SCHOOL OF CONTINUING AND DISTANCE EDUCATION

JAWAHARLAL NEHRU TECHNOLOGICALUNIVERSITY - HYDERABAD

Kukatpally, Hyderabad – 500 085, Telangana, India.

SIX MONTH ONLINE CERTIFICATE COURSES – 2023

CYBER SECURITY - ASSIGNMENT - 12

1Q) 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?

Ans:

ENISA, the European Union Agency for Cybersecurity, has recently published its **Threat Landscape Report for 2023.** The report dives into the top risks, trends, and attack methods expected to shape cybersecurity in the coming years. Drawing from events and threats spanning July 2022 to July 2023, this report serves as an important tool for understanding the evolving cybersecurity landscape. In this blog post, we delve into the key cybersecurity trends outlined in the report, dissect its major insights, and highlight ENISA's recommendations to help organizations to stay secure online.

Key cybersecurity trends

During the year from July 2022 to July 2023, experts closely examined the world of cybersecurity and noticed several important trends. These trends show how cyber threats are changing and why it's crucial to keep up with them. Below are the key trends observed during this time frame, providing a comprehensive overview of the current state of cybersecurity.

Ransomware and availability threats: these were the top concerns during the reporting period.

Geopolitical impact: Geopolitical factors continued to influence cyber operations significantly.

Double extortion: Criminal groups are increasingly blending extortion tactics with data theft, a trend known as double extortion.

Phishing evolution: Phishing remains a common initial access vector, but a new form of social engineering is emerging, involving deception in the physical world.

Business email compromise (BEC): BEC attacks remain a favored method for attackers seeking financial gain.

Data compromise increase: Data compromises saw a notable increase in 2023, following a period of relative stability in 2022.

AI chatbot impact: There has been a surge in AI chatbots impacting the cybersecurity threat landscape.

DDoS attacks: DDoS attacks are growing in size and complexity.

Internet shutdowns: Internet availability threats, particularly post-COVID, are on the rise due to increased reliance on Internet technologies.

Supply chain attacks: Threat groups are increasingly interested in supply chain attacks, leveraging employees as entry points.

Major cybersecurity threats

ENISA categorized risks into eight groups and analyzed their impact and frequency to assess their significance. As per the ETL report, the major cybersecurity threats are as follows:

Ransomware

Definition: Ransomware is a cyber-attack where malicious software encrypts files, demanding a ransom for their release. It's a serious threat, emphasizing the importance of strong cybersecurity measures.

Enisa breakdown: Ransomware remains the most prevalent danger, making up 34% of all threats in the European Union, closely followed by Distributed Denial of Service (DDoS) attacks at 28%. Ransomware targeted various sectors, with manufacturing (14%) and health (13%) topping the list, followed by public administration (11%) and services (9%).

DDoS attacks

Definition: DDoS attacks, or Distributed Denial of Service attacks, overwhelm a website or online service by flooding it with traffic. This flood of traffic is so intense that it disrupts regular operations, making the targeted service temporarily or completely unavailable. Cyber criminals use networks of compromised computers to carry out these attacks, aiming to disrupt online activities.

Enisa breakdown: DDos attacks predominantly focused on government entities (34%), followed by transportation (17%) and banking/finance (9%). Threats to internet availability primarily affected digital infrastructure (28%) and digital service providers (10%).

Supply chain attacks

Definition: Supply chain attacks occur when cyber threats infiltrate a network through trusted partners or vendors. These attacks exploit vulnerabilities in the supply chain, compromising the overall system.

Enisa breakdown: Supply chain attacks have been identified as a notable concern for upcoming elections, impacting 21% of public administration and 16% of digital service providers. The exploitation of these vulnerabilities is associated with incidents involving digital service providers (25%), digital infrastructures (23%), and public administration (15%).

AI, information manipulation, and social engineering

The report highlights the increasing risk of misinformation due to the widespread use of artificial intelligence and sophisticated social engineering tactics.

Approximately 30% of social engineering schemes targeted the general public, while 18% were directed at government agencies. Information manipulation primarily focused on individuals (47%) and government bodies (29%), with defense (9%) and media/entertainment (8%) sectors also affected.

These manipulative activities pose a significant threat to electoral integrity, particularly with the upcoming European Union elections in 2024. The report stresses the importance of enhanced monitoring to counteract the misuse of AI in propagating false information.

Artificial intelligence (AI) and Large Language Models (LLMs) demand increased vigilance. Concerns have escalated regarding their potential exploitation for **social engineering attacks**, **phishing**, information manipulation, and cybercrime.

Key recommendations

The ENISA report offers a comprehensive set of recommendations aligned with industry standards such as ISO 27001 and the NIST Cybersecurity Framework. Below, we outline the key points.

Asset management, risk assessment, and vulnerability management

Ensure comprehensive inventory, management, and control of assets.

Initiate asset discovery and conduct thorough **risk assessments.**

Perform regular vulnerability scanning to identify and address vulnerabilities.

Implement security updates and patches regularly, per your patch policy.

Establish protocols for vulnerability disclosure and incident notification with external stakeholders.

Remote access, security configuration, and data backup

Ensure secure configuration of remote access technology and exposed services.

Implement phishing-resistant **Multi-Factor Authentication (MFA)** and least privilege principles.

Maintain offline, encrypted data backups and regularly test them according to backup procedures.

Addressing emerging risks and incident response planning

Mitigate new growing risks, like AI-related threats, using encryption and cryptographic controls.

Create, maintain, and regularly test an **incident response plan.**

Document communication flows, response procedures, and incident notification protocols.

Develop contingency plans for restoring business-critical services and involve key suppliers.

Security awareness training and resource deployment

Conduct regular **security awareness training,** tailored for various departments and considering evolving threats.

Provide specific training for IT and security staff.

Planning, budgeting, and zero-trust architectures

Properly plan and budget for data management risks, aligning understanding between management and practitioners.

Implement zero-trust architectures to increase system security posture by applying the "never trust, always verify" paradigm.

Protecting your organization

In 2024, cybersecurity demands not only comprehensive technical solutions but also the cultivation of a strong cybersecurity culture. This includes fostering soft skills, ensuring legal compliance, and maintaining a vigilant stance against emerging threats. Our **awareness training** courses empower your team to recognize and evade phishing scams, contributing to the development of a robust cybersecurity culture. By staying vigilant and well-informed, we can effectively address cybersecurity challenges together.

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

Ans: **Desktop Security**

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.

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

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

Guidelines:

Physical Security:

Regularly clean your system and it's 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

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.

Recovery Disk: Always keep recovery disk supplied by Manufacturer / Vendor of the Computer System to recover the Operating System in the event of boot failures due to system changes such as uncerificated Drivers/unknown Software publisher.

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.

Browse 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.