

KRITIS:

Sicherheit & Resilienz in der Daten- & Informationstechnik



KRITIS in der Daten- & Informationstechnik – Sicherheit & Resilienz für digitale Lebensadern

Rechenzentren, Cloud-Infrastrukturen und Netzwerkknoten zählen zu den zentralen kritischen Infrastrukturen. Mit NIS2 und dem KRITIS-Dachgesetz steigen die Anforderungen an physische Sicherheit, Verfügbarkeit und Nachvollziehbarkeit deutlich. 24/7-Betrieb, externe Dienstleister, mandantenfähige Umgebungen und hochsensible IT-Assets erfordern ein durchgängiges Zutritts- und Türkonzept, das Schutz, Compliance und Betriebsabläufe gleichermaßen berücksichtigt.

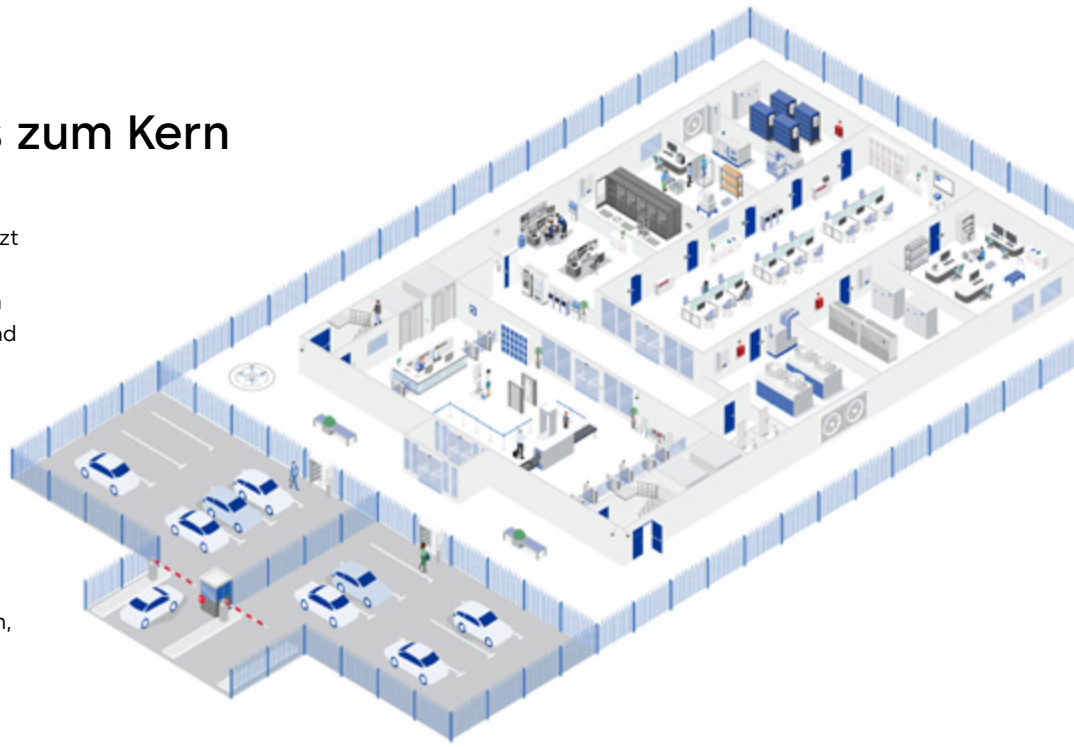
Gleichzeitig müssen temporäre Zugänge steuerbar, Zugriffe bis auf Rack-Ebene dokumentierbar und kritische Zonen vor unbefugtem Zutritt geschützt werden. Moderne KRITIS-Strategien verbinden daher mechanische Sicherheit, elektronische Zutrittskontrolle, Vereinzelungstechnik und ausfallsichere Türsysteme zu einem integrierten Gesamtsystem.

Als erfahrener Partner begleitet dormakaba Betreiber von der Risikoanalyse über das Resilienz-Assessment bis zur Umsetzung wartbarer, auditfähiger Zutritts- und Türlösungen – für einen sicheren, regelkonformen und jederzeit handlungsfähigen Rechenzentrumsbetrieb.

Vom Perimeter bis zum Kern

Unser strukturiertes Assessment übersetzt regulatorische Anforderungen aus KRITIS und NIS2 in konkrete Maßnahmen für den physischen Schutz von Rechenzentren und IT-Standorten. Betreiber erhalten eine transparente Einordnung von Risiken, Schwachstellen und Prioritäten – von Zonierung über rollenbasierte Berechtigungen bis zur Ausfallsicherheit der Zutrittslösungen.

So entsteht eine belastbare Entscheidungsgrundlage für Investitionen, Wartung und organisatorische Prozesse, die Sicherheit, Compliance und unterbrechungsfreien Betrieb miteinander verbinden.



Gefahrenvektoren in der Daten- & Informationstechnik: Risiken verstehen – kritische Bereiche gezielt schützen



Kontrollverlust am äußeren Sicherheitsperimeter

Gefahrenvektor:

Rechenzentren sind häufig exponiert. Zufahrten, Nebeneingänge, Notausgänge und Lieferzonen stellen kritische Einstiegspunkte dar.

Typische Risiken:

- Unbefugtes Betreten über Liefer- oder Nebeneingänge
- Social Engineering durch Auftreten als Dienstleister
- Manipulation von Not- und Seitentüren
- Fehlende Identitäts- und Besucherprüfung



Identitätsmissbrauch beim Gebäudezutritt

Gefahrenvektor:

Haupteingänge bündeln Personal, Besucher und Dienstleister. Unzureichende Konzepte begünstigen Tailgating und Badge-Missbrauch.

Typische Risiken:

- Tailgating
- Weitergabe oder Kopie von Zutrittsmedien
- Keine verlässliche Zuordnung von Identität zu Zutritt
- Lückenhafte Nachvollziehbarkeit für Audits



Unkontrollierte Bewegung innerhalb kritischer Zonen

Gefahrenvektor:

Nach dem Zutritt dürfen Personen sich nicht frei zwischen Büro-, Technik- und White-Space bewegen. Fehlende Zonierung schafft interne Lücken.

Typische Risiken:

- Überschreitung genehmigter Zonen
- Zu weit gefasste Rechte (Insider Risk)
- Unzureichende Trennung von Mandanten
- Manipulation von Neben- und Fluchtwegen



Direkter Zugriff auf geschäftskritische IT-Systeme

Gefahrenvektor:

Auch nach Raumzutritt bleibt der physische Zugriff auf Server, Storage und Netzwerke hochkritisch. Mechanische Schlüssel erfüllen die Sicherheitsanforderungen nicht.

Typische Risiken:

- Diebstahl von Hardware und Datenträgern
- Sabotage an Server- und Netzwerktechnik
- Keine Protokollierung auf Rack-Ebene
- Missbrauch durch Schlüssel- oder Rechtweitergabe

KRITIS-konforme Sicherheit:

mit integrierten Lösungen von dormakaba

dormakaba verbindet Zutrittsautomation, elektronische Zutrittskontrolle, Türtechnik und Serviceleistungen zu einem ganzheitlichen System – abgestimmt auf die besonderen Anforderungen von Rechenzentren und digitaler Infrastruktur. So werden Perimeter, White-Space, Technik- und Netzwerkbereiche zuverlässig geschützt, Zugriffe bis auf Cage- und Rack-Ebene nachvollziehbar gesteuert und Betriebsabläufe stabilisiert. Regulatorische Vorgaben aus KRITIS und NIS2 lassen sich praxisnah, auditfähig und mit hoher Verfügbarkeit umsetzen.



Automatische Türsysteme

Kontrollierter Durchfluss 24/7

Automatische Türsysteme steuern Personenströme an Haupteingängen, Sicherheitsübergängen und Lieferzonen zuverlässig im Dauerbetrieb. Definierte Zutrittslogiken für Mitarbeitende, Kunden und Servicepersonal ermöglichen einen sicheren Zugang auch außerhalb regulärer Zeiten.

Schleusen- und Vereinzelungssysteme reduzieren Tailgating beim Übergang von öffentlichen in geschützte Bereiche wie White-Space oder Technikzonen. In Notfall- oder Störungsszenarien sorgen vordefinierte Betriebsmodi für Evakuierungssicherheit und geregelte Zutrittsprozesse gemäß KRITIS- und NIS2-Anforderungen.

01

Kontrollierter Haupteingang 24/7

Automatische Türsysteme mit definierten Zutrittslogiken für Mitarbeiter, Servicepersonal und Besucher sichern den Betrieb rund um die Uhr

02

Schleusen & Vereinzelung

Personenschleusen und Sicherheitstüren verhindern Tailgating beim Übergang von öffentlichen zu hochkritischen Bereichen

03

Notfall- & Betriebsmodi

Definiertes Türverhalten bei Brand, Stromausfall oder Sicherheitsvorfällen erhält Evakuierungs- und Betriebsfähigkeit



Zutrittskontrollsysteme

Zonierung und Nachweisbarkeit

Elektronische Schließsysteme verbinden Türen, Cages und Serverschränke in einer einheitlichen Berechtigungslogik. Zugriffe werden rollen- und zeitbasiert gesteuert, sodass nur autorisierte Personen Zutritt zu kritischen IT-Assets erhalten.

Durchgängige Protokollierung schafft Transparenz bis auf die letzte Zugriffsebene und unterstützt Audits sowie interne Revision. Mechanische Widerstandsfähigkeit in Kombination mit elektronischer Kontrolle gewährleistet Schutz auch bei System- oder Stromausfall.

01

Zutrittskonzept mit Zonierung

Abgrenzung von Büro, Technik, White-Space und Netzwerkknoten nach Kritikalität

02

Rollenbasierte Berechtigungen

Zeitlich und ortsbezogene Berechtigungen für Mitarbeitende und Dienstleister

03

Mandantenfähigkeit

Trennung von Kundenumgebungen in Colocation-Szenarien mit separaten Rechten

03

Audit- & Protokollierungsfunktionen

Lückenlose Dokumentation aller Zutrittsereignisse



Türtechnik

Sicherheit auch im Ausnahmefall

Türtechnikkomponenten bilden die physische Basis kritischer Infrastrukturen und schützen Zugänge auch ohne Stromversorgung. Hochwertige Beschläge, Türschließer und Fluchtwegsysteme sichern Brandabschnitte, Technikräume und Fluchtwege.

Elektronische und mechanische Lösungen ergänzen sich zu einem durchgängigen Sicherheitskonzept. Intelligente Türsteuerungen, vernetzte Beschläge und integrierte Schließsysteme gewährleisten auch im Störfall definierte Betriebszustände. So bleibt der Schutz in Black-Out- oder Krisenszenarien ebenso erhalten wie im regulären 24/7-Betrieb.

01

Funktionssichere Türen

Zuverlässiges Schließen für Sabotage- und Manipulationsschutz

02

Rack-Absicherung

Elektronische Schlösser bis auf Cage- und Rack-Ebene mit einheitlicher Berechtigungslogik

03

Mechanische Absicherung im Krisenfall

Definierte mechanische Schließfunktionen als Fallback bei System- oder Stromausfall

04

Lösungen für Outdoor- & dezentrale Standorte

Wetter-, Vandalismus- und manipulationssichere Tür- & Schlosslösungen



Service

Resilienz über den gesamten Lebenszyklus

Mit Resilienz-Assessments, Lifecycle-Management und regelmäßiger Wartung unterstützt der dormakaba Service den dauerhaften reibungslosen Betrieb.

Preventive Maintenance reduziert Ausfälle an hoch frequentierten Türen, Updates halten Systeme aktuell.

Ein schneller Vor-Ort-Service mit definierten Reaktionszeiten sichert die Wiederherstellung im Störfall.

01

Resilienz-Assessment

Priorisierung kritischer Zutrittspunkte für Prävention, Reaktion und Wiederanlauf

02

Lifecycle-Management

Regelmäßige Rezertifizierung, Wartung und Instandhaltung von Zutrittssystemen, um Sicherheit zu gewährleisten

03

Preventive Maintenance

Wartungspläne für hoch frequentierte Türen (Haupteingänge, Bürobereiche), um Ausfälle zu verhindern

04

Schnelle Wiederherstellung nach Störungen

Vor-Ort-Service mit definierten Reaktionszeiten und Originalersatzteilen

KRITIS sicher umsetzen – wir begleiten Sie.

Unsere Experten unterstützen Sie von der Analyse bis zum laufenden Betrieb.

Jetzt Beratung anfragen: pre-sales.de@dormakaba.com