Případová studie: Bezpečnostní systém AreaGuard®

Profil zákazníka
Softwarová firma SODAT software spol. s r.o. skládající se z obchodního, vývojového, technického a logistického oddělení, které zastřešuje vedení společnosti. Zaměstnanci jednotlivých oddělení zpracovávající informace patřící jednomu nebo více oddělení v interním informačním systému.

Cíle
- Zavést bezpečnou autentizaci uživatelů k informačnímu systému uvnitř organizace.
- Šifrovat dokumenty a zdrojové kódy v lokálních a sdílených složkách informačního systému.
- Zajistit zálohování souborů v šifrované podobě.
- Umožnit ověřený elektronický podpis e-mailové komunikace mezi zaměstnanci uvnitř organizace.

Co systém řeší
Systém AreaGuard® doplněný hardwarovými tokeny iKey 1000 umožňuje autentizaci zaměstnanců k informačnímu systému pomocí elektronického podpisu, on-line šifrování souborů v lokálních a sdílených síťových složkách, šifrování výměnných disků k zálohování a implementace zaručeného elektronického podpisu do mailového klienta a možnost jeho vnitřního ověření.

Přínosy
- Bezpečná autentizace k informačnímu systému pomocí elektronického podpisu, kdy veškeré privátní informace jsou uloženy v HW tokenu iKey 1000 zaměstnance.
- Zaměstnanci si nemusí pamatovat hesla, ale pouze jednoduchý PIN k HW tokenu iKey 1000. Kontrola PIN je řízena HW tokenem, která neumožní vícenásobné chybné zkoušení PIN.
- Soubory s citlivými informacemi se nikdy na disku neobjeví v otevřené podobě.
- Šifrovací klíče k zašifrovaným souborům jsou vždy uloženy v HW tokenu iKey 1000.
- Na záložních CD discích jsou data zašifrována a mohou tak být uložena i v cizím externím prostředí.
- Předávání informací (úkolů) mezi zaměstnanci pomocí e-mailu s možnou kontrolou, jestli e-mail opravdu odeslal podepsaný zaměstnanec.

Produkty firmy Microsoft
MS Windows 2000 Server
MS Windows 2000 Professional
IIS 5.0, Certification Authority
MS Exchange 2000
ADO 2.6
Jiné produkty
AreaGuard®
CSP Rainbow Technologies

Zákazník
SODAT software spol. s r.o., Martin Hanzal, Sedlákova 33, 602 00 BRNO, tel.: 543 236 177, martin@sodatsw.cz

Systém AreaGuard® v informačním systému SODAT software spol. s r.o.

Společnost SODAT software spol. s r.o. se zabývá vývojem komerčního a zákaznického software a jeho následnou distribuci ke koncovým zákazníkům nebo distributorům. V informačním systému společnosti jsou uloženy zdrojové kódy k vyvíjenému software, smlouvy s uživateli a informace o případných technických supportech u zákazníka, obchodní nabídky a kalkulace, finanční, účetní data a veškeré kontakty (telefonní seznam) společnosti. V celém informačním systému je 20 uživatelů z nichž každý má oprávnění se pohybovat v určitých částech informačního systému.

Společnost si je vědoma hodnoty zpracovávaných informací a svého know-how, takže již od svého založení řeší zabezpečení uložených dat proti možnému útoku zevnitř nebo zvenčí organizace. O tom svědčí i bezpečnostní politika, která se netýká pouze informačního systému, ale také provozu kanceláří a objektu kanceláří. Veškeré informace společnosti jsou uloženy v elektronické podobě, což ještě více přispívá k nutnosti pečlivého zabezpečení těchto informací.

Problémy před zavedením systému AreaGuard®

Před zavedením systému AreaGuard® se nejčastěji na všech odděleních řešil problém s autentizací do operačního systému. Zaměstnanci si museli měnit svá přístupová hesla dle bezpečnostní politiky, ale stávalo se, že složitější hesla byla někde poznamenaná a tím i zneužitelná. Dále uložení zdrojových kódů a citlivých dokumentů organizace nemohlo být na síti, ze které je přístup do vnější sítě, což přinášelo fyzické oddělení informačního systému. Stejně tak zálohovaná data musela být pečlivě uložena v trezorech. Veškerá ochrana přístupu k datům byla řízena na serveru přístupovými právy (tehdy systém MS NT 4.0) a v případě lokálních dat nebyla ochrana žádná.

Způsob nasazení

V roce 2000 společnost vypracovala projekt nasazení zabezpečení dat pomocí systému AreagGuard®. Vlastní implementace začala v únoru 2000 a první fáze byla dokončena v srpnu 2000, kdy byly implementovány požadované bezpečnostní mechanismy do informačního systému společnosti. Na serveru společnosti byl nainstalován MS Windows 2000 Server se službami Active Directory, IIS a certifikační autoritou. Kromě produktů MS byly instalovány CSP od Rainbow a AreaGuard® Notes k šifrování souborů na serverovém disku. Koncové pracovní stanice běží na MS Windows 2000 Professional s instalovaným CSP od Rainbow a AreaGuard® Notes.

Ve společnosti byl ustanoven bezpečnostní správce, který má na starosti kontrolu nad všemi bezpečnostními mechanismy, správu nad používanými šifrovacími klíči a řízení zálohování společnosti. Tento bezpečnostní správce každému uživateli naplní HW token iKey 1000 uživatelským certifikátem a příslušným privátním klíčem, osobním šifrovacím klíčem a šifrovacími klíči pracovních skupin (oddělení), do kterých zaměstnanec patří. Na koncových pracovních stanicích nastaví bezpečnostní správce adresáře, ve kterých se nachází citlivé soubory.

Takto se podařilo zabezpečit autentizaci do informačního systému pouhým vsunutím iKey 1000 a zadáním osobního PIN, možnost mít šifrovány veškeré citlivé soubory na lokálním nebo sdíleném disku a tím i možnost mít počítače připojeny do vnější sítě, ukládání šifrovaných souborů na záložní CD disk a v neposlední řadě použít ověřený elektronický podpis v rámci společnosti a

případných partnerů, kteří budou důvěřovat vnitřní certifikační autoritě společnosti.

Vyskytnuté problémy během používání a jejich řešení
Implementace bezpečnostního řešení byla ukončena v srpnu roku 2000 bez závažnějších technických problémů. Od této doby se během provozu vyskytly spíše organizační problémy, které se postupně řešily. Prvním problémem byla možnost vytvoření a používání vlastního zaměstnancem definovaného šifrovacího klíče. K takto zašifrovaným datům by pak nebylo možné se dostat bez přítomnosti zaměstnance. Proto v listopadu 2000 byla rozšířena bezpečnostní politika používání AreaGuard® Notes o odebrání veškerých ovládacích prvků systému běžným zaměstnancům. K šifrování lze použít pouze šifrovací klíče uložené v HW tokenu iKey 1000, kde je může vytvořit pouze bezpečnostní správce.

Dalším problémem byla nemožnost on-line šifrování souborů na sdíleném serverovém disku. Zaměstnanci museli zašifrované soubory nejprve stáhnout na lokální disk a tam s nimi mohli pracovat. Při uložení zpět na síťový disk muselo být neaktivní šifrování. Mohlo se tak stát, že by se soubor objevil na sdíleném disku v nezašifrované podobě. Vše vyřešil update systému AreaGuard® Notes v březnu 2001, který již umožňuje on-line šifrování na zvolených sdílených složkách.

Od prvopočátku musel bezpečnostní správce evidovat používané šifrovací klíče a ty ukládat do HW tokenu a nastavovat na koncových pracovních stanicích do systému AreaGuard® Notes. Evidence byla prováděna pomocí Excelu. Vše bylo vyřešeno v březnu 2002, kdy byl nasazen systém AreaGuard® AdminKit, který umožňuje evidenci všech zaměstnanců, šifrovacích klíčů a konfiguraci AreaGuard® Notes na jednotlivých stanicích. AreaGuard® AdminKit dokáže plnit šifrovací klíče do HW tokenu iKey 1000 při inicializaci. Dále je možné vzdáleně konfigurovat AreaGuard® Notes na koncových pracovních stanicích, vzdálenou distribuci šifrovacích klíčů do tokenů iKey 1000. Nástrojem AreaGuard® AdminKit se správa celého řešení velmi zjednodušila a časová náročnost na provedení nějaké změny se snížila na desetinu původně stráveného času před zavedením AreaGuard® AdminKit.

Projekt pokračuje dále
V současné době je systém AreaGuard® Notes velmi jednoduchý na správu, nenápadný vůči uživateli a velmi spolehlivý. Podle bezpečnostního správce není žádný problém nasadit tento systém na stovky či tisíce počítačů a on sám by neměl obavy dělat bezpečnostního správce systému AreaGuard® Notes na takovémto množství stanic.