sodat
SOFTWARE

AreaGuard

for Windows

1. Úvod

Dostává se Vám do rukou bezpečnostní systém *AreaGuard*, který 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. Ochrana firemních dat slouží k zabezpečení dat, se kterými uživatelé (zaměstnanci) běžně pracují a mají možnost tato data odcizit v elektronické podobě. Ochrana uživatelských dat poskytuje možnost uživateli zašifrovat si vlastní soubory svým tajným šifrovacím klíčem.

AreaGuard se integruje přímo do operačního systému jako ovladač, který monitoruje práci se souborovým systémem. Ovládání ochranného systému se provádí pomocí rozšíření vlastností Průzkumníka operačního systému.

Před vlastní instalací doporučujeme prostudovat uživatelskou příručku. Bližší popis jednotlivých funkcí naleznete v HELPu systému, popřípadě je konzultujte s Vaším prodejce nebo přímo u výrobce na linkách technické podpory.

2. Instalace

Instalace systému *AreaGuard* se provádí pomocí programu SETUP, který se nachází na instalační disketě. Instalaci smí provádět pouze uživatel, který je členem skupiny „Administrators“. Tento uživatel by měl být zároveň důvěryhodným správcem dat, protože pouze tento uživatel bude moci sy-

stém *AreaGuard* nastavovat. Po nakopírování souborů a nastavení registrů je uživatel vyzván k nastavení vlastností systému *AreaGuard*. Pokud je v počítači instalována hardwarová karta *„AreaGuard Card“*, pak je uživateli umožněno uložit hlavní šifrovací klíč MEK (Master Encription Key) do vnitřní paměti karty. Zvolíte-li uložení MEK do *AreaGuard Card*, pak je zapotřebí nastavit kartě heslo pro správce a PIN, který je vyžadován, pokud karta byla vyjmuta z počítače. Pokud je heslo i PIN v kartě nastaven, není třeba jej znovu zadávat. V případě, že chcete heslo nebo PIN změnit, musíte zadat staré heslo i PIN. Šifrovací klíč MEK slouží k šifrování datové oblasti systému *AreaGuard*. MEK můžete vložit z klávesnice, kdy klíč musí mít délku nejméně 16 znaků, nebo se klíč může vygenerovat automaticky. Po dokončení instalace je zapotřebí provést restart počítače. Po novém spuštění počítače je již systém *AreaGuard* nainstalován a můžete pokračovat v nastavování jeho vlastností.

3. Ovládání

Nastavení vlastností ochrany firemních dat může provádět pouze osoba, která systém *AreaGuard* nainstalovala. Možnosti ochrany uživatelských dat mají všichni uživatelé operačního systému. Správce má možnost použít k nastavení ovládací panel *AreaGuard*, ze kterého je možné vkládat a nastavovat chráněné oblasti, privilegované aplikace a šifrovací klíče. Druhou možností nastavování je využití rozšíření funkcí Průzkumníka. Kliknutím pravým tlačítkem myši na složce nebo programu, kde se volba

„Vlastnosti“ rozšíří o záložku „AreaGuard“, ve které máte možnost nastavovat vlastnosti chráněných oblastí, privilegovaných aplikací a šifrovacích klíčů. Kliknutím pravým tlačítkem myši na libovolném souboru nebo složce se rozšíří kontextové menu každého uživatele o položku „Zašifruj“, „Dešifruj“ a „Odeslat“ pro odeslání zašifrovaného souboru e-mailem.

4. Ovládací panel AreaGuard

Tento ovládací panel může použít pouze uživatel, který je členem skupiny „Administrators“. Ovládací panel informuje o obecných nastaveních systému *AreaGuard* (šifrovací algoritmy, délky klíčů, …), nastavení *AreaGuard Card*, možnosti zálohování nastavení systému a export klíčů *AreaGuard* na disketu, informace o všech nastavených chráněných oblastech, privilegovaných programech a šifrovacích klíčích.

Nastavení AreaGuard Card – v kartě máte možnost měnit heslo správce, PIN a hlavní šifrovací klíč databáze *AreaGuard* (MEK). Pokud není *AreaGuard Card* instalována, pak lze měnit pouze hlavní šifrovací klíč MEK. Změnu klíče smí opět provést pouze uživatel, který provedl instalaci. Pokud se mění MEK v hardwarové kartě *AreaGuard Card,* je zapotřebí vždy před změnou zadat PIN, aby se karta odblokovala. Zadání PIN se řídí bezpečností karty, jejíž popis naleznete v kapitole *AreaGuard Card*. Při změně správcovského hesla a PIN karty musíte opět zadat staré heslo respektive starý PIN.

Zálohování nastavení a export klíčů – tyto dvě funkce slouží ke zvýšení spolehlivosti systému. Správce bezpečnosti má možnost uložit informace o chráněných oblastech, příslušných privilegovaných aplikacích a šifrovacích klíčích na disketu (popřípadě jiné médium). V případě havárie operačního systému je možné obnovit nastavení systému *AreaGuard* a zabránit tím možné ztrátě dat z chráněných oblastí. Export šifrovacích klíčů slouží k přenosu mezi jednotlivými počítači, kde je instalovaný systém *AreaGuard* a používají se stejné šifrovací klíče. Ukládání nastavení a export šifrovacích klíčů se musí řídit bezpečnostní politikou organizace a je zapotřebí média s těmito informacemi ukládat na bezpečné místo.

Nastavení chráněných oblastí – správce má možnost nastavit, které složky budou chráněny šifrováním. Složky lze přidávat jak z lokálního disku, tak z disků síťových. V seznamu jsou zobrazeny všechny složky, které jsou na daném počítači definované jako chráněné oblasti. Tlačítkem „Vlastnosti“ máte možnost přiřadit složkám privilegované aplikace a šifrovací klíč, kterým se data ve složce šifrují. Popis těchto funkcí naleznete v kapitole „Rozšíření vlastností Průzkumníka – nastavení AreaGuard“.

Nastavení privilegovaných aplikací – seznam všech privilegovaných aplikací, které jsou definované na daném počítači. Práce se seznamem privilegovaných aplikací je stejná jako práce s chráněnými oblastmi.

Nastavení šifrovacích klíčů – seznam všech šifrovacích klíčů, které se využívají k šifrování dat v jednotlivých chráněných oblastech. Práce s klíči je opět stejná jako u popsaných chráněných oblastí.

5. Rozšíření vlastností Průzkumníka – nastavení AreaGuard

Pokud kliknete v Průzkumníku pravým tlačítkem myši na složce nebo programu, pak se „Vlastnosti“ rozšíří o záložku „AreaGuard“, pomocí které máte možnost nastavovat chráněné oblasti (složky) nebo privilegované aplikace (programy).

Vlastnosti chráněných oblastí – v dialogu na záložce AreaGuard lze nastavit, jestli zvolená složka je chráněnou oblastí či nikoliv. Pokud je chráněnou oblastí, je možno použít tlačítko „Vlastnosti“ k upřesnění nastavení. Popis funkcí „Oprávnění“ a „Vlastnictví“ naleznete v kapitole „Řízení přístupů“. Ve vlastnostech chráněné oblasti můžete nastavit šifrovací klíč, který se používá k šifrování dat uložených v chráněné oblasti.

V horní polovině dialogu jste informováni o jménu šifrovacího klíče a typu algoritmu, který je používán k šifrování dat. Pokud chcete zadat šifrovací klíč, pak použijte tlačítka „Nalistuj“. Jestliže chcete, aby chráněná oblast nebyla šifrována, pak použijte tlačítka „Nuluj klíč“. Tlačítkem „Nalistuj“ se zobrazí seznam všech použitelných klíčů. Výběrem klíče nastavíte šifrovací klíč a algoritmus. Dále máte možnost vložit klíč nový. Každý klíč má své jedinečné jméno, hodnotu, kterou lze zadat z klávesnice nebo nechat automaticky vygenerovat a typ šifrovacího algoritmu.

V dolní polovině dialogu je seznam všech privilegovaných aplikací, které mohou k datům v této oblasti přistupovat. Aplikace můžete libovolně přidávat a mazat. Tlačítko „Přidej existující“ nabídne výběr ze seznamu již privilegovaných aplikací systému. Tlačítko „Vlastnosti“ informuje o chráněných oblastech, ke kterým má zvolená privilegovaná aplikace přístup.

Pokud změníte šifrovací klíč, pak po stisku tlačítka „OK“ se současně s uložením všech nastavených vlastností spustí konverze dat chráněné oblasti, která data automaticky přešifruje nově zadaným klíčem. Pokud není zadaný klíč, pak jsou data v chráněné oblasti převedena do standardního formátu.

Vlastnosti privilegovaných aplikací – v dialogu na záložce AreaGuard lze nastavovat, ke kterým chráněným oblastem má zvolená aplikace přístup. Opět lze libovolně vkládat a mazat chráněné oblasti. Tlačítkem „Přidej existující“ můžete vybrat chráněnou oblast z již existujících chráněných oblastí. Tlačítko „Vlastnosti“ vyvolá stejný dialog, který byl popsán v této kapitole výše.

Tlačítka „Oprávnění“ a „Vlastnictví“ jsou podrobněji popsána v kapitole „Řízení přístupů“.

6. Ovládání ochrany uživatelských dat

Uživatelé operačního systému s instalovaným systémem *AreaGuard* mají možnost si libovolný soubor popřípadě celou složku zašifrovat svým vlastním tajným šifrovacím klíčem. Kliknutím pravým tlačítkem myši na sou-

boru respektive složce má uživatel možnost zvolit volbu „Zašifruj“ nebo „Dešifruj“. Pokud zvolíte položku Zašifruj a soubor (soubory) nebyly zašifrovány, pak zadáte jméno klíče, hodnotu klíče a typ algoritmu, kterým chcete šifrování provést a soubor se podle těchto vlastností zašifruje. Pokud byl soubor již dříve šifrovaný, musíte zadat příslušný šifrovací klíč, kterým je soubor šifrován. Při práci se zašifrovanými soubory se automaticky provádí šifrování a dešifrování obsahu souboru příslušným klíčem. Pokud se soubor otevírá poprvé a šifrovací klíč nebyl zadán, pak je uživatel vyzván k zadání šifrovacího klíče.

Volbou „Dešifruj“ je možné soubor vrátit zpět do původního standardního tvaru. Zašifrovaný soubor je možné odeslat pomocí e-mailu a to volbou v kontextovém menu příslušného souboru „Odeslat“ - „Zašifrovaně e-mailem“. K ovládání šifrování uživatelských dat dále slouží „Ovládací aplikace“, jejíž aktivitu zobrazuje ikona v „Nástrojové liště“. Kliknutím na tuto ikonu můžete deaktivovat šifrování uživatelských dat, což umožní pracovat se souborem v zašifrovaném tvaru a je možné tento soubor např. kopírovat po síti nebo přenést na přenosném disku. Další možností je vymazání všech vložených šifrovacích klíčů, které se používají k šifrování uživatelských dat.

7. Řízení přístupu

Každá chráněná oblast, privilegovaná aplikace a šifrovací klíč má svého vlastníka, který daný objekt vytvořil. Vlastník má právo nastavovat vlast-

nosti daného objektu případně poskytnout oprávnění jinému uživateli, aby mohl tato nastavení u objektu měnit. Nastavení oprávnění, případně změny vlastnictví, lze vždy provádět tlačítky „Oprávnění“ a „Vlastnictví“ u jednotlivých objektů. Princip práce s těmito nastaveními je stejný jako u kteréhokoli jiného objektu u Windows NT, 2000.

8. Odinstalování systému AreaGuard

Odinstalování je možné provést z ovládacího panelu „Přidej nebo uber programy“. Při odinstalování se dešifrují data ve všech chráněných oblastech do původního stavu. Soubory, které byly zašifrovány uživatelem, zůstávají v zašifrované podobě. Při odinstalování jsou vymazány všechny odkazy a soubory systému *AreaGuard*.

9. AreaGuard Card

AreaGuard Card je hardwarová ISA karta, která zvyšuje bezpečnost systému *AreaGuard*. Karta dokáže zajistit bezpečné zavedení požadovaného operačního systému, to znamená, že neumožní zavést jiný operační systém. Další funkcí je uložení MEK, který je hlavním šifrovacím klíčem systému *AreaGuard*. Správce systému má možnost po zadání hesla nabootovat operační systém z libovolného média. Bootování z libovolného média je umožněno po stisku klávesy CTRL-B během aktivace karty, po kterém se zobrazí dialog s výzvou o zadání hesla. Pokud někdo vyjme kartu z počítače, pak po novém vložení karty je zapotřebí zadat PIN při kterém kar-

ta povolí bootování počítače. Pokud není PIN správně zadán ani po třetím zadání, pak je nutné zadat 20 místné heslo, které je pro každou kartu jedinečné. Nastavování hesla a PIN karty je popsáno v kapitole o ovládacím panelu AreaGuard.

Detailnější popisy jednotlivých části jsou uvedeny v elektronické podobě jako HLP soubory systému *AreaGuard*.

Copyright ©1999 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: support@sodatsw.cz

www.sodatsw.cz

SODAT software spol. s r.o.
www.sodatsw.cz