INFOSEC EXPOSED

Apr 2023

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 Constantinos Andreou, Cyber Security Engineer

"The FileLock Fix: How to Recover from a Ransomware Attack"

When malicious software encrypts a victim's files, it demands money in return for the decryption key. This is known as ransomware. It can spread through emails, websites, or by taking advantage of weaknesses. Some noticeable examples are the recent cases in Cyprus such as the University of Cyprus, The Open University of Cyprus and the Land Registry. What is the usual and traditional method that individuals or organizations employ to restore their systems and data following a ransomware attack?

- To restore operating systems and data to previous versions against a ransomware attack. Backups are copies of data that are kept in a secure location to avoid being damaged by a ransomware attack or other data loss. If backups are available and have not been corrupted by the ransomware attack, they can be utilized to restore the data and systems to their pre-attack state. Frequent snapshots or images of the systems or drives, may also be employed.

- If a system is compromised from a ransomware attack, a necessary action is to prevent the attack from spreading, locate the affected device(s) and isolate them from the network.

Speak to our Cybersecurity experts!

Suggested security solutions and services to avoid potential ransomware attacks:

- **EDR & XDR Ransomware**: XDR and EDR solutions are technologies that can assist safeguard your computer systems against ransomware infection. They operate by monitoring your computers and networks for any odd behavior, such as someone attempting to modify key files or executing suspicious software.
- **Vulnerability Assessment & Penetration Testing (VAPT)**: Penetration testing is a simulated attack on your systems to find weaknesses and vulnerabilities. It helps you identify possible attack routes and fix them before hackers can exploit them for ransomware attacks. Think of it as a security check-up to prevent a real attack.
- **Cybersecurity Awareness Training**: May educate staff on the hazards of ransomware attacks and how to prevent them, lowering the possibility of successful assaults using social engineering approaches.
- **Multi-factor Authentication (MFA)**: MFA may provide an extra layer of protection to your systems and apps, making it more difficult for attackers to obtain unauthorized access using stolen or guessed passwords.

What you will expect

- **Avoiding ransom payments**: If your firm is hit by ransomware, you may have to pay a large sum of money to regain access to your data. Cybersecurity services can assist you in preventing attacks, allowing you to avoid paying ransoms.

- **Minimizing downtime**: When ransomware attacks happen, they can make your computer systems stop working. This can lead to lost money because you can't do business. Cybersecurity services can help you prevent attacks or respond quickly to them, so you can get back to work faster.

- **Preventing data loss**: Ransomware can wipe crucial data from your computer systems, making it difficult to recover. Cybersecurity services may assist you with backing up and protecting your data so that you do not lose any important information.

THINK WE CAN DO THIS TOGETHER? GET IN TOUCH!