12. Bezpečnost přenosu a zpracování dat

Bezpečnost(útoky, hrozba, riziko, aktiva, zranitelná místa, bezpečnostní funkce, bezp. mechanismy)

Bezpečnost v IT znamená chránit systémy a data před neoprávněným přístupem, zneužitím, přerušením provozu, pozměněním nebo zničením.

Základními pojmy jsou:

- **Útoky** jsou cílené akce, které mají narušit bezpečnost systému – například hackerské útoky, malware nebo DoS/DDoS útoky.
- **Hrozba** představuje potenciální příčinu incidentu, která může ohrozit systém (například zranitelnost v aplikaci, phishingová kampaň, fyzický útok).
- **Riziko** je pravděpodobnost, že hrozba využije zranitelnost a způsobí škodu. Správa rizik znamená tato rizika identifikovat, hodnotit a snižovat.
- **Aktiva** jsou všechny hodnotné prvky – data, software, hardware, sítě, know-how.
- **Zranitelnost** je slabé místo systému, které může být zneužito (například nezáplatovaný systém, slabá hesla, otevřené porty).
- **Bezpečnostní funkce** jsou obecné principy ochrany (šifrování, autentizace, kontrola přístupu).
- **Bezpečnostní mechanismy** jsou konkrétní technická a procesní opatření, např. firewall, IDS/IPS, antivirové programy.

Základní požadavky na bezpečnost

Aby byl systém skutečně bezpečný, musí být zajištěny tyto hlavní principy:

- **Důvěrnost (confidentiality)**: Data musí být dostupná pouze těm, kdo mají oprávnění (ochrana před únikem informací).
- **Integrita (integrity)**: Zajištění, že data nejsou neautorizovaně změněna (ochrana před modifikací).
- **Dostupnost (availability)**: Systémy i data musí být k dispozici v případě potřeby (ochrana před výpadkem služeb).
- **Autentičnost (authenticity)**: Ověření identity uživatele nebo systému, tedy zajištění, že komunikace či data pocházejí skutečně od deklarovaného zdroje.
- **Neodmítnutelnost (non-repudiation)**: Zajištění, že autor nemůže popřít, že vykonal určitou akci (např. podepsal dokument).

Nejčastější chyby a problémy, typy útoků

Typické chyby, které ohrožují bezpečnost, zahrnují používání slabých hesel, chybějící aktualizace, špatnou konfiguraci bezpečnosti a nedostatečné vzdělávání zaměstnanců.

Mezi nejčastější typy útoků patří:

- **Phishing** – podvodné získávání citlivých údajů (např. přes e-mail nebo falešné weby).
- **Malware** – škodlivý software, který narušuje nebo poškozuje systémy (viry, trojské koně, ransomware, spyware).
- **DoS/DDoS** – útoky na dostupnost, cílem je zahltit systém a vyřadit službu z provozu.
- **SQL Injection** – zneužití špatně ošetřených databázových dotazů k provedení škodlivých příkazů.
- **XSS (Cross-Site Scripting)** – vkládání škodlivých skriptů do webových stránek.

Současná největší rizika

V současnosti mezi hlavní hrozby patří:

- **Ransomware** – šifrování dat a požadování výkupného.
- **Phishing** – cílené podvody zaměřené na zcizení údajů.
- **Vnitřní hrozby** – útoky nebo chyby zaměstnanců s přístupem do systému.
- **Problémy s bezpečností cloudu** – například špatně zabezpečené úložiště nebo nedostatečné rozdělení odpovědnosti mezi poskytovatelem a uživatelem.

Řízení přístupu (identifikace, autentizace)

Správné řízení přístupu je klíčové pro omezení rizika zneužití systému.

- **Identifikace**: Určení identity uživatele (např. zadáním uživatelského jména).
- **Autentizace**: Ověření, že uživatel je skutečně tím, za koho se vydává (např. heslo, biometrika).

Hlavní možnosti autentizace

- **Hesla** – běžná, ale zranitelná metoda, proto doporučena vícefaktorová autentizace.
- **Biometrické údaje** – otisk prstu, rozpoznání obličeje nebo hlasu.
- **Čipové karty** – fyzický nosič s uloženými autentizačními údaji.
- **Digitální certifikáty** – kryptografické ověření identity.

Škodlivý software (malware) a ochrana

Malware je zastřešující pojem pro škodlivé programy, které mohou systém poškodit, špehovat nebo šifrovat data. Typy malwaru:

- **Viry** – šíří se vkládáním do souborů.
- **Trojské koně** – tváří se jako legitimní program, ale obsahují škodlivý kód.
- **Spyware** – sleduje aktivitu uživatele.
- **Ransomware** – zašifruje data a požaduje výkupné.

Ochrana spočívá v použití antivirů, pravidelných aktualizacích systémů, správné konfiguraci a průběžném vzdělávání uživatelů.

Základy použití kryptografie: šifrování, digitální podpis

- **Šifrování** – převod čitelných dat na nečitelný formát, k přečtení je potřeba klíč.
- **Digitální podpis** – ověřuje původ dat a jejich integritu; typicky používá asymetrickou kryptografii, kde soukromý klíč slouží k vytvoření podpisu a veřejný klíč k ověření.

RSA

- Asymetrický šifrovací algoritmus, který na šifrování a dešifrování používá dvojici klíčů.

Certifikáty, certifikační autority, CRL, PKI

- **Certifikát** – elektronický dokument ověřující totožnost uživatele či serveru.
- **Certifikační autorita (CA)** – důvěryhodná organizace, která certifikáty vydává.
- **CRL (Certificate Revocation List)** – seznam neplatných/zneplatněných certifikátů.
- **PKI (Public Key Infrastructure)** – infrastruktura pro správu, vydávání a ověřování certifikátů a veřejných klíčů.

Časové razítko a elektronická značka

- **Časové razítko** je elektronický údaj, který dokládá přesný čas vytvoření nebo změny elektronického dokumentu.
- **Elektronická značka** potvrzuje původ a pravost elektronického dokumentu, často používaná při automatizovaném podepisování organizací.

Nebezpečí síťového připojení a možnosti ochrany

Připojení k síti přináší riziko **odposlechu komunikace, neoprávněného přístupu** a **šíření malwaru**.

Možnosti ochrany zahrnují:

- Používání šifrované komunikace (např. VPN, SSL/TLS)
- Firewally a IDS/IPS pro kontrolu síťového provozu
- Pravidelná aktualizace a bezpečné konfigurace systémů

Bezpečnost webových stránek a bezpečné protokoly

Webové aplikace jsou často terčem útoků – **phishing**, **XSS**, **malware**.

K ochraně se používají bezpečné protokoly, jako je **HTTPS** (přenos dat šifrovaný pomocí **SSL/TLS**). Základem je správná konfigurace webových serverů, pravidelná kontrola zranitelností a školení uživatelů.

Ochrana, mazání, ukládání a zálohování dat

Ochrana dat zahrnuje šifrování, kontrolu přístupu a zálohování.

Mazání dat se provádí:

- Jednoduchým odstraněním (lze obnovit)
- Bezpečným přepisem (trvale odstraněno)
- Skartací (fyzické zničení média)

Zálohování může být:

- Úplné – kompletní kopie dat
- Diferenciální – kopie změněných dat od poslední úplné zálohy
- Přírůstkové – kopie změn od poslední zálohy jakéhokoliv typu

Vhodná média: externí disky, NAS, cloud;

Nevhodná média: diskety, CD/DVD (nízká kapacita a životnost).

Archivování a řízené zničení médií

Archivace znamená dlouhodobé uchování dat, která se již aktivně nepoužívají, ale mohou být v budoucnu potřeba.

Řízené zničení médií zajišťuje trvalé a nezvratné odstranění citlivých dat – např. demagnetizace, skartace nebo spalování nosičů.

Budování bezpečnosti v organizaci: ochrana IS, etapy a normy

Bezpečnostní strategie organizace zahrnuje kombinaci technických opatření (firewall, IDS/IPS, antivir), školení, bezpečnostních zásad a pravidelných auditů.

Hlavní etapy budování bezpečnosti:

1. **Analýza rizik** – identifikace a vyhodnocení rizik
2. **Návrh bezpečnostní politiky** – tvorba pravidel a odpovědností
3. **Implementace** – zavedení technických a organizačních opatření
4. **Testování** – ověření účinnosti opatření
5. **Monitorování a audit** – průběžné sledování a pravidelné kontroly

Analýza rizik

Analýza rizik je proces, který zahrnuje identifikaci hrozeb, zranitelností a stanovení pravděpodobnosti a dopadu. Následně se navrhují opatření ke snížení rizik na přijatelnou úroveň.

Bezpečnostní politika

Bezpečnostní politika je klíčový dokument organizace, který definuje pravidla, odpovědnosti, procesy a postupy pro zajištění ochrany informací. Stanovuje například práva přístupu, pravidla pro šifrování a postupy při incidentu.

Havarijní plán a základní postup

Havarijní plán obsahuje opatření a scénáře pro obnovení provozu po havárii nebo incidentu. Zahrnuje identifikaci kritických aktiv, kontaktní informace, postupy obnovy, ochranu před ztrátou dat a pravidelné testování plánů.

Systém řízení bezpečnosti informací (ISMS), normy a ISO

ISMS (Information Security Management System) je systém řízení informační bezpečnosti podle standardů ISO (například ISO/IEC 27001).

Normy **ISO** stanovují požadavky a doporučené postupy pro zavádění, provoz, monitorování a zlepšování bezpečnosti informací v organizacích.