### Překlad dokumentu: Bezpečnost přenosu a zpracování dat

**Bezpečnost**: Bezpečnost je proces zajišťující ochranu systémů a údajů před neoprávněným přístupem, zveřejněním, přerušením, změnou nebo zničením. Klíčové prvky zahrnují:

* **Útoky**: akce zaměřené na narušení bezpečnosti systému, např. hackerské útoky, malware, útoky DoS.
* **Hrozba**: potenciální příčina neúmyslného incidentu, který může způsobit poškození systému.
* **Riziko**: pravděpodobnost, že hrozba zneužije zranitelnost a způsobí škodu.
* **Aktiva**: hodnotné prvky organizace jako jsou údaje, hardware, software, infrastruktura.
* **Zranitelná místa**: slabá místa v systému, která mohou být zneužita hrozbami.
* **Bezpečnostní prvky**: ochranné prvky jako šifrování, autentizace, kontrola přístupu.
* **Bezpečnostní mechanismy**: specifické metody implementace bezpečnostních prvků, jako jsou firewall, antivirus, IDS/IPS.

**Základní požadavky na bezpečnost**:

* **Důvěrnost**: zabezpečení, aby informace byly dostupné jen oprávněným osobám.
* **Integrita**: ochrana před neoprávněnou modifikací údajů.
* **Dostupnost**: zajištění, aby systémy a údaje byly dostupné v případě potřeby.
* **Autentičnost**: ověření identity uživatelů a zdrojů.
* **Neodmítnutí**: zajištění, že činnosti nebo transakce nemohou být později popřeny.

**Nejčastější chyby a problémy**:

* Slabá hesla
* Nedostatečné aktualizace a záplaty
* Nedostatečná konfigurace zabezpečení
* Nedostatečné školení zaměstnanců

**Typy útoků**:

* **Phishing**: podvodné získání citlivých informací.
* **Malware**: škodlivý software, který poškozuje nebo narušuje systémy.
* **DoS a DDoS útoky**: přetížení systému a narušení jeho dostupnosti.
* **SQL Injection**: vložení škodlivého kódu do databázových dotazů.
* **XSS (Cross-Site Scripting)**: vkládání škodlivých skriptů do webových stránek.

**Aktuální největší rizika**:

* **Ransomware**: škodlivý software, který zašifruje údaje a za jejich odemknutí požaduje výkupné.
* **Phishing**: cílené podvodné e-maily a webové stránky.
* **Vnitřní hrozby**: hrozby od zaměstnanců nebo jiných interních aktérů.
* **Problémy s bezpečností cloudu**: rizika spojená s ukládáním a zpracováním údajů v cloudu.

**Řízení přístupu – identifikace, autentifikace**: Kontrola přístupu zahrnuje procesy ověřování identity uživatele a jeho oprávnění:

* **Identifikace**: proces určení identity uživatele (např. pomocí uživatelského jména).
* **Autentizace**: proces ověřování, zda je uživatel tím, za koho se vydává (např. pomocí hesla).

**Možnosti autentifikace**:

* Hesla: nejběžnější metoda, která je však často náchylná na útoky.
* Biometrie: ověřování otisků prstů, rozpoznávání tváře, rozpoznávání hlasu.
* Čipové karty: používání fyzických karet, na kterých jsou uloženy přístupové informace.
* Certifikáty: digitální certifikáty na ověření identity pomocí kryptografie.

**Škodlivý software**: Malware je škodlivý software, který zahrnuje:

* **Viry**: programy, které se šíří vkládáním do jiných programů.
* **Trojské koně**: škodlivé programy, které předstírají, že jsou legitimní.
* **Spyware**: software, který monitoruje aktivity uživatele.
* **Ransomware**: software, který šifruje údaje a požaduje výkupné.

**Ochrana zahrnuje**:

* Používání antivirových programů.
* Pravidelné aktualizace systémů a aplikací.
* Vzdělávání uživatelů o bezpečnostních hrozbách.

**Základy kryptografie**:

* **Symetrické šifrování** používá na šifrování a dešifrování stejný klíč. Příklady jsou AES a DES.
* **Asymetrické šifrování** používá dvojici klíčů – veřejný klíč na šifrování a soukromý klíč na dešifrování. Příkladem je RSA.

**Základy používání**:

* **Šifrování**: proces převodu čitelného textu do nečitelného formátu.
* **Digitální podpis**: používá asymetrickou kryptografii na ověření integrity a pravosti zprávy.

**Digitální podpis**: je elektronický podpis, který využívá kryptografii na ověření identity a integrity zprávy.

**RSA**: je asymetrický šifrovací algoritmus, který na šifrování a dešifrování používá dvojice klíčů.

**Certifikáty, certifikační autority, CRL, PKI**:

* **Certifikáty**: digitální dokumenty ověřující totožnost držitele.
* **Certifikační autority (CA)**: organizace, které vydávají certifikáty.
* **Zoznam zrušených certifikátů (CRL)**: seznam neplatných certifikátů.
* **PKI (Public Key Infrastructure)**: infrastruktura na správu veřejných klíčů a certifikátů.

**Časové razítko**: je elektronická značka potvrzující čas vytvoření nebo úpravy dokumentu. **Elektronická značka**: potvrzuje původ a pravost elektronického dokumentu.

**Nebezpečí síťového připojení – rizika síťového připojení**: Mezi rizika síťového připojení patří:

* Odposlech komunikace
* Neoprávněný přístup
* Malware

**Možnosti ochrany**:

- Používání šifrování (např. VPN)

- Firewall - IDS/IPS

**Bezpečnost webových stránek**: Mezi rizika webové lokality patří:

* Phishing
* XSS
* Malware

**Bezpečnostní protokoly**:

* HTTPS
* SSL/TLS

**Ochrana dat**: Ochrana údajů zahrnuje různé metody a technologie na zajištění důvěrnosti, integrity a dostupnosti údajů. Mezi klíčové techniky patří:

* **Šifrování**: převod údajů do zašifrovaného formátu, který může číst jen oprávněná osoba s dešifrovacím klíčem.
* **Kontrola přístupu**: zajištění, aby k citlivým údajům měli přístup jen oprávněné osoby.
* **Zálohování**: pravidelné kopírování údajů do zabezpečeného úložiště na obnovu v případě ztráty údajů.

**Mazání dat**: Vymazávání údajů zahrnuje techniky na trvalé odstranění údajů z úložiště:

* **Jednoduché vymazání**: vymazání z indexu, ale údaje lze obnovit.
* **Bezpečné vymazání**: přepsání údajů náhodnými znaky, aby se nedaly obnovit.
* **Skartace**: fyzické zničení média obsahujícího údaje.

**Zálohování**: Zálohování je proces vytváření kopií údajů na jejich ochranu v případě ztráty nebo poškození. Zahrnuje:

* **Úplné zálohování**: kopírování všech údajů.
* **Diferenciální zálohování**: kopírování změněných údajů od posledního úplného zálohování.
* **Přírůstkové zálohování**: kopírování změněných údajů od poslední zálohy (úplné nebo přírůstkové).

Média na zálohování

Záložní média jsou zařízení nebo systémy používané na ukládání záloh:

* **Vhodná média**: externí pevné disky, NAS (Network Attached Storage), cloudové úložiště.
* **Nevhodná média**: diskety, CD/DVD (kvůli nízké kapacitě a trvanlivosti).

**Archivování**: Archivace údajů je proces dlouhodobého uchovávání údajů, které se už často nepoužívají, ale mohou být potřebné v budoucnosti. Zahrnuje:

* **Digitální archivaci**: ukládání údajů v digitální formě na serverech nebo v cloudu.
* **Fyzická archivace**: ukládání tištěných dokumentů do archivních skladů.

**Kontrolované ničení médií**: Kontrolované ničení médií zahrnuje postupy na bezpečné a nezvratné odstranění údajů z médií:

* **Odstraňování údajů**: odstraňování údajů z magnetických médií.
* **Skartovačky a skartovací stroje**: fyzické ničení médií (disků, pásek) na malé kousky.
* **Spalování**: zničení médií spálením.

**Budování bezpečnosti v organizaci**: Možnosti ochrany informačních systémů zahrnují implementaci různých technologií a postupů:

* **Firewall**: ochrana sítě před neoprávněným přístupem.
* **Antivirový software**: detekce a odstranění škodlivého softwaru.
* **IDS/IPS (Intrusion Detection/Prevention Systems)**: monitorování a blokování podezřelých aktivit v síti.

**Budování bezpečnosti**: Budování bezpečnosti v organizaci zahrnuje několik etap:

* **Plánování**: stanovení bezpečnostních cílů a požadavků.
* **Implementace**: zavedení bezpečnostních opatření a technologií.
* **Monitorování**: průběžné monitorování a hodnocení bezpečnostních opatření. - **Údržba**: pravidelné aktualizace a úpravy bezpečnostních opatření.

**Etapy**: Fáze zabezpečení budovy zahrnují:

* **Analýza rizik**: identifikace a hodnocení rizik spojených s informačními systémy.
* **Návrh bezpečnostní politiky**: vytvoření dokumentu definujícího pravidla a postupy na zajištění bezpečnosti.
* **Implementace**: zavedení bezpečnostních opatření a technologií.
* **Testování**: ověření účinnosti implementovaných opatření.
* **Monitorování a audit**: průběžné monitorování a pravidelné kontroly.

**Analýza rizik**: Analýza rizik je proces identifikace, hodnocení a řízení rizik. Zahrnuje:

* **Identifikaci rizik**: určení potenciálních hrozeb a zranitelností.
* **Hodnocení rizik**: určení pravděpodobnosti a dopadu rizik.
* **Řízení rizik**: implementace opatření na snížení nebo odstranění rizik.

**Bezpečnostní politika**: Bezpečnostní politika je dokument, který definuje pravidla, postupy a odpovědnosti na zajištění bezpečnosti informací v organizaci. Zahrnuje:

* Pravidla přístupu k údajům
* Postupy na zabezpečení údajů
* Odpovědnosti zaměstnanců

**Havarijní plán**: Havarijní plán je dokument, který obsahuje postupy na obnovení provozu po nehodě nebo poruše. Obsahuje:

* Identifikaci kritických aktiv
* Postupy na obnovu systémů a údajů
* Kontaktní informace a odpovědnosti

**Základní postup**: Základní postup pro havarijní plán zahrnuje:

* **Příprava**: identifikace kritických systémů a údajů.
* **Ochrana**: implementace opatření na minimalizaci dopadu havárie.
* **Zjišťování**: včasné rozpoznání havárie.
* **Reakce**: okamžité opatření na zmírnění dopadu.
* **Obnova**: postupy na obnovení normálního provozu.
* **Hodnocení**: analýza a poučení z nehody s cílem zlepšit budoucí plány.

**ISO**: ISO (Mezinárodní organizace pro normalizaci) je mezinárodní normalizační organizace, která vyvíjí a publikuje mezinárodní normy v různých oblastech, včetně informační bezpečnosti. Normy ISO pomáhají organizacím zavádět účinné postupy a zajišťovat kvalitu.