Bild: Adobe Stock_leowolfert

ISMS als wichtiger Teil moderner Energieversorger

„Aus meiner Sicht ergibt ein ISMS nur Sinn, wenn es ganzheitlich für die Organisation Gültigkeit hat“

Der TV-Sender Arte zeigte jüngst ein düsteres Szenario: „Terror: Atomkraftwerke im Visier“. Neben Angriffen mit Flugzeugen und Drohnen wurden auch mögliche Cyber-angriffe thematisiert. Und damit wären wir mitten im Thema. Denn es vergeht kaum ein Tag, an dem nicht über die Sicherheit von Energieversorgern in unseren digitalen Zeiten gesprochen und diskutiert wird. Eine Frage könnte lauten: Alles smart, vernetzt und unsicher? Eine nüchterne Antwort: Die öffentliche Diskussion schwankt zwischen Fortschritt und Hysterie – vor dem Hintergrund steigender Cybergefahren und gesetzlicher Anforderungen an das Energieversorgerumfeld. Die Redaktion der gis.Business sprach mit Werner Dippold, Datenschutz- und IT-Sicherheitsbeauftragter bei der Infra Fürth Unternehmensgruppe, einem regionalen Energieversorger, über Regulierung, die Informationssicherheit und deren Management sowie neue Technologien im Verbund mit Geoinformationen.

Autor: **Andreas Eicher**

Der Gesetzgeber erhöhte mit dem IT-Sicherheitskatalog vom August 2015 merklich die Regelungen für Unternehmen im Bereich der sogenannten kritischen Infrastrukturen. Haben wir es hier nur mit einem neuen Papiertiger zu tun oder sind die Regelungen für den Betrieb im Energiesektor ausreichend und vor allem zielführend?

Da sich mit dem Erlass des BSI-Gesetzes weitere Gesetze verändert haben, hängt es immer von den entsprechenden Kombinationen dieser Gesetze und den entsprechenden Vorgaben ab, ob und wie weit hier ein Papiertiger entsteht.

Was heißt das konkret auf Ihr Unternehmen heruntergebrochen?

Die Infra Fürth Unternehmensgruppe ist in Summe mit vier Sektoren (Energie, Wasser, Informationstechnik/Telekommunikation und Transport/Verkehr) der kritischen Infrastruktur betroffen. Für den Sektor „Energie", sprich Strom, Erdgas und Fernwärme, wurde über das EnWG § 11 Abs. 1a die Schaffung eines IT-Sicherheitskatalogs durch die Bundesnetzagentur beschlossen. Über diesen IT-Sicherheitskatalog werden die entsprechenden Schutzziele, Sicherheitsanforderungen und Zertifizierungsvorgaben vorgegeben. Durch die Festlegung auf ein Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001 und den in dieser Norm festgelegten Regelungen, mit einem jährlichen Überwachungsaudit und alle drei Jahre einem Wiederholungsaudit, sehe ich hier auf keinen Fall einen Papiertiger.

Was sind aus Ihrer Sicht die wichtigsten Überlegungen bei der Einführung eines Informationssicherheitsmanagements (ISMS) in einem Energieunternehmen?

Durch die Einführung eines ISMS müssen Unternehmen ihre (IT-)Risiken gezielt identifizieren, entsprechend bewerten, überwachen und letztendlich steuern. Dies ist aus meiner Sicht in der heutigen Zeit unverzichtbar für Unternehmen, wenn sie Entscheidungen für die Sicherung und Weiterentwicklung ihrer Kerngeschäfte treffen müssen.

Und welchen Mehrwert sehen Sie in einem ISMS?

Den Mehrwert eines ISMS erkannte unser Unternehmen bereits vor zwölf Jahren mit dessen Einführung. War es damals noch das „Alleinstellungsmerkmal", welches uns beim Anbieten von IT-Dienstleistungen für Dritte Vorteile brachte, so ist es heute das Wissen um den Stand unserer eingesetzten Technik. Dadurch sind wir in der Lage, unsere IT-Sicherheitsmaßnahmen entsprechend strukturiert, aber auch ressourcenschonend zu planen und einzuführen. Somit senken wir in diesem Bereich Kosten.

Aus meiner Sicht kann man hier festhalten: Ja, IT-Sicherheit kostet Geld. Aber keine oder eine schlecht geplante und umgesetzte IT-Sicherheit kostet noch viel mehr.

Was sind die besonderen Fallstricke, auf die sich Unternehmen aus dem Energiesektor einstellen müssen, sofern sie ein ISMS in der eigenen Organisation einführen möchten?

Üblicherweise gibt es in Unternehmen unserer Branche zwei Bereiche, die sich mit der IT beschäftigen: Zum einen der Bereich, der sich mit der „normalen" IT (Bürokommunikation) beschäftigt. Und zum anderen der Bereich der kritischen Infrastruktur (beispielsweise Netzleit- und Fernwirktechnik). Durch die Standardisierung bei den Systemen der kritischen Infrastruktur, den Einsatz von Windows- beziehungsweise Linux-Systemen für Netzleitstellen, aber auch den immer größeren Bedarf an Fernsteuerbarkeit der Systeme, erhöht sich auch der IT-Sicherheitsbedarf. Deshalb müssen die Unternehmen und Mitarbeiter aus beiden IT-Bereichen lernen, dass sie näher zusammenrücken. Aus meiner Sicht ergibt ein ISMS nur Sinn, wenn es ganzheitlich für die Organisation Gültigkeit hat. Ob hierbei auch beide IT-Bereiche zertifiziert

Werner Dippold

ist seit 1996 Mitarbeiter in der Infra Fürth Unternehmensgruppe. Seit 2009 ist er bestellter IT-Sicherheits- und Datenschutzbeauftragter und seit 2014 zusätzlich als Compliance-Beauftragter tätig.

Bild: Werner Dippold

werden müssen, hängt allerdings von den jeweiligen Voraussetzungen des Unternehmens ab.

Ihr Unternehmen wurde vor einiger Zeit ISMS-zertifiziert. Können Sie uns einen kurzen Abriss geben, was die wichtigsten Meilensteine in diesem Gesamtprojekt waren und welche zeitliche Dimension dahinter lag?

Unser Unternehmen ist im Bereich der Bürokommunikation bereits seit zwölf Jahren nach ISO/IEC 27001 (nativ) zertifiziert. Somit sah unser Projekt zur Zertifizierung der kritischen Infrastruktur etwas anders aus als bei dem Großteil anderer Energieversorger. Mit dieser langjährigen Erfahrung im Rücken beschlossen wir zunächst, die ISMS-Zertifizierung ohne externe Unterstützung umzusetzen.

Dann wurde zum einen das bereits bestehende ISMS mit seinen Regelungen auf die neue Situation angepasst und zum anderen mit der Zertifizierungsstelle die zukünftige Zertifizierungsstruktur abgeklärt. Dies war notwendig, da ein bereits bestehender Geltungsbereich mit einer Zertifizierung nach ISO/IEC 27001 (nativ) und ein neuer Geltungsbereich mit einer angestrebten Zertifizierung nach ISO/IEC 27001 und IT-SiKat verbunden werden mussten. Diese Vorgehensweise hatte übrigens auch positive finanzielle Aspekte. Weiter mussten die Geltungsbereiche definiert und die benötigten internen und externen Schnittstellen identifiziert werden. Mit dem Bestehen der beiden Zertifizierungsstufen im September und Oktober 2017 wurde der Prozess „Umstellung der bestehenden Zertifizierung und Neuzertifizierung“ erfolgreich abgeschlossen. Allerdings darf man hierbei nicht vergessen: Nach der Zertifizierung ist vor der Zertifizierung. Direkt im Anschluss wurde mit den Vorbereitungen zum Überwachungsaudit 2018 begonnen.

Neue Technologien mit allen möglichen „smarten“ Lösungen sollen dem Anwender das Leben mit der Energie erleichtern. Sind diese digitalen Lösungen wirklich so sicher, wie es die Werbung vermittelt, oder müssen die Nutzer nicht vielmehr die Risiken in den Fokus nehmen?

Durch die gesetzlichen Vorgaben des Messstellenbetriebsgesetzes und den zugehörigen technischen Richtlinien ist ein sehr guter Standard für die IT-Sicherheit gegeben. Trotzdem muss einem klar sein, eine hundertprozentige Sicherheit kann und wird es nicht geben. Letztendlich hängt es immer vom Interesse an den Daten und dem Aufwand ab, der betrieben werden muss, um an diese Daten zu gelangen.

Geoinformationen spielen in diesem Kontext eine immer größere Rolle, um Fernanwendungen zu erleichtern sowie die Überwachung und Kontrolle zu verbessern. Ist das nicht auch ein datenschutzrechtliches Thema, das vom Gesetzgeber viel stärker reguliert werden müsste?

Ja, definitiv ist das ein datenschutzrechtliches Thema, was durchaus auch so vom Gesetzgeber gesehen wird. Mit der Einführung der europäischen Datenschutzgrundverordnung (EU-DSGVO) wird meiner Meinung nach diesem auch Rechnung getragen.

Durch die EU-DSGVO werden Unternehmen gezwungen, ein entsprechendes Datenschutzmanagementsystem aufzubauen. Wenn man dies dann näher betrachtet, passen die beiden Thema ISMS und Datenschutz sehr gut zusammen. Bei uns wird dies schon immer so gesehen. Aus diesem Grund bin ich auch nicht nur Datenschutz- sondern auch IT-Sicherheitsbeauftragter. Im Übrigen ist bei uns immer ein Betriebsratsmitglied auch Mitglied im IT-Sicherheitsteam. Das bringt den großen Vorteil, dass bei allen Themen das Mitbestimmungsrecht des Betriebsrats gewahrt wird.

Blicken wir abschließend nach vorne. Welche Maßnahmen stehen in Ihrer Organisation zur weiteren Verbesserung der Informationssicherheit in naher Zukunft an, auch mit Blick auf die digitale Welt von morgen?

Ich denke, hier werden uns die Themen in nächster Zeit nicht ausgehen: Als erstes ist natürlich die Einführung und Umsetzung der EU-DSGVO zu nennen. Wir müssen unser bestehendes Datenschutzmanagementsystem entsprechend überprüfen und anpassen. Da wir, wie ich anfangs aufgezählt habe, von insgesamt vier Sektoren der kritischen Infrastruktur betroffen sind, müssen auch hier noch die entsprechenden Herausforderungen gemeistert werden. Nicht zu vergessen die Einführung der intelligenten Zähler mit ihren entsprechenden gesetzlichen Vorgaben.

Herr Dippold,
vielen Dank für das Gespräch!

Das Interview führte Andreas Eicher