INFORMAČNÍ SYSTÉMY VE VEŘEJNÉ SPRÁVĚ

doc. RNDr. Ing. Roman Šperka, Ph.D.

INFORMAČNÍ SYSTÉMY VE VEŘEJNÉ SPRÁVĚ

BEZPEČNOST INFORMAČNÍHO SYSTÉMU

Informace s nezanedbatelnou hodnotou,
musí být chráněny:

- aby k nim měly přístup pouze oprávněné osoby
- aby se zpracovávaly nefalšované informace
- aby se dalo zjistit, kdo je vytvořil, změnil nebo odstranil
- aby nebyly nekontrolovaným způsobem vyzrazeny
- aby byly dostupné tehdy, když jsou potřebné.

Model oblasti bezpečnosti IT se skládají z komponent:

hardware

- procesor, paměti, terminály, telekomunikace atd.

software

- aplikační programy,
- operační systém atd.

data

- data uložená v databázi, výsledky, výstupní sestavy, vstupní data atd.

lidé

- uživatelé,
- personál.

Bezpečnost

- ochrana odpovídajících IS a informací, které jsou v nich uchovávány, zpracovávány a přenášeny
- součástí bezpečnosti je i:
  - komunikační bezpečnost, tj. ochrana informace přenášené mezi počítači,
  - fyzická bezpečnost, tj. ochrana před přírodními hrozbami a fyzickými útočníky,
  - personální bezpečnost, tj. ochrana před vnitřními útočníky.

Bezpečnost

- je dána zajištěním:
  - důvěrnosti, k aktivům (k údajům) mají přístup pouze autorizované subjekty
  - integrity a autenticity, aktiva (data, software, hardware) smí modifikovat jen autorizované subjekty a pů-vod informací je ověřitelný
  - dostupnosti, aktiva (data nebo služby) jsou autorizovaným subjektům do určité doby dostupná, nedojde tedy k odmítnutí služby, kdy subjekt nedostane to na co má právo.

Kritické body:

- zranitelné místo,
- hrozba,
- riziko,
- útok,
- útočník

Zranitelné místo

- slabinu IS využitelná ke způsobení škod nebo ztrát útokem na IS
- důsledek chyb:
  - selhání v analýze,
  - v návrhu,
  - v implementaci IS,
  - ve vysoké hustotě uložených informací,
  - ve složitosti softwaru,
  - v existenci skrytých kanálů pro přenos informace jinou než zamýšlenou cestou apod.

Zranitelné místo

- podstata zranitelného místa může být:
  - fyzická, např. umístění IS v místě, které je snadno dostupné sabotáži, vandalismu, výpadek napětí
  - přírodní,objektivní faktory typu záplava, požár, zemětřesení, blesk
  - v hardwaru nebo v softwaru
  - fyzikální, vyzařování, útoky při komunikaci na výměnu zprávy, na spoje
  - lidský faktoru

Hrozba

- vlastnosti (součásti) informačního systému, jejichž existence způsobuje, že některé vlivy prostředí, ve kterém se IS provozuje, představují pro něj nebezpečí
- možnost využitkovat zranitelné místo IS k útoku na něj ke způsobení škody na aktivech

Hrozba

- hrozby lze kategorizovat na:
  - objektivní
    - přírodní, fyzické (požár, povodeň, výpadek napětí, poruchy…)
    - fyzikální (např. elektromagnetické vyzařování)
    - technické nebo logické (porucha paměti, softwarová "zadní vrátka", špatné propojení jinak bezpečných komponent, krádež …)
  - subjektivní (hrozby plynoucí z lidského faktoru
    - neúmyslné
    - úmyslné (vnější i vnitřní útočníci)

Riziko

- existence hrozby představuje riziko
- pravděpodobnost zužitkování zranitelného místa IS (hrozba se uplatní s takovou a takovou pravděpodobností).
- lze charakterizovat vedle pravděpodobnosti výskytu bezpečnostního incidentu i potenciálně způsobenou škodou.

Útok

- nazýváme i bezpečnostní incident,
- úmyslné využitkování zranitelného místa, tj. využití zranitelného místa ke způsobení škod, ztrát na aktivech IS,
- neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech

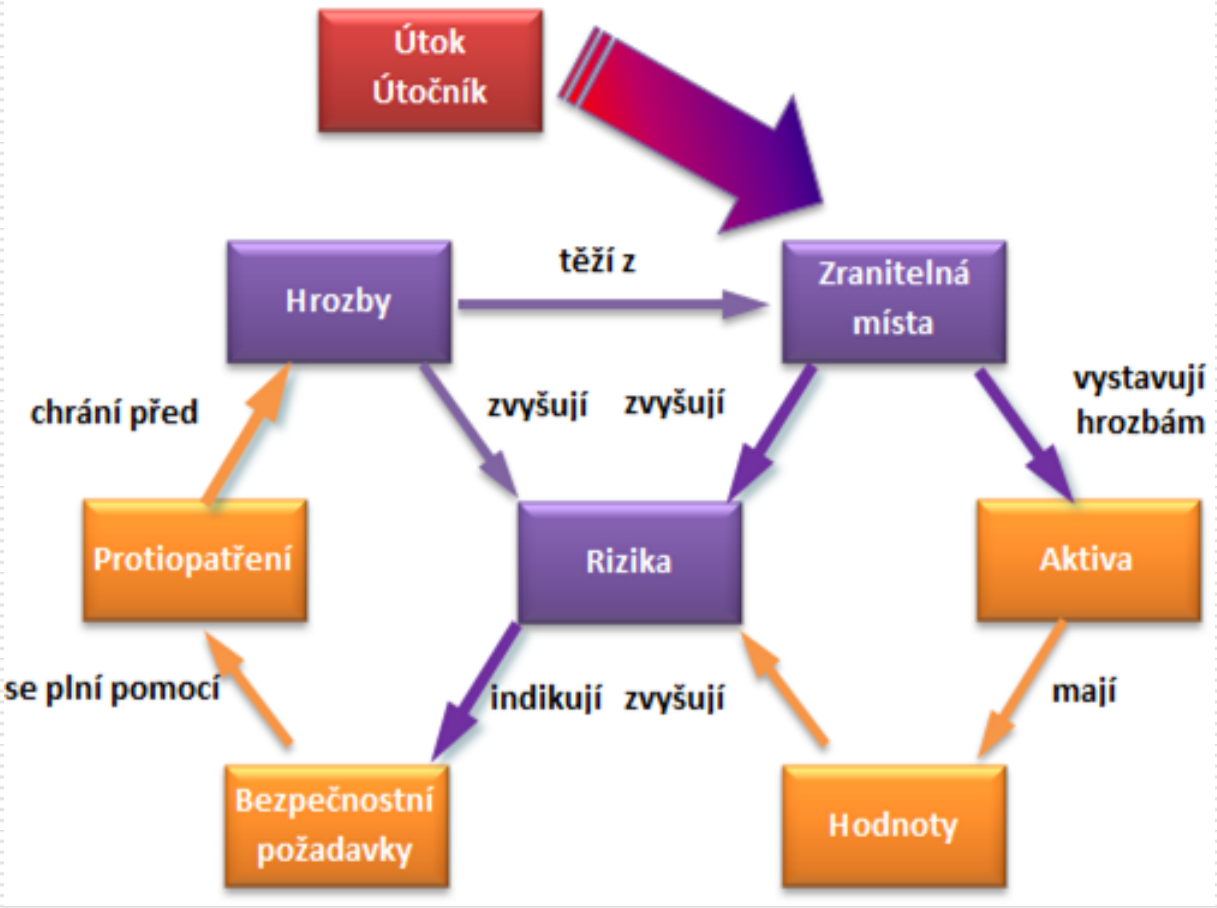
Útok

- útočit lze:
  - přerušením (aktivní útok na dostupnost, např. ztráta, znepřístupnění, poškození aktiva, porucha periférie, vymazání programu, vymazání dat, porucha v OS),
  - odposlechem (pasivní útok na důvěrnost, kdy neautorizovaný subjekt si neoprávněně zpřístupní aktiva, jde např. o okopírování programu nebo o okopírování dat)
  - změnou (aktivní útok na integritu, neautorizovaný subjekt zasáhne do aktiva, provede se např. změna uložených nebo přenášených dat, přidání funkce do programu)
  - přidáním hodnoty (aktivní útok na integritu nebo útok na autenticitu, tj. případ, kdy neautorizovaná strana něco vytvoří, např. podvržení transakce, dodání falešných dat).

Útočník

- může být vnější, ale v i vnitřní
- podle znalosti a vybavenosti rozeznáváme:
  - útočník slabé síly (amatéři, náhodní útočníci apod., stačí přijmout relativně slabá bezpečnostní opatření),
  - útočník střední síly (hackeři atd., útočníci mají omezené prostředky; opatření střední síly)
  - útočník velké síly (profesionální zločinci, nutno přijímat silná bezpečnostní opatření)

Vztahy v rámci systému bezpečnosti



Bezpečnostní politika

- je nedílnou součástí všeobecné bezpečnostní politiky organizace
- zabývá se výběrem bezpečnostních zásad a předpisů splňujících bezpečnostní politiku organizace
- 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
- stanovuje normy, pravidla a předpisy konkrétně definující způsob správy, ochrany, distribuce citlivých informací
- zahrnuje:
  - specifikace bezpečnostních opatření a způsobu jejich implementace
  - určení způsobu jejich použití, který zaručuje přiměřenou bezpečnost odpovídající požadavkům bezpečnostní politiky IT organizace
- cíle, strategie a politiky bezpečnosti se musí periodicky korigovat

Zásady výstavby bezpečnostní politiky

- Bezpečnostní politika organizace obecně vymezuje:
  - co vyžaduje ochranu
  - proti jakým hrozbám je ochrana budovaná
  - jak budeme chránit to, co vyžaduje ochranu.

Zásady výstavby bezpečnostní politiky

- Podpora dosažení požadované úrovně bezpečnost IS:
  - správa konfigurace
    - systematické vedení evidence změn konfigurace použitých,
    - posuzování změny konfigurace z hlediska dopadu na bezpečnost,
    - promítnutí změn do všech relevantních dokumentů,
    - kriticky rozsáhlá změna může vyvolat přepracování systémové bezpečnostní politiky,
    - smyslem je mít vědomost o změnách a ne zabránit změnám,
  - správa změnového řízení
    - pomocný řídicí nástroj pro identifikaci nových požadavků na bezpečnost po změně vlastností IS
    - změny představují zařazení nových provozních procedur, inovaci softwaru, revize hardwaru, zařazení nových uživatelů, nových skupin uživatelů, nová síťová spojení apod.
    - změna se musí posoudit z hlediska dopadu na bezpečnost,
    - výsledek projednání a případné rozhodnutí nutno dokumentovat

Typy bezpečnostních politik

- promiskuitní bezpečnostní politika
- liberální bezpečnostní politika
- opatrná bezpečnostní politika, resp. racionální bezpečnostní politika
- paranoidní bezpečnostní politika

Promiskuitní bezpečnostní politika

- politika nikoho neomezující,
- každému v zásadě povoluje dělat vše,
- IS s PBP jsou provozně nenákladné, mnohdy ani nenutí povinně používat pro autentizaci alespoň hesla,
- zaručují minimální nebo vůbec žádnou bezpečnost
- důvodem používání IS s promiskuitní bezpečnostní politikou může být ekonomičnost řešení,

Liberální bezpečnostní politika

- každému povoluje dělat vše, až na věci explicitně zakázané,
- zaručuje větší bezpečí než promiskuitní politika,
- často uplatňována v prostředích, ve kterých se hrozby považují za málo až průměrně závažné
- nepominutelným požadavkem je nízká ekonomická náročnost řešení bezpečnosti,
- opírá se o zásadu volitelného řízení přístupu založeného na identitě subjektů.

Opatrná bezpečnostní politika

- resp. racionální bezpečnostní politika,
- zakazuje dělat vše, co není explicitně povoleno,
- nákladnější na zavedení,
- zaručuje vyšší stupeň bezpečnosti,
- při aplikaci na IS vesměs požaduje provedení klasifikace objektů a subjektů podle jejich schopností a citlivosti,
- zásada povinného řízení přístupu založeného na rolích, ve kterých vystupují subjekty při styku s IS,
- při používání IS v Internetu je obvykle počáteční bezpečnostní politikou při zavádění firewallů.

Paranoidní bezpečnostní politika

- zakazuje dělat vše potenciálně nebezpečné, tedy i to, co by nemuselo být explicitně zakazováno (např. zákaz použití internetu, použití IS bez on-line napojení na komunikace),
- zaručuje nejvyšší stupeň bezpečnosti,
- maximální izolace systému,
- užitečná pro určitý okruh organizací
  - databázový systém zpracovávající vysoce důvěrné informace
- umožní implementaci aplikace v prostředí s nízkou systémovou režií, tudíž s dosažitelnou vyšší výkonností při zachování nižší úrovně nákladů.

Bezpečnostní funkce

- zabezpečujeme-li IS, je třeba nejprve stanovit bezpečnostní cíle a způsob jejich dosažení,
- bezpečnostní cíle jsou dílčí přínosy k bezpečnosti, kterou dosahuje IS z hlediska udržení důvěrnosti, integrity a dostupnosti
- pro jejich dosažení se aplikuje používání funkcí prosazujících bezpečnost, nazývaných rovněž bezpečnostní funkce nebo bezpečnostní opatření

Bezpečnostní funkce

- přispívá ke splnění jednoho nebo ní několika bezpečnostních cílů
- ke stanovení bezpečnostního cíle je třeba znát zranitelná místa,
- prostředek použitý pro dosažení stanovených bezpečnostních cílů IS
- mohou být typu:
  - administrativního,
  - fyzického,
  - logického.

Bezpečnostní funkce

- kategorizace podle okamžiku uplatnění:
  - preventivní (např. odstraňující zranitelná místa nebo aktivity zvyšující bezpečnostní uvědomění)
  - heuristické (snižující riziko dané nějakou hrozbou)
  - detekční a opravné (minimalizující účinek útoku podle schématu "detekce-oprava-zotavení").

Bezpečnostní funkce

- kategorizace podle způsobu implementace:
  - funkce softwarového charakteru
    - logické bezpečnostní funkce (např. softwarové řízení přístupu, funkce založené na použití kryptografie, digitální podepisování, antivirové prostředky, zřizování účtů, standardy pro návrh, kódování, testování, údržbu programů, ochranné nástroje v operačních systémech, ochranné nástroje v aplikačních systémech pro autentizaci přístupu, pro autentizaci zpráv atd.)
  - administrativního a správního charakteru
    - ochrana proti hrozbám souvisejícím s nedokonalostí odpovědnosti a řízení systému IT
    - výběr a školení důvěryhodných osob, hesla, autorizační postupy, přijímací a výpovědní postupy, právní normy, zákony, vyhlášky, předpisy, etické normy, licenční politika, nástroje provozního řízení, zpravodajství o událostech a stavech významných z hlediska bezpečnosti, sběru a analýzy statistik, konfigurace systému apod.

Bezpečnostní funkce

- kategorizace podle způsobu implementace:
  - hardwarového charakteru
    - technické bezpečnostní funkce (autentizace na bázi identifikačních karet, šifrovače, autentizační kalkulátory, firewally, archivní pásky - záložní kopie dat a programů)
  - fyzického charakteru
    - stínění, trezory, zámky, strážní, jmenovky, protipožární ochrana, záložní generátory energie

Bezpečnostní mechanizmy

- logika nebo algoritmus, který
  - hardwarově (technicky),
  - softwarově (logicky),
  - fyzicky nebo
  - administrativně

  implementuje bezpečnostní funkci.

Informační koncepce - řízení bezpečnosti ISVS

- v rámci Informační koncepce se stanovují dlouhodobé cíle bezpečnosti
  - transformují se do konkrétních požadavků na bezpečnost
  - následně se stanovuje plán, jak má být těchto cílů resp. naplnění požadavků dosaženo
  - každý požadavek by se měl opírat o projektovou bezpečnostní a provozní bezpečnostní dokumentaci
  - ákladní požadavky stanovuje Vyhláška č. 529/2006 Sb.
- Dlouhodobé cíle můžeme rozdělit na oblasti zajištění bezpečnosti:
  - dat;
  - služeb;
  - technických a programových prostředků.

Bezpečnost dat

Dostupnost dat

- měla být zajištěna vhodnou kombinací technických a programových prostředků úměrně potřebě dat
- patří sem např. použití diskových polí, clusterů, i softwarových nástrojů. Je nutné stanovit politiku zálohování a archivací (periodicita, způsoby zálohování a archivací dat, způsoby uložení dat apod.

Důvěrnost dat

- zabezpečení dat tak, aby k nim oprávněné osoby měly přístup v rozsahu svého oprávnění (umožnění čtení popř. manipulaci a úpravy) a neoprávněné osoby neměly přístup vůbec
- k datům je nutné zavést řízený přístup. Jde o aplikace základních atributů zabezpečení přístupu:
  - identifikace, každý uživatel je jednoznačně identifikován jménem nebo kódem;
  - autentizace, uživatel prokáže svoji totožnost (heslem, otiskem prstu apod.);
  - autorizace, každý uživatel je oprávněn k úkonům odpovídajícím roli, kterou zastává.

Integrita dat

- je zajištěna volbou vhodných nástrojů pro zpracování dat (řízení databází zajišťující referenční integritu, archivační nástroje atd.).

Bezpečnost služeb

Dostupnost služeb

- je zajištěna vhodnou kombinací technických a programových prostředků úměrně potřebnosti služeb
- patří sem prostředky zajišťující odolnost proti výpadku elektrické energie, komunikačních sítí, hardwarových a softwarových prvků apod. a také nástroje pro ochranu proti útokům atd.

Důvěrnost služeb

- vyžaduje, aby procesy služeb a přenosu informací mezi zdrojem a cílem byly chráněny odpovídajícím způsobem
- jedná se o aplikaci základních atributů zabezpečení přístupu, tedy identifikace, autentizace a autorizace

Integrita služeb

- týká se např. sdílení informací o uživateli, sdílení služeb datových zdrojů apod.
- tento bezpečnostní cíl pokrývá zajištění integrity služeb samostatných a spolupracujících systémů

Bezpečnost technických a programových prostředků

Dostupnost

technických prostředků

zahrnuje záložní zdroje napájení, záložní síťová připojení, duplikace hardware duplikováním, popř. násobení důležitých prvků, umístění záložních zařízení do geograficky různých lokalit atd.

programových prostředků

zahrnuje zejména používání výrobcem certifikovaných softwarových komponent, testování a včasnou aplikaci záplat programového vybavení, nasazení prostředků monitorování provozu a včasného upozornění jak na prostředky vlastního informačního systému, tak i na prostředky síťové infrastruktury, použití nástrojů softwarové ochrany (antiviry apod.), logické umístění do bezpečné zóny sítě apod.

Bezpečnost technických a programových prostředků

Důvěrnost

technických prostředků

zahrnuje především fyzickou bezpečnost (umístění technických prostředků do zabezpečeného prostoru, fyzická ochrana před riziky prostředí, další opatření), zabezpečení telekomunikační infrastruktury (nastavení switchů, routerů apod.).

programových prostředků

se týká zejména zajištění odolnosti proti úmyslně či neúmyslně chybným vstupním datům (např. odolnost proti buffer overflow, SQL injection apod. útokům), zajištění ochrany proti parazitním kódům, zajištění ochrany proti podvržení identity spolupracujících systémů.

Bezpečnost technických a programových prostředků

Integrita

technických prostředků

týká se zejména: ochrany proti přetížení a proti zničení či poškození.

programových prostředků

zahrnuje ochranu proti smazání softwarové komponenty, modifikaci či podvržení softwarové komponenty a modifikaci konfigurace softwarové komponenty.

Požadavky na bezpečnost ISVS

- souhrn požadavků, které jsou konkretizací obecných cílů bezpečnosti
- měly být být měřitelné
- měly by být vázány na cíle bezpečnosti, k jejichž naplnění směřují
- mohou být specifické pro jeden IS nebo společné pro několik IS daného správce, resp. záměry na vybudování nových IS nebo jejich skupiny
- součástí vyhodnocování IK by mělo být mj. též vyhodnocování míry a způsobu naplnění stanovených požadavků
- konkrétní bezpečnostní požadavky by měly být výsledkem
  - bezpečnostní analýzy (analýza rizik)
  - návrhu opatření odpovídajících míře rizika velikosti s ním svázané škody.

Plán řízení bezpečnosti ISVS

- časový harmonogram plnění cílů a požadavků v oblasti bezpečnosti
- má obdobnou strukturu jako plán kvality:
  - stanovení cílů bezpečnosti;
  - stanovení požadavků na bezpečnost;
  - implementace požadavků na bezpečnost;
  - prověrka dodržování požadavků na bezpečnost;
  - vyhodnocení řízení bezpečnosti

Bezpečnostní dokumentace ISVS

- součást provozní dokumentace dle Vyhlášky 529/2006 Sb.
- Tvoří ji:
  - bezpečnostní politika ISVS;
  - bezpečnostní směrnice pro činnost bezpečnostního správce systému

Bezpečnostní politika

- musí být vytvořena vždy pokud :
  - systém má vazby s ISVS jiného správce
  - orgán veřejné správy (správce ISVS) není provozovatelem tohoto systému
- obsahuje popis bezpečnostních opatření, která
  - orgán veřejné správy uplatňuje při zajišťování bezpečnosti tohoto systému
  - odpovídají požadavkům na bezpečnost stanoveným v informační koncepci
- spíše globálnější pohled na ISVS
- uvedená opatření mohou být i organizační či personální
  - např. je uvedeno, že čipovou kartu, která se používá pro označování výstupů z informačního systému, ukládá pracovník oddělení informatiky každý večer do určeného trezoru – nejedná se tedy přímo o funkcionalitu systému; dalším příkladem může být povinnost určeného zaměstnance pravidelně zálohovat data a určení místa uložení záloh
- Orgán veřejné správy předkládá při atestaci bezpečnostní politiku ISVS

Bezpečnostní směrnice

- bezpečnostní správce systému je zaměstnanec nebo jiná fyzická osoba, která zajišťuje kontrolu bezpečnosti ISVS a provádí další činnosti, které mají zajistit bezpečnost daného IS
- činnost bezpečnostního správce systému omezuje činnost správce systému
- roli správce systému a současně roli bezpečnostního správce systému může vykonávat jedna fyzická osoba pouze v případě, že se jedná o ISVS, který
  - nemá vazby s ISVS jiného správce
  - orgán veřejné správy stanovil a uplatňuje odpovídající bezpečnostní opatření, která vyloučí rizika, která by z vykonávání obou rolí jednou fyzickou osobou mohla vyplývat
- ke spojení rolí se přistupuje v případě menších systémů, kdy rozdělení funkce správce a bezpečnostního správce by bylo neefektivní
- pokud roli správce systému a roli bezpečnostního správce sytému vykonává jedna fyzická osoba, lze sloučit bezpečnostní směrnici pro činnost bezpečnostního správce systému se systémovou příručkou

Bezpečnostní směrnice

- bezpečnostní směrnice pro činnost bezpečnostního správce systému obsahuje
  - podrobný popis bezpečnostních funkcí, které bezpečnostní správce systému používá pro provádění určených činností v ISVS
  - návod na použití těchto funkcí
  - tyto funkce slouží např. ke kontrole událostí, které v systému proběhly nebo ke sledování neoprávněných pokusů přistoupit do systému apod
- definuje pro každou roli souhrn určených činností a potřebných oprávnění pro provádění těchto činností v ISVS

Kryptografie

- Kryptografie, jako jeden z důležitých bezpečnostních mechanizmů, se používá k zabezpečení:
  - důvěrnosti (utajení) informace, tedy ochrany před neautorizovaným zpřístupněním důvěrné informace;
  - prokazování integrity informace, čili ochrany před neautorizovanými změnami dat nebo proti nasazení virů apod.;
  - autentizaci, tj. prokázání totožnosti subjektu;
  - řízení přístupu k objektům (datům, programům atd.);
  - zaručeného prokazování původu zprávy, nepopiratelnosti
- spočívá v převedení zprávy (otevřeného textu) do některé z možných reprezentací (šifrového textu)

Kryptografický systém

- můžeme si ho představit jako pětici podmnožin:
  - konečná množina srozumitelných textů - prostor zpráv,
  - konečná množina možných šifer - prostor šifer,
  - konečná množina možných klíčů - prostor klíčů,
  - množina šifrovacích funkcí (pravidel, algoritmu),
  - množina dešifrovacích funkcí

Kryptografický mechanizmus

- je tvořen:
  - dvěma samostatnými algoritmy:
    - algoritmus šifrování,
    - algoritmus dešifrování,
  - kryptografickým klíčem, který spolu se šifrovanou zprávou tvoří vstupní parametry algoritmů šifrování a dešifrování.

Kryptografické bezpečnostní mechanismy

- kryptografie se používá
  - pro dosažení důvěrnosti (utajení) informace (ochrana proti neautorizovanému zpřístupnění důvěrné informace),
  - pro zaručení integrity informace (ochrana proti neautorizované změně dat, resp. ochrana proti nasazení virů do programů),
  - při autentizaci (prokázání totožnosti subjektu),
  - při řízení přístupu k objektům
  - při zaručeném prokazování původu zprávy (nepopiratelnost)

Symetrická kryptografie

- komunikující partneři používají stejný kryptografický klíč
- hovoříme také o kryptografii s tajným klíčem
- znalost tajného klíče může sloužit jako důkaz identity
- různé symetrické algoritmy používají různé délky klíčů
  - delší klíč obvykle znamená větší bezpečnost algoritmu
- mimo služby zajištění důvěrnosti ji lze použít i pro autentizaci
- problematické je předání šifrovacího klíče mezi komunikujícími před začátkem komunikace
- k tomu je nutné použít důvěryhodného, chráněného, neveřejného kanálu, nejlépe osobního předání

Asymetrická kryptografie

- klíče komunikujících partnerů se liší
- klíče musí splňovat dvě důležité vlastnosti:
  - klíče jsou navzájem neodvoditelné, čili ze znalosti jednoho klíče nemůžeme vypočíst druhý;
  - zpráva se jedním klíčen zašifruje, dešifrování stejným klíčem už není možné a provede se až druhým klíčem.
- příkladem aplikace je kryptografie s veřejným klíčem a soukromým klíčem
  - veřejný klíč se zveřejní
  - soukromý je nutné udržet v tajnosti a bezpečí

Hybridní šifrování

- symetrické šifra je lepší pro zajištění důvěrnosti, asymetrická šifra pro zajištění integrity a neodmítnutelnosti
- hybridní šifrování spojuje výhody obou řešení
- nejprve se náhodně vygeneruje klíč pro symetrickou šifru, kterým se zašifruje zpráva
- symetrický klíč se zašifruje pomocí asymetrické šifry a spolu se šifrovanou zprávou se odešle příjemci
- příjemce nejdříve klíč dešifruje klíč a pak pomocí klíče k symetrické šifře dešifruje i zprávu samotnou
- výhodou je, že
  - pomocí asymetrické šifry, která má složitější algoritmy a je pomalejší, se dešifruje pouze krátký klíč
  - mnohem delší zpráva, se šifruje rychlejším algoritmem pro symetrickou šifru
- bezpečnost systému je závislá na bezpečnosti obou použitých šifer

Certifikační autorita

- důvěru v pravost asymetrických klíčů komunikujících stran poskytuje certifikační autorita
- vydává digitální certifikáty (elektronicky podepsané veřejné šifrovací klíče)
- svojí autoritou potvrzuje pravdivost údajů, které jsou ve volně dostupném veřejném klíči uvedeny
- certifikační autorita ověří totožnost majitele asymetrických klíčů a digitálně podepíše jeden z dvojice klíčů

Certifikační autorita

- certifikát představuje datovou strukturu, která je svázána s určitou osobou
- pomocí certifikátu lze tedy tuto osobu jednoznačně identifikovat.
- pomocí certifikátu lze ověřit elektronický podpis dané osoby
- součástí vydaného certifikátu většinou jsou:
  - identifikátor certifikátu (sériové číslo, nemusí být)
  - informace o držiteli certifikátu;
  - doba platnosti:
    - datum počátku platnosti;
    - datum konce platnosti certifikátu;
  - použitý algoritmus;
  - účel použití;
  - veřejný klíč;
  - atd.

Certifikační autorita

- obsah certifikátu je podepsán vydávající certifikační autoritou, aby bylo možné prokázat, že byl touto autoritou skutečně vydán.
- tzv. kvalifikovaný certifikát definován Zákonem 227/2000 Sb. může vydat pouze akreditovaná kvalifikovaná certifikační autorita
- Ministerstvo vnitra uděluje akreditaci k působení jako akreditovaný poskytovatel certifikačních služeb a přehled udělených akreditací zveřejňuje
- řada neakreditovaných organizací poskytuje své certifikáty, většinou pro potřebu svých systémů, které můžeme nazvat komerční certifikáty

Elektronický podpis

- Při předávání dokumentů je třeba zajistit jejich:
  - autentičnost (původ, autora);
  - neporušenost (integritu);
  - nepopiratelnost (podepsaná strana nemůže později popřít, že daný dokument podepsala)

Elektronický podpis

- tety musíme použít postup, zaručující určité vlastnosti, které podepsaný dokument získá.
- strana, která získá podepsaný dokument musí být ubezpečena, že:
  - autorem dokumentu je označená osoba,
  - se seznamuje s přesným obsahem dokumentu,
  - může na základě takto získaného dokumentu konat a mít přitom určité záruky od autora dokumentu.
- někdy k tomu přistupují i nároky na utajení obsahu dokumentu před nepovolanou osobou.

Elektronický podpis

- důležitý bezpečnostní požadavek na proces zpracování, ukládání a přenášení informací je zajištění integrity těchto dat
  - tj. požadavek na zabránění neodhalené a neoprávněné modifikaci dat
- k dokumentům (datům) se připojí jistá informace, která příjemci autentizuje (prokazuje totožnost) odesílatele nebo tvůrce těchto dat, ale pouze v případě, že ji příjemce přijal spolu s daty neporušenou

Elektronický podpis

- je tvořen řetězcem bajtů, který je připojen k podepisovanému dokumentu
- délka tohoto řetězce bývá obvykle 50 až 300 bajtů podle použitého algoritmu a požadovaného stupně bezpečnosti a nezávisí na délce podepisovaného dokumentu
- od podepsaného dokumentu se nedá oddělit a následně použít k podepsání jiného dokumentu
- to v podstatě vylučuje možnost zneužití podpisu na jiný dokument, než pro který byl původně určen
- jedna osoba může mít několik různých elektronických podpisů (např. soukromý a v zaměstnání)
- Vyhláška č. 212/2012 Sb. stanovuje, že údaj, který umožňuje jednoznačnou identifikaci podepisující osoby, se uvádí ve struktuře desetimístného čísla v desítkové soustavě v rozsahu 1 100 100 100 až 4 294 967 295.

Elektronický podpis

- vlastnosti elektronického podpisu:
  - je spojen s jedním konkrétním elektronickým dokumentem
    - potvrzuje pravost a autenticitu tohoto dokumentu a nemůže být použit pro podepsání jiného dokumentu
  - může být vytvořen pouze tím, kdo zná jisté tajemství (např. soukromý klíč).
  - je nemožné vytvořit jiný dokument, sebeméně odlišný od původního dokumentu, pro který by byl původní elektronický podpis stále platný
  - jakmile je jednou elektronický podpis dokumentu vytvořen, kdokoli si může ověřit pravost tohoto podpisu, a to bez nutnosti znát tajemství (soukromý klíč), kterým byl podpis vytvořen

Elektronická značka

- v Zákoně č. 227/2000 Sb.
- jsou to údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují požadavky:
  - jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu;
  - byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou;
  - jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat.

Uznávaný elektronický podpis

- zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a obsahujícím údaje, které umožňují jednoznačnou identifikaci podepisující osoby;
- zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném poskytovatelem certifikačních služeb, který je usazen mimo území České republiky, byl-li kvalifikovaný certifikát vydán v rámci služby vedené v seznamu důvěryhodných certifikačních služeb jako služba, pro jejíž poskytování je poskytovatel certifikačních služeb akreditován, nebo jako služba, nad jejímž poskytováním je vykonáván dohled podle předpisu Evropské unie

Časové razítko

- spojuje dokument v elektronické podobě s časovým okamžikem jeho vzniku a zaručuje, že konkrétní data v elektronické podobě existovala před daným časovým okamžikem
- „razítkuje“ elektronický dokument v konkrétním čase a je vhodným doplňkem elektronického podpisu
- Kvalifikované časové razítko je podle zákona č. 227/2000 Sb. datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb
  - využívá se u elektronických dokumentů nebo dat, u kterých je nutné jednoznačné doložení času
  - propojuje elektronický dokument s okamžikem jeho vzniku, což zaručuje existenci konkrétních dat v elektronické podobně v daný okamžik

Časové razítko

- vypovídá pouze o tom, že příslušná zpráva či dokument existovala ještě před okamžikem, kdy byl otisk zaslán k vytvoření časového razítka
- nepotvrzuje však, od koho požadavek na časové razítko přišel, tedy zda data prošla např. systémem datových schránek
- to potvrzuje až elektronický podpis, ale bez časového razítka je časem problém prokazovat jeho platnost
- prodlouží platnost dokumentu s elektronickým podpisem minimálně o 5 let
- lze ho využít tam, kde je nutné prokázat, jak elektronický dokument vypadal v určitém okamžiku, např.:
  - při archivaci elektronických dokumentů;
  - při elektronických transakcích;
  - pro elektronické formuláře atd.

Děkuji za pozornost.

Otázky?