Datový trezor

Počet dat, se kterými pracujeme, roste exponenciálním tempem. S rostoucím počtem uložených dat roste i procento zajímavých informací, které jsou v nich uloženy. O informacích všeobecně platí jedno nepsané pravidlo: čím výše postavený člověk ve společnosti, tím zajímavější informace uložené na jeho počítači. V případě jejich ztráty není ohrožena jen Vaše společnost, ale zcizená data většinou obsahují i informace o Vašich klientech a spolupracovnících. Nemyslíte si že, případná ztráta důvěryhodnosti může mít mnohdy ještě vážnější následky?
Naštěstí existují řešení, které data ochrání a zajistí, že zůstanou bezpečně uložena na svém místě. Datový trezor řeší přesně ty oblasti, které jsou z hlediska bezpečnosti nejvíce zranitelné. Datový trezor není jen řešení, které obsahuje softwarové funkce, ale jedná se o komplexní řešení využívající pokročilý hardware a sofistikovaný software. Služby bezpečnostních odborníků, kteří pomohou odladit systém přímo pro Vaši společnost, jsou samozřejmostí.

Prvním místem, které je třeba zabezpečit je přihlášení uživatelů do operačního systému. Uživatelé si jen zřídka pamatují dostatečně bezpečná hesla. Není tedy překvapením, že většina z hesel, které byly vytvořeny přímo uživateli, jsou ve formátu, který je v lepším případě prolomitelný do několika hodin jednoduchým slovníkovým útokem. Řešení Datový trezor proto využívá pro přihlášení do operačního systému dvoufaktorovou autentizaci – to znamená, že uživatel něco zná a něco má. Pro přihlášení je nutný hardwarový předmět (1. faktor = vlastnictví předmětu), který je zabezpečen PINem uživatele (2. faktor = znalost PIN). Hardwarový předmět chrání přihlašovací informace, kterými se uživatelský účet autorizuje do operačního systému. Tyto údaje jsou navíc vygenerovány a uživateli neznámé. Tato metoda je podstatně bezpečnější než používání klasického uživatelského hesla, byť dostatečně dlouhého.

Bezpečné přihlášení je jen první překážkou, kterou případnému útočníkovi klademe, ale ne zcela poslední. Je potřeba se zabývat i daty, se kterými uživatelé nakládají, a patřičně je zabezpečit. Takovým zabezpečením je šifrování informací, které jsou uloženy v souborech na lokálních discích, sdílených úložištích či výměnných zařízeních. Nejúčinnější variantou je šifrování informací po souborech, které dokáže ochránit proti maximu možných rizik a útoků. Hlavní výhodou je nenáročnost vůči uživateli. Díky použití on-line transparentního šifrování uživatel, pracuje ve standardním prostředí, které ho nikterak neomezuje. Veškerá data, která uživatel vytváří, jsou automaticky šifrována nastaveným šifrovacím klíčem a zvoleným algoritmem. Při čtení dat ze šifrovaného souboru pak dochází opět k automatickému dešifrování do paměti pracovní stanice. On-line šifrování nevyžaduje interakci uživatele, protože veškeré operace běží na pozadí. Na disku jsou tak příslušné soubory vždy v zašifrovaném tvaru a nehrozí tedy jejich zneužití a i přenos dat po síti je maximálně bezpečný. Šifrované soubory se mohou nacházet na lokálním disku, výměnném nebo sdíleném disku. Pokud je šifrovaný adresář sdílen více uživatelům, pak všichni uživatelé musí mít k dispozici šifrovací klíč, kterým jsou soubory v tomto adresáři šifrovány. Pro šifrování jsou

Datový Trezor:

AreaGuard AdminKit:

- Příprava klientských instalací
- Centrální správa bezpečnostních politik napříč organizací
- Vyhodnocení aktuálního stavu ochrany dat na koncových stanicích. Kontrola použití šifrovacích klíčů na klientu
- Depozitář šifrovacích klíčů a evidence jejich užití.

AreaGuard Notes:

- Ochrana souborů uživatele prostřednictvím šifrování file-systému
- On-fly transparentní šifrování souborů na koncové stanici
- Minimální požadavky na znalosti uživatele

AreaGuard Gina:

- Bezpečné přihlášení uživatele do počítače
- Podpora nouzových situací prostřednictvím průvodce

SODATSW spol. s r.o., Horní 32, 639 00 BRNO, Tel.: 543 236 177, E-mail: info@sodatsw.cz

používány standardy, které splňují dnešní požadavky na bezpečnost. Jedná se o symetrické algoritmy s využitím šifrovacích klíčů o dostatečné délce, které jsou bezpečně uloženy v hardwarovém předmětu uživatele (jejich použití je podmíněno znalostí PIN). Díky koncepci Datového trezoru, který využívá on-line šifrování je provoz, naprosto nenápadný, a uživatel neregistruje žádné, byť sebemenší změny ve své práci s daty.

Nad celým systémem je postavena centrální správa, která slouží k vydávání, sledování a evidování hardwarových předmětů, šifrovacích klíčů a nastavení jednotlivých uživatelů. Centrální správa je nedílnou součástí řešení Datový trezor, zejména z důvodu zjednodušení správy uživatelů a jejich šifrovacích klíčů v prostředí s více jak 20 koncovými stanicemi. Obsahuje databázi všech klíčů, které byly vytvořeny a předány uživatelům, bezpečnostní politiky a automatickou instalaci pro pohodlnou distribuci ke koncovým uživatelům. Klíče, které byly v centrální správě jednou vytvořeny, jsou evidovány nejen po celou dobu jejího využívání, ale i archivovány v případě jejich deaktivace. To umožňuje správci mít okamžitý přehled o aktuálním stavu v celé organizaci. Důležitou součástí centrální správy je také průvodce recovery událostí, pomocí kterého můžete uživateli pomoci za jakékoliv situace. Jedná se o mocný nástroj, díky kterému je správa uživatelů hrou, která vás bude bavit.
Celé řešení Datový trezor je postaveno na následujících modulech z produktu **Desktop Security System AreaGuard**:

AreaGuard Gina – je rozhraní umožňující jednoduché a bezpečné přihlášení do operačního systému. Podporuje hardwarové předměty pracující na standartu PKCS#11, do kterých ukládá uživatelské přihlašovací informace. V AreaGuard Gina je implementován generátor, který umožňuje vygenerovat dostatečně bezpečné uživatelské heslo. Pro přihlášení do operačního se pak využívá 4 až 8 místný PIN, kterým je chráněn obsah kryptografického čipu.

AreaGuard Notes – uživatelsky příjemný a také vysoce účinným nástroj, který umožňuje on-line šifrování souborů ve specifikovaných adresářích (např. Dokumenty daného uživatele). Informace jsou šifrovány symetrickými algoritmy, které jsou dostatečné rychlé a bezpečné. AreaGuard Notes využívá moderních algoritmů AES, IDEA, 3DES. Šifrovací klíče jsou bezpečně ukládány do hardwarových předmětů. Plně jsou podporovány předměty kompatibilní s PKCS 11 standardem. Koncepce systému nevytěžuje koncovou stanici ani uživatele, který na ní pracuje.

AreaGuard AdminKit – umožňuje pohodlně spravovat i velké množství koncových stanic. V rámci přehledného grafického rozhraní lze rychle a efektivně sledovat i nastavovat desítky, stovky či tisíce instalací systému AreaGuard na koncových stanicích. Šifrovací klíče, certifikáty a nastavení bezpečnostní politiky jsou bezpečně uloženy v zálohované databázi, k níž má přístup pouze bezpečnostní administrátor. Aplikaci je možné využít také v případě obnovy uživatelských šifrovaných dat. AreaGuard AdminKit umožňuje vzdáleně měnit nastavení jednotlivých koncových stanic a tím i způsob šifrování dat. Konfigurační soubory lze upravovat a využívat rovněž při automatické (bezzásahové) instalaci, správě a plnění dat do hardwarových předmětů.

Klíčové funkce / Technické údaje:

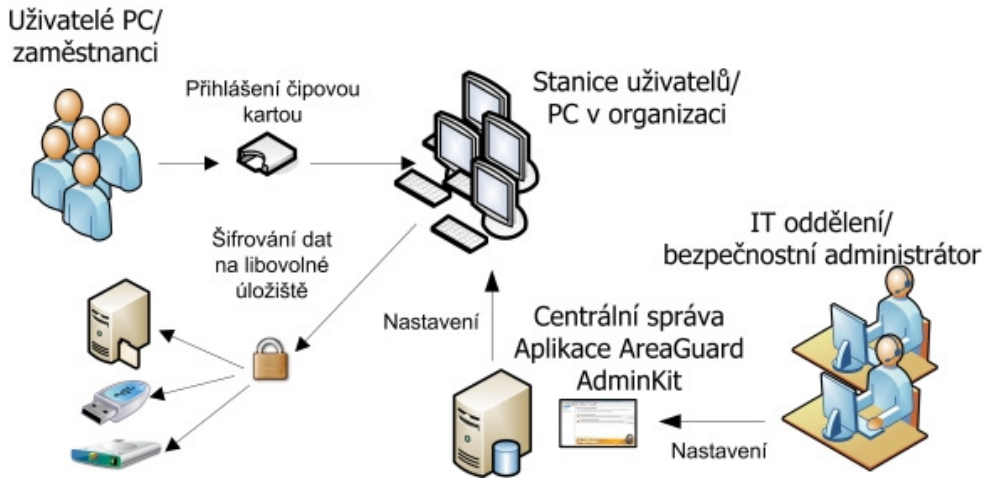
- Centrální správa řešení prostřednictvím administrátorského rozhraní
- Snadná distribuce politik
- Snadná evidence, záloha a přidělení šifrovacích klíčů uživateli
- Monitoring aktuálního stavu klienta na koncové stanici
- Snadné nastavení politik pomocí průvodce
- Ochrana dat na koncové stanici prostřednictvím symetrické kryptografie.
- Použití silného algoritmu AES 128 bit
- Podpora Microsoft Active Directory
- Možnost integrace do stávajícího PKI organizace
- Možnost využití certifikátů na čipových kartách pro zabezpečení klíčů uživatele
- Depozitář klíčů postavený na vlastní databázi
- Bezpečné přihlášení uživatele pomocí HW tokenu
- Podpora nouzových stavů

SODATSW spol. s r.o., Horní 32, 639 00 BRNO, Tel.: 543 236 177, E-mail: info@sodatsw.cz

Na rozdíl od modulů AreaGuard Gina a Notes, které jsou instalovány na koncových stanicích je centrální správa AreaGuard AdminKit, umístěná v zálohovaném úložišti. Tímto úložištěm může být jakýkoliv server společnosti, který je dostupný pro koncové stanice. Na serveru je vytvořena pouze adresářová struktura obsahující databázi, konfigurace a další soubory nutné ke spuštění aplikace. Server tedy není vytěžován žádným dodatečným procesem.

Datový trezor je ideálním řešením pro ochranu citlivých a důvěrných informací. Jeho jednoduchá a přitom propracovaná koncepce zaručuje rychlé nasazení ve vaší společnosti. Typickými oblastmi, kde se řešení využívá, jsou státní instituce a úřady, společnosti využívající notebooky, středně velké a velké firmy. Každé prostředí a každá organizace je individuální a toho jsme si plně vědomi, proto pořízením software to u nás nekončí, ale naopak začíná. Nikdy v tom nejste sami, s implementací Vám pomohou naši specialisté a navrhnou řešení tak, aby přesně splňovalo Vaše očekávání.

Schéma práce



Systémové požadavky:

Centrální správa AreaGuard úložiště dat:

- Nezávislé na operačním systému. Pouze úložiště informací a konfigurací pro klienty
- Běžný procesor použitý na daném serveru
- HDD 30 MB volného místa (doporučeno 100 MB)
- TCP/IP protokol. SMB protokol pro sdílení centrální správy v síti nebo IIS s rozšíření WebDAV, doporučená funkční služba DNS v síti

Klient AreaGuard

- Podporované operační systémy Microsoft Windows 2000 SP4 RP1, XP SP2/SP3, Vista SP1/SP2, 7 RTM
- Platforma 32 bit
- Microsoft Visual C++ redistributable package 2008
- Procesor třídy Pentium IV 1,5 GHz
- Paměť 256 MB (doporučeno 512 GB)
- HDD 30 MB volného místa (doporučeno 100 MB)

SODATSW spol. s r.o., Horní 32, 639 00 BRNO, Tel.: 543 236 177, E-mail: info@sodatsw.cz