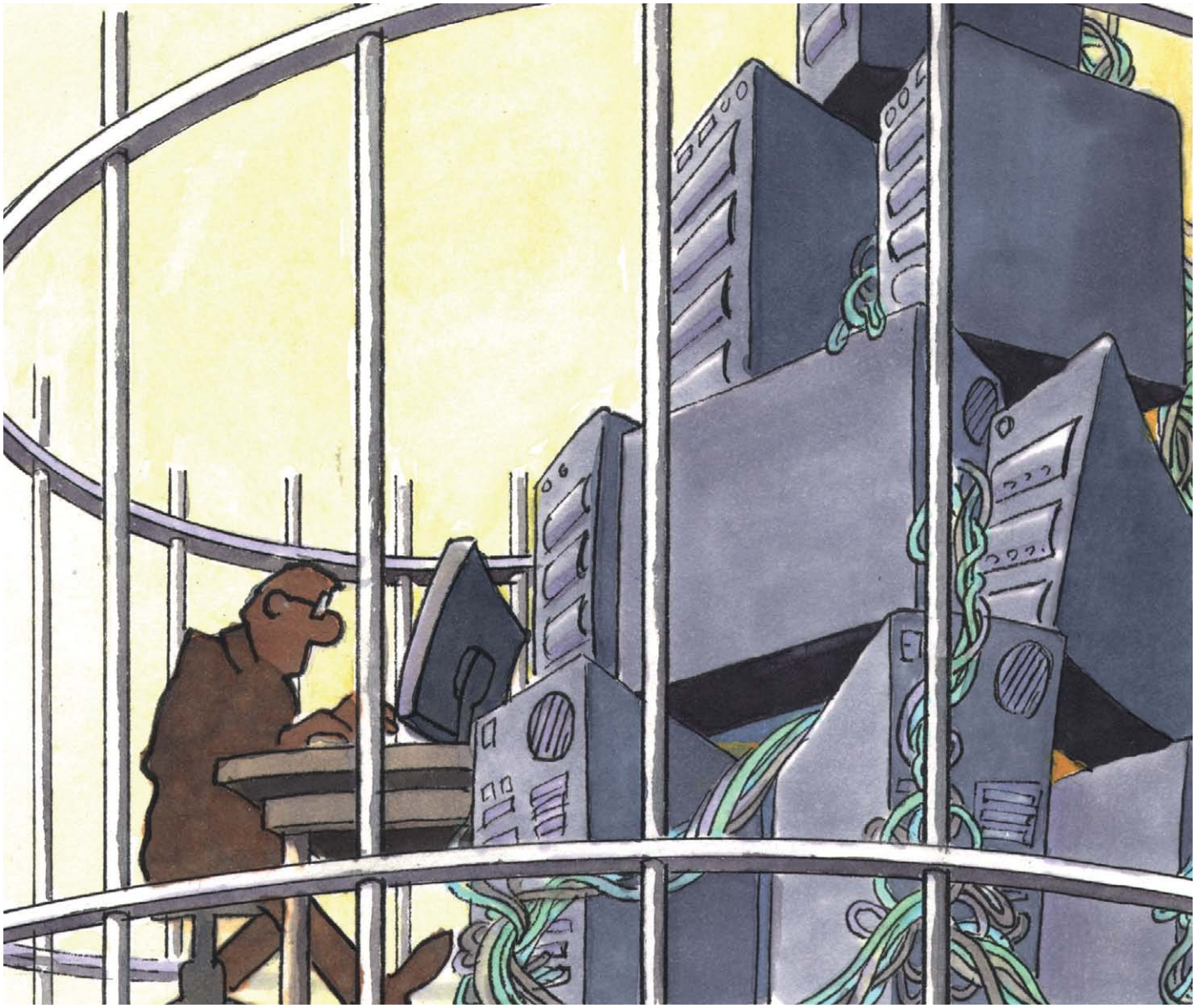
Aktiv gegen Datacenter-Gefahren

Physische Absicherung von Edge-Datacentern



Gemessen an den Herausforderungen der Digitalisierung nimmt der Bedarf an dezentralen Rechenzentrumsinfrastrukturen in Bezug auf Edge-Computing, IoT, Industrie 4.0 und kritische Infrastrukturen kontinuierlich zu. Die Absicherung eben dieser ist damit unabdinglich.

Im Gegensatz zu zentralen Rechenzentren können die Einsatzgebiete und Anwendungsfälle bei dezentralen Lösungen extrem unterschiedlich sein. Die physische Absicherung dieser verteilten IT-Infrastrukturen stellt die Verantwortlichen von Edge-Datacentern vor ganz neue Herausforderungen. Dazu gehören nicht nur die IT-Verantwortlichen, die sich den steigenden Anforderungen an die Verfügbarkeit und den Betrieb von kritischen IT-Infrastrukturen stellen müssen, sondern auch das Unternehmens-Management selbst. In Zeiten steigender Abhängigkeit von digitalen Geschäftsprozessen haben sie dafür Sorge zu tragen, normative und gesetzliche Vorgaben einzuhalten, um das Unternehmen vor haftungsrechtlichen Schäden, Imageverlusten oder Schadenersatzforderungen zu bewahren.

Anforderungen an die Absicherung

Um Geschäftsrisiken, aber auch potenzielle Bedrohungen zu identifizieren, sollte auch bei dezentralen IT-Infrastrukturen die Durchführung einer Risikoanalyse erfolgen. Risiken können dann als Grundlage für technische und organisatorische Planungsgrundlagen dienen. Eine weitere Herausforderung ist das oft fehlende Fachpersonal an den verteilten Standorten. Damit ist ein Höchstmaß an Transparenz gefordert, um sämtliche Prozesse remote und automatisiert zu regeln.

Ein Online-Umgebungs-Monitoring kann diese Transparenz realisieren und Ereignisse außerhalb und innerhalb des Rechenzentrums detektieren und visualisieren. Weiterhin sollten sämtliche Zutritte ins Rechenzentrum sowie Zugriffe an einzelne IT-Racks planbar online abgewickelt und dokumentiert sein. Um diese Anforderungen alltagstauglich erfüllen zu können, empfiehlt es sich, die wesentlichen Betriebsdaten aus den verschiedenen Standorten in einem Online-Dashboard darzustellen und somit überwachbar zu machen.

Umsetzung der notwendigen Maßnahmen

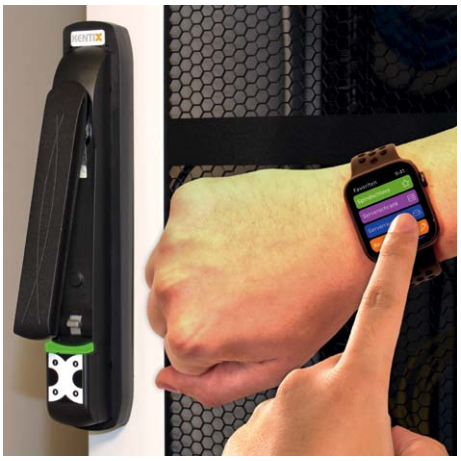
Nachdem die Anforderungen an eine zu planende oder bestehende RZ-Infrastruktur inklusive einer Analyse der Ist-Situation klarer sind, gilt es, die gewonnenen Erkenntnisse umzusetzen. Dabei sind sowohl der gesunde Menschenverstand als auch das Vermeiden einer Materialschlacht gute Ratgeber. Für die unterschiedlichen Einsatzgebiete und Anwendungsfälle von dezentralen Edge-Infrastrukturen gibt es sicher keine pauschale Lösung. Vielmehr sollten die nachfolgenden Aspekte mit in die Umsetzung einfließen.

Da es vielseitige und verändernde Einsatzgebiete und Anwendungsfälle gibt, sollte ein Fokus auf zukunftssichern Systeme liegen, die möglichst hohe Skalierungseffekte bieten. Das System sollte deshalb so beschaffen sein, dass es mit dem Unternehmen mitwachsen und sich weiterentwickeln kann, zum Beispiel bei der Anschaffung zusätzlicher Produktionsanlagen, Standorterweiterungen, Unternehmenszukäufen oder Expansionen.

Um die unterschiedlichsten Monitoring-Systeme beispielsweise im Bestand nutzen zu können, sind Sicherungssysteme mit Kommunikation in übergeordnete Drittsysteme ratsam. Das System sollte konsequent auf Web-Techniken und IT-Standards basieren. Dazu gehören standardisierte Schnittstellen SNMP, LDAP, Webhook und REST API. Die REST API hat den Status eines Industriestandards erreicht und bietet die Möglichkeit der vertikalen Integration. Solche Systeme bieten somit völlig neue Integrationsmöglichkeiten und eine enorme Erweiterung der Einsatzmöglichkeiten in digitalen Geschäftsmodellen und Cloud-Lösungen.

Wo immer möglich, sollte die Nutzung einer Mehr-Faktor-Authentifizierung erfolgen, um eine starke Verschlüsselung und Authentifizierung zu gewährleisten. Das gilt sowohl für die Hardware als auch für die Software.

Der Betrieb von Zutritts- und Zugriffssystemen sollte online und in Echtzeit erfolgen. Dadurch entfällt die Programmierung an den Endgeräten, und es ist eine lückenlose Dokumentation möglich, wer wann wie lange und aus welchem Grund Zutritt oder Zugriff erhalten hat. Auch der Türstatus jeder einzelnen Tür ist so rund um die Uhr bekannt. Systeme, bei denen die Programmierung an jedem einzelnen elektronischen Türknauf erfolgt oder keine Echtzeit-Dokumentation vorhanden ist, sind nicht mehr „State of the Art“.



Die Steuerung moderner IoT-Schließsysteme erfolgt von überall und zu jeder Zeit auch per Smartwatch. Bild: Kentix

Die Sicherungssysteme sollten netzwerkfähig und somit in der Lage sein, Updates für die Sicherheit und Funktionen durchzuführen. Autarke, statische Systemen wie beispielsweise klassische Einbruchmelde-

Checkliste

Gut informiert bei physischen Gefahren im Datacenter – zu checken ist:

- Vorhandensein eines speziell für die IT vorbereiteten Server-Raums,
- Benachrichtigung bei Brandentstehung und Möglichkeit zur sofortigen Einleitung von Maßnahmen,
- Benachrichtigung über Anstieg der Raumtemperatur,
- Benachrichtigung über Wasserleckagen durch Rohrbrüche oder eine defekte Klimaanlage,
- Information über Dauer eines Spannungsausfalles und korrekte Arbeitsweise der USV,
- Vorkehrungen gegen Einbrüche,
- Nachvollziehbarkeit der konkreten Raumbesetzung,
- Benachrichtigung über Ausfälle aktiver Komponenten und Netzwerkverbindungen,
- schnelle und IT-unabhängige Meldung über Auswirkungen menschlichen Fehlverhaltens und
- Möglichkeit zur Nachvollziehbarkeit und Rekonstruktion von Ereignissen, um zukünftige Fehler zu vermeiden.

anlagen können Cyberangriffe von außerhalb oft nicht standhalten. Um jede Art von Event, zum Beispiel Buchungen bei Zutrittskontrollsystemen oder Schwellenwertüberschreitungen bei Alarmdetektion, dokumentieren und nachverfolgen zu können, empfiehlt sich eine Videoüberwachung über IP-Kameras.

Die Integration dieser in das System sollte in jedem Fall möglichst unkompliziert ablaufen können.

Fazit

Damit die physische Sicherheit auch bei verteilten Infrastrukturen gewährleistet ist, sind mitwachsende, skalierbare Systeme nötig, die sich den steigenden Anforderungen anpassen können. Einen ausreichenden Grundschutz im Datacenter herzustellen, ist bereits mit überschaubarem Investitions- und Installationsaufwand möglich. Dazu gehört ein integriertes System aus ganzheitlichem Monitoring von Umgebungsparametern wie Temperatur, Luftfeuchte, Taupunkt, Spannung, Feuer und Einbruch sowie ein kontinuierliches Zutritts- und Zugriffs-Management mit permanenter Videoüberwachung. Sind die Komponenten IP-fähig, können die Verantwortlichen über ein Online-Dashboard auf die verschiedenen Bereiche wie Zutritt, Alarm, Klima, Energie und Video zugreifen und sie bequem und in Echtzeit aus der Ferne steuern. Dies ermöglicht ein zentrales Management dezentraler Systeme mit wenig Personalaufwand.

Frank Neubauer/am

Frank Neubauer ist Business-Development-Manager Datacenter bei Kentix, www.kentix.com.

Marktübersicht: Alarm- und Brandmeldesysteme

Anbieter	Web
Bosch	www.boschbuildingsolutions.com
Celsion	www.celsion.de
Danfoss Semco	www.danfoss.com
Gisbo Softwareentwicklung	www.gisbo.de
HAT-Protect	www.ht-protect.de
Hekatron	www.hekatron.de
iQSol	www.iqsol.biz
Kentix	www.kentix.com
Minimax	www.minimax.com
Mitel	www.mitel.com
NTI	www.networktechinc.com
Rittal	www.rittal.com
Securiton	www.securiton.de
TAS Sicherheits- und Kommunikationstechnik	www.tas.de
Telenot Electronic	www.telenot.com
Wagner	www.wagnergroup.com
Wichmann	www.wichmann.biz
Wireless-Netcontrol	www.wireless-netcontrol.com
Xtralis	www.xtralis.de