CloudCommand

Cyber Security

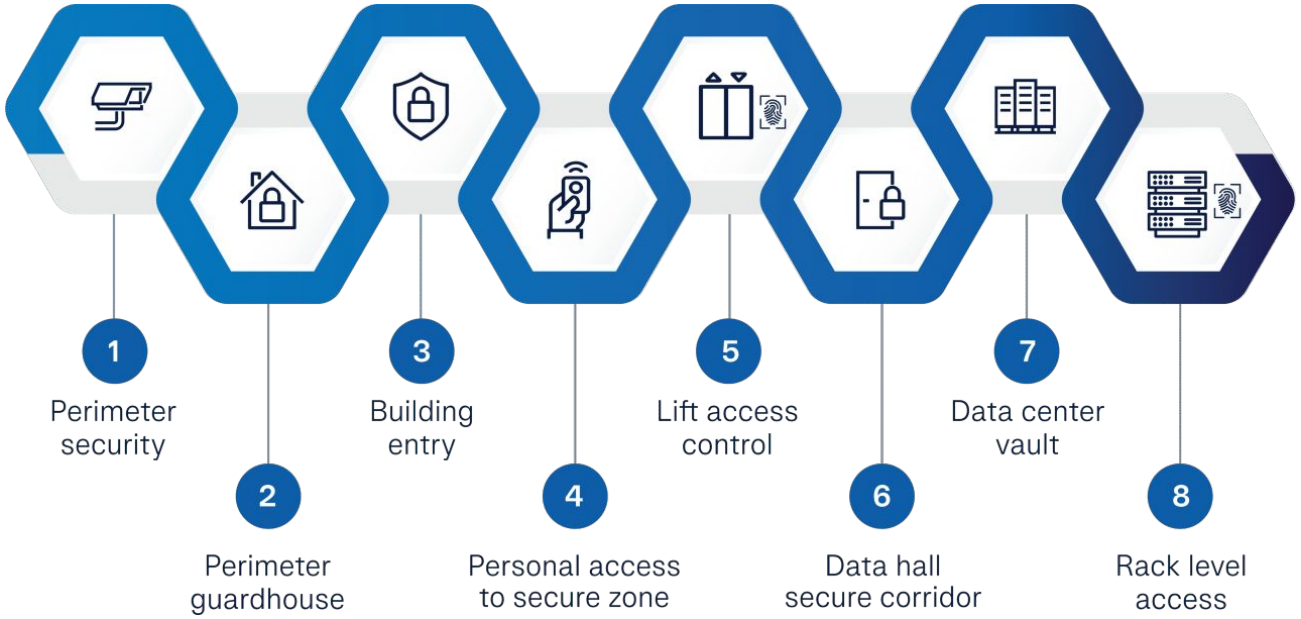
CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Physische Sicherheits-risiken identifizieren

Welche potenziellen Risiken existieren?



Fallbeispiel: Verbesserung der Rechenzentrums-Sicherheit

- Ein Unternehmen betreibt ein hochmodernes Rechenzentrum, das sensible Daten von Kunden und Geschäftspartnern speichert. Aufgrund des ständig wachsenden Datenvolumens und der zunehmenden Bedrohungen im Cyberspace hat das Unternehmen beschlossen, seine physische Sicherheitsinfrastruktur zu überprüfen und zu verbessern.

Fallbeispiel: Verbesserung der Rechenzentrums-Sicherheit

Fragen zum Identifizierte physische Sicherheitsrisiken:

- **Perimetersicherheit:**
  - Ist die Perimetersicherheit durch die Implementierung klarer Zugangskontrollen und einen sicheren Zaun gewährleistet?
- **Wachstation:**
  - Haben die Sicherheitskräfte alle erforderlichen Schulungen absolviert?
- **Gebäudeeingang:**
  - Ist die Zugangskontrolltechnologie auf dem neuesten Stand?
- **Persönlicher Zugang zu gesicherten Zonen:**
  - Haben unberechtigte Mitarbeiter Zugang zu sensiblen Bereichen?

Fallbeispiel: Verbesserung der Rechenzentrums-Sicherheit

- **Aufzugszugangskontrolle:**
  - Ist der Zugang zu den Aufzügen gesichert?
- **Sicherheitskorridor zum Rechenzentrum:**
  - Ist der Sicherheitskorridor überwacht und alarmgesichert?
- **Rechenzentrum:**
  - Sind alle Brandschutz- und Sicherheitsvorkehrungen erfüllt?
- **Rackebene:**
  - Gibt es eine individuelle Zugangskontrolle?

Fallbeispiel: Verbesserung der Rechenzentrums-Sicherheit

Ergebnisse:

- **Perimetersicherheit:**
  - Der Zaun um das Rechenzentrum weist einige Lücken und beschädigte Abschnitte auf.
- **Wachstation:**
  - Das Sicherheitspersonal hat begrenzte Schulungen in Bezug auf Identifizierung von Bedrohungen und effektive Kommunikation.
- **Gebäudeeingang:**
  - Die Zugangskontrollen basieren auf veralteten Technologien und müssen aktualisiert werden.

Fallbeispiel: Verbesserung der Rechenzentrums-Sicherheit

- **Persönlicher Zugang zu gesicherten Zonen:**
  - Mitarbeiter haben Zugang zu sensiblen Bereichen ohne klare Überprüfungen oder Authentifizierungsprotokolle.
- **Aufzugszugangskontrolle:**
  - Der Zugang zu den Aufzügen, die zu den oberen Etagen führen, ist nicht angemessen gesichert.
- **Sicherheitskorridor zum Rechenzentrum:**
  - Der Sicherheitskorridor zum Rechenzentrum ist nicht videoüberwacht und bietet begrenzte Kontrollpunkte.

Fallbeispiel: Verbesserung der Rechenzentrums-Sicherheit

- **Rechenzentrum:**
  - Der Zugang zum eigentlichen Rechenzentrum ist nur durch eine einfache Tür gesichert.
  - Klimatisierung und Brandschutzvorkehrungen müssen überprüft und aktualisiert werden.
- **Rackebene:**
  - Auf der Rackebene gibt es keine individuellen Zugangskontrollen für IT-Techniker.

PHYSISCHE SICHERHEITS-RISIKEN IDENTIFIZIEREN

Maßnahmen

- Erneuerung des Zauns um das Gelände und Implementierung von Zugangskontrollpunkten
- Verbesserung der Schulungen für das Sicherheitspersonal
- Upgrade der Zugangskontrollen am Gebäudeeingang und Implementierung moderner Authentifizierungstechnologien
- Stärkung der Aufzugzugangskontrolle und Einführung von Überwachungsmechanismen
- Installation von Überwachungskameras und Alarmsystemen im Sicherheitskorridor zum Rechenzentrum
- Verbesserung der Sicherheit des Rechenzentrums durch fortschrittliche Zugangskontrollen, Überwachung und Brandschutz
- Implementierung individueller Zugangskontrollen auf der Rackebene und Überprüfung der physischen Anordnung der Server

CloudCommand GmbH chr.schumacher@gmx.tm

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm