**Bezpečnosť**: Bezpečnosť je proces zabezpečujúci ochranu systémov a údajov pred neoprávneným prístupom, používaním, zverejnením, prerušením, zmenou alebo zničením. Kľúčové prvky zahŕňajú:

* Útoky: akcie zamerané na narušenie bezpečnosti systému, napr. hackerské útoky, malvér, útoky DoS.
* Hrozba: potenciálna príčina neúmyselného incidentu, ktorý môže spôsobiť poškodenie systému.
* Riziko: Pravdepodobnosť, že hrozba zneužije zraniteľnosť a spôsobí škodu.
* Aktíva: Hodnotné prvky organizácie, ako sú údaje, hardvér, softvér, infraštruktúra.
* Zraniteľné miesta: Slabé miesta v systéme, ktoré môžu byť zneužité hrozbami.
* Bezpečnostné prvky: Ochranné prvky, napríklad šifrovanie, autentifikácia, kontrola prístupu.
* Bezpečnostné mechanizmy: Špecifické metódy implementácie bezpečnostných prvkov, ako sú firewall, antivírus, IDS/IPS.

**Základné požiadavky na bezpečnosť**: Medzi základné požiadavky patrí:

* Dôvernosť: zabezpečenie toho, aby informácie boli dostupné len oprávneným osobám.
* Integrita: ochrana pred neoprávnenou modifikáciou údajov.
* Dostupnosť: Zabezpečenie toho, aby boli systémy a údaje v prípade potreby dostupné.
* Autentickosť: Overenie identity používateľov a zdrojov.
* Neodmietnutie: Zabezpečenie toho, že činnosti alebo transakcie nemôžu byť neskôr popreté.

**Najčastejšie chyby a problémy**:

* Slabé heslá
* Nedostatočné aktualizácie a záplaty
* Nedostatočná konfigurácia zabezpečenia
* Nedostatočné školenie zamestnancov

**Typy útoku**:

* Phishing: podvodné získanie citlivých informácií.
* Malvér: škodlivý softvér, ktorý poškodzuje alebo narúša systémy.
* Útoky DoS a DDoS: Preťaženie systému a narušenie jeho dostupnosti.
* SQL Injection: Vloženie škodlivého kódu do databázových dotazov.
* XSS (Cross-Site Scripting): Vkladanie škodlivých skriptov do webových stránok.

**Aktuálne najväčšie riziká**:

* Ransomvér: škodlivý softvér, ktorý zašifruje údaje a za ich odomknutie požaduje výkupné.
* Phishing: Cielené podvodné e-maily a webové stránky.
* Vnútorné hrozby: Hrozby od zamestnancov alebo iných interných aktérov.
* Problémy s bezpečnosťou cloudu: Riziká spojené s ukladaním a spracovaním údajov v cloude.

**Riadenie prístupu – identifikácia, autentifikácia**: Kontrola prístupu zahŕňa procesy overovania identity používateľa a jeho oprávnení:

* Identifikácia: proces určenia identity používateľa (napr. pomocou používateľského mena).
* Autentifikácia: proces overovania, či je používateľ tým, za koho sa vydáva (napr. pomocou hesla).

**Možnosti autentifikácie**:

* Heslá: Najbežnejšia metóda, ktorá je však často náchylná na útoky.
* Biometria: overovanie odtlačkov prstov, rozpoznávanie tváre, rozpoznávanie hlasu.
* Čipové karty: používanie fyzických kariet, na ktorých sú uložené prístupové informácie.
* Certifikáty: Digitálne certifikáty na overenie identity pomocou kryptografie.

**Škodlivý softvér**: Malvér je škodlivý softvér, ktorý zahŕňa:

* Vírusy: programy, ktoré sa šíria vkladaním do iných programov.
* Trojské kone: škodlivé programy, ktoré predstierajú, že sú legitímne.
* Spyware: softvér, ktorý monitoruje aktivity používateľa.
* Ransomvér: Softvér, ktorý šifruje údaje a požaduje výkupné.

Ochrana zahŕňa:

* Používanie antivírusových programov.
* Pravidelné aktualizácie systémov a aplikácií.
* Vzdelávanie používateľov o bezpečnostných hrozbách.

**Základy kryptografie**:

Symetrické šifrovanie používa na šifrovanie a dešifrovanie rovnaký kľúč. Príkladmi sú AES a DES.

Asymetrické šifrovanie používa dvojicu kľúčov - verejný kľúč na šifrovanie a súkromný kľúč na dešifrovanie. Príkladom je RSA.

**Základy používania**:

* Šifrovanie: proces prevodu čitateľného textu do nečitateľného formátu.
* Digitálny podpis: používa asymetrickú kryptografiu na overenie integrity a pravosti správy.

**Digitálny podpis**: je elektronický podpis, ktorý využíva kryptografiu na overenie identity a integrity správy.

**RSA**: je asymetrický šifrovací algoritmus, ktorý na šifrovanie a dešifrovanie používa dvojice kľúčov.

**Certifikáty,** **certifikačné autority, CRL, PKI**:

* Certifikáty: digitálne dokumenty overujúce totožnosť držiteľa.
* Certifikačné autority (CA): organizácie, ktoré vydávajú certifikáty.
* Zoznam zrušených certifikátov (CRL): zoznam neplatných certifikátov.
* PKI (Public Key Infrastructure): infraštruktúra na správu verejných kľúčov a certifikátov.

**Časové razítko**: je elektronická značka potvrdzujúca čas vytvorenia alebo úpravy dokumentu.

**Elektronická značka**: potvrdzuje pôvod a pravosť elektronického dokumentu.

**Nebezpečenstvá sieťového pripojenia - riziká sieťového pripojenia**: Medzi riziká sieťového pripojenia patria:

* Odpočúvanie komunikácie
* Neoprávnený prístup
* Malvér

**Možnosti ochrany**:

* Používanie šifrovania (napr. VPN)
* Firewall
* IDS/IPS

**Nie/bezpečnosť webových stránok**: Medzi riziká webovej lokality patria:

* Phishing
* XSS
* Malvér

**Bezpečnostné protokoly**:

* HTTPS
* SSL/TLS

**Ochrana dát**: Ochrana údajov zahŕňa rôzne metódy a technológie na zabezpečenie dôvernosti, integrity a dostupnosti údajov. Medzi kľúčové techniky patria:

* Šifrovanie: prevod údajov do zašifrovaného formátu, ktorý môže čítať len oprávnená osoba s dešifrovacím kľúčom.
* Kontrola prístupu: Zabezpečenie toho, aby k citlivým údajom mali prístup len oprávnené osoby.
* Zálohovanie: pravidelné kopírovanie údajov do zabezpečeného úložiska na obnovu v prípade straty údajov.

**Mazanie dát**: Vymazávanie údajov zahŕňa techniky na trvalé odstránenie údajov z úložiska:

* Jednoduché vymazanie: vymazanie z indexu, ale údaje možno obnoviť.
* Bezpečné vymazanie: prepísanie údajov náhodnými znakmi tak, aby sa nedali obnoviť.
* Skartácia: fyzické zničenie média obsahujúceho údaje.

**Zálohovanie**: Zálohovanie je proces vytvárania kópií údajov na ich ochranu v prípade straty alebo poškodenia. Zahŕňa:

* Úplné zálohovanie: kopírovanie všetkých údajov.
* Diferenciálne zálohovanie: Kopírovanie zmenených údajov od posledného úplného zálohovania.
* Prírastkové zálohovanie: Kopírovanie zmenených údajov od poslednej zálohy (úplnej alebo prírastkovej).

**Médiá na zálohovanie**: Záložné médiá sú zariadenia alebo systémy používané na ukladanie záloh:

* Vhodné médiá: Externé pevné disky, NAS (Network Attached Storage), cloudové úložisko.
* Nevhodné médiá: Diskety, CD/DVD (kvôli nízkej kapacite a trvanlivosti).

**Archivovanie**: Archivácia údajov je proces dlhodobého uchovávania údajov, ktoré sa už často nepoužívajú, ale môžu byť potrebné v budúcnosti. Zahŕňa:

* Digitálnu archiváciu: ukladanie údajov v digitálnej forme na serveroch alebo v cloude.
* Fyzická archivácia: ukladanie tlačených dokumentov do archívnych skladov.

**Kontrolované ničenie médií**: Kontrolované ničenie médií zahŕňa postupy na bezpečné a nezvratné odstránenie údajov z médií:

* Odstraňovanie údajov: odstraňovanie údajov z magnetických médií.
* Skartovačky a skartovacie stroje: Fyzické ničenie médií (diskov, pások) na malé kúsky.
* Spaľovanie: zničenie médií spálením.

**Budovanie bezpečnosti v organizácii**: Možnosti ochrany informačných systémov zahŕňajú implementáciu rôznych technológií a postupov:

* Firewall: Ochrana siete pred neoprávneným prístupom.
* Antivírusový softvér: Detekcia a odstránenie škodlivého softvéru.
* IDS/IPS (Intrusion Detection/Prevention Systems): Monitorovanie a blokovanie podozrivých aktivít v sieti.

**Budovanie bezpečnosti**: Budovanie bezpečnosti v organizácii zahŕňa niekoľko etáp:

* Plánovanie: stanovenie bezpečnostných cieľov a požiadaviek.
* Implementácia: Zavedenie bezpečnostných opatrení a technológií.
* Monitorovanie: Priebežné monitorovanie a hodnotenie bezpečnostných opatrení.
* Údržba: pravidelné aktualizácie a úpravy bezpečnostných opatrení.

**Etapy**: Fázy zabezpečenia budovy zahŕňajú:

1. Analýza rizík: identifikácia a hodnotenie rizík spojených s informačnými systémami.
2. Návrh bezpečnostnej politiky: Vytvorenie dokumentu definujúceho pravidlá a postupy na zaistenie bezpečnosti.
3. Implementácia: Zavedenie bezpečnostných opatrení a technológií.
4. Testovanie: Overenie účinnosti implementovaných opatrení.
5. Monitorovanie a audit: Priebežné monitorovanie a pravidelné kontroly.

**Analýza rizík**: Analýza rizík je proces identifikácie, hodnotenia a riadenia rizík. Zahŕňa:

* Identifikáciu rizík: Určenie potenciálnych hrozieb a zraniteľností.
* Hodnotenie rizík: Určenie pravdepodobnosti a vplyvu rizík.
* Riadenie rizík: Implementácia opatrení na zníženie alebo odstránenie rizík.

**Bezpečnostná politika**: Bezpečnostná politika je dokument, ktorý definuje pravidlá, postupy a zodpovednosti na zaistenie bezpečnosti informácií v organizácii. Zahŕňa:

* pravidlá prístupu k údajom
* postupy na zabezpečenie údajov
* zodpovednosti zamestnancov

**Havarijný plán**: Havarijný plán je dokument, ktorý obsahuje postupy na obnovenie prevádzky po nehode alebo poruche. Obsahuje:

* identifikáciu kritických aktív
* postupy na obnovu systémov a údajov
* kontaktné informácie a zodpovednosti

**Základný postup**: Základný postup pre havarijný plán zahŕňa:

* Príprava: identifikácia kritických systémov a údajov.
* Ochrana: Implementácia opatrení na minimalizáciu dopadu havárie.
* Zisťovanie: včasné rozpoznanie havárie.
* Reakcia: Okamžité opatrenia na zmiernenie dopadu.
* Obnova: Postupy na obnovenie normálnej prevádzky.
* Hodnotenie: Analýza a poučenie z nehody s cieľom zlepšiť budúce plány.

**Normy - Systém riadenia informačnej bezpečnosti**: Systém riadenia bezpečnosti informácií (ISMS). ISMS je systém na riadenie a zlepšovanie bezpečnosti informácií v organizácii. Zahŕňa:

* Politiky a postupy: definovanie pravidiel a postupov na zaistenie bezpečnosti informácií.
* Riadenie rizík: identifikácia, hodnotenie a riadenie rizík.
* Neustále zlepšovanie: Neustále hodnotenie a zlepšovanie bezpečnostných opatrení.

**Normy a bezpečnosť IT**: Normy bezpečnosti IT poskytujú rámec a odporúčania na implementáciu a riadenie bezpečnostných opatrení. Zahŕňajú:

* ISO/IEC 27001: Medzinárodná norma pre riadenie informačnej bezpečnosti.
* ISO/IEC 27002: Katalóg odporúčaní pre riadenie informačnej bezpečnosti.
* ITIL Security Management: Najlepšie postupy pre riadenie služieb IT a bezpečnosti.

**ISO**: ISO (Medzinárodná organizácia pre normalizáciu) je medzinárodná normalizačná organizácia, ktorá vyvíja a publikuje medzinárodné normy v rôznych oblastiach vrátane informačnej bezpečnosti. Normy ISO pomáhajú organizáciám zavádzať účinné postupy a zabezpečovať kvalitu.