

Audit přístupu k informacím – IBM Tivoli Compliance Insight Manager

Ostře sledované informace

V každé firmě jsou data, která by měla být přístupná pouze pověřeným osobám. Proto se programátoři aplikací snaží o maximální zabezpečení aplikací. Prakticky je ale obtížné precizně definovat oprávnění a nedá zakázat vše.

Také existují citlivá data, ke kterým musejí uživatelé občas přistoupit a nelze jim tento přístup odepřít, tak jako personál v hotelu má přístup do vašeho hotelového pokoje a jen těžko jim v tom můžeme zabránit. Když už tomu zabránit nemůžeme, je dobré o „podezřelých“ přístupech k citlivým informacím vědět.

Může se stát i vám

Dovolte mi jednu pravdivou příhodu. Nejmenovaný pan ředitel měl soubory s citlivým obsahem ve svém adresáři na firemním souborovém velmi dobře zabezpečeném serveru. Tyto soubory si nečestný IT správce potají kopíroval. Kdyžby se nezaplnil počítač, kam data stahoval, nikdy by se na to nepřišlo. Když totiž jiný správce zjišťoval, proč se na druhém počítači zaplnil disk, všechno mu došlo.

Dotyčný darebák si to tehdy odskákal a dotyčný ředitel se rozhodl pro používání softwaru, který dnes provádí audit přístupu uživatelů a administrátorů k citlivým informacím. Pokud by někdo měl v plánu provést podobný nekalý pokus, byl by ihned polapen.

Proč audit přístupu

Mimo to, že je z mnoha důvodů rozumné předcházet případnému zneužití dat, je audit přístupu k informacím v IT systémech některých firem ze zákona nařízen. Existuje několik mezinárodních standardů pro bezpečnostní

audit (např. BASEL II, SOX, PCI, ISO17799, SAS70, HIPAA, GLBA).

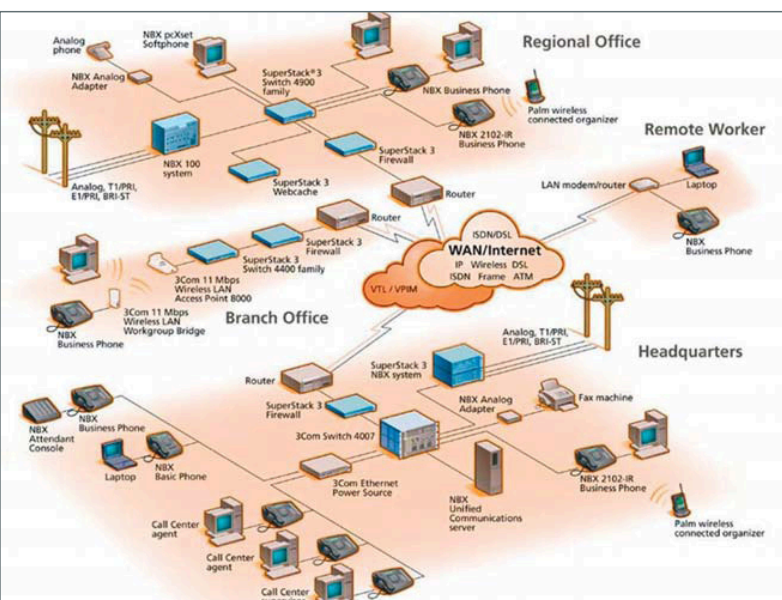
Zvládnout nároky kladené těmito auditovými standardy bez specializovaného softwaru je prakticky nemožné.

Na co se bezpečnostní auditoři ptají?

Především a nejčastěji jde o porušení ochrany osobních údajů, viz níže:

- Přistupují správci databáze k tajným informacím?
 - Nezneužívají oprávnění uživatelé osobní data?
 - Nezneužil nespokojený administrátor cizí účet (vydával se za někoho jiného)?
- Dále se auditoři ptají na porušení systémových bezpečnostních pravidel:
- Nebyly v systému provedeny neschválené změny?
 - Nevypnul některý administrátor bezpečnostní auditing/logování?
 - Nepromazal někdo bezpečnostní logy, kdy?
 - Kdo zastavil klíčové systémové procesy bez povolení?

Rovněž je zajímavá možnost zneužití pravomocí IT administrátory:



Trends 2006; USSS/CERT Insider Threat Survey 2005; CSI/FBI Survey, 2005; National Fraud Survey; CERT, various documents.)

- 87 % bezpečnostních incidentů uvnitř firem je konáno uživateli, kteří mají patřičná oprávnění přístupu.
- Mnohé jsou nedbalostním nebo neúmyslným porušením:
 - procesů pro provádění systémových změn (Change Management Process),
 - pravidel pro použití informací.
- Ostatní incidenty jsou záměrné a úmyslné:
 - odplata/pomsta (84 %),
 - zlý úmysl (92 %).
- Je velmi drahé tuto hrozbu ignorovat:
 - vnitřní útoky stojí v průměru šest procent hrubého ročního obrátu,
 - což jen v USA v době průzkumu znamená 400 bilionů dolarů

Pokud řešíte následující dilema, vězte, že je tento text psaný právě pro vaše zákazníky:

Potřebujete shromažďovat logy, ale nevím které logy uchovávat a jak. Obáváte se nevěnovat pozornost možnosti zneužití přístupu k informacím, ale technici nemají čas, vůli, někdy technickou dovednost pročitat často lidsky nesrozumitelné logy a vyhodnocovat jejich obsah. Potřebujete doložit existenci efektivního řízení bezpečnosti a reporting pro auditory, ale nemáte možnost porovnat bezpečnostní informace z mnoha zdrojů proti směrnici a reportovat podle auditových standardů.

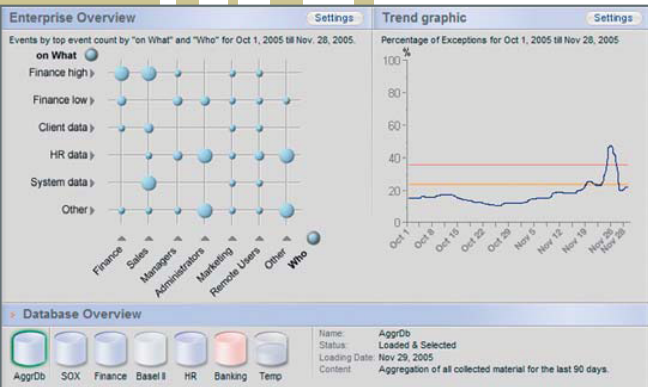
Uživatelé s oprávněním k přístupu incidentu



Zdroj: USSS/ERT Insider Threat Survey 2005

Koho se máme bát?

O tom, že sledování přístupu k informacím dnes již není možnost, ale nutnost, hovoří následující statistické údaje: (Zdroje: Forrester research, IdM



Kdo má na svědomí interní bezpečnostní incidenty?

Existuje jednoduché řešení?

Řešením pro vaše zákazníky by pro mohl být software IBM Tivoli Compliance Insight Manager (TCIM), který konsoliduje následující funkce:

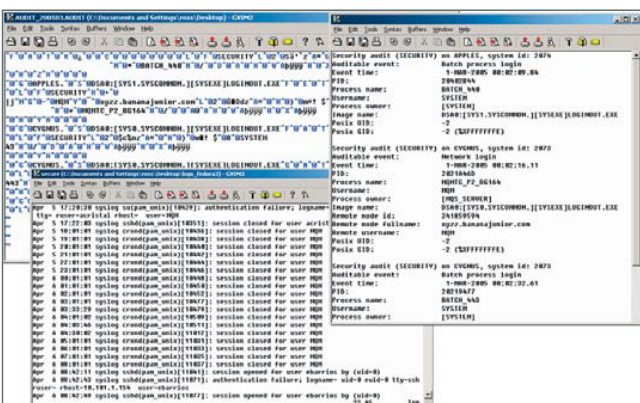
1. Zachycuje relevantní bezpečnostní a auditová data ze široké škály systémů včetně aplikací, databází, bezpečnostních zařízení a síťových zařízení.
2. Mechanismus „log continuity“ dohlíží na kvalitu a kompletnost kolekce systémových a aplikačních logů.
3. Korelace shromážděných dat je použita pro detekci potenciálních rizik. Tento bezpečnostní audit je realizován transformací událostí a alertů do patentovaného normalizovaného formátu „W7“ pro další analýzy (who, what, on what, where, when, from where, to where).
4. Poskytuje efektivní reporting, který je specifický podle role a typu aktivity uživatele systému.

Evidence přístupu k datovým objektům

Software IBM TCIM zjišťuje, kdo přistupuje a kam (např. ke kterým tabulkám v databázi, ke kterým souborům apod.), jakou operaci s datovými objekty dělá a odkud je připojen (např. jméno PC). Tyto údaje jsou prezentovány uživateli právě v jednotném normalizovaném formátu „W7“ (who, what, on what, where, when, from where, to where).

Analýza bezpečnostních rizik

Nasbírané události bezpečnostního charakteru systém TCIM vyhodnocuje pomo-



Někdy je opravdu těžké analyzovat bezpečnostní logy

ci korelačních pravidel. Pravidla se definují pro nestandardní přístupy k datům. Pokud nastane situace, která je v rozporu se standardním chováním uživatele podle korelačních pravidel, je na tuto událost upozorněno pomocí zabudovaných notificačních nástrojů. Nestandardní přístupy k datům jsou znázorněny a na první pohled evidentní také v grafu přístupu „compliance dashboard“.

Compliance dashboard je korelací mezi uživatelskými rolemi v systému a datovými skupinami/objekty (HR systémy, finanční systémy, systémové objekty apod.). Tyto kategorie jsou uživatelsky definovatelné.

K rozkrývání eskalovaného bezpečnostního incidentu na agregované úrovni je možno pomocí aplikace TCIM procházet do detailu až po zobrazení dílčí podezřelé akce uživatele včetně možnosti interaktivně zobrazit systémové či aplikační logy, které byly zdrojem pro tuto informaci. Detailní pohled na akci zobrazuje ve výše zmíněném formátu W7. V případě Active Directory například, když administrátor „Admin“ vytvořil uživatele „Pokus“, kterému přednastavil členství ve skupině „Administrators“, nebo že uživatel „User“ si zkopíroval soubor smlouva.doc z domovského adresáře uživatele „Reditel“.

Dalším analytickým přístupem zabudovaným v software IBM TCIM je tzv. PUMA analýza – „Privileged User Monitoring and Audit“. PUMA analýza detekuje neoprávněný přístup administrátorů k objektům, které nemají tito privilegovaní uživatelé číst či modifikovat, ale není možné jim fyzicky zabránit v přístupu.

Sledování administrativních zásahů

IBM TCIM průběžně sleduje činnost systémových, aplikačních a databázových administrátorů při jejich zásazích do systému.

Pokud dojde k jakékoliv změně v nastavení bezpečnosti, nastavení uživatelů a jejich oprávnění, nebo v jiném přednastavení systému, je tato akce evidována a posouzena v rámci korelační pravidel, zda není ve sporu se směrnicemi pro změny v systému.

Sledování kontinuity bezpečnostních logů

Protože hlavním zdrojem informací o akcích a změnách v systému jsou pro IBM TCIM logy (au-

diology, syslogy, tracelogy), je nutné zajistit, aby logování nebylo úmyslně pozastaveno, upraveno, nebo podvrhnuto.

- výrazně zvýší bezpečnost,
- usnadní a zefektivní práci uživatelů,
- usnadní a zefektivní správu uživatelů v IT,
- minimalizuje náklady spojené s požadavky na odemčení účtů a reset hesel,
- podporuje mezinárodní standardy,
- je cestou k úspěšnému bezpečnostnímu auditu,
- je pro malé i velké.

diology, syslogy, tracelogy), je nutné zajistit, aby logování nebylo úmyslně pozastaveno, upraveno, nebo podvrhnuto.

K tomuto účelu slouží analytický nástroj „Log Continuity Dashboard“. Přestože není možné takovému nekalému počínání oprávněných správců zabránit, IBM TCIM dokáže



takové zásahy spolehlivě detekovat a reportovat. Takový zásah pak je notifikován jako významný bezpečnostní incident.

Sledování běhu procesů

IBM TCIM lze nastavit pro sledování nepřetržitého běhu bezpečnostních procesů či programů na severech.

Archivace systémových a bezpečnostních logů

IBM TCIM shromažďuje záznamy monitorovaných logů a archivuje tyto záznamy pro zpětnou analýzu. V archivu logů lze prohledávat jak na úrovni jejich neupraveného znění, tak i ve formátu „W7“.

Reporting a standardy

Součástí IBM TCIM je nástroj pro reporting auditních údajů pro účely bezpečnostního auditu. Je možné použít certifikované moduly pro reporting podle mezinárodně uznávaných standardů ISO17799, SOX, BASELII, SAS70, HIPAA, GLBA, PCI.

Ideální neexistuje

Ideální je všechno zakázat. Z praxe ale víme, že to není možné. IBM Tivoli Compliance Insight Manager nám pomůže sledovat nežádoucí zásahy a přístupy k informacím a předcházet velkým finančním a morálním újmám.

Ing. Petr Klabeneš, Avnet Technology Solutions, IBM Software Business Development Manager. Mobile: +420 602 663 351, e-mail: petr.klabenes@avnet.com