INFOSEC EXPOSED

Feb 2022

geevo® - delivering positive change!

INSIDE

Our contact details

Tel: +357 24 023203

Email: info@geevo.eu

Visit us: www.geevo.eu

NEW FINDINGS THIS MONTH

By Nikoletta Maouri, Legal & Compliance Manager

No data no business!

Once an organization has been hacked, many questions are raised; What was breached? How and where did this happen? Who is the attacker? Questions that need to be asked to prevent hacking to take place again.

There are many areas either of law or of businesses that will be affected negatively by an attack.

What are digital forensics?

Digital forensics is defined as the process of identifying, preserving, analyzing and documenting digital evidence.

The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying, and validating the digital information to reconstruct past events. The context is most often for the usage of data in a court of law, though digital forensics can be used in other instances.

Digital forensics are not limited to computer forensics, but it has expanded to cover the investigation of any devices that can store digital data. For example, disk, network, database, email, wireless forensics etc.

Speak to our data protection and cybersecurity experts!

The Process of Digital Forensics

1. Identification

2. Prevention

3. Analysis

4. Documentation

5. Presentation

Essential Objectives of Forensics:

- ✓ Identifying the cause of the attack
- ✓ Identifying the duration of unauthorized access on the network
- ✓ Identify the evidence
- ✓ Estimate potential impact of the malicious activity
- ✓ Recovering deleted files
- ✓ Report of the investigation in process

What you will expect

- Organisation's treasure are their customer's data. Any data loss may lead an organization to face legal consequences.

- Whilst digital forensics cannot be used to prevent an attack, it helps to identify the attack or the attacker over the current security infrastructure and aids the organisation to take immediately measures to prevent continuous access to the data and prevent any future attacks.

- The attacking organisation needs to act immediately for digital forensics, to ensure the digital artifacts and evidence is best preserved for the investigation process and increases the chances of a hacker to be caught, recover any data loss and any damages to be repaired.

THINK WE CAN DO THIS TOGETHER? GET IN TOUCH.