BSKI

BUND DEUTSCHER MUSEUMS BUND

VORTRAG

NIS2 & KRITIS-Dachgesetz – Herausforderungen und Chancen für Museen in der digitalen und physischen Sicherheit

Arbeitskreis Gebäudemanagement & Sicherheit
12.Februar 2025

AGENDA

1 VORSTELLUNG

2 GESETZLICHE RAHMENBEDINGUNGEN

3 ANWENDUNGS-BEREICH

4 DAS BESTE AUS BEIDEN WELTEN

5 BEST PRACTICE

AGENDA

1 VORSTELLUNG

2 GESETZLICHE RAHMENBEDINGUNGEN

3 ANWENDUNGS-BEREICH

4 DAS BESTE AUS BEIDEN WELTEN

5 BEST PRACTICE

Holger Berens berät seit mehr als 35 Jahren internationale Unternehmen und kritische Infrastrukturen in allen Bereichen des Compliance- und Sicherheitsmanagements. Er ist **Managing Partner der Concepture Gruppe** GmbH und verantwortlich für den Bereich Informationssicherheit und BCM. Er ist **Vorstandsvorsitzender des Bundesverbandes zum Schutz Kritischer Infrastrukturen (BSKI)**. Darüber hinaus war er bis zur Emeritierung Leiter des Studiengangs Compliance und Unternehmenssicherheit (LL. M.) an der Rheinischen Fachhochschule (RFH) in Köln und Leiter des Kompetenzzentrums für Internationale Sicherheit (KIS) an der RFH.

Holger Berens ist Mitglied der Expertengruppe von DIGITAL SME, einem Small Business Standards-Projekt mit Sitz in Brüssel, einer europäischen NGO, die von der Europäischen Kommission und den EFTA-Mitgliedstaaten im Rahmen von ISO 27001 mitfinanziert wird, um ISO 27001 ff. für KMU in der EU umzusetzen.

BSKI

Bundesverband für den Schutz Kritischer Infrastrukturen e. V.

Satzungszweck

- Der Bundesverband für den Schutz Kritischer Infrastrukturen (BSKI) ist die zentrale Anlaufstelle für Entscheider aus Kritischen Infrastrukturen, um ganzheitliche Schutzkonzepte zu etablieren.
- Die Aufgabe des Bundesverbandes für den Schutz Kritischer Infrastrukturen ist es, Sicherheitsrisiken für kritische Infrastrukturen und deren Zulieferer frühzeitig zu er-kennen und durch gezielte Konzepte für Prävention, Reaktion und Postvention zu reduzieren. Dabei werden allerhöchste Schutzziele (technisch, organisatorisch, persönlich) für kritische Infrastrukturen verfolgt.

mehr Informationen unter:

AGENDA

1 VORSTELLUNG

2 GESETZLICHE RAHMENBEDINGUNGEN

3 ANWENDUNGS-BEREICH

4 DAS BESTE AUS BEIDEN WELTEN

5 BEST PRACTICE

Informationen zum Cyberangriff auf das Museum für Naturkunde Berlin

Pressemitteilung, 20.02.2024

Das Museum für Naturkunde Berlin ist Mitte Oktober Opfer eines gezielten Hackerangriffs geworden. Davon betroffen sind weite Teile unserer digitalen Infrastruktur.

Das Museum hat Anzeige erstattet, das Berliner Landeskriminalamt ermittelt zu dem Cyberangriff.

IT-Angriff auf das British Museum

News

27 Januar 2025 • 1 Minuten

Cyberangriffe

Update / Während Olympia in Paris Cyberangriffe auf Museen in Frankreich – Lösegeld gefordert

Schüsse auf das Schwule Museum

28. Februar 2023

Am Morgen des 24. Februar wurde durch Mitarbeiter*innen aus der Verwaltung festgestellt, dass sich ein Angriff auf das Schwule Museum in Berlin-Tiergarten ereignet hat. Zwei Fensterscheiben, der Leuchtschriftzug und ein Kunstwerk vor der Eingangstür wurden dabei beschädigt. Wann genau die Schüsse abgefeuert wurden, ist nicht bekannt. Es wird jedoch

Millionendiebstahl in Köln: Einbruch ins Museum für Ostasiatische Kunst | 01:45 Min. | Verfügbar bis 13.09.2025

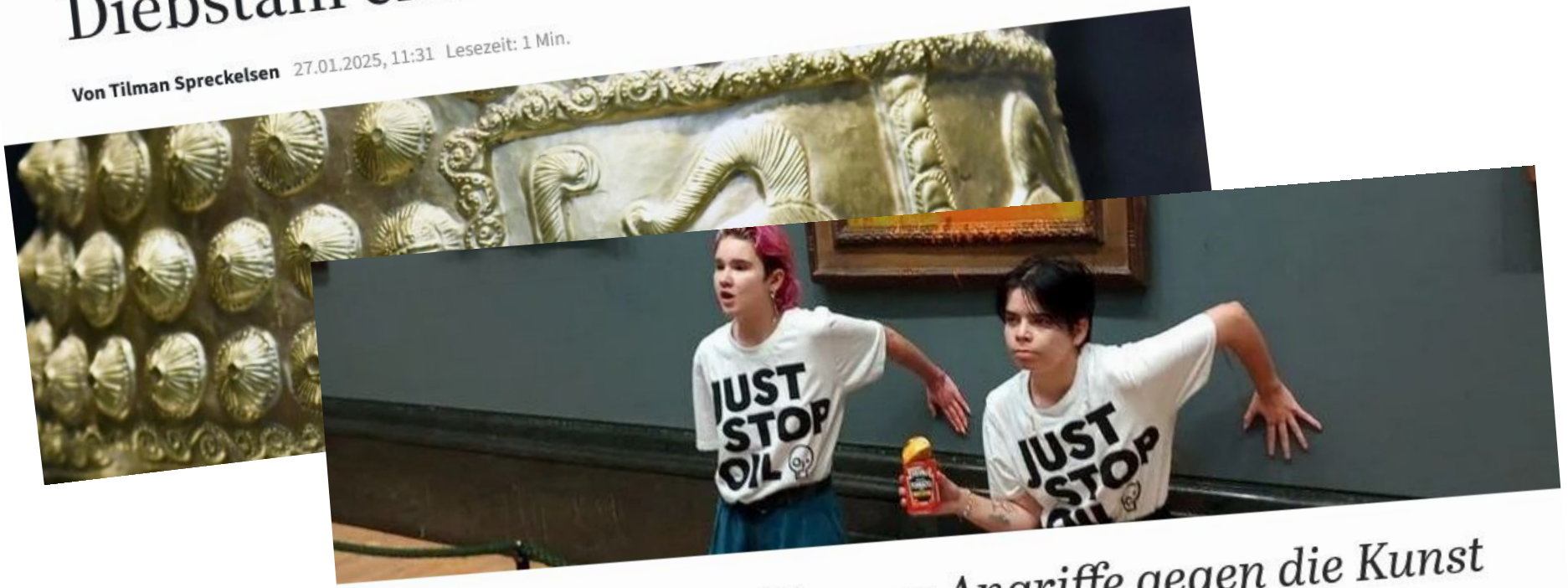
Hat Sicherheitspanne Millionendiebstahl in Kölner Museum ermöglicht?

Stand: 14.09.2023, 20:59 Uhr

Im Museum für Ostasiatische Kunst am Aachener Weiher gibt es offenbar seit länger Zeit ein Sicherheitsproblem. Nach dem Einbruch in das Museum am Mittwoch ist nun bekannt geworden, dass bereits zuvor zweimal Diebe am Museum zu Gange waren.

Diebstahl einer nationalen Ikone

Von Tilman Spreckelsen 27.01.2025, 11:31 Lesezeit: 1 Min.



Klimaprotest in Museen *Angriffe gegen die Kunst sind immer auch Angriffe gegen unsere Demokratie*

IT-Sicherheitsgesetz 1.0 Änderungsgesetz zum BSIG, EnWG, TKG, AtG und TMG: Verpflichtet Betreiber Kritischer Infrastrukturen IT angemessen abzusichern und diese Sicherheit überprüfen zu lassen.

Neue Rechtssetzung durch die EU

NIS 2 & RCE (Resilience of Critical Entities) (Umsetzung bis 17. Oktober 2024)

Neue Sektoren: z. B. öffentliche Verwaltung, Weltraum, ForschungseinrichtungenEinführung „size-cap rule"

DORA (Digital Operational Resilience Act) VO und RL (Anwendung / Umsetzung bis 17.1.2025)

BSI-Kritisverordnung
Definition Sektoren:
Schwellenwerte (Bedeutung des Versorgungsgrads)

Umsetzungsfristen

2015

2016

2017

Umsetzungsgesetz NIS 1
Neu: Regelungen für Anbieter Digitaler Dienste

2021

2022/23

IT-Sicherheitsgesetz 2.0
Einsatz von Systemen zur Angriffserkennung (§ 8a Abs. 1a)
Neuer Sektor – Siedlungsabfallentsorgung, Selbsterklärung zur IT-Sicherheit Unternehmen im besonderen öffentlichen Interesse (§ 8f)

2024

2025

2025/26

jetzt

Inkrafttreten
BISG 3.0
KRITIS-Dachgesetz

Der Cyber Resilience Act („CRA")

wurde am 20.11.2024 im Amtsblatt veröffentlicht und tritt am 09.12.2024 in Kraft.

GESETZLICHE RAHMENBEDINGUNGEN

Es gibt zwei sogenannte EU-Richtlinien, die in nationales Recht umgesetzt werden müssen:

EU-Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie)

Die CER-Richtlinie verpflichtet die Mitgliedstaaten, kritische Einrichtungen zu identifizieren und deren physische Widerstandsfähigkeit gegenüber Bedrohungen wie *Naturgefahren*, *Terroranschläge* oder *Sabotage* zu stärken.

EU-Richtlinie für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie)

Die NIS2-Richtlinie verpflichtet die Unternehmen, die in den Anwendungsbereich fallen, IT-, Cyber- und Informationssicherheit einzuführen.

Die Richtlinie ist für jeden Mitgliedstaat, an den sie gerichtet wird, hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel.

GESETZLICHE RAHMENBEDINGUNGEN

EU Richtlinien müssen in den Mitgliedstaaten in nationales Recht umgesetzt werden.

Die Umsetzungsfrist für NIS2 und CER war der 17.10.2024.

In Deutschland sind das für:

NIS2 › BSIG 3.0/ITSiG 3.0

CER › KRITIS-Dachgesetz

Die EU Kommission hat ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet, da diese Richtlinien nicht fristgerecht umgesetzt wurden.

GESETZLICHE RAHMENBEDINGUNGEN

Wegen der Neuwahlen im Februar ist nicht damit zu rechnen, dass noch im 1. Quartal 2025 die Umsetzungsgesetze in Kraft treten.

Ein genaues Datum kann nicht prognostiziert werden.

Die wesentlichen Anforderungen stehen mit den jeweiligen Entwürfen jedoch fest.

Das bedeutet, dass die Unternehmen, die in den Anwendungsbereich fallen, jetzt schon wissen, welche Maßnahmen implementiert werden müssen.

AGENDA

1 VORSTELLUNG

2 GESETZLICHE RAHMENBEDINGUNGEN

3 ANWENDUNGS-BEREICH

4 DAS BESTE AUS BEIDEN WELTEN

5 BEST PRACTICE

ANWENDUNGSBEREICH

BSKI

Sektoren ab 2025

Mit der NIS2-Umsetzung und dem KRITIS-Dachgesetz gibt es ab 2025 zwei Gruppen von Sektoren: Die *besonders wichtigen* und *wichtigen Einrichtungen* sind mittlere und große Unternehmen sowie die *Betreiber kritischer Anlagen* (KRITIS).

Quelle:
https://www.openkritis.de/it-sicherheitsgesetz/kritis-sektoren.html

ANWENDUNGSBEREICH

Das Problem ist, dass in den EU-Richtlinien und damit auch in der nationalen Umsetzung, Kultur nicht als kritische Infrastruktur definiert ist und die Richtlinien bzw. künftigen nationalen Gesetze nicht anwendbar sind.

Im Jahr 2009 hat das BMI die „Nationale Strategie zum Schutz Kritischer-Infrastrukturen“ veröffentlicht.

ANWENDUNGSBEREICH

Schaut man sich die hier vorgestellten Risiken an, wird klar, dass das Jahr 2009 die heutige hybride Situation nicht (mehr) abdeckt.

Museen sind Teil der Kritischen Infrastruktur!

BUND MUSEUMS DEUTSCHER MUSEUMS BUND

Naturereignisse	Technisches/menschliches Versagen	Terrorismus, Kriminalität, Krieg
Extremwetterereignisse, u. a. Stürme, Starkniederschläge, Temperaturstürze, Hochwasser, Hitzewellen, Dürren	Systemversagen, u. a. Unter- und Überkomplexität in der Planung, Hardware-, Softwarefehler	Terrorismus
Wald- und Heidebrände	Fahrlässigkeit	Sabotage
Seismische Ereignisse	Unfälle und Havarien	Sonstige Kriminalität
Epidemien und Pandemien bei Mensch, Tier und Pflanzen	Organisatorisches Versagen, u. a. Defizite im Risiko- und Krisenmanagement, unzureichende Koordination und Kooperation	Bürgerkriege und Kriege
Kosmische Ereignisse, u. a. kosmische Energiestürme, Meteoriten und Kometen		

Quelle: Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)

AGENDA

1 VORSTELLUNG

2 GESETZLICHE RAHMENBEDINGUNGEN

3 ANWENDUNGS-BEREICH

4 DAS BESTE AUS BEIDEN WELTEN

5 BEST PRACTICE

DAS BESTE AUS ALLEN WELTEN (KRITIS-DG)

Nach § 2 Kritis-Dachgesetz wird **Resilienz** wie folgt definiert:

„Resilienz“ [ist] die Fähigkeit eines Betreibers kritischer Anlagen, einen Vorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, einen solchen abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, einen Vorfall aufzufangen, zu bewältigen und sich von einem solchen Vorfall zu erholen;

DAS BESTE AUS ALLEN WELTEN (KRITIS-DG)

BSKI

Folgende **Mindestmaßnahmen** werden gefordert:

Vorsorge: Präventionsmaßnahmen gegen Vorfälle, Disaster und Klimawandel

Physische Sicherheit: Absicherung der ihrer Liegenschaften und Kritischen Infrastruktur mit physischen Schutzmaßnahmen, Perimeterüberwachung, Detektion und Zutrittskontrolle

Krisen: Risiko- und Krisenmanagement zur Bewältigung von Krisen, mit definierten Prozeduren, Protokollen und Alarmierung

DAS BESTE AUS ALLEN WELTEN (KRITIS-DG)

Folgende **Mindestmaßnahmen** werden gefordert:

Wiederherstellung: Business Continuity Management (BCM) und Maßnahmen zur Wiederherstellung nach Vorfällen — inkl. alternative Lieferketten

Personal: Sicherheitsmanagement und besondere personelle Sicherheit, Zutrittskontrolle, Sicherheitsüberprüfung, einschließlich externem Personal und Dienstleistern

Awareness: Beim Personal über die Resilienz-Maßnahmen

DAS BESTE AUS ALLEN WELTEN (NIS 2)

Grundsätzlich lassen sich die Anforderungen der NIS2 in drei Gruppen aufteilen:

- Hauptaufgaben
- Cyber Security Maßnahmen
- Physische Sicherheitsmaßnahmen

DAS BESTE AUS ALLEN WELTEN (NIS 2)

Hauptanforderungen:
Implementierung eines Risikomanagementsystems nach internationalem Standard (für NIS2UmsCG z.B. ISO 27001xx)

Implementierung/Nachweis der notwendigen Security Maßnahmen
(siehe Folgefolien)

Implementierung der Lieferketten-Sicherheit (Supply Chain Security)
(inkl. Regelungen zum Komponenteneinsatz)

Implementierung eines Störungsmeldungsmanagement/Incident Reporting
(innerbetrieblich und auch zu den zuständigen Behörden)

DAS BESTE AUS ALLEN WELTEN (NIS 2)

Hauptanforderungen:
Bei der Umsetzung der genannten Hauptanforderungen ist ein All-Gefahren-Ansatz (jedwede Ursache) zu berücksichtigen.

Die Mindestanforderungen müssen nach dem Stand der Technik und unter Berücksichtigung relevanter europäischer und internationaler Normen und technischer Spezifikationen umgesetzt werden.

DAS BESTE AUS ALLEN WELTEN (NIS 2)

BSKI

Cyber Security Maßnahmen

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme,
- Bewältigung von Sicherheitsvorfällen,
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement

DAS BESTE AUS ALLEN WELTEN (NIS 2)

BSKI

Cyber Security Maßnahmen

- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit

DAS BESTE AUS ALLEN WELTEN (NIS 2)

BSKI

Cyber Security Maßnahmen

- Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit,
- Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen

DAS BESTE AUS ALLEN WELTEN (NIS 2)

BSKI

Cyber Security Maßnahmen

- Verwendung von Lösungen zur MultiFaktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

DAS BESTE AUS ALLEN WELTEN (NIS 2)

Physische Sicherheitsmaßnahmen, um…

- … um das Auftreten von Vorfällen zu verhindern (Notallvorsorge, Anpassungen an den Klimawandel)
- … um angemessenen physischen Schutz ihrer Räumlichkeiten und kritischen Infrastrukturen zu gewährleisten (Objektschutz (u.a. Zäune/Sperren), Umgebungsüberwachung, Detektionsgeräte, Zutrittskontrollen)
- … um auf Vorfälle zu reagieren, abzuwehren oder Folgen zu begrenzen (Risiko- und Krisenmanagementverfahren und -protokolle, Abläufe im Alarmfall

AGENDA

1 VORSTELLUNG

2 GESETZLICHE RAHMENBEDINGUNGEN

3 ANWENDUNGS-BEREICH

4 DAS BESTE AUS BEIDEN WELTEN

5 BEST PRACTICE

BEST PRACTICE

BSKI

GDV Gesamtverband der Versicherer
Publikation der Deutschen Versicherer zur Schadenverhütung

VdS

Sicherungsrichtlinien für
Museen und Ausstellungshäuser

VdS 3511 : 2008-09 (01).

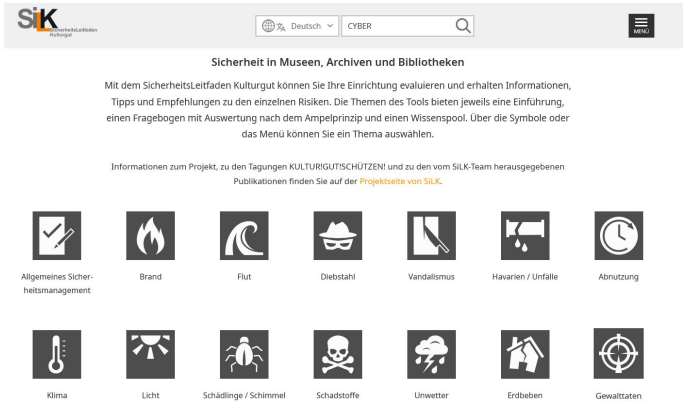
BHE

Mehr Sicherheit für Museen

Der BHE Bundesverband Sicherheitstechnik e.V. informiert www.bhe.de

Vorsorgemaßnahmen zum Schutz vor Einbruch, Diebstahl, Vandalismus und sonstigen Risiken

BHE Bundesverband Sicherheitstechnik e.V.
Feldstraße 28, 66904 Brücken
Telefon: 06386 92 14-0, Telefax: 06386 9214-99
E-Mail: info@bhe.de, Internet: www.bhe.de



Quelle: https://www.silk-tool.de/de/

BEST PRACTICE

Vorteil:
Gute Grundstruktur zur Erarbeitung eines Sicherheitskonzepts.

Nachteil:
Betrifft nur die physische Sicherheit und lässt hybride Bedrohungen außer Acht.

BEST PRACTICE

Museen stehen vor einer Vielzahl von Gefahren, die sowohl aus natürlichen als auch aus menschlichen und digitalen Bedrohungen resultieren. Eine effektive Gefährdungsanalyse und umfassende Schutzmaßnahmen sind essenziell, um Kulturgüter zu bewahren und Besucher sowie Mitarbeiter zu schützen. Durch Kombination technischer, organisatorischer und personeller Maßnahmen können Risiken minimiert und langfristige Sicherheitsstrategien etabliert werden.

BEST PRACTICE

Am Anfang steht eine Gefährdungsanalyse nach dem All-Gefahrenansatz

Gefahrenquelle	Eintrittswahrscheinlichkeit	Auswirkungen	Maßnahmen
Erdbeben	Mittel	Strukturelle Schäden, Verletzungen	Erdbebensichere Bauweise, Exponatsicherung, Notfallpläne
Überschwemmungen	Hoch	Wasserschäden, Schimmelbildung, Kurzschlüsse	Erhöhte Lagerung, Schutzbarrieren, Entwässerungssysteme
Feuer	Mittel	Totalschäden, Rauchvergiftung	Feuerfeste Lagerung, Brandmeldeanlagen, Evakuierungsübungen
Diebstahl & Vandalismus	Hoch	Verlust oder Beschädigung von Exponaten	Videoüberwachung, Sicherheitsglas, Zugangskontrollen
Terroranschläge & Sabotage	Niedrig	Gefahr für Menschenleben, Zerstörung	Sicherheitskontrollen, Notfallpläne, Schulungen
Fahrlässigkeit	Mittel	Beschädigungen durch Besucher	Verhaltensregeln, Sensibilisierung, Wartung
Hackerangriffe & Datendiebstahl	Hoch	Datendiebstahl, Manipulation	Firewalls, Sicherheitsupdates, Schulungen
Systemausfälle & Datenverluste	Mittel	Betriebsunterbrechung, Datenverlust	Regelmäßige Backups, Notfallpläne, Redundante Server
Fake News & digitale Sabotage	Mittel	Rufschädigung, Manipulation	Social Media Monitoring, Krisenkommunikation, Zusammenarbeit mit IT-Sicherheit

BEST PRACTICE

Dieses Konzept behandelt physische Sicherheit und Informationssicherheit nach ISO 27001.

Physische Sicherheit

- Zugangskontrollen
- Videoüberwachung
- Alarm- und Sicherheitssysteme
- Notfallmanagement
- Schutz vor physischem Diebstahl

BEST PRACTICE

Dieses Konzept behandelt physische Sicherheit und Informationssicherheit nach ISO 27001.

Physische Sicherheit

- Zutrittsberechtigungen definieren
- Sicherheitsbereiche festlegen
- Elektronische Zutrittskontrollsysteme nutzen

BEST PRACTICE

Dieses Konzept behandelt physische Sicherheit und Informationssicherheit nach ISO 27001.

Informationssicherheit (ISO 27001)

- IT-Sicherheitsrichtlinien
- Schutz vor Cyberangriffen
- Datensicherung & Backup
- Zugriffskontrollen & Authentifizierung
- Schulung der Mitarbeitenden

BEST PRACTICE

Dieses Konzept behandelt physische Sicherheit und Informationssicherheit nach ISO 27001.

Notfallmanagement

- Evakuierungspläne entwickeln & üben
- Sicherheitsbeauftragte benennen
- Notfallkontakte für Polizei & Feuerwehr definieren

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Kontakt:
Holger Berens

holger.berens@bski.de
h.berens@concepture.de