USB pod kontrolou

Tempo vývoje hardware, který umožňuje ukládat velké objemy dat do malého paměťového čipu je obrovské. Tímto hardware jsou především USB zařízení, které pracují na technologii plug&play. Díky této technologii může uživatel pohodlně připojit libovolné výměnné médium do svého počítače a během několika sekund s ním pracovat. I ta nejlevnější zařízení mají dnes kapacitu v řádech gigabytů a představují tak obrovské ohrožení sítě a dat organizace. Vzhledem k fantazii výrobců je navíc obrovská rozmanitost podob a tvarů, a i nenápadná propisovací tužka, hodinky, zapalovač nebo přívěšek na klíčích může skýtat prostor pro krádež Vašich dat.

Hlavním cílem USB pod kontrolou je zabránit úniku dat prostřednictvím USB zařízení, externích disků, paměťových karet a dalších podobných zařízení, která se dají do počítače snadno připojit. K dosažení cíle využívá 3 stupňů ochrany – monitoring s alerty o nebezpečných situacích, blokaci práce s výměnným zařízením a šifrování dat, která na zařízení uživatel ukládá.

Protože představa o využívání těchto zařízení ve společnosti je většinou velmi slabá nebo značně zkreslená, prvním krokem je monitoring jejich využívání. Informace jsou získávány pomocí monitoringu práce uživatelů, kteří s externími zařízeními pracují a ukládají na ně data. To má na starosti specializovaná aplikace, která je instalována přímo na stanici uživatelů. Naše řešení monitoruje veškerou činnost uživatelů na koncové stanici. K dispozici jsou pak aktivity uživatele od jeho přihlášení až po jeho odhlášení. Všechny údaje obsahují přesný datum a čas, jméno uživatele, doménu, stanice a akci, kterou uživatel vykonal. Při sledování připojení a využívání externích zařízení jsou v logu obsaženy všechny důležité informace - připojení/odpojení zařízení, čtení/zápis nebo mazání souborů, cesta k datům a název souboru. O monitorovaných údajích není uživatel informován a monitoring jej nijak neomezuje, logové soubory jsou však před ním chráněny z důvodu zachování integrity údajů.

Protože nasbírané údaje je třeba průběžně vyhodnocovat a přehledným způsobem prezentovat, je k dispozici jednoduché rozhraní, které umožňuje generování souhrnných reportů. Tímto rozhraním je jednoduchá webová aplikace databázového typu, pracující nad SQL databází. Tato aplikace využívá doménových oprávnění, a proto umožňuje vyhodnocování jednotlivých skupin uživatelů, přímo jejich vedoucími. Veškeré vygenerované reporty se dají přímo v rozhraní publikovat nebo odeslat k tisku. A protože v konečném důsledku rozhodují detaily, kromě souhrnných reportů jsou k dispozici i podrobné, umožňující chronologicky vypsat aktivity uživatele a podrobně analyzovat jeho činnosti, Navíc software, který dokáže aktivity na stanici sledovat, Vás může zároveň i informovat o podezřelé činnosti uživatelů. Na každou sledovanou činnost můžete totiž nastavit patřičnou reakci a záleží jen na Vás, jaký typ zvolíte. Mezi podporované možnosti patří odeslání e-mailu, zobrazení hlášení uživateli, odhlášení uživatele ze systému, ale i zablokování jeho učtu na doméně. Můžete tak proaktivně zasáhnout v případě podezřelých aktivit na Vašich koncových stanicích.

Ačkoliv z názvu řešení se může zdát, že se bavíme jen o USB sběrnici, není to zcela pravda. Systém pracuje s dalšími běžně používanými sběrnicemi typu - 1394, PCMCIA nebo IRDA. To jsou

USB pod kontrolou:

AreaGuard Solution:

- 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.
- Ochrana souborů uživatele prostřednictvím šifrování file-systému
- On-fly transparentní šifrování souborů na koncové stanici
- Bezpečné přihlášení uživatele do počítače
- Podpora nouzových situací prostřednictvím průvodce

OptimAccess Solution:

- Monitoring využívání výměnných zařízení
- Monitoring pohybu dat v organizace
- Omezení využívání výměnných zařízení
- Omezení na úrovni file-systému stanice

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

nejpoužívanější sběrnice pro rychlé připojení zařízení, a proto na ně také nezapomínáme.
Dalším logickým krokem v zabezpečení výměnných zařízení je omezení jejich využívání. Z monitoringu již víme, jakým způsobem uživatel pracuje, a restrikce nám dávají možnost jej usměrnit do požadovaných mezí. Veškerá zařízená v minulosti připojená k monitorovaným sběrnicím systému určí a umožní nastavení jmenovaných akcí. Při blokaci zařízení je již instalovaný driver odebrán a je zabráněno jeho opětovnému zavedení a to i v případě, že uživatel má dostatečná oprávnění. Této možnosti je docíleno konstrukcí aplikace, které využívá vlastního driveru, běžícího pod systémovým oprávněním.

Protože zakázání využívání všech výměnných médií není v dnešní době pro většinu společností myslitelné, jsou k dispozici i další možnosti. Lze blokovat jednotlivá zařízení podle jejich SN, ale i hromadně podle typů zařízení nebo použité sběrnice. Driver pak umožňuje definovat podrobná pravidla, které například umožní připojení pouze firemních zařízení a jiných ne.

Pokud tedy zaměstnancům povolíme využití některých zařízení, je nutné přenášená data dostatečně zabezpečit. To umožňuje třetí část řešení – šifrování dat. Jedná se opět o lokálně instalovanou aplikaci, která ukládaná data převádí do šifrované podoby. V případě ztráty jsou data na výměnných médiích bez patřičného šifrovacího klíče nečitelná. Přečíst je může jen oprávněná osoba. Přenos šifrovaných informací je systémem bedlivě sledován a informace o jejich pohybu máte kdykoliv k dispozici.

Celé řešení **USB pod kontrolou** je založeno na produktech **Desktop Management System OptimAccess** a **Desktop Security System AreaGuard**. Jedná se o nástroje, jejichž a kvalit využily již tisíce společností nejen z ČR. Oba produkty jsou rozděleny podle funkcí do několika modulů, z nichž pro USB pod kontrolou jsou využity následující části:

OptimAccess Remote Control je srdcem celého řešení OptimAccess umožňuje spravovat aplikaci z jakéhokoliv počítače, přebírá topologii sítě a spolupracuje s ActiveDirectory. Všemožně se tedy snaží Vám správu usnadnit. Veškeré akce můžete plánovat a mít tedy vždy potřebné informace k dispozici.

OptimAccess WorkSpy vám umožní mít veškeré informace o činnosti uživatelů vždy po ruce. Sleduje veškeré operace, které uživatel na koncové stanici provádí. Jedná se o výkonnou monitorovací aplikaci, která ale zároveň obsahuje alertovací systém. Ověřte si, zda data, která jsou pro Vás důležitá, zůstávají na svém místě. Veškeré informace máte k dispozici po zadání jednoduchého dotazu.

OptimAccess Standard obsahuje restriktivní politiky. Přitom nezáleží na právech, které na svých stanicích uživatelé využívají. Mezi možnosti, které modul poskytuje je omezení uživatele při instalaci nového software z výměnných médií, kontrola přístupu k externím zařízením typu (USB, 1394, IRDA, PCMCIA), ochrana systémových složek a registrů, omezení přístupu k souborům s konkrétní příponou a jejich modifikace.

OptimAccess Report Center je modulem konstruovaným jako webové rozhraní pro prezentaci výsledků z databáze. Umožňuje pohodně vyhodnocovat logové záznamy, které obsahují informace o činnosti uživatelů na koncových stanicích. Díky webovému rozhranní a databázovému přístupu přináší rychlé a dobře prezentovatelné

Klíčové funkce / Technické údaje:

- Centrální správa řešení prostřednictvím administrátorského rozhraní
- 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
- Bezpečné přihlášení uživatele pomocí HW tokenu
- Podpora nouzových stavů
- Omezení zařízeni prostřednictvím Black/White listu
- Kompletní monitoring aktivit uživatele

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

výsledky.

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). Šifrovat dokáže data jak na lokálním disku a síťovém úložišti, tak data ukládaná na výměnná zařízení. 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 – obsahuje centrální správu pro produkt AreaGuard. Slouží k vydávání, sledování a evidování hardwarových tokenů, šifrovacích klíčů a bezpečnostní politiky jednotlivých uživatelů. 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.

USB pod kontrolou je ideálním řešením pro ochranu citlivých a důvěrných informací, které jsou ukládány na výměnná zařízení. Díky propracované koncepci sledování pohybu dat ve společnosti máte okamžitý přehled o případných bezpečnostních incidentech. Typickými oblastmi, kde se řešení využívá, jsou středně velké a velké firmy, státní instituce a úřady, ale i menší společnosti, které mají potřebu chránit své know-how. Každá společnost má individuální požadavky a toho jsem si vědomi. Naše řešení se Vám dokáže maximálně přizpůsobit a splnit tak i ty nejnáročnější požadavky.

Systémové požadavky:

OptimAccess Solution:

- Podporované operační systémy Microsoft Windows 2000 SP4 RP1, XP SP2/SP3, Vista SP1/SP2, 7 RTM
- Windows Server 2003 SP1/SP2 R2, Server 2008 SP1/SP2 – instalace bez driverů
- Microsoft Visual C++ redistributable package 2008
- Platforma 32 bit/64 bit – beta verze
- Procesor třídy Pentium IV 1,5 GHz
- HDD 30 MB volného místa (doporučeno 100 MB)

AreaGuard Solution

- Podporované operační systémy Microsoft Windows 2000 SP4 RP1, XP SP2/SP3, Vista SP1/SP2, 7 RTM
- Platforma 32 bit
- Microsoft Visual C++ redistributable package 2005
- 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