

Kritische Infrastrukturen

Zukunftsfähig verbessern

[14.04.2016] Betreiber kritischer Infrastrukturen stehen hinsichtlich der Zuverlässigkeit, Sicherheit und Zukunftsfähigkeit aktuell vor wesentlichen Herausforderungen. Das wird mit Blick auf den Sachstand im Bereich Mission-Critical-Netze in Deutschland deutlich.

Energieversorger, Betreiber von Öl- und Gaspipelines oder Regional- und Fernbahnen sind auf hochverfügbare und sichere Kommunikationsnetze angewiesen. Sie steuern damit die effiziente Verteilung von Strom, Gas und Wasser oder bringen Menschen und Güter verlässlich an ihr Ziel. Die Telekommunikationsnetze wie auch die Leitungs- und Schieneninfrastruktur sind über viele Jahre gewachsen und müssen stetig erneuert und modernisiert werden. Andernfalls können sie ihre Aufgabe einer zuverlässigen und sicheren Versorgung eines Landes nicht erfüllen. Deshalb wird diese Infrastruktur auch als anwendungskritisch, als mission-critical bezeichnet. Der Begriff mission-critical stammt aus der Raumfahrt und charakterisiert Bauteile und Komponenten, die für den Erfolg einer Mission unverzichtbar sind. Ihr Ausfall kann nicht zuletzt Millionenschäden verursachen. Die Betreiber von Kommunikationsnetzen stehen aktuell vor drei zentralen Herausforderungen. Zum einen müssen die seit 10 bis 15 Jahren im Einsatz befindlichen Kommunikationsnetze und -systeme schrittweise um zukunftsfähige IP-Lösungen erweitert oder ersetzt werden. Darüber hinaus sind die Anforderungen aus dem seit Ende Juli 2015 geltenden IT-Sicherheitsgesetz umzusetzen und kritische Infrastrukturen besser zu schützen. Die dritte Herausforderung ist im Bereich der Wettbewerbsfähigkeit angesiedelt. Um diese aufrechtzuerhalten, müssen Verwaltung und Betrieb vereinfacht und die laufenden Kosten gesenkt werden. Traditionelle Energieversorger geraten durch neue Wettbewerber zunehmend unter Druck.

Netze effizienter schützen

Energieversorger beaufsichtigen und lenken den kontinuierlichen Betrieb ihrer Mission-Critical-Kommunikationsnetze heute noch vorrangig mit Systemen, die auf Synchron-Digitale-Hierarchie-Technologien basieren. Die leitungsbasierte SDH-Technik gewährleistet höchste Zuverlässigkeit bei der Übertragung von Daten und Steuersignalen. Zur Überwachung unbemannter Stationen oder von Verkehrsknotenpunkten kommen jedoch vor allem Ethernet/IP-basierte Systeme zum Einsatz. Bei der Modernisierung ihrer Mission-Critical-Netze müssen die Betreiber daher auf absehbare Zeit sowohl die Bestandssysteme als auch die zunehmende Integration neuer IP-basierter Systeme berücksichtigen. Die allmähliche Migration herkömmlicher leitungsvermittelter hin zu einer paketbasierten Übertragung wird sich über einen langen Zeitraum hinziehen. Eine weitere Anforderung betrifft regulatorische Änderungen. Ein Beispiel dafür ist das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, das IT-Sicherheitsgesetz. Es ist in Deutschland seit dem 25. Juli 2015 in Kraft. Die Betreiber von Mission-Critical-Kommunikationsinfrastrukturen, beispielsweise in den Branchen Energie, Telekommunikation und Verkehr, werden damit verpflichtet, ihre Netze effizienter vor Cyber-Angriffen zu schützen. Im Kern sind die Unternehmen in den betroffenen Branchen gefordert, ihre IT-Sicherheitsmaßnahmen auf den aktuellen Stand der Technik zu bringen. Was der Gesetzgeber im Detail darunter versteht, ist noch offen. Notwendig ist an dieser Stelle ein umfassendes IT-Sicherheitskonzept, das bei der Gewährleistung der Integrität, Ausfallsicherheit und Verfügbarkeit der Netze anfängt. Ein wichtiger Bestandteil ist die Umsetzung von Anforderungen wie Authentifizierung, Autorisierung, Intrusion Detection sowie eine verschlüsselte Datenübertragung.

Im Wettbewerb behaupten

Der Wettbewerb auf dem Markt der Energieversorger hat sich in den vergangenen Jahren weiter verschärft. Die Verbraucher können je nach Versorgungsgebiet unter Dutzenden von Strom- und Gasanbietern wählen. Um sich eindeutiger positionieren zu können, setzen vor allem die regionalen Anbieter darauf, ihre Infrastrukturen effizienter zu nutzen, um neue Märkte und Kundengruppen zu erschließen. Wo es um die Steuerung und Zukunftsfähigkeit von Mission-Critical-Kommunikationsnetzen geht, sollten sich Netzbetreiber für Plattformen entscheiden, mit denen sie auch künftig die Anforderungen ihrer bewährten Systeme abbilden können und die ihnen gleichzeitig die Möglichkeit einer reibungslosen Migration in Richtung paketorientierter Übertragungslösungen bieten. Netzbetreiber sind damit in der Lage, die Zuverlässigkeit und Verfügbarkeit von Diensten zu steigern, die Netzkomplexität zu reduzieren und letztlich Betriebskosten zu senken. Eine wichtige Rolle spielt dabei die Implementierung eines effizienten IT-Sicherheitskonzepts mit einer verschlüsselten Datenübertragung als Herzstück.

()

Stichwörter: Informationstechnik, Keymile, IT-Sicherheitsgesetz, Kritische Infrastrukturen