HISOLUTIONS

Notfall- und Krisenmanagement

im Energiesektor

Bild: Ausfall der Energieversorgung in Folge des „Münsterländer Schneechaos“ im November 2005

DER ENERGIESEKTOR – EINE KRITISCHE INFRASTRUKTUR

Ein Ausfall oder bereits die Beeinträchtigung der Energieversorgung führt zu

- nachhaltig wirkenden Versorgungsengpässen für die Bevölkerung,
- erheblichen Störungen der öffentlichen Sicherheit,
- sowie nicht tolerablen, wirtschaftlichen Auswirkungen für Industrie, Handel und Wirtschaft.

Auf Grundlage dieser und weiterer möglicher Auswirkungen, entschlossen sich das Bundesministerium des Innern (BMI) und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) zur Initiierung einer „Nationalen Strategie zum Schutz kritischer Infrastrukturen" (KRITIS). Ziel ist die Schaffung eines konzeptionellen Rahmens zum Schutz der für die Versorgung von Staat, Wirtschaft und Gesellschaft zuständigen, zentralen Versorgungs- und Dienstleistungseinrichtungen.

DAS IT-SICHERHEITSGESETZ – DIE RECHTLICHE GRUNDLAGE

Die Funktionsfähigkeit der Energieversorgung sowie eines sicheren Netzbetriebs sind wesentlich vom Vorhandensein einer intakten Informations- und Kommunikationstechnologie (IKT) abhängig.

Branchenspezifische Mindeststandards

Unter Berücksichtigung der zunehmenden Bedrohungslage tritt hierbei vor allem der Schutz kritischer Infrastrukturen vor Cyber-Attacken in den Vordergrund. Im Juli 2015 trat in diesem Zusammenhang das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) in Kraft. Kritische Infrastrukturen müssen seither branchenspezifische Mindeststandards erfüllen. Hierzu zählt insbesondere die Einführung eines Informationssicherheitsmanagementsystems (ISMS) nach dem internationalen Standard ISO 27001. Die Verabschiedung des IT-Sicherheitsgesetzes veranlasste darüber hinaus die Änderung weiterer Gesetze wie beispielsweise des Energiewirtschaftsgesetzes. Sämtliche Strom- und Gasnetzbetreiber werden seither verpflichtet, den IT-Sicherheitskatalog der Bundesnetzagentur umzusetzen[1].

Folgen für die Netzbetreiber

Gemäß dem IT-Sicherheitskatalog haben Netzbetreiber den ordnungsgemäßen Betrieb der relevanten informationstechnischen Systeme nachhaltig sicherzustellen. Das bedeutet in erster Linie, dass die eingesetzten Systeme und IKT-gestützten Verfahren und Prozesse zu jedem Zeitpunkt beherrscht werden. Technische Störungen sollen als solche erkannt und behoben bzw. deren Behebung anderweitig sichergestellt werden. Hierzu wird empfohlen, sich dem Umsetzungsplan KRITIS (UP KRITIS)[2] anzuschließen. Dieser umfasst u. a. weiterführende Maßnahmen zum Auf- und Ausbau von Krisenmanagementstrukturen, zur koordinierten Krisenreaktion und -bewältigung sowie zur Durchführung von Notfall- und Krisenübungen.

Neben dem Erfordernis der Einführung eines Informationssicherheitsmanagementsystems obliegen den Energieversorgern damit auch die Notwendigkeit und der Bedarf zur Etablierung eines Notfall- und Krisenmanagementsystems[3].

[1] gemäß § 11 Absatz 1a Energiewirtschaftsgesetz

[2] s. www.upkritis.de

[3] s. ISO 27019 Kapitel 14 Business Continuity Management

DAS NOTFALL- UND KRISENMANAGEMENT

Notfall- und Krisenmanagement umfasst einen kontinuierlichen Prozess aus Planung, Durchführung, Prüfung sowie Verbesserung risikoreduzierender Maßnahmen sowie Verfahren zur Sicherstellung des Geschäftsbetriebs. Die Widerstandsfähigkeit der Wertschöpfung wird erhöht. Ein definierter Notbetrieb bzw. eine zeitnahe und angemessene Krisenreaktion wird ermöglicht.

Notfallmanagement dient der Absicherung „typischer" Ausfallszenarien, z. B. wesentlicher Infrastrukturkomponenten, IT, Personalkapazitäten oder Dienstleister. Basierend auf den Anforderungen an den Geschäftsbetrieb sowie den finanziellen, personellen und technischen Möglichkeiten Ihres Unternehmens werden Notfallstrategien abgeleitet und in Notfallplänen operationalisiert.

Krisenmanagement umfasst darüber hinaus gehende Situationen, die eruptiv und nur schwer planbar sind (z. B. Schadensszenarien mit massiven Schäden aber geringer Eintrittswahrscheinlichkeit) oder solche, die sich nicht unmittelbar auf den Geschäftsbetrieb auswirken, jedoch einer schnellen Reaktion bedürfen (z. B. Erpressung).

Eine gesonderte Notfall- und Krisenorganisation im Zusammenhang mit einer gesteuerten Kommunikation, die während einer Notfall- und Krisenbewältigung aktiviert wird, bündeln alle notwendigen Kompetenzen, ungeachtet ihrer Hierarchie oder organisatorischen Zuordnung.

HISOLUTIONS AG

Als Beratungsunternehmen spezialisiert auf Notfall- und Krisenmanagement, beschäftigt die HiSolutions AG das größte Experten-Team mit umfassender und langjähriger Erfahrung im deutschsprachigen Raum.

Als Fachgröße war die HiSolutions an der Entwicklung u. a. des BSI Standard 100-4 Notfallmanagement federführend beteiligt. Experten der HiSolutions sitzen im Normungsausschuss zur ISO 22301 Reihe (Business Continuity Management) und haben den HV-Benchmark zur Beurteilung der Verlässlichkeit von IT-Dienstleistungen für das BSI[4] entwickelt.

Ein hochspezialisiertes Team unterstützt Sie mit ausgesuchten Experten beim Aufbau eines anforderungsgerechten und angemessenen Notfall- und Krisenmanagementsystems.

[4] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard04/it_grundschutzstandards04.html

KONTAKT

HiSolutions AG

Schloßstraße 1
12163 Berlin
+ 49 30 533 289 0
+ 49 30 533 289 900
info@hisolutions.com
www.hisolutions.com

ANSPRECHPARTNER

Stefan Nees

Director
info@hisolutions.com