



# **Anatomy of a ransomware attack**

## The role of governance

# Speaker

Laurent Deheyner

CISM® CDPSE®

**Director**

**Head of SOC services**

Approach Belgium





# **Anatomy of a ransomware attack**

## **The role of Governance**

- CSIRT use case
- Facts
- Key takeaways
- Conclusion

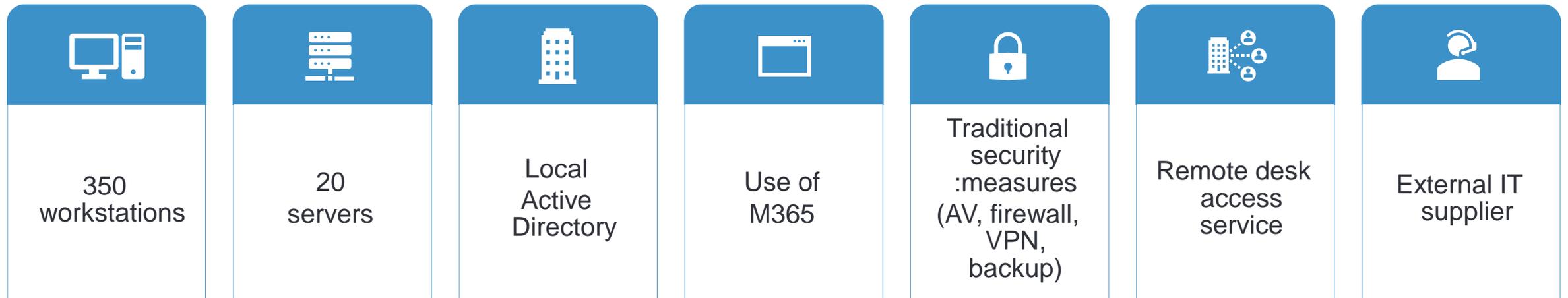


# **CSIRT use case**

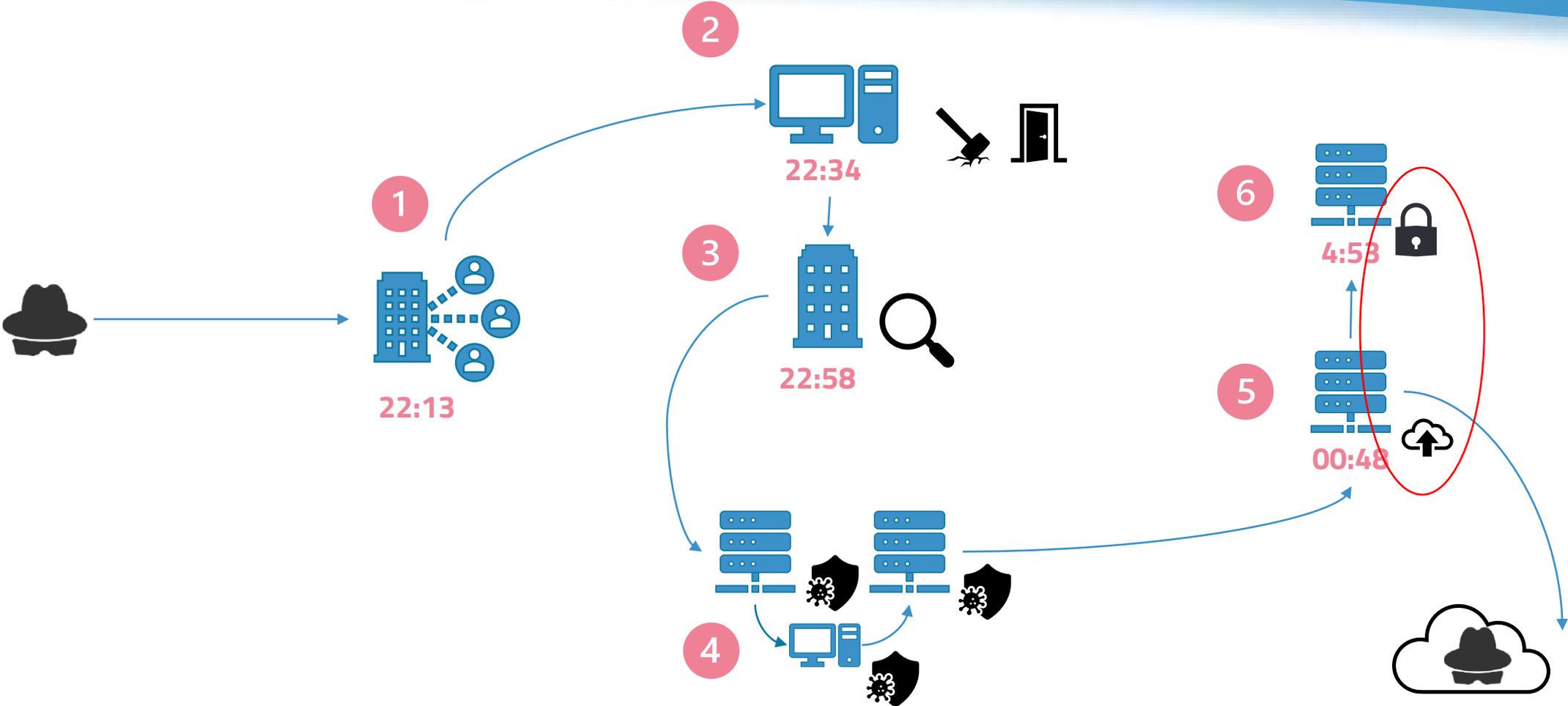
## Ransomware

# CSIRT use case: ransomware

## Context of the victim organisation

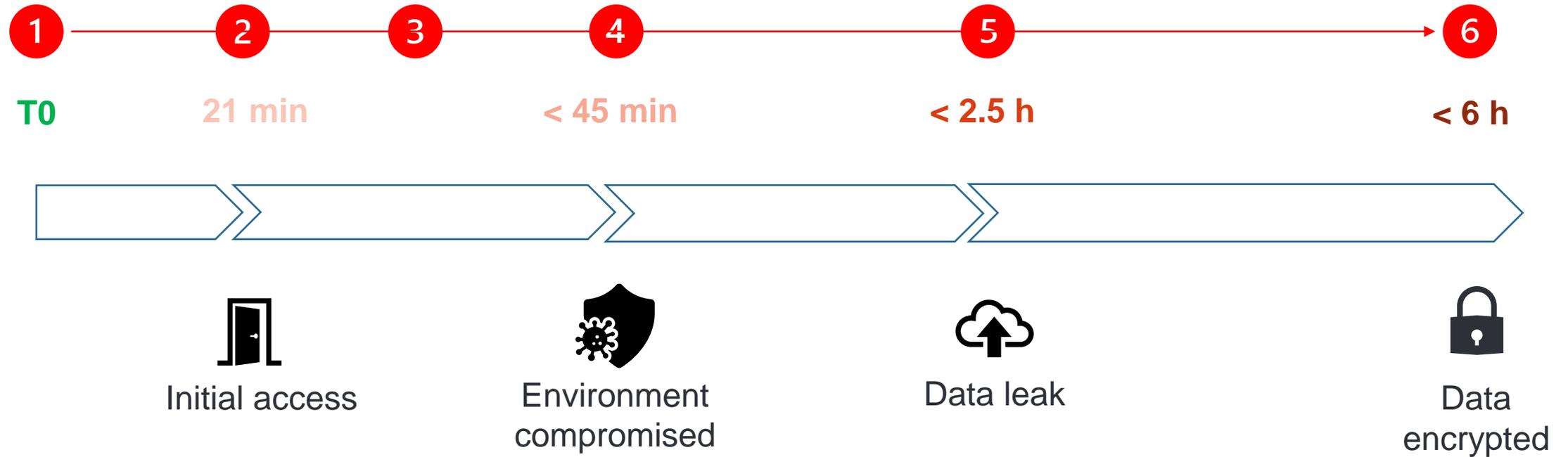


# What happened



# Analysis

## FACT N°1: The timeline



# CSIRT use case: ransomware

Fact N°2: Initial access

No artefacts explaining initial access and privilege escalation.

Potentially:

- Identifier theft
- Brute force
- CVE exploitation

*In 95.3% of the incidents, it is not known how threat actors obtained initial access into the target organization\**

\*ENISA THREAT LANDSCAPE FOR RANSOMWARE ATTACKS July 2022

# CSIRT use case: ransomware

## Fact N°3: Ransomware scenario

Assets	Lock	Encrypt	Delete	Steal
Files	✗	✓	✓	✓
Memory	✗	✓	✓	✓
Folders	✗	✓	✓	✓
Database Content	✗	✓	✓	✓
MFT	✓	✓	✓	✗
MBR	✓	✓	✓	✗
Cloud	✗	✓	✓	✓
CMS	✗	✓	✓	✗
Screen	✓	✓	✓	✗



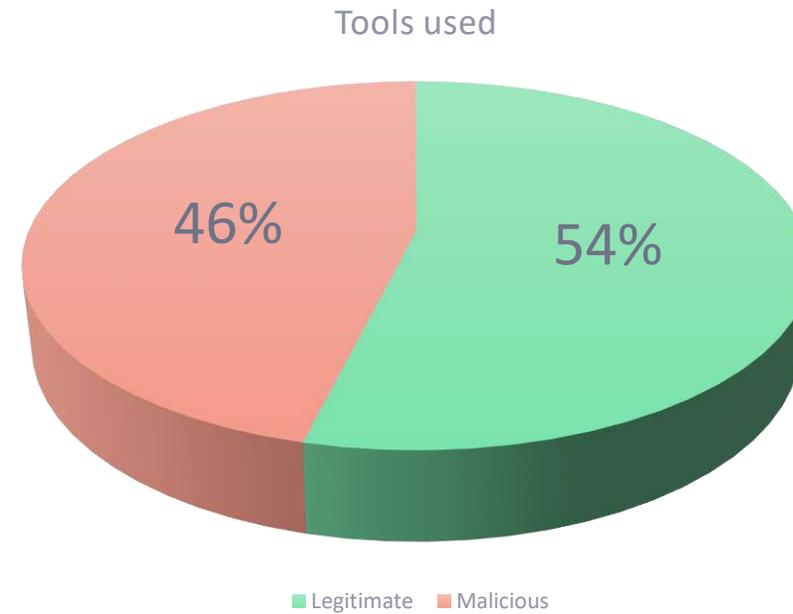
\*ENISA THREAT LANDSCAPE FOR RANSOMWARE ATTACKS July 2022

# CSIRT use case: ransomware

## Fact N°4: The tools used

Legitimate tools	MITRE ATT&CK	
	technique	tactic
OS native binary	T1056.001	EXECUTION
powershell	T1564.003	EXECUTION
net.exe	T1056.003	EXECUTION
cmd.exe	T1218.011	EXECUTION
Administrative tools	technique	tactic
ADFind.exe	T1016	DISCOVERY
Filezilla	T1048.003	EXFILTRATION
chrome.exe	T1039	COLLECTION
mspaint.exe		

Malicious tools	MITRE ATT&CK	
	technique	tactic
PowerTool64.exe	T1562.001	DEFENSE
PCHunter64.exe		EVASION
masscan64.exe	T1046	DISCOVERY
getdata-info.ps1	T1518.001	COLLECTION
xxx.exe	T1486	IMPACT
ss.dll	T1218.011	DEFENSE EVASION



# CSIRT use case: ransomware

## Fact N°5: Governance

- No response plan in place
- Clarification of roles and responsibilities
- Skilld of People involved
- Tools not ready/existing
- Business impact assessment Communication plan not existing
- ....



- Cause delay in recovery
- May have compliance/legal implications

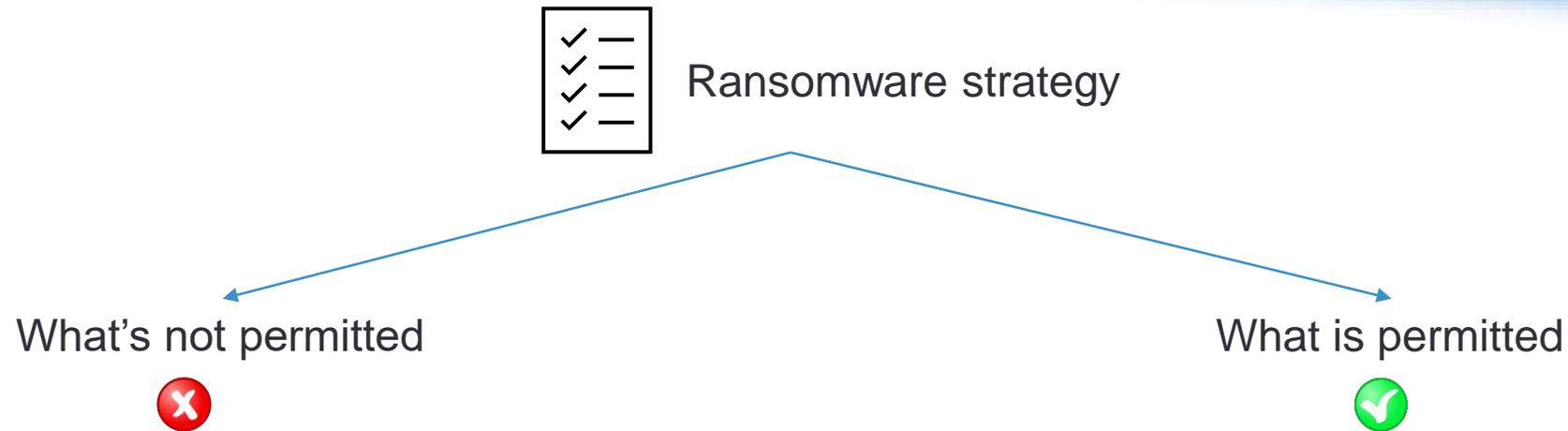


# **Key takeaways**

## **The importance of governance**

# Key takeaways

## ACTION 1: Define your strategy



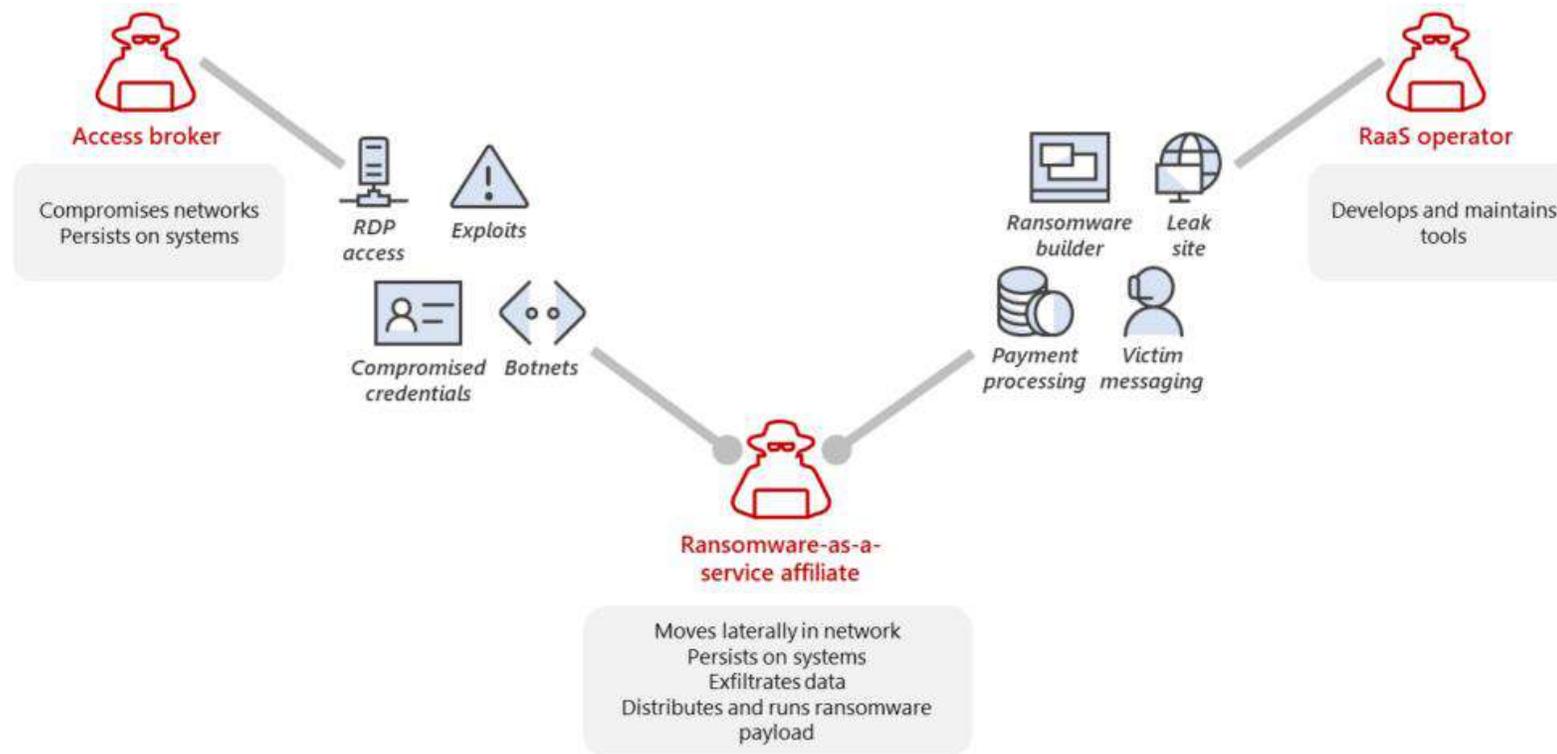
The strategy provides direction in the event of ransomware

- What are the various R&R during such an event?
- Does the organisation negotiate?
- What do we communicate, to whom, and when?
- How do we respond and recover?
- Linkage with crisis team and business continuity planning?
- Cyber insurance coverage?

# Key takeaways

## ACTION 2: Risk assessment – understanding the threat actors

### Ransomware as a service: Understanding the cybercrime gig economy



Source: <https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/>

# Key takeaways

## ACTION 3: Risk assessment – use risk scenario

### Operational scenario

Assets	Lock	Encrypt	Delete	Steal
File	✗	✓	✓	✓
Memory	✗	✓	✓	✓
Folders	✗	✓	✓	✓
Database Content	✗	✓	✓	✓
MFT	✓	✓	✓	✗
MBR	✓	✓	✓	✗
Cloud	✗	✓	✓	✓
CMS	✗	✓	✓	✗
Screen	✓	✓	✓	✗

### Strategic scenario

- Commodity/utility ransomware attacks
- Big game hunter ransomware attacks
- Ransomware-as-a-Service
- Supply chain attacks

### Framework



# Key takeaways

## ACTION N°4: Vulnerability and attack surface management

- Make sure your vulnerability management policy integrates:
  - Periodic attack surface evaluation
  - Contextual categorisation of vulnerabilities
  - Risk based remediation policy



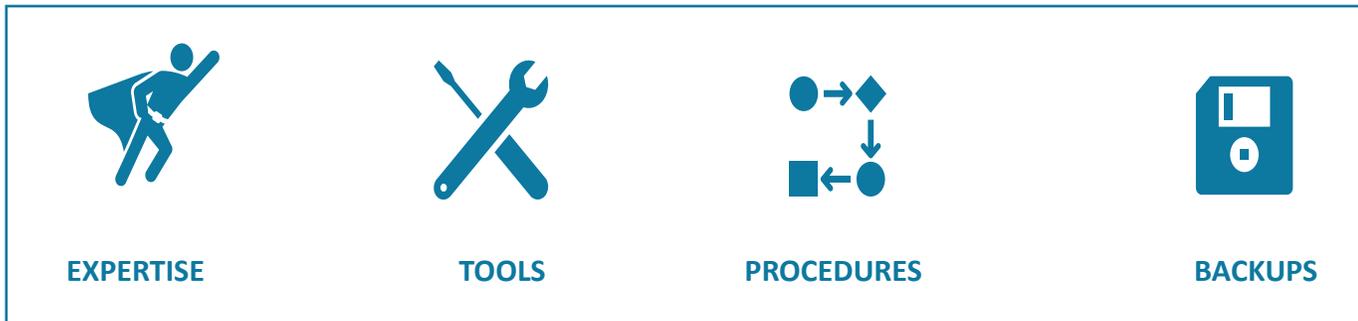
# Key takeaways

## ACTION N°5: Raise awareness and train your users

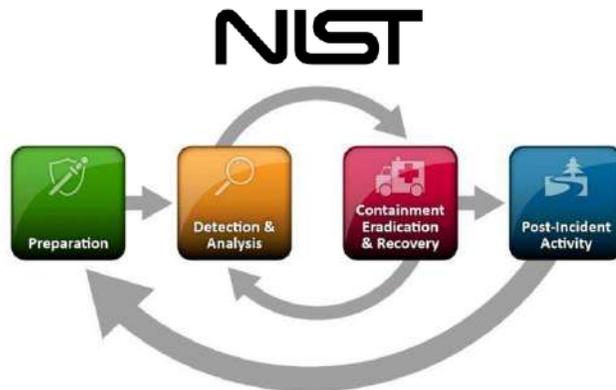
-  1 Perform human security awareness assessment
-  2 Train your users regularly on recent attack vectors and good practices
-  3 Launch phishing simulation campaigns regularly
-  4 Measure progress and create a cyber security culture

# Key takeaways

ACTION 6: Prepare for worst and have your response plan



- External CSIRT expertise
- 24/7 availability
- SLA on intervention time



INCIDENT MANAGEMENT GUIDE

# Summary

## Your action plan:

- Establish a formal strategy that provides direction in the event of a ransomware event
- Assess risks and use scenarios in order to define best response strategy
- Regularly assess your attack surface and prioritize remediation
- Train your users
- Prepare for the worst, get your response plan in hand

# ISACA Ransomware Readiness Audit Program



## Ransomware Readiness Audit Program

4 / Audit Subject

4 / Audit Objectives

5 / Audit Scope

5 / Business Impact and Risk

5 / Minimum Audit Skills

5 / Testing Steps

# Thank You!



**Approach Belgium** – Louvain-la-Neuve, Antwerp

**Approach Switzerland** – Lausanne



+32 10 83 21 11



[sales@approach.be](mailto:sales@approach.be)



[www.approach.be](http://www.approach.be)



[Linkedin](#)

