LANline

10,– €
Dezember 2019
22. November

IT ■ Network ■ Datacenter www.lanline.de

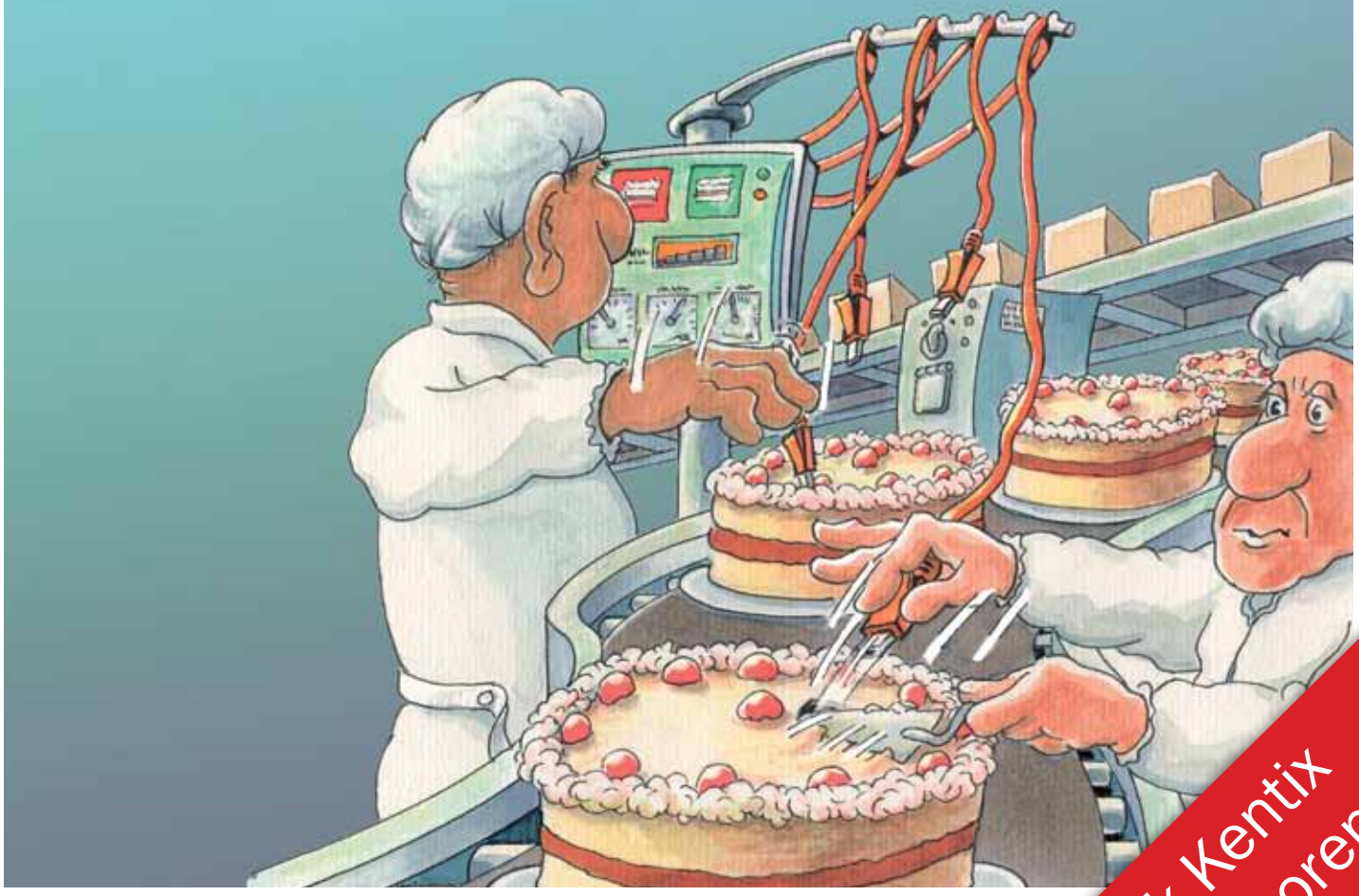
Verkabelung in IT und Industrie

Netze für das Internet of Things

Single Pair Ethernet

Alternativen zu RJ45-Steckverbindern

Mit Marktübersicht Kategorie-6_A-Kabel



Cloud-Kosten unter Kontrolle
Technik und Budget unter der Lupe

Richtlinienorientierter Sicherheitsansatz
Optimierung für die Security-Organisation

Schwer… Data…
M…

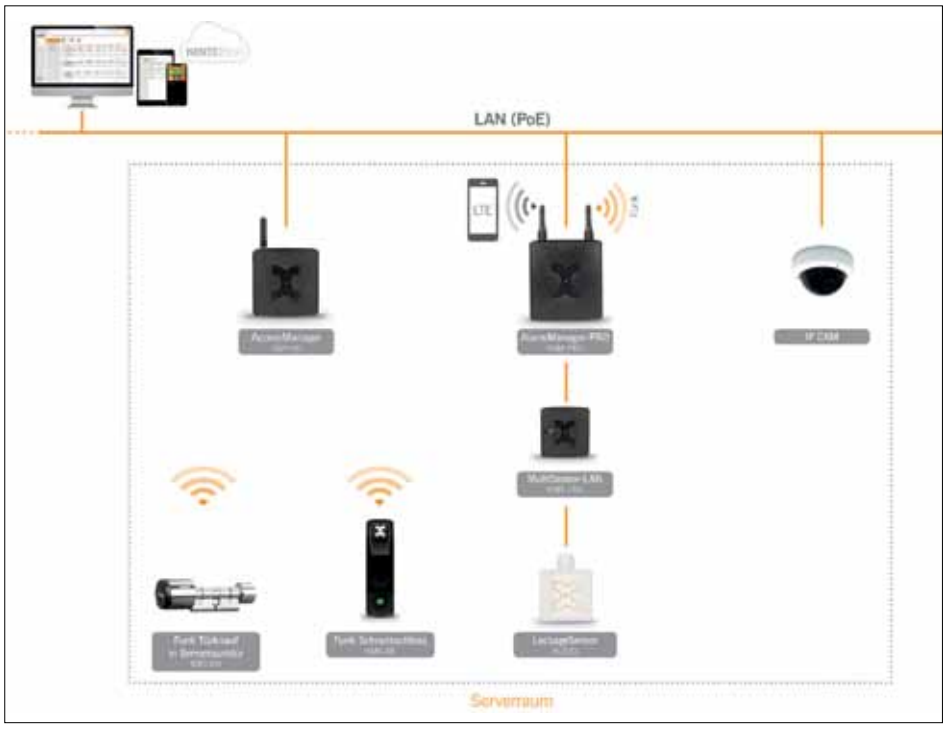
Sonderdruck Kentix
Vernetzte Sensoren sorgen für Sicherheit

Physischer Schutz von IT-Infrastruktur

Vernetzte Sensoren sorgen für Sicherheit

Ein IT-Ausfall kann bereits in kleinen Unternehmen hohe Kosten verursachen. Um einen Stillstand der Produktion oder den Ausfall von Services zu vermeiden, müssen Firmen Sicherheitsvorkehrungen treffen. Dabei gilt es, neben der IT-Umgebung auch die physische Infrastruktur abzusichern.

Die Ergebnisse einer Studie von Techconsult im Auftrag von Hewlett-Packard machen den wirtschaftlichen Schaden deutlich, der Jahr für Jahr durch IT-Ausfälle entsteht: Durchschnittlich vier Mal kommt es zum Stillstand in mittelständischen Unternehmen in Deutschland. Jeder dieser Vorfälle kostet rund 25.000 Euro stündlich und bis sämtliche Systeme wieder betriebsbereit sind, dauert es im Schnitt 3,8 Stunden. In Summe bedeutet das 380.000 Euro Schaden jährlich pro Mittelstandsbetrieb.
Und größere Unternehmen sind keinesfalls besser dran: Hier belaufen sich die Kosten laut Enterprise Strategy Group (ESG) sogar auf durchschnittlich 20,4 Millionen Euro jährlich. Doch damit sind die finanziellen Risiken noch nicht allumfassend betrachtet. Die Datenschutzaufsichtsbehörden haben sich auf ein Modell zur Bestimmung der Höhe von Bußgeldern bei Nichteinhaltung der EU-DSGVO verständigt, nach dem zukünftig auch in Deutschland Strafen in zweistelliger Millionenhöhe Realität sein können. Außerdem dürfen Unternehmensverantwortliche Image-Schäden, Umsatzverluste aufgrund von Kundenabgängen und weitere schädliche Faktoren nicht aus den Augen verlieren.



Schematische Darstellung: Absicherung eines Server-Raums durch Einsatz von Kentix SmartAccess und SmartMonitoring. Bild: Kentix

Wirksame Sicherheitsvorkehrungen sind nötig

In einer Zeit, in der jedes Business auf ein solides technisches Fundament angewiesen ist und ohne digitale Unterstützung Bänder stillstehen und Services ausfallen, wird das Thema Sicherheit immer wichtiger. Doch auch wenn der erste Gedanke in diesem Zusammenhang häufig in Richtung Cybersicherheit geht, müssen Entscheider vor allem auch die physische Sicherheit mitdenken. Immerhin sind 50 Prozent der IT-Systemausfälle nachweislich auf physisches Versagen von technischen Einrichtungen oder menschliches Fehlverhalten zurückzuführen. Die Gefahren sind vielfältig: Ob ein Verbrecher sich unbefugten Zutritt in einen Server-Raum verschafft, ein unzufriedener (Ex-)Mitarbeiter mutwillig wichtige Kabel durchtrennt oder der bedenkenlos genutzte USB-Stick gefährliche Viren in das Unternehmensnetzwerk einschleust – der Schaden kann in all diesen Fällen enorm sein. Hinzu kommen potenzielle technische Ausfälle aufgrund von Hitze, Wassereinbruch oder anderen Umgebungsveränderungen.
Alle kritischen Unternehmensprozesse sind heute von einer funktionierenden IT-Infrastruktur abhängig. Zu dem firmeneigenen Interesse an fehlerfreien Abläufen kommen stetig wachsende gesetzliche Vorgaben hinzu wie das IT-Grundschutzgesetz, die Datenschutzgrundverordnung (DSGVO), Compliance-Anforderungen und daraus resultierende Haftungsrisiken. Es gilt also, die eigene IT-Infrastruktur nach bestem Wissen und Gewissen vor negativen Einflüssen zu schützen, um Probleme zu vermeiden.
Datacenter beherbergen zahlreiche empfindliche Bestandteile: Angefangen von Servern, über die Energieversorgung bis

Die Vernetzung aller Komponenten in einem übergeordneten System ermöglicht einen transparenten Überblick und erlaubt es, dass der Techniker Änderungen nur an einer Stelle durchführen muss. Bild: Kentix

hin zu weiteren essenziellen Infrastrukturen sind unterschiedlichste Komponenten auf solide physische Sicherheitsvorkehrungen angewiesen. Die verbauten Geräte sind meist empfindlich und können bei zu hoher Temperatur oder Luftfeuchtigkeit bereits Schaden nehmen.

Dazu kommen Brand- und Einbruchsgefahren. Hochmoderne Sensoren, die man über eine PoE-Verbindung oder mit separatem Steckernetzteil mit Spannung versorgt, können von der Raumdecke aus sämtliche Zustände im Rechenzentrum aufnehmen. Ob Über- und Untertemperatur, defekte Klimaanlagen, Entfeuchter oder verstopfte Filter, Schmorbrände, Brandgase, Einbrüche, Zugriffe auf Racks und Server-Schränke, offene Fenster, defekte Rohrleitungen oder Netz-Spannungsausfällen – ein zukunftsfähiges System erkennt all diese Gefahren rechtzeitig.

Per PoE-Verbindung oder Funk gehen die Messwerte an ein zentrales Alarm-Management, das die Informationen auswertet und weiterverarbeitet: Es gleicht die gelieferten Daten mit voreingestellten Schwellenwerten ab und sendet bei kritischen Abweichungen sofort einen Alarm an einen oder mehrere Verantwortliche. Diese erhalten umgehend eine übersichtliche Aufstellung des Standorts sowie der betreffenden Werte und können so reagieren, bevor es zum Ausfall kommt.

Ein umfassendes Monitoring-System, das mittels IP-Tools wie SNMP oder einer offenen REST-API angebunden wird, schafft die notwendige Transparenz über das gesamte Unternehmen hinweg.

Im Hinblick auf die Abhängigkeit von fehlerfrei laufenden IT-Infrastrukturen, sollte solch ein intelligentes Monitoring-System zum Fundament eines jeden Unternehmens gehören. Idealerweise setzen Verantwortliche ein System ein, das modernste Technologien sowie Architekturen nutzt und entsprechend mit den künftig steigenden Anforderungen wachsen kann. Je höher die Skalierbarkeit, umso mehr Zukunfts- und Investitionssicherheit bietet die entsprechende Lösung.

Intelligente Systeme für eine präzise Zutrittskontrolle

Neben Manipulation und Umwelteinflüssen ist auch der unbefugte Zutritt ein erhebliches Risiko in Rechenzentren. Entsprechend sollten Unternehmen auf modernste Technik setzen, um den Zutritt an sämtlichen Türen wirksam zu überwachen. Möglich ist dies beispielsweise über intelligente Funk-Türknäufe oder IP-Wandlesegeräte, die in einem Management-System beispielsweise mit Access Points verbunden sind. So gelingt die Verwaltung in Echtzeit für alle Schließkomponenten des Unternehmens über eine Web-Oberfläche, die darüber hinaus als zentrales Logbuch alle Buchungsereignisse erfasst und speichert.

In besonders sensiblen Bereichen lassen sich Zutritte darüber hinaus mit einem Videobild verknüpfen. Die Vernetzung aller Komponenten in einem übergeordneten System ermöglicht einen transparenten Überblick und erlaubt es, dass man Änderungen nur an einer Stelle durchführen muss. Auch die Erweiterung der Anlage um weitere Bereiche oder Standorte ist so unkompliziert möglich.

Die Verknüpfung mit der eingesetzten Monitoring-Lösung schafft ein integriertes Gesamtsystem, indem alle Verantwortlichen jederzeit über sämtliche Zustände im Rechenzentrum informiert sind und im Gefahrenfall sofort reagieren können, bevor ein Schaden entsteht.

Physische Datacenter-Sicherheit schützt Investitionen

Zahlreiche Praxisbeispiele zeigen, dass der Einsatz von smarten Monitoring- und Access-Lösungen dank der heute verfügbaren Technologie einfach und kostengünstig möglich ist. Dabei lohnt es sich, auf Komponenten zu setzen, die sich mittels offener Schnittstellen einfach miteinander kombinieren und in ein Gesamtsystem integrieren lassen. So sind Zukunftsfähigkeit, Innovationssicherheit und Skalierbarkeit sichergestellt.

Die Auseinandersetzung mit diesem wichtigen Thema auf höchster Management-Ebene lohnt sich, denn ohne wirksame physische Sicherheitsmaßnahmen ist ein Rechenzentrum auch trotz intensiver Cybersicherheits-Bemühungen nicht umfassend geschützt. Die drohenden Schäden sind zu hoch, um in diesem Bereich ein Risiko einzugehen. Jan Sanders/ts

Jan Sanders ist Chief Sales Officer bei Kentix, www.kentix.de.