IT BEZPEČNOST

správa a využití privilegovaných účtů

Mezi časté úkoly řešené v rámci IT bezpečnosti je dokazování nevhodného nebo protiprávního chování uživatele počítačového systému. Běžná praxe je taková, že jsou ke zkoumání předány počítače zaměstnanců, kteří využívali systémy pro neautorizované přístupy do zákaznických databází nebo uzavírali nestandardní smlouvy na poskytované služby. Cílem následující stati je nastínit možná řešení pro přístup k prvkům kritické IT infrastruktury pomocí privilegovaných účtů.

Případy neloajálních řadových uživatelů počítačových systémů jsou relativně jednoduché a při správné kooperaci mezi odděleními vyšetřování, prevence kriminality a IT jsou vyřešeny během několika málo dní. Zásadní pro vyšetřování je analýza přístupů k systémům počítačové infrastruktury a korelace dat ze SIEM systémů. Problém při vyšetřování nastává v případě, že se neprovinil běžný uživatel, ale jeden nebo více administrátorů. To zejména z důvodů možnosti potlačení odpovědnosti při zneužití privilegovaných účtů (administrátorských účtů), nebo uživatelských hesel natvrdo zanesených do uživatelských nebo serverových aplikací. Každý počítačový systém, počínaje operačním systémem pro pracovní stanice, přes síťová zařízení, virtualizační systémy až po databázové služby, má vlastní administrátorský účet. Pravomoci těchto účtů se ne vždy daří personalizovat pro konkrétní osoby a je nutné privilegované účty sdílet mezi více osobami. Potom vyvstává problém možného zneužití privilegovaných oprávnění k získání interních informací, k jejich zničení nebo znepřístupnění. Navíc lze zkomplikovat následné vyšetřování odstraněním záznamu o událostech.

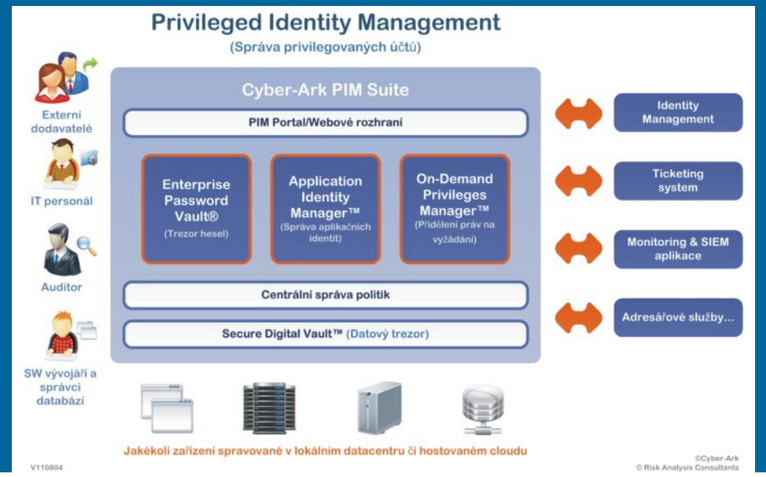
Zmíněné problémy vytvořily poptávku po systémech umožňujících sdílení privilegovaných účtů při dodržení tří hlavních podmínek. První a nejdůležitější podmínkou je bezpečné uložení hesel – datový trezor je určen pro ukládání privilegovaných účtů, to znamená, že jakákoli kompromitace dat v něm uložených by přímo ohrožovala fungování kritické firemní IT infrastruktury. Další podmínkou je řízení přístupů k jednotlivým účtům uložených v trezoru, zejména se jedná o přístupy k databázím obsahujícím zákaznické informace. Tyto systémy mohou podléhat schvalování přístupu další osobou nebo skupinou osob. Třetí podmínka je zásadní v případě auditu počítačových systémů – zde je kladen důraz na bezpečné logování s garancí ochrany před úpravou zaznamenaných logů.

Základem celého systému je trezor. Ten bývá technicky řešen jako vyhrazený síťový operační systém bez síťových služeb vyjma služeb trezoru. Jádro systému tvoří šifrovaná databáze vyhrazená pouze pro ukládání dat spjatých s funkcí trezoru. Uživatelské rozhraní a funkce jsou z důvodu zvýšení bezpečnosti systému jako celku přesunuty na další servery. Aplikace na dalších serverech zajišťují funkci centralizované správy privilegovaných účtů, záznam aktivit spojených s těmito účty a prosazování definovaných bezpečnostních politik.

Primární výhodou centralizované správy privilegovaných účtů je snadná korelace událostí. Pokud se v pracovním prostředí vyskytuje více platforem a každá z nich má vlastní systém logování událostí a jejich správy, může nastat situace, kdy organizace zjistí, že disponuje velkým množstvím dat, která ovšem nedokáže korektně interpretovat. Řešením bývá centralizace logů, to ovšem samo o sobě problém neřeší a nad centralizovanými daty je nutno zavést další procesy, které budou data přijatelně interpretovat nebo se k takové interpretaci alespoň přiblíží. Moderní systémy pro správu privilegovaných identit podporují různé platformy od MS Windows, Unix, GNU/Linux, přes databáze, síťové přenosové prvky až po webové administrační portály jednotlivých zařízení. Díky této podpoře je možno centralizovaně logovat události důležité pro auditování správy a využití privilegovaných účtů.

Bezpečnostní politiky definují procesy správy a řízení přístupů k uloženým privilegovaným účtům. Každá organizace má definovatelnou skupinu počítačových systémů, které jsou kritické pro její běžný provoz. Privilegované účty k těmto systémům mohou vyžadovat detailnější řízení přístupů formou schvalování další osobou nebo skupinou osob. Běžnou praxí je schvalování přístupu ke kritickým systémům pro administrátory na juniorských pozicích, zkušenější administrátoři mohou získat přístup automaticky po vyplnění formuláře a udání důvodu přístupu k danému systému. Neméně důležitou funkcí politik je řízení životního cyklu hesel privilegovaných účtů, kterým se definují plánované změny a komplexita hesel. Životní cykly hesel mohou být časově definovány v rozmezí měsíců až po jednorázová hesla pro zajištění maximální bezpečnosti.

O záznamu událostí jsem se již zmínil. Ale co když záznamy o jednotlivých událostech nejsou dostatečně průkazné? V takovém případě je nutno přidat další vrstvu ve formě vizuálního záznamu aktivních sezení. Vizuální záznam znamená, že veškeré akce, prováděné s privilegovaným účtem od chvíle přihlášení se ke koncovému systému až do odhlášení, jsou nahrávány formou videozáznamu. Ten je následně uložen do šifrované centrální databáze pro případ šetření negativní události nebo pro případ auditu bezpečnosti. Novým trendem pro auditování záznamů je syntaktická analýza událostí a jejich korelace s vizuálními záznamy. Možnost korelovat události s vizuální informací je velkou výhodou při auditech bezpečnosti počítačových systémů pracujících s citlivými daty.



Instalace systémů pro správu privilegovaných účtů je pro každou organizaci velkou výzvou, nejen z pohledu autonomnosti spravovaných systémů kritické informační infrastruktury, ale i z procesního hlediska. Je potřeba správně definovat a rozdělit odpovědnost k jednotlivým spravovaným systémům, a to i k samotnému systému správy privilegovaných účtů. Do tohoto procesu je potřeba zanést odpovědnost za vytváření bezpečnostních politik a jejich úprav pro maximální využití systému a minimalizaci dopadů pro jednotlivé administrátory.

Po úspěšné implementaci získá organizace centralizovanou evidenci privilegovaných účtů s integrovanou správou záznamu událostí, včetně analytických nástrojů ke snadnému splnění regulatorních požadavků pro bezpečnostní audity a certifikace. Nástroje správy administrátorských účtů přinášejí absolutní a neupravitelný přehled nad všemi operacemi provedenými administrátory, včetně videozáznamů. Detailní správa politik definující životní cykly hesel a řízení přístupů k jednotlivým privilegovaným účtům umožňuje nastavit různé úrovně bezpečnosti. Po úspěšné implementaci bude organizace schopná zjistit, kdo, za jakých podmínek a jakými nástroji prováděl úpravy v kritických systémech informační infrastruktury a tyto informace snadno transformovat do auditní zprávy nebo zprávy šetření incidentu.

Ing. Jiří Hološka, Ph.D.

Poznámka redakce

Autor pracuje ve společnosti Risk Analysis Consultants, s. r. o., na pozici forenzní analytik / konzultant informační bezpečnosti.

KALENDÁRIUM

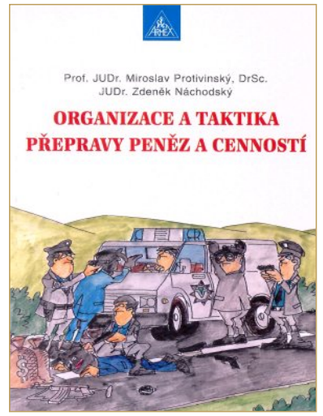
ZAJÍMAVÝCH AKCÍ

Navštívili jsme…

… ZAJÍMAVÝ VZDĚLÁVACÍ KURZ

pro přepravce hotovosti a cenných zásilek, který připravila na 22. květen 2012 společnost TRIVIS – Centrum profesní přípravy, s. r. o. Účast na této zajímavé akci byla nabídnuta rovněž členským firmám KPKB ČR. Kurz vedl JUDr. Zdeněk Náchodský, známý odborník a autor několika odborných publikací o problematice bezpečnosti a organizace převozu peněz a cenin.

Každý z účastníků kurzu obdržel výukový materiál „Organizace a taktika přepravy peněz a cenností" renomovaných autorů prof. JUDr. Miroslav Protivinského, DrSc., a JUDr. Zdeňka Náchodského.



A ještě navštívíme…

… DISKUSNÍ PANEL

odborného časopisu Facility manager na téma PROFESIONÁLNÍ OCHRANA MAJETKU A OSOB. Tato mimořádná akce je určena zástupcům státní správy a samosprávy, developerům, architektům, provozovatelům administrativních a rezidenčních objektů, kulturních a sportovních komplexů, facility manažerům nemocnic, obchodních a administrativních center, strategických objektů, zástupcům bankovního sektoru, bezpečnostním manažerům, zástupcům bezpečnostních agentur a poskytovatelům security služeb, bezpečnostním poradcům a analytikům, vývojářům a v neposlední řadě i výrobcům a prodejcům zabezpečovacích systémů.

Diskusní panel je rozčleněn na bloky:

- ochrana osob a majetku
- profesionální zabezpečení finančních, administrativních, rezidenčních a strategických objektů
- cenová politika v oblasti security (výhodná cena versus dodržení všech bezpečnostních požadavků)
- současné požadavky na bezpečnost a zabezpečení
- cenová politika v oblasti security (výhodná cena versus dodržení bezpečnostních požadavků)
- kategorie a systémy zabezpečení (zákony v praxi)
- zvláštní služby (převozy peněz, uměleckých děl, ochrana VIP apod.)

Akce je plánována na 21. červen 2012 a konat se bude v sále Malostranské besedy na pražském Malostranském náměstí.

Bližší informace:

Email: info@wagner-press.cz, Tel.: +420 224 256 676

Členové Komory podniků komerční bezpečnosti ČR

Česká ochranná služba, a. s.
Velká 2984/23
702 00 Ostrava
www.coska.cz

Agentura Pancéř, s. r. o.
Nad Šárkou 2551/6a
160 00 Praha 6
www.pancer.cz

Loomis Czech Republic a. s.
Poděbradská 186/56
198 21 Praha 9 - Hloubětín
Managing cash in society.

ELZA-TECH, s. r. o.
Tišická 396/1
181 00 Praha 8
www.elzatech.cz

ROTWYG spol. s r.o.
Černokostelecká 5
100 00 Praha 10
www.rotwyg.cz

HENIG – security servis, s.r.o.
5. května 797
470 01 Česká Lípa
www.henig.cz