Netzgesellschaft Gütersloh

Betriebsrichtlinie zum Informationssicherheitsmanagementsystem gemäß IT-Sicherheitskatalog §11 Absatz 1a EnWG

Managementleitlinie

Stand März 2018

Inhaltsverzeichnis

1. Präambel

Die Informationstechnik- (IT) und Telekommunikations- (TK)-Systeme, die zur Unterstützung der Netzbetriebsführung eingesetzt werden, nutzen zunehmend allgemeine IT-Standards, was für die Verknüpfung mit anderen Systemen zur Weiternutzung von hiermit erfassten Daten und für das die Systeme nutzende Personal hilfreich ist. Andererseits erhöhen sich dadurch die Risiken für den sicheren Betrieb dieser Systeme.

Für eine systematische Erfassung der möglichen Bedrohung für die relevanten Systeme, der Bewertung der daraus resultierenden Risiken und den daraus abgeleiteten Schutzmaßnahmen wird in der Unternehmensgruppe Stadtwerke Gütersloh, d.h. bei den Stadtwerken Gütersloh GmbH und der Netzgesellschaft Gütersloh mbH ein Informationssicherheitsmanagementsystem (ISMS) eingeführt. Dies dient der Strukturierung und Transparenz von Maßnahmen zur Erkennung von Bedrohungen und Risiken und unterstützt bei der systematischen Durchführung von Schutzmaßnahmen. Es handelt sich dabei um einen kontinuierlichen Prozess, in dem zyklisch oder bei Veränderungen der Systeme die getroffenen Festlegungen auf Veränderungsbedarf geprüft werden.
Die Schutzmaßnahmen bestehen zum einen aus technischen Maßnahmen, zum anderen aus organisatorischen Festlegungen, die nur dann ihre Wirkung entfalten können, wenn sie von allen Mitarbeitern beachtet werden, was durch entsprechende Mitarbeiterschulung gefördert werden muss.

Auch der Gesetzgeber hat die Bedeutung der Sicherheit von IT- und TK-Systemen erkannt und die Betreiber kritischer Infrastrukturen, zu denen die Netzgesellschaft Gütersloh mbH mit dem Sektor Energie (Strom und Gas) gehört, verpflichtet, einen angemessenen Schutz gegen Bedrohungen der für die Netzbetriebsführung erforderlichen IT- und TK-Systeme umzusetzen. Dieser liegt vor, wenn das eingeführte ISMS durch einen akkreditierten Prüfer zertifiziert wird. Auch der Bereich der Wasserversorgung gilt als kritische Infrastruktur. Da der Schwellenwert für eine verpflichtende Zertifizierung in der Unternehmensgruppe jedoch nicht erreicht wird, wird dieser Bereich nicht in die Zertifizierung einbezogen. Die Standards zur Erhöhung der IT-Sicherheit sollen aber auch hier gelten.

Die Geschäftsführungen der Stadtwerke und der Netzgesellschaft Gütersloh sind verantwortlich für

- die Schaffung organisatorischer Rahmenbedingungen zur wirksamen Gewährleistung von Informationssicherheit
- die Definition und Festlegung der erforderlichen Verantwortlichkeiten und Befugnisse
- die Einrichtung eines Informationssicherheits-Managements,
- die Umsetzung der vereinbarten Sicherheitsmaßnahmen einschließlich der Bereitstellung der erforderlichen Mittel,
- Eine hinreichende und geeignete Dokumentation der IT-Infrastruktur sowie aller Sicherheitsvorkehrungen und Sicherheitsmaßnahmen.

Die vorliegende Leitlinie beschreibt die allgemeinen Ziele, Strategien und Organisationsstrukturen, welche für die Initiierung und Etablierung eines ganzheitlichen Informationssicherheitsprozesses erforderlich sind.

1.1 Geltungsbereich

Das Informationssicherheitsmanagementsystem (ISMS) umfasst die Betriebsführung für das Strom- und Gasnetz gemäß den Vorgaben des EnWG. Zusätzlich und freiwillig werden in der Unternehmensgruppe Stadtwerke Gütersloh auch die Betriebsführung des Wassernetzes und der Wassergewinnung in das ISMS einbezogen.
Allein das ISMS für die Betriebsführung der Strom- und Gasnetze wird gemäß den gesetzlichen Anforderungen nach dem IT-Sicherheitskatalog der Bundesnetzagentur zertifiziert.
Die entsprechenden Systeme werden anhand der Geschäftsprozesse der Netzbetriebsführung identifiziert und in einem Netzstrukturplan erfasst. Dieser wird im Dokumentationssystem des ISMS HiScout hinterlegt.
Die vom Geltungsbereich des ISMS betroffenen Organisationseinheiten der Unternehmensgruppen sind in einem Organigramm im Anhang markiert.

1.2 Informationssicherheitsziele

Die IT- und TK-Systeme zur Netzbetriebsführung haben die Aufgabe, die Mitarbeiter bei der Netzbetriebsführung zu unterstützen. Die Informationssicherheit dieser Systeme ist so zu gewährleisten, dass diese Unterstützung jederzeit gegeben und in keinem Fall die sichere Netzbetriebsführung durch diese Systeme gefährdet ist.
Dafür haben die Verfügbarkeit der Systeme und die Integrität der verarbeiteten Daten höchste Priorität. Dies erfordert zum einen, dass vorbeugende Maßnahmen zum Schutz gegen die relevanten Gefährdungen umgesetzt werden, zum anderen, dass geeignete Vorkehrungen und Pläne entwickelt werden, um auch bei Gefahreneintritt handlungsfähig zu sein und mögliche Schäden begrenzen zu können.

1.2.1 Verfügbarkeit

Der Zugang zu Informationen für IT-Systeme im Geltungsbereich des ISMS ist für alle Mitarbeiter im Geltungsbereich des ISMS sicherzustellen, wenn diese benötigt werden. Die Mitarbeiter im Geltungsbereich werden in HiScout gepflegt.

Die für die Netzbetriebsführung notwendigen Informationen sollen rund um die Uhr an allen Tagen (24h/7d) zur Verfügung stehen. Die Systeme, die diese Informationen bereitstellen, sind entsprechend auszulegen, dass diese Verfügbarkeit gegeben ist, z.B. durch Redundanz der Komponenten.

1.2.2 Integrität

Die Informationen müssen unverändert und vollständig sein. Dies ist von den Systemen, die diese Informationen übertragen und verarbeiten, sicherzustellen.
Hierzu sind bevorzugt Übertragungs- und Verarbeitungsverfahren zu verwenden, die entsprechende Prüfalgorithmen beinhalten (z.B. die Fernwirkprotokolle IEC 60870-5, verschlüsselte Übertragung via VPN).

1.2.3 Vertraulichkeit

Es ist durch geeignete Maßnahmen sicherzustellen, dass nur die autorisierten Benutzer Zugang zu den Informationen haben. Zu diesem Zweck ist für alle Daten der Personenkreis, dem der Zugriff gestattet werden soll, zu bestimmen. Der Zugriff auf IT-Systeme, IT-Anwendungen und Daten sowie Informationen ist auf den unbedingt erforderlichen Personenkreis zu beschränken. Jeder Mitarbeiter im Geltungsbereich des ISMS erhält eine Zugriffsberechtigung nur auf die Daten, die er zur Erfüllung seiner dienstlichen Aufgaben benötigt.

1.3 Aufwand

Die Geschäftsführungen unterstützen die Zielsetzung für das Informationssicherheitsmanagement und stellen daher angemessene Ressourcen für die erforderlichen Prozesse zur Verfügung.

1.4 Organisatorische Festlegungen

Die Pflege und Weiterentwicklung des Informationssicherheitsmanagementsystems wird vom ISMS-Verantwortlichen betrieben. Er koordiniert die notwendigen Arbeiten, erarbeitet Verfahrensanweisungen und Arbeitsanweisungen und bereitet Entscheidungen für die Geschäftsführung vor. Bei Bedarf werden für Teilaufgaben weitere Mitarbeiter hinzugezogen.

Zur Unterstützung der Mitarbeiter ist das Softwaresystem HiScout zur Dokumentation und Automatisierung und Standardisierung von Abläufen eingeführt.
Zur Erhaltung der notwendigen Informationssicherheit müssen alle Mitarbeiter die festgelegten Abläufe einhalten und wachsam und mit der gebotenen Umsicht die IT- und TK-Systeme zu nutzen. Bei Nichtbeachtung greifen die im betriebsübergreifenden Betriebshandbuch festgelegten Disziplinarmaßnahmen .Auffälligkeiten und unerwartetes Systemverhalten sind umgehend den zuständigen Systembetreuern zu melden.

1.5 Aufrechterhaltung und Weiterentwicklung

Die Angemessenheit und Funktionalität des festgestellten Schutzbedarfes und der getroffenen Schutzmaßnahmen wird regelmäßig durch den ISMS-Verantwortlichen geprüft. Dabei festgestellte Verbesserungsmöglichkeiten werden durch ihn mit angemessenen Fristen umgesetzt.
Gemäß den Vorgaben der Bundesnetzagentur ist das Informationssicherheitsmanagementsystem durch einen akkreditierten Prüfer nach dem IT-Sicherheitskatalog zu zertifizieren. Eine Rezertifizierung ist nach drei Jahren erforderlich.
Zusätzlich zu den jährlichen Überwachungsaudits des akkreditierten Prüfers sollen intern jährlich Audits durchgeführt werden.

2. Überprüfung

Diese Managementleitlinie und die gemäß Anlage mitgeltenden Dokumente werden in planmäßigen Abständen überprüft. Damit wird festgestellt, ob deren Inhalt noch mit den Anforderungen der Unternehmensgruppe Stadtwerke Gütersloh in Bezug auf die Informationssicherheit übereinstimmt.

Die Überprüfung der Managementleitlinie und der dazugehörigen Handlungsleitlinie erfolgt durch die Geschäftsführungen der Unternehmensgruppe. Die weiteren nachgeordneten Leitlinien werden durch den ISMS-Verantwortlichen überprüft.
Es sollten folgende Maßnahmen durchgeführt werden:

- Überprüfen, ob die innerhalb der Unternehmensgruppe Stadtwerke Gütersloh vorgenommenen Veränderungen - seien sie technischer oder organisatorischer Natur - eine Anpassung der Sicherheitsstrategien erfordern: Ergreifung vorbeugender Maßnahmen;
- Organisation der Durchführung von Änderungen, die als erforderlich betrachtet werden;
- Mitteilung der Ergebnisse der Überprüfung an die Mitarbeiter.

Dies erfolgt

- zyklisch mindestens einmal jährlich in Vorbereitung der internen Audits
- nach erheblichen Änderungen im durch das ISMS abgedeckten Bereiches für die Managementleitlinie
- nach erheblichen Änderungen des jeweils durch die Leitlinie beschriebenen Bereiches