USB pod kontrolou

Centrálna správa bezpečnostných politík

Depozitár šifrovacích kľúčov a evidencia ich využitia

Monitoring využívania výmenných zariadení

Monitoring pohybu dát v organizácii

Obmedzenie využívania výmenných zariadení

On-fly transparentné šifrovanie súborov na koncovej stanici

Prečo uvažovať o USB pod kontrolou?

Tempo vývoja hardware, ktorý umožňuje ukládať veľké objemy dát do malého pamäťového čipu je obrovské. Týmto hardware sú predovšetkým USB zariadenia, ktoré pracujú na technológii plug&play. Vďaka tejto technológii môže užívateľ pohodlne pripojiť ľubovoľné výmenné médium do svojho počítača a behom niekoľkých sekúnd s ním pracovať. Aj tie najlacnejšie zariadenia majú dnes kapacitu v rádoch gigabytov a predstavujú tak obrovské ohrozenie siete a dát organizácie. Vzhľadom k fantázii výrobcov je obrovská rozmanitosť podôb a tvaru, a aj nenápadná prepisovacia ceruzka, hodinky, zapalovač alebo prívesok na kľúčoch môžu byť priestorom pre krádež Vašich dát, a toto riziko sa ešte ďaľej zvyšuje. Hlavným cieľom USB pod kontrolou je zabrániť úniku dát prostrednictvom USB zariadení, externých diskov, pamäťových kariet a ďalších podobných zariadení, ktoré sa dajú do počítača pripojiť. Pretože predstava o využívaní týchto zariadení v spoločnosti je väčšinou veľmi slabá alebo značne zkreslená, prvým krokom je monitoring ich využívania. Informácie sú získavané pomocou monitoringu práce užívateľov, ktorí s externými zariadeniami pracujú a ukladajú na ne dáta. To má na starosti špecializovaná aplikácia, ktorá je inštalovaná priamo na stanicu užívateľa. Naše riešenie monitoruje celú činnosť užívateľa na koncovej stanici. K dispozíci sú aktivity užívateľa od jeho prihlásenia až po jeho odhlásenie. Všetky údaje obsahujú presný dátum a čas, meno užívateľa, doménu, stanicu a akciu, ktorú užívateľ vykonal. O monitorovaných údajoch nie je užívateľ informovaný a monitoring ho nijako neobmedzuje, logové súbory sú však pred ním chránené z dôvodu zachovania integrity údajov.

Ako funguje USB pod kontrolou

Pretože nazbierané údaje je treba priebežne vyhodnocovať a prehľadným spôsobom prezentovať, je k dispozícii jednoduché rozhranie, ktoré umožňuje generovanie súhrnných reportov. Týmto rozhraním je jednoduchá webová aplikácia databázového typu, pracujúca nad SQL databázou. Táto aplikácia využíva doménových oprávnení, a preto umožňuje vyhodnocovanie jednotlivých skupín užívateľov, priamo ich vedúcimi. Všetky vygenerované reporty sa dajú priamo v rozhraní publikovať alebo odoslať k tlači. A pretože v konečnom dôsledku rozhodujú detaily, okrem súhrnných reportov sú k dispozícii aj podrobné, umožňujúce chronologicky vypísať aktivity užívateľa a podrobne analyzovať jeho činnosť. Naviac software, ktorý dokáže aktivity na stanici sledovať, Vás môže zároveň i informovať o podozrivej činnosti užívateľa. Na každú sledovanú činnosť môžete nastaviť patričnú reakciu a záleží len na Vás, aký typ zvolíte. Medzi podporované možnosti patrí odoslanie e-mailu, zobrazenie hlásenia užívateľovi, odhlásenie užívateľa zo systému, ale aj zablokovanie jeho účtu na doméne. Môžete tak proaktívne zasiahnúť v prípade podozrivých aktivít na Vaších koncových staniciach.

Hoci z názvu riešenia sa môže zdať, že sa bavíme len o USB zbernici, nie je to úplne pravda. Systém pracuje s ďalšími bežne používanými zbernicami typu - 1394, PCMCIA alebo IRDA. To sú najpoužívanejšie zbernice pre rýchle pripojenie zariadení, a preto na ne nezabúdame. Ďalším logickým krokom v zabezpečení výmenných zariadení je obmedzenie ich využívania. Z monitoringu už vieme, akým spôsobom užívateľ pracuje, a reštrikcie nám dávajú možnosť ich usmerniť do požadovaných medzí. Pri blokovaní zariadenia je už inštalovaný driver odobraný a je zabránené jeho opätovnému zavedeniu a to aj v prípade, že užívateľ má dostatočné oprávnenie. Táto možnosť je unikátna, pričom využíva vlastného driveru, bežiaceho pod systémovým oprávnením.

Pretože zakázanie využívania všetkých výmenných médií nie je v dnešnej dobe pre väčšinu spoločností mysliteľné, sú k dispozícii aj ďalšie možnosti. Je možné blokovať jednotlivé zariadenia podľe ich SN, aj hromadne podľa typu zariadenia alebo použitej zbernice. Driver potom umožnuje definovať podrobné pravidlá, ktoré napríklad umožnia pripojenie len firemných zariadení a iných nie.

Pokiaľ teda zamestnancom povolíme využitie niektorých zariadení, je nutné prenášané dáta dostatočne zabezpeciť. To umožňuje tretia časť riešenia – šifrovanie dát. Ide opäť o lokálne nainštalovanú aplikáciu, ktorá ukladané dáta prevádza do šifrovanej podoby. V prípade straty sú dáta na výmenných médiách bez patričného šifrovacieho kľúča nečitateľné. Prečítať ich môže len oprávnená osoba. Prenos šifrovaných informácií je systémom sledovaný a informácie o ich pohybe máte kedykoľvek k dispozícii.

Naše riešenie USB pod kontrolou obsahuje systémy **Desktop Management System OptimAccess a Desktop Security System AreaGuard**. Ide o nástroje, ktorých kvality využily už tisíce spoločností nielen zo SR a ČR. Obidve sú rozdelené podľa funkcií do niekoľkých modulov:

OptimAccess Remote Control je srdcom celého riešenia. OptimAccess umožňuje spravovať aplikácie z akéhokoľvek počítača, preberá topológiu siete a spolupracuje s ActiveDirectory. Všetky akcie môžete plánovať a mať vždy potrebné informácie k dispozícii.

OptimAccess WorkSpy vám umožní mať všetky informácie o činnosti užívateľa vždy po ruke. Sleduje všetky operácie, ktoré užívateľ na koncovej stanici prevádza. Ide o výkonnú monitorovaciu aplikáciu, ktorá ale zároveň obsahuje alertovací systém. Overte si, či dáta, ktoré sú pre Vás dôležité, zostávajú na svojom mieste.

OptimAccess Standard obsahuje reštriktívne politiky. Pritom nezáleží na právach, ktoré na svojich staniciach užívatelia využívajú. Medzi možnosti, ktoré modul poskytuje je obmedzenie užívateľa pri inštalácii nového software z výmenných médií, kontrola prístupu k externým zariadeniam typu (USB, 1394, IRDA, PCMCIA), ochrana systémových zložiek a registra, obmedzenie prístupu k súborom s konkrétnou príponou a ich modifikácia.

OptimAccess Report Center je modulom ako webové rozhranie pre prezentáciu výsledku z databáze. Umožňuje pohodlne vyhodnocovať logové záznamy, ktoré obsahujú informácie o činnosti užívateľa na koncových staniciach. Vďaka webovému rozhraniu a databázovému prístupu prináša rýchle a dobre prezentovateľné výsledky.

AreaGuard Gina je rozhranie umožnujúce jednoduché a bezpečné prihlásenie do operačného systému. Podporuje hardwarové predmety pracujúce na štandarde PKCS#11, do ktorých ukladá užívateľské prihlasovacie informácie. V AreaGuard Gina je implementovaný generátor, ktorý umožňuje vygenerovať dostatočne bezpečné užívateľské heslo. Pre prihlásenie do operačného systému sa využíva 4 až 8 miestny PIN, ktorým je chránený obsah kryptografického čipu.

AreaGuard AdminKit – obsahuje centrálnu správu pre produkt AreaGuard. Slúži k vydávaniu, sledovaniu a evidovaniu hardwarových tokenov, šifrovacích kľúčov a bezpečnostnej politiky jednotlivých užívateľov. Šifrovacie kľúče, certifikáty a nastavenie bezpečnostnej politiky sú bezpečne uložené v zálohovanej databázi, ku ktorej má prístup len bezpečnostný administrátor. Aplikáciu je možné využiť tiež v prípade obnovy užívateľských šifrovaných dát. AreaGuard AdminKit umožňuje vzdialene meniť nastavenie jednotlivých koncových staníc a tým aj spôsob šifrovania dát. Konfiguračné súbory je možné upravovať a využívať rovnako pri automatickej (bezzásahovej) inštalácii, správe a plnení dát do hardwarových predmetov.

USB pod kontrolou je ideálnym riešením pre ochranu citlivých a dôverných informácii, ktoré sú ukladané na výmenné zariadenia. Vďaka prepracovanej koncepcii sledovania pohybu dát v organizácii máte okamžitý prehľad o prípadných bezpečnostných incidentoch. Typickými oblasťami, kde sa riešenie využíva, sú stredne veľké a veľké firmy, štátne inštitúcie a úrady, ale aj menšie spoločnosti, ktoré majú potrebu chrániť svoje know-how. Každá spoločnosť má individuálne požiadavky a toho sme si vedomí. Naše riešenie sa Vám dokáže maximálne prispôsobiť a splniť tak aj tie najnáročnejšie požiadavky.

Pre ďalšie informácie navštívte prosím náš web: na **www.securstar.sk** alebo kontaktujte obchodné oddelenie obchod@securstar.sk