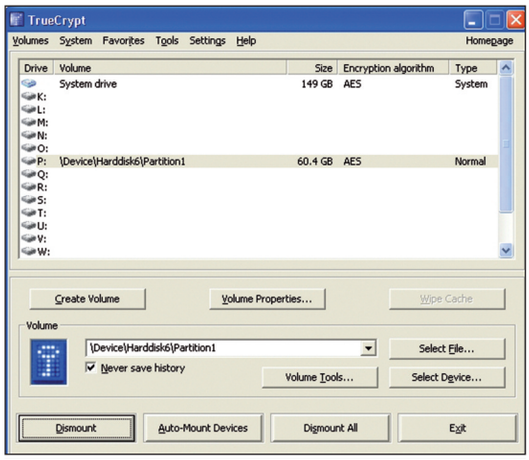
USB trezory aneb jak Pašák chránil data (2)

Pašáky nazýváme v našem seriálu „odborníky, co všechno ví, a hned jdou na věc“. V minulém čísle Sdělovací techniky bylo ukázáno, jak se jim podařilo zničit původně velice užitečný a bezpečný flash disk.



Obr. 1 Zde je šifrovaný celý pevný disk se systémem a šifrovaný flash disk je připojen jako logický disk P

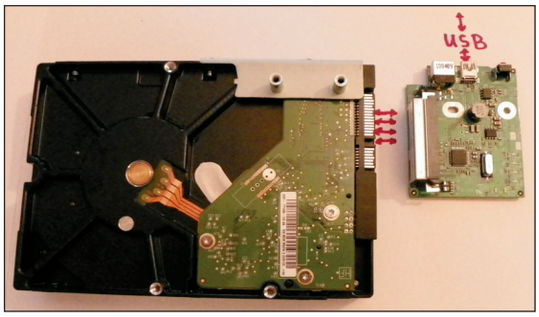
Také jsme nakousli téma, jak výhodný je hardwarově šifrovaný flash disk a zjistili jsme, že šifrování samo o sobě nestačí pokrýt všechny hrozby. Při komerční reklamě na hardwarově šifrované flash disky můžeme získat dojem, že v naší organizaci vyřeší všechny problémy s „cestujícími“ daty a cestujícími zaměstnanci. Pochopitelně to vyřeší jen málo hrozeb, ovšem i to má cenu. Pokud zjišťujeme, jakou že cenu to má, od čistě technické otázky se nakonec dostáváme k analýze hrozeb a rizik a výpočtu investice, která se vyplatí na pokrytí těchto hrozeb.

Co vyřeší hardwarově šifrovaný flash disk?

Hardwarově šifrovaný flash disk chrání především data na flash disku v případě jeho ztráty nebo krádeže. Případný zloděj nebo nálezce nemá mnoho šancí na získání dat z flash disku, řekněme, že téměř žádnou. Jenže teorie šedivá je a zelený je strom života, a tak není vůbec nepravděpodobné, že se flash disk ztratí společně s notebookem nebo naopak notebook s flash diskem. V tomto případě na notebooku jistě nalezneme data velmi podobné hodnoty (nebo dokonce shodná) s těmi, co jsou na flash disku, neboť uživatel flash disk nosí proto, že chce s těmito daty pracovat. Takže se dostáváme k podivnému závěru, že šifrovaný flash disk je nám skoro na nic, pokud také nešifrujeme data na notebooku. Není divu, vždyť jsou to naprosto shodné věci a situace – v notebooku je také disk s daty. Tento interní harddisk by měl být tedy chráněn stejně jako externí disk. A pomalu se dostáváme k závěru, že taková ochrana má už smysl a je účinná pro velmi mnoho praktických situací. Nechceme ani nemůžeme posoudit všechny případy a nuance použití dat u cestujících zaměstnanců nebo soukromých osob, ale vidíme, že řešit ochranu flash disků ve vzduchoprázdnu je nesmysl a že se dále musíme ptát minimálně na:

Obr. 2 Druhá nejčastější obrazovka Truecryptu

– bezpečnost při vkládání hesel,
– bezpečnost samotných hesel a možnost jejich zkoušení útočníkem,
– bezpečnost systému, ke kterému je flash disk připojen v době, kdy je z něj možné číst data,



Obr. 3 U velkého USB disku (2TB) zajišťuje HW šifrování přídavná destička na obrázku

– ochranu takového systému společně s ochranou flash disku.

Použitelné řešení

Prakticky použitelných řešení není mnoho. Zaměstnanci různých organizací, kde musí chránit data, vám řeknou, jak jim tyto ochrany znepříjemňují život nebo jak je obchází. V tomhle jsou uživatelé na celém světě skutečnými mistry. U soukromníků je tomu jinak, protože oni sami mají na ochraně zájem, a v případě, že uživatel spolupracuje, lze nalézt i poměrně levné řešení. Hojně používané je šifrování dat na počítačích, noteboocích i flash discích pomocí programu Truecrypt. Výhodou je, že lze nastavit šifrování všech dat na notebooku i na flash disku i na stolním počítači s OS Windows nebo Linux a že v bezpečnostních parametrech téměř nahrazuje čistě hardwarové šifrování. Dále je toto řešení zcela zdarma a samo o sobě je v současné době neprolomitelné. Kvalitu hesla, které se vkládá při bootování systému nebo při připojení flash disku si uživatel ohlídá sám. Zbývá už jen opravdu velmi malá skulinka, kterou mnozí z nás pominou v rámci její (ne)pravděpodobnosti. Jsou to sofistikované útoky na hardware v době, kdy se dostane mimo dohled uživatele. Bezpečnostní specialisté (pro mnohé paranoici) si jistě dovedou představit, že když lze nalepit falešnou klávesnici na bankomat, půjde udělat i něco s hardwarem notebooku tak, aby se získalo uživatelovo heslo. Tento bezpečnostní aspekt lze také řešit, ale nikoli snadno. Například tím, že klíč k notebooku bude právě na flash disku... Pak ovšem zase nesmíme dát z ruky flash disk... Tento téměř nekonečný proces úvah a protiopatření v praxi záhy přetnou peníze – náklady nutné na útok, předpokládaný výnos z útoku nebo naopak náklady na bezpečnost a předpokládaná úspora oproti ztrátě dat.

Ideální řešení

Podíváme se na jedno možné ideální řešení, bez ohledu na cenu. Znamená chránit notebook, flash disk i stolní počítač softwarovým nebo hardwarovým šifrováním, a to kompletně celých jejich disků. Znamená to nepoužívat hesla, ale kvalitní náhodné klíče, uložené na přístupových tokenech, jako jsou čipové karty nebo USB flash disky. Na uživateli nesmíme chtít, aby si pamatoval dlouhé heslo. Proto budeme muset flash disky, notebooky nebo stolní počítače vybavit snímačem otisku prstu a flash disky navíc klávesnicí pro vkládání PIN. Nutně musíme omezit počet nesprávně vložených PIN. Hardwarově šifrovaný flash disk s klávesnicí, displejem a snímačem otisku prstu je ideální. Podobně ideální jako snímač otisku prstu u notebooku společně s PINem. To je kvalitní a systémové řešení, které uživatel těžko obejde a útočník jen ztěží napadne. Otázka je, jestli takové najdeme. Pokud ne, vyplatí se nám z něho realizovat alespoň to, co můžeme.

Vždy je dobré udělat si svoji analýzu rizik u svého systému a realizovat opatření na míru jak svým požadavkům bezpečnosti, tak možné výši nákladů. Například je otázka, zda opravdu potřebujeme klávesnici a displej u flash disku typu klíčenka. Někdy to potřeba nebude – např. když budeme mít zajištěnu bezpečnost počítačů a notebooků, pak displej a klávesnici klíčenky můžeme myšlenkově přesunout na notebook. PIN (otisk prstu) lze pak zadávat na notebooku a klíčenka může být jen holá. Protože všechny možné podmínky a kombinace situací popsat nelze, dali jsme v obou článcích určitý návod, jak ochranu koncipovat a co je důležité.

Zkušenosti s Truecryptem

Zkušenosti? Od doby, co jsme ho nasadili, o něm téměř nevíme. Zpoždění neregistrujeme, jeho přítomnost také ne. Ovšem zdržuje nás bootování, kdy musíme zadávat heslo a heslo zadáváme opravdu dlouhé a kvalitní. Pak nás ale Truecrypt nechá na pokoji. Jen když zase chceme připojit šifrovaný flash disk, opět musíme něco udělat. Flash disk se připojí pomocí menu a opět se zadá heslo. S notebookem je to jakbysmet. Flash disk používáme velmi mechanicky odolný (náraz, voda, požár) v provedení na klíčence. Odolnost je důležitá, klíče i flash disk se při otáčení v zámku dost často „mlátí“ o kovovou zárubeň a poměrně často spadnou na dlaždice na podlahu. Flash disk používáme zároveň k zálohování důležitých dat, čili řešíme i otázku zálohování a fyzické ochrany. K zálohování používáme vynikající freewarový program SyncBack, který synchronizuje data mezi přenosným flash diskem a mezi notebookem/počítačem. Dále máme zálohu na velkých USB discích, které jsou pochopitelně také šifrované Truecryptem. Tento flash disk nepoužíváme v nebezpečném prostředí, pouze v prostředí mezi našimi počítači. Proto nepotřebujeme klávesnici na klíčence. Pokud pracujeme v nebezpečném prostředí, musíme na to mít vyhrazený jiný nešifrovaný flash disk. Tentýž disk používáme na přenášení dat od známých nebo spolupracujících.

Jak v malé firmě nebo větší organizaci?

Nezbývá smutně konstatovat, že žádné obecné řešení neexistuje ani ho nemáme k dispozici. Vždy se budou muset udělat úvahy, co a jak chránit (čili ona analýza rizik a možných řešení), a potom udělat nějaký kompromis. Tak to také skutečně vždy probíhá.

Vlastimil Klíma, kryptolog,
vlastimil.klima@knzsro.cz

LITERATURA

[1] Klíma, V., Rosa, T.: Kryptologie pro praxi (48) – Šifrování USB Flash disků zdarma. Sdělovací technika, 8/2007, str. 9.

[2] Klíma, V., Rosa, T.: Kryptologie pro praxi (47) – Šifrování datových úložišť. Sdělovací technika, 7/2007, str. 18.

[3] Články jsou dostupné elektronicky na osobních stránkách autora.