CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Best Practices

NIST Framework for Improving Critical Infrastructure Cybersecurity (USA):

NIST (National Institute of Standards and Technology) definiert ein Framework, das entwickelt wurde, um kritische Infrastrukturen in der Cybersecurity zu verbessern.

NIST Framework for Improving Critical Infrastructure Cybersecurity (USA):

Identifizieren (Identify)

- Identifizierung kritischer Ressourcen und Risikobewertung.
- Schwachstellenanalyse und Bestimmung von Sicherheitsanforderungen.
- Schaffung einer Grundlage für die Entwicklung von Sicherheitsmaßnahmen.

NIST Framework for Improving Critical Infrastructure Cybersecurity (USA):

Schützen (Protect)

- Implementierung von Sicherheitskontrollen und -prozessen.
- Entwurf und Umsetzung von Sicherheitsrichtlinien.
- Schulung von Mitarbeitern für Sicherheitsbewusstsein.

NIST Framework for Improving Critical Infrastructure Cybersecurity (USA):

Erkennen (Detect)

- Implementierung von Überwachungssystemen für die Früherkennung von Sicherheitsvorfällen.
- Nutzung von Intrusion Detection Systems (IDS) und Security Information and Event Management (SIEM).
- Erkennung von Anomalien und ungewöhnlichem Verhalten.

NIST Framework for Improving Critical Infrastructure Cybersecurity (USA):

Reagieren (Respond)

- Entwicklung von Reaktionsplänen für den Umgang mit Sicherheitsvorfällen.
- Einrichtung von Incident-Response-Teams.
- Eindämmung von Angriffen und Wiederherstellung der Integrität.

NIST Framework for Improving Critical Infrastructure Cybersecurity (USA):

Wiederherstellen (Recover)

- Entwicklung von Plänen für die schnelle Wiederherstellung nach einem Vorfall.
- Implementierung von Maßnahmen zur Minimierung von Ausfallzeiten.
- Bewertung und Anpassung von Wiederherstellungsplänen.

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm