Report: Security Awareness

BY TEAM 2:

CHIRAG GUPTA
AVINASH KUMAR
BARIGE ADARSH
HEMA SENTHIL MURUGAN
KARRI LOKESH
ROHIT PATIBALLA
POTNURU JAYANTH
SADHU SAICHANDRAM DIPAKBH

INDEX

Security Awareness

Introduction

Many small companies underestimate the importance of security testing and skip it. However, businesses run by more experienced people never skip on this. A product is after all built for the customers and thereby it is necessary to test if they are being able to use it as they intend to and whether or not they are facing any issue while they are at it.

What is Security Testing and Why is It Necessary?

Security Testing is a process intended to identify flaws in the security mechanisms of an information system that protects data and maintains functionality as intended.

Just like the software or service requirements must be met in QA,security testing warrant that specific security requirements be met.Typical security Requirements my include specific elements of confidentiality,integrity,authentication,availability,authorization and non-repudiation.

Awareness Passwords

- Use a password manager:They are many to choose from and some are free A password manager can assist in automating the fix to the below mentioned threats.
- Don’t write or print passwords on paper or in unsecured digital files.Fox example, a sticky note with the password on the backside of a laptop or a list of passwords in an unprotected excel sheet.

- Don’t use the same password everywhere. Try to use unique passwords everywhere you login.if one website or company gets hacked,and the passwords are leaked,then all accounts using that same password are at risk.
- Use long,random,but memorable passwords- also known as passphrases.
- Where possible use multi-factor authentication.if a password is know, then the second or third factor of authentication is an additional layer of protection.

Awareness Data Handling

- The use of data helps make our lives more convenient and stremlined which likely means the proliferation of online data and device are here to stay.There is one best practice that each of us can apply that will help personal data stay more secure.

Information beyond name and email such as birthdate and address should not be provided freely as a best practice you should only provide this information to trusted companies with which you have an established relationship.

Awareness Computer theft

- Having something stolen form you tends to lave an indelible feeling of violation and injustice.if what is stolen is an electronic device (leptop, phone, flashdrive), not only is the property gone but so is your data. Stolen data can be a more damaging long term than the loss of the physical device itself. The data could be personal or company date.if device is able to be used by the thief,there are many ways the device can become of value.

- The most important best practice is to not leave devices unattended in public places.this includes a locked car. In many cities, car breakins are extremely common. Even if you think your risk might be lower,don't take a chance.

Aware Phishing and Ransomware

- It is a tool and method attackers use to try and coerce people into clicking on a malicious site or download, potentially leading to a security issus.
- Ransomware is an especially dangerous consequence of falling for a phishing attempt.
- Ransomware is software the locks down data by encrypting it and won't be unlocked through
- Decryption until a ransom is paid. To protect yourself from ransomware:
    1. Be wary of suspicious emails and look for the signs.
    2. Make sure your antivirus software is up to date and running. It help stop the ransomware in its tracks.
    3. If ransomware is installed, then if you backed up your data, you can ignore the threat and restore the data. Unfortunately, in many cases and especially for large enterprises, the cost of the ransome is significantly less the cost to restore the data even if its backed up.

Aware Removable Media

- Removable media and device are portable hardware. The most common is a USB flash drive but other form could be an external hard drive or sd card.
- When it comes to cyber security best practices, removable medial and devices must only be plugged or inserted into your computer if you trust/know the source.

Aware Vishing

- The fraudulent practice of making phone calls or leving voice messages purporting to be from reputable companies in order to trick individuals to reveal personal information, such as bank details and credit card numbers.

Aware Internet Downloads

- Only download reputable software form reputable sources. If you don’t know the source, or it looks suspicious, don’t risk it , head to the official source and go from there.

Aware WI-FI

- Public WI-FI is not secure and can put your device and data at risk.

Empowering Cyber Guardians:

In the fast-changing world of modern business, security awareness steps up as a strong protector against potential risks. This smart strategy doesn't just keep data safe, but also gives people the know-how to confidently navigate the digital realm.

A key concern pops up as things change: data can be accessed, harmed, or misused. When an employee might leave, it's time for extra caution. This is where a computer forensics expert comes in. Before telling someone they're leaving, this expert makes a copy of their computer info. It's like a shield against any possible tampering after they go.

This plan isn't just about preventing data messing; it's also about backing up an employer's case. The info that's saved can help show if something was taken or prove what really happened.

But there's more to this story – it's like being a digital detective. It encourages people to learn about digital clues. By looking at deleted stuff and finding hidden evidence, we can uncover lots of important details.

Did you know that a simple computer record can tell us a lot? Security awareness is built from info like visited websites, downloaded files, and when things were used. It's like following digital footprints to find out if anything was hidden or changed.

Email is a big part of this detective work. It's important because it can show what people really think and is used a lot for business. Email can even change the outcome of legal cases.

As the digital world keeps growing, staying watchful is super important. Backups help keep a record of what happened, and they're usually kept for a long time.

People also keep money records on computers, adding another layer to this puzzle. This shows that security awareness is a big deal.

In the end, security awareness is about more than just staying safe. We become cyber guards, ready to face the digital world. We make sure data is safe and businesses are strong, all thanks to security awareness.

CYBER SECURITY DO'S

1. Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.

2. Change your passwords at least once in 45 days.

3. Use multi-factor authentication, wherever available.

4. Save your data and files on the secondary drive (ex: d:\).

5. Maintain an offline backup of your critical data.

6. Keep your Operating System and BIOS firmware updated with the latest updates/patches.

7. Install enterprise antivirus client offered by the government on your official desktops/laptops. Ensure that the antivirus client is updated with the latest virus definitions, signatures and patches.

8. Configure NIC's DNS Server IP (IPv4: 1.10.10.10 / IPv6: 2409::1) in your system's DNS Settings.

9. Configure NIC's NTP Service (samay1.nic.in, samay2.nic.in) in your system's NTP Settings for time synchronization.

10. Use authorized and licensed software only.

11. Ensure that proper security hardening is done on the systems.

12. When you leave your desk temporarily, always lock/log-off from your computer session.

13. When you leave office, ensure that your computer and printers are properly shutdown.

14. Keep your printer's software updated with the latest updates/patches.

15.Setup unique passcodes for shared printers.

16.Use a Hardware Virtual Private Network (VPN) Token for connecting privately to any IT assets located in the Data Centres.

17. Keep the GPS, bluetooth, NFC and other sensors disabled on your computers and mobile phones. They maybe enabled only when required.

18.Download Apps from official app stores of google (for android) and apple (for iOS).

19.Before downloading an App, check the popularity of the app and read the user reviews. Observe caution before downloading any app which has a bad reputation or less user base, etc.

20.Use a Standard User (non-administrator) account for accessing your computer/laptops for regular work.

21.While sending any important information or document over electronic medium, kindly encrypt the data before transmission. You can use a licensed encryption software or an Open PGP based encryption or add the files to a compressed zip and protect the zip with a password. The password for opening the protected files should be shared with the recipient through an alternative communication medium like SMS, Sandes, etc.

22.Observe caution while opening any shortened uniform resource locator (URLs) (ex: tinyurl.com/ab534/). Many malwares and phishing sites abuse URL shortener services.

23.Observe caution while opening any links shared through SMS or social media, etc., where the links are preceded by exciting offers/discounts, etc., or may claim to provide details about any current affairs. Such links may lead to a phishing/malware webpage, which could compromise your device.

24.Report suspicious emails or any security incident to incident@cert-in.org.in and incident@nic-cert.nic.in. 25.Adhere to the security advisories published by NIC-CERT (https://niccert.nic.in/advisories.jsp) and CERT-In (https://www.cert-in.org.in).

CYBER SECURITY DON'TS

1. Don't use the same password in multiple services/websites/apps.

2. Don't save your passwords in the browser or in any unprotected documents.

3. Don't write down any passwords, IP addresses, network diagrams or other sensitive information on any unsecured material (ex: sticky/post-it notes, plain paper pinned or posted on your table, etc.)

4. Don't save your data and files on the system drive (Ex: c:\ or root).

5. Don't upload or save any internal/restricted/confidential government data or

files on any non-government cloud service (ex: google drive, dropbox, etc.).

6. Don't use obsolete or unsupported Operating Systems.

7. Don't use any 3rd party DNS Service or NTP Service.

8. Don't use any 3rd party anonymization services (ex: Nord VPN, Express VPN, Tor, Proxies, etc.).

9. Don't use any 3rd party toolbars (ex: download manager, weather tool bar, askme tool bar, etc.) in your internet browser.

10. Don't install or use any pirated software (ex: cracks, keygen, etc.).

11.Don't open any links or attachments contained in the emails sent by any unknown sender.

12.Don't share system passwords or printer passcode or Wi-Fi passwords with any unauthorized persons.

13. Don't allow internet access to the printer.

14. Don't allow printer to store its print history.

15.Don't disclose any sensitive details on social media or 3rd party messaging apps.

16. Don't plug-in any unauthorized external devices, including USB drives shared by any unknown person

17.Don't use any unauthorized remote administration tools (ex: Teamviewer,Ammy admin, anydesk, etc.)

18. Don't use any unauthorized 3rd party video conferencing or collaboration tools for conducting sensitive internal meetings and discussions.

19. Don't use any external email services for official communication.

20. Don't jailbreak or root your mobile phone.

21.Don't use administrator account or any other account with administrative privilege for your regular work.

22.Don't use any external mobile App based scanner services (ex: Camscanner) for scanning internal government documents.

23. Don't use any external websites or cloud-based services for converting/compressing a government document (ex: word to pdf or file size compression)

24. Don't share any sensitive information with any unauthorized or unknown person over telephone or through any other medium.

Security Tools

Free Bot Removal Tool - For Microsoft Windows

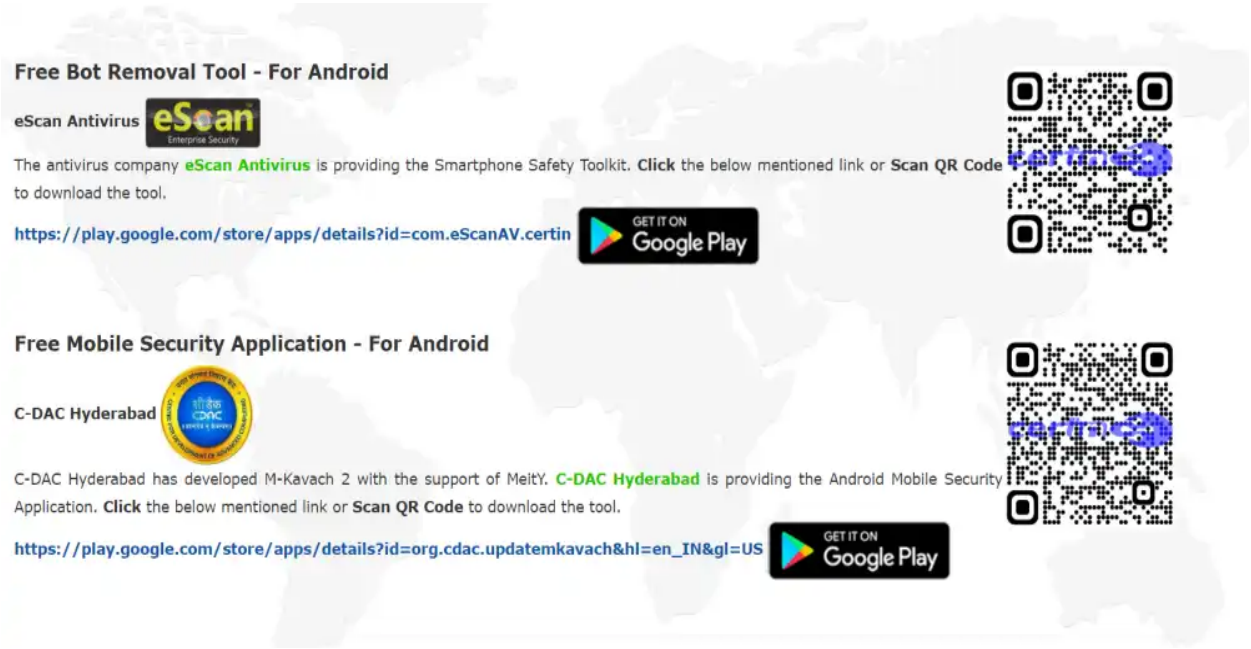
You may use any of the following Bot Removal Tool for your digital device.

Note: To identify, the architecture of your computer system whether it is 32-bit or 64-bit, right click on "My computer"/ "This PC" -> Properties-> Check your system architecture

- **eScan Antivirus**
- The antivirus company **eScan Antivirus** is providing the free bot removal Tool. Click the below mentioned link to download the tool.
  https://www.escanav.com/en/escanav-cert/escanav-cert-intoolkit.asp
  Download **K7 Security**
- The antivirus company **K7 Security** is providing the free bot removal Tool. Click the below mentioned link to download the tool.
  https://www.k7computing.com/in/k7-bot-removal-tool
  Download **Quick Heal**

The antivirus company **Quick Heal** is providing the free bot removal Tool. Click the below mentioned link to download the tool.

https://www.quickheal.co.in/bot-removal-tool Download



Industrial and Telecommunications Networks Challenges and Solutions for Critical Infrastructure Cybersecurity

Abstract: In the current digital era, the cybersecurity of critical infrastructure is a significant concern, with industrial and telecommunications networks serving as prime targets for cyberattacks. This curiosity makes me investigate the difficulties these two kinds of networks encounter and offers creative methods to improve their security. I look at prospective attack vectors, new dangers, and the effects of cyber incidents on vital infrastructure. Additionally, it emphasises the significance of cooperation between the public and private sectors as well as the incorporation of cutting-edge technologies in

order to protect these crucial systems. The research's conclusions shed important light on how industrial and telecommunications networks are to growing cyber dangers.

1. Introduction: The significance of industrial and communications networks as a component of essential infrastructure is discussed. It outlines the objectives of the research and emphasises the value of tackling certain cybersecurity difficulties.

2. Cyber Threat Landscape for Industrial and Telecommunications

Networks: In this section, the current cyber threat landscape is examined, along with the threats and attack methods that are specifically aimed at industrial and telecommunications networks. It identifies typical weaknesses and possible reasons for cyberattacks on these crucial systems.

3. The Difficulties of Securing Industrial Networks: This section focuses on the specific difficulties in securing industrial networks, such as legacy systems, connectivity issues, and complexity brought on by the convergence of operational technology (OT) and information technology (IT). Also highlighted are potential consequences of a successful cyber-attack on industrial systems.

4. The Difficulties of Securing Telecommunication Networks: The increasing reliance on 5G and the Internet of Things (IoT), the prevalence of distributed denial-of-service (DDoS) attacks, and the potential impact on crucial communication services are just a few of the cybersecurity challenges that are unique to telecommunications networks.

5. Real-world case studies of cyber events that impacted Telecommunications and industrial networks are included in the research report. These case studies give useful information about the actual consequences of successful cyberattacks on vital infrastructure, as well as lessons learned for enhancing cybersecurity safeguards.

For Telecommunications -

The Dyn Cyberattack of 2016 -

A large Distributed Denial of Service (DDoS) attack against Dyn, a business that manages a sizable chunk of the domain name system (DNS) infrastructure on the internet, was launched in October 2016. Permissions to relevant websites like Twitter, Reddit, and CNN were delayed by the attack. Multiple botnet devices were used in IoT devices which includes cameras and DVRs, were used to attack for creating a record amount of traffic and bury Dyn’s servers.

Impact: The incident exposed the internet's interconnectedness's weaknesses and the potential for worldwide internet services to be disrupted by a focused attack on a single target.

For Industrial Networks -

Malware Triton/Trisis Incident of 2017 -

A new malware family called Triton (or Trisis) targeted a petrochemical firm in Saudi Arabia in 2017. This malware was made specifically to attack safety instrumented systems (SIS), a class of industrial control system used to guarantee the security of industrial processes. The attackers may have intended to physically harm the facility instead of stealing data.

Impact: This attack brought attention to the constantly changing nature of threats to industrial networks and the potential for cyber disasters to spill over into real-world situations that result in harm or even fatalities.

6. Innovative Solutions for Industrial Networks: This section examines advance guarding strategies to support industrial networks' cybersecurity. The usage of blockchain for secure data transactions, AI and ML for anomaly detection, and ICS access control implementation are all covered in this article.

7. Innovative Solutions for Telecoms Networks: Like the previous part, this one focuses on creative approaches to boosting telecoms networks' cybersecurity. The application of advanced DDoS mitigation strategies, the implementation of security-by-design principles in 5G and IoT devices, and the usage of Software-Defined Networking (SDN) for network security are among the topics covered.

8. Concluding Reiterating the need of tackling cybersecurity issues in industrial and telecommunications networks, the conclusion section summarises the research findings. It highlights the necessity of proactive and teamwork in protecting crucial infrastructure from changing cyberthreats.

9. Reference -

https://uhra.herts.ac.uk/bitstream/handle/2299/12999/Infrastructure_Sec_NA_final_v3.pdf?sequence=2&isAllowed=y

https://books.google.co.in/books?hl=en&lr=&id=V2RzAwAAQBAJ&oi=fnd&pg=PP1&dq=Critical+Infrastructure+Security+Threats:+Industrial+Networks&ots=54CaRcszji&sig=mNkGvCGhtImbq2xzruE0A8rQGn8&redir_esc=y#v=onepage&q&f=true

Compliance and regulations

Introduction

Cybersecurity compliance and regulations are like a set of rules that organisations and businesses must follow to keep their digital information safe from hackers and cyber-attacks. These rules help protect sensitive data, reduce risks of security breaches, and make customers feel more secure. Different industries may have specific rules to follow, and sticking to them is essential to avoid legal trouble and maintain trust with customers. Adhering to specific cybersecurity frameworks, such as GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability), or PCI DSS, is essential for organisations to maintain data privacy and security, avoid legal repercussions, and ensure responsible handling of sensitive data.

Need and Significance

a. Protection against Cyber Threats: With the increasing frequency and sophistication of cyber threats and attacks, compliance and regulations help organisations adopt proactive measures to safeguard their systems and data from malicious actors.
b. Data Privacy and Confidentiality**:** Compliance frameworks like GDPR and HIPAA ensure that personal and sensitive information is handled responsibly, protecting individuals' privacy, and preventing data breaches.
c. Mitigating Cyber Risks: Following cybersecurity regulations helps identify and address vulnerabilities, reducing the risk of cyber incidents that could lead to financial losses and reputational damage.
d. Building Customer Trust: Adhering to cybersecurity standards demonstrates an organisation's commitment to protecting its customers' data, fostering trust and loyalty among clients and stakeholders.
e. Legal and Regulatory Compliance: Failure to comply with relevant cybersecurity laws and regulations can lead to severe legal consequences, including hefty fines and sanctions.
f. Industry Reputation and Credibility: Being compliant with cybersecurity regulations enhances an organisation's reputation as a responsible and secure entity, potentially attracting more customers and partners.
g. Incident Response and Recovery: Cybersecurity compliance often involves establishing incident response plans and disaster recovery procedures, enabling organisations to respond effectively in the event of a security breach.

Prominent Cybersecurity Compliance and Regulations Frameworks

i) General Data Protection Regulation (GDPR)

The GDPR is a comprehensive regulation for data protection and privacy implemented by the European Union (EU). The GDPR has significantly impacted businesses worldwide, prompting them to update their data handling practices complying with the regulation. It is regarded as one of the most far-reaching data protection laws globally and has influenced data protection legislation in other countries. The main aim of the GDPR is to strengthen and unify data protection laws across EU member states while giving individuals more control over their personal data.Example of some companies that use this compliance are: McAfee, Symantec and Trustar. Some of the Key principles are:

1. Applicability: The regulation applies to all organisations processing personal data of individuals within the EU, regardless of their location. It also covers organisations outside the EU if they offer goods or services to EU individuals or monitor their behaviour.
2. Consent: Organisations must obtain explicit and informed consent from individuals before processing their personal data. Consent must be freely given, specific, and can be withdrawn.
3. Data Subject Rights: The GDPR grants individuals various rights concerning their personal data, including access, rectification, erasure, restriction of processing, and data portability.
4. Data Protection Officer (DPO): Some organisations must appoint a Data Protection Officer responsible for overseeing data protection compliance.
5. Data Breach Notification: Organisations are obligated to notify the relevant supervisory authority and affected individuals within 72 hours (about 3 days) of discovering a data breach that could risk individuals' rights and freedoms.
6. Privacy by Design and Default: Data protection must be integrated into system design and processes, with privacy as the default setting.
7. Data Processing Agreements: Organisations acting as data processors must have written agreements with data controllers, outlining their responsibilities and obligations.
8. Cross-Border Data Transfers: Transfers of personal data to countries outside the EU must meet specific safeguards to ensure an adequate level of data protection.
9. Fines and Penalties: Non-compliance with the GDPR may result in substantial fines, depending on the seriousness of the violation.

ii) The Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act is a federal law introduced in the United States in 1996. Its main objective is to safeguard sensitive patient health information and provide individuals with specific rights and protections regarding their health data. Administered by the U.S. Department of Health and Human Services (HHS), HIPAA sets standards and regulations for covered entities, such as health plans, healthcare providers, and healthcare clearinghouses. HIPAA strives to balance patient privacy with the necessary sharing of health information for treatment and payment purposes in the healthcare industry. It has played a crucial role in promoting the adoption of electronic health records (EHRs) and enhancing the security and privacy of patient health information.

Some of the Key principles are:

1. The Privacy Rule establishes national standards for protecting individuals' medical records and other personal health information held by covered entities. It restricts the use and disclosure of protected health information (PHI) without individual authorization, except for certain permitted purposes like treatment, payment, and healthcare operations.
2. Security Rule: The Security Rule mandates covered entities to implement safeguards for electronic protected health information (ePHI) to ensure its confidentiality, integrity, and availability.
3. Breach Notification Rule: Covered entities must notify affected individuals, the HHS, and sometimes the media in case of a breach of unsecured PHI that compromises its privacy or security.
4. Transactions and Code Sets Rule: This rule defines standard electronic transactions and code sets that covered entities must be used for specific administrative and financial purposes like claims submission and payment processing.
5. Unique Identifiers Rule: Standards for unique identifiers used to identify individuals, employers, health plans, and healthcare providers in standard electronic transactions are established by this rule.
6. Enforcement: The HHS Office for Civil Rights (OCR) enforces HIPAA regulations, with violations leading to civil and criminal penalties, depending on the severity of the breach.

iii) The National Institute of Standards and Technology (NIST)

The NIST Cybersecurity Framework, developed by the National Institute of Standards and Technology, is a comprehensive set of guidelines, best practices, and standards aimed at assisting organisations in managing and improving their cybersecurity risk management processes. Released in 2014 to address the growing cybersecurity threats faced by businesses and critical infrastructure sectors, this framework offers flexibility, scalability, and adaptability for organisations of all sizes and industries. The NIST Cybersecurity Framework serves various purposes, including assessing the current cybersecurity status, prioritising improvement areas, establishing a collective understanding of cybersecurity risks, communicating risk management practices internally and externally, and fostering collaboration among organisations on cybersecurity matters. Since its introduction, the NIST Cybersecurity Framework has gained widespread global adoption, becoming a valuable resource for organisations seeking to enhance their cybersecurity resilience and risk management capabilities.Example of some companies that use this compliance are: Amazon Web Services and Cisco Systems.

The framework comprises three main components:

1. Core: The Core outlines essential cybersecurity activities, desired outcomes, and references to help organisations understand and address their cybersecurity risks. It is organised into five core functions: Identify, Protect, Detect, Respond, and Recover.
2. Framework Implementation Tiers: The Implementation Tiers allow organisations to assess their current and target cybersecurity risk management practices. They range from "Partial" (Tier 1) to "Adaptive" (Tier 4) and help organisations gauge their cybersecurity maturity and plan for improvement.
3. Framework Profiles: Framework Profiles enable organisations to create tailored representations of their specific cybersecurity requirements, considering their business needs, risk tolerance, and available resources.

v) The Information Technology (IT) Act, 2000

The Information Technology (IT) Act, 2000 is an important piece of legislation in India that was enacted on 9th June 2000. Its primary objective is to provide legal recognition for electronic transactions, facilitate e-governance, and promote e-commerce in the country. The IT Act addresses various aspects related to electronic records, digital signatures, cybercrimes, and data protection.Some of the Key principles are:

1. Legal Recognition of Electronic Records: The Act grants legal validity to electronic records and digital signatures, making them equivalent to paper documents and handwritten signatures in certain circumstances.
2. Digital Signatures: The Act defines the legal framework for digital signatures, providing authenticity and integrity to electronic transactions.
3. Cyber Crimes and Offences: The IT Act introduced various provisions to address cybercrimes, including unauthorised access to computer systems, computer-related offences, and hacking.
4. Data Protection and Privacy: The Act includes provisions for the protection of personal data and privacy. However, the concept of data protection and privacy has been further strengthened and expanded with the proposed Personal Data Protection Bill, which was introduced in 2019.Network Service Providers: The Act recognizes network service providers and their responsibilities, including implementing and maintaining reasonable security practices and procedures.
5. Cyber Appellate Tribunal: The IT Act establishes the Cyber Appellate Tribunal, which has the authority to hear appeals against certain decisions made by the Controller of Certifying Authorities and decide cybercrime-related matters. -
6. Offences and Penalties: The Act prescribes penalties and punishments for various cyber offences, including unauthorised access to computer systems, data theft, and computer-related offences.

vi) Reserve Bank of India (RBI) Cyber Security Framework

The Reserve Bank of India (RBI) is the central banking institution of India, responsible for monetary policy formulation, regulation of the financial sector, and currency issuance. The RBI also plays a crucial role in setting guidelines and regulations related to cybersecurity, data protection, and risk management in the banking and financial sector. Some of the notable RBI guidelines include:

1. Cybersecurity Guidelines for Banks: The RBI has issued cybersecurity guidelines for banks and other financial institutions to enhance the security of their information systems and digital operations. These guidelines cover areas such as information security governance, risk assessment, incident response, vendor management, and more.

2. Digital Payment Security Controls: To ensure the security of digital payment systems and protect consumers' financial data, the RBI has issued guidelines outlining security controls and practices that payment service providers must adhere to.

3. Customer Data Protection: The RBI emphasises the importance of safeguarding customer data and has issued guidelines for banks and financial institutions to establish strong data protection practices, including data encryption, access controls, and data sharing protocols.
4. Know Your Customer (KYC) Norms: The RBI has issued guidelines related to the Know Your Customer (KYC) norms, which financial institutions must follow to verify the identity of their customers, prevent money laundering, and enhance customer due diligence.
5. Fraud Risk Management: The RBI has provided guidelines for banks to manage fraud risks effectively, including detecting and preventing several types of financial fraud.
6. Mobile Banking and Digital Transactions: The RBI has issued guidelines to ensure the security and integrity of mobile banking and digital transactions, including guidelines for secure authentication methods and transaction limits.
7. Technology Risk Management Framework: The RBI has introduced a technology risk management framework for banks to manage technology-related risks and ensure the safety and stability of their operations.
8. Operational Resilience: The RBI emphasises the importance of operational resilience in financial institutions and has provided guidelines to ensure their ability to withstand and recover from disruptions.
9. Data Localization: The RBI has issued guidelines related to data localization, requiring certain categories of sensitive customer data to be stored within the country.

IDENTIFY EMERGING THREATS: MONITOR AND ANALYSE EMERGING CYBER THREATS AND VULNERABILITIES TO PROACTIVELY DEVELOP DEFENCE MECHANISMS

1.INTRODUCTION

Monitoring and analysing emerging cyber threats and vulnerabilities are of paramount importance in today's digital landscape due to the following reasons:

1. Proactive Defence: Cyber threats and vulnerabilities are constantly evolving. By actively monitoring and analysing emerging threats, organisations can detect potential risks before they become widespread and proactively develop defence mechanisms to protect their systems and data.

2. Timely Response: Early detection of emerging threats allows organisations to respond quickly and effectively. This minimises the potential impact of cyberattacks, reducing downtime, financial losses, and reputational damage.

3. Protection of Sensitive Data: Emerging threats often target sensitive data, including customer information, financial records, and intellectual property. Regular monitoring helps safeguard this critical information from falling into the wrong hands.

4. Stay Ahead of Cyber Criminals: Cybercriminals are constantly innovating and devising new attack methods. Monitoring emerging threats enables organisations to understand attackers' tactics, techniques, and procedures, enabling them to stay ahead in the cybersecurity arms race.

5. Compliance and Regulations: Many industries have stringent data protection regulations. Regular monitoring and analysis of emerging threats are crucial to meeting compliance requirements and avoiding potential penalties for data breaches.

6. Third-Party Risk Management: Organisations often work with various vendors and partners, introducing additional risk factors. Monitoring emerging threats helps identify potential vulnerabilities in third-party systems, ensuring a more secure business ecosystem.

7. Resource Allocation: Cybersecurity resources are limited, and focusing on outdated or low-priority threats can be inefficient. Monitoring emerging threats allows organisations to allocate resources more effectively and address the most critical risks.

8. Continuous Improvement: Cybersecurity is an ongoing process. Monitoring emerging threats facilitates a culture of continuous improvement, fostering better security practices and increasing resilience to future threats.

2.HOW TO IDENTIFY EMERGING THREATS:

Identifying emerging threats requires a combination of proactive measures and continuous monitoring of the cybersecurity landscape. Here are some steps to help you effectively identify emerging threats:

1. Stay Informed: Regularly follow cybersecurity news, industry publications, and reports from reputable cybersecurity organisations. Subscribe to threat intelligence feeds and mailing lists to receive updates on the latest vulnerabilities and emerging threats.

2. Participate in Cybersecurity Communities: Engage with cybersecurity forums, online communities, and social media groups where experts and professionals share information about emerging threats. These platforms can provide valuable insights and early warnings about new attack vectors.

3. Conduct Regular Threat Intelligence Gathering: Invest in threat intelligence services or platforms that provide real-time information about emerging threats. These services aggregate data from various sources, analyse trends, and provide actionable intelligence.

4. Collaborate and Share Information: Collaborate with other organisations, industry peers, and government agencies to share threat intelligence. Participate in Information

Sharing and Analysis Centres (ISACs) or other collaborative initiatives to enhance your collective security posture.

5. **Perform Regular Vulnerability Assessments**: Conduct frequent vulnerability assessments and penetration testing to identify weaknesses in your systems and applications. This proactive approach helps you discover vulnerabilities before threat actors exploit them.

6. Monitor Security Logs and Network Activity: Set up security monitoring tools and analyse logs to detect unusual activities and potential indicators of compromise. Use intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network traffic for suspicious behaviour.

7. Analyse Incident Data: Study past security incidents and data breaches to identify attack patterns and tactics used by threat actors. This analysis can provide valuable insights into emerging threats and their potential impact on your organisation.

8. Follow Industry Trends: Keep track of emerging technologies and trends in your industry. New innovations can introduce novel attack vectors or security challenges that may need specific attention.

9. Engage in Red Team Exercises: Conduct red team exercises to simulate real-world attack scenarios. This helps test your organisation's readiness to detect and respond to emerging threats.

10. Work with Cybersecurity Partners: Collaborate with cybersecurity vendors, consultants, and managed security service providers (MSSPs) who can offer specialised expertise and threat intelligence to complement your efforts.

11. Stay Updated on Regulatory Changes: Monitor changes in data protection laws and regulations. New regulatory requirements may indicate emerging threats related to specific sectors or data types.

12. Foster a Security Culture: Encourage a culture of cybersecurity awareness among employees. Employees are often the first line of defence against emerging threats, and their vigilance can help identify suspicious activities.

By combining these strategies, your organisation can enhance its ability to identify and respond to emerging threats, ultimately strengthening its overall cybersecurity posture. Remember that threat landscapes change rapidly, so a proactive and continuously evolving approach is crucial to stay ahead of cyber adversaries.

3.TYPES OF EMERGING CYBER THREATS

Emerging cyber threats can be categorised based on various criteria. Here's a breakdown of the categories:

1. Threat Vectors:

- Phishing Attacks: Emails or messages that deceive users into revealing sensitive information or downloading malware.

- Ransomware: Malicious software that encrypts files and demands a ransom for decryption.

- Supply Chain Attacks: Exploiting vulnerabilities in the software or hardware supply chain to distribute malware.

- IoT Exploits: Compromising Internet of Things devices to gain unauthorised access to networks.

- AI-Enhanced Attacks: Leveraging artificial intelligence to create sophisticated and targeted attacks.

- Fileless Malware: Malware that operates in memory without leaving traditional traces on the disk.

- Insider Threats: Threats originating from within the organisation, either intentional or accidental.

2. Industries Targeted:

- Critical Infrastructure: Attacks on sectors like energy, transportation, healthcare, and finance, which have significant implications for public safety and national security.

- Healthcare: Targeting hospitals, medical facilities, or medical research institutions to access sensitive patient data or disrupt operations.

- Financial Services: Attacks aimed at banks, financial institutions, and payment processors to steal financial information or execute fraudulent transactions.

- Government and Defence: Targeting government agencies, defence contractors, or military organisations to gain access to classified information.

- Retail and E-commerce: Cyber threats aimed at retail companies and online marketplaces to steal customer data or execute payment fraud.

3. Attack Methodologies:

- Zero-Day Exploits: Exploiting undisclosed vulnerabilities before patches are available.

- Advanced Persistent Threats (APTs): Sophisticated, long-term attacks targeting specific organisations with specific goals.

- Social Engineering: Manipulating individuals to divulge sensitive information or perform certain actions.

- Distributed Denial of Service (DDoS): Overloading a target's online services to cause disruption or downtime.

- Fileless Attacks: Malware that operates directly in memory without the need for a file on disk.

- Watering Hole Attacks: Compromising websites frequented by the target's employees or users to deliver malware.

4.MONITORING AND THREAT ALLEGIANCE

Continuous monitoring and threat intelligence gathering are crucial components of a proactive cybersecurity approach. Here's why they are of paramount importance:

1. Early Threat Detection: Cyber threats are constantly evolving, and attackers are continuously developing new tactics. Continuous monitoring allows organisations to detect unusual or suspicious activities in real-time, enabling early identification of potential threats before they escalate into full-blown attacks.

2. Timely Response: When security incidents or potential threats are identified promptly through continuous monitoring, organisations can respond swiftly and effectively. This reduces the window of opportunity for attackers, minimising the damage and potential data breaches.

3. Proactive Defence: Threat intelligence provides organisations with valuable insights into the latest attack trends, techniques, and vulnerabilities. Armed with this knowledge, cybersecurity teams can develop proactive defence mechanisms and better anticipate and block potential threats before they materialise.

4. Understanding the Threat Landscape: Cyber threat intelligence helps organisations gain a comprehensive understanding of the current threat landscape specific to their industry and geography. This knowledge enables them to prioritise security efforts and allocate resources effectively.

5. Improved Incident Response and Contingency Planning: Threat intelligence assists in incident response planning by providing context about the attackers' capabilities and tactics. Organisations can develop more robust incident response plans and contingency measures based on real-world threat data.

6. Mitigating Supply Chain Risks: Continuous monitoring and threat intelligence gathering are crucial for managing risks within the supply chain. By monitoring third-party vendors and partners, organisations can detect potential vulnerabilities and threats that could compromise their ecosystem.

7. Compliance and Regulations: Many industries have regulatory requirements for monitoring and incident reporting. Continuous monitoring and threat intelligence gathering help organisations meet compliance standards, providing evidence of due diligence in protecting sensitive data.

8. Real-Time Adaptation: Threat intelligence feeds organisations with real-time information, allowing them to adapt quickly to new threats or attack patterns. By staying up-to-date with the latest threat intelligence, organisations can adjust their security controls and configurations to counter emerging risks effectively.

9. Threat Sharing and Collaboration: Threat intelligence gathering often involves sharing information with trusted cybersecurity partners and communities. By collaborating with others, organisations can strengthen their collective defences, as shared intelligence enhances overall situational awareness.

10. Enhancing Cybersecurity Posture: Continuous monitoring and threat intelligence gathering are essential components of a holistic cybersecurity posture. They complement other security measures like intrusion detection systems, firewalls, and antivirus software, providing a more robust and layered defence strategy.

5. VULNERABILITIES TO PROACTIVELY DEVELOP DEFENCE MECHANISMS

Identifying vulnerabilities is a critical step in proactively developing defence mechanisms to protect against potential cyber threats. By understanding weaknesses in systems, applications, or processes, organisations can take proactive measures to mitigate risks and strengthen their cybersecurity posture. Here's why focusing on vulnerabilities is essential:

1. Risk Prioritisation: Identifying vulnerabilities allows organisations to prioritise their security efforts. Not all vulnerabilities have the same level of risk or potential impact. By assessing and classifying vulnerabilities based on severity and exploitability, organisations can allocate resources effectively to address the most critical ones first.

2. Patch Management: Many vulnerabilities arise from software flaws or outdated systems. Proactively identifying vulnerabilities ensures that organisations can promptly apply security patches and updates provided by vendors, reducing the window of opportunity for attackers to exploit those vulnerabilities.

3. Proactive Mitigation: Armed with information about vulnerabilities, organisations can implement proactive mitigation strategies. This might include configuration changes, network segmentation, access control, or the implementation of additional security measures to prevent potential attacks.

4. Security Awareness Training: Understanding vulnerabilities empowers organisations to conduct targeted security awareness training for employees. Educating

staff about common vulnerabilities, such as social engineering or phishing, helps create a security-conscious workforce.

5. Penetration Testing and Red Teaming: Vulnerability identification is foundational to conducting penetration tests and red team exercises. These tests simulate real-world attack scenarios, allowing organisations to gauge the effectiveness of their defence mechanisms and identify potential gaps in security.

6. Third-Party Risk Management: Organisations often rely on third-party vendors and partners. Identifying vulnerabilities in third-party systems helps organisations assess their overall risk exposure and enforce security standards throughout the supply chain.

7. Incident Response Preparedness: By understanding vulnerabilities, organisations can develop better incident response plans tailored to potential threats. This ensures a more effective and coordinated response when a security incident occurs.

8. Compliance and Regulatory Requirements: Many regulations and standards mandate vulnerability assessments and management. By proactively identifying and addressing vulnerabilities, organisations can meet compliance requirements and avoid potential fines or legal consequences.

9. Continuous Improvement: Cybersecurity is an ongoing process. Regularly identifying vulnerabilities and responding to emerging threats fosters a culture of continuous improvement in an organisation's security practices.

10. Enhanced Resilience: Proactive vulnerability management strengthens an organisation's overall cybersecurity resilience. It reduces the attack surface, making it more challenging for adversaries to exploit weaknesses and gain unauthorised access.

6 - Incident response

Incident response is a reference to companies' processes and technology for intercepting and acknowledge to cyberthreats and security breaches or cyberattacks. Objective of incident responding is to avoid cyber-attacks prior to the occurrence, and to make the business disruption and costing very minimal which is a result from any cyber-attack that occur.

An efficient incident response idea can help cyber team to disclose and hold the cyber threats and reimpose the affected systems at fast speed, and lessen the lost income, official fines and other sum related with those threats.

How incident response works

Incident response planning

These are generated and executed by Computer security incident response team(CSIRT) made of shareholders from all over the company.

An IR planning usually includes:

- The job and duty of each member of CSIRT
- Safety solutions – software, hardware, and different technologies – to place over the enterprise.
- Business continual plan procedures for recovering severely infected systems and data as early as possible in the outrage event.
- A comprehensive incident respond methodology that grounds the steps to be assured at every phase of IR process and by whom.
- Transmission plan to notify the organisation leaders, employees, customers, and Law suits about incidents.
- Guide for recording of gathering information and writing down incidents for post-mortem review.

For CISRT to write various incident response plans for various types of incidents, as every type might require a different response. Many companies have incident response plan to avoid DDoS, malware and ransomware, and phishing and almost half have plan for inner threads.

The Incident Response Process

Many IR follows the exact basic IR framework based on structures made by SANS, NIST and CISA.

- Preparation: The first phase of IR is continual also, it demands that CSIRT constantly have the best processes and tools to submit to capture, isolate and recover from incident as early as possible and with less cost disruption.
  By daily risk assessment the CSIRT recognize network loop holes, defines multiple security incidents that have a impact on network and then classify each type according to its possible effect on company.

- Detection and Analysis: In this phase, the team look thorough malicious or suspicious activities and possible threats. They analyse data, alerts and notifications collected from system logs and from different security tools.
  These days, most organizations utilize one or more security solutions—such as SIEM (security data and occasion organization) and EDR (endpoint district and response)—to help security bunches screen and analyse security occasions in veritable time, and mechanize occasion revelation and reaction shapes. (See “Incident reaction technologies,” underneath for more.)

- Containment: The event response team servers action to prevent breach which cause causing harm to the organization. Control exercises are classified into two types:
  Short-term control techniques aims on preventing latest threats from stretching out by forcing afflicted computer, by pulling contaminated devices offline.
  Long-term control pounder on securing not infected computers by enclosing them in more grounded security controls, such as isolating unstable database from other part of the company.

- Eradication: When the danger has been controlled, the group continues toward full security and complete expulsion of the danger from the framework. This includes effectively killing the actual danger — e.g., obliterating malware, booting an unapproved or rebel client from the organization — and checking on both impacted and unaffected frameworks to guarantee no hints of the break are abandoned.

- Recovery: At the point when the occurrence reaction group is sure the danger has been altogether annihilated, they reestablish impacted frameworks to ordinary activities. This might include sending patches, revamping frameworks from reinforcements, and bringing remediated frameworks and gadgets back on the web.

- Post-incident review: All through each period of the occurrence reaction process, the CSIRT gathers proof of the break and reports the means it takes to contain and destroy the danger. At this stage, the CSIRT audits this data to even more likely grasp the occurrence. The CSIRT looks to decide the main driver of the assault, distinguish how it effectively penetrated the organization, and resolve weaknesses so future episodes of this kind do not happen.

Incident response technologies

As verified above, as well as portraying the means CSIRTs ought to take in case of a security episode, occurrence reaction designs regularly frame the security arrangements that episode reaction groups ought to have set up to do or computerize key occurrence reaction work processes, like assembling and corresponding security information, identifying episodes continuously, and answering in-progress assaults.

The absolute most generally utilized episode reaction innovations include:

SIEM (security data and occasion the executives): SIEM totals and associates security occasion information from different inner security devices (for example firewalls, weakness scanners, danger knowledge takes care of) and from gadgets on the organization. SIEM can help occurrence reaction groups battle 'ready exhaustion' by marks of genuine dangers from the immense volume of warnings these apparatuses produce.

Take off (security organization, robotization and reaction): Take off empowers security groups to characterize playbooks — formalized work processes that coordinate different security tasks and apparatuses because of safety episodes — and to computerize parts of these work processes where conceivable.

EDR (endpoint discovery and reaction): EDR is programming intended to consequently safeguard an association's end clients, endpoint gadgets and IT resources against cyberthreats that move beyond antivirus programming and other conventional endpoint security apparatuses. EDR gathers information constantly from all endpoints on the organization; it breaks down the information progressively for proof of known or thought cyberthreats, and can answer naturally to forestall or limit harm from dangers it distinguishes.

XDR (broadened discovery and reaction): XDR is online protection innovation that binds together security devices, control focuses, information and telemetry sources, and examination across the crossover IT climate (endpoints, organizations, private and public mists) to make a solitary, focal endeavour framework for danger counteraction, identification, and reaction. A yet arising innovation, XDR can possibly help overstretched security groups and security tasks focuses (SOCs) accomplish more with less by disposing of by taking out storehouses between security devices and computerizing reaction across the whole cyberthreat kill chain.

UEBA (client and substance conduct investigation): (UEBA) utilizes conduct investigation, AI calculations, and mechanization to recognize strange and possibly risky client and gadget conduct. UEBA is especially powerful at recognizing insider dangers — malevolent insiders or programmers utilizing compromised insider accreditations — that can escape other security apparatuses because they mirror approved network traffic. UEBA usefulness is frequently included SIEM, EDR, and XDR arrangements.

ASM (append surface administration): ASM arrangements robotize the constant revelation, examination, remediation, and observing of the weaknesses and potential assault vectors across every one of the resources in an association's assault surface.

ASM can reveal beforehand unmonitored network resources, map connections between resources.

IR Team Structure –

1. In-house employees.
2. Partially outsourced.
3. Fully outsourced.

Factors for IR team structure –

1. Need for 24/7 availability.
2. Employee morale.
3. Full time v/s part time team members.
4. Staff Expertise.
5. Cost.

IR Team Dependencies –

1. Intrusion detection –

IR team analysis incidents more promptly and correctly based on the understanding of gains of intrusion detection technologies.

2. Advisory distribution –

The team also may issue employees within the organization regarding new vulnerabilities and threats through automated technique.

3. Education and Awareness –

Promote education and consciousness among the employees and the organization's user groups be aware about detecting, reporting, and responding to incidents via means such as workshops, newsletters, posters, and stickers on monitors or laptops.

4. Information Sharing –

Manage the company's incident data-sharing efforts.

7.CONCLUSION:

In conclusion, identifying and monitoring emerging cyber threats is essential for maintaining a robust and effective cybersecurity defence. The rapidly evolving threat landscape demands proactive measures to stay ahead of cybercriminals and protect sensitive data, systems, and operations.

Continuous monitoring, threat intelligence gathering, and vulnerability assessments are critical components of this proactive approach. By staying informed about the latest attack trends, leveraging threat intelligence feeds, and conducting regular assessments, organisations can gain valuable insights into potential risks and vulnerabilities.

Proactive defence mechanisms, informed by this knowledge, allow organisations to respond swiftly to emerging threats and implement timely mitigation strategies. This early detection and rapid response reduce the impact of cyberattacks, minimise downtime, financial losses, and safeguard the organisation's reputation.

Furthermore, fostering a security-conscious culture, encouraging collaboration with cybersecurity communities, and investing in employee training are essential for building a resilient defence against emerging threats. A dynamic cybersecurity strategy, continuously adapted to address the changing threat landscape, is key to ensuring the long-term security of an organisation's digital assets.

In a world where cyber threats are ever-evolving, vigilance, collaboration, and continuous improvement are the cornerstones of an effective cybersecurity approach. By embracing these principles and dedicating resources to identify and address emerging threats, organization can better protect themselves from cyber risks and maintain a strong cybersecurity posture.

Contributions:

Identify Emerging Threats - Lokesh , Avinash

Research And Development - Jayant

Cyber Incident Response - Chirag, Rohit

Security Awareness - Adarsh,Sadu

Compliance and Regulations - Hema

References:

https://uhra.herts.ac.uk/bitstream/handle/2299/12999/Infrastructure_Sec_NA_final_v3.pdf?sequence=2&isAllowed=y

https://books.google.co.in/books?hl=en&lr=&id=V2RzAwAAQBAJ&oi=fnd&pg=PP1&dq=Critical+Infrastructure+Security+Threats:+Industrial+Networks&ots=54CaRcszji&sig=mNkGvCGhtlmbq2xzruE0A8rQGn8&redir_esc=y#v=onepage&q&f=true

https://www.threatintelligence.com/blog/proactive-cybersecurity

https://www.commonwealth.com/insights/a-guide-to-identifying-emerging-risks-and-taking-action
https://www.exabeam.com/information-security/cyber-security-threat/
https://www.rubrik.com/products/threat-monitoring
https://www.sciencedirect.com/science/article/abs/pii/S0167739X17314723