Konsequentes Netz-Monitoring

Kritis-Betreiber in der Verantwortung für mehr Sicherheit

Andreas Hornsteiner

Vor dem Hintergrund des IT-Sicherheitsgesetzes müssen auch Unternehmen außerhalb von Telekommunikation und Informationstechnik die Sicherheit ihrer Datennetze garantieren. Wo lauern die Gefahren und wie kann man ihnen begegnen?

Die vernetzte Gesellschaft wird immer mehr zur Realität. Viele Bereiche von der Telekommunikation bis zur Strom-, Wasser- und Gasversorgung sind inzwischen so eng miteinander vernetzt, dass die Grenzen zunehmend verschwimmen. Doch auch in anderen Feldern wie Gesundheitsversorgung, Mobilität und Finanzen sorgt die Digitalisierung für eine immer höhere Abhängigkeit von Netzinfrastrukturen. Glaubt man den Prognosen, befinden wir uns immer noch in der Frühphase dieses weltweiten Trends: In Zukunft sind Datenmengen zu erwarten, die wir uns heute nur schwer vorstellen können. Die wichtigste Voraussetzung dafür ist ein leistungsstarkes Glasfasernetz, denn diese Dimensionen übersteigen die Leistungsfähigkeit von Legacy-Netzen bei weitem.

Vernetzung macht anfällig

Die zunehmende Vernetzung birgt jedoch auch Gefahren, denn wenn alle immer miteinander verbunden sind, steigen die gegenseitigen Abhängigkeiten. Nach dem alten Beispiel des Schmetterlingseffekts können kleine Unregelmäßigkeiten an einem Punkt in anderen Bereichen zu schwerwiegenden Störungen führen.
Der Gesetzgeber hat bereits im Juli 2017 mit dem IT-Sicherheitsgesetz die rechtliche Grundlage für höhere Sicherheitsstandards geschaffen. Auf europäischer Ebene beschäftigten sich die Behörden schon lange mit dem Thema. Zunächst ging es vor allem darum, die Stromnetze – und dabei insbesondere Kernkraftwerke – besser vor Terroranschlägen zu schützen. Mit zunehmender Vernetzung wurden immer mehr kritische Infrastrukturen identifiziert, die sog. Kritis. So umfasst das aktuelle Bundesgesetz die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen. Darüber hinaus zählen zu den Kritis alle Einrichtungen oder Anlagen, die „von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“, also z.B. staatliche Organe. Alle betroffenen Stellen sind danach gesetzlich verpflichtet, die Sicherheit ihrer IT-Infrastruktur und das reibungslose Funktionieren der damit verbundenen Datennetze nach dem aktuellen Stand der Technik zu gewährleisten. Mindestens alle zwei Jahre müssen sie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nachweisen, dass sie die Auflagen einhalten.

IT bedeutet nicht nur Computer

Bei dem Titel „IT-Sicherheitsgesetz“ denkt man natürlich zunächst an Hacker, Viren und ähnliche Bedrohungen, die sich gegen die vernetzten Rechner oder die darauf installierte Software richten. Doch die passiven Strukturen wie Kabelnetze, Leitungen, Schaltkästen und Betriebsräume müssen in die Planung zur Netzsicherheit mit einbezogen werden. Materialverschleiß, Bagger und Nagetiere können die Netzverfügbarkeit beeinträchtigen. Dazu kommt die wachsende Bedrohung durch menschliche Feinde wie Terroristen, Saboteure und Vandalen. Beim Fiber-Tapping z.B. zweigen Lauscher kleine Teile des Signals ab, um Telefon- oder Datennetze anzuzapfen. Gegen all diese Gefahrenquellen müssen Kritis-Betreiber ihre Netzinfrastruktur schützen. Sie müssen also einerseits das Netz selbst kontinuierlich überwachen, um schnell auf Störungen reagieren zu können. Gleichzeitig gilt es aber auch, den unbefugten Zu-

Dr. Andreas Hornsteiner leitet den Geschäftsbereich Fasertechnologien bei der Laser Components GmbH in Olching

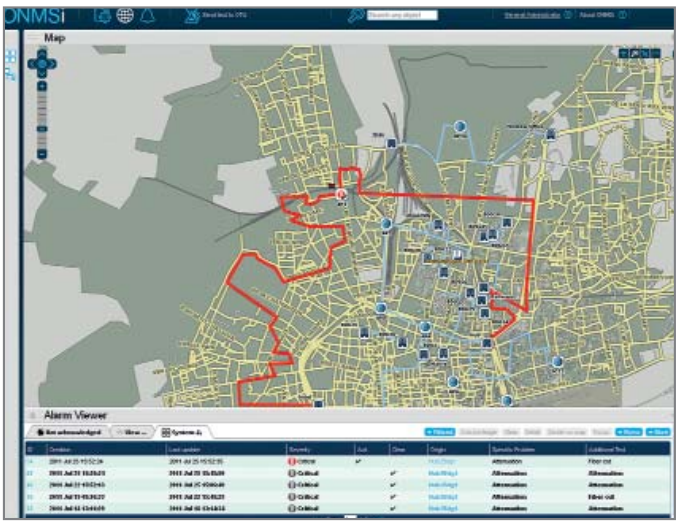

Bild 1: ONMSi-Systeme überwachen alle Netzebenen rund um die Uhr

gang zu Schaltkästen, Kabelschächten oder Rechnerräumen zu kontrollieren.

Alle Fasern immer im Blick

Rund-um-die-Uhr-Überwachung ist ein probates Mittel, um die Ausfallsicherheit des eigenen Glasfasernetzes zu gewährleisten. Beschädigte Fasern verursachen Dämpfungsverluste, die gemessen und analysiert werden können. Sie treten u.a. bei Temperaturextremen, Materialermüdung oder beim Fiber-Tapping auf. Ein bewährtes Verfahren ist die Optical-Time-Domain-Reflectometry (OTDR, optische Zeitbereichsreflektometrie). Dabei werden kurze Lichtpulse (ns bis µs) in die Faser gesendet und die auf der Rayleigh-Streuung basierende Rückstreuung in der Glasfaser ausgewertet. Über die Laufzeit der Pulse kann eine Störung, Dämpfung oder Manipulation innerhalb von Sekunden ortsgenau ermittelt werden. Dabei läuft der Messstrahl entweder über eine vom Datensignal unabhängige eigene Faser (Dark Fiber) oder er nutzt eine Wellenlänge, die sich vom Datensignal unterscheidet, meist 1.650 nm. Sobald eine Störung entdeckt wird, schlägt das System Alarm. So hält der Netzbetreiber die durchschnittliche Reparaturzeit (MTTR – Mean Time to Repair) niedrig und kann eine hohe Verfügbarkeit garantieren.

Die großen Anbieter nutzen diese Technik in servergestützten optischen Netzüberwachungssystemen wie dem ONMSi von Viavi Solutions (*Bild 1*). Damit können sie vom Backbone bis zu den einzelnen Anschlüssen alle Ebenen ihrer weitverzweigten Netze rund um die Uhr überwachen und steuern. Mit diesen komplexen Lösungen lassen sich die MTTR und Netzausfallzeiten auf ein Minimum reduzieren.

Viele Kritis-Betreiber, die nur wenige Faserstränge betreiben, betrachten solche Systeme zu Recht als überdimensioniert und verzichteten bisher auf eine konsequente Netzüberwachung. Mit der neuen Gesetzeslage änderte sich diese Einstellung: Lokale Betreiber verlangen jetzt nach benutzerfreundlichen und kostengünstigen Plug-and-Play-Lösungen, die auf ihre Anforderungen zugeschnitten sind. Systeme wie die SmartOTU von Viavi verfügen neben einer OTDR-Messeinheit auch über einen optischen Switch und vereinen so auf wenig Raum alles, was zum Tracking von bis zu 48 einzelnen Fasern nötig ist (*Bild 2*). Über eine Webschnittstelle können sie auch ohne Herstellersoftware einfach gesteuert und ausgelesen werden. Störungsmeldungen gibt es u.a. per E-Mail oder SMS. Auf diese Weise können z.B. auch Kritis-Unternehmen, bei denen lediglich zwei Standorte über einen Faserstrang verbunden sind, die gesetzlichen Auflagen erfüllen. Da sich die Datenmengen inzwischen mit unvorhersehbarer Geschwindigkeit vermehren, sind all diese Lösungen nach oben skalierbar und können nach Bedarf zu komplexen Systemen ausgebaut werden.

Bild 2: SmartOTU: kompakte Monitoring-Lösung für bis zu 48 Fasern (Bilderquelle: Viavi/Laser Components)

Sicherung von Schächten oder Kanaldeckeln

Optional sollten auch Infrastrukturen wie Schächte, Rohre, Betriebs- und Überwachungsräume überwacht werden. Dazu eignen sich faseroptische Infrastruktursensoren, die auf verschiedene Änderungen in ihrer Umgebung reagieren, wie z.B. Temperatur- oder Feuchtigkeitssensoren, Tür-, Fenster- und Schachtdeckelsensoren sowie Kipp/Neige-Sensoren. Die Signale werden über die ohnehin vorhandene Glasfaserleitung übertragen. Eine einzige Faser reicht dabei für bis zu 80 verschiedene Sensoren oder Detektoren. Viele davon nutzen zur Detektion und Alarmgenerierung eine Veränderung der Fresnel-Reflexion und funktionieren daher unabhängig vom Stromnetz.

Die Investition lohnt sich

Um hundertprozentige Datensicherheit zu gewährleisten, sind selbstverständlich weitere Maßnahmen notwendig, allen voran ein effizienter Schutz vor Viren und anderen schädlichen Programmen. Hier soll jedoch nur von der Netzsicherheit die Rede sein. Kritische Infrastrukturen müssen rund um die Uhr reibungslos funktionieren. Folgerichtig müssen auch die damit verbundenen Netze 24 h am Tag volle Leistung bringen. Durch konsequente Überwachung der Netze können Kritis-Betreiber Fehler und Ausfälle frühzeitig erkennen und verhindern. Mit der richtigen Technik und fachmännischer Beratung können sie die Allgemeinheit vor unliebsamen Überraschungen schützen und sich selbst eine gute Grundlage für die Zertifizierung schaffen. Das Angebot von Laser Components umfasst dafür nicht nur alle notwendigen Geräte und Sensoren, auf Wunsch übernimmt man auch die Installation. *(bk)*