Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Riadenie prístupu do IS

Ivan Kopáčik

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Agenda

1. Čo je riadenie prístupu
2. Požiadavky a východiská
3. Modely riadenia prístupu
4. Identifikácia a autentizácia, adresárové služby
5. Vzdialený prístup

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Agenda II.

6. QAA, STORK a federácia identity
7. Riadenie prístupu z pohľadu prevádzky a jeho administrácia
8. Normalizovaný koncept systému riadenia prístupu
9. Auditovanie systému riadenia prístupov
10. Záver a diskusia

KPMG
cutting through complexity™

Čo je riadenie prístupu

- Pod riadením prístupu chápeme prideľovanie a spravovanie oprávnení pre narábanie s počítačovými zdrojmi (dátami, aplikáciami, súbormi atď.).
- Riadenie prístupu na fyzickej úrovni vymedzuje možnosti vstupu a výstupu osôb do budov, serverovní, výpočtového strediska, kancelárií alebo iných priestorov, ktoré fyzicky obsahujú IKT komponenty (servery, PC, tlačiarne a pod.). V praxi sa využíva viacero prostriedkov na podporu riadenia fyzického prístupu ako napr. návštevnícke karty, identifikačné (ID) karty zamestnancov, kľúče, biometrické systémy.
- Riadenie prístupu na logickej úrovni predstavuje prideľovanie a kontrolovanie prístupu k logickým komponentom a zdrojom (aplikácie, transakcie, dáta, služby internetu a pod.) a aplikuje sa vždy, keď sa predmetný zdroj má použiť.

Identifikácia, autentizácia, autorizácia

- Pod identifikáciou rozumieme proces, ktorým používateľ poskytuje svoju identitu do systému (napr. zadá prihlasovacie meno).
- Autentizácia znamená overenie (potvrdenie) identity, ktorú používateľ poskytol (napr. v rámci autentizácie zadá heslo).
- Autorizácia je stanovenie, čo je používateľ oprávnený vykonať alebo aké má prístupové oprávnenia (nezamieňať s autentizáciou).

Riadenie prístupu a personálna bezpečnosť

- Riadenie prístupu vo vzťahu ku konkrétnemu používateľovi korešponduje s fázami pracovnoprávneho vzťahu. V zásade sa jedná o vytvorenie, zmeny a odobratie prístupových práv používateľa. V prípade potreby *zriadenia prístupových práv* (napr. prijatie nového zamestnanca) je potrebné vykonať spravidla nasledovné činnosti:
- vytvoriť a nakonfigurovať samostatné používateľské konto,
- poučiť používateľa o pravidlách práce s IS (ak ešte nebol poučený),
- zvoliť metódu autentizácie a oboznámiť s ňou používateľa (napr. prvotné heslo),
- prideliť používateľskému kontu potrebné oprávnenia.

Riadenie prístupu a personálna bezpečnosť

- V situáciách vyžadujúcich *zmenu prístupových oprávnení* (napr. zmeny v služobných úlohách alebo pracovných činnostiach, preloženie zamestnanca na inú pozíciu) je potrebné zabezpečiť, aby súčasne s pridelením nových oprávnení boli odobrané pôvodné a nepotrebné oprávnenia. Pri prideľovaní a zmene prístupových oprávnení musí byť zachovaná zásada pridelenia najmenších potrebných oprávnení, ktoré používateľ potrebuje používať na vykonávanie svojej činnosti.
- *Odobratie prístupových oprávnení* (napr. pri ukončení pracovného pomeru zamestnanca, závažnom porušení pracovnej disciplíny, po splnení účelu zriadeného prístupu). V niektorých prípadoch je po zrušení oprávnení zrušené aj samotné používateľské konto. Konto je možné v IS ponechať, ale v zablokovanom stave (z dôvodu zachovania integrity údajov zaznamenaných v IS, ktoré sa viažu na identitu používateľa).

Riadenie prístupov - východiská

- Výnos Ministerstva financií Slovenskej republiky č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy (ďalej len „Výnos“)

- Norma ISO/IEC 27002 Pravidlá dobrej praxe manažérstva informačnej bezpečnosti

Výnos §40 Riadenie prístupu

Štandardom pre riadenie prístupu je

a) zavedenie identifikácie používateľa a následnej autentizácie pri vstupe do informačného systému verejnej správy,

b) vypracovanie interného aktu riadenia prístupu k údajom a funkciám informačného systému verejnej správy založeného na zásade, že používateľ má prístup iba k tým údajom a funkciám, ktoré sú potrebné na vykonávanie jeho úloh,

c) určenie postupu a zodpovednosti v súvislosti s prideľovaním prístupových práv používateľom,

d) určenie požiadaviek, ktoré majú používatelia v súlade s bezpečnostnou politikou povinnej osoby dodržiavať pri používaní informačného systému verejnej správy,

e) automatické zaznamenávanie zmien v pridelenom prístupe a ich archivácia počas celej doby činnosti informačného systému verejnej správy,

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Výnos §40 Riadenie prístupu

f) určenie bezpečnostných zásad na mobilné pripojenie do informačného systému verejnej správy a pre prácu na diaľku;mobilným pripojením je najmä prenosný počítač a personal digital assistant (PDA),

g) zabezpečenie, aby používatelia nepoužívali informačné systémy verejnej správy na nelegálne účely,

h) umožniť fyzickým osobám zodpovedným za správu a prevádzku informačných systémov verejnej správy prístup iba k takým údajom a funkciám v týchto informačných systémoch verejnej správy, ktoré nevyhnutne potrebujú na vykonávanie pridelených úloh,

i) automatické zaznamenávanie každého prístupu každého používateľa vrátane administrátora do informačného systému verejnej správy, zamedzenie možnosti zmeny týchto záznamov a zamedzenie možnosti vymazania týchto záznamov bez schválenia zodpovednou osobou určenou podľa § 28 písm. c),

j) vedenie formalizovanej dokumentácie prístupových práv všetkých používateľov informačného systému verejnej správy.

KPMG
cutting through complexity™

Výnos

- § 29 Personálna bezpečnosť (prideľovanie a odoberanie prístupov počas vzniku, trvania a ukončenia pracovného pomeru)
- § 33 Sieťová bezpečnosť (riadenie prístupu medzi prepojenými sieťami)
- § 34 Fyzická bezpečnosť a bezpečnosť prostredia (riadenie fyzického prístupu osôb)
- § 42 Účasť tretej strany (riadenie prístupu tretích strán)

Súvisiaca bezpečnostná dokumentácia

- § 29 Personálna bezpečnosť: f) vypracovanie postupu pri ukončení pracovného pomeru vlastného zamestnanca a pri ukončení spolupráce s externým pracovníkom alebo treťou stranou, ktorým sa zabezpečí... 4. zrušenie prístupových práv v informačných systémoch verejnej správy
- § 33 Sieťová bezpečnosť: c) zabezpečenie, aby pre každé prepojenie podľa písmena b) bol vypracovaný interný akt riadenia prístupu medzi týmito sieťami podľa § 40
- § 40 Riadenie prístupu: b) vypracovanie interného aktu riadenia prístupu k údajom a funkciám informačného systému verejnej správy založeného na zásade, že používateľ má prístup iba k tým údajom a funkciám, ktoré sú potrebné na vykonávanie jeho úloh

Súvisiaca bezpečnostná dokumentácia II.

- § 40 Riadenie prístupu:

  f) určenie bezpečnostných zásad na mobilné pripojenie do informačného systému verejnej správy a pre prácu na diaľku;mobilným pripojením je najmä prenosný počítač a personal digital assistant (PDA),

  j) vedenie formalizovanej dokumentácie prístupových práv všetkých používateľov informačného systému verejnej správy.

ISO/IEC 27002

Hlavným cieľom riadenia prístupu je riadiť prístup k informáciám. Prístup k informáciám a prostriedkom na spracúvanie informácií a podnikateľským procesom by mal byť riadený na základe pracovných a bezpečnostných požiadaviek. Pravidlá riadenia prístupu by sa mali brať do úvahy politiky šírenia informácií a autorizácie.

(Podrobnosti neskôr)

Modely riadenia prístupu

- Riadený prístup je rozhodujúci pre ochranu dôvernosti a integrity dát.
- Definícia a modelovanie riadeného prístupu bolo uceleným spôsobom stanovené už v roku 1983, keď MO USA zverejnilo bezpečnostné kritériá TCSEC vo forme tzv. „Orange book“:
  - voliteľné riadenie prístupu DAC (discretionary access control)
  - povinné riadenie prístupu MAC (mandatory access control).
- V deväťdesiatych rokoch bola vyvinutá metóda RBAC (role-based access control), ktorá v rôznych modifikáciách pokračuje dodnes.

Základné princípy a modely riadenia prístupu

- Riadenie prístupu metódou DAC
- Riadenie prístupu metódou MAC
- Riadenie prístupu založené na pravidlách (Rule-based access Control)
- Riadenie prístupu založené na rolách (RBAC)
- Riadenie prístupu založené na obmedzení rozhrania
- Matice pre riadenie prístupu
  - Capability lists (Zoznam povolených operácií)
  - Access control lists – ACL (Zoznam povolených prístupov)
  - Mechanizmus atribútov

Základné princípy a modely riadenia prístupu II.

- Bezpečnostné modely
  - Bell-LaPadula model
  - Biba model
  - Clark-Wilson model
- Pravidlá najmenších privilégií
- Oddeľovanie povinností
- Rotácia povinností
- Oddeľovanie sietí

Riadenie prístupu metódou DAC (discretionary access control)

- Každý používateľ má plnú kontrolu nad všetkými svojimi procesmi a súbormi, pričom niektoré práva k týmto súborom a procesom môže používateľ poskytnúť aj iným používateľom.
- Systémy založené na DAC umožňujú používateľom povoliť alebo zakázať prístup k objektom v ich vlastníctve. Najčastejšia implementácia tejto metódy je pomocou tzv. zoznamu povolených prístupov (ACL).
- Obmedzenie prístupu k objektu pre čítanie je „dočasné“. Napr. používateľ A udelí používateľovi B práva na čítanie súboru -> používateľ B skopíruje obsah súboru používateľa A do objektu, ktorý sám spravuje -> používateľ B môže sprístupniť túto kópiu akémukoľvek ďalšiemu používateľovi bez toho, aby o tom používateľ A vedel (!)
- Metóda prístupu DAC nedokáže čeliť útoku typu „trojský kôň“, pretože programy dedia identitu od používateľa, ktorý ich vyvolal.

Riadenie prístupu metódou MAC (mandatory access control)

- Prístup k objektom je na základe privilégií subjektu (používateľ) a citlivosti (klasifikačných atribútov) objektu (napr. súbor), prostredníctvom stanoveného spôsobu označovania.
- Používatelia nemajú možnosť rozhodovať, kto môže pristupovať k ich dátovým súborom.
- Napr. organizácia klasifikuje dokument ako citlivý, používateľovi môže byť udelené oprávnenie typu „citlivý“ -> bude mať prístup k všetkým objektom s touto klasifikáciou prípadne aj nižšou (ak je to vyžadované).

Riadenie prístupu metódou MAC (mandatory access control)

- Organizácia prostredníctvom systému určuje potrebné úrovne (stupne) citlivosti, známe aj pod pojmom „labels“ (návestia).
- Každému objektu je priradená úroveň citlivosti a je prístupný iba pre užívateľov, ktorí sú zaradení do tejto úrovne.
- Zmeniť úroveň citlivosti objektu môže zmeniť iba administrátor systému, nie vlastník objektu.
- Model MAC je vo všeobecnosti považovaný za bezpečnejší ako model DAC.
- Parametre MAC sú definované v Orange book B-level.
- MAC systémy je pomerne zložité konfigurovať ako aj prakticky implementovať.

Model riadenia prístupov založený na pravidlách

- Špeciálny typ MAC, pri ktorom je prístup k dátam určovaný pravidlami alebo používaním klasifikačných návestí a nie na základe identity subjektov a objektov samotných.
- Zvyčajne je založený na špecifických profiloch pre každého používateľa, čo umožňuje jednoduchú zmenu bezpečnostnej informácie aj pre jedného používateľa.
- Špecifické pravidlá vytvorené administrátormi určujú čo sa môže a nemôže vykonať s konkrétnym objektom.

Model riadenia prístupov založený na rolách (Role-Based Access Control)

- Rozhodnutia o prístupe sú založené na rolách, ktoré sú priradené konkrétnym používateľom na základe organizačnej štruktúry organizácie.
- Prístupové práva sú zoskupené podľa názvu roly a využívanie konkrétnych zdrojov je obmedzené iba pre osoby, ktoré majú túto rolu pridelenú.
- Bezpečnostná administrácia súvisiaca s RBAC pozostáva z určenia operácií, ktoré musia byť vykonané osobami
- RBAC je metóda riadenia prístupu typu MAC, často je taktiež nazývaná aj „Non-discretionary access control“.

Model riadenia prístupu založený na obmedzení rozhraní

- Obmedzuje prístupové možnosti používateľov takým spôsobom, že im neumožní požadovať určité funkcie alebo informácie resp. tak, že im neumožní prístup ku špecifickým zdrojom systému**.**
- Napr:
  - obmedzenie položiek v menu : používateľom sú ponúknuté iba možnosti príkazov, ktoré môžu spustiť,
  - databázové zobrazenie : používateľský prístup k dátam je obmedzený mechanizmami prezentácie dát na úrovni databázového nástroja,
  - fyzické oddelenie prístupu k používateľskému rozhraniu.

Matice pre riadenie prístupu

- Pole obsahujúce riadok pre subjekt v systéme a stĺpec pre objekt v systéme.

Subjekt/objekt	Súbor 1	Súbor 2	Súbor 3	Proces 1
Používateľ 1	-	Read, write	-	Suspend
Používateľ 2	Execute	-	Read, write	-
Používateľ 3	Read	Write	-	-
Používateľ 4	-	-	Read	-

- Využívané sú najmä nasledovné praktické implementácie prístupovej matice:
  - Zoznam povolených operácií,
  - Zoznam povolených prístupov,
  - Mechanizmus atribútov.

Zoznam povolených operácií

- Každý subjekt je priradený k zoznamu, ktorý obsahuje povolené operácie ku všetkým zahrnutým objektom.
- Bezproblémová možnosť skontrolovať všetky prístupy, ktoré sú autorizované pre daný subjekt, je ale náročné zisťovať subjekty, ktoré môžu pristupovať k jednotlivým objektom.

Subjekt		
Používateľ 1	Súbor 2: Read, Write	Proces 1: Suspend
Používateľ 2	Súbor 1: Execute	Súbor 3: Read, Write
Používateľ 3	Súbor 1: Read	Súbor 2: Write
Používateľ 4	Súbor 3: Read	

Zoznam povolených prístupov

- Zostavuje maticu riadenia prístupu pomocou stĺpcov, ktoré tvoria zoznam používateľov a ich oprávnení vzťahujúcich sa k chránenému objektu (napr. súbor alebo adresár)
- Každý objekt má nastaviteľné bezpečnostné atribúty, ktoré identifikujú zoznam povolených prístupov pre jednotlivých používateľov
- Základné typy povoleného prístupu sú možnosti čítania, zápisu, vytvorenia, modifikácie, zmazania alebo spustenia (aplikácie).

Objekt		
Súbor 1	Používateľ 2: Execute	Používateľ 3: Read
Súbor 2	Používateľ 1: Read, Write	Používateľ 3: Write
Súbor 3	Používateľ 2: Read, Write	Používateľ 4: Read
Proces 1	Používateľ 1: Suspend	

Mechanizmus atribútov

- Je podobný ako v prípade zoznamu povolených prístupov, rozdiel je v tom, že namiesto spájania používateľov s operáciami sú atribúty spájané s objektmi.
- Delí používateľov do troch skupín (vlastník súboru, skupina a ostatní používatelia). Prístupový systém reguluje prístup k súborom pomocou atribútov: čítanie (r), zápis (w) alebo spúšťanie operácie (x).
- Operačné systémy založené na Unix-e historicky využívajú (aj) tento mechanizmus.

Bezpečnostné modely

- Na pomoc pri tvorbe viacúrovňových bezpečnostných systémov bolo vytvorených niekoľko bezpečnostných modelov.

- Medzi tieto bezpečnostné modely patria:
  - Bell-LaPadula model,
  - Biba model,
  - Clark-Wilson model.

Bell-LaPadula model

- Postavený na konceptoch stavov v systéme.
- Hlavné zameranie je zabezpečenie dôvernosti, naopak vôbec neodráža požiadavky na zabezpečenie integrity.
- BLP definuje bezpečný stav prostredníctvom troch vlastností:
  - Simple Security Property – znamená, že čítanie informácií subjektom na nižšej úrovni z objektu na vyššej úrovni nie je dovolené,
  - *property („hviezdička“ property) – znamená, že zápis informácií subjektom na vyššej úrovni do objektu na nižšej úrovni nie je dovolený („no write down“),
  - Discretionary Security property – používa prístupovú maticu na špecifikovanie DAC
- „No write down“ princíp zabraňuje umiestneniu dát, ktoré nie sú citlivé, ale sú umiestnené v citlivom dokumente, do menej citlivého súboru.

Biba model

- Model špecifikuje dve základné axiómy súvisiace s integritou (v porovnaní s BLP má pravidlá stanovené opačne):
  - Simple integrity axiom (axióma jednoduchej integrity) – znamená, že subjekt na jednej úrovni integrity nemá dovolené čítať objekt na nižšej úrovni integrity (no read down),
  - *Integrity axiom – znamená, že objekt na jednej úrovni integrity nemá dovolené modifikovať (write to) objekty na vyššej úrovni integrity (no write up). Napr. ak proces môže zapísať dáta nad svoju bezpečnostnú úroveň, môžu byť dôveryhodné dáta znehodnotené práve pridaním menej dôveryhodných dát.

Clark-Wilson model

- Model identifikuje tri pravidlá integrity:
  - neautorizovaní používatelia by nemali robiť žiadne zmeny,
  - systém by mal udžiavať vnútornú a vonkajšia konzistenciu,
  - autorizovaní používatelia by nemali vykonávať neautorizované zmeny.

- V modely sú na vynútenie integrity používané dva mechanizmy:
  - Vhodne vytvorené transakcie – dáta alebo dátový proces môžu byť zmenené iba špecifickou sadou dôveryhodných programov. Používatelia majú potom prístup k týmto programom a nie priamo k dátam.
  - Oddelenie povinností – v prípade manipulácie s dátami alebo pokusom o prienik do systému sú používatelia nútení spolupracovať z dôvodu rozdelenia právomocí a povinností medzia viacerých používateľov.

Ďalšie princípy

- V závislosti od špecifík organizácie, procesov, využívaných systémov, ...
- Minimalizácia rizík na rôznych úrovniach.
- Oddeľovanie povinností , rotácia povinností, oddeľovanie sietí...

Identifikácia a autentizácia

- Pod identifikáciou rozumieme proces, ktorým používateľ poskytuje svoju identitu do systému (napr. zadá prihlasovacie meno).
- Autentizácia znamená overenie (potvrdenie) identity, ktorú používateľ poskytol (napr. v rámci autentizácie zadá heslo).
- Proces autentizácie má niekoľko prvkov, ktoré si vyžadujú separátne zabezpečenie. Ide najmä o zadávanie a prenos autentizačných údajov, rozpoznanie používateľa, ktorý sa autentizoval, používateľa, ktorý so systémom pracuje (používateľ sa môže prihlásiť, odísť od PC a jeho miesto zaujme niekto iný, pričom systém stále akceptuje identitu predchádzajúceho používateľa).

Základné mechanizmy I&A používateľov

- Vo všeobecnosti sa využívajú tri základné mechanizmy I&A používateľov (alebo ich kombinácia) založené na:
  - niečom, čo používateľ *vie* (napr. heslo, PIN),
  - niečom, čo používateľ *má* (token – čipová karta, generátor jednorazových hesiel, klientsky certifikát),
  - niečom, čo používateľ *je* (biometrické charakteristiky ako odtlačok prsta, rozpoznávanie vlastností dúhovky, dynamika podpisu).
- Tzv. jednofaktorová autentizácia používa iba jednu z týchto troch foriem overovania, zatiaľ čo dvojfaktorová autentizácia používa kombináciu dvoch foriem a trojfaktorová autentizácia používa všetky tri formy.
- V praxi sú s každým z týchto mechanizmov spojené nároky, ktoré si často vzájomné odporujú (pohodlnosť použitia, chybovosť, finančná nákladnosť, spoľahlivosť, nenáročná administrácia).

I&A založená na niečom, čo používateľ vie

- Najčastejšia forma identifikácie a autentizácie založená na prihlasovacom mene a súvisiacom hesle.
- Formy hesiel:
  - tajná informácia (typicky reťazec znakov)
  - osobné identifikačné číslo (PIN)
  - fráza (pomerne dlhé heslo pozostávajúce z radu slov alebo úplnej vety)
- Jednoduché frázy ako "mamraddobrejedlo" sú predvídateľné, a preto pre útočníka ľahšie uhádnuteľné heslo ako "9j% # F.0", takže dĺžka hesla sama o sebe neznamená silnejšie heslo.

Problémy hesiel

- Odhalenie hesla v praxi môže spôsobiť získanie neoprávneného prístupu k viacerým systémom a aplikáciám súčasne (pri používaní tzv. single sign-on systémov).
- Slabým miestom hesiel je, že ich bezpečnosť je založené na uchovávaní hesla v tajnosti.
- Hádanie hesiel, odchytávanie hesiel, odpozorovanie hesiel, útoky hrubou silou, tzv. man-in-the-middle útoky, sociálne inžinierstvo ...

Centralizované nástroje pre správu identít a hesiel

- Zníženie počtu identifikátorov používateľských účtov a hesiel, ktoré si používatelia potrebujú pamätať.
- Single sign-on (SSO) technológia umožňuje používateľovi overiť svoju identitu (autentizovať sa) iba raz a následne získať prístup ku všetkým zdrojom, ktoré je používateľ oprávnený používať.
- SSO automatizovane vytvorí jedinečné silné heslo pre každý zdroj a pravidelne heslá mení. Používateľ obvykle pozná iba základné heslo SSO.

Adresárové služby

- Adresár (directory) je hierarchická štruktúra, v ktorej sú uložené informácie o pomenovaných objektoch, ktoré sú organizované a združované do skupín. Týmto objektom môže byť počítač, tlačiareň, služba, doména či používateľský účet.
- Adresárová služba je špecializovaná aplikácia pre prácu s údajmi vo forme adresárov – ich ukladanie, organizáciu a prístup k nim. Príkladom sú aplikácie na správu používateľov, sieťových zdrojov či telefónny zoznam.
- Adresárová služba môže byť súčasťou operačného systému, ale aj mať formu samostatnej aplikácie. Najrozšírenejším príkladom adresárovej služby je Active Directory (Microsoft). Active Directory, tak ako väčšina súčasných adresárových služieb, využíva protokol LDAP.

LDAP (Lightweight Directory Access Protocol)

- Postavený na klient/server architektúre a komunikuje prostredníctvom protokolu TCP/IP
- Základná schéma komunikácie je nasledujúca:
  1. Klient naviaže spojenie s LDAP serverom. Môže sa pripojiť anonymne alebo musí preukázať svoju identitu – vykoná sa autentizácia jednou z definovaných metód. Na naviazanie spojenia musí klient poznať IP adresu a port LDAP servera.
  2. Klient má k dispozícii spojenie na server a môže v rámci neho posielať žiadosti o vykonanie definovaných operácií nad adresárovými údajmi.
  3. Klient uzatvorí spojenie s LDAP serverom.
- Z hľadiska bezpečnosti sú v rámci protokolu LDAP riešené najmä autentizácia a autorizácia používateľa a zabezpečenie komunikácie.
- Praktickou výhodou LDAP autentizácie je možnosť jej využitia ako SSO.

Active Directory

- Adresárové údaje v AD obsahujú najmä informácie o:
  - používateľských účtoch,
  - zdieľaných prostriedkoch,
  - organizačných jednotkách,
  - stanovených politikách a pravidlách.
- Autentizácia pomocou AD je v praxi väčšinou využívaná ako SSO a umožňuje tak používateľom prístup ku viacerým zdrojom bez opätovnej autentizácie.
- AD podporuje viacero autentizačných mechanizmov, ako napr. Kerberos, NTLM, PKI certifikáty, SSL/TLS. V procese autorizácie podporuje AD na riadenie prístupu používateľov model RBAC.

I&A založená na niečom, čo používateľ má

- Kombinácia niečoho „čo viem“ s niečím „čo mám“ poskytuje podstatne silnejšiu úroveň bezpečnosti ako jednotlivé metódy využité samostatne.
- Predmety, ktoré používateľ vlastní pre použitie v I&A sa nazývajú tokeny. Existujú dve základné kategórie tokenov:
  - pamäťové tokeny
  - inteligentné (smart) tokeny.

Pamäťové tokeny

- Slúžia na ukladanie informácie, nie však na jej spracúvanie (napr. karta s magnetickým pásikom).
- Na zápis a čítanie informácií z/do pamäťových tokenov môžu byť potrebné špecializované zariadenia.
- Výhodou pamäťových tokenov (ak sa používajú v kombinácii s PINom) je podstatne vyššia úroveň bezpečnosti ako pri použití hesiel (získanie tokenu aj PINu je oveľa obtiažnejsie ako získanie používateľského mena a hesla).
- Ďalšou výhodou pamäťových tokenov je, že v čase môžu byť použité iba na jednom mieste.

Pamäťové tokeny - obmedzenia

- Voči pamäťovým tokenom existuje množstvo útokov, ktorých podstatou je najmä replikácia tokenu (resp. údajov na ňom uložených) alebo kompromitácia PINu
- Nutnosť špeciálneho zariadenia (čítačky). Čítačka musí obsahovať jednak časť, ktorá prečíta informáciu z tokenu, ako aj komponent, prostredníctvom ktorého sa dá zadať a overiť PIN.
- Strata tokenu. V prípade straty používateľ stráca možnosť autentizácie (a teda aj prístupu do systémov) dovtedy, kým nedostane nový token. Stratený token môže byť niekým zneužitý na neoprávnený prístup do systému alebo trvalo odcudzený, prípadne replikovaný a vrátený späť oprávnenému používateľovi.

Inteligentné (smart) tokeny

- Rozširujú možnosti pamäťových tokenov využitím inteligentného čipu (integrovaného obvodu) zabudovaného priamo do tokenu (token môže sám vykonať určité operácie s údajmi, ktoré sú v ňom uložené).
- Charakteristiky:
  - *Fyzický vzhľad*. Smart tokeny môžu byť smart karty (napr. platobná karta s čipom) alebo môžu vyzerať ako malé kalkulačky, USB kľúče. Smart tokenom môže byť aj mobilný telefón, v ktorom je nainštalovaná špeciálna aplikácia.
  - *Rozhranie*. Smart tokeny majú manuálne alebo elektronické rozhranie. Manuálne rozhranie zvyčajne obsahuje malú klávesnicu, prostredníctvom ktorej používateľ používa token a zobrazí kód, ktorý používateľ v procese autentizácie zadáva. Elektronické rozhranie majú napr. čipové karty.
  - *Protokol*. Smart tokeny majú k dispozícii množstvo protokolov, ktoré môžu využiť na proces autentizácie. Vo všeobecnosti sa využívajú najmä 3 základné kategórie: výmena statického hesla, generátory dynamických hesiel a systém výzva-odozva.

Inteligentné (smart) tokeny

- Výhody:
  - Všeobecne platí, že poskytujú väčšie zabezpečenie ako pamäťové tokeny.
  - Poskytujú značnú flexibilitu a môžu byť použité na riešenie mnohých problémov autentizácie.
  - Pamäť na čipe smart tokenu nie je čitateľná, pokiaľ sa nezadá PIN.
  - Smart tokeny s elektronickými rozhraniami, ako sú napr. čipové karty, poskytujú spôsob, ako pre používateľa zaistiť prístup k viacerým počítačom, systémom a aplikáciám pomocou jediného procesu prihlásenia sa.
  - Jedna čipová karta môže byť použitá na viac účelov (fyzický prístup, prihlasovanie sa do PC, evidencia dochádzky).
- Nevýhody
  - Pri smart tokenoch sa väčšina problémov týka nákladov na správu celého systému a používateľských požiadaviek a pohodlia pri práci / väčšia cena.

I&A založená na niečom, čo používateľ je

- Biometrické autentizačné technológie využívajú jedinečné vlastnosti (atribúty) osoby za účelom určenia a overenia jej identity. Zahŕňajú:
  - fyziologické atribúty (napr. odtlačky prstov, rúk, geometria dlane, vzory sietnice)
  - behaviorálne atribúty (napr. hlasové vzorky, vlastnoručné podpisy).
- Biometrické overenie môže byť technicky zložité a nákladné, pričom akceptácia jeho využívania používateľmi môže byť problematická.
- V závislosti od konkrétneho využívaného atribútu však v praxi môže byť dostatočne spoľahlivé s akceptovateľnými finančnými nákladmi a používateľsky komfortné.

Biometrická autentizácia

- Vo všeobecnosti funguje nasledovne:
  - pred prvým pokusom o autentizáciu musí používateľ vytvoriť a uložiť referenčný profil / šablónu (na základe atribútu, ktorý sa v autentizácií bude používať, napr. zosníma a uloží odtlačok palca). Výsledná šablóna je spojená s identitou používateľa a zaznamenaná pre neskoršie použitie.
  - pri pokuse o autentizáciu používateľa sa zosníma príslušný biometrický atribút (napr. odtlačok palca). Zosnímaný atribút sa porovná s atribútom uloženým v šablóne a na základe výsledku porovnania sa používateľ akceptuje alebo odmietne.
- Nedostatky v biometrickej autentizácii vyplývajú z technických ťažkostí pri meraní a profilovaní fyzikálnych vlastností ľudí, ako aj z ich premenného charakteru (môžu sa meniť v závislosti na rôznych podmienkach).
- Vzhľadom na ich relatívne vysoké náklady sú biometrické systémy obvykle používané v kombinácii s inými metódami overovania najmä v prostrediach vyžadujúcich vysokú bezpečnosť.

Výkonnosť a použiteľnosť biometrických autentizačných zariadení

- Počet chybných odmietnutí (FRR) čo znamená, koľkokrát je oprávnená osoba pri autentizácii nesprávne odmietnutá systémom.
- Počet chybne akceptovaných autentizácií (FAR), kedy biometrický systém akceptuje aj neoprávneného používateľa.
- Každý systém môže byť konfigurovateľný tak, že hodnoty FRR a FAR sa menia (zníženie jedného parametra spôsobí zvýšenie druhého a naopak).
- Biometrické autentizačné technológie využívajú osobné údaje, ktorých použitie je upravené zákonmi. Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov chápe pod biometrickým údajom „osobný údaj fyzickej osoby označujúci jej biologickú alebo fyziologickú vlastnosť alebo charakteristiku, na základe ktorej je jednoznačne a nezameniteľne určiteľná; biometrickým údajom je najmä odtlačok prsta, odtlačok dlane, analýza deoxyribonukleovej kyseliny“.

Vzdialený prístup

- Dnešné organizácie vyžadujú pripojenie vzdialeným prístupom (prístup „zvonka“) k ich informačným zdrojom pre rôzne typy používateľov, ako sú zamestnanci, dodávatelia, občania, partneri alebo zákazníci. Pri poskytovaní tejto možnosti prístupu je k dispozícii množstvo metód a postupov ako túto formu prístupu riadiť.
- Často využívaná metóda vzdialeného prístupu je založená na platforme protokolov TCP/IP (vytvorí sa VPN spojenie cez internet, ktoré zaistí bezpečnosť komunikácie v prostredí verejnej siete).
- Výhodou tejto metódy vzdialeného prístupu je jej široká dostupnosť, ľahkosť použitia, finančne nenáročné spojenie a možnosti riadenia prístupu. Nevýhodou je relatívne nižšia spoľahlivosť (v porovnaní s vyhradenými linkami) a potenciálne komplikované riešenie prípadných problémov počas prevádzky.

Vzdialený prístup - bezpečnosť

- Umožnenie vzdialeného prístupu môže znížiť bezpečnosť vnútornej infraštruktúry organizácie (šifrovaná komunikácia môže v sebe obsahovať škodlivý kód alebo závadný softvér; systémy na detekciu prienikov a antivírusové programy takúto komunikáciu bežne nemôžu kontrolovať).
- Odporúča sa všetky VPN spojenia ukončiť vždy v jednom bode (VPN koncentrátor) a zvážiť nasadenie nástrojov, ktoré dokážu dešifrovať prebiehajúcu komunikáciu, zaistiť jej analýzu a následne ju opäť zašifrovať.

Vzdialený prístup - riziká

- Riziká vzdialeného prístupu zahŕňajú:
  - odopretie služby, kedy vzdialení používatelia nebudú schopní získať prístup k dátam alebo aplikáciám, ktoré sú dôležité pre ich pracovné aktivity,
  - pokusy o neoprávnený prístup používateľov a tretích strán, ktoré sa môžu snažiť získať vzdialený prístup zneužitím bezpečnostných nedostatkov sieťových protokolov alebo sociálnym inžinierstvom,
  - nesprávne nastavený komunikačný softvér, čo môže mať za následok nesprávne nastavené prístupové oprávnenia k systémom a dátam organizácie,
  - nesprávne konfiguračné nastavenia zariadení v internej počítačovej sieti organizácie,
  - nedostatočné zabezpečenie hostiteľských systémov, ktoré tak môžu byť využívané útočníkom získaním prístupu na diaľku.

Vzdialený prístup pomocou mobilných zariadení

- Používanie mobilných zariadení ako PDA (Personal Digital Assistent), tabletu alebo smartfónu je v súčasnosti veľmi rozšírené.
- Súčasné PDA je najčastejšie smartfón alebo tablet, s integrovaným fotoaparátom a možnosťou sieťového prístupu (wi-fi, 3G, Bluetooth).
- V prípade, že PDA je pripojiteľné do internej počítačovej siete alebo synchronizované bez príslušných bezpečnostných opatrení, je riziko neoprávneného prístupu do infraštruktúry organizácie neakceptovateľne vysoké.
- Je dôležité, aby organizácia mala nastavené a zavedené vhodné politiky, procesy a postupy a používatelia si boli plne vedomí svojich zodpovedností pri používaní PDA na pracovne účely (osobitne v prípadoch, kedy sa jedná o súkromné PDA t.j. tie, ktoré nie sú vo vlastníctve organizácie).

Bezpečnosť PDA

- PDA aplikácie – povolené by mali byť iba tie aplikácie, ktoré spĺňajú stanovené organizačné smernice alebo sú štandardom výrobcu dodávaného zariadenia.
- Synchronizácia - PDA by mali byť zálohované a pravidelne softvérovo aktualizované. Informácie na PDA by mali byť synchronizované s dátovými zdrojmi na notebooku a / alebo PC. Vzdialený prístup k infraštruktúre organizácie by mal byť umožnený iba schválenými metódami a nástrojmi a mechanizmami pre synchronizáciu.
- Detekcie vírusov a ochrana - hrozby spojené s počítačovými vírusmi platia rovnako pre PDA ako platia pre notebooky a PC.

Bezpečnosť PDA II.

- Povedomie – vzdelávanie používateľov a budovanie bezpečnostného povedomia by malo zahŕňať aj pokrytie politiky bezpečnosti a využívania PDA.
- Súlad - PDA a ich využívanie musí byť v súlade s bezpečnostnými požiadavkami, tak ako sú definované v štandardoch a interných predpisoch organizácie. Existujúce politiky definujúce zdroje a IKT komponenty by mali byť rozšírené tak, aby okrem serverov/PC/notebookov zahŕňali aj PDA.
- Starostlivosť - používatelia by mali venovať náležitú starostlivosť o PDA v rámci pracovného prostredia a najmä počas cestovania a služobných ciest. Akákoľvek strata alebo odcudzenie dát z PDA ako aj samotného PDA musí byť považované za bezpečnostný incident.

QAA, STORK a federácia identity

- Riešenie procesov identifikácie a autentizácie je dôležité riesiť aj na nadnárodnej úrovni.
- Cieľom projektu STORK (Secure idenTity acrOss boRders linKed 2.0) je vytvoriť „Európsku platformu interoperability eID“, ktorá umožní obyvateľom členských štátov EÚ komunikovať s úradmi (prípadne s ďalšími poskytovateľmi služieb) naprieč hranicami, na základe preukázania sa svojim národným eID (národným elektronickým identifikačným dokladom).
- Úlohou centrálnej platformy STORK je identifikovať používateľa, ktorý komunikuje s poskytovateľom služby a zasielať mu údaje o používateľovi.
- Poskytovateľ služby môže žiadať o rôzne typy údajov, ale používateľ sám rozhodne, ktoré údaje budú skutočne poskytnuté. Ide o tzv. „na používateľa zameraný“ prístup (user-centric approach) - vždy pred sprístupnením údajov je vyžadovaný explicitný súhlas používateľa.

QAA, STORK a federácia identity

- Dôležitým aspektom autentizácie je tzv. QAA – Quality of Authentication Assurance (miera záruk dosiahnutých autentizáciou).
- Príklad: Pri kontrole občianskeho preukazu sa „autentizácia“, t.j. overenie totožnosti fyzickej osoby, ktorá sa ním preukázala, vykoná vizuálnym porovnaním jej vzhľadu a fotografie umiestnenej na OP. Reálne sa však môže stať, že iná osoba napodobní vzhľad z fotografie, najmä ak fotografia je menej kvalitná, alebo staršia – takto môže dôjsť ku sfalšovaniu identity. Z pohľadu overujúcej osoby (t.j. toho, kto chce zistiť či OP naozaj prináleží určitej osobe) sa preto dá na overenie porovnaním fotografie spoľahnúť iba do určitej miery – táto miera určuje „kvalitu“ overenia.

QAA, STORK a federácia identity

- Stupeň spoľahlivosti autentizácie sa formálne vyjadruje ako miera bezpečnostných záruk, ktoré úspešná autentizácia poskytuje overujúcemu subjektu (v rôznych situáciách je potrebná rôzna úroveň potrebných záruk)
- Z praktických dôvodov nie je vhodné vždy vykonávať autentizáciu s vysokým stupňom záruk (na tento proces je obvykle potrebné veľké množstvo zdrojov, môže byť zdĺhavý alebo obťažujúci – napr. vysoký stupeň záruk pri zisťovaní totožnosti poskytuje porovnanie DNA).
- Pre každú konkrétnu situáciu sa snažíme nájsť minimálny stupeň záruk autentizácie, ktorý však už je dostatočný.

Procesy QAA

- Miera záruk autentizácie závisí od nasledovných procesov:
  - Procesy registračnej fázy
  - Správa autentizačných údajov
  - Výkon autentizácie
- Jednotlivé procesy môžu byť vykonávané rôznymi subjektmi (v príklade s občianskym preukazom za proces registrácie zodpovedá MV SR, správu autentizačných údajov zabezpečuje držiteľ OP a výkon autentizácie overujúci subjekt – vrátnik kontrolujúci totožnosť pri vstupe do budovy).
- Z pohľadu overujúceho subjektu je dôležitý výsledný stupeň záruk, ktorý z veľkej časti závisí od procesov mimo jeho kontroly.

QAA - Procesy registračnej fázy

- Činnosti vykonávané pri vytvorení vzťahu medzi subjektom (o ktorého identitu ide) a garantom autentizačnej schémy (entity stanovujúcej procesy autentizácie, ktorá za ne aj zodpovedá). Najdôležitejšie súvisiace požiadavky:
  - Kvalita registračnej procedúry (mechanizmus, pomocou ktorého sa preukáže „skutočná“ identita subjektu garantovi autentizačnej schémy)
    - **Miera prítomnosti** subjektu (žiadateľa o identitu) - fyzická prítomnosť je považovaná za „najvyššiu“ mieru spoľahlivosti pri komunikácii so subjektom; komunikácia realizovaná medzi dvoma prítomnými osobami je považovaná za autentickú a identita subjektu je potvrdená s istotou (jeho fyzickou existenciou a vnímateľnosťou).
    - **Vierohodnosť údajov** svedčiacich o identite subjektu - za najvyšší stupeň je považované uvedenie takých údajov, ktoré sú unikátne pre subjekt a sú overiteľné v iných systémoch alebo evidenciách (napr. štátom garantované registre).
    - **Overenie vierohodnosti** údajov svedčiacich o identite subjektu - za najvyšší stupeň potvrdenia vierohodnosti údajov je považované ich opatrenie zaručeným elektronickým podpisom.

QAA - Procesy registračnej fázy

- Spoľahlivosť procesu vydania identity
  - Spôsob, akým sa subjektu odovzdajú tokeny preukazujúce identitu a autentizačné údaje alebo predmety. Čím vyšší stupeň záruk tento proces poskytuje, tým s vyššou pravdepodobnosťou je možné predpokladať, že pri doručovaní nedošlo k odcudzeniu identity alebo prezradeniu údajov.
  - V najjednoduchšom prípade doručenie prebehne čisto elektronickou formou bez špecifického zaistenia dôvernosti. Napr. heslo je zaslané na zadanú adresu elektronickej pošty, alebo sú údaje zobrazené na www stránke počas registračného procesu.
  - Najvyšším stupňom bezpečnosti je odovzdanie údajov a predmetov fyzicky prítomnej osobe. Tento prístup je však pre subjekt náročný na čas (najmä ak kvôli vydaniu identity by bolo potrebné „opäť prísť“ za garantom autentizačnej schémy).

QAA - Procesy registračnej fázy

- Spoľahlivosť garanta autentizačnej schémy (musí zaistiť dostatočnú bezpečnosť procesov registrácie a vydania identity, ale musí byť pripravený zaisťovať aj bezpečné uchovávanie údajov o identitách a autentizačné údaje a vykonávať procesy správy celého životného cyklu identít).
- Faktory, na základe ktorých je možné úroveň záruk poskytovanú garantmi
  - formalizácia procesov – vyšší stupeň záruk je možné očakávať od garantov, ktorý procesy súvisiace s prevádzkou autentizačnej schémy realizujú formalizovaným a riadeným spôsobom.
  - úroveň súladu s požiadavkami – na základe zákona, iných právnych predpisov alebo noriem. Spravidla čím vyšší stupeň záruk je potrebné dosiahnuť, tým vyšší stupeň formálneho súladu s požiadavkami je vyžadovaný, až po absolvovanie certifikácie organizácie alebo procesov predpísaným spôsobom.
  - uchovávanie záznamov – miera tvorby a uchovávania záznamov výrazným spôsobom ovplyvňuje možnosť riešenia neskorších problémov zo strany garanta.

QAA - Správa autentizačných údajov

- Bezpečnosť v tejto etape spoločne zaisťujú:
  - garant autentizačnej schémy – povinnosťou garanta je uchrániť dátové zdroje obsahujúce identity a údaje potrebné pre overenie autentizácie pred kompromitáciou či už z hľadiska ochrany dôvernosti alebo integrity (napr. aby nedošlo k neoprávnenému vloženiu novej identity).
  - autentizovaný subjekt – hlavnou povinnosťou je zaistiť bezpečné uchovanie autentizačných údajov a predmetov tak, aby nedošlo k ich odcudzeniu alebo zneužitiu. Subjekt musí rešpektovať stanovené bezpečnostné požiadavky v závislosti od požadovaného stupňa spoľahlivosti autentizácie (napr. iný stupeň ochrany pred odcudzením je potrebný pre prístupové kódy k počítačovej hre, iný pre autentizačné údaje do systémov verejnej správy).
- Vzhľadom na vznik integrujúcich technológií (napr. SSO, federácia identity, eID) vzniká častokrát predstava, že v cieľovom stave bude používateľ držiteľom iba „jednej sady“ identifikačných a autentizačných údajov, pomocou ktorých sa „prihlási všade“.

QAA – Výkon autentizácie

- Robustnosť autentizačnej metódy (voľba konkrétnej autentizačnej metódy priamo ovplyvňuje odolnosť voči útokom na prelomenie autentizačnej schémy, možnosť uhádnutia autentizačných údajov, ale aj možnosť ich odcudzenia).
- Bezpečnosť implementácie autentizačného mechanizmu (ak softvérová aplikácia, pomocou ktorej je autentizácia vykonávaná, obsahuje bezpečnostné slabiny, výsledná úroveň záruk takejto schémy nemôže byť vysoká).
- Prostredie výkonu autentizácie - prostredie, v ktorom používateľ pristupuje ku službe / kde je vykonávaná autentizácia, môže mať zásadný vplyv na výslednú mieru záruk tohto procesu. Ak má útočník kontrolu nad zariadením, s ktorým používateľ pracuje -> má prístup ku všetkým údajom, ktoré používateľ zadá ku všetkým službám, kde sa používateľ autentizuje.

QAA – Výkon autentizácie

- Pri autentizácii platí pravidlo, podľa ktorého bezpečnosť celku nemôže byť vyššia ako bezpečnosť jeho najslabšieho článku. Nemá zmysel realizovať určité procesy autentizácie na vysokom stupni bezpečnosti, ak iné (súvisiace) procesy poskytujú iba nižšiu mieru záruk.
- Zmysluplné je realizovať autentizačné schémy tak, aby vo všetkých súvisiacich procesoch bola dosahovaná konzistentná úroveň záruk bezpečnosti.
- V praxi sú preto pre určitú požadovanú úroveň záruk štandardizované konkrétne požiadavky na jednotlivé procesy

Schéma pre QAA úrovne v rámci projektu STORK

		Assurance Levels for Electronic Authentication phase			
		EA1	EA2	EA3	EA4
Assurance Levels for Registration phase	RP1	STORK QAA Level 1	STORK QAA Level 1	STORK QAA Level 1	STORK QAA Level 1
	RP2	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 2	STORK QAA Level 2
	RP3	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 3	STORK QAA Level 3
	RP4	STORK QAA Level 1	STORK QAA Level 2	STORK QAA Level 3	STORK QAA Level 4

Klasifikácia vyžadovaných záruk autentizácie - návrh elektronických služieb verejnej správy SR

- Pre každú službu je povinne stanovená hodnota v rozsahu 1 až 4 reprezentujúca úroveň zabezpečenia autentizácie v nadväznosti na bezpečnosť identifikátora, autentizačných nástrojov a bezpečnosti doručenia autentizačných prostriedkov. Môže nadobúdať hodnoty:
  - úroveň 1 - s minimálnym zabezpečením autentizácie,
  - úroveň 2 - s nízkym zabezpečením autentizácie,
  - úroveň 3 - s významným zabezpečením autentizácie,
  - úroveň 4 - s najvyšším zabezpečením autentizácie.

Federácia identity

- Koncept, ktorého cieľom je umožniť využívanie častí systému správy identít čo najširšiemu okruhu aplikácií, a to aj mimo primárnu doménu tohto systému.
- Federácia identít umožní používateľovi používať určitú identitu v mnohých aplikáciách a kontextoch, pričom procesy jej správy zostanú zachované. „Z pohľadu“ webového prehliadača ide o určitú formu SSO.
- Koncept federácie identity sa v súčasnom období rozmáha najmä z nasledovných dôvodov:
  - používateľ pristupuje k množstvu služieb/aplikácií (napr. podľa prieskumov v UK priemerný používateľ k viac ako 20), avšak chce pri prístupe využívať čo najmenej identít,
  - prostredníctvom internetu dochádza k zásadnému zvýšeniu prepojiteľnosti aplikácií,
  - používané procesy správy identít sú pre väčšinu aplikácií štandardizované, čo umožňuje jednoduchšie prepojenie.

Federácia identity

- Pri riešení federácie identity je potrebné riešiť najmä nasledovné :
  - otvorenosť – nakoľko správca identít umožní ďalším subjektom využívať v ich systémoch identity a procesy, ktoré sám zabezpečuje; federácia identity je používaná aj v uzavretých systémoch (na základe dohody účastníkov, ktorá môže zahŕňať aj odplatu za jednotlivé služby spojené so správou identít), ale najmä v otvorených systémoch, kde je možný voľný prístup k určitým službám.
  - interoperabilita – ako je technologicky náročné vytvoriť prepojenia medzi správcom identít a poskytovateľmi služieb využívajúcimi federáciu identity; táto otázka je dôležitá najmä z pohľadu poskytovateľov služieb, ktorí chcú umožniť vo svojich aplikáciách využívanie identít od mnohých správcov identít.
  - dôvera – nakoľko sa správca služby môže spoľahnúť na spoľahlivosť identity a súvisiacich procesov; tu je možné do parametrov odovzdávaných o identite zahrnúť aj štandardizované vyjadrenie miery záruk spoľahlivosti identity a autentizácie podľa dohodnutej schémy QAA.

Riadenie prístupu z pohľadu prevádzky a jeho administrácia

- Administrácia riadenia prístupu
  - Centralizované riadenie prístupu
  - Decentralizované riadenie prístupu
- Požiadavky na riadenie prístupu v organizácii
  - Politika riadenia prístupu
  - Riadenie prístupu používateľov
  - Zodpovednosti používateľov
  - Riadenie prístupu k sieti
  - Riadenie prístupu k operačnému systému
  - Riadenie prístupu k aplikáciám a informáciám
  - Mobilné výpočtové zariadenia a práca na diaľku

Administrácia riadenia prístupu

- Administrácia riadenia prístupu je dôležitou súčasťou systému autentizácie a autorizácie v organizácii a preto patrí medzi kritické procesy.
- To, či je systém riadenia prístupu implementovaný ako centralizovaný alebo decentralizovaný je závislé na tom, čo sa organizácia snaží dosiahnuť vo svojich bezpečnostných cieľoch.
- Centralizované riadenie prístupu (Radius,Tacacs+),
- Decentralizované riadenie prístupu.

Centralizované riadenie prístupu

- Za poskytovanie (nastavovanie) prístupu ku zdrojom organizácie pre jednotlivých používateľov zodpovedná práve jedna entita (oddelenie alebo konkrétna osoba)
- Výhody:
  - dôsledná a jednotná metóda riadenia prístupov používateľov a prístupových oprávnení,
  - škálovateľné riešenie.
- Príklady technológií centralizovaného riadenia prístupov:
  - RADIUS (Remote Authentication Dial-In User Service) – klient/server protokol a softvér, ktorý umožňuje komunikovať s centrálnym serverom za účelom autentizácie vzdialene pripojených používateľov a autorizácie ich prístupu k požadovaným systémom.
  - TACACS+ (Terminal Access Controller Access Control System Plus) – autentizačný protokol, ktorý umožňuje RAS poskytnúť používateľské prihlasovacie poverenia (credentials) autentizačnému serveru. TACACS je nešifrovaný protokol, a tým pádom menej bezpečný ako neskoršie vyvinuté protokoly TACACS+ a RADIUS.

Protokol RADIUS

- Bezpečný prenos autentizačných, autorizačných a evidenčných informácií medzi serverom so sieťovým prístupom, požadujúcim autentizáciu svojich spojení a zdieľaným autentizačným serverom.
- RADIUS je otvorený protokol a je šírený aj priamo v zdrojovom kóde. Môže byť prispôsobený tak, aby spolupracoval s akýmkoľvek bezpečnostným systémom, ktorý je k dispozícii.
- Základné vlastnosti protokolu RADIUS:
  - používa model klient/server,
  - transakcie medzi klientom a serverom sú autentizované prostredníctvom zdieľaného hesla,
  - šifrované je iba heslo,
  - používa vyspelé metódy a operácie súvisiace s účtovateľnosťou.

TACACS+

- Klient/server protokol určený na správu autentizácie, autorizácie a účtovateľnosti,prakticky implementovaný v zariadeniach rôznych výrobcov.
- Autorizácia môže byť uskutočňovaná pre jednotlivých používateľov alebo skupinu a je dynamická. Používateľské heslá sú spravované v centrálnej databáze, ktorá poskytuje jednoducho škálovateľné riešenie zabezpečenia siete.
- TACACS+ protokol má nasledujúce atribúty:
  - využíva mechanizmus dvojfaktorovej autentizácie hesla,
  - používatelia majú možnosť zmeniť si heslo,
  - šifruje celkový obsah,
  - služby tohto protokolu môžu byť dodávané ako súčasť operačného systému sieťových zariadení.

Decentralizované riadenie prístupu

- Používatelia tesnejšie „zviazaní“ s možnosťami riadenia prístupu.
- Riadenie prístupu k zdrojom si spravujú samotní vlastníci alebo tvorcovia zdrojov (napr. súborov).
- Prístup poskytuje väčšiu flexibilitu pre jednotlivých administrátorov, ale prináša zároveň menej dôslednu implementáciu politiky riadenia prístupov.
- Príkladom je tzv. doména – sada objektov a subjektov, ktoré majú stanovené prístupové práva k definovaným operáciám. Domény a vťahy medzi nimi sú založené na dôvere, ale vzťahy založené na dôvere môžu byť často kompromitované, pokiaľ nie sú prijaté adekvátne opatrenia. Každá bezpečnostná doména je rozdielna, pretože ich riadia rozdielne politiky a manažment.

Požiadavky na riadenie prístupu v organizácii

- Okruhy podľa normy ISO/IEC 27002
- Požiadavky na riadenie prístupu sú rozdelené do nasledujúcich oblastí:
  - politika riadenia prístupu,
  - riadenie prístupu používateľov,
  - zodpovednosti používateľov,
  - riadenie prístupu ku sieti,
  - riadenie prístupu k operačným systémom,
  - riadenie prístupu k aplikáciám a informáciám,
  - mobilné výpočtové zariadenia a práca na diaľku.

Politika riadenia prístupu

- Politika riadenia prístupu by mala brať do úvahy najmä nasledujúce :
  - bezpečnostné požiadavky jednotlivých aplikácií a systémov organizácie,
  - identifikáciu všetkých informácií vo vzťahu k jednotlivým aplikáciám a rizikám, ktorým sú informácie vystavené,
  - pravidlá pre šírenie informácií a pravidlá schvaľovania,
  - konzistenciu prístupových pravidiel a klasifikáciu informácií pre rôzne systémy a siete,
  - legislatívu a zmluvné záväzky vo vzťahu k ochrane prístupu k dátam alebo službám,
  - štandardné prístupové profily používateľov pre bežné kategórie činností,
  - riadenie prístupových pravidiel v distribuovanom a sieťovom prostredí rozoznávajúc všetky možné typy pripojení,
  - oddelenie jednotlivých rolí pre riadenie prístupu, napr. vybavovanie požiadaviek na prístup, schvaľovanie prístupu, správa prístupov,
  - požiadavky na formálne schválenie žiadosti o prístup,
  - požiadavky na pravidelné preskúmavanie prístupových práv,
  - odoberanie prístupových práv.

Riadenie prístupu používateľov

- Cieľom je zaistiť oprávnený prístup používateľov a predchádzať neoprávnenému prístupu k informačným systémom organizácie.
- Registrácia používateľa (formálne postupy pre registráciu používateľov vrátane jej zrušenia, ktorých úlohou je zabezpečiť autorizovaný prístup ku všetkým viacpoužívateľským informačným systémom a službám).
- Riadenie privilegovaného prístupu (udržiavanie popisu privilégií spojených s každým prvkom systému (napr. s OS, databázovým systémom, aplikáciami) a kategórie zamestnancov, ktorým by mali byť privilégiá pridelené).
- Správa používateľských hesiel (okrem hesiel je potrebné zvážiť aj použitie iných technológií autentizácie a identifikácie používateľa ako je napríklad biometria (napr. odtlačok prsta, očnej rohovky), elektronický podpis alebo použitie technických prostriedkov (napr. čipových kariet).
- Preskúmavanie prístupových oprávnení používateľa.

Zodpovednosti používateľov

- Používatelia by si mali byť vedomí zodpovednosti za dodržiavanie nasadených opatrení kontroly prístupu ku zdrojom organizácie, hlavne s ohľadom na používanie hesiel a bezpečnosti im pridelených prostriedkov a zariadení.
- Používanie hesiel (je potrebné definovať postupy a procedúry súvisiace s používaním hesiel, tvorbou hesiel a ich zaznamenávaním, s intervalmi zmeny hesiel (pravidelné, pri náznaku kompromitácie systému) a pod.).
- Neobsluhované používateľské zariadenia (používatelia a dodávatelia majú byť oboznámení s bezpečnostnými požiadavkami a postupmi pre primeranú ochranu neobsluhovaných zariadení).
- Politika čistého stola a čistej obrazovky (na každom pracovisku sa spravidla pohybuje viacero osôb, čo pre voľne uložené aktíva a citlivé informácie predstavuje výrazné riziko).

Riadenie prístupu k sieti

- Politika používania sieťových služieb.
- Používatelia by mali mať priamy prístup iba k tým sieťovým službám, pre ktorých použitie boli oprávnení. Neoprávnené alebo nezabezpečené pripojenie k sieťovým službám môže mať vplyv na celú organizáciu. Opatrenia sú potrebné najmä pri sieťových pripojeniach k citlivým alebo kritickým aplikáciám organizácie či pri používateľoch pripájajúcich sa z rizikových lokalít.
- Politika formulovaná vo vzťahu k sieťam a sieťovým službám by mala pokrývať autorizačné postupy určujúce, kto je oprávnený pristupovať k akým sieťam a sieťovým službám, kontrolné mechanizmy a postupy na ochranu prístupu k sieťovým pripojeniam a službám prípadne udelené výnimky prístupu.

Riadenie prístupu k sieti II.

- Autentizácia používateľa externého pripojenia.
- Prístup vzdialených používateľov by mal byť autentizovaný. Táto autentizácia môže byť zabezpečená napr. použitím kryptografických techník, autentizačných predmetov (hardware token) alebo protokolom typu výzva/odpoveď. Implementáciu takýchto techník využívajú napr. virtuálne privátne siete – VPN siete.
- Hrozbu predstavuje aj možnosť automatického pripojenia ku vzdialeným počítačom, čo môže mať za následok získanie neoprávneného prístupu k aplikáciám organizácie. Vzdialené pripojenia k počítačovým systémom by mali byť preto vždy autentizované.

Riadenie prístupu k sieti III.

- Identifikácia zariadení v sieťach (pre autentizáciu pripojení z vybraných lokalít a prenosných zariadení odporúča táto norma zvážiť automatickú identifikáciu zariadení).
- Ochrana portov pre vzdialenú diagnostiku a konfiguráciu (fyzický i logický prístup k diagnostickým a konfiguračným portom by mal byť bezpečne riadený).
- Množstvo komunikačných, počítačových a sieťových systémov môže obsahovať prostriedky na vzdialenú konfiguráciu a vzdialený prístup, ktoré využíva personál na údržbu systému. V prípade, že tieto porty nie sú chránené, predstavujú zneužiteľný prostriedok na neautorizovaný prístup do systému.

Riadenie prístupu k sieti IV.

- Princíp oddelenia sietí (oddelenie v sieťach by malo byť založené na klasifikácii ukladaných a spracovávaných informácií, úrovni dôvernosti a type činnosti, ktorými sa organizácia zaoberá tak, aby bol v prípade narušenia služieb minimalizovaný celkový dopad na organizáciu).
- Rozdelenie sietí do separátnych logických domén, inštalácia bezpečnostných brán (firewallov) medzi miesta prepojení sietí, oddelenie s využitím funkčnosti sieťových zariadení a pod.
- Riadenie sieťových spojení (pri zdieľaných sieťach, hlavne pri tých, ktoré presahujú hranice organizácie, by mali byť obmedzené možnosti pripojenia používateľov).
- Riadenie smerovania siete.

Riadenie prístupu k operačnému systému

- Bezpečné postupy prihlásenia (prístup k operačnému systému by mal byť riadený postupmi bezpečného prihlásenia, ktoré by mali byť definované vo vnútorných predpisoch organizácie).
- Identifikácia a autentizácia používateľov (všetci používatelia by mali mať pre svoje výhradné použitie priradený jedinečný identifikátor, mal by byť takisto zvolený vhodný spôsob autentizácie k overeniu ich identity).
- Systém správy hesiel (mal by byť interaktívny a zabezpečovať použitie dostatočne kvalitných hesiel).
- Používanie systémových nástrojov (možnosť použitia systémových nástrojov, ktoré môžu prekonať systémové alebo aplikačné kontroly, by mala byť v každej organizácii obmedzená a kontrolovaná).
- Časové obmedzenie relácie a spojenia.

Riadenie prístupu k aplikáciám a informáciám

- Cieľom je definovať opatrenia, ktorých implementáciou sa bude predchádzať neoprávnenému prístupu k informáciám uloženým v počítačových systémoch. Pre obmedzenie prístupu k týmto systémom by mali byť použité bezpečnostné prostriedky, logický prístup by mal byť obmedzený iba pre oprávnených používateľov.
- Obmedzenie prístupu k informáciám (používatelia aplikačných programov, vrátane pracovníkov podpory, by mali mať prístup k informáciám a funkciám aplikačných systémov obmedzený v súlade s definovanou politikou riadenia prístupu).
- Oddelenie citlivých systémov (citlivé aplikačné systémy by mali byť implementované v oddelených, prípadne izolovaných prostrediach).

Mobilné výpočtové zariadenia a práca na diaľku

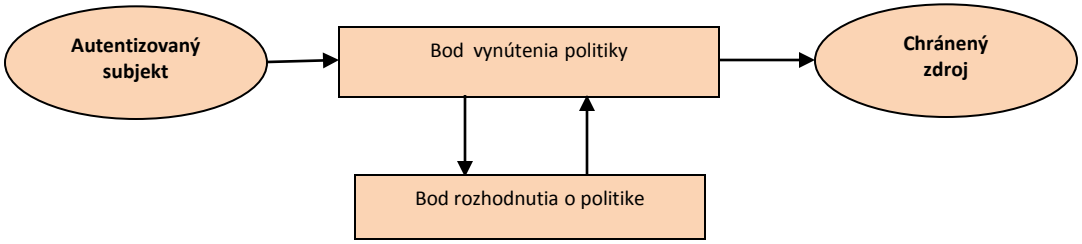
- Mali by byť prijaté formálne pravidlá zohľadňujúce riziká práce s mobilnými výpočtovými zariadeniami, hlavne v nezabezpečenom prostredí (požiadavky na fyzickú ochranu, kontrolu prístupu, kryptografické techniky, zálohovanie či antivírusovú ochranu).
- Odporúčania pre pripájanie týchto zariadení do cudzích sietí, riziko predstavujú najmä bezdrôtové siete a ich známe bezpečnostné slabiny.
- Je dôležité, aby práca na diaľku bola schvaľovaná a kontrolovaná vedúcimi zamestnancami a aby boli zavedené vhodné podmienky pre tento druh práce.

Normalizovaný koncept systému riadenia prístupu

- Podobne ako pri iných systémoch riadenia (napr. pri systéme riadenia informačnej bezpečnosti), aj pre systém riadenia prístupov k informačným zdrojom organizácie je potrebné definovať ucelený rámec komplexne pokrývajúci bezpečnú implementáciu a prevádzku tohto systému.
- Definovanie rámca pre systém riadenia prístupov je aj snahou medzinárodných organizácií ako sú ISO a IEC. V tejto oblasti vyvíjajú medzinárodne akceptovateľnú normu *ISO/IEC 29146 A framework for access management*, ktorá bude problematiku podrobne špecifikovať a určovať najlepšie postupy riadenia prístupov.

Model riadenia prístupu ku zdrojom

- Kroky realizované pri prístupe ku zdrojom organizácie:
  - autentizovaný subjekt (napr. osoba alebo systémový komponent IS) potvrdzuje požiadavku na prístup ku konkrétnemu zdroju,
  - v bode rozhodnutia o politike (angl. Policy decision point) sa overí žiadosť a vydá povolenie na prístup,
  - v bode vynútenia politiky (angl. Policy enforcement point) sa overia prístupové oprávnenia a umožní sa autentizovanému subjektu prístup ku chránenému zdroju.



Zložky systému riadenia prístupov

Norma ISO/IEC 29146 vysvetľuje nasledovné funkčné oblasti systému riadenia prístupov:

- pravidlá pre riadenie privilégií (angl. Policy and Privilege management),
- riadenie autorizačných atribútov (angl. Authorization attribute management),
- autorizácia subjektu,
- priraďovanie zdrojov subjektom (angl. Provisioning),
- monitorovanie a sledovateľnosť vykonaných činností (angl. Monitoring, accountability and traceability).

Zložky systému riadenia prístupov II.

- Pravidlá pre riadenie privilégií (proces tvorby, správy, prideľovania a odoberania privilégií konkrétnym subjektom).
- Privilégiá by mali byť špecifické pre:
  - jednotlivé subjekty a autorizačné atribúty,
  - konkrétne zdroje alebo triedu zdrojov,
  - spôsob použitia zdrojov.
- Riadenie privilégií pozostáva z nasledovných aktivít:
  - definovanie pravidiel a privilégií na prístup ku zdrojom,
  - definovanie pravidiel a privilégií pre PDP prípadne definovanie atribútov pre manažment identít,
  - aktualizácia, prehodnotenie, prípadne zrušenie konkrétnych pravidiel a privilégií,
  - uplatňovanie pravidiel a privilégií v procese overovania požiadaviek na prístup ku zdrojom organizácie.

Zložky systému riadenia prístupov III.

- Riadenie autorizačných atribútov (zahŕňa priraďovanie, modifikáciu a odoberanie týchto atribútov jednotlivým subjektom).
  - konkrétnymi atribútmi pre subjekt môžu byť napr. vek, pozícia, členstvo v skupinách, funkcia či certifikát. Pre zdroj môžu byť týmito atribútmi rôzne typy klasifikácie, adresa či certifikovaná značka (napr. vlastníctvo sieťového identifikátora).
- Autorizácia subjektu vykonávaná v súlade s pravidlami, ktoré by mali špecifikovať:
  - entity, ktoré určujú autorizačné postupy,
  - entity, ktoré uskutočňujú on-line autorizáciu,
  - procedúry, ktoré vykonávajú off-line autentizáciu,
  - úroveň zabezpečenia vyžadovanej pri autentizácii subjektu.

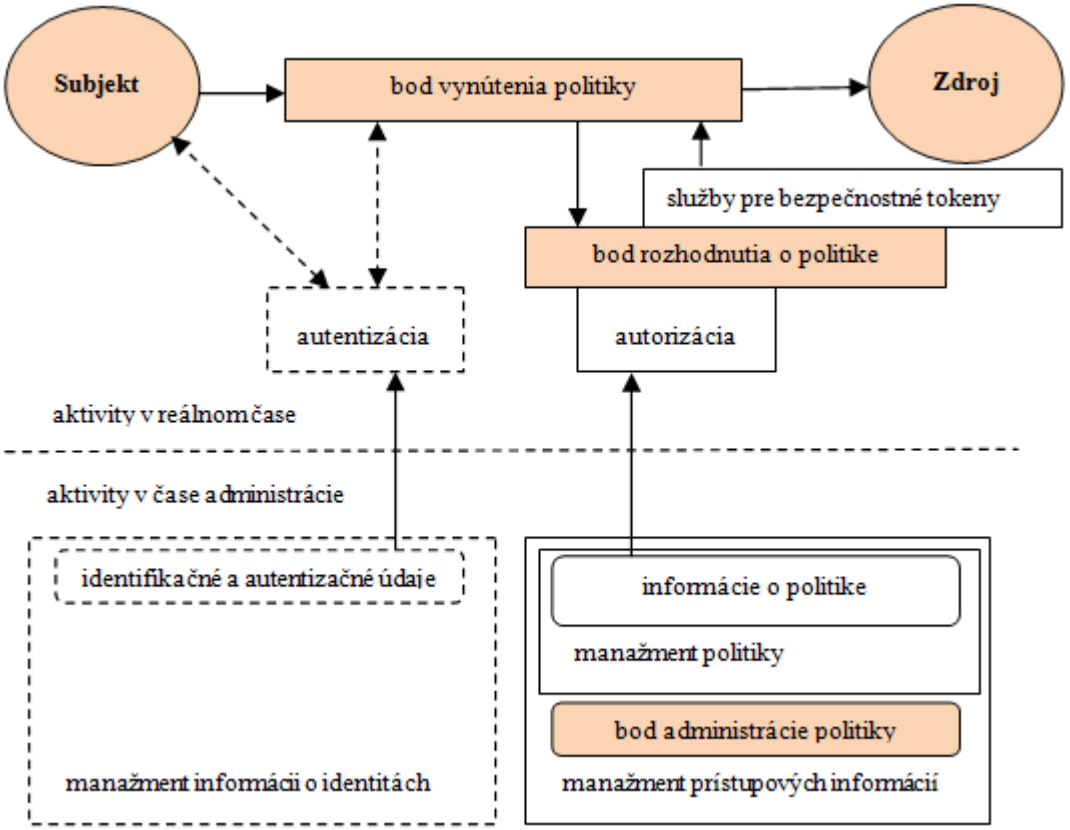
Zložky systému riadenia prístupov IV.

- Proces priraďovania zdrojov subjektom (Provisioning)
  - proces priraďovania privilégií (angl. privilege provisioning),
  - proces priraďovania zdrojov (angl. resource provisioning),
  - proces priraďovanie účtov IKT (angl. ICT account provisioning).
- Monitorovanie a sledovateľnosť vykonaných činností
- Odporúča sa monitorovať najmä nasledujúce činnosti:
  - prístup ku zdrojom personálnymi subjektmi organizácie,
  - prístupy do systémov externými subjektmi, audítormi prípadne inými poverenými osobami,
  - procedúry administrácie prístupu vykonávané administrátormi,
  - prístup vzdialených subjektov ku zdrojom systému,
  - prístup zariadení ku zdrojom systému,
  - vytváranie a bezpečnosť auditných záznamov a zápisov v registroch.

Referenčná architektúra riadenia prístupov

- Podľa ISO/IEC 29146 obsahuje nasledovné komponenty :
  - Subjekt: inicializačný bod, ktorý požaduje prístup ku zdrojom organizácie.
  - Zdroj: predstavuje koncový bod, ku ktorému je po úspešnej autentizácii a autorizácii umožnený požadovaný prístup.
  - Bod vynútenia politiky (angl. PEP – Policy enforcement point): tento komponent môže požadovať autentizáciu a následne si vynútiť autorizačné rozhodnutia. PEP popisuje atribúty jednotlivých subjektov pre potreby iných entít v rámci systému.
  - Bod rozhodnutia o politike (angl. PDP – Policy decision point): tento komponent uskutočňuje autorizačné rozhodnutia ako odpoveď na požiadavky PEP.
  - Služby pre bezpečnostné tokeny (angl. Security token service): prekladajú autorizačné rozhodnutia do tokenov, ktoré môžu byť použité na delegovanie prístupu.
  - Bod administrácie politiky (angl. PAP – Policy and attribute administration point): slúži ako centrálny administračný bod informácií o politike a atribútoch.
  - Informácie o politike (angl. Policy information): komponent obsahuje informácie o pravidlách a atribútoch jednotlivých zdrojov, ktoré sú zahrnuté v procese autorizácie.
  - Monitorovanie: tento komponent monitoruje činnosti a úlohy počas celého procesu riadenia prístupu, zvlášť v prípadoch, keď sa udeľuje alebo zamieta prístup ku zdrojom organizácie.

Referenčná architektúra riadenia prístupov



Auditovanie systému riadenia prístupov

- Výkon auditu riadenia prístupov môže byť formou interného alebo externého auditu.
- Auditovanie systému riadenia prístupov býva spravidla súčasťou komplexnejšieho auditu, ale aj ako samostatná náplň auditu.
- Zameranie na procesy, činnosti, zodpovednosti, konfigurácie, logy, prienikové testy, ...
- Audítorské štandardy a smernice ISACA, Výnos o štandardoch pre ISVS, ISO/IEC 27007:2011 Návody na výkon auditov riadenia informačnej bezpečnosti, COBIT, ...

Auditovanie systému riadenia prístupov

- Pri preskúmavaní systému riadenia prístupov by mal audítor:
  - získať všeobecný prehľad o bezpečnostných rizikách existujúcich pri spracovaní informácií prostredníctvom preskúmania príslušnej dokumentácie, dotazovaním konkrétnych subjektov, pozorovaním a používaním techník hodnotenia rizík,
  - dokumentovať a vyhodnotiť opatrenia súvisiace s prístupovými cestami do systému s cieľom posúdiť ich primeranosť, účinnosť a efektívnosť prostredníctvom kontroly funkcií softvérových a hardvérových komponentov,
  - testovať použité opatrenia súvisiace s riadením prístupov a určiť, či sú v praxi efektívne a bezpečne využívané,
  - vyhodnotiť prostredie riadenia prístupov s cieľom určiť, či sú existujúce opatrenia súvisiace s riadením prístupov implementované na základe vykonanej analýzy rizík prípadne iných auditných zistení,
  - vyhodnotiť systém riadenia bezpečnosti prostredníctvom preskúmania vnútorných predpisov organizácie, uskutočňovaných procedúr a činností súvisiacich s riadením prístupov a ich porovnaním so súvisiacimi bezpečnostnými štandardami a požiadavkami dobrej praxe.

Zoznámenie sa s IT prostredím organizácie

- Oboznámenie sa s IT prostredím organizácie by mal byť prvý krok vykonávaného auditu a obsahovať získanie jasnej predstavy o organizačnom, technickom a bezpečnostnom prostredí prevádzkovaného systému riadenia prístupov.
- Uskutočnenie rozhovorov s relevantnými osobami, fyzické preskúmanie priestorov či preskúmanie existujúcej dokumentácie súvisiacej s auditovaným prostredím.
- Podrobná identifikácia požiadaviek aplikovateľných právnych predpisov.

Dokumentovanie a posúdenie prístupových ciest ku zdrojom organizácie

- Prístupová cesta - logická postupnosť krokov, ktoré využíva koncový používateľ na získanie prístupu k informáciám uloženým na prostriedkoch výpočtovej techniky; začína zvyčajne na konkrétnom PC/terminále a končí sprístupnením dát alebo služieb používateľovi.
- Pri audite by sa mala osobitná pozornosť venovať najmä:
  - pôvodu a autorizácii dát,
  - platnosti a správnosti vstupných dát,
  - riadeniu životného cyklu prístupových oprávnení,
  - správe hesiel a ďalších autentizačných prostriedkov,
  - hrozbám zo siete internet (napr. sql injection, cross-site scripting, path traversal).

Rozhovory so zainteresovanými osobami

- Na riadenie a udržiavanie jednotlivých komponentov prístupových ciest sú spravidla vyžadovaní technickí špecialisti a experti na danú oblasť.
- Pre zistenie, s ktorými zainteresovanými osobami je potrebné uskutočniť rozhovory, by mal audítor IS konzultovať túto záležitosť s manažérom IKT ako aj preskúmať organizačnú štruktúru. Medzi kľúčové pozície patrí napr. administrátor bezpečnosti, sieťový administrátor či administrátor aplikácií.
- Audítor IS by mal uskutočniť aj rozhovory so vzorkou konečných používateľov IS s cieľom zistiť, či majú dostatočné povedomie o bezpečnostných politikách, prípadne iných vnútorných predpisoch upravujúcich povinnosti pri prístupe ku zdrojom organizácie.

Preskúmavanie záznamov z aplikácie na riadenie prístupov

- Schopnosť aplikácií na riadenie prístupu poskytovať podrobné zostavy o uskutočnených prístupoch ku zdrojom organizácie umožňuje administrátorom monitorovať dodržiavanie pravidiel súvisiacich s riadením prístupu.
- Na základe preskúmania vzorky týchto zostáv by mal byť audítor IS schopný určiť, či administrátori vykonávajú dostatočné činnosti súvisiace s administráciou, preskúmavaním či reakciou na zistené incidenty súvisiace s riadením prístupov.
- Neúspešné pokusy o prístup ku zdrojom organizácie by mali byť preskúmané a mali by mať identifikované ich atribúty ako sú čas neúspešného prihlásenia, miesto, z ktorého bol tento prístup uskutočnený ako aj dáta či služby, ku ktorým bol prístup požadovaný.

Špeciálne techniky a nástroje

- Testovacia príručka OWASP (Open Web Application Security Project) www.owasp.org
- Penetračné testovanie bez pridelených oprávnení.
- Penetračné testovanie s používateľskými oprávneniami.
- Testovanie vykonané z pohľadu všetkých rolí v aplikácii.
- Penetračné testovanie infraštruktúry, na ktorej je aplikácia prevádzkovaná: operačný systém, aplikačný server, web server, počítačová sieť.

Odkazy a referencie

- www.isaca.org
  - Auditorské checklisty, návody, postupy
  - Auditorské štandardy
  - Cobit
- csrc.nist.gov
  - Special publications
  - Federal Information Processing Standards (FIPS) publications
- www.sutn.sk
  - normy STN na internete

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Otázky a diskusia

Ďakujem za pozornosť

KPMG
cutting through complexity™