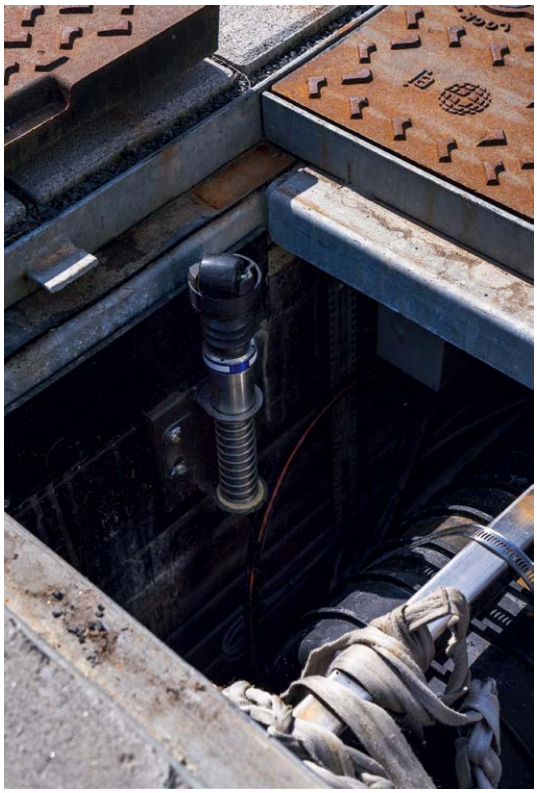
Überwachung kritischer Infrastrukturen

Faseroptische Sensoren im Praxiseinsatz

Die ununterbrochene Verfügbarkeit von Rechenzentren gehört zur Basis des gesellschaftlichen Lebens. Es gilt, das Rechenzentrum vor sämtlichen Gefahren zu schützen: Neben der Cybersicherheit gehört die physische RZ-Sicherheit zu einem umfassenden Schutzkonzept. Was hierbei oft zu wenig Beachtung findet, ist der Schutz der Verkabelung. Dieser Beitrag versetzt den Leser in die Lage eines Netzwerkadministrators, der mit einem nicht ausreichenden Schutz der kritischen Infrastruktur konfrontiert ist.

Sie sind ein erfahrener Netzwerkadministrator für eines der größten Rechenzentren im Land. Jeden Tag greifen mehrere Millionen Benutzer auf die Geräte in Ihrem Rechenzentrum zu, um E-Mails zu versenden und zu empfangen, Spiele zu spielen, Bankgeschäfte zu tätigen, fernzusehen, Filme zu streamen, einzukaufen, Videokonferenzen abzuhalten und vieles mehr. Das Netzwerk, für das Sie und Ihr Technikerteam verantwortlich sind, sorgt dafür, dass die Bürgerinnen und Bürger rund um die Uhr und an 365 Tagen im Jahr sicher und geschützt sowie gut unterhalten sind. Sie müssen dafür sorgen, dass das Rechenzentrum sicher ist und stets online bleibt.

Sie haben einen Aktionsplan für jedes erdenkliche Problem entwickelt, das in Ihrem Rechenzentrum auftreten könnte und das Netzwerk zum Erliegen bringen würde. Schließlich wären bei einem Ausfall Millionen von Menschen betroffen. Sie haben Ihre Netzwerksicherheitsprotokolle an die physischen Zugangskontrollen vor Ort gekoppelt, um zu gewährleisten, dass nur befugte Personen Zugang zu den Netzwerkgeräten haben. Das von Ihnen betreute Netzwerk wurde mit mehreren Redundanzen konzipiert, um einzelne Fehlerquellen auszuschließen. Etwaige Ausfälle im Rechenzentrum würden Benutzer nie bemerken, da Ihre Netzwerkgeräte vollständig vor Cyberbedrohungen sowie durch redundante Stromversorgungssysteme geschützt sind, falls ein einzelnes Gerät ausfällt. Als Administrator sind Sie sich auch der hohen Geldsumme bewusst, die verloren gehen würde, wenn das Netzwerk offline ist.



Der Schachtsensor überwacht Kabelschächte und funktioniert auch unter Wasser.

Bild: Connect Com

Es ist 18 Uhr an einem Freitag vor einem Feiertagswochenende. Als Sie gerade von der Arbeit nach Hause gekommen sind, klingelt Ihr Telefon. Ihr Vorgesetzte ist am Apparat und in heller Aufregung. Er teilt Ihnen mit, dass das gesamte Netzwerk des Rechenzentrums offline ist, er alle Schritte des Notfallplans ausgeführt hat und das Netzwerk immer noch nicht funktioniert. Sie machen sich sofort auf den Weg in das Büro.

Dort angekommen prüfen Sie, ob man bereits alle Maßnahmen zur Behebung eines Ausfalls erfolgreich umgesetzt hat. Das Sicherheitsteam im Rechenzentrum hat sich vergewissert, dass es keine unbefugten Besucher gab. Sie sprechen mit Ihrem Team, das verzweifelt versucht, herauszufinden, was passiert ist. Im Rechenzentrum gab es weder einen Stromausfall noch Anzeichen von Hardwarefehlern, die zu dem Ausfall hätten führen können. Es sind schon fast zwei Stunden vergangen und das Netzwerk funktioniert immer noch nicht. Sie setzen sich mit dem Netzwerkinfrastruktur-Team in Verbindung, um ihm mitzuteilen, dass es sich um ein Problem mit der physischen Infrastruktur handeln muss, da Sie Hardwareprobleme als Ursache für den Netzwerkausfall ausschließen konnten.

Eine Stunde später hat das Netzwerkinfrastruktur-Team die Fehlersuche abgeschlossen und teilt Ihnen mit, dass mehrere Glasfaser-Verbindungskabel, die den Hub des Rechenzentrums versorgen, durchtrennt waren. Bei diesen Kabeln handelt es sich um ein 864-fasriges Singlemode-Glasfaserkabel und es soll mehrere Stunden dauern, bis die Reparaturen abgeschlossen sind. Obwohl Sie das nötige Geld investiert und die notwendigen Schritte unternommen haben, um dafür zu sorgen, dass es im Rechenzentrum

keinen katastrophalen Ausfall geben wird, ist dies nun doch eingetreten. Millionen von Benutzern sind davon betroffen.

Mit der Zunahme bandbreitenintensiver Anwendungen im Laufe der Jahre ist auch die kritische Infrastruktur, die diese unterstützt, gewachsen. Ob es sich um Glasfaserkabel mit hoher Faserzahl handelt, die ein Rechenzentrum versorgen, oder um gebäudeinterne Kabel innerhalb eines Rechenzentrums – die kritische Infrastruktur stellt die Verbindung zu den Netzwerkgeräten her, die täglich Millionen von Kunden bedienen. Schäden an der kritischen Infrastruktur innerhalb oder außerhalb eines Rechenzentrums verursachen oft größere Ausfälle.

Obwohl RZ-Betreiber sehr viel Geld in die Anschaffung von Tools zur Zustandsüberwachung der Netzwerkgeräte, deren Redundanz, die unterbrechungsfreie Stromversorgung und in Cybersicherheitssoftware investiert haben, fokussieren sie sich zu selten auf die Zustandsüberwachung der kritischen Infrastruktur. Besteht der Verdacht, dass ein Netzwerkgerät ausgefallen ist, pingt man es. Wie aber überwacht man die passive kritische Infrastruktur, wenn sie die vermeintliche Ursache für einen größeren Netzausfall ist? Besteht die kritische Infrastruktur nicht einfach aus jeder Menge Kabeln? An einem Glasfaserkabel kann man sich aber nicht anmelden. Wenn die kritische Infrastruktur die Grundlage für die Konnektivität in einem Rechenzentrum ist, warum lässt man den Zustand der kritischen Infrastruktur nicht rund um die Uhr und 365 Tage im Jahr überwachen? Woher weiß man, ob jemand über einen Schacht oder einen Verteilerschrank außerhalb des Gebäudes auf die kritische Infrastruktur zugreift? Wie stellt man fest, ob durch Bauarbeiten eine Faser fast durchtrennt ist? Woher weiß man, ob jemand außerhalb oder innerhalb des Rechenzentrums außerplanmäßige Wartungsarbeiten durchführt?

Die Überwachung des Zugangs zu kritischen Infrastrukturen und der kritischen Infrastrukturen selbst haben viele Verantwortliche bisher stiefmütterlich betrachtet. Obwohl Unternehmen jedes Jahr hohe Umsatzeinbußen durch Ausfälle aufgrund von Schäden an ihrer kritischen Infrastruktur erleiden, erhöhen sie nur selten ihre Sicherheitsmaßnahmen durch die Überwachung ihrer kritischen Infrastruktur.

Zurück zu Ihrem Fall: Nach etwa acht Stunden war die kritische Infrastruktur repariert und das Netzwerk wieder online. Der Grund für den Ausfall war der unbefugte Zugang zu einem Schachtsystem, wo die kritische Infrastruktur im Rahmen eines Bauprojekts beschädigt wurde.

Sie hatten zwar einen Notfallplan für Probleme mit den Netzwerkgeräten, die einen Netzwerkausfall verursachen könnten, waren jedoch nicht für die kritische Infrastruktur verantwortlich. Die eingeleiteten Schritte zur Fehlersuche, um einen Geräte- und/oder Stromausfall als Ursache auszuschließen, kosteten wertvolle Zeit und Ressourcen. Die Kunden hatten einen Service-Ausfall und das Unternehmen selbst hat gegen das Service-Level-Agreement (SLA) verstoßen, welches eine Verfügbarkeit von 99,9 Prozent garantiert. Ihnen ist bewusst, dass es eine große Schwachstelle zwischen dem Netzwerkteam und dem Infrastrukturteam gibt, die es zu beheben gilt. Ihre unmittelbare Aufgabe besteht darin, die Netzüberwachung auf die kritische Infrastruktur auszuweiten. Sie müssen die Kommunikationslücke zwischen dem Netzwerkteam und dem Infrastrukturteam schließen, um eine durchgängige Überwachung zu gewährleisten.

Hier stehen bereits Lösungen auf dem Markt zur Verfügung, die die Lücke zwischen der Netzwerküberwachung und der Überwachung kritischer Infrastrukturen schließen können. Die Lösung FiberSecure von Connect Com beispielsweise ermöglicht es den Anwendern, den Zustand ihrer kritischen Infrastruktur mit Hilfe faseroptischer Sensoren zu überwachen. Dies umfasst stromlose Glasfasersensoren, die sich in Schächten oder Verteilerschränken anbringen lassen, Überwachung von Glasfaserverbindungen, die Manipulationen, Vibrationen und Schäden erkennen kann, oder hochmoderne Sensoren, die Erdarbeiten in der Nähe ihrer Glasfaserstränge erkennen können. Funktionen wie Fiber Forensics, optische Warnschwellen und ein Tool zur schnellen Fehlerbehebung sorgen für eine reibungslose Zusammenarbeit zwischen dem Netzwerkteam und dem Team für kritische Infrastrukturen. So lässt sich das Rechenzentrum sowohl vor hardwarebedingten Netzwerkausfällen als auch vor größeren Ausfällen aufgrund von Schäden an der kritischen Infrastruktur schützen. Die Software Infrastructure-Monitoring-System (IMS) bietet eine intuitive Oberfläche, die es jedem ermöglicht, seine Infrastruktur jederzeit zu pingen. Das IMS-Dashboard enthält eine Karte der gesamten kritischen Infrastruktur mit farbcodierten Statusanzeigen für Glasfaserverbindungen und allen Zugangspunkten zur kritischen Infrastruktur wie Schächte und Glasfaser-Verteilerschränke. Bei Manipulationen oder Schäden an der kritischen Infrastruktur löst das IMS sofort einen Alarm aus und schickt den Notdienst zum Schadensort. Ein spezielles Tool zur schnellen Fehlerbehebung dient als digitales Aufzeichnungssystem für alle kritischen Infrastrukturereignisse, auf welches man in Sekundenschnelle zugreifen kann. Kommt es zu einem Ausfall, verursacht durch eine Beschädigung der kritischen Infrastruktur, können die Netzwerkteams einfach alle Ereignisse, die kurz vor dem Ausfall aufgetreten sind, abrufen und so die Ursache sofort ermitteln. Das IMS-Dashboard steht dem Netzwerk- und Infrastrukturteam jederzeit zur Verfügung. Auf diese Weise lässt sich die Kommunikationslücke zwischen den beiden Teams schließen.

90 Tage sind vergangen. Das Rechenzentrum hat die Netzwerküberwachung auf die kritische Infrastruktur ausgeweitet. Sie haben bereits Feierabend, als Ihr Handy klingelt. Es ist wieder Ihr Vorgesetzter. Diesmal fragt er, ob Sie Wartungsarbeiten an der kritischen Infrastruktur nach Feierabend genehmigt haben, weil er gerade eine Warnung von seinem Netzwerksicherheitsteam erhalten hat. Offenbar ist ein Schacht offen und ein Glasfaserkabel war in Bewegung. Als Netzwerkadministrator bestätigen Sie Ihrem Vorgesetzten die Richtigkeit der Wartungsarbeiten und klären somit die Situation auf. Andreas Haupt/am

Andreas Haupt ist tätig in der Geschäftsfeldentwicklung bei Connect Com.