ZABEZPEČENÍ PŘENOSNÝCH POČÍTAČŮ

NÁVRH, NASAZENÍ, UPGRADE, ZABEZPEČENÍ A SVĚŘENÁ SPRÁVA

KROMĚ ZVÝŠENÉ MOBILITY S SEBOU PŘENOSNÉ POČÍTAČE PŘINÁŠEJÍ I VÝRAZNĚ ZVÝŠENÁ RIZIKA KOMPROMITACE FIREMNÍCH DAT. ZÁKLADNÍ OBRANOU PROTI TOMUTO STÁLE ROSTOUCÍMU RIZIKU JE CELODISKOVÉ ŠIFROVÁNÍ.

Přenosné počítače se staly v posledních letech nedílnou součástí pracovního procesu mnoha lidí. Na jednu stranu zvyšují produktivitu, dostupnost a komfort zaměstnanců, na druhou stranu však s sebou přináší nová rizika.

[PROČ ZAVÁDĚT ŠIFROVÁNÍ PŘENOSNÝCH POČÍTAČŮ]

Ztráty a krádeže přenosných počítačů se rok od roku zvyšují a s nimi rostou i ztráty korporátních dat. Podle studie společností Mediaresearch a Intel provedené v České republice se průměrná cena ztráty pracovního notebooku pohybuje okolo čtvrt milionu korun. Z toho jen asi pětina představuje cenu zařízení, zbylá hodnota vyjadřuje nacenění ztráty firemních dat. Množství citlivých dat na počítačích je často podceňováno, neboť lidé si často neuvědomují, jaká všechna data na jejich zařízení jsou. Jedná se nejen o dokumenty, e-maily, kontakty, schůzky či úkoly, ale také například o hesla používaná pro přístup k počítači a často k autentizaci vůči pracovní doméně, privátní klíče od certifikátů, nastavení wifi sítí a VPN připojení. Všechny tyto informace jsou i pro průměrně schopného zloděje lehce dostupné.
Vhodně zavedené šifrování umožňuje snížit cenu ztráty přenosného počítače na cenu hardwaru plus ztrátu produktivity. Je však nutné zajistit, že všechna citlivá data na přenosném počítači jsou zašifrována. Zajistit šifrování všech citlivých dat v případě souborového šifrování je velice náročné.

VLASTNOSTI A VÝHODY

- Bitlocker umožňuje využívat TPM čip pro uložení části klíče a zvyšuje tak bezpečnost řešení
- Správu počítačů šifrovaných Bitlockerem je možné provádět běžnými prostředkysystému Microsoft Windows
- Bitlocker je obzvláště vhodný pro zabezpečení přenosných počítačů s operačními systémy Microsoft Windows, neboť je jejich standardní součástí v edicích běžně pořizovaných ve firemním prostředí

Důvody jsou následující:

- Nutnost správného určení citlivých informací
- Potřeba zajistit kvalitní smazání citlivých informací, které vznikly nezašifrované
- Potřeba ochrany dočasných souborů, které si vytvářejí různé aplikace ve kterých jsou data zpracovávána
- Potřeba ochránit hibernační a stránkovací soubory, které mohou obsahovat citlivá data

Z výše uvedených důvodů je pro ochranu dat na přenosných počítačích vhodnější zavést šifrování celých pevných disků místo šifrování souborového. Takové šifrování je pak pro uživatele zcela transparentní a jediná změna souvisí se způsobem spouštění počítače, kdy je nutné zadat šifrovací klíč ve formě hesla a/nebo usb klíčenky. Následně už se počítač chová stejně jako předtím než byl zašifrován.

[NABÍZENÉ TECHNOLOGIE]

Od verze Vista obsahuje operační systém Microsoft Windows celodiskový šifrovací prostředek Bitlocker umožňující šifrování disků obsahujících operační systém, který zajišťuje v Microsoft Windows Vista a Windows 7 jak ochranu zbytkových informací, tak i částečnou integritní ochranu operačního systému. Ve Windows 8 lze docílit podobného výsledku při použití Bitlockeru v kombinaci s funkcí Secure Boot.

Velkou výhodou Bitlockeru je jeho integrace s operačním systémem, která výrazně zjednodušuje řešení problémových situací, které mohou nastat například při narušení souborového systému, potížích s drivery či jiných podobných situacích.

Verze Windows 10 již obsahuje nástroj Bitlocker i v edici Pro (nejenom Enterprise jako u Windows 7).

[VYUŽITÍ TPM MODULU]

Velká většina přenosných počítačů, které byly v prodeji poslední 3 roky, obsahuje speciální hardwarový modul umožňující ukládání šifrovacích klíčů a kryptografickou kontrolu stavu počítače. Bitlocker je schopen tento modul využít a tím dále zvyšuje kvalitu zabezpečení.

[FUNKČNÍ SPECIFIKACE]

Šifrovací algoritmy

Bitlocker využívá dvě schémata:

- AES v CBC
- EAS v XTS

AES v CBC módu je prověřený způsob šifrování a velmi kvalitně zajišťuje důvěrnost dat jím zašifrovaných. Přidaná hodnota Elephant difuzéru pak spočívá ve zvýšení bezpečnosti CBC módu proti některým známým útokům vůči integritě zašifrovaných dat.

Způsoby autentizace

Bitlocker umožňuje několik různých způsobů odemykání zašifrovaných disků. V případě použití celodiskového šifrování disku s operačním systémem jsou možné např. následující možnosti:

- Heslo
- TPM
- TPM+PIN(heslo)
- TPM+USB klíč
- TPM+USB klíč +PIN

Další možností (protektorem) je Network Unlock. Síťové odemykání využívá podobného principu jako protektor TPM + Startupkey. Pouze klíč není uložen na USB klíčence, ale je distribuován po síti při zapnutí zařízení chráněného BitLockerem. Kromě uživatelského komfortu (uživatel, je-li připojen do firemní sítě, nemusí např. zadávat PIN při startu zařízení) je hlavním přínosem možnost administrace zašifrovaných zařízení, i když na ně není nikdo přihlášen – například aktualizace, údržba, vzdálená správa a další.

Která z možností má být použita, záleží na specifikách daného projektu, a musí o tom být rozhodnuto již ve fázi analýzy.

[KOMPLEXNÍ ŘEŠENÍ]

Pro kvalitní zabezpečení přenosných počítačů v korporátním prostředí je vhodné zavést jejich komplexní správu. Bitlocker a potažmo celodiskové šifrování z tohoto ohledu není všelék, ale jedná se o nutnou, byť ne postačující podmínku kvalitního zabezpečení.

OBCHODNÍ KONTAKT

ICZ a.s. Na hřebenech II 1718/10
140 00 Praha 4
TEL.: +420 222 271 111
FAX: +420 222 271 112
E-MAIL: marketing@i.cz