AP Cybersecurity

Key Definitions · 核心定义

Security answers are marked on precision: a threat is not a vulnerability, and a control is not a policy. Using the right word is usually the difference between a described answer and a scoring one. 安全类答题重在用词准确*:* 威胁、脆弱性与控制措施必须区分清楚。

Core principles

Confidentiality 保密性 — ensuring information is accessible only to those authorised to have it

Integrity 完整性 — ensuring information has not been altered, accidentally or maliciously, between creation and use

Availability 可用性 — ensuring authorised users can access information and services when they need them

Authentication 身份验证 — establishing that a user is who they claim to be

Authorisation 授权 — determining what an authenticated user is permitted to do

Non-repudiation 不可否认性 — assurance that a party cannot deny having sent a message or performed an action

Least privilege 最小权限原则 — granting each user or process only the access its task requires, and no more

Defence in depth 纵深防御 — layering independent controls so that the failure of one does not expose the system

Threats and vulnerabilities

Threat 威胁 — a potential cause of harm to a system – an actor, an event or a circumstance

Vulnerability 脆弱性 — a weakness in a system that a threat could exploit; a vulnerability with no threat is not yet a risk

Risk 风险 — the combination of the likelihood a threat exploits a vulnerability and the impact if it does

Attack surface 攻击面 — the sum of the points at which an unauthorised user could try to enter or extract data

Malware 恶意软件 — software written to damage a system, steal data or gain unauthorised access

Ransomware 勒索软件 — malware that encrypts a victim's data and demands payment for the key

Social engineering 社会工程学 — manipulating people into revealing information or taking actions that compromise security, bypassing technical controls entirely

Phishing 网络钓鱼 — a message impersonating a trusted sender, designed to obtain credentials or deliver malware

SQL injection SQL 注入 — supplying input that a program inserts into a database query unchecked, so the input is executed as code

Zero-day vulnerability 零日漏洞 — a vulnerability unknown to the vendor, for which no patch yet exists

Controls

Firewall 防火墙 — a control that inspects traffic crossing a network boundary and permits or blocks it against a rule set

Encryption 加密 — transforming data with a key so that it is unreadable without the corresponding key

Hashing 哈希 — producing a fixed-length digest from data by a one-way function; unlike encryption it cannot be reversed, which is why it suits password storage

Digital signature 数字签名 — a hash of a message encrypted with the sender's private key, which proves origin and integrity

Multifactor authentication 多因素认证 — requiring two or more independent kinds of evidence: something you know, something you have, something you are

Patch management 补丁管理 — the process of tracking, testing and applying vendor fixes so known vulnerabilities are closed

Intrusion detection system 入侵检测系统 — a system that monitors traffic or hosts for signs of an attack and raises an alert; it detects rather than blocks

Air gap 物理隔离 — physically isolating a system from unsecured networks so no network path exists to it

Operations and response

Incident response 事件响应 — the planned process of preparation, identification, containment, eradication, recovery and lessons learned

Penetration testing 渗透测试 — authorised simulated attack to find exploitable weaknesses before an attacker does

Backup (3-2-1 rule) 备份 — three copies of data on two kinds of media with one held off-site – the control that makes ransomware survivable

Security policy 安全策略 — a documented statement of what an organisation requires; a control is the mechanism that enforces it