ISMS
Einführung nicht verschlafen

[15.8.2016] Die Einführung eines Informations-Sicherheits-Management-Systems (ISMS) sollte kein Hexenwerk sein. Dennoch tun sich viele Stadtwerke schwer. Das liegt an aktuellen Fehleinschätzungen ebenso wie an alten Versäumnissen, zeigt eine Umfrage der Unternehmensberatung Axxcon.

Bei der Einführung eines zertifizierten Informations-Sicherheits-Management-Systems (ISMS) bis zum 31. Januar 2018 tun sich Stadtwerke und andere Energieversorger schwer. Das zeigt die Studie "Informationssicherheit: Sind die Energieversorger schon ISMS-ready?" der Unternehmensberatung Axxcon, für die 106 Geschäftsführer, IT-Leiter und IT-Sicherheitsbeauftragte befragt wurden. Demzufolge werden viele der Unternehmen den gesetzlich vorgeschriebenen Termin nicht einhalten können.
Das liegt unter anderem an einer zu knappen Planung der ISMS-Einführung: So wollen 43 Prozent der Unternehmen den Prozess bis zum zweiten Quartal 2017 abschließen. Bis zum vierten Quartal 2017 wollen 89 Prozent fertig sein, im ersten Quartal 2018 schließlich alle. Dabei wurde offenbar nicht bedacht, dass ein ISMS mindestens sechs Monate im Einsatz sein muss, bevor seine Funktionsfähigkeit und Effektivität nachgewiesen sind und das System zertifiziert werden kann. Das wird einem Großteil der Unternehmen alleine aus Zeitgründen nicht gelingen. Hinzu kommt: Bauen alle Unternehmen auf eine Abnahme kurz vor Ablauf der Frist, wird es zu einem Engpass bei den Zertifizierern kommen. Bei einem Verzug drohen den Stadtwerken jedoch empfindliche Geldstrafen.
Ohnehin dürfte die Einführung des ISMS für die Energieversorger deutlich teurer werden als geplant: So haben knapp zwei Drittel der Unternehmen laut der Studie nicht mehr als 100.000 Euro veranschlagt. Diese Summe wird jedoch nicht ausreichen: Realistisch betrachtet, kostet die Einführung im Durchschnitt 500.000 Euro. Und auch bei einem kleineren Stadtwerk wird die benötigte Summe deutlich über 100.000 Euro liegen.

Aufwand wird unterschätzt

Dass den Stadtwerken bei der ISMS-Einführung solch gravierende Fehleinschätzungen unterlaufen, kann sich schmerzlich bemerkbar machen. Darüber hinaus zeigt es Versäumnisse bei ihrer technischen IT auf – welche gern von der kommerziellen oder kaufmännischen IT, wie zum Beispiel SAP-Anwendungen,

abgegrenzt wird. Schließlich sind die vom Gesetzgeber aufgestellten Anforderungen an das Informations-Sicherheits-Management-System keineswegs neu. So sind die entsprechenden Prüfmodelle und Prozesse für die Informationssicherheit in anderen IT-Bereichen längst Standard. Auch die ISO 27001, nach der die Zertifizierung des ISMS erfolgen soll, ist bereits etabliert, ebenso wie die vollständige Inventarisierung der IT, welche die Grundlage für ein ISMS darstellt.
Anders sieht es offenbar im Bereich der technischen Infrastruktur aus, die in den Stadtwerken oftmals historisch gewachsen ist. So haben laut der Studie bislang erst 43 Prozent der befragten Energieversorgungsunternehmen alle sicherheitsrelevanten Netze und Geräte vollständig erfasst. Lediglich zwölf Prozent der Unternehmen haben die potenziellen Bedrohungen und Risiken abschließend identifiziert. Hier macht sich die ungünstige Ausgangslage bemerkbar. Denn: Muss ein Unternehmen bei der Inventarisierung bei Null anfangen, dauert allein die Aufstellung eines Netzstrukturplans je nach Größe eines Stadtwerks mehrere Wochen bis hin zu einigen Monaten.
Nicht zuletzt weist das Fehlen vollständiger Netzstrukturpläne auf eine falsch gewählte Reihenfolge bei der ISMS-Einführung hin. Schließlich ist zu empfehlen, zuerst einen Netzstrukturplan zu erstellen, aus dem auch Schnittstellen und Verantwortlichkeiten hervorgehen und der als Grundlage für alle weiteren Schritte dient. Anschließend wird definiert, welche Bereiche relevant für den wirtschaftlichen Erfolg und die Handlungsfähigkeit des Unternehmens sind. Im nächsten Schritt müssen die relevanten (Informations-)Werte definiert und die Risiken analysiert werden. Erst jetzt können die Maßnahmen festgelegt und umgesetzt werden. Schließlich folgt die Review-Phase mit Korrekturmaßnahmen, der Einführung eines kontinuierlichen Verbesserungsprozesses und der Durchführung von internen Audits zur Erreichung der Zertifizierungsreife.

Mangel an Know-how

Wie auch die Beratungspraxis zeigt, ist eine solch systematische Vorgehensweise in den Unternehmen häufig nicht gegeben. Oft liegt dies an einem Mangel an Know-how, der laut der Studie in kleinen Unternehmen mit bis zu 200 Mitarbeitern am stärksten ausgeprägt ist. 71 Prozent von ihnen sind nach eigenen Angaben nur teilweise, sechs Prozent noch gar nicht mit den Mindestanforderungen für ein zertifiziertes ISMS vertraut. Ebenfalls brisant: Bei mehr als jedem zweiten Unternehmen fehlt es an Mitarbeitern für die Umsetzung, Implementierung und den

Betrieb des ISMS.
Häufig verfügen gerade mittelgroße und kleine Stadtwerke aufgrund ihrer Personalstruktur nicht über die richtigen Mitarbeiter, um ein ISMS zügig umzusetzen. Darüber hinaus fehlt oft auch die Bereitschaft, sich mit dem Thema Sicherheit auseinanderzusetzen – nicht zuletzt, weil den Mitarbeitern dessen Ernsthaftigkeit nicht bewusst ist. Ein Grund dafür könnte sein, dass Hacker-Angriffe bislang noch keinen großen Einfluss auf das Tagesgeschäft der EVUs hatten. Es ist jedoch davon auszugehen, dass gezielte Angriffe auf die Infrastruktur zunehmen werden. Und auch der Stromausfall in einem kleineren Stadtwerk kann Industriekunden schädigen und erhebliches Gefahrenpotenzial bergen. Wichtig sind daher nicht nur Informationsveranstaltungen und Schulungen für die IT-Experten, die direkt an der Einführung des ISMS beteiligt sind. Auch alle anderen Mitarbeiter des Unternehmens müssen für Sicherheitsfragen sensibilisiert werden.
Insgesamt ist die Informationssicherheit im Unternehmen eine Sache der Unternehmenskultur und muss dringend zur Chefsache erklärt werden. Dies gilt umso mehr, da die IT-Sicherheit ein wichtiges Zukunftsthema ist. Denn die Einführung von Smart Meter und Smart Grid wird die Anforderungen an die Sicherheitssysteme in Zukunft drastisch erhöhen.

Dirk Stieler und Torsten Beyer sind Partner und ISMS-Experten bei der Unternehmensberatung Axxcon.

http://www.axxcon.com
Hier kann die Studie zur Informationssicherheit bei Energieversorgern bestellt werden. (Deep Link)
Dieser Beitrag ist im stadt+werk-Sonderheft "IKT-Lösungen für Stadtwerke und kommunale Betriebe" erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren. (Deep Link)

Stichwörter: Informationstechnik, IT-Sicherheit, Informations-Sicherheits-Management-System

---

Quelle: www.stadt-und-werk.de