Insights from the Cybersecurity in Austria – September 2024

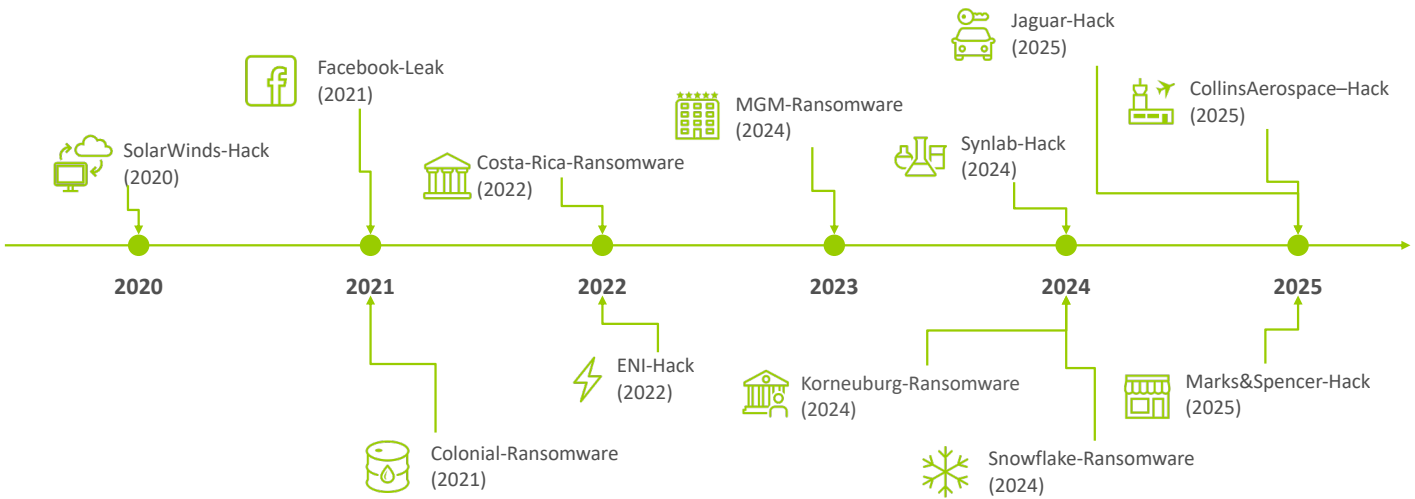
Dr. Alexander Andreas Schierhuber, CEO

VOR
DER VERKEHRSVERBUND

Overview Cybersecurity

VOR
DER VERKEHRSVERBUND

Overview of current cyber attacks



VOR
DER VERKEHRSVERBUND

Source: Die Bedeutung von Informationssicherheit für resiliente Organisationen, accilium

Overview of selected information security threat scenarios

Data breach

An unauthorized access to sensitive data such as PII, financial, or corporate information through theft, viewing, or disclosure.

Espionage / Sabotage

Espionage involves obtaining confidential information for competitive or strategic advantage. Sabotage deliberately disrupts operations to cause damage.

Malware / Ransomware

Malicious software that disrupts systems, steals data, or attacks IT infrastructures – e.g., viruses or Trojans.

Social Engineering

Manipulation of people by exploiting trust or fear to obtain confidential information or system access.

Availability of security tools and services

Failure of digital services or applications that disrupts or limits critical business processes.

Availability of physical Infrastructures

Failure of critical facilities such as power supply or data centers, impairing or halting essential services.

VOR
DER VERKEHRSVERBUND

Source: Die Bedeutung von Informationssicherheit für resiliente Organisationen, accilium

Data breach

Definition:

A data compromise is a security incident in which data is accessed or disclosed by unauthorized individuals or groups due to human error, insecure transmission paths, or targeted theft. This often involves personal data (PII), company information, financial data, or other sensitive materials.

Current cases:

Facebook-Leak (2021)

GIS-Data leak (2020)

How can this happen?

- **Negligence & Unawareness:** Accidental sending to the wrong recipients or unintentional forwarding of sensitive data
- **Incorrect Access Rights:** Overly broad, not deleted, or unclear permissions
- **Insecure Data Processing:** Mixing of data from different utilities or errors in processing workflows
- **Insecure Data Transmission:** Insecure cloud links or communication tools
- **Manipulation & Physical Risks:** Social engineering, sharing of accesses, unsecured printouts or USB sticks

Possible impacts?

- **Disclosure of confidential information:** Sensitive data becomes public or falls into the wrong hands
- **Reputation and trust loss:** Damage to image, loss of customer trust
- **Legal and financial consequences:** Claims for damages from customers or third parties as well as possible fines
- **Loss of contracts or clients:** Risk of losing legal mandates

VOR DER VERKEHRSVERBUND

Source: Die Bedeutung von Informationssicherheit für resiliente Organisationen, accilium

Espionage / Sabotage

Definition:
Espionage is the acquisition of secret or confidential information from undisclosed sources or its disclosure with the aim of gaining a (business) advantage.
Sabotage is the deliberate disruption or obstruction of the proper functioning of a process or activity, or the use of necessary means to cause damage.

Current cases:

OMV [OMV-Espionage (2025)]

[Tesla-Sabotage (2024)]

How can this happen?

- **Physical access:**
  Careless external parties (e.g., cleaning staff, visitors) or open offices allow access to documents and devices
- **Insiders & information leaks:**
  Employees or external parties with malicious intent pass on confidential data or take documents
- **Insecure networks & devices:**
  Public Wi-Fi, compromised smartphones, or insecure online meetings
- **Organizational weaknesses:**
  Incorrect permissions, losing access data, or unsecured communication channels make systems vulnerable

Possible impacts?

- **Disclosure of confidential information:**
  Business secrets become public, sensitive data is intercepted or stolen
- **Incorrect decision-making basis:**
  Manipulated or incomplete information leads to wrong decisions
- **Financial & legal impacts:**
  Claims for damages, financial losses, and legal consequences
- **Reputation & competitive disadvantage:**
  Loss of trust, long-term image damage, and loss of contracts

VOR DER VERKEHRSVERBUND

Source: Die Bedeutung von Informationssicherheit für resiliente Organisationen, accilium

Malware / Ransomware

Definition:
Malware is malicious software designed to damage systems, steal data, or disrupt IT systems. It is an umbrella term for many types of threats, such as viruses and Trojans.
Ransomeware is a type of Malware with aim of blackmailing the users. The Software encrypts files or blocks access to systems, and attackers demand ransom to restore access.

Current cases:

Jaguar-Hack (2025)

Ransomware Korneuburg (2024)

How can this happen?

- **Links and attachments:** Malware delivered via malicious links, newsletters, or infected attachments
- **Removable media & devices:** USB sticks or unsecured company laptops can be used as entry points
- **Insecure networks:** Public Wi-Fi or unsecured Bluetooth connections allow external attacks
- **Apps & Websites:** Manipulated apps, pop-ups or visiting insecure websits allow ransomware to enter
- **Insider & Exploits:** Employees with malicious intent or targeted 0-day exploits compromise systems

Possible impacts?

- **Loss of data & information:** Leakage, theft, manipulation, or complete loss of sensitive data
- **Operational disruption:** Work stoppage, system lockouts, or blocked important processes
- **Financial damage:** Ransom payments, incorrect financial transactions, or additional costs
- **Reputation & trust damage:** Long-term image damage, loss of trust from customers and partners, loss of contracts

VOR DER VERKEHRSVERBUND

Source: Die Bedeutung von Informationssicherheit für resiliente Organisationen, accilium

Social Engineering

Definition:
Social engineering exploits human traits such as helpfulness, trust, fear, or respect for authority to manipulate individuals. Criminals trick victims into revealing confidential information, bypassing security functions, making transfers, or installing malware on corporate systems.

Current cases:

AI - Phone fraud (2025)

Payment fraud Hagenbrunn (2025)

How can this happen?

- **Manipulation via personal contacts:** Threats to close relatives, fake friendships, or fake networking at events
- **Authority impersonation:** Exploiting power dynamics or authority positions
- **Baiting & luring:** Baiting through supposed profits with the aim of gaining advantages
- **Pretexting & Blackmailing:** Exercising emotional pressure through pretexting or physical blackmailing

Possible impacts?

- **Financial damage:** Unauthorized transfers, contract cancellations, or additional costs
- **Disclosure of confidential information:** Data leaks, privacy breaches, or release of sensitive information
- **Reputation & trust loss:** Long-term image damage, loss of trust from customers and partners
- **Manipulation & unfair advantage:** Influence on decisions or unequal information benefits

VOR
DER VERKEHRSVERBUND

Source: Die Bedeutung von Informationssicherheit für resiliente Organisationen, accilium

Availability of security tools and services

Definition:

An availability interruption occurs when essential digital applications, software tools, or IT services (e.g., communication platforms, databases, or operational applications) fail completely or partially, restricting the use or provision of critical functions. Such interruptions can significantly impact business continuity.

Current cases:

Microsoft-Outage (2024)

Hospital IT-Outage (2025)

How can this happen?

- **Technical Blackout:** Server, cloud, or database outages (e.g., MS Server, Office 365) prevent access to critical applications
- **IT problems & incompatibilities:** Software errors, system updates, compatibility problem or interface issues hinder the operation
- **External providers & banks:** Partner issues, telebanking outages, or cyberattacks on service providers can disrupt the services
- **Sabotage or misconfiguration:** Malware attacks, intentional shutdowns, or errors can block the system

Possible impacts?

- **Payment & financial disruptions:** Payments to suppliers or employees cannot be processed
- **Operational & process disruptions:** Delays in ongoing business processes
- **Reputation damage:** Outage can lead loss of trust among partners and customers
- **Decision-making limitations:** Lack of access to critical tools or data hinders strategic and operational decisions

VOR DER VERKEHRSVERBUND

Source: Die Bedeutung von Informationssicherheit für resiliente Organisationen, accilium

Availability of physical Infrastructures

Definition:

An availability interruption of physical infrastructure occurs when critical systems (e.g., power supply, data centers, production facilities) fail, disrupting essential services. Under NIS2, this is considered a security-relevant incident as it threatens the continuity of critical services.

Current cases:

Heathrow Shutdown - Fire (2025)

Pipeline-Shutdown (2021)

Wie kann es dazu kommen?

- **Fires, explosions, and bomb threats:** Physical damage from fire, terrorism, or explosions directly affect facilities and systems
- **Supply failures:** Blackouts, defective cooling, or water damage lead shutdown of the operation
- **Natural & environmental events:** Earthquakes, floods, or storms disrupt process
- **Traffic & access disruptions:** Protests, physical damage, or blocked access routes

Possible impacts?

- **Operational disruption & productivity loss:** Work stoppages, delays, and dependency on remote work
- **Technical limitations:** Restricted access to systems, data centers, or devices
- **Economic consequences:** High costs, production losses, and financial disadvantages
- **Reputation & trust loss:** Negative public perception and long-term image damage

VOR DER VERKEHRSVERBUND

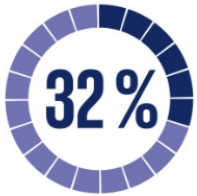
Source: Die Bedeutung von Informationssicherheit für resiliente Organisationen, accilium

Cybersecurity Incident Statistics in Austria

VOR
DER VERKEHRSVERBUND

1 in 7 cyberattacks in Austria is successful.

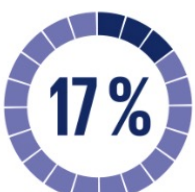
Over 28% of cyberattacks are linked to state-sponsored actors



One in three companies experienced cyberattacks on their suppliers or service providers that had a substantial impact on their own operations

In 62% of cases, cyberattacks were identified by employees before being detected by technical systems or solutions

10% of social engineering attacks now involve deepfake-based voice and video content.



Only 17% of respondents believe AI has improved cybersecurity — suggesting that its potential is still far from being fully realized

55% of respondents say that Austria is inadequately prepared to handle major cyberattacks on its critical infrastructure

60% of respondents would prefer security solutions from Austrian providers, marking a 23% increase over the previous year

VOR
DER VERKEHRSVERBUND

› Source: Survey conducted with Austria's leading enterprises: KPMG Cybersecurity in Österreich 2025

Critical Cyber Incidents Affecting Austrian Public Services - Heavy rain event in September 2024

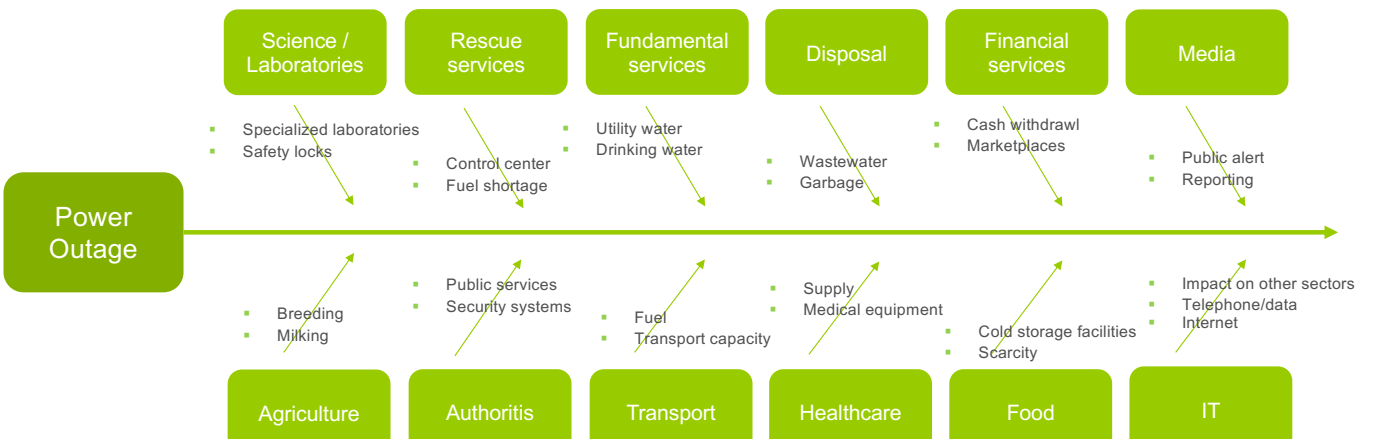
VOR
DER VERKEHRSVERBUND

Heavy rain event in September 2024
“Thousands without power, hundreds without heat”

VOR
DER VERKEHRSVERBUND

Source: Tausende ohne Strom, Hunderte ohne Wärme - noe.ORF.at

Power outages can restrict access to cyber infrastructure, affecting multiple areas of operation



VOR
DER VERKEHRSVERBUND

Source: Risiken und Herausforderungen für die öffentliche Sicherhiet in Deutschland, S. 22

Cybersecurity Risks Associated with Heavy Rain Events

-> While no direct cyberattacks have been reported as a result of the flooding itself, access restrictions to cyber infrastructure have been observed, which could potentially increase the risk of cyberattacks.

-> Heavy rain event in September 2024 highlighted the importance and necessity of proactive cybersecurity

VOR
DER VERKEHRSVERBUND

Another cybersecurity incident also occurred in September 2024

VOR
DER VERKEHRSVERBUND

Cyber attacks (DDoS) targeting the Austrian elections

When? – 16-20. September 2024

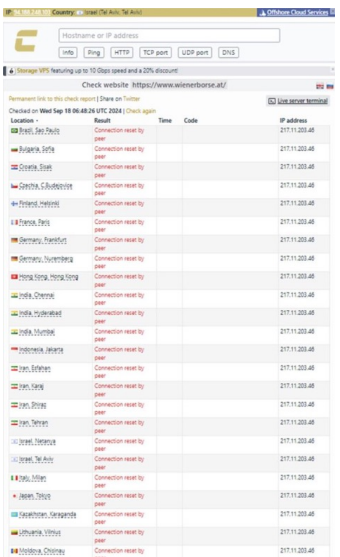
Who were behind?

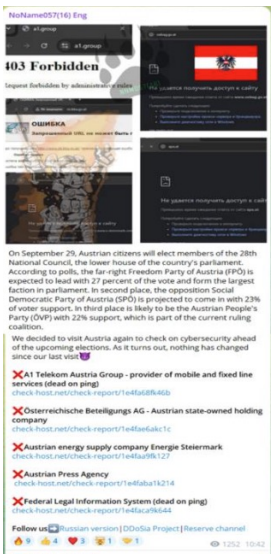
- NoName057(16)
- OverFlame

➔ These pro-russian hacker groups are known for targeting countries that support Ukraine.

Targets of attacks:

- Austrian government websites
- Airports
- Financial institutions
- Political parties e.g. ÖVP, SPÖ, FPÖ





Source: Pro-Russian Hacktivists Target Organizations in Austria With DDoS Attack Campaign

Impact of Cyber Attacks on the Austrian Election

- The cyber attacks aimed to create confusion before the election

- However, they had no direct impact on the election results
- Austria's electoral system remained secure and resilient

-> Nevertheless, the incidents highlighted vulnerabilities in digital infrastructure and the growing threat of politically motivated cyber attacks

VOR
DER VERKEHRSVERBUND

DDoS Attacks also affected VOR (Verkehrsverbund Ost-Region) and our Response Measures taken

Initial attack (September 2024):

- Website temporarily inaccessible due to DDoS.
- Geo-blocking activated: access limited to Austria.
- Full global access restored after 2 days.

Observed attack types :
SYN-Flood, ACK / SYN

Second Attack (Nov 2024):

- Targeted external IP address.
- New IP provided by hosting provider (Abaton).
- Attack neutralized without further geo-blocking.

Ongoing Protection (Since Janurary 2025):

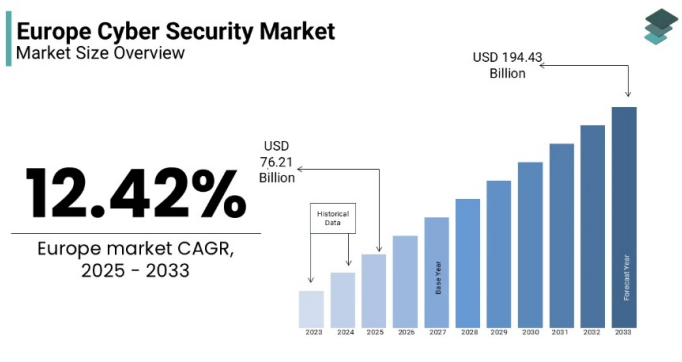
- Additional DDoS protection active.
- Automated traffic filtering ensures long-term availability.

VOR
DER VERKEHRSVERBUND

Cybersecurity Efforts and Challenges in Austria

- **Government-Level Response**
  Joint Cybersecurity Center operated collaboratively by various government agencies
- **Growing Market**
  Cybersecurity market projected to reach USD 745 million by 2028
- **Focus on Public Sector**
  Strong awareness and investment from large enterprises and government institutions
- **Challenges**
  Only 20% of companies with 50+ employees have an emergency cyber response plan

  -> Need for regulations and support to increase preparedness



Source: Austria - Cyber Security, Austrian Strategy for Cybersecurity 2021

Thank you!

Verkehrsverbund Ost-Region (VOR) GmbH
Management für Wien, Niederösterreich und Burgenland.
Europaplatz 3/3
A-1150 Wien

VOR
DER VERKEHRSVERBUND