Assignment 12

1. According to the ENISA Threat Landscape report for 2023, what emerges as the primary threat within cyberspace? Why is this particular threat deemed particularly alarming? Furthermore, based on the insights provided in the document, what strategies are recommended to effectively mitigate this threat?

As cyberspace continues to expand its integral role across countless aspects of society, the need for vigilance against emerging threats becomes increasingly apparent. This is where the European Union Agency for Cybersecurity (ENISA) steps in. As the central EU cybersecurity agency, ENISA works tirelessly to make Europe's digital landscape more secure and resilient.

Initially established in 2004, ENISA has seen its mandate grow over the years, most recently through adoption of the EU Cybersecurity Act. The agency collaborates closely with member states and EU bodies, striving to develop key cybersecurity policies, enhance response capabilities, foster cooperation against threats, and build essential expertise. A primary focus is on critical infrastructure sectors like energy, transport, and finance, where disruption could have severe consequences.

The ENISA Threat Landscape (ETL) 2023 report emerges as a pivotal document in the cybersecurity domain, offering a comprehensive analysis of the multitude of threats that saturate our digital environment. It serves as a crucial resource weaving together a detailed combination of strategic and technical analyses. The insights provided by the ETL on the evolution of cyber threats are invaluable for guiding both strategic and tactical decision-making.

The report, which garners support from the ENISA ad hoc Working Group on Cybersecurity Threat Landscapes (CTL) and the ENISA National Liaison Officers (NLO) Network, highlights a significant increase in cybersecurity incidents during the latter half of 2022 and the first half of 2023. This period is characterized by an unprecedented rise in the

scale, sophistication, and impact of cyber attacks, showcasing an expanding diversity in the types of incidents.

Geopolitical tensions, particularly those stemming from the conflict in Ukraine, have had a profound impact on the cybersecurity landscape, fuelings a notable increase in cyber engagements. This timeframe has also witnessed the emergence of new hacktivist groups and a significant escalation in ransomware activities, marking an alarming increase in ransomware incidents unparalleled in previous years.

A key aspect of the ETL 2023 is its focus on the repercussions of cyber threats on essential sectors. The report explores the unique vulnerabilities and challenges these sectors face, underlining the potential for interdependencies and the critical need for sector-specific cybersecurity insights.

ENISA runs cybersecurity exercises, provides training, and promotes the adoption of best practices. The agency's threat intelligence and incident response capabilities have also expanded significantly. Each year, ENISA releases its Threat Landscape report, offering invaluable insights for cybersecurity, information governance, and legal discovery professionals. The report highlights emerging threats and trends, arming organizations with the knowledge to strengthen defences and reduce risks.

At the core of the ETL 2023 are eight principal threat categories that encapsulate the main challenges in cybersecurity:

1. **Ransomware:**

Description: Attackers seize control of a target's assets, demanding ransom for their release. This threat remains significant, evidenced by numerous high-profile incidents.

Motivation: Financial gain, disruption, ideological motives.

2. **Malware:**

Description: Malicious software designed to perform unauthorized actions that compromise the confidentiality, integrity, or availability of a system.

Motivation: Financial gain, espionage, sabotage.

3. **Social Engineering**:

Description: Techniques that exploit human error to gain unauthorized access to information or services.

Motivation: Identity theft, financial fraud, corporate espionage.

4. Threats against Data:

Description: Incidents that lead to the unauthorized disclosure, alteration, loss, or destruction of personal data.

Motivation: Financial gain, espionage, sabotage.

5. Threats against Availability - Denial of Service (DoS):

Description: Attacks that disrupt service access by overwhelming targets with excessive requests.

Motivation: Financial extortion, competitive advantage, activism.

6. Threats against Availability - Internet Threats:

Description: Disruptions that result in outages, affecting electronic communications.

Motivation: State censorship, cyber warfare, criminal activities.

7. **Information Manipulation**:

Description: Efforts to influence public opinion or political processes through deceptive practices.

Motivation: Shaping public opinion, undermining democratic processes.

8. **Supply Chain Attacks**:

Description: Attacks that target vulnerabilities in the supply chain to compromise multiple entities.

Motivation: Unauthorized access to data, compromising critical infrastructure, espionage.

The ETL 2023 report provides a detailed examination of each threat category, offering insights into trends, attack methodologies, and strategies for mitigation.
This document is a call to action for those navigating the digital landscape, offering the tools and knowledge necessary to confront the myriad cyber threats that loom in our increasingly connected world. The comprehensive analysis provided by the ENISA Threat Landscape report is instrumental in understanding and combating the digital dangers that pervade our contemporary digital environment.

ENISA runs cybersecurity exercises, provides training, and promotes the adoption of best practices. The agency's threat intelligence and incident response capabilities have also expanded significantly. Each year, ENISA releases its Threat Landscape report, offering invaluable insights for cybersecurity, information governance, and legal discovery professionals.

The report highlights emerging threats and trends, arming organizations with the knowledge to strengthen defences and reduce risks.

Industry Report Summary

Cyberspace Under Siege: ENISA's 2023 Threat Report Reveals Mounting Risks

Published on October 19, 2023, the European Union Agency for Cybersecurity's (ENISA) annual Threat Landscape report should not be ignored by professionals across sectors, including cybersecurity, information governance, and eDiscovery. This comprehensive review captures data from July 2022 to June 2023 and presents key insights that are particularly alarming for the upcoming European Union elections in 2024.

The Stakes for Trust in Democracy

Juhan Lepassaar, the Executive Director of ENISA, encapsulates the crux of the issue, stating, "Trust in the EU electoral process will critically depend on our capacity to rely on cybersecure infrastructures and on the integrity and availability of information." Lepassaar's words serve as a dire warning, emphasizing the critical need to bolster cybersecurity measures to protect democratic processes.

Dissecting the Numbers: Incident Overview

According to the report, approximately 2,580 cybersecurity incidents were recorded over the 12 months. Of these, 220 targeted more than one EU member state. This multi-state targeting amplifies the risks associated with the cyber threats and increases their potential impact. The public administration sector was hardest hit, absorbing 19% of all incidents, followed by the healthcare sector at 8%.

The Cascading Effect: Multi-Sector Impact

One of the alarming facets of the report is the concept of the ‘cascading effect,’ where a single cybersecurity incident can ripple through multiple sectors due to their interdependencies. ENISA noted that 6% of all incidents had such an impact, affecting manufacturing, transport, and finance sectors simultaneously.

Nature of Threats: Ransomware and DDoS Attacks

When it comes to the nature of the threats, the report reveals that ransomware attacks led the charge, accounting for 34% of all incidents, with Distributed Denial of Service (DDoS) attacks trailing closely at 28%. Financial motivations were predominantly behind these types of attacks.

Social Engineering and Information Manipulation

As for social engineering tactics and information manipulation campaigns, ENISA found that these forms of threats are on the rise and could pose significant risks to democratic processes such as elections. Out of total incidents related to social engineering, 30% targeted the general public, 18% were aimed at public administrations, and 8% were indiscriminate attacks against all sectors. Information manipulation campaigns were considered to be particularly menacing to electoral processes, targeting individual citizens in 47% of the cases and public administrations in 29%.

Emerging AI Threats

In addition, the report signals a worrying trend of artificial intelligence increasingly being employed to amplify cyber threats. AI-enabled chatbots, deepfakes, and Large Language Models (LLMs) were cited as emerging tools for more targeted and realistic social engineering attacks.

Evolution of the Perpetrators

As for the perpetrators, state-nexus actors, those with a connection to governmental organizations, and cybercriminals are both evolving their tactics. While state actors are adopting advanced techniques like spear phishing and targeted malvertising, cybercriminals are exploiting cloud misconfigurations to infiltrate networks.

Implications for the 2024 European Elections

Given the specific mention of AI-enabled threats and information manipulation campaigns, ENISA's report makes it clear that a new kind of cyber threat landscape is emerging, one that has direct implications for the 2024 European elections. If the trends identified by ENISA are any indication, policymakers and professionals in cybersecurity, information governance, and eDiscovery must prepare for more complex and multifaceted cyber threats in the immediate future.

Conclusion: A Call for Immediate Action

With sectors ranging from public administration to healthcare under persistent threats, and state-nexus actors adopting more advanced techniques, the 2023 Threat Landscape report from ENISA serves as a comprehensive and timely warning. It underscores the need for multi-layered cybersecurity measures, including advanced countermeasures against AI-specific threats, to safeguard the integrity of upcoming European elections in 2024.

Therefore, this critical intelligence calls for immediate action from all stakeholders to fortify cyber defences and develop targeted strategies to counter these evolving threats.

2. Visit the website www.csk.gov.in and outline some of the recommended best practices for securing personal computers.

Best practices for securing personal computers recommended by the government of India

In Today's world computers play vital role in our day to day life. A **computer** is a modernized machine that has made our daily activities easy and simple. It has made documenting an easy task. In the recent

past, **Computers** and their importance have widely grown and diversified. It is now a necessary component in every field of the industry. It records a numerable amount of data and presents it whenever necessary. Documenting, organizing, and storing data is made simple with the use of computers.

Internet is easily accessible on computers which broaden its use and benefits of it. **Computers** can also be used for recreational purposes like playing games and watching movies. Digitalization has been possible for the improvement of computers. E-commerce sites and online banking are all made possible with computers.

The **"Cyber Swachhta Kendra"** (Botnet Cleaning and Malware Analysis Centre) is a part of the Indian Computer Emergency Response Team (CERT-In). It has been set up for analyzing BOTs/malware characteristics and providing information and enabling citizens for removal of BOTs/malware. In addition, "Cyber Swachhta Kendra" will strive to create awareness among citizens to secure their data, computers, mobile phones and devices such as home routers.

The "**Cyber Swachhta Kendra**" collaborates with industry and academia to detect systems infected by bots. It also collaborates with the Internet Service Providers to notify the end users regarding infection of their system and providing them assistance to clean their systems. The center will also enhance awareness of common users regarding botnet, malware infections and measures to be taken to prevent malware infections and secure their computers / systems / devices.

Mission

To enhance the cyber security of Digital India's IT infrastructure by providing information on botnet/malware threats and suggesting remedial measures.

Some of the Desktop Security recommended by cert in

82 % of Home Users experienced at least one security threat during 2011 .To setup your computer safely Read the Vendor document carefully and follow the guidelines The olden phrase is always golden... Prevention is better than Cure.

Why do you need to secure your Desktop?

A personal computer used without proper security measure could lead to exploiting the system for illegal activities using the resources of such insecured computers. These exploiters could be Virus, Trojans, Keyloggers and sometimes real hackers. This may result in data theft, data loss, personal information disclosure, stealing of credentials like passwords etc. So, protect and secure your Personal Computer before it is compromised.

Things to remember …. While using your personal computer

Always install Licensed Software so that you have regular updates of your Operating system and Applications.

In case of open source software, make sure to update frequently.

A Read the “Terms and Conditions” / “License Agreement” provided by vendor/software before installation.

A Properly shutdown and switch off your personal computer after the use along with your external devices like Monitor, Modem and Speakers etc.

Software Installation

Installation of Operating System

- Get proper Licensed Operating System and read License agreement carefully before installing the OS.
- Switch on your personal computer and go to BIOS Settings and change your first boot drive to CD Drive.
- Insert your CD/DVD into the CD drive and restart your system using **Ctrl+Alt+Delete**.
- After restart, the system boots from the CD/DVD
- Follow the installation steps as specified by the vendor document.

Use the CD provided by the Vendor to install your

- Motherboard drivers
- Monitor drivers
- Audio & Video drivers
- Network drivers

Guidelines

Physical Security

- Regularly clean your system and its components.

Note: Turn your PC Off before cleaning it.

- Properly organize the power cables, wires, to prevent from water, insects etc.
- While working at PC, be careful not to spill water or food items on it.
- Always follow “Safely Remove” option provided by the Operating System while disconnecting the USB devices.
- By setting BIOS password, you can prevent unauthorized access to your personal computer.
- Switch off the computer when it’s not in use.

Note: To setup BIOS password refer “Setting password to BIOS” section.

Internet Security:

- Follow Internet Ethics while browsing.
- Check the copyright issues before using the content of Internet.
- Always access the site which uses https (Hyper Text Transfer Protocol Secure) while performing online transactions, Downloads etc, which is secure.
- If the site uses SSL, verify the Certificate details like Who is the owner, Expiry date of the certificate etc to confirm whether it is trusted or not. You can do this by clicking the lock icon.

- Use only Original Websites for downloading the files rather than Third Party websites.
- Scan the downloaded files with an updated Anti-Virus Software before using it.
- Install and properly configure a Software firewall, to protect against malicious traffic.

Data Security:

- Enable Auto-updates of your Operating System and update it regularly.
- Download Anti-Virus Software from a Trusted Website and Install. Make sure it automatically gets updated with latest virus signatures.
- Download Anti-Spyware Software from a Trusted Website and Install. Make sure it automatically updates with latest definitions.
- Use “Encryption” to secure your valuable Information.
  Note: For encryption password is required, always remember the password used while encrypting it, else data would not be available thereafter.
- Strong password should be used for “Admin” Account on computer and for other important applications like E-mail client, Financial Applications (accounting etc).

Backup:

- Periodically backup your computer data on CD / DVD or USB drive etc. in case it may get corrupted due to HardDisk failures or when reinstalling/format ting the system.

Browser Security:

- Always update your Web Browser with latest patches.
- Use privacy or security settings which are inbuilt in the browser.
- Also use content filtering software.
- Always have Safe Search “ON” in Search Engine.

E-Mail Security:

- Always use strong password for your email account.
- Always use Anti-Spyware Software to scan the eMails for Spam.
- Always scan the e-Mail attachments with latest updated Anti-Virus and Anti-Spy ware before opening.
- Always remember to empty the Spam folder.

Wireless Security:

- Change default Administrator passwords.
- Turn On WPA (Wi-Fi Protected Access) / WEP Encryption.
- Change default SSID.
- Enable MAC address filtering.
- Turn off your wireless network when not in use

Modem Security:

- Change the default passwords.
- Switch off when not in use.

Do's

Read the vendor document carefully and follow the guidelines to know how to setup the personal computer Connect

i. Keyboard
ii. Mouse
iii. Monitor
iv. Speakers and
v. Network Cable …...
vi. CPU (Central Processing Unit) as directed in vendor document.
vii. Connect CPU and Monitor to Electrical Outlets.

Don'ts

Do not install pirated software such as

- Operating System Software (Windows, Unix, etc.).
- Application Software (Office, Database.etc).
- Security Software (Antivirus, Antispyware.etc).
- Note: Remember, some Pirated Software themselves can be rogue programs.
- Do not plug the computer directly to the wall outlet as power surges may destroy computer. Instead use a genuine surge protector to plug a computer.
- Don't eat food or drink around the PC.
- Don't place any magnets near the PC.
- Never spray or squirt any liquid onto any computer component. If a spray is needed, spray the liquid onto a cloth and then use that cloth to rub down the component.
- Don't open the e-Mail attachments which have double extensions

Setups

BIOS (Basic Input / Output System) Settings:

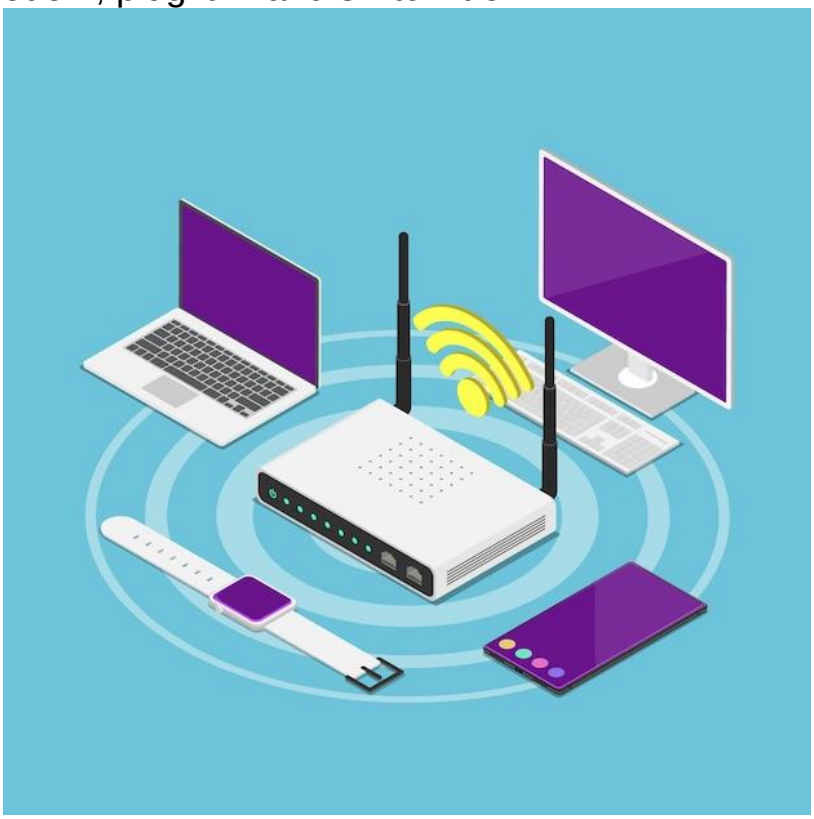
- Computers BIOS is the first program that runs when computer is started. You can tell the BIOS to ask for a password when it starts, thus restricting access to your computer.
- To enter the BIOS setup program, sometimes called CMOS setup:
- Turn on or reboot your computer. The screen will display a series of diagnostics and a memory check. A message will come "Hit the

How to connect a Wireless Modem to a Desktop Computer….

Instructions to be followed while connecting the Wireless Modem

- Make sure you have the necessary equipment. Your wireless modem package should include the wireless modem (or wireless adapter);
- An installation CD-ROM with a manual;
- an Ethernet cable (or a USB cable if you have a wireless USB modem);
- A wireless antenna (conforming to wireless standards such as 802.11a, 802.11b, or 802.11g); and a power adapter. Call the retailer or the manufacturer of your wireless modem if any of these items are missing.

- Read the manual to learn how the equipment functions. For example, use the wireless antenna to connect to the wireless network ;
- Use the Ethernet cable (or USB cable) to connect the computer to the modem.
- Attach your wireless antenna to the modem.
- Hook up an Ethernet cable from your computer to a LAN/Ethernet port on the modem. Or, if you have a wireless USB modem, connect the USB cable to the USB port of the computer.
- Connect the power adapter to the power connector of the modem, plug it in and switch it on



Setting up the Wireless Modem

- Open your Web browser and enter the URL of the modem's administrative site. If you can't find it in the users' manual, call the modem manufacturer's/vendor's customer service.
- Log in to the administrative site by entering the user name and password provided in the user manual. Again, if you cannot locate these, call the modem

manufacturer's/vendor's customer service. Usually the default username and password is "Admin."

- Select the Internet connection type. There are four types of Internet connection: "Dynamic IP Address," "Static IP Address," "PPPoE/PPPoA" and "Bridge Mode." Call your Internet service provider (ISP) to ask which setting best suits their wireless service.
- Choose "Dynamic IP Address" to get an IP address automatically from the ISP's server. For every wireless Internet connection you make, you receive an IP address. In some cases the IP address is dynamic (it changes every time you connect to the Internet), and in other cases it is static (the IP address remains the same even after you disconnect and reconnect to the Internet). If the address is dynamic, you will have to choose this setting so that the modem automatically takes the IP from the ISP's server whenever a new wireless connection is established. Enter your modem's MAC Address (usually found at the back of the modem) and other details. Refer to the user manual or call the modem manufacturer's / vendor's customer service to get these details.
- Select "Static IP Address" if you are provided with a static IP. You will need to fill in the fields for "VPI," "VCI," "IP Address," "Subnet Mask," "ISP Gateway Address," "Server Address," "Primary DNS Address," "Secondary DSN Address" and "Connection Type." These details can be obtained from your ISP.
- Opt for "PPPoE/PPPoA" if your ISP uses this type of connection. DSL users may use this connection. Enter your user name, password and other details. These will be provided by your ISP.
- Select the "Bridge Mode" if your ISP uses this connection type. Enter the relevant details provided by your ISP.
- Finish the process by clicking on the icon that says "Finish" or "OK" or something similar. Your modem should be set up now.
- Enter any URL address in your browser's address window to check whether Internet is coming or not.