

INFORMAČNÍ SYSTÉMY VE VEŘEJNÉ SPRÁVĚ

10. Bezpečnost



**SLEZSKÁ
UNIVERZITA**
OBCHODNĚ PODNIKATELSKÁ
FAKULTA V KARVINĚ

Ing. Radim Dolák, Ph.D.

Cíle přednášky

- ✓ Definovat pojmy bezpečnost, hrozba, identifikace, autentizace, autorizace a kryptografie
- ✓ Pochopit základní principy zajištění bezpečnosti
- ✓ Znat problematiku identifikačních dokladů a jejich zabezpečení





- ❑ **Problematika bezpečnosti je oblastí, která je hodně diskutovaná a zdůrazňovaná. Přesto je to mnohdy podceňována a zanedbávaná oblast provozu IS.**
 - ❑ **Je třeba chránit informace, jejichž ztráta, zneužití nebo neoprávněná modifikace mohou způsobit škodu:**
 - **před lidmi vně organizace;**
 - **před neoprávněnými osobami uvnitř organizace.**
-

Bezpečnost



**SLEZSKÁ
UNIVERZITA**
OBCHODNĚ PODNIKATELSKÁ
FAKULTA V KARVINĚ

- ❑ **Informace s nezanedbatelnou hodnotou musí být chráněny, aby:**
 - **k nim měly přístup pouze oprávněné osoby;**
 - **se zpracovávaly nefalšované informace;**
 - **se dalo zjistit, kdo je vytvořil, změnil nebo odstranil;**
 - **nebyly nekontrolovaným způsobem vyzrazeny;**
 - **byly dostupné tehdy, když jsou potřebné.**
-

Bezpečnost - definice

- **Bezpečnost je schopnost informačního systému chránit data a informace tak, aby neautorizované osoby neměly možnost je číst nebo je modifikovat a zároveň aby autorizovaným subjektům nebyla zamítnuta možnost přístupu k datům na stanovené úrovni.**



Hrozba



- ❑ Hrozba je možnost využít zranitelné místo IS k útoku na něj ke způsobení škody na aktivech.
 - ❑ Je to potenciální příčina incidentu, která může mít za následek poškození organizace.
 - ❑ Je to potenciální příčina nežádoucího incidentu, který může mít za následek poškození systému nebo organizace.
 - ❑ Hrozby lze rozdělit na objektivní (přírodní, fyzické, fyzikální, technické nebo logické) a subjektivní, hrozby plynoucí z lidského faktoru (neúmyslné nebo úmyslné).
-

Zranitelné místo



- ❑ Zranitelné místo je slabina IS využitelná ke způsobení škod nebo ztrát útokem na IS.
 - ❑ Jde o důsledek chyb, selhání v analýze, v návrhu nebo v implementaci IS.
 - ❑ Příčina může být rovněž ve vysoké hustotě uložených informací, ve složitosti softwaru, v existenci skrytých kanálů pro přenos informace jinou než zamýšlenou cestou apod.
 - ❑ Zranitelná místa jsou vlastnosti (součásti) IS, jejichž existence způsobuje, že některé vlivy prostředí, ve kterém se IS provozuje, představují pro něj nebezpečí.
-

- Existence hrozby představuje riziko.
 - Riziko je pravděpodobnost zužitkování zranitelného místa IS (hrozba se uplatní s takovou a takovou pravděpodobností).
 - Lze charakterizovat vedle pravděpodobnosti výskytu bezpečnostního incidentu i potenciálně způsobenou škodou.
 - Při analýze rizik identifikujeme a hodnotíme aktiva, hrozby, zranitelná místa a dopady na aktiva.
 - Na základě bezpečnostních rizik se připravují potřebná bezpečnostní opatření, která umožňují plnit bezpečnostní požadavky.
-

Útok, bezpečnostní incident, útočník



**SLEZSKÁ
UNIVERZITA**
OBCHODNĚ PODNIKATELSKÁ
FAKULTA V KARVINĚ

- ❑ Útok nazýváme bezpečnostní incident, při kterém jde o úmyslné využitkování zranitelného místa, tj. využití zranitelného místa ke způsobení škod, ztrát na aktivech IS apod. nebo neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech.
 - ❑ Útočit lze např. přerušením, odposlechem, změnou a přidáním hodnoty.
 - ❑ Útočník vede útok a může být vnější, ale v i vnitřní.
 - ❑ Podle znalosti a vybavenosti rozeznáváme útočníky slabé, střední a velké síly.
-

Bezpečnostní politika



**SLEZSKÁ
UNIVERZITA**
OBCHODNĚ PODNIKATELSKÁ
FAKULTA V KARVINĚ

- ❑ **Bezpečnostní politika v oblasti IT je nedílnou součástí všeobecné bezpečnostní politiky organizace**
 - ❑ **Představuje souhrn bezpečnostních zásad a předpisů definujících způsob zabezpečení organizace, zahrnující např. fyzickou ostrahu, ochranu profesních zájmů, popř. ochranu soukromí a lidských práv.**
 - ❑ **Zabývá se výběrem bezpečnostních zásad a předpisů splňujících bezpečnostní politiku organizace a obecně definujících bezpečné používání informačních zdrojů v rámci organizace, nezávisle na konkrétně použitých informačních technologiích.**
 - ❑ **Určuje, která data jsou pro organizaci citlivá, kdo je za ně odpovědný, předpisuje infrastrukturu zabývající se v rámci organizační struktury organizace bezpečností, vymezuje základní omezení, která se musí respektovat apod.**
-

Bezpečnostní politika



**SLEZSKÁ
UNIVERZITA**
OBCHODNĚ PODNIKATELSKÁ
FAKULTA V KARVINĚ

Bezpečnostní politika je deklarace cílů a požadavků na úroveň bezpečnosti v organizaci a stanovení rámce co, kdo a jakým způsobem se má dosáhnout.

Obecně vymezuje:

- co vyžaduje ochranu;
 - proti jakým hrozbám je ochrana budovaná;
 - jak budeme chránit to, co vyžaduje ochranu.
-

Identifikace



- ❑ **Obecně řečeno se jedná o přiřazení známé veličiny v rámci systému neznámé entitě, takže ta se stane systému známou.**
 - ❑ **Zmíněná známá veličina se nazývá identifikátorem (často označovaným ID), což je ve většině případů jméno nebo nějaké kódové označení.**
 - ❑ **Aby nedocházelo ke komplikacím, je požadováno, aby identifikátor byl jedinečný alespoň v rámci daného systému.**
 - ❑ **Příkladem identifikace je představení se.**
-

Autentizace

- ❑ Tento proces stvrzuje pravost (autenticitu) identifikace.
- ❑ U autentizace osob se jedná o ověření, zda se jedná opravdu hlásící se osobu, autentizace objektů zpravidla znamená potvrzení jejich původu.

Autorizace

- ❑ V tomto procesu přiřazujeme identifikované a autorizované osobě práva, kterými disponuje v daném systému.
 - ❑ V praxi se jedná o přiřazení zařízení, přístupu k datům, rozsah funkcionality poskytované služby, práva vykonávat určité činnosti v rámci systému atd.
 - ❑ Většinou se to děje na základě přidělování registrovaných rolí přihlašovanému uživateli.
-

Způsoby autentizace



Způsoby autentizace osob můžeme rozdělit na autentizace:

- **na základě znalosti vstupních kódů, popř. postupů (textový login, textové heslo, PIN, posloupnost operací atd.);**
 - **na základě vlastnictví identifikačního předmětu (karta, čárový kód, hardwarový klíč identifikační doklad apod.);**
 - **na základě toho, že člověk má určitou jedinečnou vlastnost, biometrika (biologické vlastností uživatele, např. otisky prstů, sítnice apod.).**
 - **při přihlašování do počítačové sítě po identifikaci vložení jména, popř. kódu, se autentizujeme vložení hesla.**
-

Identifikační prvky



- ❑ Mezi identifikační prvky se řadí metody identifikace na základě vlastnictví identifikačních prvků, tokenů, což jsou předměty, které autentizují svého vlastníka. Musí být jedinečné a nepadělatelné. Patří sem:
 - systémy čárových kódů;
 - systémy karet;
 - systémy radiofrekvenční identifikace;
 - hardwarové klíče;
 - elektronické klíče.

 - ❑ Biometrika je metoda identifikace podle biologických vlastností uživatele. Mezi tyto metody patří: otisky prstů, oční sítnice, oční duhovka, tvář, hlas, podpis, geometrie ruky.
-

- ❑ **Můžeme si vymežit dvě skupiny dokladů:**
 - **doklady, jejichž primární funkcí je určení totožnosti majitele, např. občanský průkaz apod.;**
 - **doklady, pomocí kterých majitel prokazuje určité oprávnění, např. řidičský průkaz apod.**
-

Specifikace strojově čitelných cestovních dokladů jsou stanoveny v dokumentu Mezinárodní organizace pro civilní letectví (ICAO). Podle těchto norem se u strojově čitelných cestovních dokladů strana s osobními údaji dělí na dvě zóny:

- zóna vizuální kontroly – Visual Inspection Zone, VIZ, obsahující označení dokladu, fotografii obličeje držitele, osobní údaje a údaje týkající se vydání dokladu a jeho platnosti;
 - strojově čitelná zóna – Machine Readable Zone, MRZ, obsahující některé z informací obsažených v zóně vizuální kontroly v podobě alfanumerických znaků a symbolu „<“, a to ve dvou či ve třech řádcích. Tuto posloupnost znaků lze přečíst pomocí čtecího zařízení a usnadnit tak kontroly cestovních dokladů. (OCR – Optical Character Recognition (082) – speciální font písma pro strojově čitelné CD – OCR-B)
-

- ❑ Šifrování spočívá v převedení zprávy (otevřeného textu) do některé z možných reprezentací (šifrovaného textu).
 - ❑ Cílem šifrování je skrýt obsah zprávy před každým, komu tato zpráva není určena. Konkrétní šifrový text je určen klíčem.
 - ❑ Kryptografie představuje mechanismus, který je tvořen:
 - dvěma samostatnými algoritmy: o algoritmus šifrování, o algoritmus dešifrování,
 - kryptografickým klíčem, který spolu se šifrovanou zprávou tvoří vstupní parametry algoritmů šifrování a dešifrování.
 - ❑ Jak klíč, tak použité funkce mají rozhodující význam pro šifrování. V současné době se používají dvě základní třídy šifrovacích algoritmů:
 - symetrické;
 - asymetrické.
-

DĚKUJI ZA POZORNOST