sodat

AreaGuard

for Windows

Úvod

Příručka *Začínáme s bezpečnostním systémem AreaGuard®* je určena pro základní instalaci a spuštění bezpečnostního systému. Detailní postupy, popis ovládání, postupy pro odstraňování problémů a řadu jiných užitečných informací naleznete v elektronické nápovědě bezpečnostního systému AreaGuard®.

Příručka obsahuje následující kapitoly:

- V části Seznámení se systémem AreaGuard® jsou základní informace o bezpečnostním systému a jeho dostupných verzích.
- Sekce Šifry a druhy šifrování přibližuje způsob možného používání šifer a zabývá se otázkou jejich bezpečnosti.
- Bezpečnostní systém AreaGuard® podporuje používání bezpečných hardwarových prvků. Vysvětlení jejich funkce a způsobu použití naleznete v odstavcích Bezpečný hardware.
- Podle instrukcí v části Instalace nainstalujete bezpečnostní systém AreaGuard®.
- S pomocí rad v části Hesla můžete nastavit optimální heslo pro ochranu vašich dat pomocí bezpečnostního systému.
- V případě havárie bezpečnostního systému jej lze deaktivovat dle postup v části Nouzové odstavení systému.
- Nedílnou součástí příručky je i Příloha A: Licenční ujednání. Rozhodně si ji pečlivě prostudujte dříve než se pustíte do instalace bezpečnostního systému.

Struktura elektronické nápovědy

- Základní informace o bezpečnostním systému naleznete v elektronické nápovědě pod heslem Seznámení s bezpečnostním systémem AreaGuard®.
- Popis instalace systému plus další informace týkající se technické podpory a omezení systému naleznete v elektronické nápovědě pod heslem Začínáme s programem AreaGuard®.
- Postup jak nakonfigurovat bezpečnostní systém pro spolupráci s bezpečnými hardwarovými prvky naleznete v elektronické nápovědě pod heslem Bezpečný hardware.
- Popis ovládacího rozhraní systému a konfigurace jeho funkcí naleznete v elektronické nápovědě pod heslem Ovládání aplikace.
- Rady a doporučení výrobce pro optimální konfiguraci a vyladění bezpečnostního systému naleznete v elektronické nápovědě pod heslem Doporučený postup konfigurace.
- Informace o kolizích a řešení případných možných problémů jsou umístěny v elektronické nápovědě pod heslem Odstraňování problémů.
- Vysvětlení základních použitých pojmů naleznete v elektronické nápovědě pod heslem Slovníček.

Seznámení se systémem AreaGuard®

Bezpečnostní systém AreaGuard® slouží k zabezpečení firemních a uživatelských dat šifrováním před jejich zcizením a následným zneužitím nežádoucí osobou. Integruje se přímo do operačního systému Windows NT, Windows 2000 nebo Windows XP. 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. Vůči uživateli je vlastní proces on-line šifrování plně transparentní. Běžný uživatel, který pracuje s firemními daty neregistruje žádné změny a pracuje ve standardním prostředí. Systém rovněž podporuje práci v méně pohodlném režimu off-line šifrování. Více informací o šifrách a jednotlivých režimech šifrování naleznete v odstavcích Šifry a druhy šifrování dále v této příručce.

Z hlediska bezpečnosti je doporučeno používat současně se systémem AreaGuard® rovněž prvky bezpečného hardware. Podrobnější informace o této problematice naleznete v části Bezpečný hardware dále v této příručce.

Bezpečnostní systém je možné na základě zakoupené licence provozovat v těchto verzích:

- *AreaGuard®* – plná verze systému nabízí zabezpečení firemních i uživatelských dat; k provozování je třeba operační systém Windows NT, Windows 2000 nebo Windows XP; typickým nasazením je aplikace firemní bezpečnostní politiky včetně pravidel firemního plotu;
- *AreaGuard® Server* – specielní verze bezpečnostního systému, určeného pro šifrování dat uložených na MS serverech s platformou Windows NT, Windows 2000 nebo Windows XP; typickým použitím je ochrana databázových, poštovních, souborových a jiných serverů, kdy při útoku zvenčí nelze data získat v čitelné podobě – data nelze získat ani při krádeži hardware nebo pevného disku;
- *AreaGuard® Notes* – verze nabízí pouze uživatelské on-line šifrování soukromých a firemních dat formou plné integrace do operačního systému Windows NT, Windows 2000 nebo Windows XP; typickým nasazením je šifrování dat na noteboocích či pracovních stanicích, kdy lze jejich ztrátu odepsat za cenu vlastního hardware;
- *AreaGuard® Notes off-line* – verze nabízí pouze méně bezpečné a uživatelsky více náročné off-line šifrování; může být použita i na systémech platformy Windows 9x, Windows ME, Windows NT, Windows 2000 nebo Windows XP.

Šifry a druhy šifrování

Jediným výpočetně bezpečným způsobem je chránit dokumenty s pomocí silných šifrovacích algoritmů. Je důležité si uvědomit, že neexistuje pojem dokonalé bezpečnosti. Síla těchto algoritmů je založena na skutečnosti, že jediný možný způsob jejich prolomení je použití útoku hrubou silou. Potenciální útočník musí zkoušet všechny možné kombinace a doba potřebná k prolomení šifry je závislá na délce použitého klíče. Při současné úrovni technologie jsou délky používaných klíčů voleny tak, aby útok na šifru musel trvat desítky či stovky let. A změnou délky používaného klíče lze šifru adaptovat na vývoj technologií.

Ochranný systém AreaGuard® podporuje šifrování a dešifrování šiframi 3DES, IDEA, RC4 a AES (Rijndael). Při použití šifrovacích klíčů délek 128 (či 112 v případě 3DES) resp. 256 bitů lze tyto šifry považovat za výpočetně bezpečné.

On-line versus off-line šifrování

Jaký je z pohledu uživatele rozdíl mezi on-line a off-line šifrováním?

- Při *off-line* šifrování je dokument v okamžiku úprav uživatelem uložený na pevném disku v nešifrované podobě. Před započetím úprav jej musí uživatel rozšifrovat. Po skončení úprav jej musí uživatel opět zašifrovat a smazat nešifrovanou podobu.

- Je-li použito *on-line* šifrování, dokument je na pevném disku stále v šifrované podobě. V okamžiku úprav je programem samočinně rozšifrován do paměti. Tento proces je plně automatický a nevyžaduje od uživatele žádné zvláštní kroky.

Při použití off-line šifrování je třeba vždy dokument manuálně šifrovat. Navíc se z hlediska existence nešifrované podoby dokumentu na disku nejedná o zcela bezpečné řešení. V případě vhodné integrace do operačního systému je on-line šifrování vůči uživateli plně transparentní. Na první pohled tak není vůbec patrné, že je použito nějaké šifrování.

Bezpečný hardware

Jako HW prostředek k uložení šifrovacích klíčů a certifikátů k autentizaci a digitálnímu podpisu lze použít HW token Rainbow iKey 1000 případně libovolný jiný prostředek dle požadavků uživatele (např. čipová karta).

Podrobnější informace o bezpečných hardwarových prvcích a jejich nasazení v rámci bezpečnostního systému AreaGuard® naleznete v elektronické nápovědě pod heslem Bezpečný hardware. Následující odstavce jsou věnovány autentizačnímu hardwarovému tokenu iKey 1000 od firmy Rainbow, který je doporučen pro používání s bezpečnostním systémem AreaGuard®.

Token Rainbow iKey

Autentizační token iKey 1000 firmy Rainbow je malé zařízení podobné přívěsku na klíče. Jednou z hlavních funkcí tokenu iKey 1000 je možnost bezpečného uložení šifrovacích klíčů pro šifrování souborů, digitálních certifikátů včetně šifrovacích klíčů používaných při digitálním podepisování a šifrování elektronických zpráv – e-mailů. K počítači připojuje prostřednictvím běžného USB portu, kterým jsou dnes standardně vybavovány všechny počítače. Není proto nutné používat speciální čtecí zařízení jako v případě čipových karet.

PIN kódy

Při používání tokenu je digitální identita uživatele chráněna dvěma způsoby – vlastnictvím tokenu a znalostí kódu PIN. Na rozdíl od platební karty si PIN pro přístup k certifikátům a klíčům uloženým v tokenu můžete sami zvolit a změnit pomocí obslužného programu a to včetně počtu možných pokusů chybného zadání. Podrobnější informace o způsobu manipulace s PIN jsou uvedeny v dokumentaci *Token iKey 1000*.

Pro iKey 1000 existuje hlavní ovládací PIN – jde o tzv. *master PIN*, *SO PIN* či *Security Officer PIN*. Tento je vyžadován jako autorizace všech nastavení týkajících se tokenu. Z výroby je tento hlavní PIN nastaven na hodnotu „rainbow“ (užívejte malá písmena, systém rozlišuje malá a velká písmena). Základní PIN je z výroby nastaven na hodnotu „12345678“.

Instalace

Po vložení distribučního média systému AreaGuard® se automaticky spustí *Instalační program*. Ten nakopíruje soubory potřebné pro systém na pevný disk vašeho počítače a provede veškeré úpravy nutné pro jeho korektní funkci.

Manuální spuštění instalace

Manuálně lze instalaci spustit souborem *Setup.exe* z kořenového adresáře distribučního média.

Obsah distribučního disku

Všechny soubory potřebné pro instalaci ochranného systému jsou v kořenovém adresáři distribučního média. Soubory z distribučního média je při dodržení Licenčního ujednání možné kopírovat na pevný disk počítače a instalaci pak následně provádět z pevného disku. Lze je zkopírovat i prostřednictvím počítačové sítě, například v případech, kdy je třeba instalovat systém na počítač bez disketové či CD-ROM mechaniky.

Součástí plné verze systému AreaGuard® Notes je rovněž freewarová verze AreaGuard® Notes off-line. Tato freewarová verze dešifruje bez jakýchkoliv omezení, ale umožňuje šifrovat pouze algoritmem RC4 a délkou klíče omezenou na 40 bitů. Tento freeware můžete v souladu s licenčními podmínkami poskytnout třetím osobám za účelem dešifrování vámi zašifrovaných dat. Instalace freeware AreaGuard® Notes off-line je na distribučním disku umístěna v adresáři *AGNOFFLINE FREEWARE* a spouští se souborem *setup.exe*.

Postup instalace na PC

1. Před vlastní instalací ochranného systému je doporučeno ukončit všechny běžící aplikace.
2. Po spuštění instalačního programu se zobrazí úvodní dialog se základními informacemi. Po jeho přečtení pokračujte v instalaci stiskem tlačítka *Další >*.
3. Nyní se vás instalační program táže na souhlas s Licenčním ujednáním. Jeho tištěnou podobu můžete nalézt na Registrační kartě a nebo jako přílohu příručky *Začínáme s bezpečnostním systémem AreaGuard®*. Po důkladném přečtení svůj souhlas můžete vyjádřit označením volby *S licenčním ujednáním souhlasím* a v instalaci pokračovat stiskem tlačítka *Další >*. Nesouhlasíte-li s ustanoveními Licenčního ujednání, ukončete instalaci stiskem tlačítka *Storno*.
4. V následujícím dialogu máte možnost zvolit druh instalace bezpečnostního systému (jejich popis naleznete v sekci Seznámení se systémem AreaGuard® na začátku této příručky) a instalovat systém včetně podpory hardwarového tokenu. Hardwarový prvek může se systémem AreaGuard® sloužit:
   - pouze pro bezpečné úložiště šifrovacích klíčů systému AreaGuard®;
   - jako úložiště šifrovacích klíčů systému AreaGuard®, autentizační předmět operačního systému Windows a úložiště klíčů pro elektronický podpis v rámci poštovního klienta Outlook.

   Po zvolení požadované podpory hardwarového tokenu pokračujte v instalaci stiskem tlačítka *Další >*.
5. Nyní dochází ke zkopírování souborů systému AreaGuard® na pevný disk počítače dle dříve provedených nastavení.
6. Instalujete-li systém včetně podpory tokenu iKey 1000 pro autentizaci, instalační program automaticky spouští instalaci firmy Rainbow. Ta na svém konci vyžaduje provedení restartu počítače. Odložte restart počítače později do dalšího kroku tohoto postupu.
7. Některé verze systému vyžadují pro dokončení své instalace provedení restartu počítače. V tom případě máte v závěrečném dialogu instalace možnost nastavit použití jedné z voleb: *Ano, chci provést restart počítače.*, kdy bude počítač restartován ihned anebo *Ne, provedu restart sám později.*, kdy počítač restartujete až ve vámi zvoleném okamžiku. Instalaci ukončíte stiskem tlačítka Dokončit.

Od okamžiku provedení restartu, je-li konkrétní verzí bezpečnostního systému vyžadován, se proces instalace považuje za ukončený. Nyní jsou na pevném disku počítače nakopírovány všechny soubory potřebné pro korektní funkci bezpečnostního systému AreaGuard®.

Informace o nastavení a konfiguraci bezpečnostního systému naleznete v elektronické nápovědě pod heslem Doporučený postup konfigurace.

Hesla

Proč by měl uživatel tajit své heslo a jakými způsoby data šifrovaná pomocí hesla získat bez jeho znalosti? Odpověď na první otázku je jednoduchá – pokud cizí osoba získá neoprávněný přístup k heslu, může libovolně manipulovat s daty jimi šifrovanými (číst, modifikovat nebo je vymazat). Je tedy v zájmu každého uživatele, aby své heslo tajil.

Druhá otázka je složitější. Je-li heslo správně zvoleno (doporučení pro jeho správnou volbu naleznete v následujících odstavcích Jak zvolit správné heslo) a nedojde-li k jeho kompromitaci vyzrazením ze strany uživatele či systému (například po napadení trojským koněm), musí potenciální útočník hádat naprosto neznámou kombinací znaků. V tom případě odpovídá riziko získání smysluplné podoby šifrovaných dat riziku prolomení šifry prostřednictvím útoku hrubou silou. Šifrovaná data tedy nelze získat v rozumném časovém horizontu – lze je označit jako výpočetně bezpečná.

Jak zvolit správné heslo?

V předchozím textu jsme se snažili zdůraznit, že volba hesla je důležitou stránkou bezpečnosti. Jaká jsou tedy doporučení pro volbu hesla? Heslo by nemělo být:

- kratší než 8 znaků;
- složené pouze z písmen nebo pouze z číslic – používejte rovněž speciální znaky;
- odvoditelné ze jména ani z jiných dostupných informací (jméno přítelkyně/manželky, domácího mazlíčka, datum narození a podobně);
- nemělo by se vyskytovat v žádném přirozeném jazyce.

Dobré heslo:

- obsahuje i nepísmenné speciální znaky a/nebo číslice;
- je dostatečně dlouhé;
- je velmi obtížně uhodnutelné či odvoditelné;
- je zapamatovatelné, aby si ho uživatel nemusel poznamenávat;
- je naprosto nezapamatovatelné a uloženo v tokenu.

Pro správnou volbu hesla můžete použít například tyto metody:

- zvolte dvě krátká slova (či více části slov) a spojte je libovolným nepísmenným znakem; pokud možno použijte velká i malá písmena;
- vyberte si nějakou snadno zapamatovatelnou větu a jako heslo použijte první písmena (slabiky) slov.

Jak s heslem správně nakládat?

Samozřejmě zásadním předpokladem pro správnou ochranu dat je rovněž odpovídající chování uživatele při manipulaci s heslem či potažmo šifrovacím klíčem. Nikdy tedy:

- nezadávejte heslo za přítomnosti cizí osoby, která může odezírat z klávesnice;
- neukládejte heslo napsané na papíru či formou ASCII textu v souboru – pouze ve vaší hlavě je heslo v bezpečí a nemůže být kompromitováno;
- nepoužívejte dále heslo v případě, máte-li podezření o jeho kompromitaci, neboť v tom okamžiku nejsou šifrovaná data dostatečně chráněna – dojde-li k této situaci, neprodleně zvolte jiné heslo a všechna data zašifrujte pomocí nového hesla;
- neodcházejte od počítače v okamžiku, jsou-li v jeho paměti uloženy šifrovací klíče;
- nesdělujte heslo prostřednictvím pošty, telefonu, faxu či e-mailu; jste-li nuceni okolnostmi předat heslo jiné osobě, je jediným možným způsobem předání osobní sdělení či použití prostředků pro bezpečnou výměnu šifrovacích klíčů.

Ztráta hesla resp. šifrovacího klíče

Je důležité uvědomit si že neexistují žádná zadní vrátka ani pro oprávněné uživatele. Pracujete s prostředky silné kryptografie.

<1> V případě kdy ztratíte šifrovací klíč či zapomenete heslo, neexistuje žádný způsob, jak data v reálném či únosném čase zpětně dešifrovat.

Nouzové odstavení systému

Máte-li problémy při zavádění operačního systému Windows NT/2000/XP, lze ovladače bezpečnostního systému odstavit z první fáze zavádění operačního systému ihned po restartu počítače tímto způsobem:

- prostřednictvím editoru otevřete soubor *boot.ini* umístěném v kořenovém adresáři primárního disku;
- v sekci *[operating systems]* uveďte na konec dané verze systému, jenž nelze zavést, přepínač */noloadsag*.

Příloha A: Licenční ujednání

Nepoužijte aplikaci, dokud si nepřečtete toto Licenční ujednání. Použitím této aplikace (nebo povolením jiné osobě ji použít) vyjádříte souhlas s následujícím Licenčním ujednáním. Pokud nesouhlasíte s ustanovením tohoto ujednání, můžete aplikaci do 10-ti dnů od koupě vrátit oproti úhradě ceny dodavatelem

Licenční závazek. SODAT software spol. s r.o. se zavazuje na základě Vaší koupě a ve smyslu následujících ustanovení poskytnout Vám nevýhradní a nepřenosné právo používat přiloženou kopii aplikace maximálně pro takový počet kompatibilních počítačů, odpovídající počtu zakoupených licencí.

Ochrana aplikace. Souhlasíte s tím, že provedete všechny rozumné kroky k zajištění aplikace a dokumentace proti neoprávněnému kopírování či použití. Zdrojový kód aplikace obsahuje a představuje obchodní tajemství firmy SODAT software spol. s r.o. nebo jejich poskytovatelů licence. Zdrojový kód a obsažené obchodní tajemství nejsou předmětem tohoto Licenčního ujednání. Souhlasíte s tím, že nebudete rozebírat ani dekompilovat zakoupenou aplikaci za účelem odhalení obchodního tajemství obsaženého ve zdrojovém kódu.

Kopírování a úpravy. S výjimkou případů ošetřených tímto Licenčním ujednáním nesmíte vytvářet ani umožnit vytvoření jakékoli kopie nebo úpravy této aplikace mimo takových kroků, které vedou k umožnění použití této aplikace, k archivním účelům nebo zálohování této aplikace. Veškeré doklady vlastnických práv musí být věrohodně reprodukovány a uvedeny u veškerých kopií a úprav. Nesmíte kopírovat dokumentaci, pokud to v ní není explicitně povoleno.

Termín. Tato smlouva nabývá platnost dnem, kdy poprvé použijete tuto aplikaci a její platnost bude trvat dokud nebude zrušena.

Omezení ručení. Ručení firmou SODAT software spol. s r.o. vzniklé na základě nebo související s tímto licenčním ujednáním či aplikací nebo dokumentací se omezuje pouze na celkovou částku placenou Vámi za tuto licenci. SODAT software spol. s r.o. v žádném případě nebude ručit za žádné zvláštní, náhodné, následné, nepřímé nebo postihnutelné škody.

Sedlákova 33, 602 00 BRNO
Tel./fax: +420 - 5 - 4323 6177(8)
e-mail: support@areaguard.cz
www.areaguard.cz

. . . and users have a better sleep

SOFTWARE spol. s r.o.
www.optimaccess.cz
www.optimaccess.com