

KRITIS: Sicherheit & Resilienz im Finanzwesen



KRITIS im Finanzwesen – Sicherheit, die Vertrauen und Zahlungsfähigkeit schützt

Banken und Finanzinstitute zählen zu den zentralen kritischen Infrastrukturen und stehen durch NIS2 und KRITIS vor neuen Anforderungen an Sicherheit und Resilienz.

Offene Filialen, 24/7-SB-Zonen, hohe Kundenfrequenz und sensible Bereiche wie Cash-Processing, Tresor oder IT erfordern ein durchgängiges Zutritts- und Türkonzept, das Schutz, Betriebsstabilität und regulatorische Vorgaben gleichermaßen berücksichtigt.

Ebenso müssen externe Dienstleister steuerbar, temporäre Zugänge begrenzt und geschäftskritische Prozesse vor unbefugtem Zutritt geschützt werden.

Moderne KRITIS-Strategien verbinden daher mechanische Sicherheit, elektronische Zutrittskontrolle, automatische Lösungen und Fluchtwegtechnik zu einem integrierten Gesamtsystem.

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

Vom Perimeter bis zum Kern

Unser strukturiertes Assessment übersetzt regulatorische Anforderungen aus KRITIS und NIS2 in konkrete Maßnahmen für den physischen Schutz von Banken und Finanzinstituten.

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 reibungslosen Geschäftsbetrieb miteinander verbinden.



Gefahrenvektoren im Finanzwesen:

Risiken verstehen – kritische Bereiche gezielt schützen

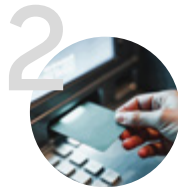


Unkontrollierte Öffentlichkeit & Personenströme

Gefahrenvektor:
Öffentlich zugängliche Filialen, SB-Zonen und Empfangsbereiche mit hoher Kundenfluktuation ermöglichen unbefugte Bewegungen in interne Gebäudeteile.

Typische Risiken:

- Unbefugtes Eindringen in Backoffice- und Personalbereiche
- Tailgating an Übergängen
- Überfall- und Zwangslagen
- Sabotage über Nebeneingänge



Unzureichender Schutz von Bargeld & Cash-Infrastruktur

Gefahrenvektor:
Bargeldbereiche, Tresore, Cash-Processing und Übergaben an Werttransporte sind besonders attraktive Ziele für Diebstahl und Manipulation.

Typische Risiken:

- Diebstahl & Manipulation
- Insider-Risiken
- Unkontrollierte Servicezugänge
- Fehlende Nachvollziehbarkeit



Physischer Zugriff auf IT- & Zahlungsinfrastruktur

Gefahrenvektor:
Serverräume, Netzwerk- und Payments-Operations sind geschäftskritisch für den Zahlungsverkehr und die Verfügbarkeit.

Typische Risiken:

- Sabotage oder Manipulation an IT-Systemen
- Unberechtigte Wartung durch Externe
- Diebstahl von Datenträgern und Komponenten
- Fehlende Trennung zu Büroflächen



Unkontrollierte Dienstleisterzugänge & Social Engineering

Gefahrenvektor:
Externe mit legitimem Anlass erhalten durch Social Engineering weitreichendere Zugänge als vorgesehen.

Typische Risiken:

- Nutzung von Seitentüren ohne Kontrolle
- Schlüsselweitergabe und Ausweismissbrauch
- Fehlende Rezertifizierung von Rechten
- Bewegungen außerhalb des Auftragsbereichs

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 kritischer Finanzinfrastruktur. So werden Filialen, SB-Zonen, Cash- und Tresorbereiche sowie IT- und Zahlungsprozesse zuverlässig geschützt, Betriebsabläufe stabilisiert und regulatorische Vorgaben aus KRITIS und NIS2 praxisnah umgesetzt.



Automatische Türsysteme

Kontrollierter Durchfluss 24/7

Automatische Türsysteme steuern Personenströme zuverlässig an Haupteingängen, in Filialen und an sensiblen Übergängen zwischen Kunden- und Personalbereichen. Betriebsmodi wie Tag/Nacht oder Intercom-Anmeldung ermöglichen einen kontrollierten Zugang auch außerhalb regulärer Öffnungszeiten.

Getrennte Wege für Kunden, Mitarbeitende und Dienstleister reduzieren unkontrollierte Zutritte, während definierte Zutrittslogiken in SB-Zonen und ATM-Lobbys die Verfügbarkeit der Services auch im 24/7-Betrieb sicherstellen.

01

Kontrollierter Haupteingang 24/7

Automatische Türen mit Tag-/Nachtmodus, Anbindung an Empfang oder Intercom sowie zentrale Steuerung der Zutrittslogik

02

Kunden- & Besucherlenkung

Getrennte Wegeführung für Kunden, Personal und Dienstleister – Reduzierung von Tailgating und unkontrollierten Übergängen ins Backoffice

03

SB-Zonen & ATM-Lobbys

Zutritt über Bankkarte mit Zeitprofilen und Betriebsmodi; Schutz vor Vandalismus und Stabilisierung der SB-Verfügbarkeit



Zutrittskontrollsysteme

Zonierung und Nachweisbarkeit

Elektronische Zutrittskontrollsysteme trennen Bereiche nach Schutzstufen – von öffentlichen Zonen über Backoffice bis zu hochkritischen Bereichen wie Tresor, Cash-Processing oder IT. Rollen- und zeitbasierte Berechtigungen stellen sicher, dass Mitarbeitende und Dienstleister nur notwendige Zugänge erhalten.

Temporäre Rechte mit Ablaufdatum, Zwei-Faktor-Optionen und Dual-Control erhöhen das Schutzniveau in sensiblen Zonen. Alle Zutritte werden revisionssicher dokumentiert und gewährleisten die Nachweisbarkeit für Audits sowie KRITIS- und NIS2-Anforderungen.

01

Zutrittskonzept mit Zonierung

Zonierung nach Schutzstufen von öffentlich bis hochkritisch mit klaren Übergängen für Filiale, Backoffice, Operations, Cash und IT

02

Schutz von Bargeld- & Tresorbereichen

Rollen- und zeitbasierter Zutritt mit Protokollierung, optional Zwei-Faktor/Dual Control

03

Schutz kritischer IT- & Payments-Zonen

Zutritt nur für autorisierte Rollen, temporäre Dienstleisterrechte und restriktive Regeln außerhalb der Betriebszeiten



Türtechnik

Sicherheit auch im Ausnahmefall

Türtechnik in Banken und Finanzinstituten muss auch bei hoher Frequentierung zuverlässig funktionieren und Manipulationsversuchen standhalten. Robuste Schließlösungen in Cash-, IT- und Operations-Bereichen sichern kritische Prozesse ohne Beeinträchtigung des Betriebs.

Für Krisen- und Black-Out-Szenarien stehen mechanische Fallback-Funktionen bereit, sodass kontrollierte Zugänge auch bei System- oder Netzausfall erhalten bleiben. Geregelte Flucht- und Rettungsweglogiken gewährleisten dabei die Einhaltung der Sicherheitsanforderungen.

01

Funktionssichere Türen

Zuverlässiges Schließen in Cash-, IT- und Operations-Bereichen für hohe Verfügbarkeit und Manipulationsschutz

02

Mechanische Absicherung im Krisenfall

Definierte Fallback-Funktionen bei System- oder Netzausfall für kontrollierte Zugänge

03

Flucht- & Rettungswegtechnik

Geregelte Türlogiken mit definierter Freigabe im Notfall



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 hochfrequentierte Türen (SB-Foyers, 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