CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Internationale Gesetze und Verordnungen

Datenschutz-Grundverordnung (DSGVO)

DSGVO ist eine EU-Verordnung aus 27. April 2016.

- Einheitlichen und harmonisierten Rechtsrahmen für den Datenschutz in der gesamten EU
- Allgemeine Regeln für die Verarbeitung personenbezogener Daten
- Im Vergleich zu BDSG legt die DSGVO höhere Geldstrafen (bis zu 20 Milionen Euro)

Datenschutz-Grundverordnung (DSGVO)

Artikel 32 Absatz 1 DSGVO

- "Der Verantwortliche und der Auftragsverarbeiter treffen geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten..."
- **Physische Zugangskontrolle** ist eine wesentliche Maßnahme zur Erfüllung der Anforderungen von Artikel 32 Absatz 1 der Datenschutz-Grundverordnung (DSGVO)

Datenschutz-Grundverordnung (DSGVO)

Artikel 5 Absatz 1 Buchstabe f DSGVO

- “Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine **angemessene Sicherheit der personenbezogenen Daten gewährleistet…**”
- "...einschließlich **Schutz vor unbefugter** oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem **Verlust**, unbeabsichtigter **Zerstörung** oder unbeabsichtigter **Schädigung** durch geeignete technische und organisatorische Maßnahmen (‚Integrität und Vertraulichkeit‘)." (Artikel 5 Absatz 1 Buchstabe f DSGVO).

Datenschutz-Grundverordnung (DSGVO)

Artikel 5 Absatz 1 Buchstabe f DSGVO

- Beispiele zu Physischer Schutz
  - Zugangskontrolle als Schutz vor Unbefugten
  - Biometrie als physischer Schutz personenbezogener Daten
  - Überwachung

Datenschutz-Grundverordnung (DSGVO)

Artikel 33 Absatz 1 DSGVO

- "Bei Verletzungen des Schutzes personenbezogener Daten benachrichtigt der Verantwortliche unverzüglich und möglichst binnen 72 Stunden nach Erlangen davon die Aufsichtsbehörde..."
- "...sofern nicht der Verstoß voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt."
- **Maßnahmen** bei physischen Sicherheitsverletzungen
  - Unverzügliche Benachrichtigung bei physischen Vorfällen.
  - Schnelle Reaktion auf physische Sicherheitsverletzungen.
  - Betroffenenbenachrichtigung, es sei denn, geringes Risiko.

NIS-Richtlinie (Richtlinie (EU) 2016/1148)

Hintergrund:

- Die erste NIS-Richtlinie wurde 2016 (EU 2016/1148) erlassen
  - um ein hohes Sicherheitsniveau für Netz- und Informationssysteme in der EU zu gewährleisten.
  - Definition von NIS (Netz- und Informationssystemen) als Gerät oder Gruppe von Geräten, die automatische Verarbeitung digitaler Daten durchführen.
- Ziel: Eindämmung von Cyberbedrohungen für Unternehmen, die wesentliche Dienste in kritischen Sektoren erbringen.
- **Aktualisierung** auf NIS2 im Dezember 2022

NIS2-Richtlinie (Richtlinie (EU) 2022/2557)

Umsetzung:

- Umsetzung in den Mitgliedsstaaten erfolgte durch unterschiedliche nationale Gesetze (z. B. das deutsche IT-Sicherheitsgesetz).

Anforderungen an Betreiber von Netz- und Informationssystemen (NIS):

- Betroffene Unternehmen müssen angemessene
  - technische
  - operative
  - organisatorische
- Maßnahmen ergreifen, um Sicherheitsrisiken zu beherrschen

NIS2-Richtlinie (Richtlinie (EU) 2022/2557)

Einige der verbindlichen Mindestanforderungen der NIS2:

- Risikoanalyse und Sicherheitskonzepte
- Grundlegende Verfahren für Cyberhygiene
- Schwachstellenmanagement
- Authentifizierung
- Kommunikation
- Zugriffskontrolle und Anlagenmanagement

NIS2-Richtlinie (Richtlinie (EU) 2022/2557)

Betroffene Unternehmen:

- Mäßige Unternehmen (50–250 Beschäftigte, Umsatz 10–50 Mio. EUR oder Bilanzsumme bis zu 43 Mio. EUR).
- Große Unternehmen (über 250 Beschäftigte und mehr als 50 Mio. EUR Umsatz oder Bilanzsumme über 43 Mio. EUR).
- Öffentliche Verwaltung, digitale Infrastruktur und Anbieter kritischer Dienste, unabhängig von der Größe.

Europäische Norm EN 50132-7: CCTV-Systeme für den Überwachungssysteme

EN 50132-7 → CCTV-Systeme

- Standard für Closed-Circuit-Television (CCTV) oder Videoüberwachungssysteme

Europäische Norm EN 50132-7: CCTV-Systeme für den Überwachungssysteme

Zentralen Aspekte

- Systemdesign und Installation
- Datensicherheit und Integrität
- Überwachung und Aufzeichnung
- Funktionale Anforderungen

Europäische Norm EN 50132-7: CCTV-Systeme für den Überwachungssysteme

Systemdesign und Installation:

- Richtlinien für das physische Design der CCTV-Infrastruktur.
- Anforderungen an die Installation, Wartung und Betriebssicherheit.
- Vorgaben für eine effiziente Integration in Sicherheitsumgebungen.

Datensicherheit und Integrität:

- Maßnahmen zur Sicherung der aufgezeichneten Daten vor unbefugtem Zugriff.
- Schutzmechanismen, um die Integrität der Daten sicherzustellen.
- Datenschutzaspekte im Hinblick auf gesetzliche Anforderungen.

Europäische Norm EN 50132-7: CCTV-Systeme für den Überwachungssysteme

Überwachung und Aufzeichnung:

- Qualitätsanforderungen an die aufgezeichneten Bilder.
- Bestimmungen für die Aufbewahrung und Archivierung von Aufzeichnungen.
- Richtlinien zur Gewährleistung einer effektiven Überwachung.

Funktionale Anforderungen:

- Definition von Funktionen und Leistungsfähigkeit des CCTV-Systems.
- Anforderungen an die Benutzerfreundlichkeit und Bedienbarkeit.
- Vorgaben zur Integration mit anderen Sicherheitsinfrastrukturen.

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm