CYBERYOUTH
Non-formal education for cyber-security training
& resilience of youth organisations and young people

Policies and Procedures in Incident Response

Activity 1: Locked Out

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Project No: 2021-1-IT03-KA220-YOU-000028668

Welcome!

In this activity, we’ll join forces to learn more about the procedures and policies to follow if we suffer a cybersecurity incident.

Let’s see if you could make the right decisions to keep your data safe!

CYBERYOUTH

Co-funded by
the European Union

But first…

Let’s start with a quick energizer!

Let’s play a game called…
What’s on your phone?

- Raise 5 fingers
- We will name things that might be on your phone
- For each thing on your phone, lower one finger
- The people with the most remaining fingers raised after 10 questions win!

CYBERYOUTH

Co-funded by the European Union

What we will learn together…

- How to respond to a ransomware attack
- How to mitigate the damage this causes
- How to react and recover your data
- The importance of clear policies in case of incidents

CYBERYOUTH

Co-funded by the European Union

Locked Out

Picture this…

It’s Monday morning at the offices of YouthHelp Inc. Alex, a project manager, goes to turn on his computer but then…

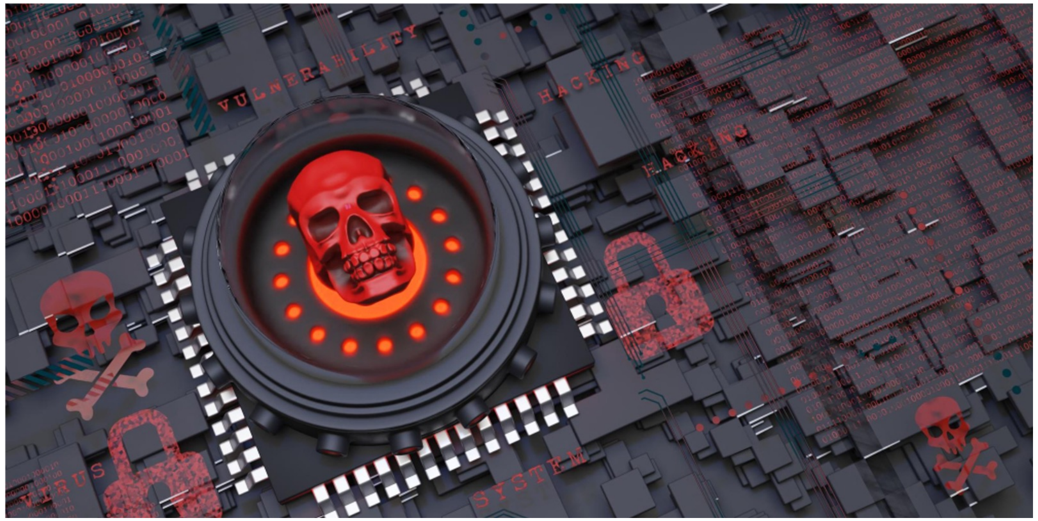
CYBERYOUTH

Co-funded by the European Union

Locked Out

Alex has been locked out of his workstation by ransomware!

A message is displayed on his screen. “Pay 5000€ in Bitcoin to unencrypt your hard drives, or lose your data forever”.



CYBERYOUTH

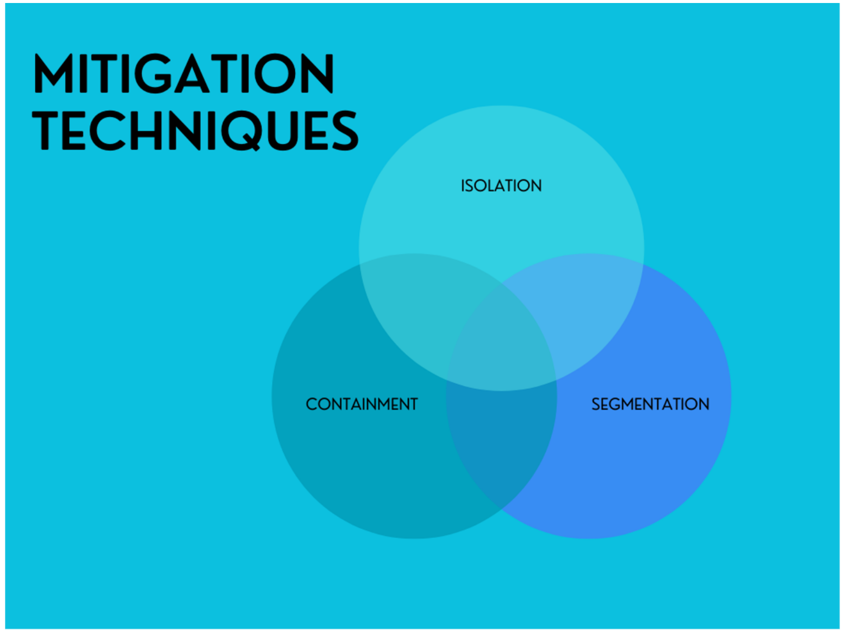
Co-funded by the European Union

What should Alex do?

- What are the first steps to take in case of any incident? What about ransomware-specific security steps?
- Should Alex try to solve the issue himself, or consult with his co-workers or supervisors?
- Should Alex and YouthHelp pay the price indicated by the attacker? If not, how should they proceed in solving the incident?

Let’s make a response plan

- To ensure the security of the company’s data, and the safety of all users and employees, let’s make a plan to respond to this incident and deal with it in the most effective way possible.
- Keep in mind the techniques that we have available to mitigate damages. Which is the best way to solve the issue?



Let’s get to it!

Each group has 10 minutes to plan their outline for an ideal response to the incident, then we will discuss.

Let’s go!

Let’s discuss

- How do you think your team did? Let’s take a look at the key points of an incident response plan and see how each group covered them:
  - Mitigation: How did your team prevent the problem from spreading?
  - Did you take the 4 phases of digital forensics into account to deduce a possible cause and solution? If not, what information were you missing?
  - Would having a defined framework for incident response make the activity we just realized easier? If so, why?

CYBERYOUTH
Non-formal education for cyber-security training & resilience of youth organisations and young people

Policies and Procedures in Incident Response

Activity 2: Fix the Flaw

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Project No: 2021-1-IT03-KA220-YOU-000028668

Welcome!

In this activity, we will build on the discoveries and plans made in Locked Out by acquiring missing information and understanding the bigger picture of the incident.

Co-funded by
the European Union

What we will learn together…

- How to gather complete information from an incident through forensics
- How to deal with security flaws in a productive manner
- Understanding how to prevent further incidents by building a positive security environment

CYBERYOUTH

Co-funded by
the European Union

Fix the Flaw

Wow, that was close!

If not managed properly, a situation such as a ransomware attack (or any other cybersecurity incident) can deeply affect an organization. Equipment is replaceable, but the integrity of the data an organisation deals with is the key component of success.

Co-funded by the European Union

Fix the Flaw

Now that we managed to avoid the worst case scenario…

One of the most important points in reincidence prevention is a thorough forensic process to understand what went wrong and why. If we understand a problem, we take away its power to confuse us!

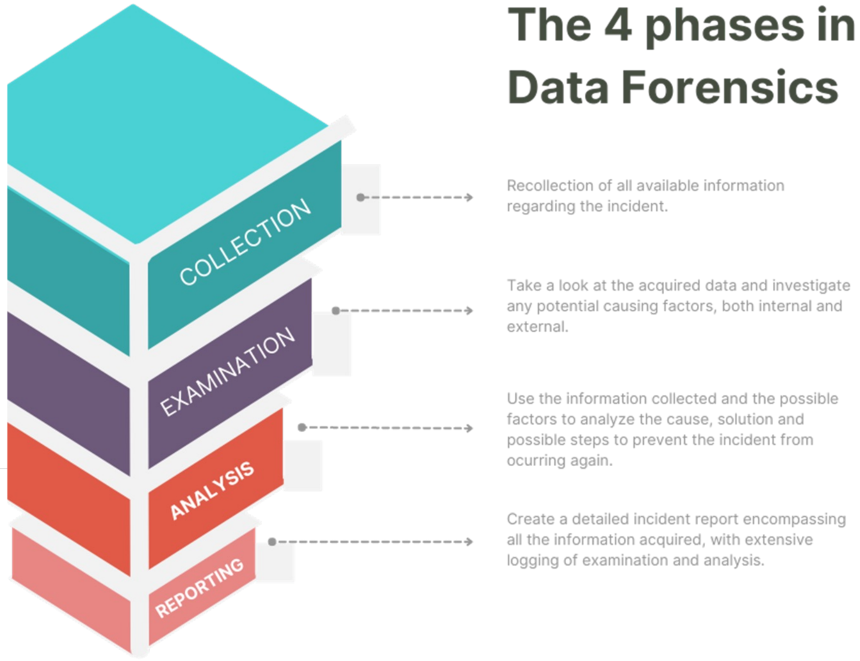
CYBERYOUTH

Co-funded by the European Union

Fix the Flaw

The 4 phases

In any data forensic investigation, there are 4 key phases. Let’s go through them and see what happened!



The 4 phases in Data Forensics

Recollection of all available information regarding the incident.

Take a look at the acquired data and investigate any potential causing factors, both internal and external.

Use the information collected and the possible factors to analyze the cause, solution and possible steps to prevent the incident from ocurring again.

Create a detailed incident report encompassing all the information acquired, with extensive logging of examination and analysis.

Co-funded by the European Union

Fix the Flaw

Collection

It seems as though the ransomware was downloaded from Alex’s computer, but Alex insists it wasn’t him. His computer was left unattended during his lunch break, and if locked, was inaccessible as no one knows Alex’s password.

The problem is, when asked, Alex can’t remember if he locked his computer or not. The section of the office Alex works in isn’t covered by the security cameras, and the only person he shares this area with is George. Alex’s lunch break is from 1pm until 2pm.

CYBERYOUTH

Co-funded by the European Union

Fix the Flaw

Examination

When checking Alex’s computer, it seems as though the ransomware program was disguised as an Office package, but Alex already has Office installed through the company’s license.

It seems as though George does not have the Office package installed even though the IT team installed it for him during his onboarding process, and the download was made during Alex’s lunch break.

CYBERYOUTH

Co-funded by
the European Union

Fix the Flaw

Analysis

Now that we have all the information, let’s get to the fun part!

Analyse the information we have found and try to come to a conclusion, not just of what happened, but why, and how it could have been prevented.

CYBERYOUTH

Co-funded by the European Union

Let’s get to it!

Each group has 10 minutes to discuss the issues that led to the breach and how each one could be prevented or avoided.

Let’s go!

Fix the Flaw

Reporting

Before we make our 100 page report, let’s discuss the issues we found and the solutions we proposed as a group.

Do we think any problems were bigger than others? Or was this a collection of misunderstandings and miscommunications that led to one big problem?

Perhaps if George had communicated his mistake to the IT staff instead of trying to fix it himself, or if Alex had locked his computer when he left, this wouldn’t have happened. But the most important point in any investigation is to tell the truth! There is no shame in making a mistake, but lying to cover it up only makes finding a solution harder.

CYBERYOUTH

Co-funded by the European Union

Policies and Procedures in Incident Response

What did you think of the activities we did? Did you find them interesting? Or maybe even boring?

Did they help you understand the importance of proper policies in case of an incident?

In cybersecurity, incidents or events are incredibly common, which is why we have to try to avoid them, but also be prepared in case we suffer an attack or incident anyway!

CYBERYOUTH

Co-funded by the European Union

CYBERYOUTH
Non-formal education for cyber-security training
& resilience of youth organisations and young people

Policies and Procedures in Incident Response

Activity 3: Red Alert

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Project No: 2021-1-IT03-KA220-YOU-000028668

Red Alert

Let’s go through one last thing. This is a game we like to call “Red alert”

CYBERYOUTH

Co-funded by the European Union

Red Alert

We will start with some cards. Each card will have a type of cybersecurity incident or attack assigned. Once we draw a card, we have 60 seconds to come up with an idea on how to respond to the incident. Understood? Let’s go!

Co-funded by the European Union

Red Alert

Remember everything we discussed in previous activities and try and keep calm while you think of a plan!

CYBERYOUTH

Co-funded by the European Union

THANK YOU!

CYBERYOUTH

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Project No: 2021-1-IT03-KA220-YOU-000028668

Co-funded by the European Union