sodat
SOFTWARE

AreaGuard

bezpečnostní šifrovací systém využívající standardizovaných algoritmů

chrání firemní data před zcizením uživatelem, který s nimi pracuje

šifruje uživatelská data soukromým šifrovacím klíčem

stabilní, vysoce bezpečný s využitím hardwarové karty

jednoduše obsluhovatelný s nenápadným provozem

ve verzi Light pouze na softwarové bázi

www.sodatsw.cz

... and users have a better sleep

Bezpečnostní systém AreaGuard

Bezpečnostní systém AreaGuard slouží k zabezpečení firemních a uživatelských dat šifrováním, před jejich zcizením a následným zneužitím nežádoucí osobou. AreaGuard se integruje do operačního systému Windows NT nebo 2000.

První část bezpečnostního systému AreaGuard je určena k „Ochraně firemních dat", se kterými uživatelé (zaměstnanci) běžně pracují a mají možnost tato data odcizit v elektronické podobě.

Druhou částí je „Ochrana uživatelských dat", pomocí níž si běžní uživatelé mohou svá data šifrovat vlastním šifrovacím klíčem. Tuto funkci ocení uživatelé, kteří mají zájem archivovat svá soukromá data, posílat je e-mailem či předávat je na paměťových médiích, aniž by je mohla zneužít nežádoucí osoba.

Předností bezpečnostního systému AreaGuard je jeho nenápadný provoz. Běžný uživatel, který pracuje s firemními daty a dodržuje nařízení správce neregistruje žádné změny. Výjimkou jsou situace, kdy jeho aktivity směřují k potenciálně nebezpečným situacím.

Jednotlivé části bezpečnostního systému AreaGuard

„Ochrana firemních dat" systému AreaGuard se zaměřuje na data, která jsou majetkem firmy, ale pracuje s nimi množství zaměstnanců. Bezpečnostní správce definuje tato nastavení systému AreaGuard:

- šifrovací klíč a šifrovací algoritmus
- „Chráněnou oblast", kam umístí chráněná diskrétní data (adresář na lokálním nebo síťovém disku)
- „Privilegované aplikace", které jako jediné mohou pracovat s daty umístěnými v chráněné oblasti.

V chráněných oblastech jsou diskrétní data uložena v zašifrované podobě. Privilegované aplikaci je umožněno pracovat s daty standardně a AreaGuard zajistí transparentní šifrování a dešifrování dat. Privilegovaná aplikace nemůže data ani jejich část uložit, exportovat nebo přenést do jiné než chráněné oblasti. Pokud privilegovaná aplikace čte data z chráněné oblasti, která je na jiném než lokálním disku, po síti se přenáší data v zašifrované podobě a k dešifrování dochází až na lokální stanici. Chráněná data, zpracovávána privilegovanými aplikacemi, není možno přenést do jiných aplikací ani za pomocí schránky (clipboardu). Systém AreaGuard poskytuje možnost zvýšení bezpečnosti On-line šifrováním stránkovacích souborů PAGEFILE.SYS a dočasných souborů v adresářích TEMP. Veškeré informace o systému AreaGuard (šifrovací klíče, seznam chráněných oblastí a privilegovaných aplikací) jsou uloženy v AGD „AreaGuard Database", která je součástí registrační databáze operačního systému. AGD je šifrovaná pomocí MEK „Master Encryption Key", který je uložen v bezpečné hardwarové kartě „AreaGuard Card".

Druhou částí bezpečnostního systému AreaGuard je šifrování souborů uživatelem, který má možnost zvolené soubory nebo adresáře zašifrovat pomocí definovaného šifrovacího klíče, který je jeho tajemstvím. Kontextové menu adresářů a souborů se rozšiřuje o položky „Zašifruj" a „Dešifruj", pomocí kterých může uživatel soubory nebo celé adresáře zašifrovat nebo dešifrovat. Při práci se šifrovanými soubory probíhá opět transparentní On-line šifrování a dešifrování pomocí klíče, který uživatel zadá z klávesnice.

Princip činnosti

AreaGuard se integruje přímo do jádra operačního systému jako ovladač souborového systému. Vysoké bezpečnosti se dosahuje jeho zavedením ihned po aktivaci Windows NT Kernel (jádra), ještě před aktivací ovladače prvního File Systému. Bezpečnost se ještě zvýší použitím hardwarového doplňku AreaGuard Card. Nastavení parametrů AreaGuard se děje v ovládacím panelu AreaGuard, který je k dispozici pouze bezpečnostnímu správci. Veškeré přístupy k nastavení systému podléhají bezpečnostní politice operačního systému Windows NT, 2000. Prvotní instalace bezpečnostního systému AreaGuard je snadná, časově nenáročná a lze ji provést do již nainstalované stanice.

Spolehlivost a bezpečnost systému AreaGuard

Bezpečnost systému AreaGuard je postavena na síle šifrovacího algoritmu a délce šifrovacího klíče. Bezpečnostní správce může použít standardizované algoritmy DES a CAST s délkou klíče 64 a 128 bitů, což je v dnešní době považováno za nerozluštitelné v reálném čase. Veškeré operace se dějí přímo v jádru operačního systému. Bezpečnostní správce může celé nastavení AreaGuard exportovat na záložní médium, které slouží k obnovení nastavení v případě havárie systému.

AreaGuard Card

Bezpečnostní hardwarová ISA karta AreaGuard Card zabezpečí start správného operačního systému a zároveň bezpečně uchovává MEK. Jakmile se aktivuje ovladač AreaGuard, karta je deaktivována a nelze s ní dále komunikovat. Pokud je vyjmuta z počítače, nelze zavést operační systém a při následném vložení AreaGuard Card vyžaduje zadání PIN kódu, který zná pouze bezpečnostní správce. AreaGuard light je čistě softwarová ochrana, která nepoužívá AreaGuard Card a je tedy i cenově dostupná pro uživatele, kteří mají nižší nároky na bezpečnost.

Bližší informace, aktuality, TRIAL verze, technickou podporu a další naleznete na našich webových stránkách.

SODAT software spol. s r.o.
Sedlákova 33, 602 00 BRNO
Tel./fax: +420 - 5 - 4323 6177(8)
Hot-line: +420 - 602 - 702 780
e-mail: info@sodatsw.cz, support@sodatsw.cz
www.sodatsw.cz