Zutrittssteuerung und Absicherung

Der Blick auf das IT-Rack

Zur IT-Sicherheit gehört es auch, zahlreiche gesetzliche Vorgaben und Normen zu erfüllen. Dies gilt insbesondere bei der Zutrittssteuerung und bei der Absicherung von zentralen und verteilten IT-Schränken. Intelligente Infrastruktur hilft bei der Umsetzung.

Um physische Risiken zu reduzieren, Manipulationen zu verhindern, Schäden zu vermeiden und ausreichende Dokumentation von Vorfällen zu erreichen, ist der Zutritt zu kritischen IT-Infrastrukturen auf IT-Rack-Ebene abzusichern. Diese Anforderungen finden sich zu Recht zum Beispiel in mehreren Normen und Verordnungen. Dies gilt etwa für das IT-Grundschutzgesetz nach ISO 27001. Im Baustein INF.2 des BSI-Grundschutzkompendium sind eine Zutrittskontrolle sowie das Schließen und Sichern von kritischen Infrastrukturen zwingend vorgeschrieben. In der EN 50600-2-5 für Sicherheitssysteme von Rechenzentren wird man ebenfalls fündig.

Danach sollen Zugangskontrollen und Absicherungen unnötige oder unerwünschte Zutritte zu Server-Schränken verhindern. Ähnliches gilt für die Datengrundschutzverordnung (DSGVO): Die physische Sicherheit von IT-Systemen ist herzustellen, da diese personenbezogene Daten verarbeiten und speichern. Außerdem gibt es branchenspezifische Anforderungen wie etwa die TISAX (Automotive), BAIT (Banken), VAIT (Versicherungen), worin weiterführende Anforderungen an Zutrittssteuerung, deren Dokumentation und zur Absicherung kritischer IT-Infrastrukturen genannt sind.

In der Praxis sollten Betreiber vier Faktoren für eine effiziente Umsetzung der genannten Anforderungen beachten. Zunächst gibt es mehrere Methoden der sicheren Authentifizierung von Zutritten per (a) RFID-Transponder auf Basis der ISO 14443/15693 (Mifare Desfire oder Legic Advant), per mehrstelligem PIN-Code (b) und zwar einzeln oder zusammen mit RFID-Transpondern zur Zwei-Faktor-Authentifizierung. Hinzu kommen (c) Mobilgeräte mit digitalen Token und Apps für flexible Berechtigungen etwa für Service-Mitarbeiter sowie (d) eine Fernöffnung durch zentrale Instanzen wie Control- oder Operations Center und (e) biometrische Verfahren zur Zutrittsauthentifizierung vorgeschalteter Räume

Intelligenter Rack-Hebel für den Zutrittsschutz von zentralen und dezentralen IT-Schränken. Bild: Kentix

Der zweite Faktor ist die revisionssichere Protokollierung und Überwachung von Zugriffen in Echtzeit. Eine zentrale Protokollierung berechtigter und unberechtigter Zutritte in Echtzeit ist essenziell, denn verantwortliche Personen können auf diese Weise kritische Ereignisse direkt nachvollziehen und bewerten. Das System muss darüber hinaus über Sensoren verfügen, um den korrekten Schließ- und Verriegelungszustand der Türen, aber auch der Seitenwände erkennen zu können. Letztere sind häufig mit einfachen Mitteln zu öffnen und ermöglichen somit Zugriff auf die installierten Systeme.

Drittens geht es um die zeitgemäße Integration und ein einfaches sowie sicheres System-Management. Zur problemlosen Integration in bestehende oder übergeordnete Sicherheitssysteme muss das Zutrittssystem über eine frei skalierbare Systemarchitektur verfügen und frei von proprietären Standards sein. REST-API, Webhooks, LDAP, SNMP v2/3, E-Mail und Push-Nachrichten sind heute Standards, die für eine zeitgemäße Integration unverzichtbar sind.

Ein von zentraler Stelle zu bedienendes Web-Frontend stellt ein einfaches System-Management bereit und gewährleistet eine Statusübersicht sowie Alarme beispielsweise im Fall offener Türen. Moderne Schrankschließsysteme erfüllen die Anforderungen an die Sicherung kritischer Infrastrukturen und vernetzen weitere Funktion zu direkten Systemkomponenten wie Sensoren oder Stromverteilerleisten (PDUs) in den IT-Schränken.

Für die Installation und den Betrieb sind auch folgende Punkte sehr vorteilhaft: eine einfache Verkabelung mit Patch-Kabeln, nur wenige PoE-Ports für viele IT-Schrankschlösser, keine Vermischung von operativem und Management-LAN im IT-Schrank sowie eine redundante Stromversorgung. Zutritt und Dokumentation sollten auch bei einem bei PoE-Ausfall weiter erhalten sein. Das Einspielen notwendiger Software-Updates sollte außerdem mühelos von einer zentralen Stelle aus möglich sein. Des Weiteren ist in allen Unternehmen ein geringer Stromverbrauch pro IT-Schrankschloss für eine gute Ökobilanz und geringe Betriebskosten wichtig.

Jan Sanders/jos

Jan Sanders ist Chief Sales Officer bei Kentix.