Physische Sicherheit von IT-Infrastrukturen

Alles im Blick: Monitoring-Systeme mit wachsamem Auge für KRITISche Dateninfrastruktur und Co.

Peter W., IT-Systemintegrator in einem mittelständischen Maschinenbauunternehmen, ist sauer. Wieder einmal wurde er bei der Beförderungsrunde übergangen – und das trotz seiner vielen Überstunden. So lässt er nicht mit sich umgehen! Denen da oben wird er es jetzt mal zeigen! Wenig später kommt in der Fertigungshalle plötzlich Unruhe auf: die Werker können am IT-Terminal offene Aufträge nicht mehr abrufen und benötigtes Material für die Maschinen nicht mehr auslagern. Es droht ein völliger Produktionsstopp – eine Katastrophe!

Ein unzufriedener Mitarbeiter, der sich mit IT-Sabotage an seinem Arbeitgeber rächt und so den Betrieb lahmlegt – ein Szenario, das nur auf dem Papier besteht? Ganz im Gegenteil: Laut dem Branchenverband der deutschen Informations- und Telekommunikationsbranche Bitkom ist der deutschen Wirtschaft im Zeitraum 2020/2021 durch Diebstahl, Spionage und Sabotage ein Schaden von mehr als 220 Milliarden Euro pro Jahr entstanden. Und der Bericht nennt weitere erschreckende Zahlen: 88 Prozent der mehr als 1000 befragten Unternehmen aus allen Branchen waren im selben Zeitraum Ziel von Angriffen. Dabei sind keinesfalls nur Attacken von außen die Ursache. Nach Datendiebstahl und Spionage rangiert Sabotage auf Rang drei der größten Bedrohungen für die IT-Sicherheit!

Wenn die IT-Infrastruktur KRITISch ist

IT-Infrastrukturen wie Server, Rechenzentren oder Micro Data Center sind in Zeiten von Digitalisierung und Vernetzung die Lebensader eines jeden Unternehmens. Das gilt in besonderem Maße für Unternehmen oder Einrichtungen, die zur kritischen Infrastruktur (KRITIS) zählen. „Charakteristisch für KRITIS ist, dass sie die Grundlage für das Funktionieren unserer Gesellschaft bilden“, sagt Ralf Mayer, Geschäftsbereichsleiter apraNET. KRITIS stammen für gewöhnlich aus den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen. Kommt es hier zu einem Ausfall oder einer Beeinträchtigung, ist die Versorgung oder die allgemeine Sicherheit erheblich gefährdet. KRITIS sind in besonderem Maße voneinander abhängig: Kommt es zu einer Störung, kann das einen Dominoeffekt auslösen. Ein Beispiel: Ein Stromausfall führt nicht nur dazu, dass im Supermarkt die TK-Ware auftaut, sondern hat unter Umständen auch Auswirkungen auf die Wasserversorgung. Denn ohne Strom können die Pumpen das Trinkwasser nicht in das Leitungsnetz transportieren. Deshalb gelten KRITIS auch als besonders schützenswert: Die Richtlinie der Bundesämter für Bevölkerungsschutz und Katastrophenhilfe (BBK) und für Sicherheit in der Informationstechnik (BSI) schreibt ein umfangreiches Risiko- und Krisenmanagement vor. Das betrifft unter anderem den Schutz der IT-Infrastruktur vor Gefahren wie Naturereignissen, technischem Versagen oder vorsätzlichen Handlungen.

Hochsensible Bereiche

Jedoch ist die IT-Infrastruktur nicht nur in KRITIS-Unternehmen ein hochsensibler Bereich, wie das fiktive Beispiel des Mitarbeiters Peter W. zeigt. „Außer mutwilligen Sabotageakten bedrohen auch Umweltfaktoren wie Hitze, Staub oder Nässe die Verfügbarkeit von IT-Systemen“, weiß Michael Neroth, Produktmanager bei apra. Doch welche Maßnahmen können Verantwortliche ergreifen, um ihre digitalen Daten und Prozesse optimal zu schützen – insbesondere an Standorten, die nur unregelmäßig mit Personal besetzt sind? „Eine praktikable und kosteneffiziente Lösung sind Monitoring-Systeme, mit denen sich der Zutritt und die Raumumgebung überwachen lässt“, sagt Michael Neroth. Der Clou: Sensoren erfassen die relevanten Parameter wie Temperatur und Luftfeuchtigkeit. Anhand festgelegter Schwellwerte lösen Monitoring-Systeme Voralarmierungen aus, wodurch Störungen frühzeitig erkannt und potenzielle Systemausfälle verhindert werden. „Übersteigt etwa die Temperatur im Raum den definierten Wert, können Maßnahmen

apraNET
Geschäftsbereich Netzwerktechnik
der apra-norm
Elektromechanik GmbH
vertrieb@apranet.de
www.apranet.de

wie Kühlung oder personenbezogene Alarmierungen automatisch aktiviert werden“, erläutert der Produktmanager. Mit dem hauseigenen Monitoringsystem EMI-One von apra lässt sich auch eine Zugangskontrolle realisieren, da elektronische Grifflösungen angebunden werden können.

So schützen eine Klinik, Stadtwerke und ein Felgen-Hersteller ihre IT

Wie Monitoring-Systeme wie EMI-One in der Praxis funktionieren und welchen Beitrag sie zum Schutz der IT leisten, zeigt das Beispiel des Klinikums Stuttgart. Das größte Krankenhaus in Baden-Württemberg gehört zu den KRITIS-Unternehmen und muss deshalb in der IT- und Telekommunikationsinfrastruktur besonders hohe Standards erfüllen. Schließlich ist es essenziell, dass das Personal jederzeit Zugriff auf Patientendokumente hat. So ist eine An- und Abmeldung von Patienten möglich und Laborwerte können digital abgerufen werden. Im Rahmen des Projekts „Clean“, das eine übersichtlich geordnete Struktur der IT- und Telekommunikationsinfrastruktur zum Ziel hat, lässt das Klinikum bis zu 150 Netzwerk- und IT-Schränke durch EMI-One überwachen. „Bei diesem Projekt überwacht und dokumentiert unsere Monitoring-Lösung genau, wer wann Zugriff hatte, und erfasst diese Informationen in einer Logdatei. Aber auch Temperatur und Feuchtigkeit werden präzise gemessen“, erklärt Michael Neroth.

Zugriff exakt kontrollieren

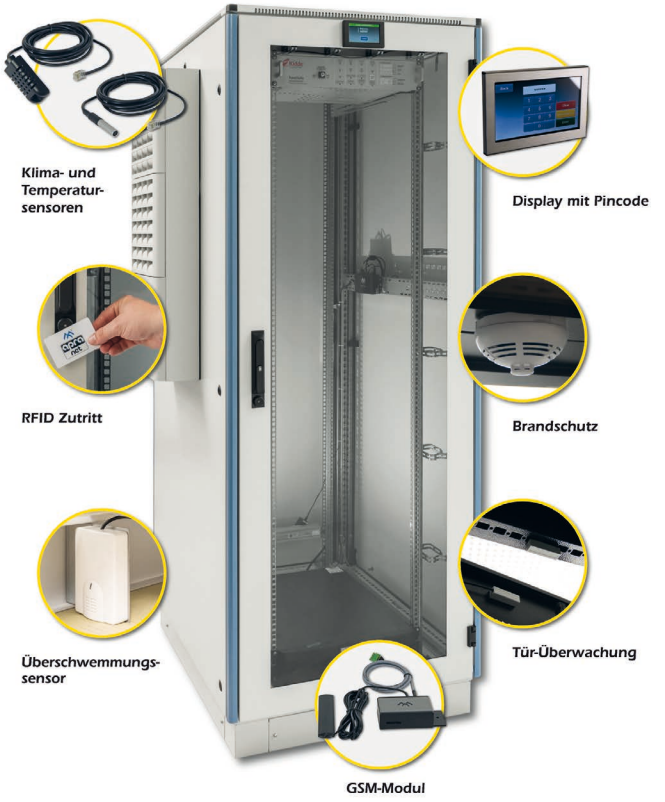
Ein weiterer Anwendungsfall ist die Borbet GmbH Thüringen, ein international führender Hersteller von Leichtmetallrädern. In der Fertigung des Unternehmens läuft die Produktionssteuerung über ein Micro Data Center, das auf dem Schranksystem TiRAX von apra basiert. „EMI-One wurde in dieses Schranksystem integriert und registriert und verarbeitet Parameter wie Klima, Rauch und Türkontakt. Angeschlossen ist zudem das EMI-Lock-System mit Mifare-RFID-Leser, um den Zugriff exakt zu kontrollieren und möglichen Sabotageakten direkt einen Riegel vorzuschieben“, berichtet Michael Neroth.

Schutz vor Vandalismus

Zu den Dienstleistungen von Stadtwerken zählt unter anderem Fibre to the home (FTTH), also die Verlegung von Glasfaserkabeln bis in die Wohnung. Um die Netzwerktechnik in den Kellern von Mehrfamilienhäusern vor Vandalismus und Sabotage zu schützen, – denn das könnte die Telekommunikation im gesamten Haus lahmlegen – werden in einem aktuellen Projekt alle rund 1500 Lokalisationen eines lokalen Internetproviders mit EMI-One von apra nachgerüstet. Jede EMI-One-Einheit ist in einen digitalen Stadtplan eingebunden. Sobald jemand einen Schrank öffnet, wird der Vorgang auf der Karte angezeigt und direkt signalisiert, ob es sich um einen regulären oder nicht geplanten Zugriff handelt.

Fazit

Monitoring-Lösungen als wachsames Auge und „digitaler Türsteher“. Es muss nicht immer die medienwirksame Cyberattacke sein – manchmal reicht schon ein unzufriedener Mitarbeiter oder ein Rohrbruch, damit IT-Systeme ernsthaft in Gefahr geraten. Dann kann der entstandene Schaden aber durchaus groß sein: die Produktion kommt zum Erliegen, die medizinische Versorgung kann nicht mehr gewährleistet werden oder Internet und Festnetz sind plötzlich nicht mehr verfügbar. Mit Blick auf den physischen Schutz der IT-Infrastruktur gilt deshalb: Vorsicht ist besser als Nachsicht – wer Risiken frühzeitig erkennt, kann rechtzeitig reagieren und Schlimmeres verhindern. Monitoring-Lösungen auf Sensorbasis überwachen relevante Parameter und regeln als „digitale Türsteher“ den Zugang zu sensiblen IT-Bereichen. Unternehmen und andere Einrichtungen können so sicherstellen, dass sie betriebsfähig bleiben und teure Störungen oder Verzögerungen vermeiden.



Wer schreibt

apra-norm Elektromechanik GmbH gehört zur apra-Gruppe mit Sitz in Mehren (Rheinland-Pfalz). Die 1969 gegründete Firmengruppe ist spezialisiert auf Schrank- und Gehäusesysteme aus Metall und Kunststoff. Ca. 400 Mitarbeiter arbeiten an den Standorten Daun, Mehren, Neukirchen (bei Chemnitz) sowie in den Vertriebsgesellschaften in Frankreich und Polen. ◄