**SAD Lab**

**Exp-1**

**Name: Shashwat Tripathi**

**Division: D20A**

**Roll no: 64**

**Aim:** To study different laws and standards of cyber security.

**Theory:**

**Cybersecurity laws**

Cyber laws, more commonly known as internet laws, are laws that are related to legal informatics, regulating the digital distribution of information, e-commerce, software, and information security. It usually covers many related areas, such as usage and access to the Internet, freedom of speech, and privacy.

Many security and privacy issues arise with the use of the internet. Ingenious criminals have been known to use advanced strategies to carry out unauthorized activities and potential fraud. Therefore, the need to protect against them is substantial, and the most effective method of doing so is to enforce a cyber security policy.

These cyber security laws and policies are made to protect individuals and businesses online by holding these criminals accountable for their malicious actions and sentencing them to appropriate punishment as decided by the federal government.

There are different types of cyber laws around the world, here are the main types of cyber laws:

1. Data Protection Laws

* **Purpose:** Protects personal data from unauthorized access and misuse.
* **Key Principles:** Consent, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality.
* **Examples:** The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011; Proposed Personal Data Protection Bill, 2019.

1. Cybercrime Laws

* **Purpose:** Criminalize illegal activities conducted via the internet or other digital means.
* **Key Areas:** Hacking, identity theft, cyberstalking, online fraud.
* **Examples:** The Information Technology Act, 2000 (IT Act); Indian Penal Code (IPC) Sections related to cybercrimes.

1. Cybersecurity Laws

* **Purpose:** Ensure the security of information systems and critical infrastructure.
* **Key Requirements:** Risk assessments, incident response plans, reporting breaches.
* **Examples:** The National Cyber Security Policy, 2013; The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

1. Copyright and Intellectual Property Laws

* **Purpose:** Protect creators' rights over their intellectual works.
* **Key Elements:** Exclusive rights to reproduce, distribute, perform, and display the work.
* **Examples**: The Copyright Act, 1957; The Patents Act, 1970; The Trade Marks Act, 1999.

1. E-commerce Laws

* **Purpose:** Regulate online business activities.
* **Key Areas**: Electronic contracts, consumer protection, data privacy.
* **Examples:** The Information Technology Act, 2000 (IT Act); The Consumer Protection (E-commerce) Rules, 2020.

1. Digital Signature Laws

* **Purpose:** Validate the legal status of digital signatures.
* **Key Principles:** Authenticity, integrity, non-repudiation.
* **Examples:** The Information Technology Act, 2000 (IT Act); Controller of Certifying Authorities (CCA) regulations.

1. Domain Name Laws

* **Purpose:** Manage the registration and use of internet domain names.
* **Key Issues:** Trademark infringement, cybersquatting, domain disputes.
* **Examples:** INDRP (IN Domain Name Dispute Resolution Policy); The Trade Marks Act, 1999.

1. Privacy Laws

* **Purpose:** Protect individuals' privacy rights and personal information.
* **Key Elements:** Consent, access rights, data security.
* **Examples:** The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011; Proposed Personal Data Protection Bill, 2019.
* **Purpose:** Ensure the right to express opinions and ideas without censorship.
* **Key Limitations:** Hate speech, defamation, incitement to violence.
* **Examples:** Article 19(1)(a) of the Indian Constitution; The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

1. Freedom of Expression Laws

* **Purpose:** Ensure the right to express opinions and ideas without censorship.
* **Key Limitations:** Hate speech, defamation, incitement to violence.
* **Examples:** Article 19(1)(a) of the Indian Constitution; The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

1. Consumer Protection Laws

* **Purpose:** Safeguard consumer rights and ensure fair trade practices.
* **Key Areas:** Product safety, fair advertising, right to redress.
* **Examples:** The Consumer Protection Act, 2019; The Consumer Protection (E-commerce) Rules, 2020.

**Cybersecurity standards**

**1. ISO/IEC 27001:**

Description: This standard specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). It is designed to be applicable to all organizations, regardless of type, size, or nature.

Purpose: To manage the security of assets such as financial information, intellectual property, employee details, and information entrusted by third parties.

Benefits: Demonstrates to clients and stakeholders that the organization is managing the security of their information effectively.

**2. ISO/IEC 27002:**

Description: This standard provides guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.

Purpose: To serve as a reference for selecting controls within the process of implementing an ISMS based on ISO/IEC 27001.

Benefits: Helps organizations implement commonly accepted information security controls.

**3. ISO/IEC 27005:**

Description: This standard provides guidelines for information security risk management.

Purpose: To help organizations identify and manage risks associated with the use of information and information systems.

Benefits: Supports the risk management framework of ISO/IEC 27001.

**4. ISO/IEC 27032:**

Description: This standard focuses on cybersecurity and provides guidance for improving the state of cybersecurity.

Purpose: To address issues of cyber risks and how to manage them in different contexts such as cyber incidents, cyberspace, and critical information infrastructure protection (CIIP).

Benefits: Enhances cybersecurity posture and collaboration among different sectors and stakeholders.

**5. ISO/IEC 27017:**

Description: This standard provides guidelines for information security controls applicable to the provision and use of cloud services.

Purpose: To ensure that cloud service providers and their customers have clear guidance on securing cloud environments.

Benefits: Improves the security of cloud-based systems and data, ensuring compliance with information security standards.

**6. NIST Cybersecurity Framework (CSF):**

Description: Developed by the National Institute of Standards and Technology (NIST), this framework provides a policy framework of computer security guidance for how private sector organizations in the US can assess and improve their ability to prevent, detect, and respond to cyber attacks.

Purpose: To provide a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes.

Benefits: Helps organizations manage and reduce cybersecurity risks in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

**7. CIS Controls:**

Description: The Center for Internet Security (CIS) Controls are a set of best practices for securing IT systems and data against cyber attacks.

Purpose: To provide actionable steps to improve an organization's cybersecurity posture.

Benefits: Offers prioritized and simplified practices to improve cybersecurity.

**8. GDPR (General Data Protection Regulation):**

Description: A regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas.

Purpose: To give individuals control over their personal data and to simplify the regulatory environment for international business.

Benefits: Ensures robust data protection for all individuals within the EU and EEA.

**9. HIPAA (Health Insurance Portability and Accountability Act):**

Description: A US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other healthcare providers.

Purpose: To ensure that individuals' health information is properly protected while allowing the flow of health information needed to provide high-quality health care.

Benefits: Protects sensitive patient health information from being disclosed without the patient's consent or knowledge.

**10. PCI-DSS (Payment Card Industry Data Security Standard):**

Description: A set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

Purpose: To protect cardholder data from breaches and theft.

Benefits: Helps organizations that handle card payments to prevent credit card fraud, hacking, and various other security vulnerabilities and threats.

**Cybersecurity Attacks:**

**1. Session hijacking**

* **Description :** Session hijacking is one of multiple types of MITM attacks. The attacker takes over a session between a client and the server. The computer being used in the attack substitutes its Internet Protocol (IP) address for that of the client computer, and the server continues the session without suspecting it is communicating with the attacker instead of the client. This kind of attack is effective because the server uses the client's IP address to verify its identity. If the attacker's IP address is inserted partway through the session, the server may not suspect a breach because it is already engaged in a trusted connection.
* **Prevention :** To prevent session hijacking, use a VPN to access business-critical servers. This way, all communication is encrypted, and an attacker cannot gain access to the secure tunnel created by the VPN.

**2. Brute force attacks**

* **Description :** A brute-force attack gets its name from the “brutish” or simple methodology employed by the attack. The attacker simply tries to guess the login credentials of someone with access to the target system. Once they get it right, they are in. While this may sound time-consuming and difficult, attackers often use bots to crack the credentials. The attacker provides the bot with a list of credentials that they think may give them access to the secure area. The bot then tries each one while the attacker sits back and waits. Once the correct credentials have been entered, the criminal gains access.
* **Prevention :** It is wise to use random passwords without regular words, dates, or sequences of numbers in them. This is effective because, for example, even if an attacker uses software to try to guess a 10-digit password, it will take many years of non-stop attempts to get it right.

**3. Web attacks**

* **Description :** Web attacks refer to threats that target vulnerabilities in web-based applications. Every time you enter information into a web application, you are initiating a command that generates a response. Attackers work within the frameworks of these kinds of requests and use them to their advantage.
* **Prevention :** To avoid web attacks, inspect your web applications to check for—and fix—vulnerabilities. One way to patch up vulnerabilities without impacting the performance of the web application is to use anti-CSRF tokens. A token is exchanged between the user’s browser and the web application. Before a command is executed, the token’s validity is checked. If it checks out, the command goes through—if not, it is blocked.

**4. Insider threats**

* **Decsription :** People within the organization often have an in-depth understanding of its cybersecurity architecture, as well as how the business reacts to threats. This knowledge can be used to gain access to restricted areas, make changes to security settings, or deduce the best possible time to conduct an attack.
* **Prevention :** While MFA may not prevent all attacks on its own, it makes it easier to ascertain who is behind an attack—or an attempted one—particularly because only relatively few people are granted access to sensitive areas in the first place. As a result, this limited access strategy can work as a deterrent. Cybercriminals within your organization will know it is easy to pinpoint who the perpetrator is because of the relatively small pool of potential suspects.

**5. Trojan horses**

* **Description :** A Trojan horse attack uses a malicious program that is hidden inside a seemingly legitimate one. When the user executes the presumably innocent program, the malware inside the Trojan can be used to open a backdoor into the system through which hackers can penetrate the computer or network. This threat gets its name from the story of the Greek soldiers who hid inside a horse to infiltrate the city of Troy and win the war. Once the “gift” was accepted and brought within the gates of Troy, the Greek soldiers jumped out and attacked.
* **Prevention :** To prevent Trojan attacks, users should be instructed not to download or install anything unless its source can be verified. Also, NGFWs can be used to examine data packets for potential threats of Trojans.

**6. Drive-by attacks**

* **Description :** In a drive-by attack, a hacker embeds malicious code into an insecure website. When a user visits the site, the script is automatically executed on their computer, infecting it. The designation “drive by” comes from the fact that the victim only has to “drive by” the site by visiting it to get infected. There is no need to click on anything on the site or enter any information.
* **Prevention :** To protect against drive-by attacks, users should make sure they are running the most recent software on all their computers, including applications like Adobe Acrobat and Flash, which may be used while browsing the internet. Also, you can use web-filtering software, which can detect if a site is unsafe before a user visits it.

**7. XSS attacks**

* **Description :** With XSS, or cross-site scripting, the attacker transmits malicious scripts using clickable content that gets sent to the target’s browser. When the victim clicks on the content, the script is executed. Because the user has already logged into a web application’s session, what they enter is seen as legitimate by the web application. However, the script executed has been altered by the attacker, resulting in an unintended action being taken by the “user.”
* **Prevention :** One of the most straightforward ways of preventing XSS attacks is to use a whitelist of allowable entities. This way, anything other than approved entries will not be accepted by the web application. You can also use a technique called sanitizing, which examines the data being entered, checking to see if it contains anything that can be harmful.

**8. Eavesdropping attacks**

* **Descrption :** Eavesdropping attacks involve the bad actor intercepting traffic as it is sent through the network. In this way, an attacker can collect usernames, passwords, and other confidential information like credit cards. Eavesdropping can be active or passive.
* **Prevention :** Both active and passive eavesdropping are types of MITM attacks. One of the best ways of preventing them is by encrypting your data, which prevents it from being used by a hacker, regardless of whether they use active or passive eavesdropping.

**9. Birthday attack**

* **Description :** In a birthday attack, an attacker abuses a security feature: hash algorithms, which are used to verify the authenticity of messages. The hash algorithm is a digital signature, and the receiver of the message checks it before accepting the message as authentic. If a hacker can create a hash that is identical to what the sender has appended to their message, the hacker can simply replace the sender’s message with their own.
* **Prevention :** To prevent birthday attacks, use longer hashes for verification. With each extra digit added to the hash, the odds of creating a matching one decrease significantly.

**10. Malware attack**

* **Description :** Malware is a general term for malicious software, hence the “mal” at the start of the word. Malware infects a computer and changes how it functions, destroys data, or spies on the user or network traffic as it passes through. Malware can either spread from one device to another or remain in place, only impacting its host device.
* **Prevention :** In a malware attack, the software has to be installed on the target device. This requires an action on the part of the user. Therefore, in addition to using firewalls that can detect malware, users should be educated regarding which types of software to avoid, the kinds of links they should verify before clicking, and the emails and attachments they should not engage with.

**Conclusion:**

Thus, we have studied about different laws and standards of cybersecurity