INCIDENT REPORT

RANSOMWARE ATTACK ON DATA CENTER

Incident Identification:

- **Date and Time of Incident:** 01/12/2023 @ 1:30 PM
- **Location of Incident:** Data Center
- **Attack Type:** Ransomware Attack (.nemesis extension)

Incident Overview:

On Saturday, 02 Dec 2023, at 07:30 AM, the IT department received reports of servers becoming inaccessible. Upon physical inspection, it was observed that all files were encrypted by a ransomware method (.id_560306237.nemesis), accompanied by a text file named ### DECRYPT MY FILES ###. The content of the file instructed:

"ALL YOUR WORK AND PERSONAL FILES HAVE BEEN ENCRYPTED. To decrypt your files, you need to buy the special software – Nemesis decryptor. Details/buy decryptor + key/questions via email: winalgri@tuta.io & winalgri@mail.com. Your personal ID: (see the file)."

With initial assistance, it was determined to be a ransomware attack, prompting immediate isolation of servers, disconnection from the internet, and notification to management.

A detailed investigation revealed that the Primary server (hosting 4 VMs), Secondary server (hosting 6 VMs), and the backup server were all encrypted. A manual backup on an external hard drive from Saturday, 30 Nov 2023, before the attack was available. A plan was devised to restore the backup on a temporary server, resulting in all services being up and running within half a day of work.

Incident Response:

- **Immediate Actions Taken to Contain the Incident:**
  - Isolation of all affected servers.
  - Disconnection from the network.
  - Notification to management.
  - Verification of backup availability.
  - Restoration of backup on a temporary server to minimize downtime.
  - Investigation to check for client infection.

Impact Assessment:

- **List of Affected Servers:**
  - Primary Server (Physical)

    - Domain Controller (VM)
    - SAP Server (VM)
    - SQL Database Server (VM)
    - SQL Salary Server (VM)
    - Secondary Server (Physical)
    - Quickbooks Server
    - Management Client Server
    - Client Access Server
    - ZainHR Server
    - Unifi Controller Server
    - Voice Over IP Server
    - Local Backup Server (Physical)

- **Data Encrypted:**
  - All servers' data encrypted by ransomware with a public key (.id_560306237.nemesis).
- **Client Affected:**
  - No client PCs affected.
- **System Log:**
  - Log files were cleared after the attack by the attacker.

Technical Details:

- **Nature of the Ransomware:** Public key data encryption.
- **Entry Point:** Physical Servers.
- **Spread Mechanism:** All Connected Servers.
- **No Client PCs Infected.**

Mitigation Steps:

- Immediate mitigation steps taken.
- Repatriation of hard drives and reinstallation of operating systems.
- Turned off Remote Desktop connections.
- Enhanced Windows Firewall and Windows Defender.
- Changed administrator credentials.

Lessons Learned:

- Security assessment is necessary.
- Multiple backups (on-premises, off-premises, and manual backup).

- Manual backup on external HD and disconnection from the system is always a better option.
- Staff training.
- End-User cybersecurity awareness training.

Recommendations:

- Install a physical firewall to protect the data center.
- Deploy advanced endpoint protection and rollback solutions for servers and end-users.
- Regularly update antivirus definitions and security software.
- Regularly scan and update systems to address vulnerabilities.
- Enforce multi-factor authentication for access to critical systems.
- Implement network segmentation to isolate critical systems.
- Isolate the guest network from corporate networks.
- Implement certificate-based VPN access for outside users.
- Implement certificate-based access for remote desktop users.
- Remove all third-party remote access software from servers.
- Use reputed and licensed applications.
- Limit user access using GPO.
- Block USB -storage media for all users and enforce them to use one drive for data sharing.
- Block access to social media platforms on corporate networks.
- Implement a robust backup strategy (On-Site, Off-Site, Cloud, and manual backup on external hard drive).
- Regularly check and test backups.
- Develop and regularly update an incident response plan.
- Implement robust monitoring solutions.
- Maintain detailed logs and review them regularly.
- Conduct regular cybersecurity awareness training.
- Collaborate with cybersecurity experts for security assessments and penetration testing.
- Password Policy