ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Secured Business Habits

Physical & Virtual Security Aspects

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Physical Isolation for Security

1-Human Factor - Educate & Train Employees

PROBLEM:
Employees are often the weakest link hackers look for in order to penetrate a network. Employees lack cyber awareness.

SOLUTION:

- TRAINING EMPLOYEES: employees need to be trained against different cybersecurity risks to detect any loopholes in the company
- KEEP DEVICES SECURED: keep devices safe from suspicious people

Co-funded by the
Erasmus+ Programme
of the European Union

Physical Isolation for Security

2-Security Cameras

The company needs a surveillance system to keep track of all the foot traffic and actions happening in all their offices where employees do their office work.

As for the secured camera system, there are generally two types:

- Traditional System (DVR, NVR or VMS, with an internet connection)
- Cloud-Managed System (VSAAS, all video recordings are stored and managed through the cloud)

Both of these systems have their own flaws and advantages but cloud-managed systems tend to be more secure and scalable.

USING IP CAMERAS:

- IP cameras are not very much recommended for company use because they are more prone to threats
- Do not use default passwords for IP cameras. Hackers can easily exploit these default passwords to know exactly what's happening inside an organization.

Co-funded by the
Erasmus+ Programme
of the European Union

Physical Isolation for Security

3-Securing Devices

- BYOD (Bring your own Device) Concept: This concept might be very tempting as it saves costs but it also comes with greater risks (50% of the companies that implemented this concept got compromised because of their employee's devices)

- Securing Devices: Best case scenario is when a company has its own devices (such as Laptops and Smartphones) for just office-purpose, because:
  - regular security checks can easily be scheduled on these machines.
  - It very unlikely for employees to download any malicious software or spyware that might be secretly tracking activities

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Physical Isolation for Security

4-Visitor Management Policy

- Security cameras can be used to identify any incoming and outgoing visitors by implementing an identification system
- Everyone in the company should have a badge of their own with their stated position (employee badges different from visitor badges)
- Visitors should also be constantly instructed about the restricted elements, areas and actions while inside the company
- Employees should never hand over their personal devices to visitors because of security reasons
- Sensitive areas should be protected from regular visitors and their access to any company device should be limited with proper authorized permission

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Virtual Isolation for Security

1-AntiVirus Solutions & End-Point Attack Prevention

- Organizations can be breached in various ways by endpoint attacks. Among the possibilities are:
  - Viruses can infect a corporate system if an infected device contacts it
  - Malware may be downloaded onto a portable device.
  - Hackers use methods that deceive users into installing malicious software.
- Attacks examples: Emotet, TrickBot, Trojan
- Prevention against End-Point Attacks:
  - Most malware attacks can be prevented by using antivirus software
  - Any attachment that contains a malicious script (mostly .dll or .exe files) must be blocked
  - Prevent files (.zip files) that you can't scan right away
  - Restrict any ports that are unnecessary

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Virtual Isolation for Security

2-Disk Encryption for Device Protection

- Strong disk encryption will prevent hacking from getting access to the actual data that can be harmful to the company

- How Disk Encryption Works: Data and files on a hard drive can be encrypted through full disk encryption, along with the operating system and software programs. Comparable to home security, this type of encryption protects your information.

- Companies Disk Encryption:
  - Back up every device regularly
  - Protect passwords or encryption keys
  - Using encrypted disks can result in permanent data loss if the disks crash or become corrupted

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Virtual Isolation for Security

3-Backup Strategy

- To avoid any loss of data, backups are essential. cloud backup is ideal because it allows you to access data whenever you need it.

- 3-2-1 Backup Strategy: the company should have 3 copies of their data that should include their main data along with 2 copies of backup on two different mediums such as cloud or hard drives with one copy off-site for a disaster recovery plan

Co-funded by the
Erasmus+ Programme
of the European Union

Virtual Isolation for Security

4-Next-Generation Firewall (NGFW)

- Network traffic is inspected by a traditional firewall in a stateful manner. Its main objective is to detect and block sophisticated attacks by applying security policies at the application, port and protocol levels. Next-generation firewalls (NGFWs) are a third generation of firewall technology, which is installed on different mediums.

- Why is NGFW Better?:
  - NGFWs block applications that are not desired by the user
  - Filtering out certain types of network traffic is possible with port blocking. Ports act as termination points for connections among devices.
  - Their main advantage is that they are capable of controlling applications at the application level, rather than simply static inspection as traditional firewalls do.

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Virtual Isolation for Security

5-DNS RPZ

- Malicious infections to the company's devices are common and such malicious executions are carried out with the help of a DNS server. Some people refer to DNS RPZ as similar to a firewall and it is also called a DNS firewall.
- This method is currently not applied among the companies and it is still under development
- Leveraging the DNS can add a layer of security to a flat network at a low cost

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Virtual Isolation for Security

6-Use of VPN

- It provides access to the targeted network over the Internet from your local network. With the tunnelling features, your location is changed and all traffic from the device is tunnelled safely without any interference.
- A VPN protects your privacy with encryption methods. By using a VPN, you can prevent hackers from intercepting your internet traffic and stealing information
- Using VPN for Masses: Companies often go for services like OpenVPN and WireGuard to protect all their company devices

Co-funded by the
Erasmus+ Programme
of the European Union

Virtual Isolation for Security

7-URL Filtering

- URL Filtering is a successful method used by big organizations and companies to prevent their employees from visiting malicious, scammy or phishing pages. URL filtering uses a database as a reference to block all sites that are out of that database.

- URL filtering works through either local databases or by using a master-cloud database where required categories and associated policies are extracted

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Virtual Isolation for Security

8-Two Factor Authentication

- Two Factor Authentication or 2FA is one of the most popular, reliable and easy ways to protect yourself as an individual or as an employee in a company. If a company has a system of their own where users log in and log out on a routinely basis then the business should make 2FA necessary for all businesses.

- This two-factor authentication can be attached with their mobile number or even email. This will also help to notify the authority whenever some unauthorized person tries to access your account. 2FA is certainly one of the strongest yet easiest ways to protect your business devices and accounts.

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Virtual Isolation for Security

9-Data Leak Protection (DLP)

- Many organizations store huge databases which hold sensitive information about customers and business contacts as well as email addresses, medical records, and financial information that could be accessed by unauthorized individuals. There are a number of laws that require that you protect data, from HIPAA to CCPA
- 85% of companies around the world have suffered some form of loss of data during the past 24 months.
- Organizations can implement DLP security tools to take control of emails, instant messages, applications downloaded and used, web browsing, and so on

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Virtual Isolation for Security

10-Safe Password Enforcement

- Hackers can easily guess weak passwords by using different tools that use combinations of letters, numbers, and symbols to find these passwords (e.g. Dictionary attacks)

- Strong Password Criteria:
  - Strong passwords are an effective means of protecting your organization from password attacks.
    When words, letters, and symbols are combined with numbers and symbols, they can form a unique password. By using all the elements in a password, it becomes more difficult for hackers to crack the password.
  - Change passwords once a week
  - Develop a good password strategy

Co-funded by the
Erasmus+ Programme
of the European Union

Virtual Isolation for Security

11-Securing Remote Access to Internal Devices

- The foremost method for a business to secure remote access is to limit it to internal devices only.

- The following guidelines should also be followed for extra protection:
  - Limit access using firewalls.
  - Enable Network Level Authentication
  - Limit users who can log in using Remote Desktop
  - Must have an account lockout policy in place.

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Virtual Isolation for Security

12-Secured WiFi

- Securing WiFi is a basic security guideline for every business to follow, since WiFi is a gateway for your business and misuse of this service can cost really high

- Securing Business WiFi:
  - Place it at a secure physical location where everyone cannot access the router physically
  - The default router information must be changed and strong usernames and passwords should be used
  - Change your network SSID for more clarity. Currently, the WPA2 protocol is considered more secure, hence businesses are suggested to use it
  - Use your router's firewall to prevent any malicious connections
  - Limit or altogether disable DHCP and turn off the WPS that can expose your network to many threats

ENGINE

Co-funded by the
Erasmus+ Programme
of the European Union

Virtual Isolation for Security

13-Session Timeouts

- Session timeout is a simple yet effective technique used by businesses to automatically log out of your device or account after a certain amount of time without any activity
- The session time is reset at the start of the session whenever the user opens a device or connects to the server. Session timeouts prevent unauthorized access even if an attacker tries to use the account.
- Session time ranges from 15 to 45 minutes depending on the sensitivity level of the information. Businesses can set their own session times based on their requirements.