APG

30.09.2024

NIS2-Gesetz und zukünftige Cybersecurity-Herausforderungen

Die Bedrohungslandschaft im Cyberspace (exemplarischer Auszug)

~2010

Stuxnet: Malware, um Industriesteuerung im Iran zu manipulieren

2015

Sandworm: weltweit erster großer Stromausfall durch Hackerangriff

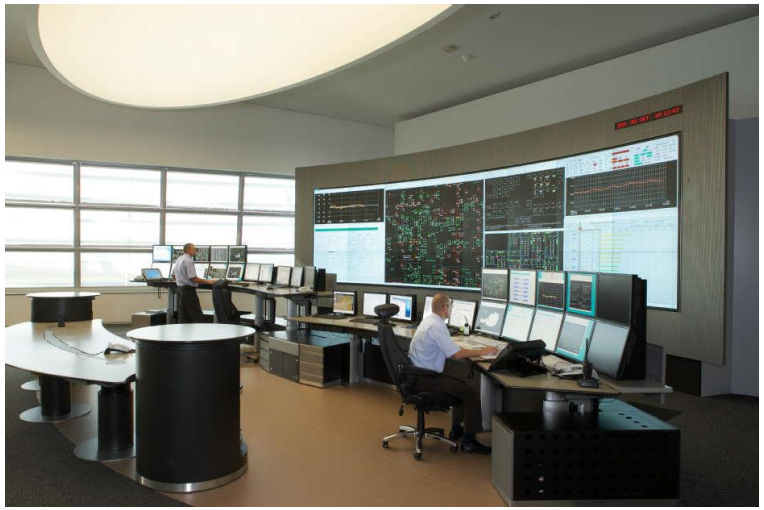
2021

Ransomware-Angriff auf Systeme zur Rechnungslegung mit Auswirkungen auf die Gesellschaft

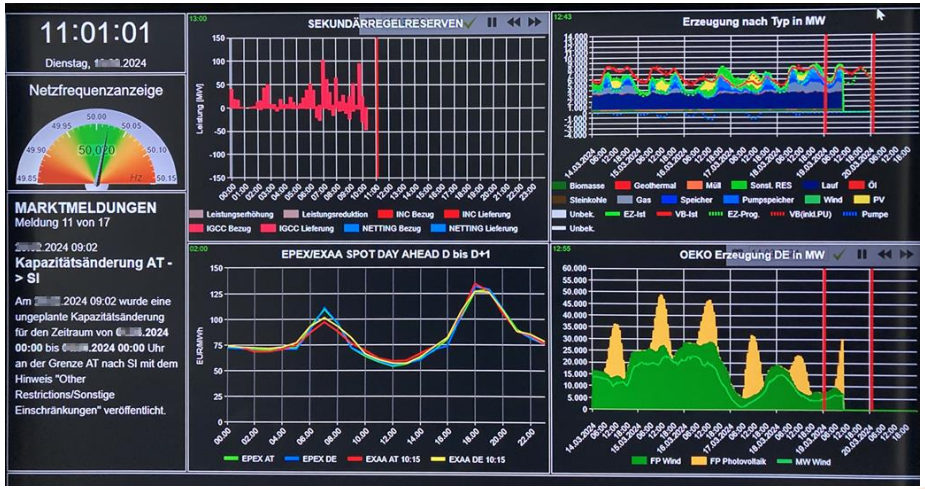
Bitte was funktioniert noch ohne Strom?

https://www.youtube.com/watch?v=v-MYtqwxGLA

Welche Werte müssen wir schützen?



Assets & Daten



Grundlagen der Cybersecurity?

ENISA: Cyber-Hygiene-Praktiken in ganz Europa

1. **Verzeichnis aller Hardware**
2. Verzeichnis aller **Software** + Sicherstellung aller **Updates**
3. Verwendung sicherer **Konfigurations-/Härtungsleitfäden** für alle Geräte
4. **Datenverwaltung** IN und AUS dem Netzwerk
5. Alle eingehenden **E-Mails scannen**
6. Minimierung der **administrativen Konten**
7. Regelmäßige **Datensicherungen** und **Wiederherstellungstests**
8. Erstellen Sie einen **Plan zur Reaktion auf Vorfälle**
9. Durchsetzung ähnlicher **Sicherheitsniveaus** in der gesamten **Lieferkette**
10. **Sicherheitskontrollen** in **Dienstleistungsvereinbarungen** (einschließlich Cloud-Diensten)

https://www.enisa.europa.eu/publications/cyber-hygiene/

Pflichten und Sicherheitsmaßnahmen eines Übertragungsnetzbetreibers

Freiwillig (seit 2007) → Gesetzlich (seit 2019) → Ab 2025?

1. Governance und Risikomanagement
2. Umgang mit Dienstleistern, Lieferanten und Dritten
3. Sicherheitsarchitektur
4. Systemadministration
5. Identitäts- und Zugriffsmanagement
6. Systemwartung und Betrieb
7. Physische Sicherheit
8. Erkennung von Vorfällen
9. Bewältigung von Vorfällen
10. Betriebskontinuität
11. Krisenmanagement

→ NIS2 DIRECTIVE

- Jedes Jahr Überwachungsaudit
- Jedes 3. Jahr Rezertifizierungsaudit

- Netz- und Informationssystemsicherheitsgesetz (NISG)
- alle 3 Jahre Nachweis der Compliance nach NISG an Ministerium (BMI)
- https://www.nis.gv.at/

Cybersecurity-Ausblick für die nächsten 3-5 Jahre und deren Herausforderungen in der Umsetzung

Regulierung

- Steigende gesetzliche Anforderungen (europäisch und national)
- Strategische europäische Neuausrichtung:
  1. “EU action plan for digitalisation the energy system”
  2. Neue Legistik für Daten, AI und Cyber-Domäne (u.a. Data Act, Data Governance Act, AI Act, NIS2, NCCS)

Digitale Transformation

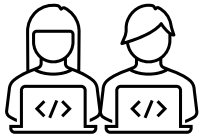
- Chancen & Risiken durch neue Technologien
- Herausforderungen durch ChatGPT, Deep Fakes (Faktor Mensch!)
- Rasante Geschwindigkeit auf mehreren Ebenen → Menschen mitnehmen

Komplexität

- Zunehmende Komplexität in der gesamten Wertschöpfungskette (stark steigende Vernetzung inkl. Dienstleister und Lieferanten)
- Viele neue gegenseitige Abhängigkeiten
- Übergreifendes Verständnis über Geschäftsprozesse und Abhängigkeiten u.a. von Dritten

Lifecycle

- Ausbau, Instandhaltung und Erneuerung von IT/OT und Betriebsanlagen (Bestand, Erweiterungen, Third/Fourth Parties)
- Organisatorische Entwicklung des Unternehmens

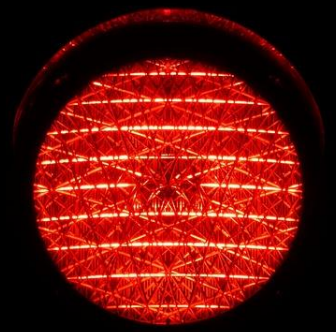


Fachkräfte

- Halten und Ausbilden von Personal (allgemein und speziell IT, OT, Cyber, Data)
- „Upskilling“: Aktive Mitarbeiter:innen-Weiterentwicklung → gesuchtes Personal, Allrounder und Spezialisten, selbst aufbauen

AI .. Artificial Intelligence
NIS .. Netz- und Informationssystemsicherheit
NCCS .. Network Code on Cybersecurity

Sicherer Umgang mit unsicheren Situationen



Innehalten

Genau
hinsehen

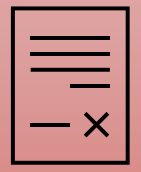
Nicht
unbedacht
handeln

Cybersecurity – take aways

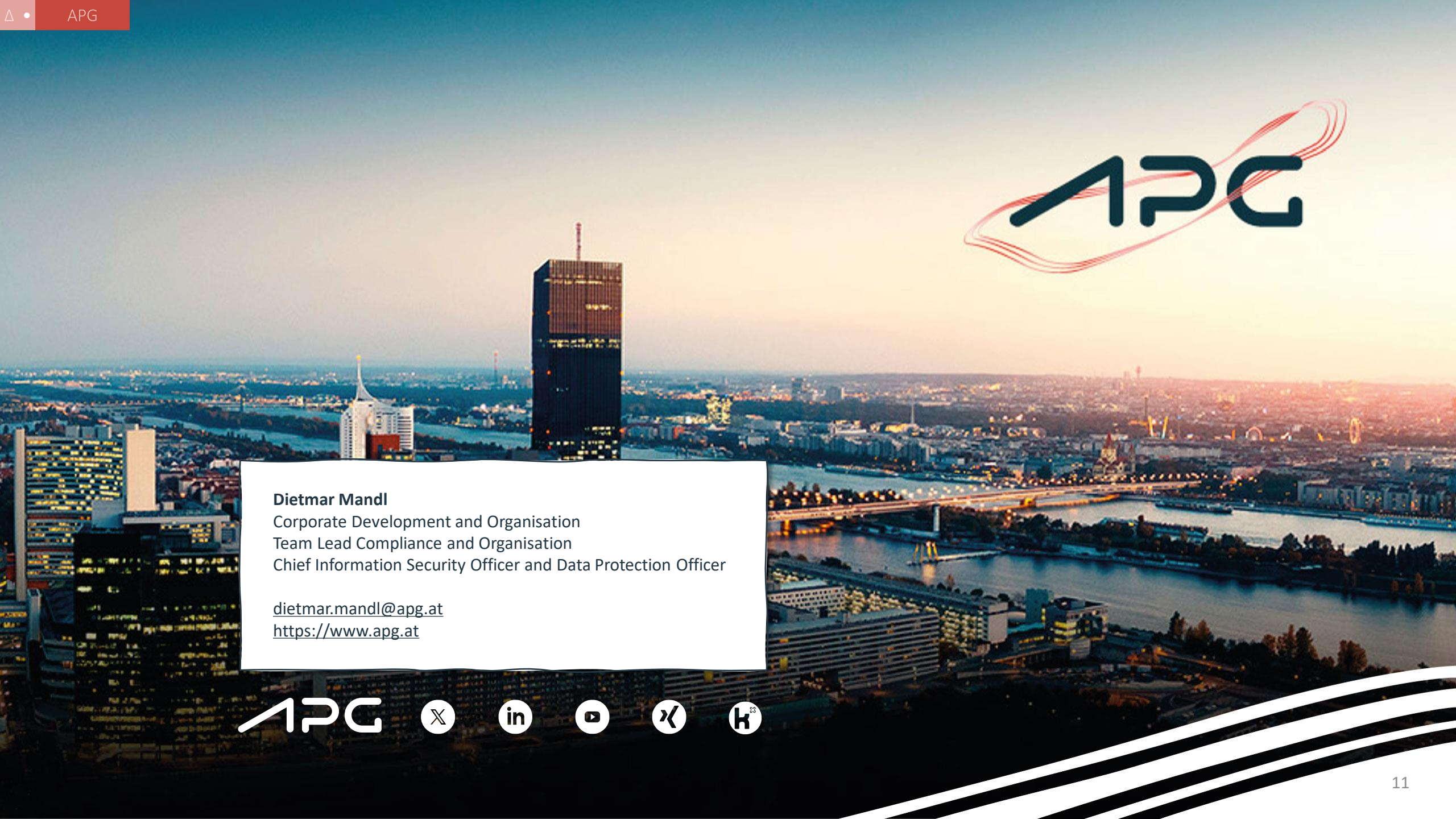
Ganzheitliches, interdisziplinäres Verständnis fördern – Business-Kontext!

Risikomanagement – Was ist wie wichtig für das Unternehmen? Priorisierung!

Basismaßnahmen umsetzen → Cyber-Hygiene!



Sicherheitsmaßnahmen bei Dienstleistern und Lieferanten berücksichtigen!



Dietmar Mandl
Corporate Development and Organisation
Team Lead Compliance and Organisation
Chief Information Security Officer and Data Protection Officer

dietmar.mandl@apg.at
https://www.apg.at