Safeguarding Judicial Institutions from cyber attacks

Mr. Justice A. Muhamed Mustaque
High Court of Kerala

eJudiciary and Cyber attacks - Is The Threat Real?

- The notion that judicial institutions are immune from cyber attacks is false.
- Judiciary has experienced a **sharp increase in cyber incursions** in the US and the Europe the past years.
- 24 million attempts in 2019 as compared to 9 million attempts of cyber attacks in 2016 in the US alone.
- Judiciary is a goldmine of data and hence it is bound to be attacked.

Cyber attack waves that hit Ukraine

- In 2017 UkrainIan Government, Banks and Health system was subjected to a “Massive Coordinated Cyber Invasion”.
- Unlike a Ransomware attack like WannaCry attacks on the NHS of UK and elsewhere this was a targeted attack that was more surgical that random.
- The particular malware in this instance was a modified version of a known Ransomware called Petya.
- While a typical Ransomware attack is done on the unsuspecting for financial motives similar institutions in governance may be targeted to sow chaos and destabilize a regime, Key targets being: Administration, Defense, and most importantly the justice system.
- In an increasingly connected world reliant on complex computer systems malware is another WMD not unlike a Nuclear Weapon

Why Is Judiciary Susceptible To Cyber Attacks

- Often in large networks with weak links, any **one unguarded entry point** may provide unfettered access to all of the connected system.
- Network security is frequently overlooked in an institution older than the computer age and has since adopted it.
- Personnel involved in the Judiciary are not always adept to best practices involved in keeping the system safe from cyber attacks.
- Any one attack maybe mean access to a large amount of crucial data that may be valuable to criminal enterprises, such as bank details, Adhaar numbers, et cetera.
- Individual systems are often not updated and running operating systems long past the developer has dropped support for it.

Categories of Cyber Attacks

- **System Attack** - any attempt to gain authorized access to a computer, computing system, or computer network with the intent to cause damage. Cyber attacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems. Eg: DDOS Attack

- **Network Attack** - any method, process, or means used to maliciously attempt to compromise network security.There are two main types of network attacks: passive and active. In passive network attacks, malicious parties gain unauthorized access to networks, monitor, and steal private data without making any alterations. Active network attacks involve modifying, encrypting, or damaging data.

Categories of Cyber Attacks

- **Web Application** - an application that runs on a web server and users access it using a web browser. Web applications often deliver content from a database based on what the user selects. they often do a lot of processing on the side of the browser, not the server. web applications used to be called widgets. eg: chrome, internet explorer. Web applications are very vulnerable to attacks because, by design, they cannot be protected by firewalls. they must be available to everyone, all the time, unless they are on an intranet. Malicious hackers can, therefore, try to exploit them easily. Attacks usually exploit the fact that web applications accept user input and this input may not be screened for malicious content. There are two ways to protect against these attacks: Firstly - find and eliminate vulnerabilities: this can be done manually by hiring specialists but can also use a professional scanner. Secondly - web application firewalls but they do not eliminate problems and can be bypassed by attackers

Categories of Cyber Attacks

- **Human Base/ Social Engineering Attack** - Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.Social engineers manipulate human feelings, such as curiosity or fear, to carry out schemes and draw victims into their traps. Eg : Baiting , Scareware , Pretexting , Phishing , Spear Phishing

Types of Cyber Attacks

- **Advanced persistent threat (APT)** attacks attempt to maintain ongoing, extended access to a network by continually rewriting malicious code and using sophisticated evasion techniques. A successful APT attack results in complete invisible control of systems over a lengthy period time. APTs typically use socially engineered attacks to get a foot in the network's door.
- **Code-injection** attacks involve the submission of incorrect code into a vulnerable computer program without detection. Through these attacks, cybercriminals trick the target system into executing a command or allowing access to unauthorized data. The most common code injection attack uses **Standard Query Language (SQL)** through an online application.

Types of Cyber Attacks

- **Slow connections In denial of service (DoS) and distributed denial of service (DDoS)** attacks, systems are overloaded with irrelevant data requests. Resources for legitimate data requests are stretched and system response slows noticeably. Often, systems may crash.
- **Pop-ups** that appear to be a legitimate mechanism for blocking a cyber attack may actually be malicious software. Pop-ups might include disguised links to malicious websites, fake coupons, or digital ads.
- **Hacktivism** is the act of misusing a computer system or network for a socially or politically motivated reason.Their goal is to disrupt services and bring attention to a political or social cause.Hacktivists often use denial-of-service or distributed DoS (DDoS) attacks where they overwhelm a website and disrupt traffic.

Risk, Threat, and Vulnerability

- **Risk** - the potential for loss or damage when a threat exploits a vulnerability. Eg: financial loss. It is the potential loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability
- **Vulnerability** - a known weakness of an asset (resource) that can be exploited by one or more attacks. in other words, it is a known issue that allows an attack to succeed. eg: outdated antivirus installed in the system making it vulnerable to attack.
- **Threat** - a new or newly discovered incident that has the potential to harm a system or your company overall
- **Threat exploits vulnerability which leads to risk can damage assets of the organization and it can be safeguarded by adopting suitable countermeasures. This is also called a Risk Life Cycle.**

Basic Security Domains

1. **Proactive Services**

- technical audit - A thorough verification of a supplier's manufacturing processes and quality control systems to provide confidence that your standards will be met or that any shortfalls will be resolved.
- compliance audit - an assessment as to whether the provisions of the applicable laws, rules, and regulations made thereunder and various orders and instructions issued by the competent authority are being complied with.
- red team audit - Red Teaming is a process that tests the current security of an organization’s system by trying to hack them like a real-world hacker.The red team will try to get in and access sensitive information in any way possible, as quietly as possible.
- security management
- security consulting

Basic Security Domains

2. Active Services

- security operations center
- real-time monitoring

3. Reactive Services

- CERT is a service-computer emergency response team. The Indian Computer Emergency Response Team (CERT-IN or ICERT) is an office within the Ministry of Electronics and Information Technology of the Government of India. It is the nodal agency to deal with cyber security threats like hacking and phishing.
- Digital forensics - focuses on identifying, acquiring, processing, analyzing, and reporting on data stored electronically.
- investigation
-

Preventive Measures

- Awareness amongst the personnels regarding the best practices and Standard Operating Procedures.
- A dedicated IT professional team, to manage the systems and make sure the software is kept up to date and all security patches are installed.
- Redundant storage systems to ensure a safe and secure copy of all important data sets are accessible in the case of a cyberattack.
- A regular threat assessment of the complete system to ensure all the safety checks are working in the optimal condition.
- Using a variant of Linux that is less likely to be vulnerable to an attack unlike a mainstream Windows operating system
- Systematic updation of all softwares and systems.

Best practices and SoP to stave off Cyber attacks

- Temporary files shall be deleted from time to time.
- Two Factor Authentication for logging in preferably with a physical randomized security key
- Logging out from all accounts at the end of the day
- Using VPN and related services to mask access to extraneous networks
- Being vigilant of common phishing attempts; such as, being aware of the difference between a secured site (https - green) and an unsecured site (http)
- Avoiding the opening of unauthorized websites and/or logging into accounts that may have access to the system
- Installation of Antimalware software ,which gives a threat analysis on a day to day basis, in all the systems
- Avoid using open networks
- Test the devised post - attack recovery plan on a regular basis

Response to a cyber incursion

- Creating an attack response team
- Devise a plan which can be put into action post an attack
- Data Backup and using cloud storage for data recovery
- Assess the situation - understand how far the data have been compromised, understand the nature of the intrusion. Assess where the vulnerability was found
- Block - preventing further damage is the highest priority. It may be necessary to take
- disruptive and costly steps such as removing infected computers and temporarily
- shutting down the court's website to limit the damage. Consider reformatting hacked
- computers and restoring data with clean backups, or simply buying new computers
- Collect - gather as much data as possible
- about the attack and do a thorough analysis and investigation. Understanding
- what happened is key to identifying the intruder, but more importantly, to
- prevent further intrusion.

Precautions An Individual Can Take

- Updation is the key - make sure all your softwares and systems are regularly updated
- Installing an antimalware software in your office system
- Use two factor authentication passwords
- Avoid using an open network
- Clear temporary files , cookies and unwanted extensions regularly
- Be careful while downloading email attachments - make sure its from a reliable source and be wary of proxy google
- clear unwanted services → this can be done by contacting a system engineer and cleaning it on a regular basis.