34. JAHRGANG | März 2025 | AUSGABE 3

GIT SICHERHEIT

30 926

MAGAZIN FÜR SAFETY UND SECURITY

Titelthema Seite 66:

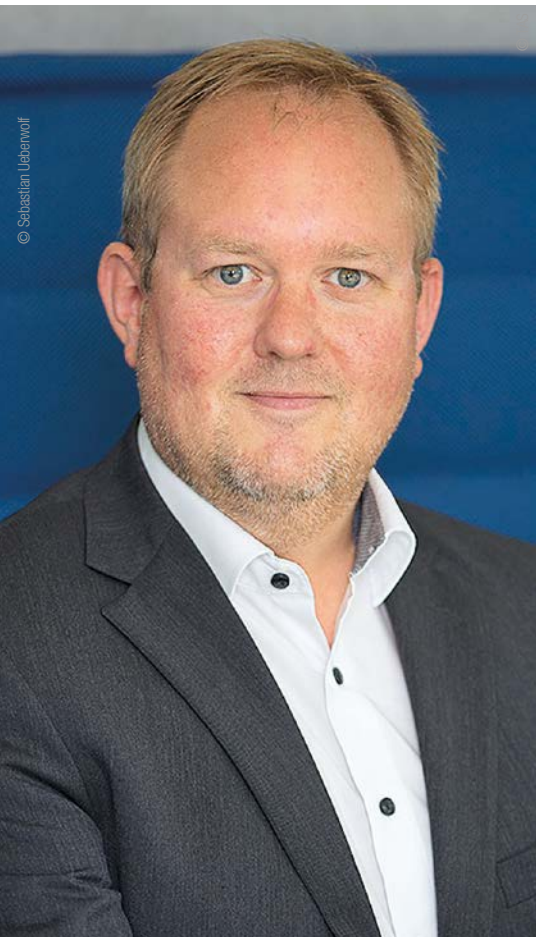
(Zukunfts-)Sichere Automation

Warum funktionale Sicherheit ohne Cyber-Security im digitalen Zeitalter nicht mehr ausreicht

HEFT IM HEFT

Ausgabe ONLINE lesen:

WILEY



Carsten König, Bereichsverantwortlicher für das bundesweite Errichtergeschäft der TAS

ZUTRITT

3-fach-Authentifizierung für Hochsicherheitsbereiche

Carsten König von TAS über mehrstufige Sicherheitskonzepte für Rechenzentren

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert Rechenzentren als „technische Schalt- und Speicherstellen der modernen Informationsgesellschaft“. Als Teil der Kritischen Infrastruktur unterliegen sie neben NIS2 für EU-weite Mindeststandards im Bereich Cyber Security auch den Regularien des KRITIS Dachgesetzes für Physical Security. GIT SICHERHEIT sprach mit Carsten König, Bereichsverantwortlicher für das bundesweite Errichtergeschäft der TAS, über mehrstufige Sicherheitskonzepte, die in aktuellen Projekten umgesetzt werden. Das Unternehmen verfügt als Spezialist für vernetzte Sicherheits- und Alarmierungssysteme über profundes Know-how für komplexe Aufgabenstellungen in Hochsicherheitsbereichen.

GIT SICHERHEIT: Herr König, welche physischen Sicherheitsmaßnahmen sind bei einem Rechenzentrum notwendig?

Carsten König: Es sind viele Bausteine, zentrales Element ist jedoch die Zutrittskontrolle. In einem Rechenzentrum werden hochsensible Unternehmensdaten gespeichert. Und oft erfolgt von hier aus auch die Steuerung der Verkehrsleittechnik und Stromversorgung. Die sichere Authentifizierung von Berechtigten für den Zutritt zu einem Rechenzentrum bzw. Teile davon, ist im wahrsten Sinne des Wortes der Schlüssel für ein hohes Sicherheitsniveau. Dabei setzen wir in vielen unserer Projekte auf parallele Verfahren, die den Zugang nach drei verschiedenen Kriterien regeln. Das erste Kriterium ist Besitz, z. B. durch eine ID-Karte, zweitens Wissen, z. B. durch einen PIN-Code, und drittens sind es die Eigenschaften, z. B. durch biometrische Merkmale. Diese 3-fach Authentifizierung bietet einen sehr hohen Schutz. Wir setzen sie nicht nur bei Rechenzentren ein, sondern auch bei Finanzdienstleistern und selbst bei Privathäusern für Personen mit einem besonderen Risikoprofil.

Es gibt verschiedene biometrische Verfahren, welche präferieren Sie?

Carsten König: Ob Iris- oder Venenscan, Fingerprint oder Gesichtsfelderkennung – alle tragen zu einer sicheren Authentifizierung bei. Aus der Praxis kann ich aber sagen, dass der Handvenenscan ein besonders fälschungssicheres Verfahren ist. Venen sind nun mal eindeutig. Zudem ist die Handvenenerkennung weniger fehleranfällig als andere biometrische Verfahren, braucht weniger Zeit zur Identifikation im Vergleich zu einem Iris-Scan und ist – da kontaktlos – hygienischer als ein Fingerprint. Als Systemintegrator achten wir auch darauf, dass die biometrische Zutrittskontrolle problemlos in die Sicherheitsarchitektur eingebunden werden kann, z. B. durch gängige Hardware-Schnittstellen.

Ein weiterer Vorteil ist die DSGVO-konforme Sicherung der biometrischen Daten. Beim von der Firma Icognize angemeldeten Split-Template-Verfahren werden die Daten in zwei oder mehr Datenanteile gespalten. Die einzelnen Teile werden anschließend auf unterschiedlichen Medien und an verschiedenen Orten gespeichert, wie etwa RFID-Karte und Server innerhalb der IT-Infrastruktur. Durch die Splittung sind die erfassten biometrischen Daten nicht mehr personenbezogen im Sinne der DSGVO, da keine Rückschlüsse zum eigentlichen Datensatz möglich sind. Das Split-Verfahren verhindert zudem, dass bei Cyberattacken komplette Datensätze gestohlen werden können. Dieses Verfahren ist im Übrigen nicht nur auf die Biometrie beschränkt.

Viele Betreiber großer Rechenzentren vermieten als Colocation-Anbieter Flächen an Unternehmen und Institutionen für Server und Racks. Bei allen hohen Sicherheitsanforderungen, die erforderlich sind – ist das dreistufige Authentifizierungsverfahren nicht zu komplex?

Carsten König: Zunächst ist festzuhalten, dass wir nur an zentralen Zutrittspunkten auf das dreistufige System setzen. Hat man diese passiert, bewähren sich Multifunktionsterminals – beispielsweise von der Firma Autec – für Zutrittskontrolle und Zeiterfassung in Verbindung mit RFID und der Eingabe des Pin-Codes für die Authentifizierung. Neben dem Zugang wird auch das Verlassen des Rechenzentrums erfasst, um bei einer nicht regelkonformen Abmeldung

Durch das Split-Template-Verfahren sind biometrische Daten, wie beim Handvenenscan nicht mehr personenbezogen.

den erneuten späteren Zutritt verweigern zu können.

Eine weitere Reduzierung der Komplexität ist allein durch das in der Regel vielschichtige Berechtigungskonzept nicht möglich. Denn neben einer Whitelist für Berechtigte mit einem permanenten Zugang werden auch temporäre Zugänge vergeben – sowohl personell als auch örtlich.

Rechenzentren stehen oft „auf der grünen Wiese" ohne personelle Besetzung. Birgt das nicht Gefahren?

Carsten König: Wir kombinieren das Zugangskontrollsystem mit Überwachungskameras und einer Einbruchmeldeanlage. Im Außenbereich kommt noch eine Perimetersicherung hinzu, bei der Wärmebildkameras und Radartechnologie verdächtige Aktivitäten erfassen. Die Gewerke werden dabei über Schnittstellen an ein übergeordnetes Managementsystem angebunden. Durch die Vernetzung können die Systeme in Echtzeit überwacht sowie Meldungen aus unterschiedlichen Bereichen erfasst und analysiert werden, um schnell auf Bedrohungen und ungewöhnliche Ereignisse reagieren zu können. So lassen sich beispielsweise Türen automatisch verriegeln und Stromquellen abschalten. Und nicht zuletzt achten wir darauf, nur „sichere" Produkte einzusetzen, heißt: Alle Komponenten folgen dem Secure-by-Design-Prinzipien, wie automatisierte Firmware-Upgrades, verschlüsselte Kommunikation, IP-Adressen-Filterung und vieles weitere mehr.

Wie lassen sich Projekte dieser Größenordnung stemmen?

Carsten König: So viel Expertise wir auch als Systemintegrator haben und Erfahrung in der Sicherung von Anlagen der Kritischen Infrastruktur mitbringen – dieser mehrschichtige Sicherheitsansatz lässt sich nur mit einer intensiven, vertrauensvollen Zusammenarbeit mit dem Kunden sowie Partnerunternehmen bewältigen. Das ist umso wichtiger, da IT, IoT und Physical Security in ein ganzheitliches Sicherheitskonzept münden. GIT

TAS – Telefonbau Arthur Schwabe GmbH & Co. KG
www.tas.de