77500 · ISSN 1866-2420 · Einzelverkaufspreis: 14,- €

November/Dezember 6/2019

SECURITY insight

Fachzeitschrift für Unternehmenssicherheit
und Wirtschaftsschutz

Titelthema

Künstliche Intelligenz

Spitzengespräch

Nils Busch-Petersen, Hauptgeschäftsführer des HBB

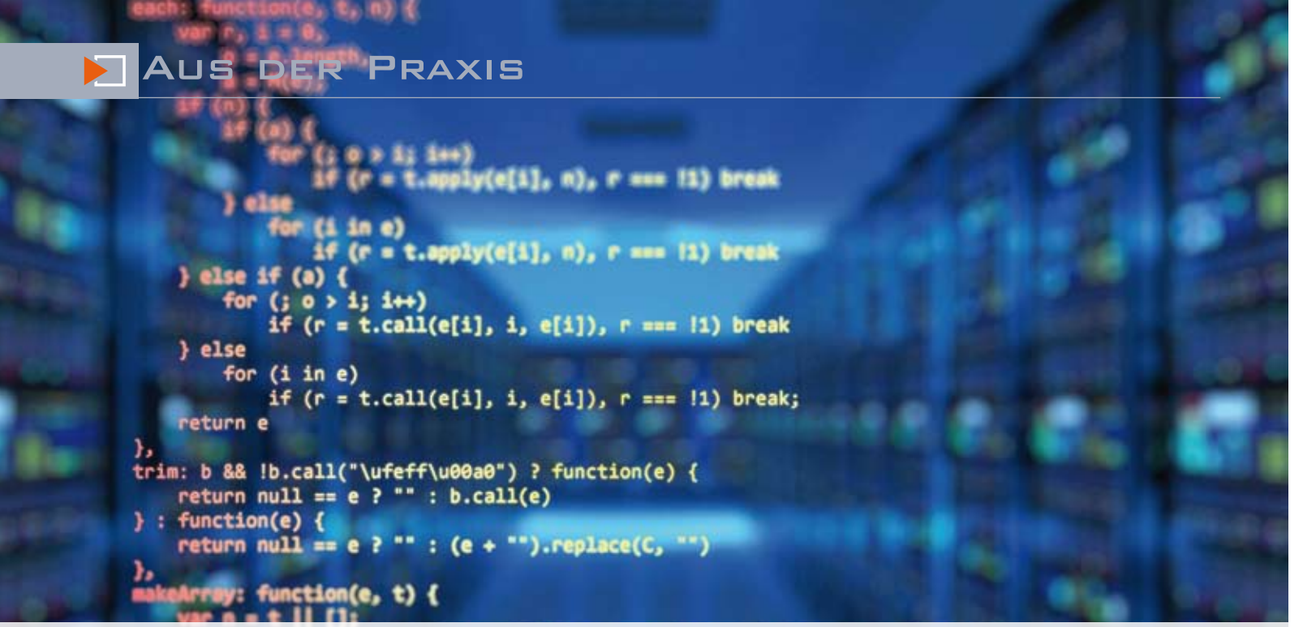

Foto: Elchinator – Pixabay

Alarm-und Zutrittsmanagement für Rechenzentren

Moderne Rechenzentren sind geradezu Hochsicherheitstrakte, schließlich geht es um fast alles: angefangen vom Schutz einer Unmenge von sensiblen Unternehmensdaten bis hin zur Sicherung der kritischen Infrastruktur in unserem Land. Denn neben Daten beherbergen Rechenzentren heute auch sämtliche vernetzte Technologien z. B. für die Steuerung der Verkehrsleittechnik oder zur Stromversorgung.

Neben den baulichen Gegebenheiten – es gibt Datacenter, die in umgebauten Atomschutzbunkern betrieben werden – trägt die Sicherheitstechnik maßgeblich zum hohen Sicherheits- und Verfügbarkeitsstandard bei. Hierzu gehören beispielsweise Brandfrüherkennungs-Systeme, die bereits dann auslösen, wenn ein Widerstand anfängt zu verkohlen. In Verbindung mit intelligenten Löschsystemen sind diese eine wirksame Maßnahme, damit sich Brände erst gar nicht ausbreiten können.

Komplettiert wird das individuelle Sicherheitskonzept um Sicherheitsmanagementsysteme, Einbruchmeldetechnik, Videoüberwachung und Zugangskontrollsysteme in unterschiedlichen Kombinationen.

Wer darf wann, wo und wie hinein?

Die Berechtigung für den Zutritt zum Rechenzentrum stellt eine immer komplexere Anforderung dar. Die meisten Unternehmen nutzen die Rechenzentrums-Infrastruktur externer Partner. Diese sog. Colocation Anbieter vermieten Flächen für Server und Server-Racks. In der Folge bedeutet dies: Die Zugänge zu den Serverräumen bzw. Flächen werden personell, zeitlich und örtlich begrenzt vergeben. Einfach gesagt stellen sich diese Fragen: Wer darf wann und wo hinein? Wie werden die Personen identifiziert? Wie werden die Zutritte unter den Vorgaben der Datenschutzgrundverordnung DSGVO protokolliert? Und schließlich, was passiert im Notfall – bei einem unberechtigten Zutritt? Oder einem Brand?

Carsten König, Vertriebsleiter Systemgeschäft TAS Sicherheits- und Kommunikationstechnik

Für Carsten König, Vertriebsleiter Systemgeschäft bei TAS Sicherheits- und Kommunikationstechnik, ist daher klar: „Angesichts der hohen Komplexität bei der Zutrittskontrolle aber auch der Einbindung und Vernetzung weiterer Sicherheitstechnik müssen diese unter einer einheitlichen Bedienoberfläche visualisiert und gesteuert werden. Das gilt selbstverständlich nicht nur für Rechenzentren. Wichtig ist die zentrale Überwachung auch für Unternehmen, Finanzinstitute, Versicherungen oder bei öffentlichen Einrichtungen."

Zentrales Alarmmanagement für Liegenschaften

Die TAS, Spezialist für vernetzte Sicherheitssysteme, Übertragungstechnik und automatische Alarmierung, setzt hierbei auf das etablierte Produkt TARSOS© – ein durch hochwertige Verschlüsselungsverfahren geschütztes Alarmmanagement. Bei der modular aufgebauten Kommunikations- und Sicherheitslösung für Liegenschaften können Meldungen aus den unterschiedlichsten Bereichen visualisiert und dokumentiert werden.

Das herstellerunabhängige System basiert auf der bewährten XMP-Babylon-Software, die speziell im globalen Gebäudemanagement erfolgreich eingesetzt wird. Diese ermöglicht es nicht nur, Zutrittskontrolle, Zeitwirtschaft, Aufzugkontrolle und Gefahrenmanagement in komplexen Gebäude- und Anlagenstrukturen abzubilden, sondern bietet auch Module für die Gebäudeautomation. Die Übertragung der Meldungen erfolgt entweder über ein eigenes Netzwerk oder Alarmübertragungsgeräte wie den Gerätefamilien TAS-Link und SIRO-Port, die ebenfalls bei der TAS entwickelt und hergestellt werden. Diese ermöglichen eine sichere Übertragung von Gefahren- und Störmeldungen über alle gängigen Übertragungswege.

Alles im Blick

An den Bedienplätzen eines technischen Leitstandes wie dem NOC (Network Operation Center) ist alles im Blick und unter Kontrolle, auch wenn mehr als 50 Rechenzentren angebunden sind. Das NOC weiß dank eines vernetzten Zutrittskontrollsystems, Grundrissplänen und der Aufschaltung von Kameras jederzeit, wie viele und welche Personen sich in den verschiedenen Bereichen der Liegenschaft befinden – nicht nur im Falle einer Evakuierung im Notfall ein unschätzbarer Vorteil, sondern auch um die Arbeitsplatzsicherheit zu gewährleisten.

Zugangsrechte und Zutrittsprofile liegen genauso vor wie Maßnahmenpläne, sie werden ebenfalls grafisch angezeigt. Selbstverständlich können die Zugänge nach Voranmeldung und entsprechender Buchung von Zeitfenstern auch manuell freigegeben werden – beispielsweise über ein Webportal oder per SMS. Durch die Möglichkeiten des Mobile Access können Berechtigungen ohne Identifikationsmedien heute schon direkt verschlüsselt an ein Mobilgerät versendet werden. Wichtig ist es hierbei eine Zwei-Faktor-Authentifizierung einzuplanen, um den höchstmöglichen Sicherheitsstandart zu erreichen.

Höchste Verfügbarkeit

Betreiber von hochsicheren zertifizierten Rechenzentren mit einer garantierten Verfügbarkeit von 99,982 Prozent stellen die gleichen Anforderungen an das Alarmmanagement. Bei Systemen wie TARSOS© werden sämtliche Übertragungs- und Kommunikationswege auf ständige Verfügbarkeit überwacht. Durch einen vollständig redundanten Systemaufbau lassen sich auch hier nahezu 100 Prozent Verfügbarkeit erreichen.

WWW.TAS.DE