INFOTECH
[ IT & Communication ]

# 28. InfoTechDay

16.11.2023

## Herzlich willkommen!


# IT Security im Rückspiegel

## Was wir tun hätten sollen, um jetzt für NIS 2 bereit zu sein

# Ziele von NIS2

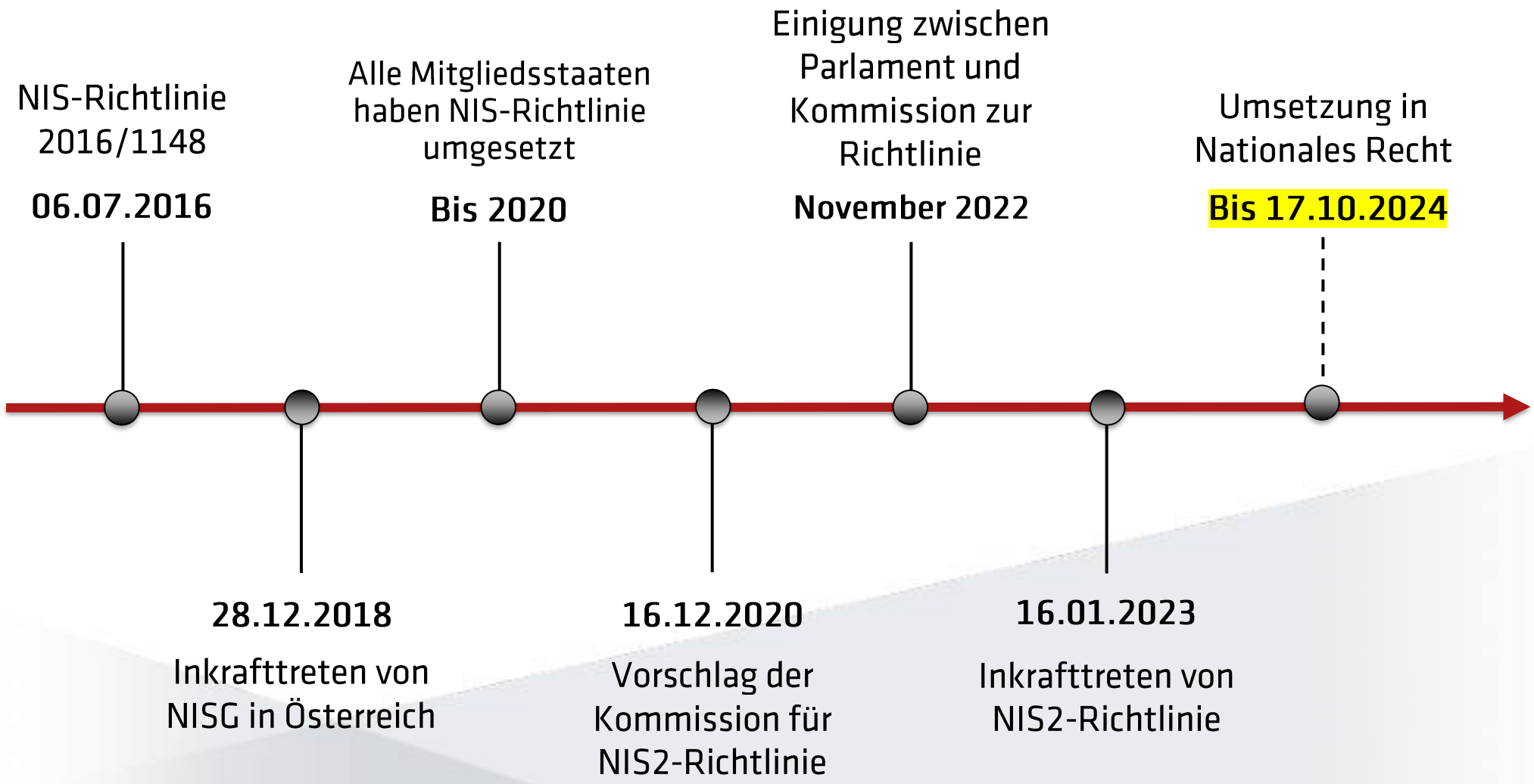
Netz- und Informationssystemsicherheitsgesetz (NISG)

INFOTECH
[IT & Communication]

- **Sicherstellen eines hohen, einheitlichen Sicherheitsniveau von Netz- und Informationssystemen in der EU**
- **Stärkung der Resilienz gegen Angriffe**
- **Sicherheit von Lieferketten (Supply Chain Security)**
- **Schaffung/Verschärfung von Meldepflichten**
- **Aufsicht und Überwachung durch Behörden**
- **Aufbau von nationalen CERTs + Datenaustausch**

# Historie

INFOTECH
[IT & Communication]




Ihr Systemhaus.

# Wer ist Betroffen?

INFOTECH
[IT & Communication]

| Sektoren mit hoher Kritikalität | Sonstige kritische Sektoren |
|---|---|
| Energie | Post- und Kurierdienst |
| Verkehr | Abfallbewirtschaftung |
| Ban | Produktion, Herstellung und Handel mit chemischen Stoffen |
| Fina | Produ mitteln |
| Gesu | s/herstellendes Gewerbe |
| Trin | ste |
| Abwasser | Fors |
| Digitale Infrastruktur | |
| Verwaltung von IKT-Diensten | |
| Öffentliche Verwaltung | |
| Weltraum | |

**Große Un**
**→ wesentliche**

**Mittlere Unternehmen**
**→ wichtige Einrichtung**

**→ wichtige Einrichtung**

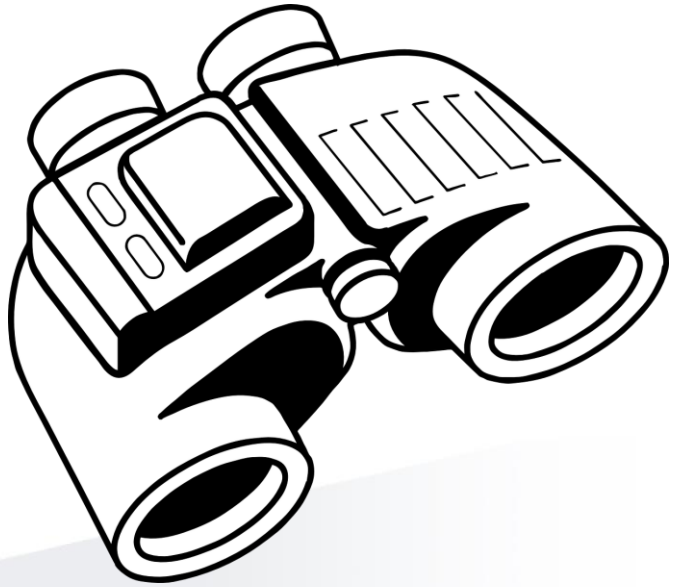
https://ratgeber.wko.at/nis2/

Ihr Systemhaus.

# Aufsicht/Prüfung

INFOTECH
[IT & Communication]

- **Wesentliche Einrichtungen**
  - Regelmäßige und gezielte Sicherheitsprüfung („ex-ante“ + „ex-post“)
  - Stichprobenkontrollen



- **Wichtige Einrichtungen**
  - Überprüfung nur bei begründetem Verdacht („ex-post“)
  - Vor-Ort-Kontrollen und externe nachträgliche Aufsichtsmaßnahmen

# Berichtspflichten (Art. 23)

INFOTECH
[IT & Communication]

- **Frühwarnung: 24 Stunden**
- **Meldung: 72 Stunden**
- **Abschlussbericht: 1 Monat**

- **Erheblicher Sicherheitsvorfall:**
  - Schwerwiegende Betriebsstörung oder schwerwiegende finanzielle Verluste
  - Beeinträchtigung von Personen durch erhebliche materielle oder immaterielle Schäden

# Sanktionen

## Verstöße gegen NIS2 (insbesondere Art. 21 & 23)

INFOTECH
[IT & Communication]

- **Wesentlichen Sektoren:**
  - mind. 10 Mio. Euro **oder**
    2 % des weltweiten Umsatzes

- **Wichtigen Sektoren:**
  - mind. 7 Mio. Euro **oder**
    1,4 % des weltweiten Umsatzes

- **Natürliche Personen (leitende Angestellte) können für Pflichtverletzungen haftbar gemacht werden**


Was hätten wir tun sollen?

# Cyberhygiene und Schulungen zu Cybersicherheit
## Artikel 21 Abs. 2 g)

INFOTECH
[IT & Communication]


Ihr Systemhaus.

# Cyberhygiene und Schulungen zu Cybersicherheit Artikel 21 Abs. 2 g)

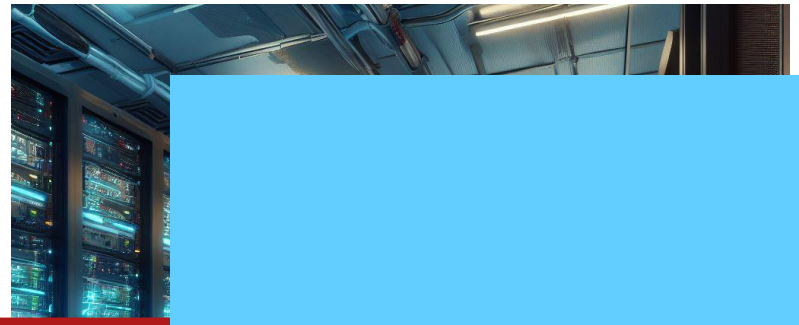
INFOTECH
[IT & Communication]

## my.bizcloud.Awareness

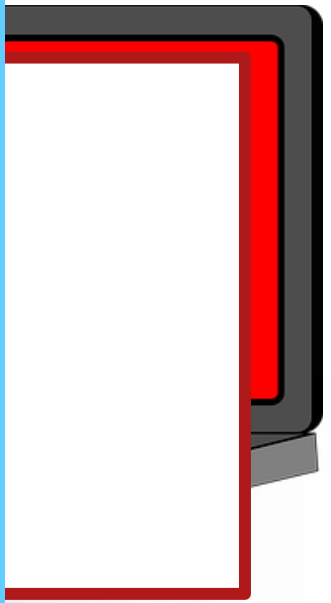
- Online Lernplattform
- Datenschutz und Informationssicherheit
- Sicherheitsbewusstsein fördern
- Risiko von Vorfällen minimieren
- Mensch als Sicherheitslücke Nr. 1

Ihr Systemhaus.

INFOTECH
[IT & Communication]







Ihr Systemhaus.

my.biz cloud

# BACKUP

**Eine funktionsfähige Datensicherung (Backup) von Daten und Systemen zu haben, ist heutzutage eine der wichtigsten Herausforderungen für Unternehmen aller Größenordnungen. Die Implementierung einer Strategie zur Datensicherung wird für Unternehmen immer wichtiger – nur so kann im Ernstfall die Verfügbarkeit der Daten sichergestellt werden.**

# Multi-Factor-Authentication

INFOTECH
[IT & Communication]

- **Wer verwendet extern erreichbare Dienste?**
- **Wer schützt (zumindest) diese Dienste mit MFA?**
- **Warum zeigen nicht alle auf?**

Ihr Systemhaus.

# MFA und gesicherte Kommunikation
# Artikel 21 Abs. 2 j)

INFOTECH
[IT & Communication]

- **Verwendungen von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikation innerhalb der Einrichtung**

# Organisatorische Themen – Risikomanagement
# Artikel 21 Abs. 2 a)

INFOTECH
[IT & Communication]

- **Risikomanagement etablieren**
  - Risiken systematisch erheben und nachvollziehbar behandeln
  - Entscheidungsgrundlage für weitere Maßnahmen (Angemessenheit)
  - Es muss nicht immer ein teures Tool zum Einsatz kommen

# Organisatorische Themen – Lieferantenmanagement (§ 30 Abs. 2 d)

INFOTECH
[IT & Communication]

Zulieferer von wesentlichen oder wichtigen Unternehmen könnten geprüft werden

- **Sicherheitsrichtlinie**
  - Erfassen aller Dienstleister (interne Freigaben)
  - Prüfung der Dienstleister vor Einstufung
  - Vertragliche Verpflichtung der Lieferanten (Geheimhaltung, Recht auf Prüfung, Meldung von Sicherheitsvorfällen, ...)

Ihr Systemhaus.

# Anforderungen für betroffene Unternehmen

## (Zusammenfassung Artikel 21 NIS2)

INFOTECH
[IT & Communication]

| | |
|---|---|
| **Risikomanagement** | • Verpflichtung zu regelmäßigen Risikobewertungen<br>• Senken der Wahrscheinlichkeit für erfolgreichen Cyberangriff |
| **Vorfallsmanagement** | • Schnell und effektiv auf Sicherheitsvorfälle reagieren<br>• Notfallpläne |
| **Technische und organisatorische Maßnahmen** | • Zugriffskontrolle, Verschlüsselung, digitales Überwachungssystem<br>• Risiko von Cyberangriffen und Datenlecks verringern<br>• Verwendung von MFA<br>• Cyberhygiene und Schulungen im Bereich Cybersicherheit |
| **Buisness Continuity** | • Pläne zur Aufrechterhaltung des Betriebs bei Sicherheitsvorfällen<br>• Ausfallzeit minimieren und kritische Dienste aufrechterhalten |
| **Sicherheit der Lieferkette** | • Beachtung der Sicherheit von Lieferketten<br>• Risiko für Cyberangriff über die Lieferkette senken<br>• Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung |

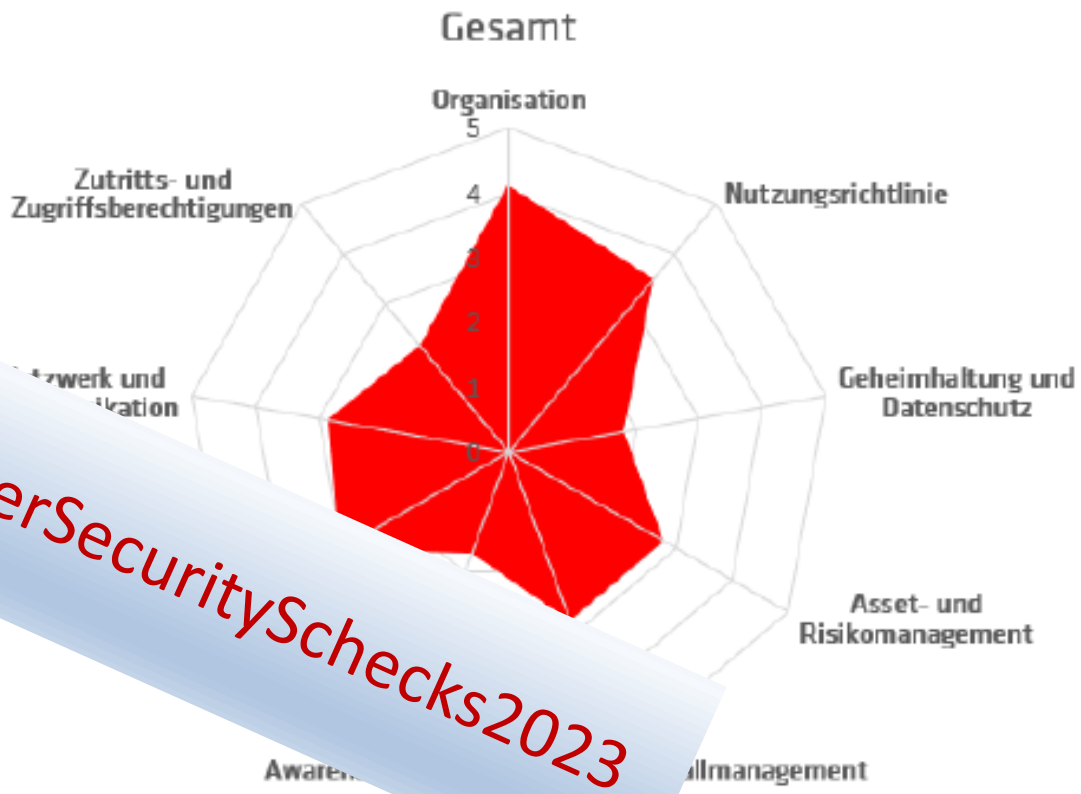
# Die Umsetzung

INFOTECH
[IT & Communication]

**Features:**

- Gem… …des IST-Standes
- Basieren… …dards wie z. B. ISO / IEC 27000, … usw.
- Identifikation von poten…
- Kategorisierung der Schwachst… deren Kritikalität
- Darstellung von Verbesserungspotential
- Erstellung eines umfangreichen Berichts über die besprochenen Punkte
- Gemeinsames Review der Findings nach 1 Jahr

https://www.ffg.at/ausschreibung/CyberSecuritySchecks2023




Ihr Systemhaus.

# Warum eigentlich NIS2?

INFOTECH
[IT & Communication]

- **Mehr als jeder achte Cyberangriff ist erfolgreich**
- **Zunahme an Cyberangriffen um 201 % gegenüber von letztem Jahr**

**Phishing Attacken**
**→ 100%**

**Social Engineering**
**→ 57%**

**Ransomware**
**→ 33%**

**Deepfake Attacken**
**→ 22%**

Quelle: KPMG/KSÖ Studie „Cybersecurity in Österreich 2023“

Ihr Systemhaus.

INFOTECH

[IT & Communication]

Ihr Systemhaus.