

SODATSW Case Study | 2009 Nasazení řešení Datový trezor ve společnosti Synthesia, a.s.



Klient

Organizace : Synthesia, a.s.
Odpovědná osoba : Ivana Pavlíková
Pozice : Vedoucí Odboru informatiky

Dne : 12. března 2009

Vypracoval

Organizace : SODATSW spol. s r.o.
Odpovědná osoba : Jan Kozák
Pozice : Senior Product Specialist

Hlavní přínosy řešení

- Nezpochybnitelná a bezpečná autentizace uživatele do operačního systému
- Zabezpečení dat organizace před zcizením pomocí transparentního on-line šifrování
- Ochrana dat nejen na lokálním disku stanice, ale i dat uložených na sdíleném či výměnném úložišti
- Uživatelé pracují ve standardním prostředí a jejich způsob práce se nijak nemění
- Centrální management s definováním bezpečnostní politiky
- Nezávislost šifrování na uživateli
- Kombinace s HW předměty jako s bezpečnými úložišti šifrovacích klíčů a přihlašovacích údajů

Díky řešení od SODATSW se již Synthesia neobává ztráty citlivých informací

Zákazník potřebuje zabránit možnému zneužití informací při ztrátě zařízení

Společnost Synthesia byla postavena před problém, kdy došlo ke ztrátě několika notebooků obchodních zástupců firmy. Bohužel nebylo možné přesně zjistit, jaká data byla na zařízeních uložena. Hrozilo tak reálné riziko, že obsahovala informace o dodavatelích a výrobcích společnosti. Což jsou přesně ta data, kterých může konkurence snadno využít pro svůj prospěch. K zabezpečení přístupu do operačního systému se doposud využívalo pouze uživatelské heslo a obavy tak byly oprávněné.

Bylo tedy nutné nalézt takové řešení, které by do budoucna zcela vyloučilo možnost zneužití informací třetí stranou. Společnost Synthesia oslovila celkem tři firmy zabývající se vývojem a implementací bezpečnostních řešení. Jednotlivé produkty prošly testovacím provozem přímo v prostředí organizace. Byly zváženy veškeré přednosti a nedostatky jednotlivých řešení.

Nejlépe se v testech osvědčilo řešení Datový trezor od společnosti SODATSW, které splnilo všechny důležité požadavky kladené společností Synthesia. SODATSW pracovala na vývoji řešení od roku 1997 a v roce 2000 oficiálně představila první plně provozovatelnou verzi. Inovátorské technologie použité v tomto software byly oceněny hned dva krát a to Křišťálovým diskem a Best of Invex 2000.

Datový trezor je bezpečnostním řešením, které chrání data pomocí on-line transparentního šifrování souborů. Je možné šifrovat data na lokálních discích, přenosných médiích a lze jej využít i k zabezpečení sdílených složek a souborů. Jeho výhodnou je možnost využití hardware předmětů (tokeny nebo čipové karty) jako bezpečného úložiště šifrovacích klíčů, hesel a certifikátů. Díky kryptografickému čipu je nemožné takto uložené informace zneužít. Soubory zašifrované těmito klíči jsou dostupné jen pro uživatele, který vlastní odpovídající klíč.

Řešení má i řadu dalších benefitů. Jedním z nich je eliminace ohrožení ze strany vlastních zaměstnanců. Využití symetrické kryptografie umožňuje, bezpečnostní klasifikaci dat dle přidělených šifrovacích klíčů. K určité informaci má přístup pouze oprávněná osoba, což umožňuje prostředí společnosti certifikovat. Celé řešení Datový trezor je postaveno na modulech z produktu Desktop Security System AreaGuard. Ten obsahuje celkem šest modulů, přičemž Datový trezor tvoří moduly AreaGuard Gina, AreaGuard Notes a AreaGuard AdminKit.

Technické údaje

Šifrování souborů

- Provádí filesystémový driver pro Windows 2000/XP/Vista
- On-line šifrování souborů v okamžik jejich použití
- Využití symetrické kryptografie – typicky AES 128bit
- Oddělené od operačního systému, snadná recovery
- Nastavení podle lokace souboru nebo typu souboru
- Šifrování na úrovni filesystému chrání data před maximem možných způsobů krádeže dat – od krádeže celého zařízení (NTB) až po jejich kopírování na USB disk

Data společnosti jsou v bezpečí

Datový trezor používá společnost Synthesia od roku 2004, kdy na základě předchozích zkušeností a se stále rostoucím počtem zaměstnanců, kteří používají mobilní zařízení, rostlo i riziko ztráty citlivých informací. Systém v organizaci pomáhal nasadit přímo společnost SODATSW jako výrobce a implementátor tohoto řešení. Datový trezor je v organizaci využíván k ochraně informací na notebookech vedoucích pracovníků a zařízeních, která obsahují pro firmu důležité informace.

Díky vynikající spolupráci za strany společnosti Synthesia proběhlo nasazení systému bez potíží. Samotných uživatelů mobilních zařízení se implementace nedotkla a neměla vliv na jejich pracovní činnost. U zaměstnanců, kteří mají svá zařízení chráněna řešením Datový trezor, proběhlo zaškolení a seznámení se všemi možnostmi a funkcemi. Samotný systém při dodržování správných postupů neklade na jeho uživatele žádné zvláštní nároky. Na první pohled není zřejmé, že data jsou šifrována. Zaškolení techniků, kteří systém spravují, probíhalo současně s instalací klientských stanic a díky tomu byl celý systém spuštěn ve velmi krátkém čase.

Šifrování je tou správnou volbou

O tom co řešení Datový trezor společnosti Synthesia přineslo, jsme hovořili s paní Ivanou Pavlíkovou, vedoucí Odboru informatiky: „*Nedávno jsme museli řešit krádež notebooku jednoho z našich zaměstnanců. Ztráta zařízení je vždy nepříjemná. Díky tomu, že na notebooku bylo nainstalováno šifrování dat a uživatelé dodržují bezpečnostní politiku, která nařizuje mít token oddělený od zařízení, nedošlo k úniku dat. Nevznikl tak žádný bezpečnostní incident a společnost mohla být klidná. Právě kvůli podobným situacím, jsme Datový trezor pořizovali*“

Synthesia není první organizací, kde Datový trezor zabránil uniku citlivých informací. Díky řešení od společnosti SODATSW se zde data nedostala do nepovolaných rukou. Velmi často se ovšem z různých médií dozvídáme o organizacích, které byly finančně poškozeny právě v důsledku ztráty citlivých informací. Svě o tom ví i pracovníci společnosti SODATSW, kteří se s případy, kdy společnost o svá data reálně přišla, setkávají běžně. Takové problémy Synthesii opravdu nehrozí.

Synthesia využívá všech výhod, které ji řešení Datový trezor poskytuje. Se systémem jsou spokojeni a účel, ke kterému byl pořízen, plní bez chyb. Vedení organizace se neobává ztráty citlivých informací a ani případného zneužití vlastními zaměstnanci.

Technické údaje

Podporované HW předměty

- Typické využití s tokeny nebo kontaktními čipovými kartami
- Vyžaduje PKCS#11 kompatibilní zařízení
- Standardně dodávaný hardware: řešení společnosti SafeNet (tokeny iKey, čipové karty DataKey), řešení společnosti Aladdin (tokeny eToken PRO, tokeny s flash pamětí eToken NG FLASH, karty eToken SmartCard)
- Možnost dalšího využití HW předmětů

Součásti řešení Datový trezor:

AreaGuard Gina

je rozhraní umožňující jednoduché a bezpečné přihlášení do operačního systému. Podporuje hardwarové předměty pracující na standardu PKCS#11, do kterých ukládá uživatelské přihlašovací informace. V AreaGuard Gina je implementován generátor, který umožňuje vygenerovat dostatečně bezpečné uživatelské heslo. Pro přihlášení do operačního se pak využívá 4 až 8 místný PIN, kterým je chráněn obsah kryptografického čipu.

AreaGuard Notes

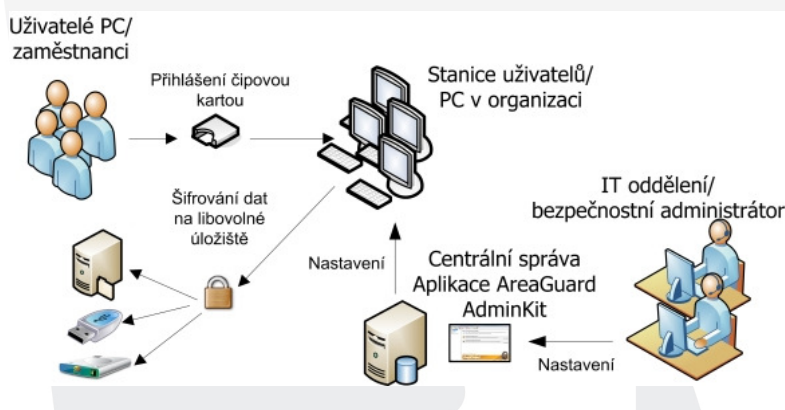
je uživatelsky příjemný a také vysoce účinný nástroj, který umožňuje on-line šifrování souborů ve specifikovaných adresářích (např. Dokumenty daného uživatele). Informace jsou šifrovány symetrickými algoritmy, které jsou dostatečně rychlé a bezpečné. AreaGuard Notes využívá moderních algoritmů AES, IDEA, 3DES. Šifrovací klíče jsou bezpečně ukládány do hardwarových předmětů. Koncepte systému nevytěžuje koncovou stanici ani uživatele, který na ní pracuje.

Výhodou on-line šifrování prostřednictvím AreaGuard Notes je naprosto nenápadný provoz, kdy uživatel neregistruje žádné byt' sebemenší změny ve své práci s daty.

AreaGuard AdminKit

umožňuje pohodlně spravovat i velké množství koncových stanic. V rámci přehledného grafického rozhraní lze rychle a efektivně sledovat a nastavovat desítky, stovky či tisíce instalací produktu AreaGuard. Šifrovací klíče, certifikáty a nastavení bezpečnostní politiky jsou bezpečně uloženy v zálohované databázi, k níž má přístup pouze bezpečnostní administrátor. Aplikaci je možné využít také v případě obnovy uživatelských šifrovaných dat. AreaGuard AdminKit umožňuje vzdáleně měnit nastavení jednotlivých koncových stanic a tím i způsob šifrování dat.

Schéma práce:



Zákazník

Synthesia, a.s.

Synthesia je předním evropským výrobcem kvalifikované chemie s více než osmdesátipětiletou tradicí. Společnost Synthesia zaměstnáváme 2 100 zaměstnanců a její obrat v roce 2007 přesáhl 126 milionů EUR. Což ji řadí mezi největší tuzemské výrobce chemie. Její podnikatelské aktivity jsou zacíleny do tří tržních segmentů: pokročilých organických intermediátů, derivátů celulózy a pigmentů a barviv. Společnost je součástí skupiny AGROFERT, která obchoduje s komoditami chemického a zemědělsko-potravinářského sektoru. Tato skupina je dnes obrátově největší skupinou v českém zemědělství a druhou největší v české chemii.



Poděkování

SODATSW děkuje společnosti Synthesia a všem zúčastněným za vstřícný přístup a poskytnutí všech potřebných informací, bez kterých by tato případová studie nemohla vzniknout.

SODATSW spol. s r.o.

Společnost SODATSW spol. s r.o. je výrobcem a dodavatelem originálních řešení určených pro správu a bezpečnost pracovních stanic v sítích bankovního a komerčního sektoru, státní správy, školství a v neposlední řadě i domácích uživatelů.

Cílem společnosti SODATSW je poskytovat svým zákazníkům komplexní služby a řešení, které jsou špičkou ve svém oboru a přinášejí zákazníkům konkurenční výhody v jejich podnikání. Dbáno je také na důvěru a spokojenost zákazníků, které jsou založené na dlouhodobých vztazích, vstřícném přístupu a vysoké kvalitě poskytovaných služeb a řešení.

Reference společnosti SODATSW je možné nalézt na adrese <http://www.sodatsw.cz/o-nas/reference.html>

SODATSW spol. s r.o., Horní 32, 639 00 Brno, Tel.: +420 543 236 177
e-mail: info@sodatsw.cz
www.sodatsw.cz

AreaGuard[®]

www.areaguard.cz



KŘIŠŤÁLOVÝ DISK

