Umsetzung der Kritis-Anforderungen am Beispiel der Talsperre Eibenstock

Heiko Rentsch
Landestalsperrenverwaltung des Freistaates Sachsen (LTV), Pirna, Deutschland

Entsprechend der hohen gesellschaftlichen Bedeutung Kritischer Infrastrukturen sind deren Betreiber verpflichtet, die dafür maßgeblichen Systeme und Prozesse gegen Ausfälle und Manipulation nach dem Stand der Technik zu sichern. Daraus ergeben sich konkrete Anforderungen an unterschiedliche Bereiche wie zum Beispiel an die Prozessleit- und Automatisierungstechnik (OT), die Informationstechnik (IT) oder die bauliche Sicherheit. Die LTV hat unterschiedliche Erfahrungen bei der Ermittlung und Umsetzung dieser Kritis-Anforderungen gesammelt, insbesondere wie sich die Arbeit in den einzelnen Bereichen dadurch verändert.

Motivation

Die Cyberkriminalität nimmt immer mehr zu und mittlerweile ist nicht mehr die Frage ob, sondern wann es die eigene Organisation trifft. Immer mehr Unternehmen auch im direkten Geschäftsumfeld werden nach der Verschlüsselung ihrer Daten von Kriminellen erpresst. Beobachtet werden aber auch steigende Fälle von Sabotage vor Ort. Diese Bedrohungen stellen immer höhere Anforderungen an den Schutz der Kritischen Infrastruktur. Auch der Gesetzgeber trägt dem Rechnung und verpflichtet Betreiber Kritischer Infrastrukturen „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen [...] zu treffen [...]. Dabei soll der Stand der Technik eingehalten werden."

Ermittlung der Anforderungen

Die LTV ermittelt die Anforderungen, die zu einem bestimmten Zeitpunkt dem Stand der Technik entsprechen, aus dem branchenspezifischen Sicherheitsstandard (B3S) Wasser/Abwasser der Deutschen Vereinigung für Wasserwirtschaft, Abwasser und Abfall e.V. (DWA) und dem IT-Grundschutz Kompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Diese allgemeinen Anforderungen werden in Form von themenbezogenen Richtlinien für die jeweilige Zielgruppe übersetzt und an die konkreten Gegebenheiten der LTV angepasst.

Umsetzung der Anforderungen

Die erstellten Richtlinien betreffen viele unterschiedliche Bereiche wie zum Beispiel die OT- und IT-Systeme, die Zutrittskontrolle und bauliche Sicherheit, aber auch die Geheimhaltung von sensiblen Information. Deswegen ist die Einbeziehung des gesamten Personals gefordert. Bei jeder technischen, baulichen oder organisatorischen Änderung sind neben der technischen Sicherheit auch immer die Belange der Informationssicherheit zu berücksichtigen. Dabei werden Defizite und deren Relevanz eher erkannt, wenn der eigene Verantwortungsbereich aus der Sicht eines Angreifers betrachtet wird. Wir unterscheiden hier

- entfernte Angriffe aus dem Internet und
- direkte Angriffe vor Ort.

Diese Bedrohungen sind für das eigene Personal oft neu im Gegensatz zu Störungen, die durch technische Ausfälle oder Naturereignisse verursacht werden. Deswegen ist eine verstärkte Sensibilisierung, Schulung und Beratung in diesem Bereich erforderlich. Das wird auch durch die gemeinsame, interdisziplinäre Entwicklung von spezifischen Sicherheitskonzepten unterstützt. Neben zahlreichen IT-Maßnahmen sind dabei die folgenden Punkte von Bedeutung:

- Umsetzung des Prinzips der minimalen Berechtigungen bzgl. Zutritt, Zugang und Zugriff
- bauliche Absicherung von sensiblen Bereichen
- Überwachung der technischen und baulichen Infrastruktur
- Übungen auf der Basis von Notfall- und Wiederherstellungsplänen

Fazit

Ein durchgehendes und angemessenes Sicherheitsniveau ist von entscheidender Bedeutung, um einen wirkungsvollen Schutz der Kritischen Infrastruktur zu erreichen. Die Einbeziehung aller Beteiligten ist dabei eine wesentliche Voraussetzung.