

Chraňte svá data

Společnost SODAT software se už několik let etabluje na poli ochrany hardwaru i softwaru. Její poslední novinkou je nová verze bezpečnostního šifrovacího systému AreaGuard Notes.

Jde o technické a programové řešení ochrany počítačů, využívající metodu "vlastnit a znát". To, co vlastníte, je hardwarový předmět, kterým je buď USB Smart Token (iKey), nebo čipová karta (Smart Card), a znát musíte PIN. V tokenu je uložen certifikát uživatele a uživatelův podpisový klíč, který je přístupný pouze po zadání PIN. Prostřednictvím PIN se přihlásíte k tokenu a ten zajistí vše další.

Osobní strážce

Systém AreaGuard Notes (dále jen AGN) umožňuje:

- * autorizovaný přístup k operačnímu systému počítače pomocí tokenu;
- * on-line šifrování souborů, které je dostatečně rychlé a uživatel ho nevnímá;
- * vytvoření bezpečného, šifrovaného, komunikačního kanálu v rámci virtuální privátní sítě. Šifrování a dešifrování probíhá v paměti lokální stanice;
- * ukládání souborů jen na určené místo v chráněné oblasti. V této oblasti jsou data zašifrována. S daty mohou pracovat jen privilegované aplikace. Ty mohou soubory číst z privilegované oblasti a jen do ní je ukládat.

Ochrana počítače je podstatně spolehlivější než pouhé heslo pro vstup do počítače. Zcizením počítače (notebooku) se nezcijí data - jsou zašifrována, v reálném čase nerozlušitelná.

Rozšíření bezpečnosti operačních systémů

AGN nevyžaduje souborový systém NTFS. Umožňuje on-line šifrování souborů a celých složek na libovolném disku: lokálním, výměnném i síťovém. Šifrovací klíče jsou uloženy na tokenu (předmětu). Umožňují šifrování a elektronický podpis e-mailové komunikace, administrátor firemní sítě tedy nemůže e-maily číst. Lze nastavit časovou platnost šifrovacích klíčů. Tajné části šifrovacích klíčů se nacházejí v šifrované databázi Access, AD nebo LDAP. Při reinstalaci operačního systému nedojde ke ztrátě certifikátů a dat.

S čím AGN pracuje

Pro bezproblémovou práci AGN je zapotřebí počítač s USB portem. Do něho se zasouvá iKey. Na počítačové stanici by měl běžet operační systém Windows od verze 9x a na serveru Windows 2000 nebo XP. Tokeny, iKey 1000, 1032, 2000 nebo 2032 či čipové karty jsou od renomované firmy Rainbow Technologies. Vyhovují standardu PKCS#11, obsahují mikroprocesor a velice snadno se instalují.

Jak AGN pracuje

AGN "se tváří" v operačním systému jako ovladač souborového systému. Tím, že se zavádí bezprostředně po jádru systému, před aktivací prvního souborového systému, je dána jeho vysoká bezpečnost. Pro šifrování lze vybrat jeden z následujících algoritmů a délku klíče: 3-DES (112 bitů), IDEA (128), RC4 (40 a 128) a AES (Rijndael, 128). Systém se skládá ze dvou částí. První z nich slouží pro ochranu stanic a je tvořena USB portem s iKey a softwarem AGN. Druhou částí je správa stanic ze serveru. Tu tvoří USB port s iKey a software AreaGuard AdminKit. AdminKit je určen k centrální správě bezpečnostního systému AGN. Umožňuje nastavovat, sledovat, obsluhovat a evidovat uživatele a tokeny, šifrovací klíče a uživatelské certifikáty a nastavení AGN na pracovních stanicích. Nastavení parametrů se děje prostřednictvím AdminKitu, který je k dispozici pouze bezpečnostnímu správci. Umožňuje správu stanic na dálku, a to i v automatickém režimu. Uživatel nemůže nastavení tokenu měnit. Lze dokonce určit, aby pro práci AdminKitu muselo být přítomno více osob současně.

Přednosti systému

Oproti prostředkům Windows je AGN méně časově náročný, má snadnou administraci a umožňuje hromadné nasazení ve firmě. Systém myslí i na situace, které se mohou zdát samozřejmé, ale ne u všech bezpečnostních systémů tomu tak je. Např. reinstalací operačního systému se zachová ochrana a čtení

dat. Ztratíte iKey? Žádná pohroma. Stačí zavolat bezpečnostnímu správci, který vám nadiktuje heslo, a počítač bude plně funkční. Po návratu do firmy se nastaví nová ochrana. Token lze přidat zcela snadno ke klíčům od bytu, a tak je pravděpodobnost jeho odložení či ztráty velice malá. Přenos dat mezi aplikacemi (buď stejnými) není možný pomocí schránky Windows ani schránky sady Office. Lze šifrovat i soubory v dočasných adresářích, \Temp. Do šifrované složky může mít přístup více uživatelů. Čte-li privilegovaná aplikace z chráněné oblasti v síti, data se přenáší v zašifrované podobě. Není omezení na velikost souboru. Nastavení AreaGuardu lze uložit na záložní médium a použít k obnově nastavení při havárii systému. O všech operacích s AdminKitem je veden žurnál, takže lze kontrolovat i bezpečnostního správce. Volitelným doplňkem produktu je AreaGuard FirmWall, který umožňuje chránit data proti zcizení zaměstnancem firmy tím, že lze data ukládat jen na médium, jež určí bezpečnostní správce, do oblastí, které jsou zašifrovány.

Komu padne?

Ochrana dat systémem AreaGuard Notes je zaměřena na ochranu dat šifrováním on-line na pozadí. Kombinací softwarové a hardwarové ochrany se dosahuje vysokého stupně bezpečnosti. Jde o plně profesionální aplikaci, zabezpečující data na 100 %. Lze ji využít jak k nasazení na několik počítačů, tak do rozsáhlé sítě. Pro koho může být AGN přínosem? Pro všechny, kteří pracují s důvěrnými daty: pro vedoucí pracovníky, právníky, personalisty apod. Systém je velice vhodný pro "mobilní kanceláře".

Milan Brož

AreaGuard Notes, verze 2

Bezpečnostní systém.

Pro operační systémy Stanice: Windows 9x, NT, 2000 a XP Server: Windows 2000 a XP

Výrobce SODAT software spol. s r. o. www.areaguard.cz

Cena podle počtu licencí 1 licence AreaGuard Notes 2099 Kč Token iKey 1565 Kč