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
6. 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 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 pre špecialistov)

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

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.

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.

- 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).

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,
  - 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.

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 prístupu pri ukončení alebo zmene pracovného pomeru - ciele

Zabezpečiť, aby zamestnanci opustili organizáciu alebo zmenili podmienky svojho pracovného vzťahu primeraným spôsobom, nenarúšajúcim informačnú bezpečnosť.

Definovanie zodpovedností - opustenie organizácie zamestnancom má byť riadené, bude navrátené všetko poskytnuté vybavenie, budú odňaté príslušné prístupové práva.

Zmena zodpovednosti a pracovného vzťahu v rámci organizácie by mala prebehnúť riadeným spôsobom (je potrebné mať definovaný postup a náležitosti takejto zmeny).

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Vrátenie aktív

Pri ukončení pracovného vzťahu je zamestnanec povinný odovzdať všetky aktíva, ktoré sú v jeho správe a spolupracovať pri prevedení činností, ktoré vykonával, na iného zamestnanca.

Navrátanie aktív má byť evidované (výstupný list zamestnanca).

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Vrátenie aktív

V procese výpovede musí byť zahrnuté odovzdanie:

- pracovných pomôcok,
- hardvérového a softvérového vybavenia,
- dokumentov v listinnej aj elektronickej forme, správy elektronickej pošty obsahujúce dôležité pracovné informácie,
- všetkých ostatných poznatkov dôležitých z hľadiska zaistenia kontinuity výkonu činností (nezdokumentované postupy, korešpondencia, špecifické znalosti nadobudnuté počas pracovného vzťahu...).

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Odňatie prístupových oprávnení

Prístupové práva všetkých zamestnancov a zmluvných partnerov k informáciám a prostriedkom na ich spracúvanie musia byť na základe ukončenia pracovného resp. zmluvného vzťahu bezodkladne odobrané (cieľom je zabrániť neoprávnenému prístupu alebo zneužitiu prístupových práv).

KPMG
cutting through complexity™

Odňatie prístupových oprávnení

Prístupové práva, ktoré by mali byť odňaté alebo modifikované zahŕňajú:

- fyzický a logický prístup,
- kľúče, identifikačné karty,
- prostriedky na spracúvanie informácií,
- predplatené služby,
- odstránenie zo všetkej dokumentácie, ktorá ich zaraďuje k aktuálnym zamestnancom organizácie.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Otázky a diskusia

Ďakujem za pozornosť

KPMG
cutting through complexity™