IT-Sicherheitsleitlinie

Ziel und Zweck dieser Anweisung

Diese Anweisung beschreibt die Organisation der IT-Sicherheit bei Gasunie Deutschland (GUD) und die grundsätzliche Ausrichtung und Gestaltung des GUD Informationssicherheitsmanagementsystems (ISMS) sowie der zu Grunde liegenden Rahmenbedingungen und Prinzipien.

Inhaltsverzeichnis

1. Notwendigkeit und Stellenwert der Informationssicherheit

GUD steht für einen sicheren und zuverlässigen Gastransport. Aufgrund seiner besonderen Bedeutung für das Funktionieren des Gemeinwesens stellt ein zuverlässiger Gastransport eine kritische Dienstleistung im Sinne des § 10 Absatz 1 Satz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik dar.

Für die Sicherstellung des Gastransportes sowie die Ausführung weiterer wesentlicher Geschäftsprozesse ist GUD abhängig von einer funktionsfähigen und sicheren Informationsverarbeitung. Zudem stellen Informationen und Systeme, mit denen Informationen elektronisch verarbeitet werden, einen erheblichen Unternehmenswert dar. Aufgrund der zentralen Bedeutung informationsverarbeitender Systeme für die Geschäftsprozesse und der weltweit steigenden Zahl von Angriffen auf IT-Systeme hat die Informationssicherheit einen hohen Stellenwert bei GUD.

Die Hauptrisiken für die elektronische Informationsverarbeitung bei GUD sind länger anhaltende Ausfälle von geschäftskritischen Systemen, die Gefährdung von geschäftskritischen Systemen und Informationen durch Schadsoftware, Manipulationen oder kriminelle Personen sowie der Diebstahl oder die Verfälschung schützenswerter Informationen. Diese Bedrohungen können zur einer temporären Nichtverfügbarkeit und dem Verlust der technischen Integrität von Systemen führen sowie in einen ernsthaften Datenverlust resultieren. Hierdurch kann die Versorgungssicherheit beeinträchtigt und für GUD ein finanzieller Schaden sowie ein Ansehensverlust in der Öffentlichkeit entstehen.

2. Erfordernisse und Erwartungen interessierter Parteien an die IT-Sicherheit

Neben den eigenen Anforderungen an die IT-Sicherheit zur Aufrechterhaltung des Geschäftsbetriebes unterliegt GUD gesetzlichen, behördlichen sowie vertraglichen Vorgaben, welche einzuhalten sind.

Kunden und Partner verlassen sich darauf, dass an GUD übermittelte Informationen sowie vertragliche Vereinbarungen ausreichend vor dem Zugriff und der Einsichtnahme durch unberechtigte Personen geschützt werden und die kontrahierten Leistungen zuverlässig und sicher von GUD erbracht werden. Eine Übersicht der interessierten Parteien sowie relevanter interner und externer Themen ist in Anlage MM-2-112-001-02 dargestellt.

Darüber hinaus sind eine Reihe von behördlichen Vorgaben und Gesetzen umzusetzen und einzuhalten. Hierbei handelt es sich insbesondere um die im Juli 2015 durch das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) geschaffenen neuen Regelungen des Gesetzes über die Elektrizitäts- und Gasversorgung (EnWG), das

Bundesdatenschutzgesetz und den „IT-Sicherheitskatalog" der Bundesnetzagentur. Eine Liste der für GUD relevanten Gesetze und behördlichen Vorgaben mit Bezug zur Informationssicherheit findet sich in Anlage MM-2-112-001-01.

3. Ziel der IT-Sicherheit

Entsprechend den eigenen Anforderungen sowie den Erfordernissen und Erwartungen von Kunden, Partnern und Behörden ist es das Ziel der IT-Sicherheit bei GUD, die Verfügbarkeit von Informationen bzw. der Systeme, mit denen diese verarbeitet werden, so zu schützen, dass die Vertraulichkeit, die Integrität sowie die Verfügbarkeit in einem dem jeweiligen Stellenwert der Informationen angemessenen Maß gesichert sind.
Die Schutzziele sind dabei wie folgt definiert:

- **Vertraulichkeit:** Schutz von Informationen vor nicht genehmigter Preisgabe oder unbefugtem Zugriff
- **Integrität:** Schutz der Informationen und Systeme vor unerlaubter Manipulation (Veränderung bis hin zur Löschung und Zerstörung)
- **Verfügbarkeit:** Schutz vor ungeplantem Stillstand der Systeme und Nichtverwendbarkeit der Informationen.

4. Informationssicherheitsmanagementsystem (ISMS)

Zur Erreichung der vorgenannten Schutzziele hat die GUD-Geschäftsführung beschlossen, ein Informationssicherheitsmanagementsystem (ISMS) entsprechend den Anforderungen der internationalen Normen zur Informationssicherheit ISO 27001 in Verbindung mit den Vorgaben des IT-Sicherheitskatalogs der Bundesnetzagentur einzuführen, aufrecht zu erhalten und ständig zu verbessern.

4.1 Zertifizierung des ISMS

Die Normkonformität des ISMS wird für alle IT-Systeme, die für einen sicheren Netzbetrieb notwendig sind, regelmäßig unabhängig durch eine anerkannte akkreditierte Prüfstelle geprüft und im Rahmen einer Zertifizierung bestätigt. Von der Zertifizierung erfasst sind das zentrale Netzleitsystem, das Prozessdatenübertragungsnetzwerk (PDÜ), das Wide Area Network (WAN) sowie die dezentralen Prozessleitsysteme der Verdichter- sowie Mess- und Regelstationen. Zusätzlich befinden sich für die Sicherstellung des Netzbetriebes erforderliche Gasapplikationen sowie die dazu gehörigen Server und Datenbanken als auch das Exchange- und Citrix-System im Scope der Zertifizierung.

4.2 Grundsätzliche Gestaltung des ISMS

Das GUD ISMS ist integraler Bestandteil des Gasunie Deutschland Managementsystems (GMS). Die im Rahmen des GMS definierten allgemein gültigen unternehmensweiten Pro-

zesse und Regelungen finden auch für das ISMS Anwendung. Dieses gilt auch für die Vorgaben zur Erstellung, Revision, Ablage und Nutzung von Dokumenten.
Regelungen mit ausschließlich IT-sicherheitsspezifischen Inhalten sind Bestandteil des GMS Systems „IT-Sicherheit".
Die vorliegende IT-Sicherheitsrichtlinie bildet dabei die Grundlage für alle IT-Sicherheitsanweisungen bei GUD.
Basierend auf dieser Anweisung sind die Verantwortlichkeiten, organisatorische Maßnahmen sowie grundlegende Verfahren und Prinzipien der IT-Sicherheit in der BA-1-112-001-00 „Sicherheit der Informationsverarbeitung" weiter definiert.
Konkrete Beschreibungen der Umsetzung bzw. Ausgestaltung finden sich in weiteren BA-Anweisungen sowie AA-Anweisungen des Systems 11.2 aber auch in den anderen GMS-Systemen, sofern allgemeine Unternehmensprozesse berührt sind (z.B. Risikomanagement, Einkauf, Änderungsmanagement, Bewertung/Verbesserungsprozess).

4.3 Geltungsbereich

Das ISMS gilt für alle Personen, die IT-Services der Gasunie nutzen und für alle IT-Systeme, die durch oder im Auftrag von GUD betrieben werden. Als IT-Systeme gelten sämtliche IT-Komponenten und IT-Applikationen sowie Telekommunikationssysteme.

5. Verantwortlichkeiten

Die Geschäftsführung ist für alle Informationen des Unternehmens verantwortlich und damit auch für deren Schutz und Sicherung. Zur Erreichung der Informationssicherheitsziele wurde eine IT-Sicherheitsorganisation eingerichtet und ein ICT-Security Manager benannt.
Dem ICT-Security Manager stehen für die Wahrnehmung seiner Aufgaben Focal Points in allen GUD-Funktionen, die IT-Systeme betreiben, zur Verfügung.
Im Rahmen der Organisationsstruktur sind IT-Sicherheitsvorfälle zu melden und dem ICT-Security Manager unmittelbar bekannt zu machen.
Der ICT-Security Manager wurde von der Geschäftsführung beauftragt, im Rahmen des ISMS unternehmensweite Regelungen für IT-Sicherheit zu entwickeln und fortzuschreiben. Die Regelungen zum Datenschutz bleiben davon unberührt.
Für die Umsetzung und Kontrolle der Einhaltung der Regelungen des ISMS sind alle Vorgesetzten innerhalb ihres Zuständigkeitsbereiches verantwortlich.
Alle Nutzer von GUD IT-Systemen sind verpflichtet, die Regelungen zur IT-Sicherheit zu befolgen und sorgfältig mit den ihnen anvertrauten Informationen, Authentifizierungsmitteln und Systemen umzugehen.
Die Geschäftsführung stellt die für die Einführung, Aufrechterhaltung und Verbesserung des ISMS erforderlichen personellen und technischen Ressourcen bereit.

6. Prinzipien der IT-Sicherheit

Dem ISMS der GUD liegen die in den nachfolgenden Kapitel aufgeführten Prinzipien zu Grunde.

6.1 Sensibilisierung

Alle Benutzer von GUD IT-Systemen müssen die Regelungen des ISMS kennen und beachten. Durch regelmäßige Schulungen und Überprüfungen muss sichergestellt werden, dass das Bewusstsein der Benutzer für Informationssicherheit ihren IT-Nutzungsrechten und dem daraus resultierenden Schadenspotential entspricht. Die Verantwortung hierfür liegt bei den einzelnen Funktionen.

6.2 Prinzip der „Minimalen Rechte"

Ein wichtiges Grundprinzip für die IT Sicherheit ist das "Prinzip der minimalen Rechte". Zugriffsrechte für schützenswerte Informationen und Systeme sind dementsprechend nur in dem Umfang zu gewähren, wie sie zur Aufgabenerfüllung notwendig sind („Need to know, need to do"). Sie dürfen nur durch dafür Befugte erteilt werden und sind in regelmäßigen Abständen zu überprüfen.

6.3 Nachvollziehbarkeit

Zugriffe auf schützenswerte Informationen und Systeme müssen nachvollzogen werden können. Die Zugriffskontrollsysteme müssen es daher ermöglichen, die Zugriffsrechte für Benutzer auf Ressourcen anhand von Regeln zu kontrollieren und zu verwalten. Die Identifikation und Authentifikation von Benutzern muss bei allen sicherheitsrelevanten Anwendungen einen eindeutigen Rückschluss auf die Person ermöglichen, die Funktionalitäten nutzt oder auf Daten zugreift. Zugriffe auf geheime Informationen sind, sofern technisch möglich, zu protokollieren.

6.4 Persönliche Verantwortung

Jeder Benutzer ist für die von ihm durchgeführten Handlungen verantwortlich.

6.5 Risikomanagement

Die Durchführung von Risikobewertungen gemäß GMS System 2.1 „Risikomanagement" stellt ein zentrales Element der IT-Sicherheit dar. Für die Feststellung und Überprüfung von IT-Systemrisiken gilt die Anweisung BA-2-021-401-00 „IT-System Risk Assessment". Die Implementierung und Durchsetzung von IT-Sicherheitsmaßnahmen müssen das mit der Nutzung von IT-Systemen verbundene Risiko auf ein für GUD akzeptables Restrisiko reduzieren. Die getroffenen Maßnahmen müssen sich innerhalb eines akzeptablen Kostenrah-

mens bewegen sowie die Verantwortung und das Verhalten des Benutzers angemessen berücksichtigen.

6.6 Eigentümerschaft

Jedes System und jede Information hat einen Eigentümer, der festgelegte Pflichten zum Schutz der Systeme und Informationen hat. Dazu gehört die Festlegung der Anforderungen an die Integrität und Verfügbarkeit des Systems sowie die Vertraulichkeit.

7. Wirksamkeit und Verbesserung des ISMS

Die Leistungsfähigkeit des ISMS wird monatlich anhand von Kennzahlen gemessen, die vom ICT-Security Manager an das Management der GUD berichtet werden. Dieses entscheidet bei Abweichungen von den gesetzten Zielwerten über eventuelle Maßnahmen. Schwere, die Leistungsfähigkeit des ISMS betreffende Vorfälle werden zusätzlich im wöchentlich tagenden Managementforum thematisiert und ggf. Adhoc-Maßnahmen eingeleitet.
Zudem werden die implementierten Maßnahmen und Regelungen zur Erhaltung und Steigerung der Informationssicherheit regelmäßig im Rahmen interner Audits auf ihre Aktualität und Wirksamkeit überprüft. Einmal jährlich wird eine Systembewertung, das so genannte Managementreview, vorgenommen.

Inhalte der Systembewertung sind:

- der Status von Maßnahmen vorheriger Managementbewertungen;
- Veränderungen bei externen und internen Themen, die das ISMS betreffen;
- Rückmeldung über die Informationssicherheitsleistung unter Einbeziehung der Entwicklungen bei Nichtkonformitäten und Korrekturmaßnahmen, Ergebnissen von Überwachungen, Messungen und Audits, die Wirksamkeit des ISMS bezüglich der Erfüllung der Normenforderungen und der IT-Sicherheitspolitik und -ziele / Ergebnisse von Audits;
- Rückmeldung von interessierten Parteien;
- Ergebnisse der Risikobeurteilung und des Risikobehandlungsplans;
- Möglichkeiten zur fortlaufenden Verbesserung und Weiterentwicklung des ISMS.

Die Geschäftsführung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Alle Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an die hierfür jeweils benannten Stellen (siehe BA-1-112-002-00 Benutzung der IT-Systeme") weiterzugeben. Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung soll das angestrebte Sicherheits- und Schutzniveau sichergestellt werden. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand zu halten.

8. Ergänzende Dokumente / Verweise

Keine

9. Anlagen

MM-2-112-001-01 „Relevante gesetzliche Regelungen und behördliche Vorgaben mit Bezug zur Informationssicherheit"
MM-2-112-001-02 „Interessierte Parteien - interne und externe Themen"

Relevante gesetzliche Regelungen und behördliche Vorgaben mit Bezug zur Informationssicherheit

MM-2-112-001-01

Nachfolgende Liste gibt eine Übersicht über die für GUD relevanten gesetzlichen Regelungen und behördliche Vorgaben mit Bezug zur Informationssicherheit.

- Gesetz betreffend die Gesellschaften mit beschränkter Haftung („GmbH-Gesetz") (§ 43 Abs. 1)
- Handelsgesetzbuch (§ 317 Abs. 4)
- Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)
- Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz und Informationssystemen in der Union
- Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV)
- Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz - EnWG) (insbesondere § 11 (1a-c), §59)
- IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz
- Verordnung (EU) 2015/703 der Kommission vom 30. April 2015 zur Festlegung eines Netzkodex mit Vorschriften für die Interoperabilität und den Datenaustausch
- Bundesdatenschutzgesetz (BDSG)
- Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
- Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU-DSAnpUG-EU)

Interessierte Parteien - interne und externe Themen	MM-1-112-001-02