Data v péči

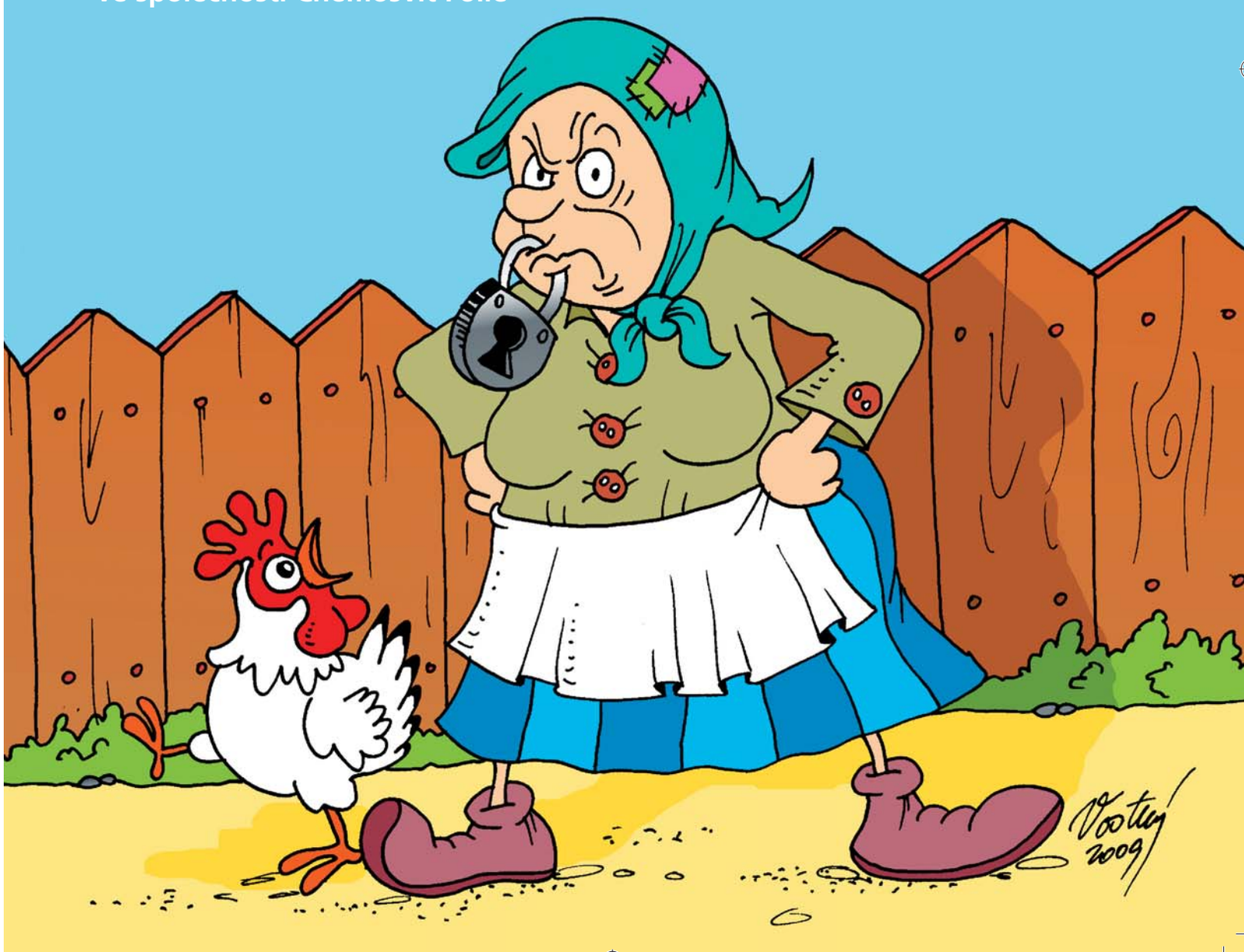
MHM

ČÍSLO 16 | PROSINEC 2009 | MHM COMPUTER A. S.

Proč zavést
identity a access management

Bezpečnost dat
u diskových a archivních systémů Hitachi

Bakbone NetVault
ve společnosti Chemosvit Folie



Bezpečnost informací trochu jinak

Každý jistě četl romány či povídky z období první republiky. Postava obecního pošťáka či strážníka věděla vše o obyvatelích „své čtvrti“. Na vesnicích věděli všichni všechno a nic nebylo utajeno zraku hodné sousedky. Krásné časy, hlavně proto, že ti, co všechno věděli, nikomu nic neřekli a „svá tajemství si s sebou vzali do hrobu“ aby, jak praví autor, „nepřivedli někoho do neštěstí“. Prostě idyla.

Zároveň však jiní spisovatelé začali psát science fiction romány a povídky popisující totální manipulaci se společností, kdy privilegovaná vrstva („alfy“, „členové strany“ nebo jen „vyvolení“) ve jménu Všeobecného Dobra řídila společnost. Všeobecné Dobro však nebývalo tak všeobecné a týkalo se vlastně jen té vládnoucí vrstvy. Není důležité, jaké technické prostředky vládnoucí vrstvy pro ovládání lidí v románech používaly, důležité je, že všechny zákony a nařízení, které sloužily pouze vládcům, byly vždy prezentovány jako ochrana a zlepšení života pro ovládané.

Ze všech těchto románů jaksi navíc vyplývá, že základem umožňujícím absolutní manipulaci byla (mimo jiné) absolutní informovanost vládců. O všem a o každém. O každém se vědělo vše. Jak se chová, zda je zdráv, jakými nemocemi trpí, z čeho má strach, co si kupuje, kdy, proč a kam jezdí, co dělá ve svém volném času, co čte a co si myslí. A zvláště se vědělo o tom, když jednotlivec dělal něco, co nebylo povoleno.

Od doby těchto románů se svět vyvinul a technologicky pokročil. V zájmu boje proti kriminalitě se instalují sledovací kamery, pro ulehčení placení používáme platební karty, abychom se lépe domluvili, používáme mobilní telefony. Aby nás lékaři mohli lépe léčit, sestavují se databáze popisující naše nemoci a diagnózy. Pro naše dobro se mají do aut instalovat identifikační systémy záchranného volání. Vytváří se databanky DNA. Jsme nadšeni sociálními sítěmi na internetu a bez rozpaků zde o sobě sdělujeme všechny informace: co máme rádi a co ne, jaké máme přátele, jakou práci hledáme, co jsme četli a co se nám nelíbí. Stovky satelitů sledují a fotografují zemi v rozlišení, o kterém průměrný občan nemá ani tušení.

Souběžně se sbíráním informací pracují vědecké týmy na systémech, které mají umožnit jejich zpracování a vyhodnocení. Avšak vždy s dobrými úmysly. Například identifikace osob zachycených kamerou slouží pro lepší rozpoznání závadových osob (např. teroristů). Automatická identifikace automobilu (eCall, zatím pouze při nehodě) poslouží k záchraně lidských životů. Kamery na silnicích přispějí k bezpečnosti provozu.

Jsem si téměř jist, že 99,99 % lidí ani netuší, jaké informace jsou o nich sbírány, v jakých databázích jsou uloženy a kdo je sbírá. A hlavně kdo a jak je využívá. Do těchto 99,99 procent zahrnuji jak sebe, tak bohužel i většinu pracovníků všech úřadů pro ochranu osobních dat na celém světě.

Vím ovšem, že idealizované časy 19. století se nemohou vrátit. Nelíbí se mi však kamery, databáze biometrických údajů, které vznikají při překročení hranic států, nelíbí se mi, že telefonní společnosti zaznamenávají, odkud a kam telefonuji, nelíbí se mi, že někdo sleduje jaké webové stránky si čtu, nelíbí se mi ani eCall. A co se mi zvláště nelíbí, jsou tvrzení, že vše je zaváděno pro naše Dobro nebo že kdo nedělá nic zakázaného, ten se přece nemusí ničeho obávat. Kdo ví, co nám přinese budoucnost. Doufám jen, že se nedožijeme éry Všeobecného Dobra.

Martin Miloschewsky

Vyhrajte s MHM!

DÁMSKÁ KOŽENÁ PENĚŽENKA ČEKÁ NA ŠŤASTNÉHO VÝHERCE.
PODROBNOSTI A SOUTĚŽNÍ OTÁZKU HLEDEJTE NA STRANĚ 15.

Data v péči MHM

Občasník
Vydáno: prosinec 2009
Neprodejné
Vydává:
MHM computer a. s.
U Pekáren 4
102 00 Praha 10 – Hostivař
telefon: +420 267 209 111
fax: +420 267 209 222
www.mhm.cz

Ve spolupráci s časopisem Computerworld
ve vydavatelství IDG Czech, a. s.

COMPUTERWORLD

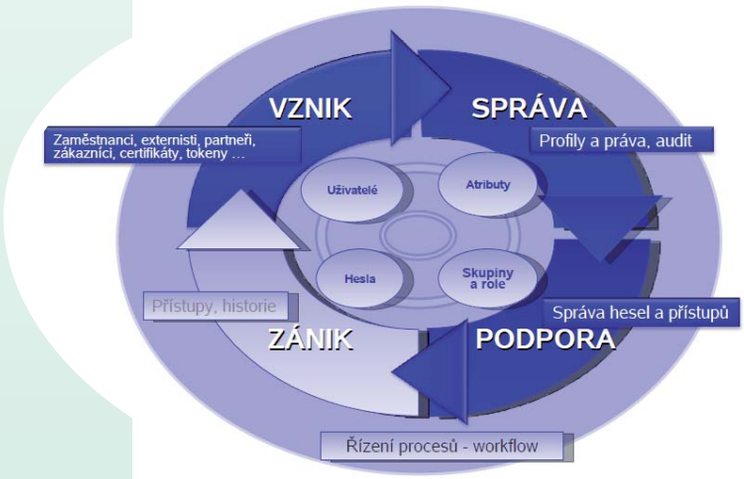
Obálku ilustroval Mirek Vostrý.
Připomínky a náměty pište na
redakce@datavpeci.cz, případně na adresu vydavatele.

ISSN 1803-604X

Proč zavést identity a access management

Hlavním úkolem identity a access managementu (IAM) je stanovit a řídit, kdo a k jakým informacím bude mít v rámci informačního systému společnosti přístup v určitém časovém období. IAM procesy zahrnují vytváření identit pro jedince přistupující ke zdrojům informačního systému a jejich asociaci s uživatelskými účty jednotlivých systémů a aplikací, které organizace využívá. Nedílnou součástí IAM jsou rovněž nástroje umožňující komplexní auditování a monitoring. Co bylo kdysi jednoduchou záležitostí, se však postupem času stalo rostoucím problémem.

Jedním ze zdrojů rostoucí komplexity při řízení identit a přístupových práv je skutečnost, že ve většině společností existuje heterogenní prostředí zahrnující větší množství aplikací na různých operačních systémech s IT službami poskytovanými jak centrálně, tak distribuovaně. Každá platforma či aplikace pak vyžaduje vlastní správu uživatelů a přístupových oprávnění, což činí celý proces jejich správy komplikovanější. Ke zdrojům informačního systému navíc přistupují nejen vlastní zaměstnanci, ale rovněž další skupiny uživatelů, jako jsou zákaz-



Životní cyklus identit

níci, dodavatelé či partneři, přičemž samotný přístup se může realizovat několika různými způsoby, například přes terminál, klient-server či webové rozhraní. Decentralizovaná správa identit uživatelů a jejich privilegií prostřednictvím manuálních postupů nejen značně zatěžuje správce systémů, ale rovněž není sto zajistit patřičnou úroveň informační bezpečnosti společnosti na úrovni definované například mezinárodním standardem ISO27000. Identity a access management přinášejí řešení uvedených problémů prostřednictvím důsledné centralizace správy identit a privilegií v rámci jejich životního cyklu.

Proces správy uživatelů a oprávnění sleduje několik hlavních cílů, které tvoří hlavní důvody pro implementaci řešení IAM.

DODRŽOVÁNÍ ZÁKONNÝCH POŽADAVKŮ

Řízení přístupů k informačním aktivům je jednou ze stěžejních oblastí informační bezpečnosti. Regulatorní rámec Sarbanes-Oxley tak například požaduje, aby byly organizace schopny zajistit oddělení odpovědností při vykonávání specifických kontrolních činností a prokázat, kdo měl přístup k určitým údajům a jakým způsobem je zpracovával. Basel II ukládá povinnost monitorovat operační rizika včetně neoprávněných přístupů ke klíčovým datům a informačním systémům. To vyžaduje implementaci nástrojů, které umožňují monitorování a auditování přístupů jednotlivých uživatelů k objektům informačního systému. Předpisy v oblasti ochrany osobních údajů pak ukládají povinnost omezit uživatelům přístup k osobním údajům pouze na ty, které bezprostředně potřebují k vykonávání svých pracovních funkcí.

VYŠŠÍ BEZPEČNOST INFORMACÍ

Implementace IAM umožňuje vytvořit standardní prostředí pro řízení bezpečnosti informací napříč celou organizací. Zlepšuje se tak schopnost včasného odhalení rizik a incidentů neoprávněných vstupů do IS. Rovněž se eliminuje riziko přístupů uživatelů, kterým již autorizace ke vstupu do systému vypršela, nebo došlo ke změně jejich uživatelských práv.

KONTROLA NÁKLADŮ A ZVÝŠENÍ EFEKTIVITY

Při decentralizované uživatelské správě je nutné spravovat identity a oprávnění zvlášť na každém systému, což vyvolává vysoké náklady na administraci. Rovněž velké množství volání na helpdesk se vztahuje k řešení problémů s přístupy do jednotlivých aplikací například z důvodu zapomenutých hesel nebo požadavků na umožnění přístupu k novým aplikacím či funkcím. Neexistují-li v organizaci centrálně spravované popisy rolí definující přístupová oprávnění, trvá při přijetí nového zaměstnance mnohdy i několik týdnů, než jsou mu umožněny základní přístupy do IT systémů.

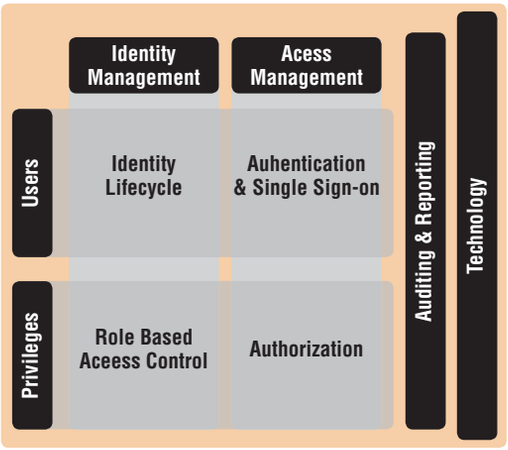
ZVÝŠENÍ EFEKTIVITY

K zajištění efektivního fungování správy přístupů je potřeba centrální a napříč platformami jdoucí automatizovaný systém pro uživatelskou správu a správu přístupů, který je založen na rolích definovaných z hlediska potřeb byznysu. Systém musí umožnit přizpůsobit se podnikovým procesům a převést rutinní administrativní funkce i rozhodování ze správců na uživatele a jejich vedoucí pracovníky, aby rozhodnutí o tom, co uživatelé skutečně potřebují, činily osoby, které to nejlépe vědí. Zavedení IAM umožňuje rovněž efektivní plánování softwarových licencí, protože společnost disponuje přesnými informacemi v podobě mapy aplikací pracovních pozic ohledně toho, jaké aplikace využívají zaměstnanci při své pracovní činnosti.

SPOKOJENOST UŽIVATELŮ

Při decentralizované správě uživatelů a přístupů si musejí uživatelé pamatovat mnoho různých hesel. Vezme-li se navíc v úvahu nutnost hesla obměňovat

při jejich expiraci, stává se management přístupů pro uživatele těžko zvladatelný. Zavedení IAM je tak důležitým faktorem, který ovlivňuje spokojenost všech uživatelů.



Dimenze IAM

KONCEPCE IAM

Identity a access management se skládá ze tří oblastí. První, tvořící jádro IAM, je centrální funkcionalita managementu identit a přístupových práv. Druhou oblastí jsou podpůrné funkce v oblasti reportingu a auditování. Třetí oblast představuje technologická platforma, která tvoří podloží pro obě výše uvedené oblasti funkcionalit. Centrální IAM funkcionalita může být nahlížena ze dvou odlišných perspektiv, z pohledu dat a z pohledu provozně-funkčního. Z pohledu dat se jedná o informace o uživatelských identitách a oprávněních. Z pohledu provozně-funkčního je IAM možno rozdělit na administraci identit a přístupových oprávnění a na prosazování pravidel a politik (například autorizace či autentizace) v reálném čase. Administrativní část IAM se zpravidla označuje jako „Identity Management", zatímco „Access Management" je odpovědný za prosazování pravidel a politik. Obrázek na této stránce zobrazuje všechny dimenze IAM.

ARCHITEKTURA ŘEŠENÍ

V současnosti jsou na trhu dostupné balíčky řešení identity a access managementu od několika velkých nadnárodních společností. IAM řešení zpravidla obsahuje tyto základní komponenty:

Centrální úložiště identit – autoritativní zdroj uživatelských informací pro všechny aplikace a systémy, poskytuje základ pro centralizované řízení přístupů. Centrální úložiště identit zpravidla obsahuje:

- informace o uživatelích (jméno, příjmení, osobní číslo, pracovní pozice, e-mail, tel. číslo…)
- informace o stavu uživatelských účtů v systému
- informace o aplikacích a systémech
- informace o všech rolích a skupinách i o atributech na úrovni aplikací
- organizační strukturu a její provázání s aplikačními rolemi
- přiřazení rolí na úrovni organizace a rolí na úrovni aplikací k jednotlivým uživatelům

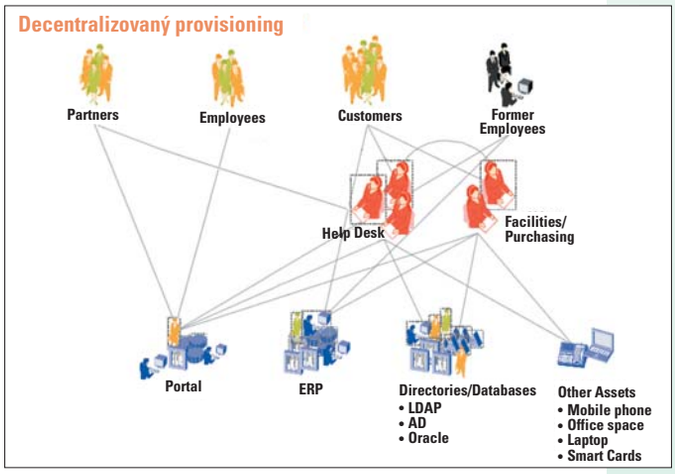
Meta-adresářové služby – služby, prostřednictvím kterých je centrální úložiště identit provázáno s ostatními aplikacemi. Slouží k propojení a integraci dat souvisejících s identitou z jednotlivých subsystémů do centrálního úložiště. Meta-adresářové služby umožňují distribuované vlastnictví takto vzniklé „virtuální identity" všemi ostatními systémy a aplikacemi. K propojení s jednotlivými aplikacemi je využíváno celé škály adaptérů, konektorů a agentů.

Nástroje k managementu identit a přístupů – úkolem těchto nástrojů je centrální administrace uživatelských identit, rolí a oprávnění, hesel, workflow, samoobslužných služeb atd. prostřednictvím jediné aplikace. Řadí se sem rovněž nástroje pro audit a reporting identit a přístupů.

Workflow (schvalovací procesy) – funkcionalita IAM, která slouží k tomu, aby povolování rolí a přístupových oprávnění probíhalo uživatelsky přívětivou formou. Prostřednictvím workflow provádějí povolování rolí a přístupových oprávnění ti, kdo jsou za ně zodpovědní, tedy zpravidla nadřízení, a nikoliv ti, kdo rozumí IT technologiím (administrátoři systémů).

FUNKČNÍ RÁMEC IAM

V následující části si popíšeme hlavní funkcionality IAM řešení a nejdůležitější kroky, které organizace musí učinit k tomu, aby těchto funkcionalit plně využívala.

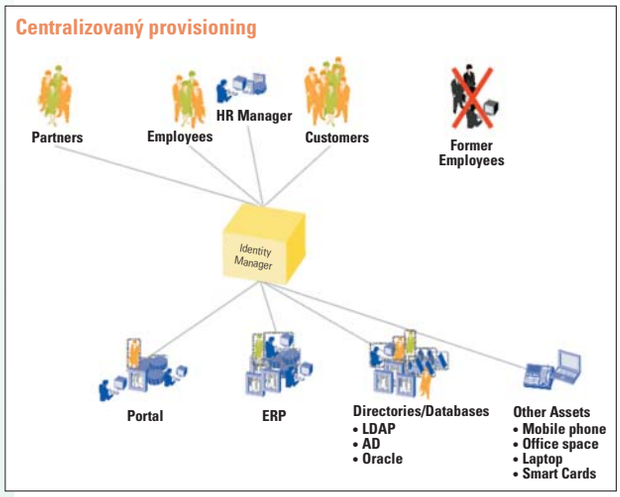


Management identit a přístupů

Identity management musí vzít v potaz všechny formy identit, které se v organizaci vyskytují. To mohou být identity fyzických osob, které přistupují k IT zdrojům organizace, ale také identity, které se neváží k fyzickým osobám, jako jsou účty aplikačních služeb či účty IT hardwarových zařízení. Management identit probíhá v rámci jejich celého životního cyklu, od vytvoření identity, jejího modifikování až po její smazání. Každá identita je popsána definovanou soustavou identifikátorů či atributů a je asociována s aplikačními účty, ke kterým přistupuje. Identity lze vytvářet manuálně prostřednictvím vlastních nástrojů IAM řešení nebo je lze exportovat a synchronizovat z jiných zdrojů identit, jako například HR, CRM nebo ERP systémů.

Provisioning

Pod pojmem provisioning se rozumí funkce IAM řešení spočívající zpravidla v on-line poskytování informací o identitě a o přístupových právech ostatním systémům v jimi požadované podobě. Systém správy identit zajišťuje řízené a kontrolované provedení požadovaných operací závislých na změnách, které se dotýkají identity nebo její reprezentace, v koncových systémech.



Správa privilegií, skupin, oprávnění a rolí

Privilegia jsou obecným pojmem pro různé způsoby přístupových práv. Jsou přidělována uživatelům buďto manuálně na základě workflow, nebo automaticky na základě prováděcích směrnic. Poté, co se privilegia promítnou prostřednictvím provisioningu do cílových systémů, ovládají jejich přístupová práva. Privilegia bývají realizována skupinami, oprávněními a rolemi. Skupina, jako základní stavební jednotka systému privilegií, představuje soubor přístupových práv v jednom cílovém systému. Je-li uživatel členem skupiny, má přístupová práva, která jsou této skupině přiřazena. Skupinu lze přiřadit uživateli přímo nebo prostřednictvím oprávnění a rolí. Oprávnění je střední článek systému privilegií, který spojuje soubor skupin z jednoho nebo více cílových systémů. Role je nejvyšším stupněm modelu privilegií, který organizaci umožňuje strukturovat přístupová práva dle byznys rolí. Kontrola přístupu na bázi rolí (RBAC – Role Based Access Control) je vhodná pro naplnění regulatorních požadavků na oddělení pravomocí (SoD – Segregation of Duties), kdy je vyžadováno, aby určitý pracovní úkon či operace byla autorizována dvěma či více osobami.

Uživatelská samoobsluha, delegovaná správa, správa hesel

Většina enterprise řešení IAM obsahuje funkce pro samoobslužnou správu uživatelů. K samoobslužným funkcím patří:

- změna osobních údajů
- změna či obnovení hesel
- požadavek na přidělení privilegií
- delegování přístupových práv na jiné uživatele

Delegovaná správa v IAM zahrnuje proces správy uživatelských účtů a přidělování privilegií jiným uživatelům. Například vedoucí projektu může přiřadit či odebrat přístupová práva členům projektového týmu.

Správa hesel je v centralizovaném konceptu IAM autentizována tak, aby každý uživatel musel udržovat pouze jedno heslo, jehož změna je ihned propagována do všech relevantních IT systémů organizace. Je důležitá přítomnost funkce upozornění uživatele na nutnost změny hesla v souladu s politikou ochrany hesel.

AUTENTIZACE A AUTORIZACE, SINGLE SIGN-ON

Autentizace a autorizace patří mezi hlavní funkcionality řízení přístupů (Access Management). Autentizace uživatele je proces, ve kterém je uživatel systémem identifikován a ověřen jako platný uživatel. Autorizace je pak proces, který určuje, které aktivity budou uživateli v IT systému povoleny na základě přístupových práv přiřazených k uživatelské identitě.

Autentizace osob se dá provádět na základě:

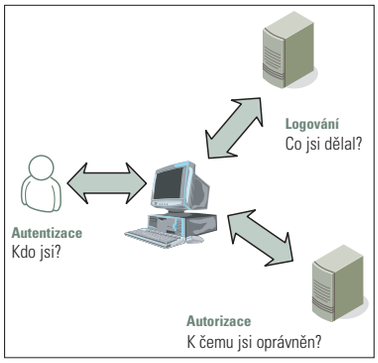
- určité znalosti (heslo, šifrovací klíč)
- vlastnictví nějakého předmětu (mechanické klíče, magnetické karty, USB token)
- určité fyzické vlastnosti uživatele (otisk prstu, dlaně, obraz očního pozadí, hlasu apod.)
- provedení požadované akce (dynamika podpisu, dynamika psaní na klávesnici)

Podle počtu použitých autentizačních metod se autentizace dělí na jednofaktorovou, dvoufaktorovou a třífaktorovou. Třífaktorová kombinuje například použití hesla, vlastnictví USB tokenu a ověření otisku prstu.

Komplexní řešení IAM dnes zpravidla zahrnuje také funkcionalitu SSO (Single Sign-on), která umožňuje centrální identifikaci a ověření uživatele v jednom kroku pro všechny IT systémy. SSO bývá v IAM doplněn centralizovanou autorizační službou pro všechny aplikace.

LOGOVÁNÍ, MONITOROVÁNÍ A AUDIT

Každý dodavatel řešení IAM zakomponoval do svého balíčku řešení jiný soubor monitorovacích a auditních nástrojů. K běžným monitorovacím a auditním funkcím dnes patří například schopnost auditovat vznik, změny či zánik uživatelských účtů a k nim přiřazených oprávnění, monitorovat neúspěšná přihlášení do systému a změny hesel, poskytnout rychlý přehled všech oprávnění určitého uživatele či jejich skupin, reportovat uživatele dle aplikací, platforem a uživatelských rolí, nebo identifikovat spící účty.



PODMÍNKY ÚSPĚŠNÉHO ZAVEDENÍ IAM

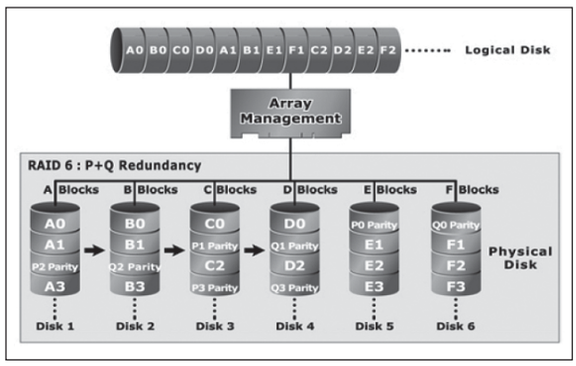
Mnoho společností vnímá zavádění IAM jako jednorázový IT projekt, místo aby byl vnímán jako trvale probíhající program řízení oblasti identit a přístupů, přičemž zanedbává vytváření vize a strategického plánování, což typicky vede k zanedbání kritických součástí úspěšné realizace IAM, mezi které patří:

- získání podpory nejvyššího vedení pro zavádění IAM
- jasná vize a strategie programu IAM
- plán realizace založený na postupných krocích
- zahrnutí business požadavků a zohlednění kultury společnosti
- robustní projektový management

Jaroslav Fojtík, Convenio Consulting

Bezpečnost dat u diskových a archivních systémů Hitachi

Na bezpečnost uložených dat můžeme pohlížet ze dvou různých úhlů. První směřuje ke způsobu, jakým jsou ukládaná data chráněna před jejich ztrátou v případě selhání hardwaru. Druhý úhel pohledu zkoumá, jak jsou uložená data chráněna před jejich zcizením, podvržením nebo smazáním. Někde na pomezí obou leží takzvaná správa uživatelů, kteří mohou spravovat samotný diskový nebo archivní systém. Metody používané ke kompletní ochraně dat, zohledňující obě zmíněná stanoviska, pracují na hardwarové úrovni a v tomto článku si představíme ty, které používají diskové a archivní systémy renomovaného výrobce Hitachi.



Bezpečné uložení dat je u Hitachi vždy na prvním místě a všechny ostatní funkce jsou tomu podřízeny. Pokud například diskový systém vlivem nějaké poruchy nemůže garantovat bezpečné uložení „cachovaných“ operací write, sám vypne funkci cachování dat v paměti cache a data se budou ukládat přímo na disky diskového systému – aktivuje se tzv. Write Through mód. To sice sníží výkonnost celého diskového systému, ale je garantováno bezpečné uložení dat. Bezpečnostní mechanismy starající se o bezpečné uložení dat jsou u Hitachi implementovány již od nejnižší úrovně, od samotného zápisu dat na fyzický disk. Zde Hitachi nezapisuje standardních datových 512 bajtů jako většina konkurentů, ale přidává k nim svoji paritní informaci o velikosti 8 bajtů. Další podobnou funkcí pracující na této nízké úrovni, navrženou speciálně pro SATA (Serial ATA) disky, je funkce write & compare. SATA disky jsou známé svou menší spolehlivostí v porovnání s FC (Fibre Channel) nebo SAS (Serial Attached SCSI). Proto Hitachi každý zápis na SATA disky překontroluje.

Jednotlivé fyzické disky jsou na vyšší úrovni organizovány do tzv. raidových skupin. Hitachi podporuje raidové skupiny typu: RAID 0 (stripe), RAID 1 (mirror), RAID 1+0, RAID 5 a RAID 6. Protože RAID 0 není fault tolerant, tedy v případě výpadku jediného disku v konfiguraci RAID 0 dochází ke kompletní ztrátě všech dat, Hitachi nedovoluje konfiguraci RAID 0 na SATA discích. Jednotlivé typy RAID byly již v našem časopise jednou probírány, proto se k nim nebudeme dále vracet – až na RAID 6. Ten je kombinací stripovaného zapisování dat s generováním dvou různých paritních informací (viz obrázek). Díky těmto dvěma paritám RAID 6 chrání uložená data před výpadkem až dvou fyzických disků a společnost Hitachi byla jednou z těch, které se zasloužily o standardizaci RAID 6. RAID 6 je primárně navržen pro použití na velkokapacitních SATA discích. Jak již víme z předchozího odstavce, SATA disky jsou méně spolehlivé, ale zato velmi objemné (v současnosti 1 TB, příští rok 2 TB). V případě výpadku jednoho fyzického disku je raidová skupina RAID 6 stále fault tolerant, data jsou tedy chráněna před výpadkem dalšího disku.

Jiné RAID typy (např. RAID 5) přestávají být ve stejné situaci fault tolerant (raidová skupina není chráněna) a výpadek dalšího disku představuje ztrátu dat. Aby diskový systém minimalizoval dobu, po kterou není raidová skupina chráněna, okamžitě po výpadku fyzického disku aktivuje tzv. spare disk (náhradní disk) a data ze selhaného disku jsou na tento disk rekonstruována. Jakmile je tento proces dokončen, stává se postižená raidová skupina opět fault tolerant. Problémem však zůstává skutečnost, že proces rekonstrukce je značně časově náročný (u 1TB disků to jsou desítky hodin), a po tuto dobu nejsou data chráněna, navíc ostatní fyzické disky postižené raidové skupiny jsou zatěžovány procesem rekonstrukce. V kombinaci se SATA disky toto představuje značné riziko výpadku dalšího disku a ztráty dat. Právě tato skutečnost stála za zrodem RAID 6, který v těchto situacích minimalizuje riziko ztráty dat.

O úroveň výš data dále chrání zrcadlení cache paměti. Zrcadlení dat se aplikuje pouze na zapisovaná data (write IO). Za normálních okolností (bezchybný stav) jsou write IO operace zapisovány do cache paměti použitého řadiče (kontroleru), následně zrcadlena do cache paměti párového řadiče, a teprve až když existují dvě nezávislé kopie těchto dat, je write IO operace potvrzena a může být generována další. Teprve později jsou tato data uložena z cache paměti na fyzické disky. Před výpadkem proudu jsou cache paměti chráněny dvěma nezávislými bateriemi, které jsou schopny uchovat data v cache paměti po dobu 48 hodin. V případě, že diskový systém není schopen garan-

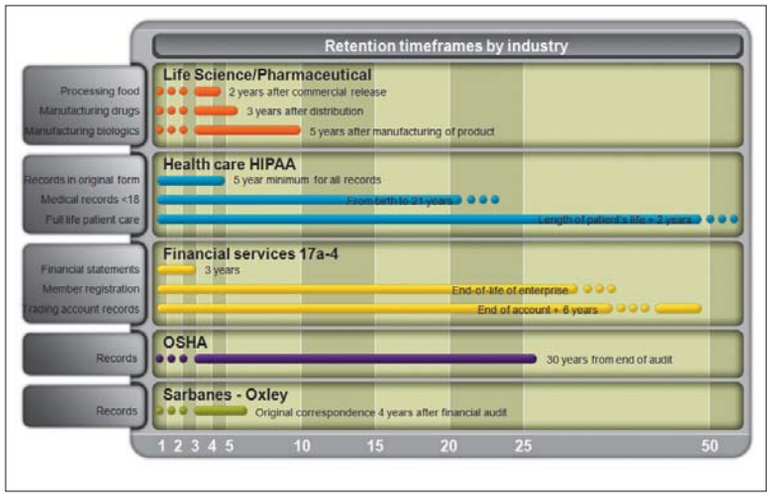
tovat existenci dvou „cache“ kopií (selhání cache paměti nebo celého řadiče) nebo následné bezpečné uložení dat z cache na fyzické disky (selhání obou cache baterií), dojde k přepnutí diskového systému do write through režimu a write IO operace jsou zapisovány přímo bez cachování na fyzické disky.

OCHRANA PŘED ZCIZENÍM A ZMĚNOU

Na úrovni řadičů, konkrétně backend direktorů, má Hitachi v současnosti implementovánu funkci šifrování dat pouze na enterprise systémech. Šifrování se provádí na hardwarové úrovni diskového systému, zapisovaná data jsou on-line šifrována a v zašifrované podobě ukládána na fyzické disky diskového systému. Tím jsou chráněna před zcizením fyzického disku a následným obnovením.

Funkce zabraňující podvržení dat nebo pozdější účelné modifikaci dat se u Hitachi jmenuje Data Retention. Je to volitelná funkce diskových systémů umožňující nastavit retenční periodu, tj. dobu, po kterou nemohou být data smazána nebo změněna v řádu dnů, roků nebo navždy. Po jejím nastavení nelze retenční periodu zkrátit nebo odstranit. Akceptované je pouze prodloužení již nastavené retenční periody. Funkce Data Retention na diskových systémech pracuje na úrovni celých LUNů (Logical Unit), je nezávislá na typu operačního systému a je certifikována, tudíž může být použita pro účely auditu ve všech prostředích.

Pro účely archivace dat má Hitachi speciálně navržené řešení HCAP (Hitachi Content Archive Platform), které umožňuje nastavovat retenční periodu na úrovni archivovaných souborů v řádu sekund, minut, hodin, dnů, měsíců a roků. Lze nastavit takzvanou absolutní retenci, tedy explicitní nastavení data a času, dokdy nebude možné archivovaná data měnit nebo smazat (například 6. 10. 2077). Nebo může být retence nastavena relativně, například 20 let, 5 dnů, 6 hodin a 23 minut od data archivace. Podobně jako u diskových systému ani v HCAP nelze retenční periodu zkrátit nebo odstranit. Retenční periodu lze pouze prodloužit. HCAP také podobně jako diskové systémy podporuje šifrování dat.



HCAP je digitální archiv schopný archivovat data po velmi dlouhou dobu (50, 100 let). Za tímto účelem obsahuje další funkce a mechanismy ochraňující archivovaná data. Jednou z nich je funkce DPL (Data Protection Level). DPL určuje počet (1, 2, 3 a 4) interních bezpečnostních kopií archivovaných souborů. Jednotlivé DPL kopie jsou rozmístěny a udržovány na různém hardwaru tak, aby v případě výpadku jednoho hardwaru byla vždy dostupná jiná kopie. Počet funkčních DPL kopií je neustále monitorován. V případě, že je interních kopií nedostatek (vlivem poruchy), je automaticky vytvořena další interní kopie tak, aby počet odpovídal nastavení DPL. V opačném případě (odstranění poruchy), kdy je počet interních kopií větší než nastavení DPL, dojde k redukci na správný počet.

Velmi důležitá funkce týkající se bezpečnosti dat je bezpečné smazání dat, tzv. shredding. Tato funkce zabrání obnovení smazaných dat. Princip této funkce spočívá v tom, že oblast smazaných dat je následně několikrát přepsána jinými, různými daty. Uživatel má možnost zvolit si metodu, jak bude smazaná oblast následně přepisována. Standardní nastavení je, že se smazaná oblast přepíše nejdříve nulami, potom jedničkami a na závěr náhodnými hodnotami. Hitachi má funkci bezpečného vymazání data jak pro diskové systémy, tak i pro digitální archiv HCAP.

SPRÁVA UŽIVATELŮ

Poslední záležitostí zmíněnou v úvodu je správa uživatelů, kteří mohou spravovat diskový systém nebo digitální archiv, a tudíž nesou jistou míru zodpovědnosti za bezpečnost uložených dat. V prvé řadě je nutno zmínit, že pokud chceme naše data maximálně ochránit, je třeba povolit přístup k diskovému nebo archivnímu systému pouze proškolenému odpovědnému personálu. K tomuto účelu lze na diskových a archivních systémech Hitachi vytvořit každému spravujícímu uživateli jeho účet (user name, password) s příslušným oprávněním a auditovat všechny provedené operace. Tyto účty jsou spravovány na úrovni diskového systému nebo archivu, v tomto případě se jedná o lokální účty. Hitachi také podporuje tzv. remote (vzdálené) účty, spravované v MS Active Directory nebo RADIUS serverem. To usnadňuje život především lidem spravujícím bezpečnost uživatelských účtů.

Bezpečné uložení dat v případě systémů Hitachi bylo, je a vždy bude na prvním místě. Ostatní funkce jsou tomu podřizovány. Hitachi neustále pracuje na zdokonalování existujících ochranných mechanismů a vyvíjí další nové funkce chránící data před jejich ztrátou, zcizením, smazáním nebo modifikaci. V novém roce budou určitě představeny další z nich. Máme se tedy na co těšit.

Radim Petržela, MHM computer

Hitachi Data Systems – leader v oblasti bezpečnosti storage řešení

V roce 2005 kybernetický zločin poprvé překonal profitabilitu ilegálního obchodu s drogami. Pokuty za nediskrétní zacházení s daty jsou na vzestupu a zároveň se rozšiřuje okruh citlivých dat. Když nahlédneme do novin, zjistíme, že regulatorní a právní požadavky se valí ze všech stran a ovlivňují ochranu a zabezpečení dat. Vládní organizace používají komerční sítě ke své činnosti v situaci, kdy se kybernetická válka odehrává mezi vojenskými, politickými a kriminálními protivníky. Jaká jsou tedy obranná opatření, která mohou pomoci udržet v bezpečí obchodní, průmyslová a vládní data? Kde začíná bezpečnost pro vás?

STRATEGIE PRO BEZPEČNOST VAŠICH ULOŽENÝCH DAT

Hitachi Data Systems nabízí storage řešení, která podporují regulatorní požadavky na zabezpečení dat, nabízejí bohatou sadu funkcí pro jejich ochranu a pokročilé vlastnosti zabezpečení. Hitachi leadership je ve standardech a průmyslových fórech pevně etablován. Standardy jsou zastoupeny položkami, jako jsou například All Fibre Channel standards – ANSI/INCITS T11, IP storage, IP security, Transport Layer Security – IETF, Security in Storage Working Group (encryption & key export) – IEEE/P1619, Hardware roots of trust – Trusted Computing Group, U.S. cyber security standards – ANSI/INCITS CS1 a World Wide Web Consortium (W3C) – Key Web standards. Ke standardizaci a diskusi o bezpečnosti dále přispívají i různé skupiny v rámci Storage Network Industry Association (SNIA) a Distributed Management Task Force (DMTF), kterých se Hitachi velmi aktivně účastní.

Nejistota ohledně požadavku na bezpečnost stále existuje mezi mnohými dodavateli storage. Datová agregace, konsolidace storage a nové technologie storage včetně SAN, NAS, WAFS vzdálených replikací atd. se zaměřují na oblast dostupnosti dat, avšak zpravidla nikoliv již na kontrolu přístupu, integritu a požadavky na utajení. Bezpečnost je často téměř ignorována. To však není případ výrobce storage zařízení Hitachi Data Systems, jehož specialisté se zaměřují rovnoměrně na obě důležité oblasti: storage a security.

COMMON CRITERIA JAKO UNIFIKOVANÝ MEZINÁRODNÍ BEZPEČNOSTNÍ STANDARD PRO IT

Common Criteria představují výsledek mezinárodního snažení o standardizaci a podporu sjednocení a vývoje existujících evropských a severoamerických bezpečnostních kritérií. Common Criteria projekt harmonizuje normy ITSEC, CTCPEC (Kanada) a US Federální kritéria (FC) do sjednocených Common Criteria for Technology Security Evaluation (CC). Tato kritéria jsou používána pro ohodnocení produktů a systémů a pro definici bezpečnostních požadavků pomocí standardu. Postupně nahrazují národní a regionální kritéria celosvětově standardem ISO15408. Common Criteria byla navržena za účelem sjednocení existujících standardů tak, aby společnosti prodávající IT do oblasti obrany nebo zpravodajských služeb prováděly vyhodnocení bezpečnosti pouze proti jednomu standardu. Common Criteria byla původně akceptována zeměmi, jako jsou Kanada, Francie, Holandsko, Velká Británie a USA, postupně se však přidávají i další, zvláště země okruhu NATO. Common Criteria poskytují jistotu, že procesy specifikace, implementace a evaluace bezpečného IT produktu byly prováděny pečlivým a standardním postupem.

ZÁKLADNÍ DEFINICE BEZPEČNOSTI SYSTÉMU STORAGE

Porozumění vyvíjejícímu se jazyku bezpečnosti storage pomůže všem, kteří se zabývají vývojem a implementací bezpečnostních řešení včetně bezpečnostních požadavků specifických pro prostředí storage. Některé základní pojmy definované asociací SNIA (Storage Network Industry Association) jsou uvedeny níže:

- Storage System Security (SSS) – zabezpečení vnitřních operačních systémů a aplikací spolu s integrací IT a bezpečnostní infrastruktury, jako jsou například externí autentizační služby, centralizované logování a firewally.
- Storage Resource Management (SRM) – bezpečné přidělování, monitorování, ladění, re-alokace a řízení storage zdrojů tak, že data mohou být ukládána a používána. Zahrnuje veškerý storage management.

- Data In-Flight (DIF) – zabezpečení důvěrnosti, integrity a/nebo dostupnosti dat během přenosu po storage, LAN nebo WAN síti.
- Data At-Rest (DAR) – zabezpečení důvěrnosti, integrity a/nebo dostupnosti dat uložených na serverech, diskových polích, zařízeních NAS, zálohovacích knihovnách a dalších médiích (zejména páskách).

POKROČILÁ OCHRANA DAT

Hitachi dnes poskytuje nejucelenější soubor služeb Storage Security, který odpovídá zvyšujícím se požadavkům korporací a vládních institucí na prokazatelnost, že data jsou fyzicky a logicky chráněna, jsou nezměnitelná, auditovatelná, a pokud je potřeba, tak i bezpečně skartovatelná.

Hitachi potvrzuje svůj zásadní závazek zajistit bezpečnost dat jako první prioritu při návrhu storage architektury. Jako příklad tohoto postoje můžeme uvést diskové pole Enterprise kategorie Hitachi Universal Storage Platform V (USP V) a jeho unikátní schopnost izolovat a oddělit aplikace vyžadující vysokou bezpečnost ve všech bodech storage hierarchie od portů přes cache až k diskům. Hitachi nabízí stálou podporu pro své zavedené a ve své třídě nejlepší služby na trhu v oblasti ochrany dat a bezpečnosti storage systémů. Tyto služby zahrnují bezpečné smazání dat (Data Shredding), funkce LUN Security pro zabezpečení přístupu k LUNům pomocí WWN, WORM (Write Once Read Many)

software pro dlouhodobou ochranu dat, přístupové služby založené na rolích, auditovatelný log soubor, do kterého se ukládá historie všech uživatelských přístupových operací na systému, Fibre Channel Secure Protocol Authorization A (FC-SP Auth A) pro autentizaci Fibre Channel zařízení a rovněž podporu pro šifrovací zařízení, jako jsou například NeoScale a Decru. Hitachi také získalo Common Criteria (ISO 15408) certifikaci pro svůj bezpečný software s funkcí logical partitioning. Virtual Partition Manager představuje jediný software na trhu umožňující partitioning, zajišťující, že data jsou zabezpečena proti přístupu mimo particii a také proti přístupu administrátorů jiných particií. Dále pouze zákazníci používající diskové pole Hitachi Universal Storage Platform V mohou získat garanci spolehlivosti a dostupnosti jedinečnou na trhu – 100% garanci dostupnosti dat.

KDE HITACHI STORAGE SYSTÉMY A SOFTWARE VYTVÁŘEJÍ OBRANNOU LINII

Bezpečnost dat je integrální součástí strategie společnosti Hitachi Data Systems poskytovat servisně orientovaná storage řešení (SOSS, Services Oriented Storage Solutions). Hitachi Data Systems věří, že storage systémy mohou představovat efektivní prvek strategie obranné linie a tím rozšířit schopnost organizace naplnit všechny zákonné a regulační požadavky při dosažení optimální infrastruktury pro ukládání dat. Pomocí strategie SOSS jsme schopni zajistit provozně odolnou infrastrukturu, která umožní našim zákazníkům splnit požadavky na bezpečnost dat a ochranu dat pomocí následujících funkcí, které zahrnují:

- Odpovědnost za vrstvu storage s rozšířenou autentizací, autorizací a auditováním logů
- Analýza slabých míst – nepřetržité skenování a analýza pro identifikaci operačních rizik
- Zajištění použitelnosti a jednoduchosti – bezpečnostní opatření s minimálním dopadem na produktivitu

Implementace ochrany dat:

- Dostupnost dat – replikační řešení typu „disaster recovery/business continuity", které zahrnuje synchronní a asynchronní kopie jak pro lokální, tak i pro vzdálený diskový systém
- Integrita dat – kontrolní součty, časová razítka a „read-after-write" Serial-ATA technologie

Umožnění bezpečnosti dat:

- Neměnnost dat – použitím technologie WORM, vytvoření nesmazatelných a nepřepsatelných dat pro danou časovou periodu
- Jednoznačně identifikovatelné objekty uložené v systému aktivního digitálního archivu HCAP (Hitachi Content Archive Platform) pro zajištění dlouhodobé neměnnosti dat
- Údržba dat – řízené vymazání nepotřebných dat (skartace dat)
- Utajení dat – technologie „data in-flight" a „data at-rest" šifrování s použitím externích zařízení
- Podpora zařízení pro šifrování dat – integrace s předními dodavateli na trhu
- Storage architektura, která umožňuje bezpečné a oddělené ukládání dat, logický partitioning a oddělení řídicích dat od vlastních dat
- Syslog přístup pro auditování logů
- Bezpečný interface pro správu zařízení založený na SMI-S standardech
- Nabídka Hitachi Data Systems Global Solution služeb založená na ITL standardech
- Bezpečná komunikace prostřednictvím interoperability s hlavními dodavateli v oblasti síťových zařízení pro zabezpečení „data in-flight" technologií
- Přístup ke kompletní řadě poznatků Hitachi z oblasti bezpečnosti, interface (CERT) a dalších unikátních technologií

Pro více informací, jak produkty a řešení od Hitachi Data Systems mohou pomoci naplnit vaše požadavky na bezpečnost dat, kontaktujte lokální obchodní partnery společnosti Hitachi Data Systems a/nebo navštivte webové stránky na adrese *www.hds.com/security*.

Hitachi Data Systems

Bezpečnostní novinky v systémech Windows Server 2008 R2 a Windows 7

OPERAČNÍ SYSTÉMY WINDOWS SERVER 2008 R2 A WINDOWS 7 SE VYZNAČUJÍ ŘADOU NOVINEK V OBLASTI BEZPEČNOSTI – MIMO JINÉ NAPŘÍKLAD STANDARDIZOVANOU PODPOROU BIOMETRICKÝCH ZAŘÍZENÍ NEBO ZMĚNAMI V UAC. V NÁSLEDUJÍCÍM TEXTU SE ZAMĚŘÍME NA TY NEJDŮLEŽITĚJŠÍ Z NICH. PROTOŽE V DOBĚ, KDY VZNIKL TENTO ČLÁNEK, JEŠTĚ NEBYLA K DISPOZICI FINÁLNÍ VERZE SYSTÉMŮ, JSOU NOVINKY POPISOVÁNY NA VERZI RC.

NOVINKY V BIOMETRICE

Až dosud nenabízel Microsoft ve Windows žádnou standardní podporu pro biometrická zařízení nebo biometrické aplikace, takže jste byli odkázáni jen na software výrobců těchto zařízení. To ztěžovalo uživatelům jejich použití a administrátorům jejich správu.

Windows 7 a Windows Server 2008 R2 obsahují Windows Biometric Framework, který zajišťuje jednotnou cestu pro používání čteček otisků prstů i jiných biometrických zařízení a poskytuje konzistentní rozhraní pro vyhledání a spouštění biometrických aplikací.

Konkrétně nabízí:

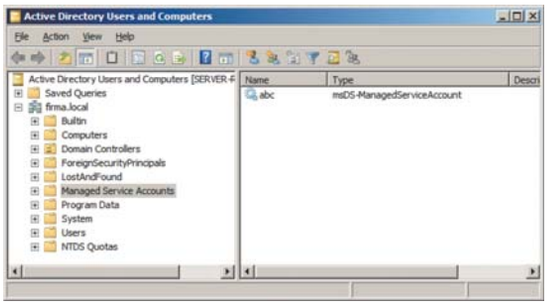
- V ovládacích panelech položku Biometric Devices, dovolující uživatelům kontrolovat dostupnost biometrických zařízení a zjistit, zda toto zařízení může být použito pro přihlášení k lokálnímu počítači nebo do domény.
- Biometrická zařízení nyní mohou být použita pro zvýšení oprávnění přes UAC.
- Pomocí Group Policy můžete povolovat, zakazovat nebo omezovat použití biometrických dat pro lokální počítač nebo doménu. Group Policy nastavení také mohou zabránit instalaci biometrického zařízení a jeho softwaru nebo jeho odinstalaci.
- Ovladače k biometrickým zařízením jsou nyní k dispozici přes Windows Update.

NOVINKY V SERVISNÍCH ÚČTECH

Jedním z bezpečnostních nastavení pro kritické síťové aplikace, jako jsou například IIS nebo SQL Server, je výběr typu účtu, pod kterým aplikace poběží a bude přistupovat k dalším informacím. Na lokálním počítači může administrátor nastavit aplikaci, aby běžela pod účtem Local Service, Network Service nebo Local System. Tyto účty ale nabízejí jen základní konfiguraci, jsou typicky sdíleny mezi několika aplikacemi a nedají se spravovat na doménové úrovni.

Jestliže nakonfigurujete aplikaci s vytvořeným doménovým účtem, můžete omezit privilegia tohoto účtu a tím přístup aplikace k datům, ale musíte manuálně spravovat hesla pro tento účet a SPN (Service Principal Name), které je požadováno pro autentizaci Kerberos. Někteří administrátoři řešili problém s hesly tím způsobem, že nastavili účet tak, že heslo je stále platné, a toto heslo pak bylo účtem používáno i několik let.

Ve Windows Server 2008 R2 a Windows 7 přibyly dva nové typy účtů: managed service account a virtual account. Managed service account je navržen pro aplikace jako například SQL Server nebo IIS k omezení přístupu k informacím prostřednictvím doménového účtu bez nutnosti manuálně spravovat hesla nebo SPN pro tento účet. Hesla jsou nastavována a pravidelně měněna automaticky, podobně jako například hesla u účtů počítačů v Active Directory. Virtual accounts jsou „managed service accounts“, které používají počítačová pověření (credentials) k přístupu k síťovým prostředkům.



Microsoft TechNet

Microsoft TechNet je program, který se snaží o zajištění komplexních služeb pro IT odborníky. Většina těchto služeb je zdarma a jejich smyslem je IT odborníkům pomoci při jejich práci a pravidelně a rychle je informovat o všech novinkách, které pro ně Microsoft připravil, v českém jazyce, českými odborníky a zaměstnanci společnosti Microsoft.

Mezi tyto služby patří:

– TechNet Fóra, *www.technetforum.cz*
– TechNet Flash zpravodaj, *www.technetflash.cz*
– TechNet Blog, *www.technetblog.cz*
– TechNet Videa, *www.technetwebcast.cz*
– TechNEt Konference, *www.technetkonference.cz*
– TechNet Subscription, *www.technetsubscription.cz*

Jde o fóra, kde si IT odborníci radí navzájem, Flash zpravodaj se všemi novinkami z českého rybníka, Blog, který téměř každý den informuje nejen o životě v Microsoftu, záznamy z českých konferencí a seminářů, nepravidelně pořádané konference a v neposlední řadě jedinou placenou službu TechNet Subscription, která umožňuje stahovat všechny produkty společnosti Microsoft (kromě vývojářských) v plných verzích k testovacím účelům.

Pro tyto účty je vytvořen v Active Directory Users and Computers speciální kontejner Managed Service Accounts (viz obrázek na předcházející straně) a vytváří se a konfigurují se výhradně přes Windows PowerShell 2.0.

Konkrétně je potřeba pro konfiguraci těchto účtů v PowerShellu naimportovat modul pro Active Directory (Import-Module ActiveDirectory) a účet vytvořit pomocí cmdletu New-ADServiceAccount.

Více o požadavcích na vytváření managed service accounts a návod, jak je vytvářet a konfigurovat, najdete v dokumentu Service Accounts Step-by-Step Guide.

NOVINKY V UAC = USER ACCOUNT CONTROL (ŘÍZENÍ UŽIVATELSKÝCH ÚČTŮ)

Za standardních okolností běžní uživatelé a administrátoři přistupují k prostředkům a spouští aplikace v bezpečnostním kontextu běžného uživatele. Když se uživatel přihlásí do počítače, systém mu vytvoří tzv. access token. Ten obsahuje informace o úrovni přístupu, která je uživateli dána, včetně příslušných SIDů a Windows privilegií. Když se přihlásí administrátor, jsou pro něj vytvořeny dva oddělené access tokeny: běžný uživatelský access token a administrátorský access token. Jeho běžný uživatelský access token obsahuje tytéž informace jako administrátorský, ale všechny Windows privilegia a SIDy jsou z něho odstraněny. Běžný uživatelský access token je pak použit pro start aplikací, které nevyžadují administrátorské oprávnění (běžné uživatelské aplikace).

Když pak uživatel chce spustit aplikaci vyžadující administrátorská oprávnění, je vyzván ke změně nebo ke zvýšení bezpečnostního kontextu z běžného uživatele na administrátora, nazývaného Admin Approval Mode.

Ve Windows Server 2008 R2 zabudovaný účet administrátora (Administrator) neběží v Admin Approval Mode. Všechny následně vytvořené administrátorské účty ale už běží v Admin Approval Mode automaticky. Ve Windows 7 je to trochu jinak. Stejně tak jako například ve Windows Vista je zabudovaný účet Administrator po instalaci zakázán (disabled). Pokud je ale během upgradu z Windows XP zabudovaný účet Administrator jediným aktivním lokálním administrativním účtem, Windows 7 ponechá tento účet povolený a navíc mu dovolí běžet v režimu Admin Approval Mode. Pokud provedete čistou instalaci Windows 7, první uživatel je vytvořen jako lokální administrátor v Admin Approval Mode (UAC enabled). Všechny další účty jsou pak vytvářeny jako běžní uživatelé.

Ještě složitější je to s přihlášením v nouzovém režimu (Safe Mode) pomocí zabudovaného účtu Administrator. Pokud počítač není v doméně a zároveň existuje nejméně jeden další lokální administrátorský účet, pak se nemůžete přihlásit do nouzového režimu počítače pomocí zabudovaného účtu Administrator. Pokud je ale poslední lokální administrátorský účet smazán, zakázán nebo odstraněn z administrátorů, pak nouzový režim počítače dovolí přihlásit se zakázaným (disabled) zabudovaným účtem Administrator. Pokud je počítač v doméně, pak není možné v žádném případě přihlásit se v nouzovém režimu pomocí zabudovaného účtu Administrator. Pokud neexistuje jiný lokální administrátorský účet, můžete se přihlásit v nouzovém režimu pomocí nakešovaného účtu, který je členem skupiny Domain Admins. Pokud se doménový administrátor na klientském počítači nikdy nepřihlásil, musíte nastartovat počítač v nouzovém režimu se sítí (Safe Mode with Networking).

Ve Windows 7 a Windows Server 2008 R2 došlo také k omezení počtu výzev ohledně UAC. Tato redukce se týká souborových operací, výzev v Internet Exploreru při spuštění instalace aplikace a ActiveX prvků. Jinými slovy: Pro tyto operace je uživateli už zobrazena jen jedna výzva místo několikanásobného odklepnutí dialogu na eskalaci nebo povolení operace.

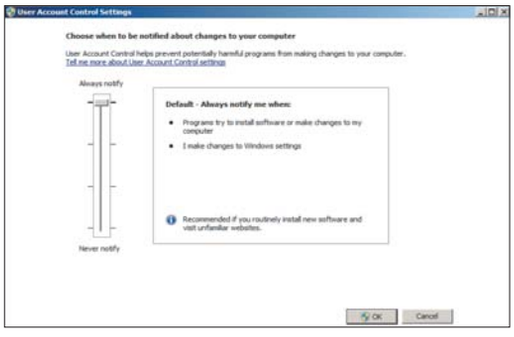
Navíc si nyní může běžný uživatel bez jakékoliv výzvy ze strany UAC instalovat aktualizace z Windows Update, instalovat ovladače, které jsou staženy z Windows Update nebo jsou zahrnuty v operačním systému, prohlížet nastavení Windows, párovat Bluetooth zařízení s počítačem, resetovat síťový adaptér a provádět ostatní diagnostiky a opravy sítě.

Další změna se týká nastavení úrovní UAC. Windows Vista nabízejí pouze 2 úrovně UAC: vypnuto a zapnuto. Windows 7 a Windows Server 2008 R2 nabízejí 4 úrovně UAC (řazeno od nejméně bezpečné):

- Never notify me – Nebudete upozorňováni během jakýchkoliv změn v nastavení Windows nebo během instalace softwaru.
- Only notify me when programs try to make changes to my computer – Nebudete upozorňováni během změn v nastavení Windows, které budete dělat osobně, ale budete upozorňováni na změny, které se pokouší provádět programy.
- Always notify me – Budete upozorňováni během změn v nastavení Windows, které budete dělat osobně, i na změny, které se pokoušejí provádět programy bez přepnutí na zabezpečenou plochu.
- Always notify me and wait for my response – Budete upozorněni na všechny administrativní zásahy na zabezpečené ploše a bude vyžadována vaše odezva. Tato volba je shodná se současným nastavením UAC ve Windows Vista.
- Výchozí úrovní pro administrátory je úroveň 3 a pro běžné uživatele je výchozí úrovní 4 (viz obrázek na této straně).

Pomocí bezpečnostních nastavení v Group Policy můžete nyní změnit chování UAC zpráv pro administrátory v Admin Approval Mode. K dispozici jsou tyto volby:

- Elevate without prompting. Dovoluje privilegovaným účtům provádět operace vyžadující eskalaci oprávnění bez výzvy k zadání autentizačních informací.



- Prompt for credentials on the secure desktop. Když operace vyžaduje eskalaci oprávnění, uživatel je vyzván na zabezpečené ploše, aby zadal jméno a heslo privilegovaného účtu.
- Prompt for consent on the secure desktop. Když operace vyžaduje eskalaci oprávnění, uživatel je vyzván na zabezpečené ploše, aby pro danou operaci zvolil dovolit nebo zakázat (Permit or Deny).
- Prompt for credentials. Když operace vyžaduje eskalaci oprávnění, uživatel je vyzván ke vložení jména a hesla privilegovaného účtu.
- Prompt for consent. Když operace vyžaduje eskalaci oprávnění, uživatel je vyzván, aby pro danou operaci zvolil dovolit nebo zakázat (Permit or Deny).
- Prompt for consent for non-Windows binaries. Standardně předvoleno. Když operace pro aplikaci, která není od Microsoftu, vyžaduje eskalaci oprávnění, uživatel je vyzván na zabezpečené ploše, aby pro danou operaci zvolil dovolit nebo zakázat (Permit or Deny).

Pomocí bezpečnostních nastavení v Group Policy můžete nyní změnit chování UAC zpráv i pro běžné uživatele, a to takto:

- Prompt for credentials. Když operace vyžaduje eskalaci oprávnění, uživatel je vyzván ke vložení jména a hesla privilegovaného účtu.
- Automatically deny elevation requests. Když operace vyžaduje eskalaci oprávnění, uživateli je automaticky zobrazena hláška zakazující operaci.
- Prompt for credentials on the secure desktop. Standardně předvoleno. Když operace vyžaduje eskalaci oprávnění, uživatel je vyzván na zabezpečené ploše, aby zadal jméno a heslo privilegovaného účtu.
- Více informací o konfiguraci UAC najdete např. v dokumentu User Account Control Step-byStep Guide.

NOVINKY V BEZPEČNOSTNÍM AUDITU

Ve Windows 7 a Windows Server 2008 R2 byly značně rozšířeny možnosti auditu bezpečnostních událostí, které se definují pomocí Group Policy. Původních 9 je nyní rozšířeno na 53 nastavení. Ta nyní dovolují administrátorům mnohem jemněji specifikovat typy aktivit, které chtějí sledovat, aniž by zbytečně logovali události, které je nezajímají. Navíc přibyla zcela nová kategorie auditu, a to Global Object Access Auditing. Tato kategorie dovoluje definovat globálně na celý počítač SACL (Security Access Control List), který se aplikuje buď na celý souborový systém, nebo na celý registr Windows. Výhodou tohoto nastavení je, že už nemusíte specifikovat diskové jednotky, složky nebo cesty v registrech, které chcete sledovat, ale automaticky jsou sledovány všechny složky, soubory a popřípadě i registry na celém počítači, na který je politika aplikována. Stačí v politice definovat, koho a jaké operace chcete sledovat.

Všechna nová nastavení auditu najdete v Group Policy objektu v Computer Configuration\ Policies\ Windows Settings\Security Settings\Advanced Audit Policy Configuration.

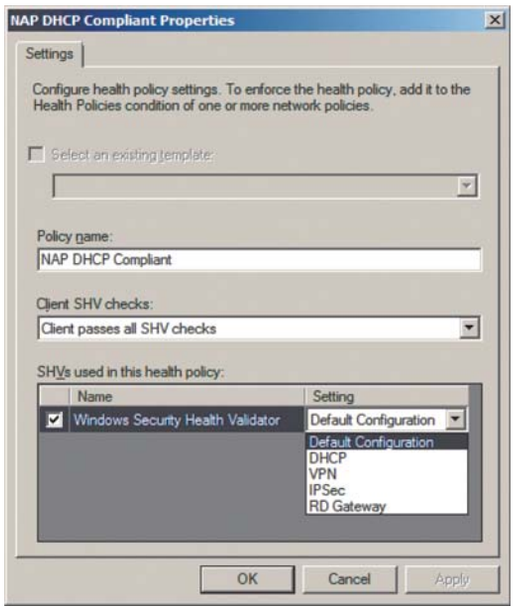
Seznam všech nových nastavení auditu s vysvětlivkami najdete na http://technet.microsoft.com/en-us/library/dd560628(WS.10).aspx.

NOVINKY V NAP

Řadu novinek přináší také systém NAP (Network Access Protection). Jde konkrétně o:

Multi-konfigurační SHV. Ve Windows Server 2008 R2 můžete nyní definovat více konfigurací SHV (System Health Validator), přičemž každá může být definována s jinou sadou požadavků na bezpečnostní nastavení. To potom umožňuje při konfiguraci Health Policy specifikovat různá nastavení pro jednotlivé enforcement metody. Například vytvoříte nastavení pro DHCP Enforcement, kde budete vyžadovat zapnuté automatické aktualizace, a jiné nastavení pro VPN enforcement, kde budete vyžadovat zapnutý firewall a zapnutou a aktuální antivirovou ochranu (viz obrázek 3).

Zlepšení uživatelského rozhraní NAP klientů. Ve Windows 7 je nyní integrováno uživatelské prostředí NAP klienta do konzole Action Center.



NPS šablony. NPS šablony dovolují vytvořit konfigurační elementy NPS serveru jako např. RADIUS klienty, Health policy nebo IP filtery, použít tyto elementy na lokálním NPS serveru nebo je exportovat pro použití na jiném NPS serveru. Template Management umožňuje tyto šablony vytvářet, editovat, ukládat, exportovat nebo importovat z/do souborů.

Nové možnosti logování RADIUS. Pomocí nového průvodce můžete nastavit logování do lokálního nebo vzdáleného SQL serveru, do textového souboru nebo nastavit kombinaci obou dvou typů logování.

Změny v autentizačních a šifrovacích protokolech.

Některých vylepšení se dočkalo i použití autentizačních a šifrovacích protokolů. Novinky jsou především následující:

- Windows 7 a Windows Server 2008 R2 podporují pro protokol Kerberos pouze:
- AES256-CTS-HMAC-SHA1-96
- AES128-CTS-HMAC-SHA1-96
- RC4-HMAC

Pokud chcete z důvodu zpětné kompatibility používat starší šifrovací algoritmy (DES-CBC-MD5 a DES-CBC-CRC), musíte je povolit manuálně v Group Policy v nastavení Configure encryption types allowed for Kerberos, které najdete v Computer Configuration\Security Settings\Local Policies\Security Options.

Windows 7 a Windows Server 2008 R2 podporují v protokolu Kerberos také kryptografii založenou na eliptických křivkách (ECC) pro přihlášení čipovou kartou pomocí certifikátu X.509. Ačkoliv tato změna není viditelná pro koncového uživatele, použití silnější kryptografie je určitě dobrým zlepšením celkové bezpečnosti. Podpora ECC nevyžaduje žádné konfigurační změny ze strany administrátora.

Protokol NTLM je nyní nastaven po instalaci operačního systému tak, aby vyžadoval 128bitové šifrování. Toto nastavení se dá v případě potřeby vypnout v Group Policy.

Nově pomocí nastavení v Group Policy můžete omezit nebo zcela blokovat použití protokolu NTLM na klientech, serverech nebo řadičích domény. Dále můžete analyzovat a auditovat použití protokolu NTLM pomocí nových audit policy. Návod jak omezit použití NTLM najdete v Resticting NTLM Usage Step-by-Step Guide a návod pro analýzu NTLM autentizace najdete v Discovering and Auditing NTLM Usage Step-by-Step Guide.

V popisovaných nových operačních systémech je nyní implementována nová verze Transport Layer Security protokolu TLS v1.2. Nová verze nyní navíc podporuje:

- Hash negotiation. Klient i server si mohou domluvit jakýkoliv hash algoritmus, který je podporován operačním systémem. Předvoleným algoritmem je nyní SHA-256 místo původní dvojice MD5/SHA-1.
- Certificate hash or signature control. Můžete nakonfigurovat, aby žadatel o certifikát mohl akceptovat pouze specifikovaný hash a podpisový algoritmus v certifikační cestě.
- Suite B-Compliant cipher suites. Byla přidána podpora Suite B algoritmů (algoritmy založené na ECC) v TLS přidáním dvou šifrovacích balíčků:
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

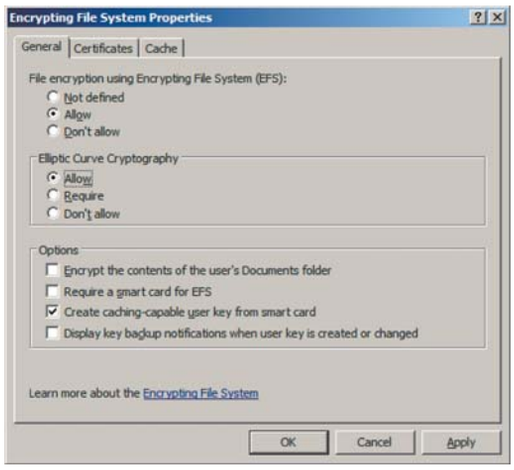
Zapnout podporu TLS v1.2 můžete pomocí bezpečnostního nastavení Group Policy v System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing a následně v Internet Exploreru v menu Tools\Internet Options na záložce Advanced zaškrtnutím Use TLS 1.2.

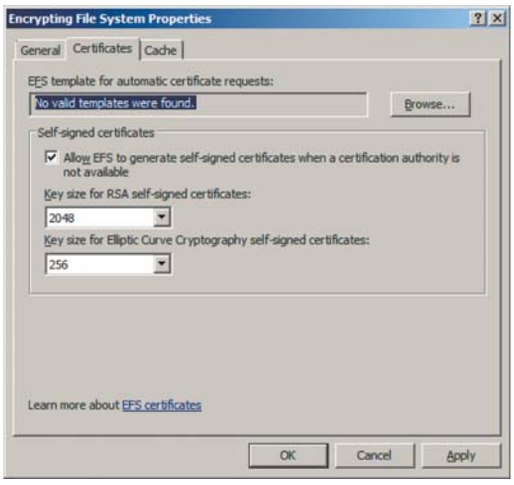
Více informací o TLS v1.2 najdete v TLS/SSL Technical Reference. Informace pro vývojáře aplikací pro použití TLS v1.2 jsou v článku Secure Channel v MSDN Library.

ZMĚNY V EFS (ENCRYPTING FILE SYSTEM)

EFS přidalo vedle podpory algoritmu RSA také podporu ECC (Elliptic Curve Cryptography). Pro self-signed RSA certifikáty je nyní předvolená délka klíče 2048 bitů a pro self-signed ECC certifikáty 256 bitů. Nejmenší RSA klíče lze nastavit na 1024 bitů, největší na 16 384 bitů. Nejmenší ECC klíče jsou dlouhé 256 bitů, největší 512 bitů. Pomocí nových nastavení v Group Policy můžete nejen definovat délku klíčů pro jednotlivé algoritmy, ale i vynutit si použití pouze ECC, vynutit si použít čipovou kartu pro EFS a řadu dalších nastavení (viz následující obrázky).

K parametrům /K a /R řádkového příkazu cipher.exe přibyla také možnost specifikace délky klíče pomocí parametru /ECC:délka (jako délku je možné použít 256, 384 a 512).





NOVINKY V DNS

DNS server a DNS klient ve Windows Server 2008 R2 a DNS klient ve Windows 7 nyní podporují DNSSEC (Domain Name System Security). DNSSEC je množina rozšíření, která přidává zabezpečení do protokolu DNS. Tato rozšíření jsou specifikována v RFC 4033, RFC 4034 a RFC 4035 a dovolují digitální podepsání DNS zóny a všech jejích záznamů. Když DNS server, který hostuje digitálně podepsanou zónu, dostane dotaz na její záznam, automaticky vrací s odpovědí i její digitální podpis. Dotazující se počítač (klient nebo server) může obdržet veřejný klíč a pomocí něho ověřit podpis na odpovědi od DNS serveru, a tak zjistit, zda je odpověď autentická a během přenosu nebyla modifikována.

Toto rozšíření pak nabízí ochranu proti man-in-middle útoku, spoofingu a útokům typu cache poisoning. Nabízí i 4 nové typy záznamů:

- DNSKEY – veřejný klíč pro danou doménu, 2 druhy: ZSK (Zone Signing Key) pro podepisování zóny a KSK (Key Signing Key) pro podepisování ZSK

- RRSIG (Resource Record Signature) – digitální podpis, obsahuje používaný kryptografický algoritmus, jméno klíče, kterým byl podepsán a čas uvedení i expirace podpisu
- NSEC (Next Secure) – pro negativní výsledky, obsahuje odkaz na další autoritativní záznam v zóně
- DS (Delegation Signer) – hash klíče ze subdomény, kterým zajišťuje důvěru mezi nadřazenou doménou a subdoménou delegovanými v samostatných zónách

Další informace o DNSSEC najdete např. na Wikipedii nebo v dokumentu o Domain Name System Security Extensions na Microsoft downloadu, a to včetně informací, jak DNSSEC nakonfigurovat. Nástroje zjednodušující práci s DNSSEC najdete na http://www.dnssec-tools.org/.

DALŠÍ ODKAZY

Kompletní popis všech bezpečnostních a dalších novinek najdete v následujících článcích na stránkách TechNet:

Changes in Functionality from Windows Server 2008 to Windows Server 2008 R2 (RC) – http://technet.microsoft.com/en-us/library/dd391932(WS.10).aspx

What's New for Security in Windows Server 2008 R2 – http://technet.microsoft.com/en-us/library/dd560640(WS.10).aspx

Jiří Hýzler, OKsystem

Success Story: Chemosvit Folie, alebo…
Ako si Bakbone NetVault cestu ku zákazníkovi našiel

Keď nás požiadali z redakcie časopisu Data v péči o článok o zálohovacom softvére Bakbone NetVault, spomenul som si na spoločnosť Chemosvit Folie. Prečo práve na Chemosvit? Okrem iného preto, lebo je to jeden z našich prvých zákazníkov na Slovensku, ktorý začal používať tento softvér a v podstate celé succes story je založené na tom, že si ho vybrali v Chemosvite spomedzi viacerých softvérov na základe testovania.

Vráťme sa však niekoľko rokov dozadu. Pred niekoľkými rokmi nás požiadali z Chemosvitu o ponuku na komplexný backup. V tom čase sme mali širšie portfólio backup produktov a s NetVaultom sme na našom trhu len začínali. Najlepšou možnosťou ako presvedčiť potenciálneho zákazníka na kvalitný produkt sa nám zdala forma bezplatného zapožičania trial licencie a pri NetVaulte sa nám to v prípade Chemosvitu (a nie len u neho) potvrdilo.

Dovolil som si preto pánovi Vladimírovi Mešárovi z Chemosvitu položiť niekoľko otázok, na ktoré mi ochotne odpovedal.

Chemosvit patrí na Slovensku medzi popredné výrobné priemyselné spoločnosti už dlhé roky. Môžete nám v stručnosti priblížiť, čím sa zaoberá vaša spoločnosť Chemosvit Folie?

Chemosvit Folie je dcérskou spoločnosťou Chemosvit. Nosným programom spoločnosti Chemosvit Folie je výroba, zušľachťovanie a predaj obalových materiálov. Naše produkty slúžia pre náročné aplikácie balenia potravín, hygienických a toaletných výrobkov, tabakových výrobkov, záhradníckych potrieb a spotrebného tovaru. Dôležitou súčasťou výroby v spoločnosti Chemosvit Folie je potláčanie fólií technológiou hĺbkotlače alebo flexotlače. Spoločnosť má vlastnú prípravu tlače, počnúc grafickým štúdiom, až po výrobu tlačových foriem – hĺbkotlačových valcov a flexoštočkov. Práve v oddelení prípravy tlače je nasadený zálohovací softvér NetVault.

Všetky technológie v príprave tlače sú digitalizované. Dáta majú grafickú podobu, čo sa prejavuje v ich veľkých kapacitách. Technologické pracovné stanice a RIPy sú postavené z väčšej časti na počítačoch Apple Macintosh, dátové servery na platforme windowsových a linuxových operačných systémov, vo virtuálnom prostredí VMware. Počítače sú pospájané v relatívne samostatnej lokálnej sieti vo vlastnej doméne.

Výberu nového zálohovacieho softvéru ste venovali veľa času aj úsilia. Testovali ste zálohovanie od viacerých výrobcov. Čo bolo hlavnou príčinou, že ste sa rozhodli pre centralizované zálohovanie s NetVaultom?

Dôležitou podmienkou pri našom výbere bolo, aby zálohovací softvér pracoval aj v prostredí Apple Macintosh. NetVault to splnil bez potreby dokupovať ďalšie licencie, podobne splnil aj naše nároky na podporu iných platforiem.

Dôraz sme dávali aj na intuitívne užívateľské prostredie, aby sme sa vyhli potrebe absolvovať náročné školenia. Tejto podmienke NetVault vyhovuje priam excelentne: Sami sme softvér bez zaškolenia inštalovali, testovali, ba bez problémov aj vyskúšali špeciálne situácie, napríklad obnovu systému v prípade poruchy samotného zálohovacieho servera.

Ďalšou dôležitou požiadavkou bola krátka doba obnovy dát. Niektoré zálohovacie systémy poskytujú paralelizmus zápisu dát z rozsiahlej sieti na jedno médium. Táto filozofia je zameraná na rýchlosť zálohovania, menej na rýchlosť obnovy dát. Keďže v príprave tlače je potrebné zálohovať veľké objemy dát, koncepcia spojitého zápisu na jedno médium, ktorá pri NetVaulte výrazne zrýchľuje aj obnovu dát, lepšie spĺňuje naše požiadavky.

Na produkte NetVault sme ocenili technológiu nazvanú LAN-free backup. Pri tejto technológii tzv. smart-klienti posielajú dáta priamo na zálohovacie zariadenia po SAN sieti bez využívania zálohovacieho servera. Zálohovací server prijíma cez LAN iba informácie o zálohovaných dátach. Tým sa výrazne zrýchľuje zálohovanie a zároveň sa nezaťažuje LAN.

Pri testovaní produktu sme ocenili aj jednoduchú prácu pri vytváraní a spravovaní virtuálnych knižníc.

Medzi akými, prípadne koľkými zálohovacími softvérmi ste sa rozhodovali?

Okrem softvéru NetVault od BakBone sme svoju pozornosť zamerali na Legato Networker, HP Data Protector, IBM Tivoli Storage Manager a Veritas NetBackup.

Ako dlho už používate tento softvér a ako ste s ním spokojný?
Používame ho v prevádzke od konca roku 2005. Vcelku vyhovuje našim požiadavkám. Sme s ním spokojní.

Koľko ľudí prípadne kto sa stará o administráciu backup softvéru?
Dvaja systémoví administrátori.

Ako máte momentálne nastavený systém záloh?
Softvér používame v režimoch archivovanie a zálohovanie.

V režime archivovanie sa určené dáta pravidelne podľa konkrétnych požiadaviek archivujú na páskové médiá.

Zálohy sa uskutočňujú jedenkrát denne, a to v noci. Plnú zálohu („full“) nahradzujeme konsolidovanou zálohou, pri ktorej sa konsoliduje obsah pások prepisovaním na nové pásky podľa skutočného stavu dát (podľa posledného „incrementu“). Tento proces sa uskutočňuje iba v páskovej knižnici – na dvoch mechanikách. Proces prebieha mimo LAN.

Medzi dvoma plnými zálohami sú naplánované zálohy typu increment. Algoritmus záloh je postavený tak, aby aj počas plnej zálohy bola vždy k dispozícii na médiách ďalšia platná záloha zálohovaných dát. Okrem zálohovania sú dáta on-line replikované do inej lokality inými technickými prostriedkami.

Čo by ste chceli vylepšiť na vašom zálohovaní, prípadne akú funkcionalitu očakávate od NetVaultu?
V nasledujúcom čase chceme využiť staršie uvoľnené diskové pole ako priestor pre virtuálne páskové knižnice. Zálohy do virtuálnych knižníc sa výrazne zrýchlia a tak sa skráti „backup okno“. Z virtuálnych knižníc potom dáta poputujú na páskové médiá mimo siete LAN iba v rámci zálohovacieho servera a siete SAN.

Akú novú funkcionalitu by sme očakávali? Určite deduplikáciu dát pri zálohovaní. Implementovaním algoritmov deduplikácie dát do zálohovacieho procesu by sa znížili požiadavky na kapacitu páskovej knižnice, ktorá u nás už nepostačuje.

Dovoľujem si na záver týmto poďakovať pánovi Mešárovi za to, že sa s nami podelil o svoje skúsenosti so zálohovacím softvérom Bakbone NetVault.

Mne ostáva len dodať, že deduplikácia bude dostupná v NetVaulte s novou verziou 8.5, ktorá príde na trh do konca roka. Viac informácií o deduplikácii s NetVaultom nájdete na našej webovej stránke *www.mhm.sk*, prípadne v ďalších číslach nášho časopisu.

Ak máte záujem vyskúšať zálohovanie s Bakbone NetVault, môžete si tento zálohovací softvér vyskúšať priamo u vás. Potrebnú trial licenciu nájdete na nasledujúcej stránke: http://bbbe1.bakbone.com/downloads/

Radoslav Pirohár, MHM computer Slovakia

Soutěž

V této rubrice přinášíme soutěžní otázky a jsme zvědavi na vaše odpovědi.

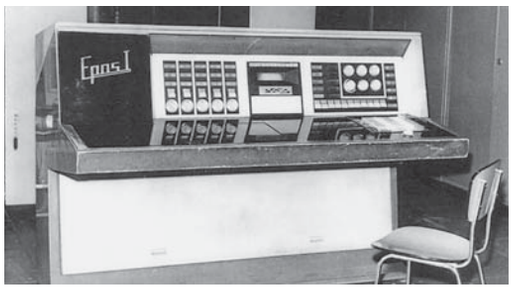
V minulém čísle jsme se ptali, na jaké frekvenci pracoval první československý samočinný elektronkový počítač EPOS1 postavený v roce 1963. Velká většina z vás, devadesát procent, odpověděla správně.

Byl-li EPOS1 elektronkový počítač, byly tedy základním stavebním kamenem elektronky.

A dnešní otázka tedy zní:

Jaký typ elektronky byl v převážné míře používán v klopných obvodech tohoto počítače a jaké měla tato elektronka označení?

ECC88 – dvojitá trioda
E88CC – dvojitá trioda
PCL82 – trioda pentoda



OTÁZKA Z MINULÉHO ČÍSLA ZNĚLA:

Na jaké frekvenci pracoval první československý samočinný počítač první generace EPOS 1?

a) 1 MHz
b) 8 MHz
c) 16 MHz

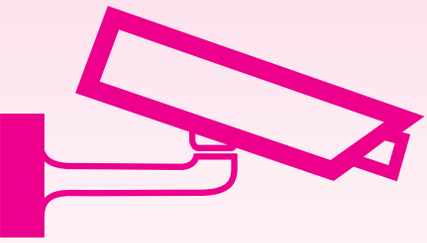
Správná odpověď zní:
1 MHz

Z mnoha správných odpovědí byl vylosován pan Martin Kopejtko z Prahy.
Gratulujeme a zasíláme malou pozornost od společnosti MHM.

ODPOVĚĎ NA AKTUÁLNÍ OTÁZKU PROSÍM PIŠTE DO ODPOVĚDNÍHO FORMULÁŘE NA *WWW.DATAVPECI.CZ.* ODPOVĚĎ NA SOUTĚŽNÍ OTÁZKU NAJDETE V PŘÍŠTÍM ČÍSLE. NA VÝHERCE, KTERÝ BUDE VYLOSOVÁN ZE SPRÁVNÝCH ODPOVĚDÍ DNE 1. 2. 2010, ČEKÁ JAKO OBVYKLE DÁREK, TENTOKRÁT OD SPOLEČNOSTI MHM COMPUTER.

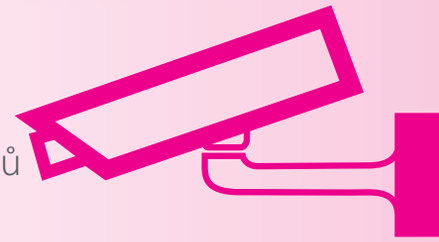
PROVOZUJETE KAMEROVÝ SYSTÉM?

Splňujete veškeré povinnosti stanovené zákonem č. 101/2000 Sb. o ochraně osobních údajů?



VÍTE, ŽE MUSÍTE

- zpracovat a zdokumentovat technicko-organizační opatření k zajištění ochrany osobních údajů?
- stanovit účel, prostředky a způsob zpracování osobních údajů?
- plnit oznamovací povinnost o zpracování osobních údajů vůči Úřadu pro ochranu osobních údajů?
- plnit informační povinnost při shromažďování osobních údajů nebo na žádost subjektů údajů?



CONVENIO CONSULTING NABÍZÍ KOMPLEXNÍ SLUŽBY:

- vypracování bezpečnostní směrnice pro ochranu osobních údajů
- audit kamerového systému z pohledu ochrany osobních údajů
- návrh opatření v oblasti bezpečnosti osobních údajů
- příprava podkladů pro oznámení o zpracování osobních údajů Úřadu pro ochranu osobních údajů

S naší pomocí splníte všechny legislativní požadavky v oblasti ochrany osobních údajů při provozování kamerového systému.

www.convenio.cz

CONVENIO CONSULTING