SYSTÉMOVÝ BEZPEČNOSTNÍ AUDIT

Autor článku: **Karel Miko – DCIT, s.r.o.**
http://www.dcit.cz

Článek zveřejněn v časopise **IT Systems** 5/2003
http://www.systemonline.cz

Úvod

Systémovým bezpečnostním auditem je v kontextu tohoto článku míněna funkcionalitu systémů (operačních systémů, databází, aplikací apod.), která umožňuje zaznamenávat klíčové události a stavy během provozu, přičemž se zároveň vyznačuje vysokou mírou odolnosti před zničením či pozměněním pořízených záznamů a lze o něm tedy hovořit jako o jakési „černé skříňce“ daného systému.

Systémový audit není záležitostí posledních dnů, jeho zásady a principy jsou známé a v řadě systémů implementované již řadu let, stejně jako je všeobecně znám jeho význam a hlavní přínosy. Původní myšlenkou, která stojí za systémovým auditem jsou bezpečnostní aspekty provozování IT systémů, neboť hlavní úkoly systémového auditu spadají do oblasti zaznamenávání bezpečnostních incidentů, pokusů o překročení stanovených přístupových práv atd. Dříve byl systémový audit otázkou poměrně úzkého okruhu speciálních systémů, s postupem času ovšem byla tato funkčnost implementována i do běžných systémů, ve kterých je sice dostupná, nicméně je pouze velmi zřídka využívána.

Základní terminologie

Jednoznačná a všeobecně rozšířená definice systémového auditu se hledá velmi obtížně, různé formy monitorovacích a logovacích mechanizmů jsou implementovány prakticky ve všech operačních systémech, databázových systémech a u většiny aplikací.

Při vymezení pojmu systémový bezpečnostní audit je zřejmě nejvhodnější vyjít z normy ISO/IEC 15408-2 (Common Criteria) nebo některých jejích předchůdců (ITSEC, TCSEC). Podle těchto norem: *Systémový audit by měl zahrnovat rozpoznávání, zaznamenávání, ukládání a analýzu informací souvisejících s aktivitami relevantními z hlediska bezpečnosti systému. Výsledné auditní záznamy pak mohou být použity ke stanovení, kdy nastaly ty které aktivity dotýkající se bezpečnosti systému a který uživatel je za ně zodpovědný.*

Z praktického hlediska je subsystém systémového auditu povinnou součástí všech systémů a aplikací certifikovaných např. pro stupeň 4 EAL (Evaluation Assurance Level) dle ISO 15408 nebo dříve pro třídu bezpečnosti C2 dle TCSEC – což je případ většiny komerčních operačních systémů (Windows 2000, Solaris, HP-UX, AIX, Tru64 Unix apod.), ale také řady databázových systémů (Oracle, Sybase, Informix aj.). V této souvislosti je však nutno zdůraznit, že má-li systém příslušný certifikát, neznamená to automaticky, že je za všech okolností bezpečný, nýbrž zjednodušeně řečeno k tomu má všechny předpoklady – tj. má např. zmíněný auditovací subsystém, ovšem to, je-li aktivován nebo ne, je plně v rukou provozovatele systému.

Proč auditovat?

Obecně lze auditní záznamy považovat za „důkazní materiál“ potřebný pro dohledání událostí a aktivit v rámci šetření bezpečnostních incidentů nebo řešení nestandardních stavů. Základní důvody pro systémový audit lze rozdělit následovně:

- Účel detektivní – zaznamenáváme vybrané události s tím, že záznamy uchováváme pro účely dohledání příčin zjištěných bezpečnostních incidentů někdy v budoucnu. Tento způsob je v praxi nejčastější.
- Účel proaktivní – pořizované záznamy jsou průběžně zpracovávány (strojově či manuálně), na základě této průběžné analýzy jsou odhalovány incidenty, podezřelé stavy a jiné anomálie.

Primárním cílem systémového auditu bylo a je odhalení bezpečnostních incidentů jako např. neplatné pokusy o přihlášení, odmítnutí přístupu z důvodu nedostatku přístupových práv atd. Z hlediska bezpečnosti jsou ovšem zajímavé i události, při nichž nedochází k porušení definovaných práv a nastavené politiky (např. provedení některých nevratných operací, hromadná manipulace s daty, mazání dat).

Pořízené záznamy o chování systému či aplikace mohou také výrazně usnadnit vyřešené některých funkčních problémů, neboť v rámci auditu jsou rovněž zaznamenávány chybové a nestandardní stavy systému.

Pokud si navíc poctivě přiznáme, že i u renomovaných produktů existuje nezanedbatelné riziko napadení systému, kdy je útočník schopen se dostat do systému různými „postranními“ cestami, dojdeme k závěru, že obzvláště u exponovaných systémů se vyplatí logovat spíš více než méně.

Jak systémový audit funguje

Události zaznamenávané systémovým auditem jsou vždy velmi silně závislé na daném systému. Pochopitelně se kategoricky liší tyto mechanizmy např. u operačních systémů, databází a aplikačních systémů, nicméně i dva operační systémy mohou používat velmi rozdílné mechanizmy např. z důvodů různé architektury. Škálu auditovaných událostí bych si dovolil ukázat právě na případu operačního systému, kde se obvykle zaznamenávají následující typy událostí:

- Object Auditing – asi neobsáhlejší oblast auditu umožňující zaznamenávat prakticky libovolnou operaci s objekty (čtení, zápis, odstranění, …), přičemž objektem je nejčastěji soubor, tiskárna či jiný prostředek OS.
- Process Auditing – události související s životním cyklem procesu (vytvoření, ukončení, …).
- Account Auditing – události jednotlivých uživatelů systému (přihlášení, odhlášení, změna hesla atd.)
- Action/Event Auditing – zaznamenávání speciálních událostí, jako např. strartup/shutdown systému, manipulace s audit trailem, zásahy do bezpečnostní politiky systému apod.
- Syscall Auditing – u některých systémů je možno zaznamenávat některá systémová volání včetně použitých parametrů (používá se spíše pro ladící než provozní účely).

Samotný auditovací mechanizmus je zpravidla implementován přímo v jádře a pokud systém běží nelze jej prakticky nijak obejít (předpokládáme-li, že není chyba v samotné implementaci této části jádra). V řadě případů je pro využití jeho možností nutno aktivovat speciální subsystém – např. Basic Security Module (BSM) u Solarisu, OSFC2SEC u Tru64 Unixu nebo Trusted Computing Base (TCB) u HP-UX apod.

Z provozního hlediska je třeba zdůraznit, že systémový audit s sebou přináší jisté navýšení zátěže systému a není zcela jednoduché najít optimální nastavení z hlediska objemu zaznamenávaných informací a přiměřeného nárůstu zátěže.

Pořízené záznamy (audit trail) jsou případ od případu ukládány různě, přičemž právě způsob ukládání logů velmi výrazně ovlivňuje, do jaké míry budou pořízené záznamy chráněny před nežádoucí modifikací a bude tak zajištěna jejich nepopiratelnost. Několik příkladů:

- Soubor – v řadě systémů je pro zaznamenávání využíváno definovaného souboru umístěného přímo na souborovém systému, tento soubor bývá po celou dobu běhu systému exkluzivně otevřen aplikací či systémem, tudíž k souboru není možno přistupovat přímo (ani na čtení), ale pouze pomocí speciální systémové utility.
- Speciální diskový oddíl nebo speciální zařízení (např. /dev/audit) – toto bývá využíváno především na úrovni operačních systémů, kdy řízení přístupu k takto uloženým záznamům je implementováno přímo v jádře operačního systému. (je využíváno zejména u UNIXových systémů)
- Remote logging – pro ukládání auditních záznamů lze použít vzdáleného počítače, na který jsou záznamy přenášeny po síti, tento způsob přináší výhodu zejména v omezení možnosti zničení auditních záznamů (zahlazení stop), je tu však jisté riziko výpadku komunikační infrastruktury.

Závěr

Přestože možnost systémového bezpečnostního auditu v současnosti nabízí většina dostupných systémů, praktická zkušenost je taková, že v reálném provozu je systémový bezpečnostní audit používán jen velmi výjimečně. Důvody lze spatřovat především v tom, že většina systémů (u interních prakticky všechny) jsou provozovány s důrazem na funkčnost nikoli bezpečnost a provozování systémového auditu není vnímáno jako přidaná hodnota.

Objektivně řečeno však důsledné využívání této funkcionality s sebou přináší i řadu praktických úskalí jak v rovině technické – netriviální konfigurace, zvýšená zátěž; tak v rovině organizační – pořízené záznamy je nutno průběžně vyhodnocovat a aktivně využívat při odhalování a řešení bezpečnostních incidentů.

Zcela nepochybně však monitorování a zaznamenávání klíčových událostí, do níž systémový bezpečnostní audit spadá, patří mezi oblasti, které by měly být v každé organizaci v rámci řešení problematiky informační bezpečnosti jednoznačně pokryty.