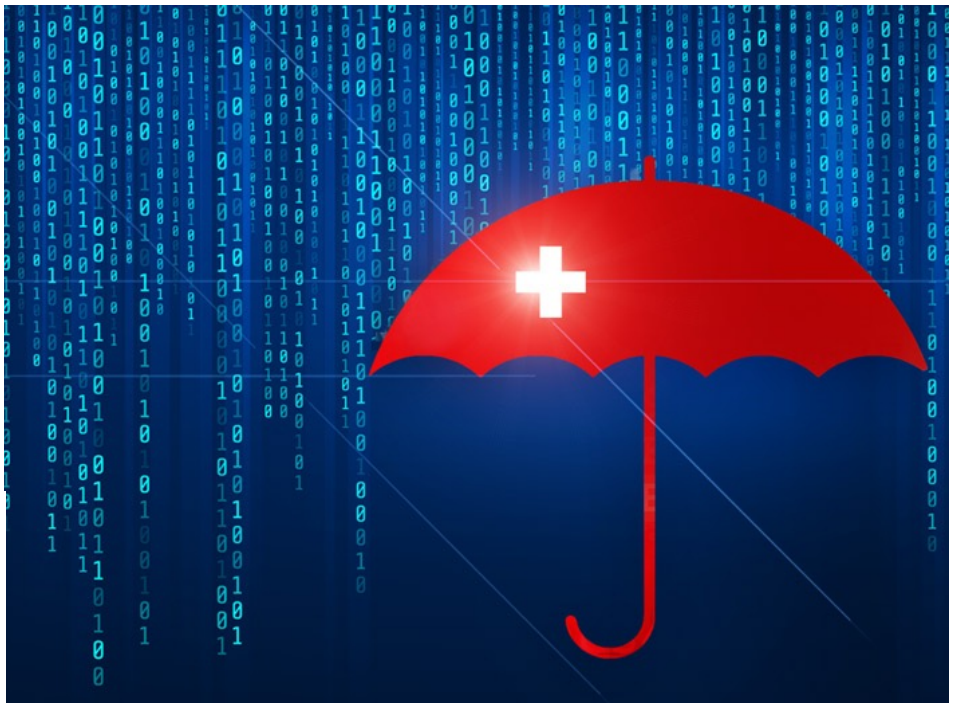
HSLU Hochschule Luzern

Cyber- Resilienz in der kritischen Infrastruktur der Schweiz:

Ein Überblick über regulatorische Anforderungen

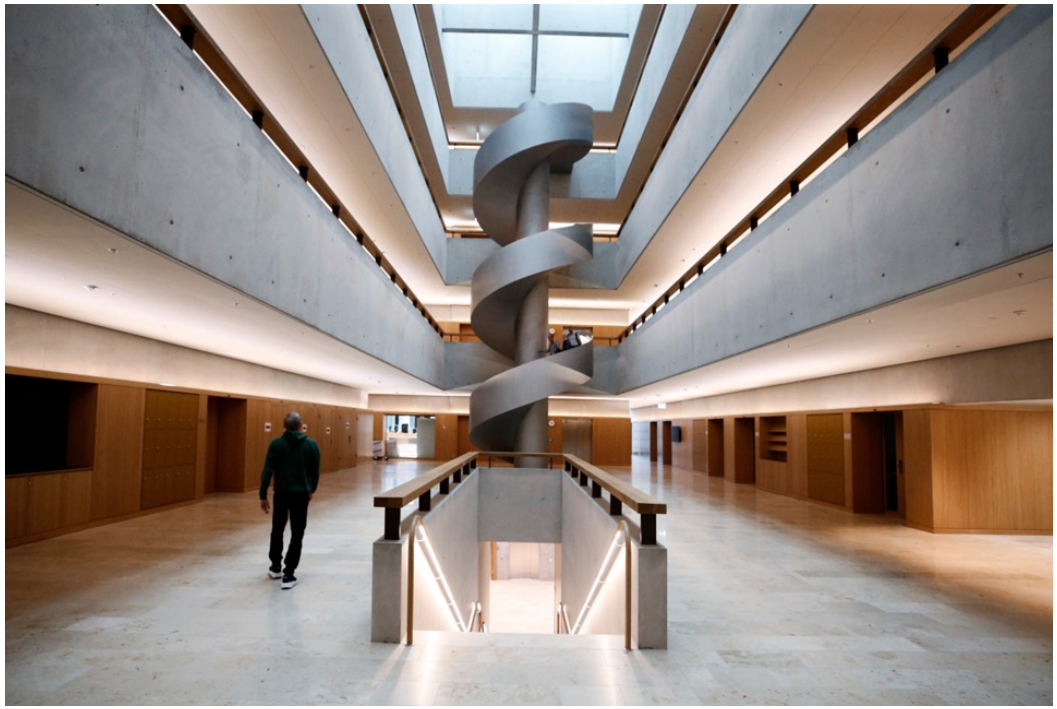


Juan Carlos Lopez Ruggiero
CISO & Dozent Hochschule Luzern

28. September 2023
FH Zentralschweiz

Agenda

1. **Einleitung**
2. **Bedrohungen für kritische Infrastruktur**
3. **Rechtlicher Rahmen in der Schweiz**
4. **Ziele der regulatorischen Anforderungen**
5. **Umsetzung der regulatorischen Anforderungen**
6. **Weitere Details**



Einleitung

In unserer zunehmend digitalisierten Welt ist die Gewährleistung der Sicherheit unserer nationalen Infrastruktur von entscheidender Bedeutung.

Cyber Resilienz - die Fähigkeit, sich gegen Cyberangriffe sich zu schützen und rasch zu erholen - ist von entscheidender Wichtigkeit.

Besonders relevant sind hierbei die **regulatorischen Anforderungen**, die einen rechtlichen Rahmen schaffen, um die **Sicherheit** unserer **kritischen Infrastruktur** zu garantieren und die Auswirkungen von Cyberangriffen zu minimieren.

Während dieser Präsentation werden wir einen Einblick in die regulatorischen Anforderungen geben und Ihnen **praxisnahe Umsetzungsstrategien** vorstellen.

Bedrohungen für kritische Infrastruktur

Die Sicherheit kritischer Infrastrukturen ist von zunehmender Relevanz, da die Bedrohungslandschaft immer komplexer wird.
Laut NCSC und Eidgenössische Finanzdepartement, haben Cyberangriffe auf kritische Infrastrukturen in den letzten Jahren um 25% zugenommen.

Bedrohungen

i. Gezielte Hackerangriffe: Gezielte Angriffe, um in Systeme einzudringen und gezielt Schaden anzurichten.

i. Malware/Ransomware: Die Verbreitung von schädlicher Software kann die Betriebsfähigkeit von Systemen ernsthaft beeinträchtigen.

ii. Distributed-Denial-of-Service (DDoS) Attacken: Durch die Überflutung von Netzwerken mit einem hohen Datenaufkommen wird die Verfügbarkeit von Diensten beeinträchtigt.

iii. Phishing-Attacken: Durch die Täuschung von Benutzern versuchen Angreifer Zugangsdaten oder andere sensible Informationen zu erlangen.

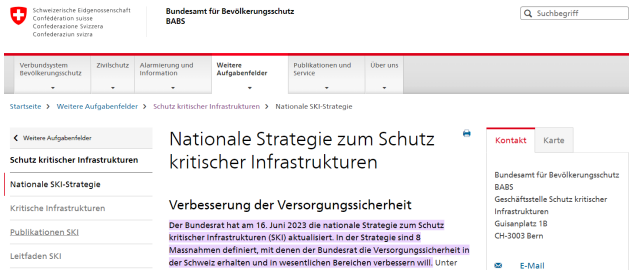
iv. Insider-Bedrohungen: Interne Personen können eine Gefahr darstellen, sei es absichtlich oder durch fahrlässiges Verhalten.

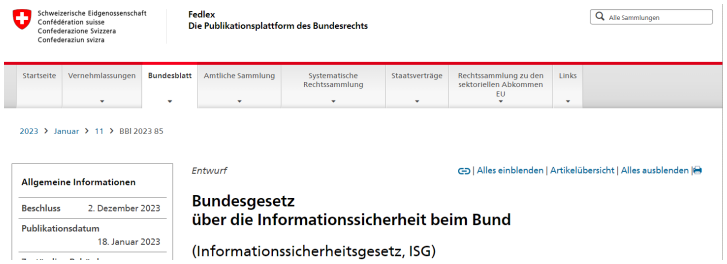
Beispiele aus der Praxis

- **Ein Energieversorger wurde Opfer eines gezielten Hackerangriffs**, bei dem Angreifer versuchten, die Steuerungssysteme zu manipulieren .
- **Eine Ransomware-Attacke legte die IT-Systeme einer Klinik inaktiv**, was zu einer vorübergehenden Unfähigkeit führte, lebenswichtige medizinische Aufzeichnungen abzurufen.
- **Ein Online-Handelsunternehmen wurde Opfer einer DDoS-Attacke**, die zu einem Ausfall des Webshops führte und erheblichen finanziellen Schaden verursachte.
- **Mitarbeiter eines Unternehmens erhielten gefälschte E-Mails**, die scheinbar von der Geschäftsführung stammen, und sie dazu aufforderten, vertrauliche Informationen aufzugeben.
- **Ein ehemaliger Mitarbeiter mit Rachegefühlen griff auf sensible Unternehmensdaten zu** und veröffentlichte vertrauliche Informationen im Internet.

Welches rechtliche Rahmen?

Der Zusammenhang zwischen Cyberbedrohungen und dem rechtlichen Rahmen bezüglich Resilienz in kritischen Infrastrukturen in der Schweiz ist von **entscheidender Bedeutung** für die Sicherheit und den Schutz dieser wichtigen Systeme.





Das ISG legt für verpflichtete Organisationen und Behörden zahlreiche Vorgaben. Hier einige Beispiele:

Informationssicherheits-Management-System (ISMS):

- Beurteilung des Schutzbedarfs der Informationen und deren Klassifizierung
- Die Identifizierung und laufende Beurteilung von Risiken
- Die Festlegung eines Sicherheitsverfahrens sowie Sicherheitsmassnahmen.
- Identitätsverwaltungssysteme (Art, 24-26 ISG).

Informationen

- Identifikation, Schutz und Klassifikation der verarbeiteten Informationen.

Riskmanagement

- Massnahmen zur Vermeidung und Reduzierung von Risiken (deutlich benannt, nachweislich akzeptiert und entsprechend gehandhabt werden)

Zusammenarbeit mit Dritten

- Sicherstellen, dass gesetzliche Vorgaben eingehalten werden. Dies soll vertraglich geregelt (Artikel 9 ISG).

Ziele der regulatorischen Anforderungen (Makro-Ziele)

Gewährleistung der Kontinuität kritischer Dienstleistungen

Aktivitäten:

- Erstellung eines Business Continuity Plans (BCP) für kritische Dienstleistungen..
- Durchführung von regelmässigen Tests und Übungen des BCP.
- **Ergebnisse**
- Sicherstellung, dass kritische Dienstleistungen auch im Falle eines Sicherheitsvorfalls aufrechterhalten werden können.
- Minimierung von Betriebsunterbrechungen und finanziellen Verlusten.

Minimierung der Auswirkungen von Cyberangriffen:

Aktivitäten:

- Entwicklung von Reaktionsplänen für verschiedene Arten von Cyberangriffen.
- Implementierung von IDS und SIEM-Lösungen.

Ergebnisse

- Schnelle Erkennung von Sicherheitsvorfällen und effektive Reaktion zur Minimierung von Schäden.
- Reduzierung der Auswirkungen von Cyberangriffen auf kritische Systeme und Dienstleistungen

Schutz sensibler und personenbezogener Daten

Aktivitäten:

- Implementierung von Verschlüsselungstechnologien.
- Etablierung von Zugriffssteuerungen und Berechtigungsmechanismen..

Ergebnisse

- Gewährleistung der Vertraulichkeit und Integrität von sensiblen und personenbezogenen Daten.
- Einhaltung gesetzlicher Datenschutzvorschriften und Vermeidung von Datenschutzverletzungen.

Einhaltung gesetzlicher Vorgaben und Standards

Aktivitäten:

- Regelmässige Überprüfung von Gesetzen und Vorschriften im Bereich Cybersecurity und Datenschutz.
- Implementierung von Sicherheitskontrollen und Massnahmen zur Einhaltung spezifischer rechtlicher Anforderungen.

Ergebnisse

- Nachweis der Einhaltung gesetzlicher Anforderungen und Schutz vor rechtlichen Konsequenzen.
- Aufrechterhaltung eines positiven Unternehmensimages und Vertrauens bei Kunden und Partnern.

Umsetzung der regulatorischen Anforderungen

Organisation in vier Dimensionen bewerten

Wichtige Aktivitäten und Ergebnisse

Identifikation kritischer Komponenten:

- **Identifikation und Kategorisierung** von kritischen Komponenten innerhalb der Infrastruktur.

Outcome: Liste der als kritisch identifizierten Komponenten und ihre Priorisierung.

Schwachstellenanalyse:

- Die Analyse möglicher **Schwachstellen** in den essenziellen Komponenten und Systemen.

Outcome: Identifizierten Schwachstellen und ihre potenziellen Auswirkungen (Riskmanagement)

Bedrohungsanalyse

- Die **Bewertung** der **verschiedenen Bedrohungen**, denen die kritische Infrastruktur ausgesetzt ist.

Outcome: Bedrohungen, Wahrscheinlichkeit und Gegenmassnahmen

Risikobewertung und –Quantifizierung

- Die Einschätzung der Risiken, die aus den identifizierten Schwachstellen und **Bedrohungen** resultieren.

Outcome: Matrix zur Klassifizierung und Priorisierung der Risiken

Entwicklung von Notfallplänen:

- Die Ausarbeitung von **Notfallplänen**, um auf Krisensituationen reagieren zu können.

Outcome: Notfallpläne für verschiedene Szenarien.

Überprüfung und Aktualisierung

- Die Einschätzung von Risiken wird regelmässig angepasst und aktualisiert, um stets auf dem **neuesten Stand** der verfügbaren Informationen und Entwicklungen zu sein.

Outcome: Aktualisierte Risikobewertung sowie die Notfallpläne.

Umsetzung der regulatorischen Anforderungen

Organisation in vier Dimensionen bewerten

Wichtige Aktivitäten und Ergebnisse

Physische Sicherheit

- Physische Sicherheitsmassnahmen beziehen sich auf bauliche und technische Vorkehrungen, die darauf abzielen, den **unerlaubten Zutritt zu sensiblen Bereichen** zu verhindern..

Outcome: Physische Integrität der Infrastruktur geschützt und unbefugte Zugriffe minimiert werden.

Technischer Schutz (Cybersecurity):

- Implementierung von Softwarelösungen, Firewalls, und Intrusion Detection Systemen usw., um **die IT-Infrastruktur vor Cyberangriffen zu schützen.**

Outcome: Die IT-Infrastruktur wird vor unberechtigten Zugriffen und schädlichen Angriffen geschützt

Regelmässige Überprüfungen und Schulungen

Regelmässige Sicherheitsüberprüfungen und Mitarbeiterschulungen sind wesentliche Bestandteile eines effektiven Sicherheitsmanagements.

Outcome: Schwachstellen werden erkannt und behoben, und Sicherheitsbewusstsein steigt.

Notfallpläne und Krisenmanagement

- Notfallpläne sind **vordefinierte Massnahmen**, die im Falle eines Sicherheitsvorfalls ergriffen werden.

Outcome: Eine geordnete Reaktion, minimieren Schäden und beschleunigen die Wiederherstellung der kritischen Dienstleistungen

Kontinuierliches Monitoring und schnelle Reaktion:

- Das permanente Überwachen der Infrastruktur für die frühzeitige Erkennung von Anomalien und ungewöhnlichen Aktivitäten.

Outcome: Prompte Reaktion, Auswirkungen von Sicherheitsvorfällen und bessere Widerstandsfähigkeit.

Regelmässige Updates und Sicherheitspatches

- Aktualisierungen von Software und Systemen sind entscheidend, um Sicherheitslücken zu schliessen und die Resistenz gegen aktuelle Bedrohungen zu erhöhen.

Outcome: Schliessen von Sicherheitslücken, Erhöhung der Resilienz.

Umsetzung der regulatorischen Anforderungen

Organisation in vier Dimensionen bewerten

- Risikobewertung
- Sicherheits-Massnahmen
- **Schulungen und Sensibilisierung**
- Notfallplanung

Wichtige Aktivitäten und Ergebnisse

Mitarbeiter-Schulungen zu Sicherheitsverfahren

- Regelmässige Schulungen für Mitarbeiter zu aktuellen Cyberfälle, **Datenschutzrichtlinien** und Best Practices.

Outcome: Erhöhtes Sicherheitsbewusstsein

Simulierte Sicherheitsübungen und Szenarien:

- Durchführung von simulierten Sicherheitsübungen, um die Reaktionsfähigkeit der **Mitarbeiter im Falle eines Sicherheitsvorfalls zu testen**.

Outcome: Verbesserte Fähigkeit der Mitarbeiter, effektiv auf Sicherheitsvorfälle zu reagieren, minimierte Auswirkungen von Vorfällen.

Sensibilisierung für Social Engineering und Phishing-Angriffe

Schulungen zur Erkennung von Social Engineering-Techniken und Phishing-Angriffen.

Outcome: Reduzierung von Fehlern gegenüber manipulativen Angriffen.

Sicherheitsrichtlinien und Best Practices-Kommunikation

- Kontinuierliche Kommunikation zu aktuellen Sicherheitsrichtlinien und bewährten Praktiken, regelmässige Meetings, informative Rundschreiben.

Outcome: Stärkung das Verständnis für die kritischen Sicherheitsmassnahmen.

Schulungen zur sicheren Nutzung von Technologien

- Themen wie sichere Passwortverwaltung, verschlüsselte Kommunikation und verantwortungsvoller Umgang mit sensiblen Daten .

Outcome: Die Mitarbeiter, digitale Werkzeuge effektiv und sicher einzusetzen.

Umsetzung der regulatorischen Anforderungen

Organisation in vier Dimensionen bewerten

Wichtige Aktivitäten und Ergebnisse

Regelmässige Notfallübungen und Simulationen inklusive Blue Team / Red Team Szenarien

- Durchführung von **Blue Team** (verteidigend) und **Red Team** (angreifend) Szenarien.

Outcome: Reaktionsfähigkeit und Koordination der Teams, Fähigkeit, sich gegen gezielte Angriffe zu verteidigen und Sicherheitsmassnahmen zu optimieren

Krisenstab einrichten (Einsatzleitung)

Benennung eines Krisenstabs, der die Verantwortung für die Koordination und **Entscheidungsfindung** während der Krise übernimmt

Outcome: zielgerichtete Koordination; Verantwortlichkeiten und Zuständigkeiten deutlich definiert; schnelle und fundierte Entscheidungsfindung

Koordination mit Behörden und externen Partnern

- Die Koordination mit Behörden und externen Partnern ist ein **Schlüsselelement für ein effektives Krisenmanagement** und trägt massgeblich zur Resilienz der kritischen Infrastruktur bei.

Durch die enge Abstimmung mit Behörden und externen Partnern kann eine schnellere und koordinierte Reaktion auf kritische Ereignisse erfolgen.

Wie und wo kann man mehr Details erfahren?

Internet

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Fedlex
Die Publikationsplattform des Bundesrechts

Nationale Strategie zum Schutz kritischer Infrastrukturen

https://www.newsd.admin.ch/newsd/message/attachments/50747.pdf

Schutz kritischer Infrastrukturen

https://www.babs.admin.ch/de/aufgabenbabs/ski.html

Nationales Zentrum für Cybersicherheit (NCSC)

https://www.ncsc.admin.ch/ncsc/de/home.html

Vorträge

Beispielsweise wie die heutige Veranstaltung

Weiterbildung

HSLU Lucerne University of Applied Sciences and Arts

CAS Resilient Industrial Infrastructures Resilienz im industriellen Kontext verstehen und prozessorientiert auf Infrastrukturen anwenden

Wie und wo kann man mehr Kenntnisse erhalten?

Danke schön
Merci
Grazie
Grazia

Juan Carlos Lopez Ruggiero
juancarlos.lopezruggiero@hslu.ch