sodat
SOFTWARE

AreaGuard

bezpečnostní šifrovací systém využívající standardizovaných algoritmů

chrání Firemní data před zcizením uživatelem, který s nimi standardně pracuje

šifruje Uživatelská data soukromým šifrovacím klíčem

stabilní, vysoce bezpečný, s využitím Tokenu pro uložení klíčů a autentizaci

jednoduše obsluhovatelný s nenápadným provozem

ideální pro řešení bezpečného přenosu dat v rámci VPN

. . . 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. AreaGuard® zde tvoří Firemní plot, jehož nastavení definuje bezpečnostní správce.
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 absolutně chránit svá soukromá data a to i před správci systému, ukládat nebo je zálohovat jinam než na NTFS, případně je posílat prostřednictvím e-mailu v zašifrované podobě. Dále se takto chráněná data dají sdílet jiným uživatelům, kteří znají hodnotu šifrovacího klíče. AreaGuard® je ideálním prostředkem pro bezpečný přenos dat v rámci VPN (Virtual Privat Network), kdy zprostředkuje bezpečný komunikační kanál mezi jednotlivými vzdálenými sítěmi.
Předností bezpečnostního systému AreaGuard® je jeho nenápadný provoz. Běžný uživatel, který pracuje s firemními daty neregistruje žádné změny a pracuje ve standardním prostředí.

Části bezpečnostního systému

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 diskrétní data (adresář na lokálním, výměnném, nebo síťovém disku)
- Privilegované aplikace, které jako jediné mohou pracovat s daty umístěnými v chráněné oblasti. Proces Privilegované aplikace je jednoznačný a nelze data přenést jinou byť stejnou aplikací.

V chráněných oblastech jsou diskrétní data uložena v zašifrované podobě. Privilegované aplikaci je umožněno pracovat s daty standardně a AreaGuard® zajistí jejich transparentní On-line šifrování a dešifrování. 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 v zašifrované podobě a k dešifrování dochází až v paměti lokální stanice. AreaGuard® dokáže takto zpracovávat libovolně dlouhé soubory bez omezení. Chráněná data zpracovávaná 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 bezpečnostní správce může uložit do hardwarového prostředku Tokenu.
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, případně je načten z Tokenu.
AreaGuard® může vygenerovat samodešifrovací SFX soubor, který lze dešifrovat po zadání klíče i na stanici, kde AreaGuard® není nainstalovaný.

Princip činnosti

AreaGuard® se integruje přímo do jádra operačního systému jako ovladač souborového systému. Vysoké bezpečnosti se dosahuje jeho zavedením hned po aktivaci Windows NT Kernel (jádra), ještě před aktivací ovladače prvního File Systému. Bezpečnost se ještě zvýší použitím hardwarového doplňku Tokenu. 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

Bezpečnost systému AreaGuard® je postavena na síle šifrovacího algoritmu a délce šifrovacího klíče. Bezpečnostní správce může použít standardizované algoritmy 3DES, IDEA nebo RC4 s délkou klíče 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® a Token

Při ochraně Firemním plotem je možné uložit MEK do hardwarového Tokenu, pomocí kterého se uživatel autentizuje a systému předá MEK. V případě Uživatelského šifrování je zde možné uložit šifrovací klíče a není tedy nutné je zadávat z klávesnice.

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)
e-mail: info@areaguard.cz, support@areaguard.cz
www.areaguard.cz