Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

# Bezpečnosť prevádzky
# Časť 2

Erik Saller, Ivan Oravec

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

# Kontrola nad privilegovaným prístupom

- Privilegovaný používateľ je používateľ, ktorému je kvôli jeho funkcii, dôveryhodnosti a/alebo znalostiam pridelené oprávnenie pristupovať k zdrojom IKT na úrovni administrátora, teda vo významne širšom rozsahu ako má väčšina ostatných používateľov toho istého systému.
- Kontrola nad privilegovaným prístupom sa v praxi realizuje na rôznych úrovniach, môže sa jednať o obmedzenie používateľského prístupu na úrovni fyzického vstupu do budovy, operačného systému, informačného systému apod.

KPMG
cutting through complexity™

# Kontrola nad privilegovaným prístupom (pokr.)

- Príkladom riešenia pre flexibilnú kontrolu nad privilegovaným prístupom k prostriedkom operačného systému je nástroj SElinux (Security-Enhanced Linux). Je systémovým nástrojom moderných operačných systémov Linuxového typu.
- Požiadavka na sprístupnenie zdroja (typicky sa jedná o prístup na úrovni procesov, používateľov a soketov) je najprv posudzovaná oproti stanovenej bezpečnostnej politike.

# Kontrola nad privilegovaným prístupom (pokr.)

- V prípade, že sú podmienky politiky splnené, objekt je sprístupnený používateľovi.
- Tento prístup ku kontrole nad privilegovaným prístupom pomáha zabraňovať potenciálne nebezpečnej eskalácii oprávnení neprivilegovaných  používateľov.

# Kontrola nad privilegovaným prístupom (pokr.)

- Každý bežný používateľ má len určitú úroveň prístupu, ktorá je nevyhnutná pre realizáciu každodenných úloh v konkrétnom systéme.

# Kontrola nad privilegovaným prístupom (pokr.)

- Každý systém má systémové súbory, ktoré sú pre beh systému dôležité.
- Pri neautorizovanej modifikácii týchto súborov môže dôjsť ku kompromitácii systému, narušeniu behu operačného systému alebo dôležitej služby, prípadne znemožneniu riešenia denných povinností používateľmi.

# Kontrola nad privilegovaným prístupom (pokr.)

- Privilegovaný prístup administrátora poskytuje možnosť využívať pri plnení povinností súvisiacich s údržbou tie časti informačného systému, ktoré nie sú bežným používateľom prístupné.
- Vyžadovanie prihlásenia administrátora do privilegovaných častí systému je prínosné, pretože znižuje riziko úmyselného, alebo neúmyselného poškodeniu systému záškodným, alebo neskúseným administrátorom.

# Kontrola nad privilegovaným prístupom (pokr.)

- Oprávnenia na privilegovaný prístup by mali byť pridelené iba na limitovanému okruhu používateľov. Používateľ s privilegovaným prístupom k operačnému systému (administrátor, v linuxových systémoch nazývaný „root“) má práva inštalovať nový softvér, odinštalovať softvér, meniť nastavenia systému , ...

# Kontrola nad privilegovaným prístupom (pokr.)

- Administrátor operačného systému má zväčša takisto možnosť modifikovať nastavenie kontroly prístupu tak, aby umožnil prístup neautorizovaným používateľom.
- Ak dôjde ku kompromitácii mechanizmov riadenia prístupu, útočníkovi je spravidla umožnený prístup ku všetkým zdrojom, ku ktorým má prístup samotný systém.

# Kontrola nad privilegovaným prístupom (pokr.)

- Administrátor je obvykle oprávnený pozmeniť auditné záznamy operačného systému a (napr. pri súčasnej kompromitácii systému IDS/IPS) ovplyvňovať nastavenia detekcie incidentov tak, aby jeho potenciálne nebezpečné aktivity zostali nezachytené.
- Takto napadnutý systém môže byť často pozmenený a môže byť negatívne ovplyvnená funkcia detekcie a zneškodnenia škodlivého kódu („malware“).

# Kontrola nad privilegovaným prístupom (pokr.)

- Eventuálne na ňom môže dôjsť tiež k nasadeniu tzv. zadných vrátok („backdoorov“), ktoré umožňujú útočníkovi spätné prihlásenie a prístup ku kompromitovanému systému. Detekcia takto pozmenených používateľských staníc a serverov je problematická a často neefektívna.

# Kontrola nad privilegovaným prístupom (pokr.)

- Nasadenie systému na odhalenie a prevenciu prieniku (Intrusion Detection/Prevention System - IDS/IPS) na detekciu odchýlky od korektného fungovania používateľských staníc a detekciu indikátorov narušenia sieťovej prevádzky infraštruktúry organizácie útočníkom má priaznivý vplyv na prevenciu súvisiacich incidentov.
- Často však ani metódy použité IDS/IPS systémami akými sú napr. detekcia neobvyklých vzorov správania v sieťovej prevádzke, alebo hĺbková kontrola prenášaných paketov (anglicky „deep packet inspection“) nezaručujú úplnú ochranu voči existujúcim hrozbám.

# Kontrola nad privilegovaným prístupom (pokr.)

- Administrátorské práva, ktoré by za normálnych okolností mali byť pridelené len úzkej skupine administrátorov, môžu byť nevyhnutné aj pre zamestnancov na pozíciách vývojárov, operatívy, alebo systémového monitorovania.
- Dobrou praxou je v takom prípade model riadenia prístupu, v ktorom sú používatelia zaradení do skupín (anglicky „groups“), ktoré majú špecifické úrovne prístupu a práva.

# Kontrola nad privilegovaným prístupom (pokr.)

- Toto definovanie privilegovaných prístupov pre skupiny používateľov a s ním súvisiace prideľovanie a odnímanie prístupových práv sa deje kontrolovaným spôsobom podľa druhu činnosti vykonávanej používateľmi.
- Správne odstupňovaným riadením prístupu používateľov k zdrojom je systém vystavený nižšiemu riziku incidentov spojených s neautorizovaným prístupom a pozmenením dôležitých nastavení.

# Kontrola nad privilegovaným prístupom (pokr.)

- Implementácia obmedzenia neautorizovaných aktivít administrátorských používateľov nie je jednoduchá a preto **je vhodné zaviesť monitoring systémových zmien** pomocou ktorého je možné aktivity administrátorov posudzovať v kontexte ostatných bezpečnostne relevantných udalostí a to „zvonka“ systému (teda tak, **aby ich útočník nemohol zmeniť na napadnutom lokálnom systéme**).

# Kontrola nad privilegovaným prístupom (pokr.)

- Medzi takéto upresňujúce udalosti patrí napríklad informácia:
  - z ktorého účtu bežného používateľa došlo k eskalácii privilégií - pokiaľ nešlo o priame prihlásenie administrátorského užívateľa,
  - či ku eskalácii privilégií došlo po prvej výzve na zadanie administrátorského hesla,
  - či k privilegovanému prístupu došlo v čase, alebo mimo času bežnej prevádzky,
  - aké príkazy boli spustené a ktoré systémové súbory boli zmenené.

# Kontrola nad privilegovaným prístupom (pokr.)

- Na to, aby sme mali dôveryhodný záznam o všetkých týchto podrobnostiach činností administrátorov, je nutné práve splnenie predpokladu zachovania integrity a autentickosti auditných záznamov.
- Dobrou praxou je okamžite (resp. v stanovených intervaloch) prenášať záznamy o bezpečnostne relevantných udalostiach na iný systém v sieťovej infraštruktúre, ktorý sa stará o ich vyhodnocovanie, ukladanie, triedenie a prípadné vyvodzovanie vhodných protiopatrení.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

# Separácia kanálov pre administráciu od kanálov pre bežnú prevádzku

- Používanie spoločných účtov pre viacero používateľov nie je v súlade so štandardami bezpečnostných politík a predovšetkým pri administrátorskom prístupe predstavuje veľké riziko zneužitia.
- Ideálne je preto zabezpečiť separáciu účtov pre administráciu od účtov pre bežnú prevádzku.

KPMG
cutting through complexity™

# Separácia kanálov pre administráciu od kanálov pre bežnú prevádzku (pokr.)

- Získanie prístupu do privilegovaného účtu z účtu bežného používateľa sa v ideálnom prípade deje až pri splnení vopred stanovených podmienok (autentifikácia) a je nevyhnutné zabezpečiť riadne zaznamenávanie (auditovanie) takejto činnosti, tak aby bolo jasné, kto a kedy vyžiadal administrátorské práva.

# Separácia kanálov pre administráciu od kanálov pre bežnú prevádzku (pokr.)

- Zaznamenávanie operácií vykonaných používateľmi a administrátormi sa nazýva „accounting“. Jeho implementáciou v prístupe k sieťovým zariadeniam je napr. TACACS+.
- Tento nástroj však neplní iba funkciu accountingu, ale okrem nej vykonáva ešte autentifikáciu (anglicky „authentication“) a autorizáciu (anglicky „authorization“).

# Kontrola integrity

- V praxi sa hlavne pri snahe vyhovieť prísnejším štandardom (napr. v bankovej sfére) nasadzujú nástroje na overovanie integrity systémových a aplikačných komponentov a ich aktualizácií pred inštaláciou pomocou hašovania súborov a ich porovnávania s „etalónovými“ hašmi.
- Etalónovými hašmi máme na mysli také, ktoré sú v databáze softvérového nástroja na kontrolu integrity vedené ako vzorové a boli správne overené. Tento postup má význam pri kontrolovaní konfigurácií a logov a prevencii neautorizovaného zásahu.

# Kontrola integrity (pokr.)

- Nástroje používané pri kontrole integrity (napríklad Tripwire) detegujú pozmenenie dát neoprávnenou osobou a v prípade ak je to vhodné a možné vykonajú aj nápravné opatrenia (napr. korekciu vlastníctva a prístupových práv súborového systému).
- Môžu byť súčasťou kontrolných mechanizmov slúžiacich na priebežné vyhodnocovanie dodržiavania bezpečnostných politík organizácie.
- Poskytujú možnosti korelácie logov a vyvodenia záverov o súvislostiach incidentu. Ich výstup je možné využiť pri zbieraní digitálnych dôkazov, napr. podľa štandardu stanovenom v dokumente ISO 27037 (Guidelines for identification, collection, acquisition and preservation of digital evidence).

# Zmena počiatočnej konfigurácie po inštalácii

- V praxi často dochádza k tomu, že i pri implementácii kvalitného a drahého informačného systému s pokročilými bezpečnostnými funkciami sa **pozabudne na zmenu prednastavených hesiel**, prípadne sa v systéme ponechá menej bezpečné nastavenie komunikačnej metódy, ktoré umožní útočníkovi prienik do systému, alebo poslúži ako medzi krok k úspešnému prieniku.

# Zmena počiatočnej konfigurácie po inštalácii (pokr.)

- Typickými príkladmi sú nastavenia slabých hesiel pre administrátorského používateľa ako napr. „admin“, „administrator“, „root“, „toor“ , alebo iné triviálne uhádnuteľné znenia.
- Pokiaľ ide o konfiguračné nedostatky, môže sa stať, že je aj pokročilé VPN riešenie pri nasadzovaní a nastavení dodávateľom ponechané s **nevhodným protokolom na výmenu kľúčov, ktorý má slúžiť iba ako dočasné riešenie.**

# Zmena počiatočnej konfigurácie po inštalácii (pokr.)

- Za všetky problematické nastavenia spomeňme agresívny mód VPN sietí, anglicky „aggresive mode“, pri ktorom má útočník možnosť relatívne triviálnym útokom odchytiť autentifikačný hash založený na tzv. preshared key - zdieľanom kľúči, použitom na nie veľmi bezpečnú komunikáciu dvoch koncových uzlov VPN siete.
- V prípade VPN riešení je neporovnateľne jednoduchšie útočiť na takto nedostatočne nastavené úrovne zabezpečenia, ako sa napr. púšťať do kryptografickej analýzy prenášaných dát.

# Zmena počiatočnej konfigurácie po inštalácii (pokr.)

- Predovšetkým pri proprietárnych systémoch tiež existuje riziko, že systém bude obsahovať predprogramované používateľské mená a heslá („hard-coded credentials“), ktoré môžu potenciálnemu útočníkovi poslúžiť ako zadné vrátka a predstavovať veľké bezpečnostné riziko neautorizovaného prístupu.
- Pri aktualizácii dôležitých systémových a aplikačných softvérových komponentov (napr. v exponovaných prevádzkach) sa musí postupovať v súlade so štandardami, ktorých dobré praktiky odporúčajú pravidelné „rozbaľovanie“ nových verzií informačných systémov, operačných systémov a softvérových balíkov vo všeobecnosti najprv do testovacieho prostredia.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

# Zmena počiatočnej konfigurácie po inštalácii (pokr.)

- Až po ich dôkladnom otestovaní dochádza k ich nasadeniu do tzv. produkčnej prevádzky, ktorá pracuje s reálnymi dátami v „ostrej“ prevádzke.
- Zo skúseností je možno konštatovať, že proprietárne systémy sú spravidla väčšmi náchylné na výskyt chýb pri vývoji, hlavne pokiaľ používajú neštandardné protokoly na výmenu dát, alebo neštandardné metódy na ukladanie dát.
- Tieto chyby poskytujú priestor pre zraniteľnosti, ktorých zneužitie útočníkom predstavuje potenciálne riziko narušenia dôvernosti spracovávaných dát, ich vymazanie, alebo neautorizovanú modifikáciu, nestabilitu softvéru a nedostupnosť produkčného systému na ktorom je tento softvér nasadený.

# Zmena počiatočnej konfigurácie po inštalácii (pokr.)

- Iniciatívy vývoja softvérových produktov s otvoreným zdrojovým kódom („open source“) a štandardizácia metód vývoja softvéru pomáha zmierňovať výskyt incidentov zapríčinených softvérovými chybami.
- Tým, že sú softvérové produkty s otvoreným zdrojovým kódom masovo využívané a ich testovanie je vykonávané veľkou komunitou výskumných pracovníkov v oblasti bezpečnosti aj „masou“ používateľov na celom svete, je zabezpečená včasná eliminácia veľkej väčšiny softvérových chýb.

# Zmena počiatočnej konfigurácie po inštalácii (pokr.)

- Príkladom komunitného softvéru, ktorý má široké uplatnenie na produkčných platformách je webový server Apache.
- Pri ochrane systémového a aplikačného kódu a údajov proti neoprávnenej manipulácii počas prevádzky pomáha kontrola integrity pomocou hašovania dôležitých súborov a archivácia výstupov hašovacích algoritmov, kvôli neskoršiemu porovnaniu.
- Implementáciou tohto prístupu je napríklad už spomínaný nástroj Tripwire a v praxi sa využíva jeho nasadzovanie naprieč všetkými produkčnými serverovými systémami v produkcii.

# Zmena počiatočnej konfigurácie po inštalácii (pokr.)

- V prípade nasadzovania nových komponentov do existujúcej infraštruktúry je nutné, aby nový hardvér a softvér zapadol do aktuálnej „mozaiky“ IKT prostredia a podľa možností nespĺňal úlohy, ktoré už za neho pokrýva iný systém (pokiaľ to nie je explicitne vyžadované).
- Niekedy dochádza k zbytočným kolíziám technológií kvôli nesprávnemu plánovaniu, napr. pri použití viacerých VPN riešení naraz.

# Zmena počiatočnej konfigurácie po inštalácii (pokr.)

- Pripojenie na VPN, ktorá sprístupňuje sieťové zdroje (dátové úložiská, informačné systémy, webové lokality, atď.), z nej následné pripojenie na inú VPN, kvôli prístupu k iným zdrojom nemusí vždy fungovať práve kvôli tomu, že dochádza ku kolíziám s ktorými sa nerátalo pri pôvodnom plánovaní.
- Príkladom môže byť problém v prístupe k lokálnym, alebo naopak vzdialeným sieťovým zdrojom (kolízia adresného priestoru podsietí v lokálnej sieti s rovnakým adresným priestorom vo vzdialenej sieti, napr. obe siete by nemali používať rozsah 192.168.1.x).

# Aktualizácia softvéru

- Centralizovaná správa aktualizácií informačných systémov v prostrediach so zložitejšou infraštruktúrou sa typicky rieši vyhradenými repozitármi aktualizácií v rámci konkrétnej organizácie, ktoré sú v danom prostredí (na konkrétnych platformách, napr. hardvérových) riadne odskúšané a pri ich následnom nasadeni  na koncových staniciach a serveroch nedochádza k nepredvídateľným chybám.
- Aktualizácia používaných systémov je dôležitá, pretože aktualizácie systémov alebo aplikácií sú dodávateľmi vytvárané s cieľom dostránenia známej bezpečnostnej alebo inej chyby v ich produkte.

# Aktualizácia softvéru (pokr.)

- Pri nasadzovaní aktualizácií je potrebné myslieť aj na riziká z tohto procesu vyplývajúce. S každou novu nasadenou aktualizáciou sa totiž systém vystavuje napr. riziku nestability. Paradoxne sú po aplikovaní záplaty niekedy do systému vnášané zraniteľnosti.
- Typickým príkladom takéhoto nežiadúceho dôsledku bolo, keď v máji 2008 vývojový tím linuxovej distribúcie Debian vydal novú „stabilnú“ verziu balíka OpenSSH s výrazne zmenšeným priestorom generovaných SSH kľúčov, čím vystavil produkčné servery na celom svete riziku úspešného útoku hrubou silou.

# Kontrola nad hardvérom

- Dokonca aj pri korektne nastavených pravidlách riadenia prístupu, správnom manažmente používateľských účtov a hesiel na sieťových zariadeniach, dobrej politiky konfiguračného manažmentu a aktualizácií softvéru môže útočník využiť niektorú z metód neautorizovaného pripojenia na hardvér za účelom získania a zneužitia citlivých informácií.
- Používané techniky zahrňujú pripojenie sledovacieho nástroja na „trunk“ port sieťového zariadenia kvôli monitorovaniu a eventuálnej modifikácii sieťovej prevádzky, priamy prístup k administrátorskému rozhraniu komponentu IKT/informačného systému, alebo v špecifických prípadoch o použitie sondy, ktorá aktívne, alebo pasívne narúša dôvernosť a/alebo integritu prenosu dát po zbernici počítača, alebo sieťovej, resp. telekomunikačnej linke.

# Kontrola nad hardvérom (pokr.)

- Prístup k systémovým zdrojom je kontrolovaný operačným systémom/firmvérom, ale treba mať na pamäti, že zariadenia pripojené k tomuto systému môžu tiež poskytnúť útočníkovi informáciu, ktorej vyzradenie pre nás môže predstavovať riziko.
- Z týchto dôvodov je potrebné dodržiavať režimové opatrenia a riadiť prístup tiež na úrovni fyzickej bezpečnosti, v rámci ktorých povolíme prístup do serverovní a kancelárií, kde sú umiestnené prvky IKT iba obmedzenému okruhu osôb, ktoré sú dostatočne dôveryhodné a poučené o zásadách bezpečnej manipulácie s dátami a citlivými dokumentmi.

# Kontrola nad hardvérom (pokr.)

- V prípade ak je potrebné, aby cudzia osoba pristupovala k týmto priestorom, je nutné aby sa tak vždy dialo v sprievode kvalifikovaného a poučeného personálu.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

# Riadenie zmien

- Riadenie zmien je jednou z kľúčových oblastí manažmentu prevádzky. Zabezpečuje kontrolovanú implementáciu autorizovaných zmien v produkčných systémoch.
- Tieto produkčné systémy môžu predstavovať systémový, alebo aplikačný softvér, môže sa však tiež jednať o hardvérové komponenty, alebo iné platformy
- Požiadavky na zmeny môžu vo všeobecnosti prichádzať z celej organizácie.

KPMG
cutting through complexity™

# Riadenie zmien (pokr.)

- Je dôležité určiť, **kto je oprávnený požiadavky na zmeny špecifikovať** a zabezpečiť ich integráciu s procesmi, ktoré podporujú.
- Úloha zostavenia stratégie je v rukách manažmentu a príslušnej stratégii podliehajúce technologické zmeny musia byť odsúhlasené architektmi a inými osobami v roli zodpovednej za **ohodnotenie možných rizík** navrhovaných zmien (biznis vlastník, oddelenie bezpečnosti, alebo osoby v príslušnej roli).

# Riadenie zmien (pokr.)

- Úlohou manažmentu spolu s oddelením IT by malo byť zabezpečenie toho, aby do IT prostredia boli zavedené **iba autorizované a adekvátne otestované zmeny**. Potom je možné pristúpiť k ich samotnej implementácii.
- Zmeny v produkčných systémoch napr. zahŕňajú:
  - implementáciu nových aplikácií,
  - modifikáciu existujúcich aplikácií,
  - odstraňovanie starých aplikácií,
  - aktualizáciu, alebo zaplátavanie systémového softvéru.
- **Z bezpečnostného hľadiska nás zaujíma potenciálny dopad týchto zmien**, a tiež či ich implementácia nie je riadne zdokumentovaná (napr. automatizovaným systémom pre riadenie zmien, anglicky IT Service management), a riadne schválená manažmentom (napr. pomocou informačného systému pre formálne schvaľovanie navrhovaných zmien, ktorý môže byť integrovaný rovnako tak v IT Service management softvéri).

# Riadenie zmien (pokr.)

- V praxi sa formálna stránka riadenia zmien často obchádza. Zmeny sa nedokumentujú do informačného systému na to určeného, ale sa robia na „dobré slovo“ (komunikáciou cez email, telefón, alebo interný chat).
- Dôvodom pre takýto nesprávny prístup je buď neexistencia samotného formálneho systému na riadenie zmien, alebo to, že implementácia zmien bez ich dokumentovania je menej časovo náročná.
- Tento prístup má však ďalekosiahle negatívne následky a preto je potrebné v každej organizácii zaviesť politiku riadenia zmien, ktorá okrem iného určuje ich riadne dokumentovanie.

# Riadenie zmien (pokr.)

- Politika riadenia zmien sa môže špecificky venovať:
  - operačným systémom,
  - sieťam,
  - hardvérovým komponentom informačných a komunikačných technológií
  - podpornej infraštruktúry potrebnej pre prevádzku IT prostredia (chladenie, klimatizácia, elektrické rozvody).
- Politika je nevyhnutná kvôli zvýšeniu efektivity (možno nie okamžitej, ale v konečnom dôsledku sa systematické zavádzanie zmien odzrkadlí v lepšie fungujúcej infraštruktúre) a prehľadnosti vykonaných zmien.

# Riadenie zmien (pokr.)

- Procesy definované politikou tiež stanovujú **náležitosti notifikácie** (riadneho komunikovania uskutočňovaných zmien) smerom k používateľom, ktorých sa uskutočňovaná zmena dotýka.
- Takáto notifikácia používateľov je veľmi dôležitá, keďže cieľom riadenia zmien je implementovať zmeny v informačných systémoch a IKT prostredí, ktoré vo väčšine prípadov slúžia práve im.
- Každý (ohlásený, alebo neohlásený) výpadok služby IKT by mal **negatívny dopad na efektivitu nimi vykonávaných činností.**

# Riadenie zmien (pokr.)

- Organizácie si väčšinou osvojujú proces riadenia zmien a **modifikujú procesy pre svoje individuálne potreby**. Procesy riadenia zmien by mali byť navrhnuté tak, aby **zohľadňovali náklady vynaložené na implementáciu zmeny vo vzťahu k výhodám z nej plynúcim**. Toto zhodnotenie sa anglicky nazýva „business case“.

# Riadenie zmien (pokr.)

- Business case navrhovanej zmeny musí byť riadne zanalyzovaný a malo by byť priebežne hodnotené jeho plnenie.
- Zmeny systémov by sa mali teda diať kontrolovaným spôsobom podľa štandardov. V tomto snažení pomáhajú tiež dobré praktiky zhrnuté v norme ISO 27002, ktorá poskytla vzor pre legislatívny rámec metodiky informačnej bezpečnosti vo výnose MVSR č. 312/2010.

# Riadenie zmien (pokr.)

- **Náležitosti procesov bežného riadenia zmien**:
  - vyžiadanie zmeny vyplnením formálnej požiadavky,
  - posúdenie zmenovej požiadavky, okrem iného architektom zodpovedným za danú oblasť,
  - analýza možností implementácie zmeny,
  - analýza nákladov súvisiacich so zmenou,
  - zaznamenanie vyššie uvedených analýz a odporúčaní pre zmenu,
  - zmenová požiadavka môže byť podaná komisii (riadiacemu výboru, anglicky „steering committee“) na posúdenie a uznesenie sa na konečnom rozhodnutí o jej implementácii (zmenovej požiadavke sa pridelí, alebo odmietne tzv. „green light“),
  - odsúhlasené zmeny sú vykonané a zaznamenané,
  - metodika implementácie zmien je posúdená osobou v roli kontrolóra kvality, interným, alebo externým auditom.

# Riadenie zmien (pokr.)

- Na tomto procese by sa malo **od prvých fáz** podieľať tiež **oddelenie bezpečnosti**, alebo zamestnanci plniaci jeho rolu v rámci IT oddelenia kvôli posúdeniu toho, či je zmena v súlade s bezpečnostnými politikami.
- Cieľom celého procesu je predovšetkým to, aby sa zmeny diali kontrolovaným spôsobom, aby vďaka nim došlo k **eliminácii problémov a chýb, ktoré znižujú bezpečnosť a stabilitu** informačných systémov a IKT prostredia.

# Riadenie zmien (pokr.)

- Na to, aby sme zabezpečili tieto ciele, je potrebné:
  - v prostredí, kde je nevyhnutná vysoká dostupnosť zabezpečiť dostatočnú redundanciu,
  - komunikovať zmeny používateľom – napriek tomu, že malé zmeny sa môžu zdať významné iba pre malú časť používateľov, môže sa stať, že zasiahnu širší okruh používateľov, je preto dôležité zvážiť notifikáciu širokého okruhu používateľov, aby mali čas sa pripraviť na prípadný výpadok,
  - vypracovať analýzu zmien a prezentovať hlavné výhody a riziká z nej vyplývajúcich. Poskytnutie riadnej dokumentácie tejto zmeny je dobrým (aj keď nie jediným) predpokladom pre predchádzanie kritickým incidentom. Analýza popisuje úmysel pôvodcu požadovanej zmeny a je dôležitá kvôli predchádzaniu implementácie zbytočných, alebo škodlivých zmien,
  - redukovať dopad zmien na dostupnosť poskytovanej služby – služby IKT a informačných systémov musia byť dostupné, keď ich organizácia potrebuje. Nesprávne posúdenie zmien, chybné implementácie zmien a neadekvátna príprava patrí k najčastejším chybám, ktoré nie sú v tomto procese žiaduce. Dobre štruktúrované procesy riadenia zmien zamedzujú problémom a umožňujú nepretržitý beh poskytovanej služby.

# Riadenie zmien (pokr.)

- zaznamenanie zmeny do zmenového logového záznamu („change log“), ktorý poskytuje dokumentáciu samotnej zmeny (okrem iného tiež popis časového harmonogramu a testovanie zmeny). Tento zmenový logový záznam by mal byť aktualizovaný v priebehu procesov schvaľovania, plánovania a implementácie zmeny,
- časové rozvrhnutie zmeny – po uskutočnení dôkladnej prípravy a zhodnotenia dopadov zmeny z časového hľadiska by mal byť naplánovaný proces implementácie.
- Čas implementácie by mal byť zvolený tak, aby mali osoby zodpovedné za odsúhlasenie zmeny dostatok času na posúdenie zmeny.

# Riadenie zmien (pokr.)

- Pri diskusii s osobami zodpovednými za posudzovanie zmien by mali byť prediskutované všetky možné dopady implementovanej zmeny.
- Ak dôjde k dohode na tom, že je možné pristúpiť k implementácii, je vložená do harmonogramu plánovaných zmien a označená za odsúhlasenú.
- Všetky odsúhlasené aj neodsúhlasené zmeny by mali byť komunikované písomnou formou s riadnym popisom dôvodov.
- implementovanie zmien – posledným krokom v zmenovom procese je aplikovanie zmien na hardvérové a softvérové časti IKT. Ak zmena funguje podľa plánu, je vhodné to zapísať do zmenovej požiadavky a formálne ju uzavrieť.

# Riadenie zmien (pokr.)

- Ak zmena nefunguje podľa očakávaní je potrebné zozbierať príslušné informácie o dôvodoch nefunkčnosti, zapísať ich do zmenovej požiadavky a uskutočniť opatrenia na nápravu.
- Táto informácia sa dá neskôr využiť pri analýze vzniknutej situácie a je možné pomocou nej **zabrániť výskytu rovnakého problému**.
- V prípade, že by ani po pokuse o nápravu nedošlo k úspešnej implementácii zmenovej požiadavky mala by byť vyhotovená správa.
- Táto správa spravidla obsahuje informáciu o tom, ako by neúspešná zmena mohla ovplyvniť prostredie, alebo aká alternatívna metóda je použitá na obnovu prevádzky pokiaľ nedôjde k náprave vzniknutého stavu, reportovanie nasadených zmien manažmentu – dôkladný report sumarizujúci informácie o zmenovom procese by mal byť periodicky poskytovaný manažmentu.

# Riadenie zmien (pokr.)

- To zabezpečuje, že manažment si je vedomý toho, aké problémy s **kvalitou služby mohli eventuálne vzniknúť a má možnosť adekvátne reagovať, napr. zmenou v plánovaní a stratégii.**
- Tieto kroky by mali byť riadne zdokumentované a komunikované relevantným stranám zapojeným v zmenovom procese. Potom, čo dôjde k spusteniu konkrétneho zmenového procesu, mala by byť k nemu pridelená osoba zodpovedná za jeho dôkladné riadenie a súvisiacu agendu.
- V prípade nesprávneho procesu zmenového manažmentu by mohlo dôjsť k bezpečnostným incidentom, únikom dát a narušeniu funkčnosti existujúcej infraštruktúry.

# Riadenie zmien (pokr.)

- Každá pripravovaná zmena by mala podliehať tzv. **UAT (User acceptance testing)**, teda procesu testovania a získania spätnej väzby od používateľov. Odborník na konkrétny testovaný systém (vlastník, alebo používateľ sa v tejto súvislosti nazýva Subject matter expert, skrátene „SME“) skontroluje implementovanú zmenu z používateľského pohľadu a podá správu o tom, či je funkčná zmena v súlade so stanovenými požiadavkami.
- Vo vývoji softvéru je takéto testovanie **jednou z posledných fáz projektu** a väčšinou sa realizuje predtým, než zákazník príjme nový systém. Pokiaľ systém funguje správne počas UAT, je veľmi pravdepodobné, že bude vyhovovať a stabilne plniť svoju funkciu aj v produkcii.

# Riadenie zmien (pokr.)

- Tieto používateľské testy sa väčšinou nezaoberajú gramatickými, „kozmetickými“ chybami v používateľskom rozhraní, dokonca ani výraznými chybami, akými je softvérová nestabilita. Tieto chyby sú odstraňované v skorších fázach testovania. **Podmienky tohto druhu testovania sú často zahrnuté v zmluve s dodávateľom**.
- Pri testovaní musí byť zabezpečené oddelenie vývojového, testovacieho a produkčného prostredia.
- Segregácia právomocí pri takomto oddelení spočíva v rozdelení každej z funkcií vývoja, testovania a prevádzky delegovaným osobám, ktoré vlastnia príslušné roly v procese, prípadne je vhodné oddeliť povinnosti a aplikovať konkrétne roly medzi existujúcich zamestnancov, ale vždy tak, **aby boli v konkrétnej roli nestranní**.

# Riadenie zmien (pokr.)

- Cieľom je zamedziť skresleným výsledkom testovania spôsobených neobjektívnym pohľadom zainteresovaných strán. Napríklad programátor, ktorý sa dlho venuje jednej oblasti môže potrebovať pohľad nezainteresovanej strany, ktorá má od problému „odstup“, aby identifikoval príčinu problému.
- Pre vedenie záznamov o systémoch, prevádzke a zmenách sa používajú automatizované informačné systémy. Väčšinou sa v ňom zaznamenávajú údaje relevantné k náprave incidentov, teda napríklad v prípade evidencie technických detailov hardvéru sú to informácie o fyzickom umiestnení servera v datacentre, údaje o spôsobe pripojenia ku konzole kvôli údržbe, o operačných systémoch a o biznis vlastníkoch služieb bežiacich na týchto operačných systémoch (napr. aj kvôli ich notifikácii o pripravovanom vypadku).

# Riadenie zmien (pokr.)

- Príprava prác musí zahŕňať vyhradenie časového okna určeného na údržbu. Jeho správne načasovanie je kritické pre spoľahlivosť služby, pretože údržba často súvisí s dočasným jej výpadkom.
- Pokiaľ robíme údržbu systému, ktorý používajú tisíce používateľov, nemôžeme si dovoliť výpadok počas „najsilnejšej“ dennej prevádzky, preto sa s ohľadom na majoritnú časť používateľov väčšinou výpadok načasuje na hodiny nočnej prevádzky, riadne sa komunikuje všetkým používateľom, prípadne sa im oznamuje možnosť použitia alternatívnej služby.
- Manažment riadenia zmien vydáva tiež operačné inštrukcie zohľadňujúce prípady, kedy službu nie je možné po zásahu obnoviť.

# Riadenie zmien (pokr.)

- V takýchto prípadoch sa uplatňuje tzv. „rollback“, teda urýchlené vrátenie systému do pôvodného stavu a volí sa náhradný rozvrh implementácie zmien.
- Konverzia dátových formátov pri importe a exporte dát medzi systémami sa deje obyčajne tiež v čase mimo hlavnej prevádzky a je užitočné zohľadňovať tiež krízové prípady, kedy sa import neukončí korektne, prípadne ak celkom zlyhá.
- Centralizovaná databáza konfigurácií pregeneruje individuálne nastavenia a nakopíruje ich na jednotlivé prvky infraštruktúry, prípadne ich uloží do centrálneho úložiska dát.
- Konverzia systémov (napr. pokiaľ príde k nahradeniu zastaraného systému novším) sa vo všeobecnosti riadi štandardami zmenového manažmentu popísanom vyššie.
- Často sú na implementáciu nových riešení nevyhnutné rozsiahlejšie časové okná, ale ak si to prevádzka vyžaduje, systémy sa nastavia už v prípravných fázach a čas výpadku sa tým minimalizuje.

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

# Otázky?

KPMG
cutting through complexity™