Cyber Attack in ELI Beamlines

Birgit Ploetzeneder

Context

CYBERATTACK IN ELI BEAMLINES

On 28.03.2023 ELI Beamlines experienced a **sophisticated ransomware attack**.
It exploited misused credentials of an employee.

OPERATIONAL IMPACT

- ca 350 servers + work stations encrypted
- 2 weeks with limited operations, some delays of commissioning activities
- No direct impact on operational technology (network segregation was sufficient)

DATA IMPACT

- no evidence of data exfiltration found
- some loss of data (administrative, designs, simulations)

FINANCIAL IMPACT

- Post Incident-Measures: 260kEUR
- Midterm Measures: 270kEUR
- Long-Term Strategy Implementation: 500kEUR

Lessons Learned

PHASE	COMMON EXPERIENCE	FACILITY EXAMPLE
PRE-ATTACK	• Threat Landscape significantly changed: Frequency of attacks highly increased, sophisticated threat actors (state actors / commercial groups) 1	• ELI Beamlines is 1 of 4 major (known) Big Physics facilities victimized in 2023 • Attack pattern associated with known hacker group
INTRUSION / LATENT PHASE	• often months before attack based on stolen credentials • 2010s best practices are insufficient at detection 2	• 19 out of 21 antivirus softwares failed to detect mechanism – typical for current ransomware 3
ACUTE ATTACK	• Activation often overnight; detection early morning • Accepting ransom demands has 30-60% success rate: but leads to revictimization in 80% of cases within 1 month	• Attack between 1-5am; first detection at ca 6:30am • Ransom demand: Non-option

1 Consider ability to prevent limited; invest in **business continuity.** Ensure **backup resilience** and **segregation sufficiency**.

2 Highlight importance of proactive cybersecurity, **adaptability to evolving threats, skills development**

3 Invest in state-of-the-art **forensic capabilities**

eli

Data Sources: ENISA, T-Mobile/Telekom Security Cross Border Services

Lessons Learned

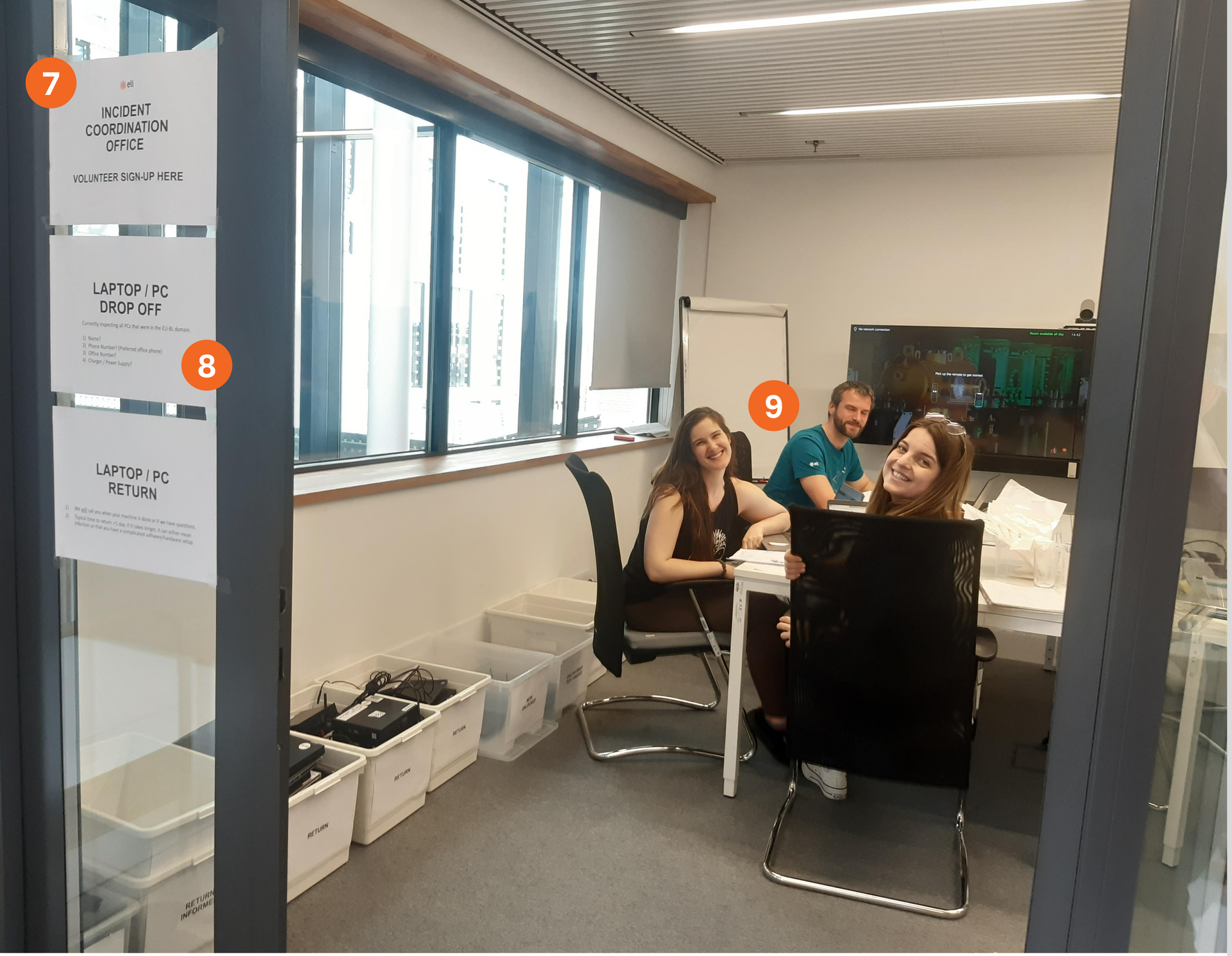
PHASE	COMMON EXPERIENCE	FACILITY EXAMPLE
CRITICAL RESPONSE	• Rapid response required to contain and reduce damage • Engagement of external expertise – rarely on-site staffing capacity and expertise (5) • Obtaining situational overview and ensuring containment is challenging, shows limitations and gaps in documentation	• Shutdown of facility operations started within minutes of detection. (4) • On-site external response team at ca 10:00am • Relatively smooth division of labor between laser/office building; still: “there’s systems we didn’t know we had..” (6)
RECOVERY	• Typical process follows the establishment of detection / disinfection capabilities and a “clean / safe” new infrastructure, and then transfer of all systems into it. • Phase is characterized by serious capacity gaps	• XDR (Extended Detection and Response) Solution – Crowdstrike – was chosen and implemented • Detailed Recovery Plan established on day 3 and executed.

Data Sources: ENISA, T-Mobile/Telekom Security Cross Border Services

4 Given prevalence of early-morning detections and potential absence of escalation mechanisms, **ensure IT staff can shut down operations**.

5 Retain **potential incident support in advance,** invaluable also for process advisory

6 Ensure **reasonable quality of asset management**, documentation of **critical network connections**, **policy on non-IT provided ICT equipment**.



7 **Communications and coordination plans** are critical part of preparedness – consider unavailability of networks, mailservers,..

8 Rapid recovery depends on **mechanisms to scale and distribute solutions** (1000s of computers to scan, 100s to reinstall).

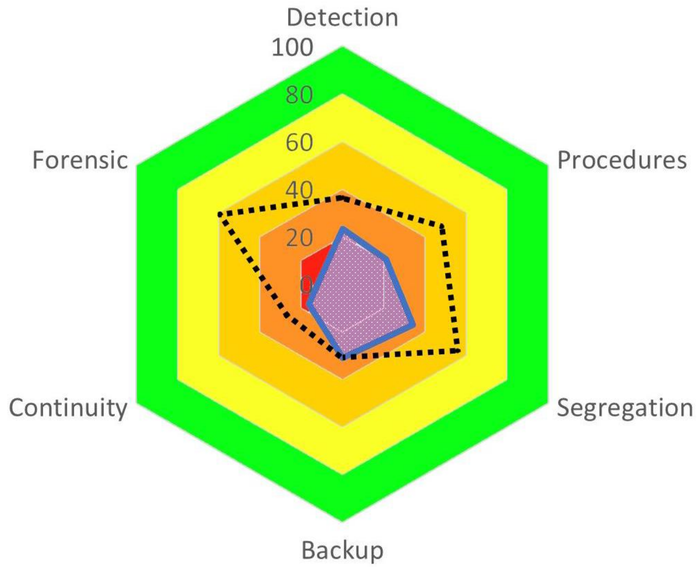
9 **Involvement of non-IT staff** significantly accelerates recovery

Post-Incident Measures

AUDIT FOCUSED ON 6 KEY ASPECTS

- Detection Capabilities
- Incident Management Procedures
- Segregation Sufficiency
- Backup Resilience
- Business Continuity Measures
- Forensic Capabilities

Engagement of 4 certified experts who in past executed CISO/CSO role



RECOMMENDATIONS

- Improve Cyberattack Detection
- Strengthen Continuity Management
- Enhance Backup and Incident Response
- Strengthen Segregation and Forensic Capabilities

Definition of security baselines and mid-term and long-term strategy

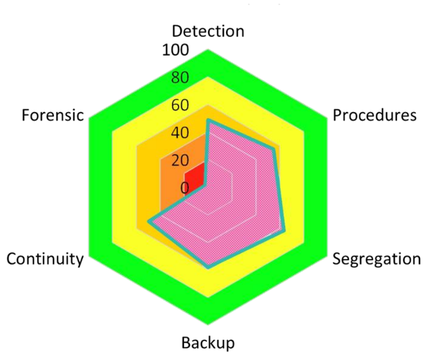
eli

Post-Incident Measures

SECURITY BASELINE

reasonable level of assurance that reoccurrence is prevented

- EDR + EDR Alert System
- Policy Development
- Finalization of pre-incident security technologies
- Active Directory Hardening
- Immutable backup using available on-site solutions
- Log and Patch Management

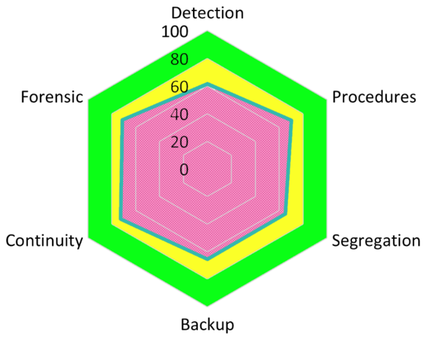


Cost incl. response: 260kEUR

MID-TERM MEASURES

reasonable level of security established

- Security Operation Center (SOC) Implementation
- Infrastructure Hardening
- Certification Authority
- Help Desk & Asset Management improvements
- Data Offsite Backup Phase 1
- Multi-factor authentication

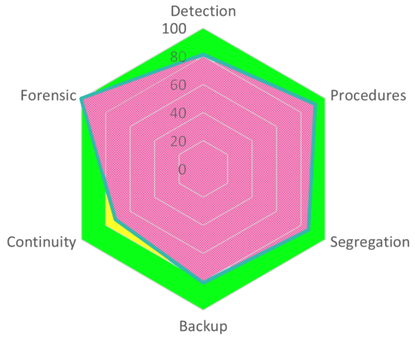


Expected cost: 270kEUR

LONG-TERM STRATEGY

long-term sustainable cybersecurity maturity level

- Identity Management
- System Measures (Cybersecurity, Business Continuity, Disaster Recovery)
- SIEM (Security Information and Event Management)
- Net-Traffic Probes
- Data Offsite Backup Phase 2
- CISO Role



Expected cost: 500kEUR

Conclusion and Key Recommendations

CONCLUSION

The security environment around us has changed, and it is necessary to respond to it.

KEY INSIGHT

- Cost and risk of cyberattacks are significant.
- This requires pro-active response with focus on adaptability to evolving threats.

RECOMMENDED ACTIONS

Implement security strategy with focus on 6 areas:

- Detection Capabilities
- Incident Management Procedures
- Segregation Sufficiency
- Backup Resilience
- Business Continuity Measures
- Forensic Capabilities