Cyber Security at E.ON:
Strategy, Execution & Outlook

Sebastian Weber – CIO E.ON

Playmaker of the Green Transformation

Employees

78.000

Customers

47M

Energy grids

1.6M

Kilometers

Investments

8.5B €

Connected renewable energy plants to E.ON Network

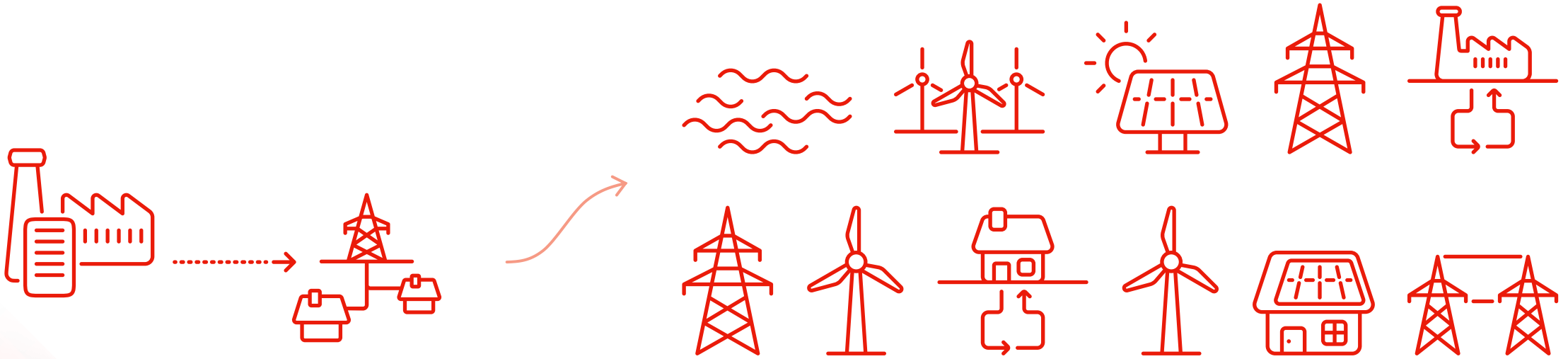
1.5M

Adjusted EBITDA

9.8B €

At a glance (financial year 2025)

IT Powers Green Transition in a Rapidly Transforming Energy World



Centralised
energy generation

Renewable
energy supply

Power Outages & Cyber Risks make digital Resilience crucial

e·on

Blackouts In Spain & Portugal Likely Caused By A Cyber Attack

Uploaded on 2025-04-29 in NEWS-Cybersecurity News, FREE TO VIEW, BUSINESS-Production-Utilities, BUSINESS-Production-Energy

A massive power outage struck the Iberian Peninsula on April 28, plunging millions of people into darkness as electricity supplies were suddenly cut across Spain and Portugal. According to Juanma Moreno, President of the Andalusian regional government, hostile activity by cyber criminals is the most likely cause of the blackout.

Portugal's grid operator, RNA, offered an alternative explanation for the massive power outage when it It blamed a rare atmospheric phenomenon which caused "oscillations" and "vibrations" in high power lines, which in turn resulted in "synchronisation failures" across the national grid.

It is unclear how such oscillations might have affected power supply across Spain.

Portuguese minister admits that a cyberattack could be behind the electricity blackout affecting Europe

PRESENT / INTERNATIONAL

AUTHOR: We Are Pueblo Media | April 28, 2025 | 3 min. reading

Power outage in Europe: The spectre of a cyberattack looms

Jacques Cheminat, published on 28 April 2025

Travel News

What caused the power outage in Prague? Latest updates after blackout hits European city – was it a cyber attack?

By Isabella Boneham
Reporter

Share Comment

Published 4th Jul 2025, 13:08 BST

Blackout in the heart of Europe: Accident or link in a chain of hybrid attacks?

EUROPEAN EXPERTS WEIGH IN ON CALIBER.AZ

Samir Ibrahimov

05 July 2025 17:00

The Czech Republic was hit by a blackout. Almost the entire country lost power, the country's fire and rescue service reported on July 4.

Spain and Portugal power outage: what caused it, and was there a cyber-attack?

Several countries in Europe have been scrambling to restore electricity after a huge power cut caused blackouts

Government of Spain does not completely rule out the hypothesis of cyberattack after blackout

April 30, 2025 / Cyberattack, Incident, Infrastructure

The Government suspects that a cyberattack on one of the companies in the sector caused the great electricity blackout in Spain

The Moncloa creates a special commission with Defence, the CNI and Ecological Transition to investigate the security of the entire electricity system, including the possibility of computer sabotage of one of the companies involved.

ALBA MOLINA WEDNESDAY, APRIL 30, 2025 Reading time: 2 min

Root cause research after blackout in Spain: Cyber attack as a possible cause?

05/08/2025, 05:19 AM

Spain, Portugal: power cut or cyberattack? Algeria on alert, is Morocco concerned?

Zineb Jazouli Posted in Hespress on 28 - 04 - 2025

OVERVIEW

Massive blackout in Spain: "They think it was a cyberattack" said a missionary based in Malaga

Daniela Oviedo April 30, 2025, 10:23 AM

NATIONAL

Can a cyberattack cause a blackout in Costa Rica?

See what a specialist says about this possibility, after Spain and Portugal suffered a massive power cut on April 28.

International

Historic blackout in Spain unleashes suspicions of cyberattack

By Eight Columns Apr 29, 2025

POWER OUTAGE: COULD A MASSIVE CYBERATTACK PLUNGE FRANCE INTO DARKNESS?

Théotim Raguet 29/04 at 17:20

Blackout: Madrid subway evacuated

Cyber attack? Massive power outage in Spain and Portugal

Total power outage in Spain: could it be a cyberattack?

Miharintsoa R. May 2, 2025 2 min read Hackers, Coffee Break

E.ON's Cyber Security Strategy

Building Cyber-Resilience is essential

- In a **digitalized** world **business, IT, OT, and cyber security** are **strongly intertwined.**
- **Cyber crime** models remain **attractive**.
- **Hackers** constantly **enhance capabilities** and make **use** of **AI**.
- Technical **vulnerabilities** and **people**'s trust are easiest to **exploit.**
- Secure working **anytime** from **anywhere** with **any device.**

Secure Growth, Sustainability & Digitalization

Enhance cyber security across the organization to secure Growth, Sustainability and Digitalization.

- Implement **Zero Trust**[1], **standardization** and a **reduced attack surface** as the non-negotiable foundation
- Increase efficiency through best practices based on **standards, automation and AI**

Empower people on cyber security

Build a culture where cyber security is **always considered**, and teams **deliver** secure solutions

- Reach the next level of **cyber security culture** by enabling **teams** in taking **end to end responsibility** for their products
- Deliver **secure solutions** with **excellent customer and user experience** and lean & effective processes

Strengthen cyber resilience

Efficiently manage cyber risks and **respond proactively** to emerging threats

- Foster **risk transparency** and **security hygiene** throughout business units and the supply chain
- Promote **continuous innovation** to strengthen our capability for **detection**, **response**, and **recovery**

We foster **standardization and automation at E.ON, empower teams**, and strengthen our **cyber resilience** together.

[1] Zero Trust is a security model that assumes breach of our systems and relies on the principle "never trust, always verify"

Myth #1

More tools and platforms strengthen our security posture

Myth #2

Our operational environment (OT) is safe, because it is largely isolated

Myth #3

Cyber risk is driven primarily by highly sophisticated actors

Myth #4

Cyber incidents primarily affect data

Myth #5

We can prevent cyber incidents

Future Trends to Prepare for already TODAY

Architecture

AI, AgenticAI etc. require security by-design for extreme scenarios

Threat Landscape

Geopolitics drive AI-powered, state-level cyber threats

Quantum Encryption

Today's crypto will break – quantum safe is essential

Automation

AI speeds up both attacks & defense

Fake Identity

AI fuels deepfakes & identity abuse

LLMs

AI accountable for detection, protection, and response

Thank you!

Q&A