

SAFEGUARD LAN CRYPT

Strážce dat před vnitřním i vnějším narušitelem

PETR BUCHMAIER

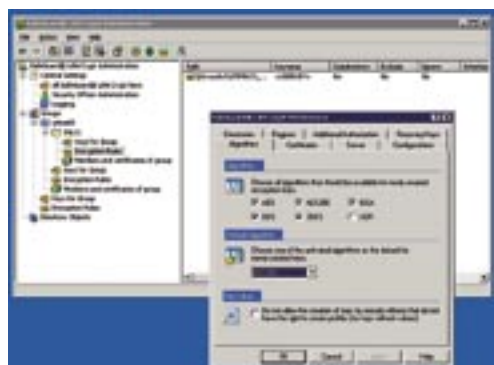
SafeGuard LAN Crypt (SGLC) je produkt pro inteligentní a transparentní šifrování složek a souborů na lokálních počítačích i v sítích. Princip šifrování je založen na PKI struktuře nebo s použitím programem vygenerovaných veřejných a soukromých klíčů.

Ty jsou využívány k aktivaci balíků soukromých a skupinových symetrických klíčů, jejichž pomocí jsou šifrovány jednotlivé soubory podle popisu adresářů. Vlastní privátní klíče mohou být uloženy jak v počítači, tak i na smartkartách nebo tokenech.

Správa

Administrační program pracuje s daty v databázi Microsoft SQL (k programu se dodává Desktop verze Microsoft SQL), nebo ORACLE. Pokud tedy databázi nemáte, pak ji nejdříve nainstalujete. Poté nainstalujete samotný modul administrace. Správa produktu je řízena přes účet Master Security Office, kterému v první chvíli buď vygenerujete, nebo nainportujete privátní klíč a spustíte aplikaci. Činnost správce lze rozdělit do čtyř částí:

- nastavení a auditování administrátorského programu,
- nastavení klientských programů prostřednictvím skupinové politiky GPO,
- správa uživatelů a skupin, kteří jsou importovány z LDAP databáze (Active Directory, Novell), domény nebo ručně připraveného seznamu uživatelů,
- nastavení pravidel pro vlastní šifrování souborů uživateli a skupinami.



Klient

Program pro klientské stanice je velmi jednoduchý. Instalovat ho lze jak ručně, tak i pomocí MSI balíčku na dálku. Po úspěšné instalaci a re-

startování počítače se objeví malá ikona klíče v pravé dolní části obrazovky. Při prvním spuštění program načte váš privátní klíč a požádá o zadání jeho přístupového hesla.

Barva ikony klíče odpovídá stavu běžícího programu. Zelený svítí v případě správné funkce, červený při nesprávné funkci a žlutý při vypnutém stavu, kdy program nešifruje ani nedešifruje.



Hlavní funkce

Pro samotnou činnost produktu SGLC je nutné nejdříve zanalyzovat prostředí a potřeby jednotlivých uživatelů a skupin na šifrování dat. Následně v administrátorské konzole načteme uživatele a skupiny, nastavíme pravidla pro šifrování vybraných dat, uživatelům vygenerujeme privátní klíče a vše uložíme do souboru politiky. Ty jsou vygenerovány pro každého uživatele samostatně do námi nadefinované cesty, ze které si jej jednotliví uživatelé načítají.

Pak klientský program ví, co a čím má šifrovat. Samotný proces šifrování se děje automaticky a nezávisle na uživateli.

Pod pokličkou

Program podle pravidel definovaných administrátorem vygeneruje uživateli jeho privátním klíčem zašifrovaný soubor politiky. Ten obsahuje jak informace o adresářích, které se mají šifrovat, tak i samotné symetrické klíče typu AES, AES-256,



3DES, IDEA, které jsou rychlejší pro samotnou práci se soubory než asymetrická šifra.

Tento soubor se při každém přihlášení uživatele načítá na lokální počítač, a tak má vždy aktuální nastavení a zároveň i dostupné v okamžiku, kdy není připojen k síti.

SHRNUTÍ

Šifrování programem SGLC je velmi snadné na ovládání a nevyžaduje prakticky žádný zásah uživatele. Velkou výhodou je, že šifrování i dešifrování probíhá přímo na lokálním počítači, nezatěžuje serverovou část, a tak jsou data během přenosu po síti i na serverech vždy proti útoku chráněna.

HODNOCENÍ

- + Safeguard LAN Crypt**
 - + jednoduchá centrální instalace, konfigurace a administrace
 - + oddělení systémové a bezpečnostní zodpovědnosti administrace
 - + jednoduchost použití pro uživatele
 - + podpora smartkaret a USB tokenů

- nelokalizován do češtiny**



K recenzí poskytla firma:
NETPROSYS, www.netprosysty.cz
Cena: 5 licencí včetně centrální správy 23 382 Kč (bez DPH)

Článek připravil Petr Buchmaier (pbuchmaier@netprosysty.cz), systémový inženýr společnosti NETPROSYS, s. r. o., ve spolupráci s externím konzultantem Petrem Kučerňákem