Certified Professional in Cyber Security for Project Managers

Risk Management in Cyber Security

Certified Professional in Cyber Security for Project Managers Glossary

A

Access Control: Access control is a security feature that determines who is allowed to access resources or perform actions. It involves limiting access to authorized users and denying access to unauthorized users. Access control mechanisms include passwords, biometric authentication, and access control lists.

Advanced Persistent Threat (APT): An advanced persistent threat is a targeted cyber attack in which an unauthorized user gains access to a network and remains undetected for an extended period. APTs are typically carried out by nation-state actors or organized cybercriminal groups.

Attack Surface: The attack surface refers to all the points where an attacker could potentially exploit a system. This includes vulnerabilities in hardware, software, and network configurations. Reducing the attack surface is a key component of risk management in cybersecurity.

Authentication: Authentication is the process of verifying the identity of a user or system. This typically involves providing credentials such as a username and password or using biometric data like fingerprints. Strong authentication mechanisms are essential for protecting against unauthorized access.

B

Backup and Recovery: Backup and recovery are essential components of a comprehensive cybersecurity strategy. Regularly backing up data ensures that it can be restored in the event of a cyber attack or data loss. Recovery involves restoring systems and data to their original state after an incident.

Botnet: A botnet is a network of compromised computers or devices that are controlled by a central command and used to carry out malicious activities. Botnets are often used to launch distributed denial-of-service (DDoS) attacks or send spam emails.

C

Compliance: Compliance refers to adhering to regulations, standards, and best practices related to cybersecurity. Organizations must comply with laws such as the General Data Protection Regulation (GDPR) and industry standards like the Payment Card Industry Data Security Standard (PCI DSS) to protect sensitive data.

Confidentiality: Confidentiality is one of the three pillars of information security, along with integrity and availability. It ensures that sensitive information is only accessible to authorized users and protected from unauthorized disclosure.

Countermeasure: Countermeasures are security controls or actions taken to prevent or mitigate cyber threats. Examples of countermeasures include firewalls, intrusion detection systems, and encryption. Implementing effective countermeasures is essential for protecting against cyber attacks.

Cybersecurity: Cybersecurity is the practice of protecting computer systems, networks, and data from cyber threats. It includes measures to prevent, detect, and respond to attacks, as well as ongoing monitoring and risk assessment.

D

Data Breach: A data breach occurs when sensitive information is exposed to unauthorized parties. This can result from hacking, insider threats, or accidental disclosure. Data breaches can have serious consequences for organizations, including financial loss and damage to reputation.

Denial of Service (DoS): A denial-of-service attack is a cyber attack that disrupts the availability of a system or network by overwhelming it with traffic. DoS attacks can prevent legitimate users from accessing services and cause downtime for organizations.

E

Encryption: Encryption is the process of encoding data so that only authorized parties can access it. It converts plaintext information into ciphertext using algorithms and keys. Encryption is essential for protecting sensitive data in transit and at rest.

Endpoint Security: Endpoint security focuses on securing individual devices such as computers, smartphones, and tablets. It includes measures like antivirus software, firewalls, and device encryption to protect against malware and unauthorized access.

Exploit: An exploit is a piece of software or code that takes advantage of a vulnerability in a system to carry out a cyber attack. Exploits can be used to gain unauthorized access, steal data, or cause system damage.

F

Firewall: A firewall is a network security device that monitors and controls incoming and outgoing traffic. It acts as a barrier between a trusted internal network and untrusted external networks, filtering traffic based on predefined rules to prevent unauthorized access.

H

Hacker: A hacker is an individual who uses technical skills to gain unauthorized access to computer systems or networks. Hackers can be motivated by financial gain, activism, or curiosity. Ethical hackers, also known as white hat hackers, use their skills for legitimate purposes like penetration testing.

I

Incident Response: Incident response is the process of responding to and managing a cybersecurity

incident. It involves detecting and analyzing threats, containing the incident, eradicating the threat, and recovering systems. Incident response plans are critical for minimizing the impact of cyber attacks.

Integrity: Integrity is the assurance that data has not been altered or tampered with in an unauthorized manner. Maintaining data integrity is essential for ensuring the accuracy and reliability of information. Integrity checks like hash functions and digital signatures can help detect data tampering.

IoT Security: IoT security focuses on securing the Internet of Things (IoT) devices connected to networks. These devices, such as smart thermostats and wearable fitness trackers, often lack built-in security features and can be vulnerable to cyber attacks. IoT security measures include device authentication, encryption, and regular updates.

IP Spoofing: IP spoofing is a technique used by attackers to disguise their identity by falsifying IP addresses in network packets. This can be used to launch denial-of-service attacks, bypass access controls, or carry out other malicious activities. Implementing measures like ingress filtering can help prevent IP spoofing.

L

Least Privilege: The principle of least privilege states that users should only be given the minimum level of access necessary to perform their job functions. Limiting user privileges reduces the risk of unauthorized access and helps prevent insider threats.

M

Malware: Malware is malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. Common types of malware include viruses, worms, Trojans, and ransomware. Protecting against malware requires antivirus programs, regular updates, and user education.

N

Network Security: Network security focuses on protecting the integrity, confidentiality, and availability of data transmitted over networks. It includes measures like firewalls, intrusion detection systems, and virtual private networks (VPNs) to secure network traffic and prevent unauthorized access.

P

Penetration Testing: Penetration testing, also known as pen testing, is a simulated cyber attack on a computer system or network to identify vulnerabilities. Pen testers use a variety of tools and techniques to exploit weaknesses and provide recommendations for improving security.

Phishing: Phishing is a social engineering technique used to trick individuals into revealing sensitive information such as passwords or financial data. Phishing attacks often involve fraudulent emails or websites that impersonate legitimate organizations. Training employees to recognize phishing attempts is essential for preventing data breaches.

R

Ransomware: Ransomware is a type of malware that encrypts a victim's files and demands a ransom for their release. Ransomware attacks can cause significant damage to organizations by disrupting operations and extorting money. Prevention measures include regular backups, security patches, and user awareness training.

Risk Management: Risk management in cybersecurity involves identifying, assessing, and mitigating risks to protect against cyber threats. It includes processes like risk assessment, vulnerability scanning, and incident response planning. Effective risk management strategies help organizations minimize the impact of security incidents.

S

Security Awareness Training: Security awareness training educates employees about cybersecurity best practices and helps them recognize and respond to threats. Training topics include password security, phishing awareness, and device security. Security awareness programs are essential for building a culture of security within organizations.

Social Engineering: Social engineering is a manipulation technique used by attackers to deceive individuals into revealing sensitive information or performing actions that compromise security. Common social engineering tactics include phishing, pretexting, and baiting. Educating users about social engineering risks is key to preventing successful attacks.

Spyware: Spyware is software that secretly collects information about a user's online activities without their knowledge or consent. Spyware can track browsing habits, capture keystrokes, and steal sensitive data. Anti-spyware programs help detect and remove spyware from infected systems.

Threat Intelligence: Threat intelligence is information about potential cyber threats that can help organizations identify and respond to security incidents. Threat intelligence sources include security vendors, government agencies, and open-source feeds. Using threat intelligence effectively can enhance threat detection and response capabilities.

V

Vulnerability: A vulnerability is a weakness in a system that can be exploited by attackers to compromise security. Vulnerabilities can exist in software, hardware, configurations, or user behavior. Regular vulnerability assessments and patch management are essential for addressing vulnerabilities and reducing the risk of exploitation.

W

Wireless Security: Wireless security focuses on securing wireless networks and devices from unauthorized access and attacks. Measures like encryption, strong passwords, and network segmentation help protect against eavesdropping, man-in-the-middle attacks, and unauthorized connections. Wireless security is essential for safeguarding sensitive data transmitted over Wi-Fi networks.