AFOI 2003 - Bezpečnost v realitě denní praxe provozu IS

Provozní hlediska systémového auditu v aplikacích a systémech

Karel Miko, CISA (miko@dcit.cz)

DCIT, s.r.o (www.dcit.cz)

DCIT

Systémový (bezpečnostní) audit – základní vymezení pojmů

- Systémový audit = funkcionalita týkající se zaznamenávání klíčových událostí a stavů během provozu systémů a aplikací
- Nejedná se o konkrétní produkt konkrétního výrobce (obvykle součástí aplikací/systémů)
- Nejedná se o žádnou specifickou formu bezpečnostního posouzení (audit) systému

DCIT

Obsah příspěvku

Systémový audit ~ logování (logging)

- Nejedná se o nic „nového“ či „převratného“
- Dříve doména spec. systémů, dnes je tato funkčnost dostupná už i běžných systémů/aplikací
- O jeho významu a potřebnosti hovoří prakticky všechny bezpečnostní normy
- U běžných systémů je v praxi využíván velmi zřídka

Jak funguje?

Proč jej provozovat?

Jaké očekávat komplikace?

DCIT

Co je a co už není systémový bezpečnostní audit?

- Neexistuje jasná všeobecně zavedená definice
- S pojmem „auditing“ operují různé standardy ITSEC, TCSEC, Common Criteria (ISO 15408) aj.

  ISO 15408: Systémový audit zahrnuje rozpoznávání, zaznamenávání, ukládání a analýzu informací souvisejících s aktivitami relevantními z hlediska bezpečnosti systému. Výsledné auditní záznamy mohou být použity ke stanovení, kdy nastaly ty které aktivity dotýkající se bezpečnosti systému a který uživatel je za ně zodpovědný.

- Do jisté míry je auditing uvedenými standardy „vynucen“ (např. každý C2-certifikovaný systém musí mít implementovánu funkčnost auditingu)

DCIT

Jak si lze představit systémový audit v konvenčních systémech?

- **V UNIXových systémech obvykle 2 roviny:**
  - Tradiční OS „logging features“ – syslog, lastlog apod.
  - Speciální systémový bezpečnostní auditing (zejména doména komerčních UNIXů)
- **Systémový audit v MS Windows**
  - EventLog – obecný systém logování událostí
  - Security EventLog – události relevantní z hlediska bezpečnosti
- Obecně ne každé logování lze považovat za systémový audit

Atributy systémového auditu

- **Důvěryhodnost mechanizmu pořizování záznamů**
  - *Odolnost vůči neoprávněné deaktivaci, „obejití“ mechanizmu či „zahlazení stop“*
  - *Měl by být schopen monitorovat i administrátora*
- **Vypovídací hodnota pořízených záznamů**
  - *Zaznamenávané informace musí být přiměřeně komplexní (datum/čas, identifikace uživatele, terminálu, …)*
  - *Záznamy jsou potenciálně důkazní materiál*
- **Nepopiratelnost záznamů**
  - *Chráněné úložiště záznamů (audit trail)*
  - *Odolnost před zkreslením záznamů (při jejich pořizování nebo u již uložených záznamů)*

Co lze obvykle auditovat?

- **Operační systém**
  - Object auditing – operace se soubory/tiskárnami apod.
  - Account auditing – přihlášení, odhlášení, změna hesla, …
  - Process auditing – vytvoření/ukončení procesu
  - Action/event – startup/shutdown, manipulace - audit trail
  - Syscall auditing – záznamy o systémových voláních
- **Databáze**
  - prakticky libovolný SQL statement (SELECT, INSERT, …)
  - klíčové události události - start/stop, zásah do ACL
- **Aplikace**
  - obvykle transakce na aplikační úrovni
  - kritické operace – např. nevratné hromadné operace

Jak je systémový bezpečnostní audit řešen technicky?

- často nutno aktivovat speciální subsystém - Basic Security Module, OSFC2SEC, Trusted Computing Base apod. (obvykle implicitně deaktivován)
- typicky relativně netriviální konfigurace
- zásadní otázka – ochrana audit trailu:
  - úložiště – soubor, tabulka v databázi (SYS.AUD$), spec. diskový oddíl či zařízení (/dev/audit), vzdálené ukládání, …
  - často speciální binární formát, záznamy přístupné pouze přes volání (API) operačního systému
  - audit trail nutno „chránit“ i před administrátorem

Příklad - auditing v Microsoft Windows

- je využito **Eventlogu** (v systému existuje několik logů - jeden z nich je tzv. „Security Eventlog“)
- audit trail je uložen **v souboru** (není přímo přístupný) c:\windows\system32\config\security.log
- přistupovat k záznamům lze pomocí „**eventlog viewer**“ nebo přes speciální API
- přístup k Security eventlogu se přiděluje jako **speciální uživatelské oprávnění**
- ani uživatel s právem manipulovat se security eventlogem nemůže audit trail beze stopy smazat
- ochrana audit trailu funguje pouze pokud je počítač „pod vládou“ operačního systému

DCIT

Proč systémový audit?

- sběr důkazního materiálu pro šetření bezpečnostních incidentů a nestandardních stavů
- může usnadnit odhalení některých funkčních problémů
- zejména u exponovaných systémů se vyplatí zaznamenávat spíš více než méně, a to i záležitosti související s bezpečností jen nepřímo
- **základní důvody**
  - účel proaktivní – průběžné vyhodnocování
  - účel detektivní – záznamy ukládáme pro dohledání incidentů v budoucnu

DCIT

Praktická úskalí systémového auditu (1)

Absence skutečné potřeby

- prioritou obvykle funkčnost+dostupnost (ta se nezvýší)
- systém má sice certifikát C2 („naše alibi“), ale režim, v němž je provozován, je tomu hodně vzdálen

Dopad na výkonnost systému

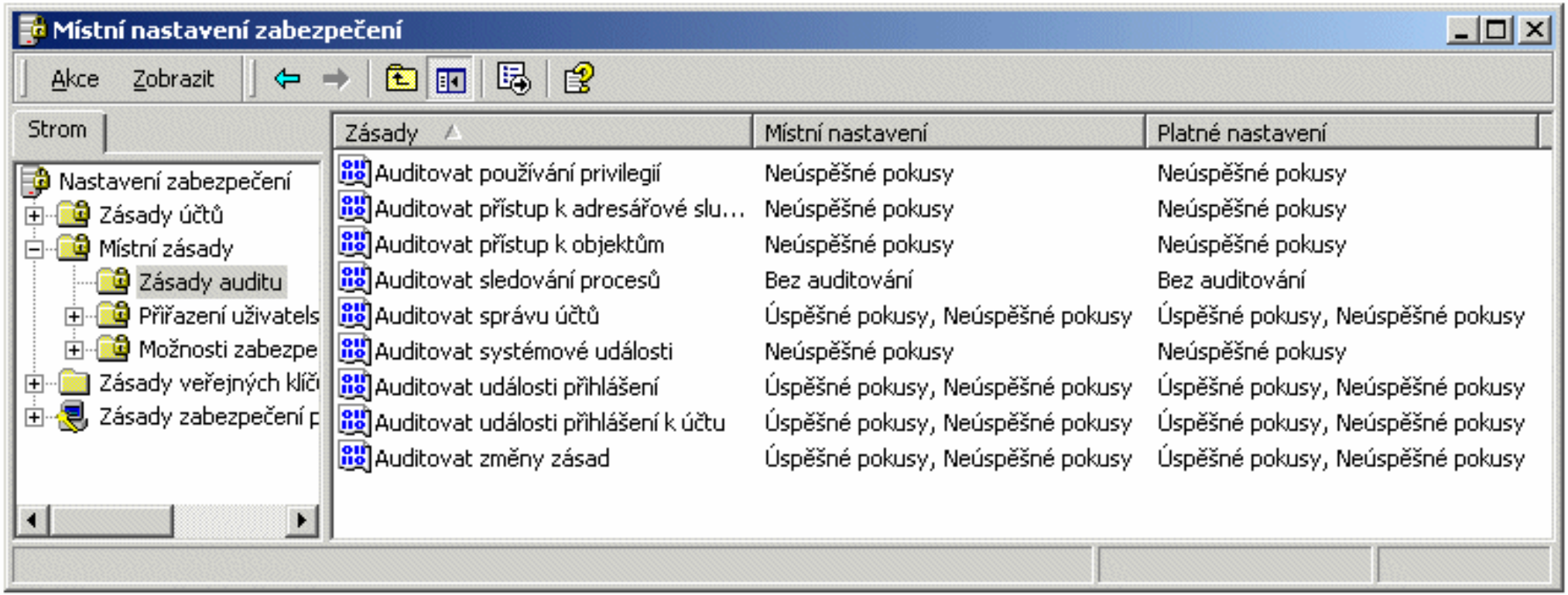
- nejčastější záminka proč audit nepoužívat
- aktivace syst. auditu systém „nezrychlí“, nicméně téměř vždy lze nalézt kompromis (ovšem dá to práci)

Vysoká náročnost administrace

- nastavení je velmi specifické pro danou situaci
- viz ukázka

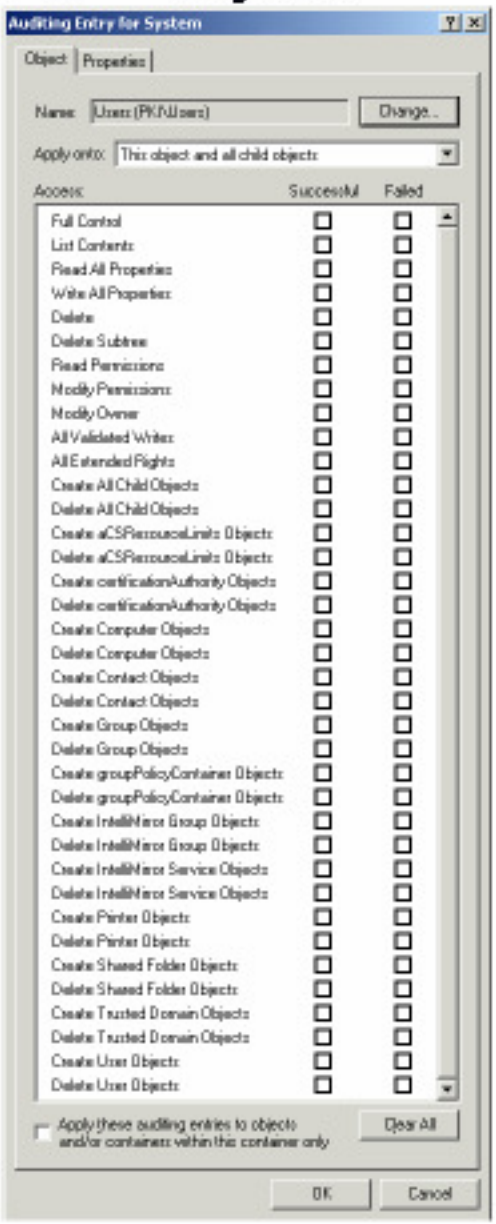
DCIT

MS Windows 2000 - Auditing

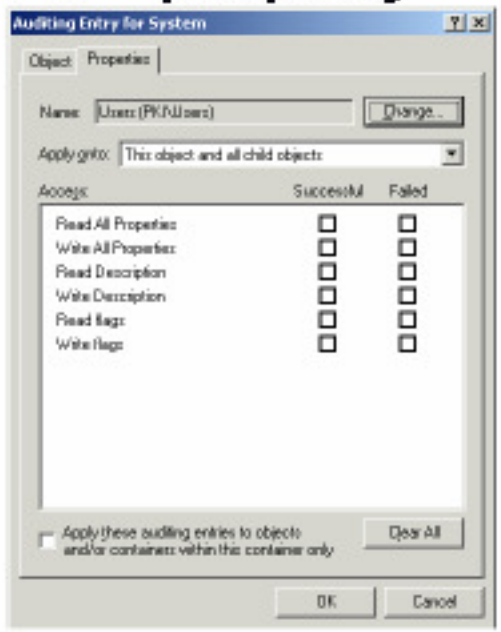


tím však nastavení systémového auditu pouze začíná .....

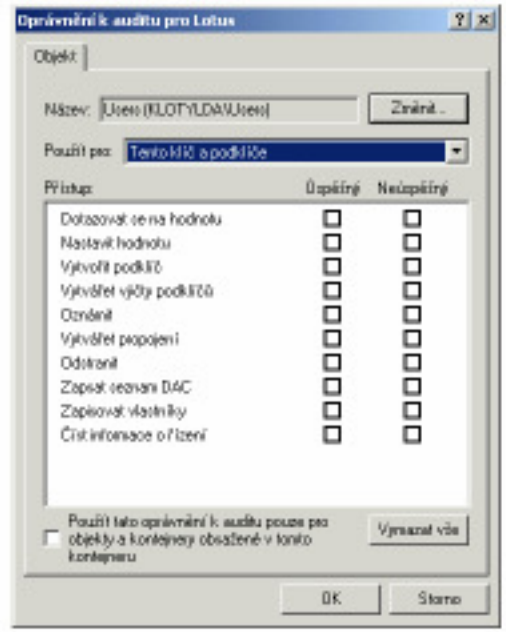
AD - object



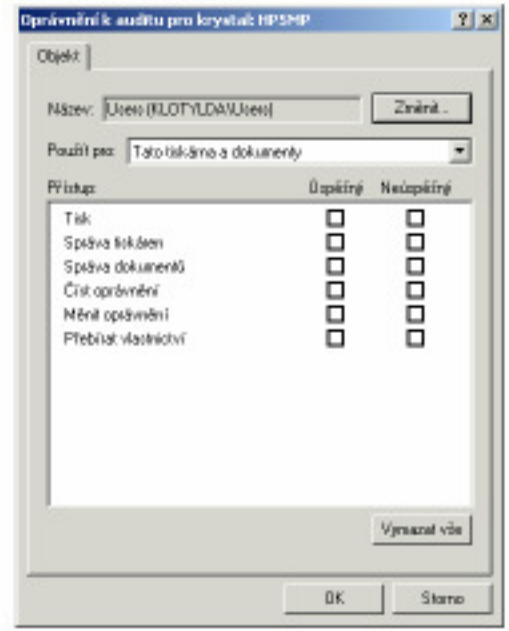
AD - property



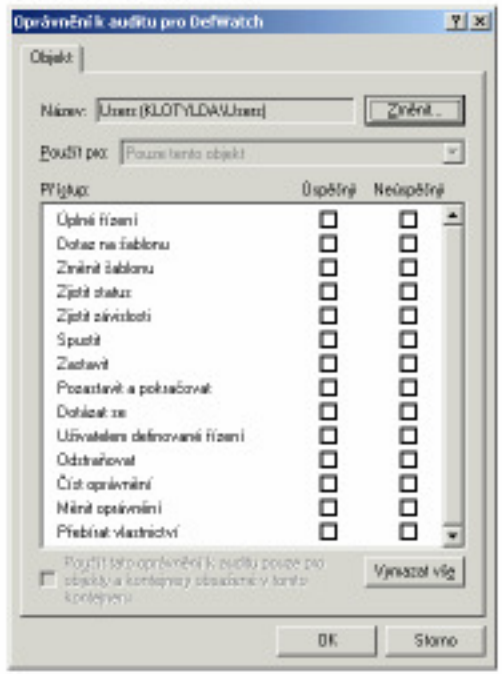
Registry



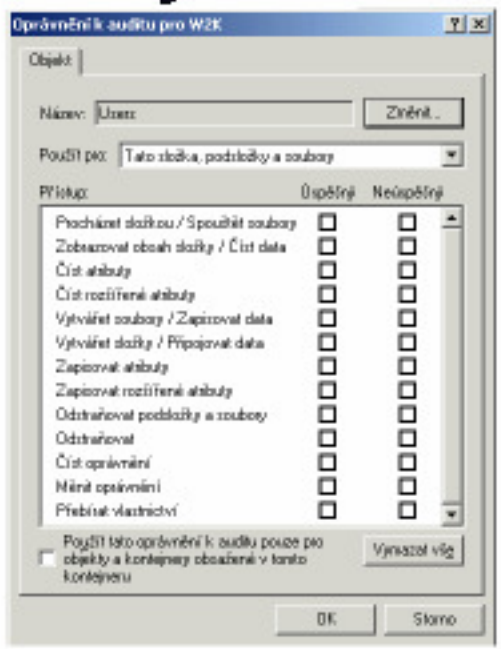
Printers



Services



Filesystem



Praktická úskalí systémového auditu (2)

Vypovídací hodnota záznamů

- často získáme velmi podrobnou informaci, s téměř nulovým praktickým přínosem
- často tvůrci systémů přenáší problém na uživatele – *„umožníme zaznamenat kdykoli, cokoli, jen si vybrat“*

Zpracování záznamů

- obvykle jsou záznamy pořízeny a uloženy (v lepším případě) pro dohledání incidentů v budoucnu
- průběžné zpracování vyžaduje nasazení speciálního produktu, a to i v relativně malém prostředí (obvykle nevystačíme se standardními prostředky)
- řešení existují, to optimální se hledá obtížně (cena – výkon – přínos)

DCIT

Praktická úskalí systémového auditu (3)

Nejen technické, ale i organizační aspekty

- provoz systému není jen o technickém nastavení, ale také o souvisejících procesech
- filozofie – co chceme vědět? informovat uživatele?
- strategie – rotace, ukládání, archivace záznamů
- administrace systému – oddělení rolí
- manipulace se záznamy mimo systém
- možnost fyzického přístupu/manipulace se systémem
- relevantní provozní dokumentace
- kontrolní mechanizmy

DCIT

Shrnutí

- význam pořizování důkazního materiálu jako základní funkci systémové auditu málokdo zpochybňuje
- v praxi je přesto využíván výjimečně (není-li standardně aktivován při instalaci)
- zavedení systémového auditu do praxe něco stojí (úsilí, čas, příp. peníze) a přináší komplikace
- je nutno jej vnímat jako jeden ze základních elementů zajištění bezpečnosti systémů v jejich provozu

DCIT

Otázky

kontakt: Karel Miko, miko@dcit.cz

DCIT