringer Mess- und Zählerwesen Service GmbH

Thüringer Mess- und Zählerwesen
Digital unterschrieben von Lutze, Jörn
Datum: 2020.05.19 12:58:27 +02'00'

GFM-T

Thüringer Mess- und Zählerwesen
Digital unterschrieben von Berger, Lutz
Datum: 2020.05.19 12:26:00 +02'00'

GFM-V

Inhaltsverzeichnis

1 Einleitung

Für die Thüringer Mess- und Zählerwesen Service GmbH (nachfolgend TMZ genannt) haben Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität von Informationen einen außerordentlich hohen Stellenwert. Aufgrund der Bedeutung der Informations- und Kommunikationstechnik (IKT) für einen sicheren Betrieb der Smart Meter Gateway Administrationsprozesse (SMGW-A) ist die Informationssicherheit innerhalb der strategischen unternehmerischen Ziele von großer Tragweite zu sehen.

Die Informationssicherheit ist ein sich schnell entwickelndes Umfeld. Beinahe täglich gibt es Veröffentlichungen zu neuen Sicherheitslücken oder Angriffsszenarien. Zusammengefasst wird dies gern mit der Devise „Sicherheit ist kein Produkt, sondern ein Prozess". Entsprechend muss sich auch das Informationssicherheitsmanagementsystem (ISMS) der TMZ fortlaufend an neue Gegebenheiten und Herausforderungen anpassen. Erreicht wird dies durch einen kontinuierlichen Verbesserungsprozess.

Die Geschäftsführung der TMZ ist verpflichtet, auf der Grundlage der einschlägigen gesetzlichen Regelungen ein ISMS aufzubauen, zu betreiben und zertifizieren zu lassen.

2 Rahmenbedingungen

2.1 Kontext

Die vorliegende Leitlinie zur Informationssicherheit bildet den Ausgangspunkt für die darauf aufbauende Struktur zu Richtlinien der Informations- und IT-Sicherheit sowie zu entsprechenden Arbeitsanweisungen, Prozessbeschreibungen, technischen Konzepten und betrieblichen Dokumentationen. Insofern werden mit ihr Ansatz, Ziele und Methoden zur dauerhaften Gewährleistung einer angemessenen Informationssicherheit im Unternehmen beschrieben.

Die Leitlinie zur Informationssicherheit ist zudem Auftrag an die Sicherheitsorganisation der TMZ. Durch die Leitlinie soll sichergestellt werden, dass dem jeweiligen Schutzzweck angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahmen ergriffen werden, um Informationswerte und personenbezogene Daten hinreichend zu schützen sowie die Verfügbarkeit von informations- bzw. kommunikationstechnischen Verfahren einschließlich der sie unterstützenden Systeme der IKT zu gewährleisten.

Dabei sind insbesondere:

- Prozesse zur Steuerung, Überwachung und Verbesserung der Informationssicherheit zu etablieren,
- risikoorientierte Richtlinien und Arbeitsanweisungen zu erlassen sowie deren Umsetzung und Effektivität fortlaufend zu überwachen und zu verbessern.

2.2 Adressaten

Die Inhalte dieser Leitlinie sind verbindlich für das Personal der TMZ (Arbeitnehmer, Mitarbeiter aus Arbeitnehmerüberlassung, Praktikanten, Werkstudenten, Auszubildende). Weiterhin sind die Inhalte verbindlich für Dritte, die:

- Geschäftsprozesse der TMZ als Dienstleistung ausführen,
- an Geschäftsprozessen der TMZ teilnehmen,
- auf interne, nicht öffentliche Informationen zugreifen,
- Zugang zu internen IKT-Systemen bekommen und
- Zutritt zu Räumlichkeiten mit Bezug zu Informationen oder zur Informationsverarbeitung haben.

2.3 Erfüllung des gesetzlichen Rahmens

Zur Zulassung vom Bundesamt für Sicherheit in der Informationstechnik (BSI) sind Anbieter von SMGW-A-Dienstleistungen verpflichtet Risikoanalysen durchzuführen und angemessene Maßnahmen zum Schutz der IKT zu ergreifen und diese permanent den Erfordernissen anzupassen.

Zur Steuerung der dazu notwendigen Prozesse sind ein Informationssicherheitsmanagementsystem nach DIN EN ISO/IEC 27001:2017 einzuführen, Maßnahmen entsprechend der DIN EN ISO/IEC 27002:2017 und BSI TR 03109-6 umzusetzen sowie die Wirksamkeit des ISMS durch ein Zertifikat nachzuweisen.

3 Informationssicherheit der TMZ

3.1 Schutzziele der Informationssicherheit

Eine der Grundlagen des gesellschaftlichen Lebens in der Bundesrepublik Deutschland besteht in einer zuverlässig funktionierenden Energieversorgung. Ein länger anhaltender flächendeckender Ausfall der Energieversorgung hätte gravierende Folgen für das gesamte Gemeinwesen. In der modernen Energieversorgung mit einer Vielzahl dezentraler Erzeugungsanlagen kommt der Steuerbarkeit von Erzeugern und Verbrauchern eine zentrale Bedeutung zu. Die Einführung intelligenter Steuerungsalgorithmen und –technologien birgt Risiken, durch Schädigung oder Angriff auf die hochkomplexen Systeme bzw. deren Ausfall.

Die Schutzziele zur Gewährleistung eines sicheren Mess- und Steuerungsbetriebes umfassen:

- **die Sicherstellung der Verfügbarkeit der zu schützenden Systeme und Daten,**

  (Gewährleistung des nutzbaren und bedarfsorientierten Zugangs zu Systemen, Informationen und zugehörigen Werten für berechtigte Benutzer)

- **die Sicherstellung der Integrität der verarbeiteten Informationen und Systeme,**

  (Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden)

- **die Gewährleistung der Vertraulichkeit der mit den betrachteten Systemen verarbeiteten Informationen,**

  (Gewährleistung des physikalischen beziehungsweise logischen Zugangs zu Informationen nur für Zugriffsberechtigte)

- **die Sicherstellung der Authentizität von Informationen und Identitäten.**

  (Sicherstellung der nachweisbaren Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit von Informationen und Identitäten)

3.2 Vertragliche Anforderungen an die Informationssicherheit

Im Rahmen von Service Level Agreements (SLAs) mit Dritten vereinbart die TMZ Qualitätsziele und deren Einhaltung mit qualitativen und quantitativen Anforderungen bzw. Angaben (u. a. Reaktionszeiten und Verfügbarkeiten). Bei Notwendigkeit werden entsprechende Vertraulichkeitsvereinbarungen abgeschlossen bzw. vertraglich vereinbart.

3.3 Informationssicherheitsmanagementsystem

Die Beschreibung des Informationssicherheitsmanagementsystems umfasst die Leitlinie, Richtlinien, Arbeitsanweisungen, Prozesse sowie weitere betriebliche Dokumentationen (Abb. 1).

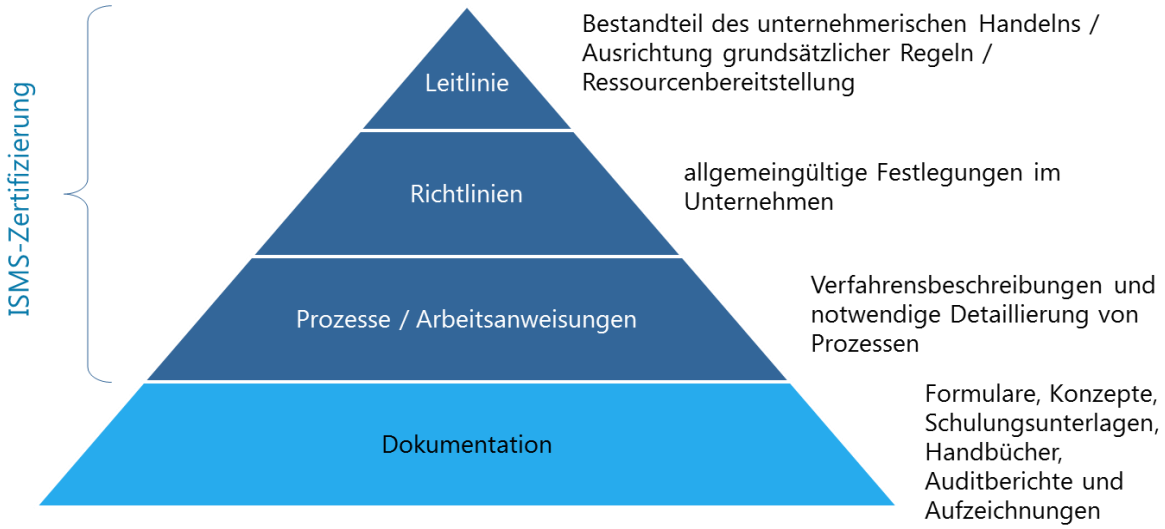

Abb. 1: Dokumentenpyramide des Informationssicherheitsmanagementsystems

3.4 Sicherheitsmaßnahmen

Unternehmensinformationen sind ein wichtiger Vermögenswert. In digitaler wie in physischer Form müssen diese ordnungsgemäß behandelt werden, um sie vor Verlust und Diebstahl zu schützen und um sicherzustellen, dass sie dem Unternehmen jederzeit zur Verfügung stehen.

Um die Informationssicherheit zu garantieren, sind die folgenden Sicherheitsmaßnahmen notwendig:

- technische Maßnahmen (physischer Art, Hardware, Software, Konfigurationen)
- organisatorische Maßnahmen (verbindliche Regeln und Vorgaben)
- personelle Maßnahmen (Schulung, Personalmanagement)

Die Sicherheitsmaßnahmen werden in

- Richtlinien,
- Arbeitsanweisungen und
- Prozessbeschreibungen

geregelt und in

- Technischen Handbüchern,
- Dokumentationen und
- Aufzeichnungen

beschrieben und nachgewiesen.

Als verbindliche Sicherheitsmaßnahmen gelten insbesondere:

- Jeder, der Informationen nutzt, ist im Rahmen der Vorgaben für deren Sicherheit verantwortlich.
- Jede schützenswerte Information ist gemäß dem erforderlichen Sicherheitsniveau zu behandeln.
- Nur eindeutig ausgewiesene Personen mit entsprechenden Berechtigungen erhalten Zugang bzw. Zugriff auf schützenswerte Informationen.
- Berechtigungen für den Zugriff auf Informationen werden nur dann vergeben, wenn es für die jeweilige Tätigkeit notwendig ist. Es werden nur die Berechtigungen vergeben, die im Rahmen der Aufgabenerfüllung benötigt werden.
- Jeder Mitarbeiter ist aufgefordert, jederzeit aktiv an der Erkennung und Vermeidung von Sicherheitsvorfällen mitzuwirken.
- Alle Systeme der IKT werden gemäß den Richtlinien und Arbeitsanweisungen genutzt.
- Soweit möglich, werden personalisierte Benutzerkennungen und Passwörter benutzt, welche zweckgebunden vergeben werden.
- Der Grundsatz eines aufgeräumten Büros bzw. Schreibtisches sowie des „leeren" Bildschirms wird beachtet.

4 Organisation

4.1 Aufbau der Sicherheitsorganisation

Zur Erlangung der Wirksamkeit des ISMS wird eine Sicherheitsorganisation im Unternehmen etabliert, welche alle Aktivitäten zur Lenkung, Umsetzung und Verbesserung der Informations-sicherheit überwacht.

Folgende Gremien werden definiert:

- ❖ Management-Gremium „Informations- und IT-Sicherheit"
- ❖ Notfall-Gremium (engl. Emergency Response Team, ERT)
- ❖ Änderungs-Gremium (engl. Change Advisory Board, CAB)

Folgende Rollen und Verantwortlichkeiten werden definiert:

- ❖ **Geschäftsführung**
  - Gesamtverantwortung für die Informationssicherheit und die IKT-Systeme des Unternehmens
    - ✓ Initiieren und Koordinieren des ISMS
    - ✓ Ressourcen für das ISMS zur Verfügung stellen
    - ✓ Besetzung der Rollen und Verantwortlichkeiten
    - ✓ Integration der Anforderungen des ISMS in die Geschäftsprozesse
    - ✓ Festlegung der Ziele der Informationssicherheit
    - ✓ Awareness für Informationssicherheit sicherstellen
    - ✓ Sicherstellung von Schulungen zur Informationssicherheit

- ✓ organisatorische Verankerung von Aktivitäten zur Etablierung, Erhaltung und Weiterentwicklung des ISMS
- ✓ angemessene Einbettung des ISMS in die Strukturen und Hierarchien
- ✓ Gesamtverantwortung für die Risiken der Informationssicherheit in Bezug auf das ISMS der TMZ

❖ **Informationssicherheitsbeauftragte/r der TMZ**
- Umsetzung der Ziele der Informationssicherheit
- Berichtspflicht an die Geschäftsführung

❖ **ISMS-Organisation der TEAG**
- Etablierung, Erhaltung, kontinuierliche Verbesserung und Weiterentwicklung des ISMS
- Integration des ISMS in die Geschäftsprozesse und entsprechende Kontrolle

❖ **IT-Administratoren und IT-Koordinatoren (extern)**
- Umsetzung der festgesetzten Maßnahmen des ISMS

❖ **Verantwortliche /r Personalmanagement (extern)**
- Sicherstellung der Umsetzung von personellen Maßnahmen und Schaffung der Voraussetzungen

❖ **Verantwortliche /r Facility-Management (extern)**
- Sicherstellung der Umsetzung aller Maßnahmen und Schaffung der Voraussetzungen für Verwaltungsstandorte

❖ **Mitarbeiter /innen**
- Einhaltung der Vorgaben zur Informationssicherheit über ihr entsprechendes Verhalten im Arbeitsumfeld

4.2 Unterweisungs- und Sensibilisierungsmaßnahmen

Um sicherzustellen, dass das Personal der TMZ die für sie zutreffenden Richtlinien und Arbeitsanweisungen sowie diese Leitlinie kennt und beachtet, erfolgt regelmäßig eine Unterweisung über die Vorgaben des ISMS. Die Wirksamkeit dieser Unterweisungen wird im Rahmen von Audits/Reviews sowie selektiv durch die Befragung der Mitarbeiter überprüft.

Dies bedeutet im Einzelnen:

- regelmäßige Unterweisungen des Personals sicherzustellen,
- neues oder versetztes Personal über Informationssicherheit und das ISMS zu informieren,
- Personal über Problematiken und Risiken regelmäßig zu informieren (mindestens jährlich),
- Unterweisungen über Gefahren und Maßnahmen der Informationssicherheit für Personal in besonders sensitiven Bereichen durchzuführen.

4.3 Sanktionen

Für die Einhaltung der in dieser Leitlinie definierten Rahmenbedingungen, Regeln und Vorgaben zur Informationssicherheit sind neben den Mitarbeitern auch dessen Vorgesetzte verantwortlich. Die Regelungen dieser Leitlinie entfalten im Arbeitsverhältnis direkte Wirkung. Die Nichtbeachtung ihrer Inhalte kann damit arbeits- oder sonstige zivil- und/oder strafrechtliche Konsequenzen haben.

5 Kontinuierlicher Verbesserungsprozess

Durch eine kontinuierliche Verbesserung der Regelungen und deren Einhaltung (PDCA Zyklus) mittels jährlicher interner Audits, eine beständige Rückkopplung von Verbesserungsmöglichkeiten von Seiten der Mitarbeiter an den Informationssicherheitsbeauftragten sowie die Nutzung konzerninterner Erkenntnisse zu Verbesserungsmöglichkeiten über die ISMS-Organisation der TEAG, wird das angestrebte Informations- bzw. IKT-Sicherheitsniveau sichergestellt. Abweichungen sollen mit dem Ziel analysiert werden, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand zu halten. Im Rahmen eines kontinuierlichen Verbesserungsprozesses unterliegt die vorliegende Leitlinie einer regelmäßigen Verbesserung und Aktualisierung.

Das bedeutet insbesondere:

- regelmäßige Überprüfung von Einhaltung, Aktualität und Wirksamkeit der Leitlinie,
- zwingende Überprüfung der Leitlinie (Veränderungen der Bedrohungslagen, Änderungen von Technologien, aktuellen Ereignissen, gesetzlichen o. normativen Änderungen),
- monatliche Überprüfung des Maßnahmenabarbeitungsstandes in Quentic durch den ISB,
- mindestens jährliche Überprüfung (z. B. im Rahmen eines internen Audits).

6 Änderungsdokumentation

Version	Datum	Änderung	Name / OE
1.0	12.06.2019	Ersterstellung	v.Rein, Dr. Stöpel
1.1	28.02.2020	Überarbeitung Abs. 4.1	Dr. Stöpel
1.2	19.05.2020	Kap. 5, Ergänzung monatliche Maßnahmen	Dr. Stöpel