SECURITY POLICIES, LAWS AND COMPUTER CRIMES

- **SOCIAL ENGINEERING, IDENTITY THEFT, AND RECOVERY**
- **ISSUES SURROUNDING THE MISUSE OF ACCESS AND BREACHES IN SECURITY**
- **CRIME PREVENTION STRATEGIES**

SOCIAL ENGINEERING

- Includes different tactics used to convince someone to share specific information or do a particular thing for inappropriate reasons.
- Using tricks to manipulate people's minds and gain access to an IT system.
- Combining technology with psychological tricks to achieve goals beyond the IT world.

The increasing use of IT technologies has naturally led to an increase in the use of such techniques.

SOCIAL ENGINEERING TECHNIQUES & ATTACK TYPES

PHISHING: Aim to convince people to share important information like passwords or financial details. These attacks use a mix of trickery and social engineering.

PRETEXTING: This method involves using a pretext, which is a false justification for a particular action, to build trust and deceive the victim. For instance, the attacker might pretend to be from IT support, asking the target for their password under the guise of performing maintenance.

BAITING: When someone tricks you into doing something by offering something you really want.

QUID PRO QUO: which means "something for something" in Latin, refers to a situation where someone requests information in exchange for compensation.

TAILGATING: aim to convince people to share important information like passwords or financial details. These attacks use a mix of trickery and social engineering.

IDENTITY THEFT

also called **identity fraud**, is a criminal act where a person acquires essential pieces of personally identifiable information (PII), like Social Security or driver's license numbers, intending to pretend to be someone else.

THE TWO TYPES OF IDENTITY THEFT

True-name identity theft occurs when the thief utilizes personally identifiable information (PII) to open new accounts. This may involve the thief opening a new credit card account, setting up cellular phone service, or establishing a new checking account to obtain blank checks.

Account-takeover identity theft occurs when the imposter utilizes personally identifiable information (PII) to access the person's existing accounts. Usually, the thief changes the mailing address on an account and accumulates charges before the victim becomes aware of the issue.

Examples of identity theft include the following:

- **Financial identity theft** is the most common form, focusing on using a stolen identity to gain economic benefits.
- **Medical identity theft** occurs when someone steals information like health insurance member numbers to receive medical services. The victim might see fraudulent bills in their health insurance account.
- **Criminal identity theft** happens when a person under arrest provides stolen identity information to the police. If successful, the victim gets charged instead of the thief.
- **Senior identity theft** targets individuals over 60, considering them vulnerable. Seniors should stay aware of evolving methods used by thieves to steal information.
- **Identity cloning for concealment** involves a thief pretending to be someone else to evade law enforcement or creditors. Since this isn't always financially motivated, it's challenging to trace without a clear paper trail.
- **Synthetic identity theft** occurs when a thief creates a false identity by combining pieces of personally identifiable information (PII) from various sources. For instance, they might use a stolen Social Security number with an unrelated birthdate. Tracking this type of theft is difficult because the thief's activities are recorded under a fabricated identity not belonging to a real person.

Identity theft techniques

- **Mail theft** involves stealing credit card bills and junk mail from a victim's mailbox or public mailboxes on the street.
- **Dumpster diving** is when an identity thief retrieves personal paperwork and discarded mail from dumpsters. This can be an easy way for them to get information, especially if people discard preapproved credit card applications without shredding them, increasing the risk of credit card theft.
- **Shoulder surfing** occurs when the thief gathers information by watching the victim fill out personal details on a form, enter a passcode on a keypad, or provide a credit card number over the phone.

Phishing uses email to trick people into providing their personally identifiable information (PII). Phishing emails may contain malicious attachments designed to steal PII or links to fake websites where individuals are prompted to enter their information.

Warning signs of identity theft include the following:

- Bills for items you did not buy.
- Debt collection calls for accounts you did not open.

- Information on your credit report for accounts you did not open.
- Denials of loan applications.
- Mail stops coming to, or is missing from, your mailbox.

Identity theft recovery

I**f someone's personal information is stolen**, they must reach out to the relevant organization depending on the type of information involved. This might include contacting their bank, credit card company, health insurance provider, or the IRS (Internal Revenue Service).

If your personal information (PII) is exposed in a data breach, contact the company responsible to learn about the assistance and protections they provide for victims and their data. It's important to follow up to ensure appropriate measures are taken to address the situation

File a police report:
Banks are also concerned about scams. If you're a victim of identity theft, some banks might ask for a police report before refunding any unauthorized charges or withdrawals. Make sure to report the identity theft to your local law enforcement promptly.

ISSUES SURROUNDING THE MISUSE OF ACCESS AND BREACHES IN SECURITY

1. The Threat:

Privilege abuse is a critical security threat allowing attackers to access confidential data, delete critical data, and modify system configurations.

Over 90% of security incidents involved some form of privilege abuse in 2020.

Organizations face devastating consequences like unauthorized access, data theft, and financial losses due to privilege abuse.

2. Attacker Tactics:

Attackers exploit vulnerabilities like operating system and application issues using brute force, social engineering, and malware.

Once access is gained, they install backdoors, create admin accounts, or modify existing ones.

3. Prevention Strategies:

Strong authentication: Implement multi-factor authentication and complex passwords.

Least privilege model: Grant users only the minimum privileges needed for their tasks.

Vulnerability management: Regularly assess and patch vulnerabilities.

User training: Educate users on data protection best practices and security protocols.

4. Required steps on Controlling and Managing Abuse:

Role-based access control (RBAC): Limit access based on assigned roles.

Regular credential checks: Monitor usernames, passwords, and MFA usage.

Least privileged user access (LPUA): Minimize user privileges to essential needs.

Reviewing privileged accounts: Ensure users have necessary and correct privileges.

Monitoring audit logs: Track user activity and system changes for suspicious behavior.

5. Additional Measures:

Inventory of privileged accounts: Identify and track all accounts with elevated access.

Restricting new privileged accounts: Require authorization for creating new accounts.

Enforcing accountability: Implement disciplinary guidelines for privilege abuse violations.

Overall, the article emphasizes the seriousness of privilege abuse and provides actionable steps organizations can take to prevent, detect, and manage this threat.

CRIME PREVENTION STRATEGIES

Access Control Measures

3 Types of Access Control:

Discretionary Access Control (DAC): Discretionary Access Control (DAC) gives control to resource owners or administrators to decide who gets access and at what level. In this model, each resource has an owner who determines access permissions, and Access Control Lists (ACLs) are used to define these permissions.

Role-Based Access Control (RBAC): Role-Based Access Control (RBAC) focuses on assigning access based on organizational roles rather than individual users. System administrators define roles and determine the resources each role needs access to. Users are then assigned to roles, each providing specific permissions.

Attribute-Based Access Control (ABAC): Attribute-Based Access Control (ABAC) is a more complex strategy that considers multiple attributes for both users and resources. Users can only access resources that align with corresponding attributes, which may include user demographics, resource properties, or environmental factors.

Multi-Factor Authentication (MFA) significantly enhances security by requiring users to provide multiple forms of identification before gaining access to a system or platform. The primary goal is to add extra layers of defense beyond traditional password-based authentication.

Examples: Biometric Authentication and SMS Code

The effectiveness of MFA lies in mitigating common security threats:

Credential Theft: Even if attackers steal a user's password, they would still need the additional factor (e.g., a temporary code from a mobile app) to successfully authenticate.

Phishing Attacks: MFA can protect against phishing, as attackers would need more than just a username and password to gain unauthorized access.

Brute Force Attacks: Even if an attacker manages to guess or crack a password, MFA introduces an additional layer that makes it exponentially more difficult to compromise an account.

Encryption and Data Protection:

Data encryption transforms data into a coded form (ciphertext) that requires a secret key or password for decryption. It safeguards digital information during storage and transmission, with encrypted data referred to as ciphertext and unencrypted data as plaintext

The main purpose is to **ensure the confidentiality of digital data**, protecting it from unauthorized access both when stored on computer systems and during transmission over networks.

Types of Encryptions:

Symmetric-Key Ciphers: Uses the same key for encryption and decryption.Fast but requires secure key exchange.

Asymmetric Cryptography: Uses different public and private keys. RSA algorithm is widely used for secure data transmission.

Incident Response Planning: Incident response planning contains specific directions for specific attack scenarios, avoiding further damages, reducing recovery time and mitigating cybersecurity risk. Incident response procedures focus on planning for security breaches and how organizations will recover from them.

Explanation: Incident response planning is an outline on how to minimize the duration and damage of security incidents, identifies stakeholders, improves recovery time, and reduces negative publicity.

Who is Responsible for Incident Response Planning?
Organizations should form a computer security incident response team (CSIRT) who is responsible for analyzing, categorizing and responding to security incidents.

Incident response manager:
oversees and prioritizes actions during detection, containment and recovery of an incident.

Security analysts:
support and work directly with affect resources, as well as implementing and maintaining technical and operational controls.

Threat researchers:
provide threat Intelligence and context around security incidents. They may use third-party tools and the Internet to understand current and future threats.

How to create a well-incident response plan
An incident response plan should be set up to address a suspected data breach in a series of phases. Within each phase, there are specific areas of need that should be considered.

4 Types of Threat Intelligence

1. **Tactical Threat Intelligence** - This type of threat intelligence deals with the specific methods and tools used by cybercriminals. It provides information about the immediate threats facing an organization such as new malware or phishing techniques.

2. **Operational Threat Intelligence** - Operational threat intelligence focuses on the tactics, techniques and procedures of threat actors, and provides a deeper understanding of the threat landscape. It offers insights into the behaviors and methods of cybercriminals, helping businesses anticipate and prepare for possible attacks.

3. **Strategic Threat Intelligence** - This form of threat intelligence looks at the bigger picture. It provides insights into the long-term trends and emerging threats in the cybersecurity landscape. It helps businesses understand how higher-level factors such as changes in technology, law or geopolitics can influence cyber threats.

Explanation: Strategic threat intelligence allows businesses to plan their long-term cybersecurity strategy, understanding where to invest and how to adapt as the threat landscape evolves.

4. **Technical Threat Intelligence** - Being most data-centric, technical threat intelligence provides information about malicious indicators such as IP addresses, domains, URLs and malware hashes associated with threat actors. It is used primarily by firewalls, intrusion detection systems and antivirus software to identify and block known threats.

Legal and Ethical Considerations aspects of crime prevention strategies:

Laws and Regulations: Different countries have specific laws governing data privacy, surveillance, and cybersecurity. Obey to these laws while implementing crime prevention strategies is crucial to avoid legal consequence

Ethical Aspects

Privacy Concerns: Implementing surveillance or data monitoring techniques for crime prevention should balance the need for security with individuals' rights to privacy.

Bias and Discrimination: Certain crime prevention technologies, like predictive policing algorithms, might maintain biases. Ensuring fairness and avoiding discrimination in implementing these strategies is an ethical important.

Transparency and Accountability: Ethical crime prevention involves being transparent about methods used and being accountable for their consequences. Transparency helps build trust between authorities and the public.

Crime prevention strategies often involve various techniques, technologies, and approaches on ethical and legal consideration.

Responsible Disclosure Policies: Reporting Vulnerabilities: Responsible disclosure involves ethically reporting discovered vulnerabilities to the affected organization without publicly disclosing them immediately.

Cooperation and Collaboration: Ethical hackers should cooperate with organizations to fix vulnerabilities, allowing time for patches to be developed and deployed before making the issue public.

Recognition and Acknowledgment: Organizations should recognize the efforts of ethical hackers who report vulnerabilities and collaborate in resolving security issues

References:

Exploring Privilege Abuse in Cyber Security: Uncovering the Impact and Strategies to Prevent Unauthorized Access and Misuse of Data (cdomagazine.tech)

What Is Threat Intelligence? Definition, Types & Process – Forbes Advisor

What is an Incident Response Plan? | UpGuard

https://www.cloudmask.com/blog/data-breaches-threats-and-consequences

https://www.cdomagazine.tech/opinion-analysis/article_94796266-d85c-11ed-b27b-f7a62e3cf746.html

https://www.techtarget.com/searchsecurity/definition/identity-theft#:~:text=Identity%20theft%2C%20also%20known%20as,numbers%2C%20to%20impersonate%20someone%20else.

https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering