Federal Chancellery

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Cyber Communities in Action

A Strategic Cyber Security Simulation Game

Maria Leitner, AIT
Timea Pahi, AIT

Background

- → Strategic cyber simulation game
- → Preparation for cyber conference in December 2018
- → Simulation of strategic decision making processes

Start

- → Grab your phone, tablet or laptop
- → Go to menti.com
- → Enter the code
- → Ready, Steady, Go!

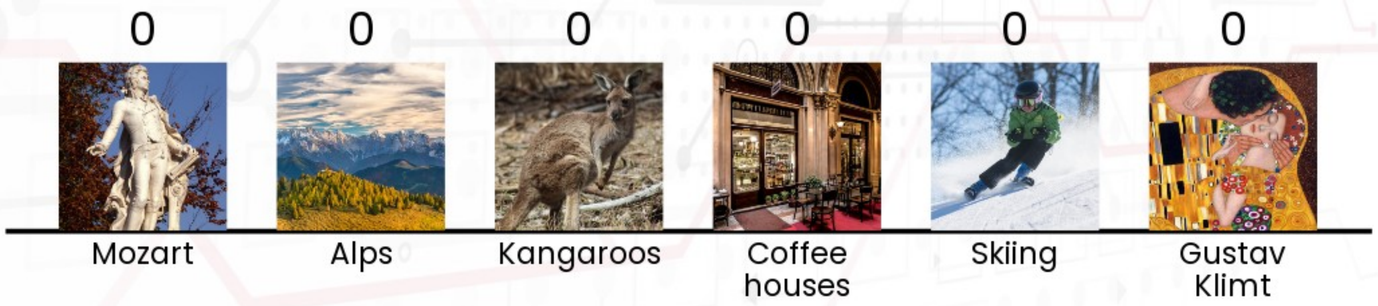
Interaction in the Game

- Select answers with your tablet, phone or laptop
- Discuss the questions with your neighbours
- Make a careful decision
- You cannot change your answer

What do you associate most with Austria?

Federal Chancellery

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY



How many minutes do you usually spend in social media per day?

Federal Chancellery

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

- Less than 1 hour
- Between 1 and 2 hours
- More than 2 and less then 4 hours
- More than 4 hours

Who is the conference organizer of this conference?

0	0	0
Austrian federal chancellery	Federal ministry the interior	Ministry of defence

Let's start the simulation game!

Please select the stakeholder group that you can associate yourself most of the time?

Federal Chancellery

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

- Government
- Industry
- Academia, research & development

Please select the cyber community that you can associate yourself most of the time?

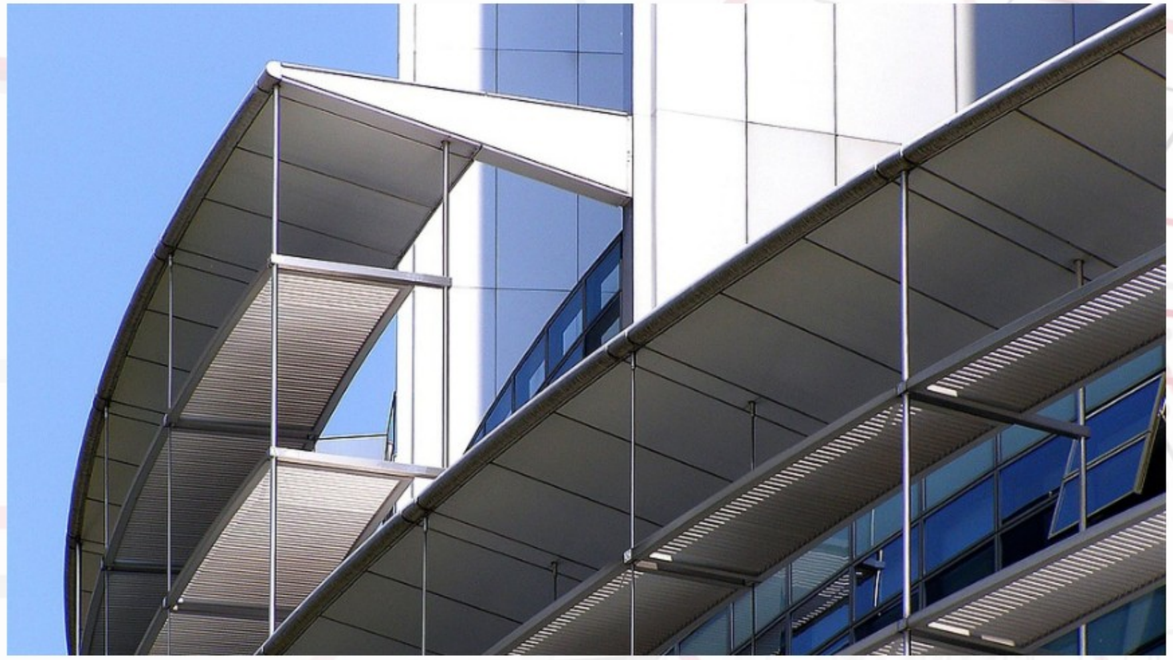
Federal Chancellery

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

- Security
- Defence
- Justice in cyber space / crime
- Diplomacy / policies

Wasnela

- EU-member country since 1958 / Schengen area member since 1995
- Official EU languages: Wasnelian / English
- Size: 126 000 km2
- Population: 7 million
- GDP: 86 PPS
- Geography: Mountains with rivers (e.g. Ebune)
- Energy supply: Wasnela has 4 main energy providers. Main energy source are hydropower plants.



Wasnelian National NIS Authority

- Sector: Public Authority
- Security Level: High
- Incident Team: Yes
- Critical Infrastructure: Yes
- Securing governments systems
- Supporting critical infrastructures

Wasnela Energy Ltd.

- Sector: Energy
- Security Level: Low-Middle
- Incident Team: No
- Critical Infrastructure: Yes
- Responsible for the Holper Run-of-River hydroelectric generation plant

Infrastructure of Wasnela Energy Ltd

- The Holper power plant was built between 1959 and 1964 and was the second power plant built along the Ebune.
- Power plant damps up the Ebune 15 meter high and has the highest drop height of all Wasnelian power plants on the Ebune
- After 40 years in operation, it took 4 years to renovate the main engine from 2006 to 2010

Personnel at Wasnela Energy Ltd

- → 250 employees
- → IT team has 15 team members
- → 3 team members where just recently recruited
- → 4 members will retire soon

As a CISO of Wasnela Energy What would be an optimal size for a cyber security team?

Federal Chancellery
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

- 1-10 members
- 11-20 members
- 21-30 members
- 31 or more members

Investing in Capabilities

- The management of Wasnela Energy Ltd has acknowledged the need for cyber security
- A budget for 2019 was defined specifically for cyber security capacities
- The company reserved a budget of approx. 100,000 EUR (100%) for cyber security
- As the CISO of Wasnela Energy Ltd, you can decide about the investments

How would you allocate the investments?

Federal Chancellery

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

0%	Training and education of IT team (e.g., certifications)
0%	IT security awareness campaigns
0%	Software to extend network security, application security (e.g., IDS, firewalls, threat intelligence)
0%	External consulting and audit of IT security measures
0%	Cyber security exercises and testing of contingency plans
0%	Start certification of organization based on ISO 27000
0%	Hiring personnel for IT department and IT security
0%	Outsourcing specific cyber security services and responsibilities

Which topics of training would you be interested?

Federal Chancellery

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

- IT management standards (e.g., ISO 27000, ITIL, Cobit, CISM, CISSP)
- Technical vendor-specific training (e.g. firewalls, threat intelligence)
- Ethical hacking, penetration testing
- IT security awareness training
- Privacy and data protection

Incident Reporting

- The IT team of the Holper power plant finds an obvious anomaly within their system
- It turns out to be a Remote Access Trojan (RAT) Software already building connection with their Command and Control server
- The team informs the CISO
- The IT team detected an effective phishing campaign targeting the office staff

As CISO you have to report the incident to the management. How would you explain a Remote Access Trojan (RAT)?

Federal Chancellery

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

0	0	0	0
An attempt to trick someone into giving information over the internet.	A software that gives a person full control over a tech device remotely.	An attack in which multiple compromised computer systems attack a target.	A rogue wireless access point that masquerades as a legitimate Wi-Fi access point.

Situation Assessment

- After an investigation of the IT team has categorized the incident with low criticality
- The intrusion affected mainly the office department (5 laptops)
- There was no confidential information on customers or personal data of employees.
- No systems were affected in the OT network

As the CISO of Wasnela Energy Ltd, how would you assess the current situation?

Federal Chancellery

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

- Information (no further activity needed)
- Notice (normal but significant conditions)
- Warning (warning conditions)
- Error (error conditions)
- Critical (critical conditions)
- Alert (action must be taken immediately)
- Emergency (system is unusable)

As CISO, which information sharing policy would you recommend at this point?

Federal Chancellery

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Please select the stakeholder group that you can associate yourself most of the time?

- Government
- Industry
- Academia, research & development

0	0	0
Only internal information sharing	Informal information sharing	Formal information sharing

As CISO, which incident information would you recommend sharing at this point?

Federal Chancellery
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

0	0	0	0	0	0
Name of organisation	Sector	Incident information (e.g., state, services)	Technical incident information (e.g., IPs, logs)	Measures	Impact

Please select the cyber community that you can associate yourself most of the time?

- Security
- Defence
- Justice in cyber space / crime
- Diplomacy / policies

Where would you request information (such as Indicators of Compromises) or help for cyber incidents outside of your organization?

Federal Chancellery

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

0
Only internal requests or help

0
Trusted industry partners, consulting firms, trust circles

0
National or sector-specific CSIRTs

0
National NIS authority

0
National data protection authority

0
CSIRTs network

0
ENISA

0
European Cyber PPP

0
NIS Cooperation Group

Reorganizing Budget & Investments

- The local press received information about the attack on Wasnela Energy Ltd and begins to speculate immediately
- The management board expects fast answers on novel long-term solutions to prevent cyber attacks
- As CISO, you decide to reallocate the budget for cyber security

After the incident, has your vision on cyber security investments shifted? Which capacities would you require?

Federal Chancellery

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Please select the stakeholder group that you can associate yourself most of the time?

- Government
- Industry
- Academia, research & development

Supplier Selection based on Labels and Certifications

- As CISO you decided to invest mainly in software
- Your team informs you that there are several tools to discover and eliminate the malicious RAT of the incident
- Cost for licenses vary slightly but maintenance costs are similar for all
- Your return on investment would at least be 25.000 EUR in the first year

As CISO and IT team, which software would you most likely select?

Federal Chancellery

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Extremely unlikely

"DelRAT", Open source, is actively supported in communities (LC: 0 EUR).

Software "NewGEN" by a well-known German small enterprise. Has the label with EU cybersecurity assurance level substantial (LC: 5000 EUR).

Software "STARK", by well-known global Canadian software manufacturer with high reputation (LC: 3500 EUR).

Software "GENX" from Japanese software start-up. The product owner is not well known, with EU cybersecurity assurance level high (LC:500 EUR).

Extremely likely

Assessment and Prioritizing

- The Wasnela Energy Ltd informs the national NIS authority about the incident
- Wasnela's national NIS authority is closely linked to the national CSIRT
- It aims to supervise governmental systems and national critical infrastructures
- The CSIRT has the common responsibilities as described by ENISA

As the national CSIRT or NIS authority, how would you categorize the current situation?

Federal Chancellery

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

0	0	0	0	0	0	0
Daily business	Incident with minor impact	Incident with substantial impact	Incident with significant impact	National crises	Cross-border cyber incident and/or crises	International crises

As NIS authority, which measures and recommendations would you suggest in this situation?

Federal Chancellery

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Establish a national incident information sharing platform	Provide technical support to affected organisations	Establish a national energy CSIRT	Start a national cyber task force	Establish a national crises management	Contact partners with cyber diplomacy	Develop a long-term cyber security strategy	No activity
0	0	0	0	0	0	0	0

Please select the cyber community that you can associate yourself most of the time?

- Security
- Defence
- Justice in cyber space / crime
- Diplomacy / policies

Federal Chancellery

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Thank You for inputs and recommendations.
Wasnela has established a national task force on cyber security.
Wasnela is establishing long-term strategies for cyber security.

Questions?

Recap and review

Federal Chancellery

Thank You for Your participation

Maria Leitner
AIT Austrian Institute of Technology
maria.leitner@ait.ac.at