

Bez řízení přístupu není bezpečnost možná

PETR BUCHMAIER

Program SafeGuard Advanced Security (SGAS) je spojením několika modulů, které pomáhají při řešení problémů s řízením přístupu do jednotného celku. Tyto moduly vhodně doplňují šifrovací funkce ostatních programů z rodiny SafeGuard.

Modulární struktura umožňuje použít správný modul na požadavky, které chceme řešit, a tak šetřit prostředky, abychom nepoužívali systém, jehož funkce nevyužijeme.

Systém SafeGuard Advanced Security se skládá z následujících modulů:

- Base Module – základní modul, který vytváří podporu pro ostatní moduly v oblasti podpory čipových karet a auditu;
- Single Sign On – automatizované přihlášení do aplikací, web stránek terminálu;
- Removable Media Management – řízení přístupu k výměnným médiím;
- Plug and Play Management – řízení použití PnP zařízení v systému;
- Application Specific Access Rights (ASAR) – řízení přístupu uživatelů k datům a aplikacím.

Správa

Systém SafeGuard Advanced Security nemá zvláštní program pro centrální správu. Ke správě jsou používány šablony pro GPO, které používají rozšíření (GPO Extensions). Informace o nastavení a chování jsou uloženy v template GPO, která slouží jako databáze informací pro politiky, které řídí chování na klientských počítačích a pro uživatele. Centrální správa je potom jednoduchá na obsluhu, politika se aplikuje na OU obsahující uživatele nebo počítače dle potřeby.

Modul

Application Specific Access Rights (ASAR)

Modul ASAR slouží pro řízení přístupu uživatelů k datům a aplikacím v třívrstevném modelu. Dodávány jsou základní šablony pro nastavení přístupu k operačnímu systému a pro pokrytí aplikací, které jsou asociovány podle souborových přípon. Aplikace se mohou řadit do aplikačních skupin a lze určovat jejich spojení s daty. Uživatel při přístupu může používat pouze povolené aplikace a tyto aplikace mohou mít nastaven přístup dle masek k souborům.

Když správce nastavuje řízení přístupu, klade si následující otázky:

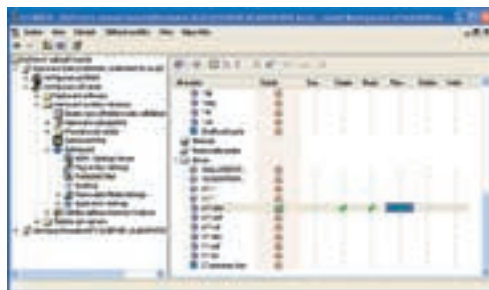
- Ke kterým datům má mít uživatel přístup?
- Kteří uživatelé mají mít přístup ke specifickým datům?
- Jaké oprávnění mají jednotliví uživatelé mít?

- Které aplikace mají mít přístup k specifickým souborům?
- Které soubory vyžaduje daná aplikace pro funkci bez chyb (například vytváření .tmp souborů)?

Po nalezení odpovědí na všechny položené otázky může přistoupit k nastavení systému.

Pojďme se podívat na příklad. Uživatel může otevřít v aplikaci soubory ke čtení z libovolného umístění, ale pro zápis je omezen pouze do sírového adresáře, který může být například šifrovan pomocí SafeGuard LanCrypt. Pokud se pokusí k těmto souborům přistoupit například pomocí aplikace na správu souborů, je přístup zamítnut, protože tato aplikace nemůže s daty manipulovat. Pro umístění souborů jsou definovány obecné skupiny místních, síťových, případně vyměnitelných úložišť.

Pro usnadnění správy je možné nacíst aplikace a souborová rozšíření, které má asociovány a provést export do nastavení politiky. Pro sledování systému a zjištění důvodů jak systém funguje, lze zapnout režim protokolování, který pouze sleduje systém.



Pro objekty lze nastavit následující přístupy:

- spouštění souborů,
- vytváření souborů,
- čtení souborů,
- přejmenování souborů,
- smazání souborů,
- zápis do souborů.

U aplikací je také možno nastavit, jak budou předávána práva v režimu parent/child například pro procesy, které jsou prostřednictvím aplikace vyvolány. Pokud není jasné, které nastavení bude

aplikováno, lze nastavit prioritu pro uživatelské nebo aplikační nastavení.

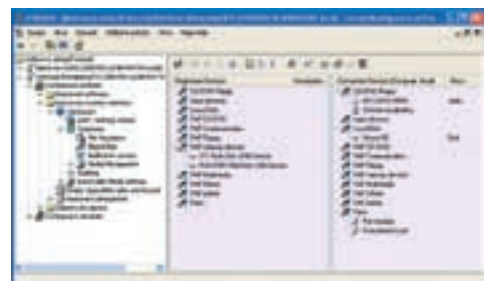
Pokud je aplikováno více pravidel, které vyhovují masce zadání, je použito jako poslední pravidlo, které má nejvíce konkrétní nastavení.

Modul

Plug and Play Management (PnP)

Pokud uživatelé používají externí média, nebo další zařízení, je žádoucí omezit uživatelům přístup k těmto prostředkům, aby nemohli do informačního systému nahrávat neschválené programy, nebo vynášet data. Modul PnP pracuje na principu registrace schválených zařízení a uživatelům povoluje použití pouze těchto schválených zařízení. Administrátor podobně jako v předchozím modulu používá jednu politiku jako databázi schválených a registrovaných zařízení a v politice, která se aplikuje na uživatele tato zařízení, povoluje, zakazuje, nebo přiřazuje logické jednotky.

Zařízení PnP nemusí být jen flash disky, nebo multimediální karty, ale mohou to být různá PnP zařízení, která umožňují i výstup informací z počítače. Vstupní zařízení jako jsou klávesnice, myši, scannery atd. nejsou kontrolována. Mezi výstupní zařízení mohou patřit i síťové karty, WiFi zařízení, externí modemy, například CDMA modem atd.



Mezi tyto typy zařízení patří:

- CD-Floppy (všechny lokální floppy/CD/DVD jednotky),
- Input devices (Smartcard čtečky atd.),
- Local Disk (všechny lokální hard disk jednotky),
- PnP CD-DVD (všechny externí připojené CD/DVD jednotky),
- PnP Communication (všechna zařízení připojená přes COM/LPT porty),
- PnP Floppy (všechny externí floppy jednotky),
- PnP memory devices (USB Memory Sticks, výměnná média),
- PnP Multimedia (digitální fotoaparáty atd.),
- PnP Others (podporovaná zařízení, která nebyla rozpoznána Windows),
- Ports (lokální porty).

Pokud uživatel použije neschválené zařízení, je zařízení rozpoznáno a před připojením uživateli zablokováno. Uživatel je o zablokování zařízení informován a může požádat správce o registraci zařízení, které potřebuje ke své práci.

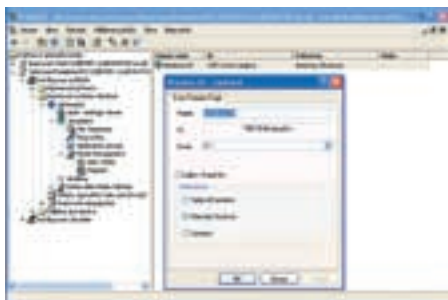
Ve spojení s předchozím modulem lze definovat zařízení, které bude připojeno jako konkrétní disková jednotka, ke které je definován přístup. Nelze například spouštět EXE programy, ale lze zapisovat DOC soubory. Ve spolupráci s dalšími produkty lze

stanovit pevnou politiku například pro šifrování výměnných zařízení.

Modul

Removable Media Management

Pomocí tohoto modulu lze určovat, jaká média CD/DVD budou schválena pro použití a v případě použití neregistrovaných bude přístup zamítnut. Správce provádí načtení seznamu CD/DVD ve formě kontroly názvu média, nebo kontroly adresářové struktury, nebo kompletního obsahu CD/DVD. Správce pak má jistotu že se používají například schválené výukové programy a uživatel nemůže provádět čtení neschválených titulů.



Modul Single Sign-On

Modul Single Sign-On umožňuje přihlášení do aplikací pomocí scriptů a uživatelských informací. Šablony jsou připraveny pro aplikace SAP/Lotus Notes/Novell a terminálové přístupy. Uživatel si může vytvořit vlastní systémy pro přihlášení do aplikací, nebo terminálových služeb případně do webovských stránek.

SHRNUTÍ

Modulární systém SafeGuard Advanced Security umožňuje řízení přístupu jak k datům a aplikacím, tak i k zařízením, které mohou být do systému připojeny.

HODNOCENÍ

- + Centrální správa přes GPO politiky, jednoduchá instalace a konfigurace
- + Modulární systém
- + Pevné řízení přístupu
- + Podpora čipových karet a USB tokenů

- Nelokalizován do češtiny



Článek připravil **Petr Buchmaier**, systémový inženýr společnosti NETPROSYS, s. r. o. Kontaktovat ho můžete na adrese pbuchmaier@netprosysty.cz

Telco roste

Na telekomunikačních trzích po celém světě získává stále větší význam konvergence služeb – propojování hlasových a datových služeb spolu s různými formami přenosu vysílání. V Evropě roste poptávka po službách spojených s pevnými sítěmi a širokopásmovým připojením, naproti tomu v Asii jednoznačně dominují mobilní služby. Každý měsíc tam v uvedeném segmentu přibývá 15 milionů nových uživatelů.

Tato a řadu dalších zjištění přináší studie společnosti KPMG International nazvaná „Global Telecommunications Financial Performance Tracker“. Materiál publikovaný koncem loňského roku analyzuje hospodářské výsledky šesti desítek největších telekomunikačních operátorů za rok 2005. Tyto společnosti byly rozděleny do tří skupin podle regionů, v nichž působí – tj. jednak Evropa, Blízký východ a Afrika (EMEA), dále USA, Kanada a Latinská Amerika, a konečně oblast Asie a Pacifiku (ASPAC).

Zatímco v roce 2004 celkové tržby poklesly ve všech sledovaných regionech, rok 2005 byl opět ve znamení růstu – nejvíce v Evropě (z 1,9 v roce 2004 na 6,4 procenta) a Asii (ze 4,1 na 5,1 procenta). Telekomunikačním operátorům zároveň rostly marže a s výjimkou amerického regionu se zlepšovalo i jejich cash flow.

Jistě není překvapivým zjištěním, že všechny tři regiony charakterizuje ostrý konkurenční boj. Jednotlivé telekomunikační společnosti hledají cesty, jak uspět a být neustále o krok před konkurencí – usilují zejména o maximální rozšiřování a propojování svých služeb, nezaměřují se již výhradně na lokální klienty. Nové technologie a obchodní modely jim umožňují operovat i na zahraničních trzích. Řada firem roste a proniká na nové trhy také prostřednictvím fúzí a akvizic jiných firem.

Konsolidace v Evropě

Na „starém kontinentu“ vzrostl zisk telekomunikačních firem za rok 2005 ve srovnání s předchozím rokem o 10,5 miliardy amerických dolarů. Evropský trh charakterizuje vysoký podíl mobilních telefonů a značná koncentrace velkých telekomunikačních společností. Přesto zde stále není taková konkurence (mj. pokud jde o ceny) jako například v Severní Americe. Na většině evropských trhů poskytují své služby pouze dva mobilní operátoři. „Slabší konkurence je dána tím, že evropské trhy jsou menší než trhy v Severní Americe a silnější pozici zde mají lokální firmy, které si svá teritoria chrání,“ vysvětluje Jan Martínek, partner společnosti KPMG Česká republika.

Přesto byl rok 2005 pro evropské trhy v jistém smyslu zlomovým. Došlo k výrazné konsolidaci služeb, většina telekomunikačních společností investovala značné prostředky do rozšiřování poskytovaných služeb a začleňování dříve oddělených mobilních služeb do komplexní nabídky. Výrazně rostla poptávka po službách s pevným

připojením – především po připojení širokopásmovém.

„Penetrace mobilními službami dosáhla v Evropě téměř maxima. Naopak trh s pevným širokopásmovým připojením představuje pro telekomunikační společnosti vítaný zdroj růstu, zvláště když se dosud nedaří využít potenciál 3G služeb,“ pokračuje Jan Martínek a přidává hodnocení situace v České republice: „Došlo k další konsolidaci alternativních operátorů, která bude jednoznačně pokračovat i v budoucnu. Pro úspěšný rozvoj alternativních operátorů však bude nezbytná jejich schopnost nabídnout i mobilní služby.“

Fúzující Amerika

Telekomunikační trh Severní i Jižní Ameriky, který v roce 2005 zaznamenal nárůst zisku o celých 20 miliard dolarů, se nesl ve znamení fúzí a akvizic, které připravily půdu pro ostrý cenový boj. I zde se telekomunikační společnosti zaměřovaly na sjednocování a slučování různých služeb, až už šlo o vnitrostátní hovory, dálkové hovory či mobilní služby.

V Severní Americe probíhá mezi telekomunikačními společnostmi a poskytovateli kabelové televize mnohem intenzivněji než jinde bitva o zákazníka. Vytváří se tak mimořádně konkurenční a nasycený trh, který nutí jednotlivé společnosti neustále investovat do nových multimediálních služeb, což ovšem v konečném důsledku způsobuje erozi zisků pro jednotlivé poskytovatele.

Mobilní Asie

Telekomunikační trh v Asii zaznamenal v roce 2005 pokles zisku o 1,7 miliardy dolarů, jenž analytici přičítají výrazné cenové konkurenci mezi tamními operátory. Přesto se vývoj na asijských trzích vyznačoval masivním nárůstem poskytovaných služeb i zákazníků – během každého měsíce roku 2005 bylo zaregistrováno více než 15 milionů nových uživatelů mobilních sítí, přičemž celá polovina z nich připadla na Indii a Čínu. I na nejméně rozvinutých trzích regionu se tak mobilní spojení již stává obvyklým standardem.

Telekomunikační společnosti působící na vyspělých trzích v Koreji, Japonsku či Tchajwanu reagovaly na mobilní invazi masivním rozvíjením širokopásmových služeb. Místní operátoři, patřící v globálním měřítku mezi největší, také významně posilují konvergované služby, především 3G síť

– dč