ISMS

Fünf Grundsätze zur Einführung

[07.04.2016] Energieversorger müssen laut Gesetz ein Informations-Sicherheits-Management-System (ISMS) einführen. Ein strukturiertes Vorgehen, das sich an fünf Grundsätzen orientiert, verhilft zum Erfolg.

Seit das IT-Sicherheitsgesetz im Juli 2015 in Kraft getreten ist, müssen Betreiber kritischer Infrastrukturen Standards nach aktuellem Stand der Technik erfüllen. Die Bundesnetzagentur (BNetzA) hat diese Anforderungen für Energieversorgungsunternehmen in IT-Sicherheitskatalogen detailliert festgehalten. Der Entwurf des Sicherheitskatalogs für Energienetzbetreiber ist bereits veröffentlicht. Demnach müssen die Betreiber künftig ein Informationssicherheits-Management-System (ISMS), nach ISO 27001 einführen. Dabei sind branchenspezifische Ergänzungen durch die ISO 27019 zu berücksichtigen. Die Zertifizierung muss bis 31. Januar 2018 erfolgen. Vergleichbare Vorgaben werden auch für den IT-Sicherheitskatalog für Energieanlagenbetreiber erwartet. Konkret beschrieben sind die neuen Sicherheitsvorgaben im IT-Sicherheitskatalog, Paragraf 11 Absatz 1a EnWG.

Handlungsdruck ist gegeben

Laut Vorgabe müssen die betroffenen Unternehmen belegen, dass sie die Regeln einhalten. Die etwa 1.000 Energienetzbetreiber in Deutschland können das durch eine Zertifizierung auf der Basis von DIN ISO/IEC 27001 nachweisen, die aktuell von der Bundesnetzagentur gemeinsam mit der Deutschen Akkreditierungsstelle (DAkkS) entwickelt wird. In der Regel dauert es mindestens 15 Monate vom Projektstart bis zur Zertifizierung des ISMS. Wie viel Zeit genau eingeplant werden muss, hängt vom individuellen Status der Informationssicherheit in den jeweiligen Unternehmen ab – und von einer Besonderheit der Energieversorger: Sie müssen die infrastrukturelle Sicherheit dezentraler Komponenten mit der IT-Sicherheit ihrer Netze kombinieren. Um für eine mögliche Zertifizierungsprüfung ausreichende Nachweise der Effektivität und Wirksamkeit erbringen zu können, müssen die Unternehmen das konzeptionierte ISMS erfahrungsgemäß mindestens sechs Monate betrieben haben.
Auch sollten ausreichend Finanzmittel für die Einführung eines ISMS bereitgestellt werden. Der Projektaufwand liegt inklusive Risikoanalysen, Begleitung der Umsetzung organisatorischer und technischer Maßnahmen sowie zusätzlicher Management-Kapazitäten schnell im mittleren sechsstelligen Bereich. Darin sind noch nicht die Kosten der technischen Maßnahmen an sich sowie laufende Kosten berücksichtigt. So findet sich in den Erläuterungen des IT-Sicherheitsgesetzes beispielsweise die Schätzung, dass jede Meldung eines Störfalls mit 660 Euro zu Buche schlägt.

Grundsätze der Einführung

Vor der ISMS-Einführung empfiehlt sich eine sorgsame Analyse des Status quo der Informationssicherheit. Bewährt hat sich auch, ein Projekt zur Einführung aufzusetzen. Denn um die vielen Anforderungen bewältigen zu können, ist ein strukturiertes Vorgehen wichtig. Dieses sollte sich an fünf Grundsätzen orientieren.
Zunächst sind die Erwartungen klar zu definieren. Bei der Definition der Ziele und Erwartungen sollten explizit auch die aller Stakeholder einbezogen werden. Dazu zählen nicht zuletzt externe Dienstleister und die Frage, ab welchem Prozessschritt sie einbezogen werden sollten. Projektdauer und -kosten können auf die individuellen Möglichkeiten des Energieversorgungsunternehmens angepasst werden.

Der zweite Grundsatz ist, den Geltungsbereich sinnvoll zu beschränken. Die Bundesnetzagentur macht in ihrer finalen Version des IT-Sicherheitskatalogs für Energienetzbetreiber technische Vorgaben für den Mindestumfang des ISMS-Geltungsbereichs. Die meisten Energieunternehmen bestehen aus verschiedenen Gesellschaften, die unterschiedlichen Regularien unterliegen. Eine wesentliche Frage ist deshalb, welcher Teil der Konzernstruktur durch ein ISMS abgedeckt werden soll. Um den Aufwand für Konzeption, Betrieb und Zertifizierung des ISMS minimal zu halten, sollten nur die notwendigen Bereiche einbezogen werden. Dabei sind zwei Aspekte zu beachten: Zum einen kann die Verflechtung der einzelnen Gesellschaften dazu führen, dass ein größerer Teil des Unternehmens in den Geltungsbereich des ISMS aufzunehmen ist. Zum anderen kann es unabhängig von den aktuellen Verpflichtungen vorausschauend sein, einen größeren Geltungsbereich zu wählen, um spätere Aufwände zu verringern. Auch strategische Erwägungen, wie der Zukauf und Verkauf von Unternehmensteilen bei gleichzeitigem Erhalt der Zertifizierung, können sich auf den Geltungsbereich auswirken.

Ähnliche Prozesse schaffen Synergien

Der dritte Grundsatz besagt, dass die Energienetzbetreiber ähnliche Strukturen bündeln. Das gilt auch, wenn zentrale Dokumente erstellt und Prozesse aufgesetzt werden. Dadurch werden Risikoeinschätzung und Maßnahmenentwicklung erheblich vereinfacht. Eine sinnvolle Zusammenführung schafft Übersichtlichkeit und Verständlichkeit. Das gilt insbesondere, wenn in die Konsolidierung auch Dokumente und Prozesse aus anderen Normvorgaben wie dem Qualitätsmanagement (ISO 9000) oder Umweltschutz einbezogen werden. Sind entsprechende Normen bereits etabliert, können Synergien geschaffen werden. Laut dem vierten Grundsatz sollten vorhandene Sicherheitselemente, etwa eine Zutrittskontrolle oder Virenscanner, bei der Einführung des ISMS aufgegriffen, ergänzt und in ein umfassendes Konzept integriert werden. Das senkt Kosten und erhöht die Akzeptanz des Projekts im Unternehmen. Denn immerhin bedeutet die Einführung eines ISMS dort oft einen grundlegenden Wandel. Neue Prozesse müssen gelebt und neue Regeln eingehalten werden.
Sofort zu starten, ist der fünfte Grundsatz. Falls es im Unternehmen noch Klärungsbedarf über notwendige Schritte zur ISMS-Einführung gibt, kann zunächst eine Analyse des Status quo in Form einer Reifegradanalyse vorgeschaltet werden. Ansonsten gilt: sofort loslegen, um den Zeitrahmen nicht zu überschreiten.
Neben diesen fünf Grundsätzen kann es sich außerdem lohnen, bei der ISMS-Einführung die Expertise eines erfahrenen Partners einzubeziehen. Denn Einsteiger werden allein durch die umfangreichen Dokumentationspflichten vor viele Fragen gestellt.

()

Dieser Beitrag ist in der März/April-Ausgabe von stadt+werk erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: Informationstechnik, ISMS