Furatul sau pierderea drive-ului USB cu date sau, şi mai rău, a întregului laptop poate avea consecinţe foarte grave. Pierderea datelor importante pentru companie poate cauza probleme în lucru sau în realizarea anumitor proiecte.

Windows 8 poate cripta toate drive-urile USB externe, toate hard disk-urile mobile, chiar şi hard disk-urile calculatoarelor şi a laptopurilor din companie fără a utiliza un hardware suplimentar. Astfel vă puteţi asigura un avantaj faţă de cel care vă fură laptopul. Datele vor fi criptate şi acesta poate folosi doar hardware-ul, dar nu poate ajunge la datele dvs.

Pentru criptarea datelor, Windows 8 foloseşte cipul TPM (Trusted Platform Module). Cipul TPM este un microcip hardware care există pe placa de bază a calculatorului şi care se foloseşte pentru stocarea cheii care se foloseşte pentru criptarea datelor. Dacă pe calculator nu aveţi cipul TPM 1.2, puteţi folosi un USB drive pentru a stoca cheia pe acesta.

BitLocker este instrumentul lui Microsoft care ştie să folosească cipul TPM şi să cripteze date şi volume întregi. Volumele care sunt criptate cu BitLocker pot fi decriptate doar de către persoana care are acces la cheia pentru decriptare, cunoscută ca Full Volume Encryption Key. Windows 8 păstrează FVEK în cadrul metadatelor volumului. Metadatele sunt, de asemenea, criptate cu Volume Master Key (VMK). Şi VMK, şi FVEK folosesc metoda AES pentru criptarea datelor, folosind astfel chei de 256 de biți pentru criptare.

În momentul pornirii sistemului, se verifică dacă toate componentele sunt aici şi dacă totul este în regulă. Abia atunci, dacă nu au fost niciun fel de modificări, cipul TPM îi dă lui Boot Manager VMK-ul decriptat de care are nevoie pentru a decripta FVEK-ul şi pentru a putea citi datele de de disk.

Paşii care sunt parcurși la pornirea calculatorului sunt:

1. Se verifică integritatea sistemului.

2. Se introduce PIN-ul pentru decriptare sau se conectează USB drive-ul pe care se află cheia (opțional)

3. Boot Manager trimite o cerere la cipul TPM pentru a decripta VMK folosind PIN-ul sau cheia care este ataşată.

4. Sistemul de operare se activează.

5. Sistemul de operare preia VMK-ul.

6. Windows foloseşte VMK pentru a decripta FVEK.

7. Windows foloseşte FVEK pentru a decripta datele de pe volumul care este criptat cu BitLocker.

Volumul şi datele de pe el vor rămâne închise doar dacă:

1. Cipul TMP este dezactivat în BIOS.

2. Cipul TMP este deteriorat.

3. Hard disk-ul este mutat pe un alt calculator.

4. Apar modificări în fişierele Windows Boot.

5. PIN-ul nu este introdus corect sau cheia de pe USB drive nu este introdusă.

Dacă drive-ul rămâne închis, va trebui să introduceţi cheia Recovery pentru a deschide drive-ul. În caz contrar, el rămâne închis şi, practic, inutilizabil.

La sistemul de operare Windows 8, administratorii pot activa şi dezactiva BitLocker şi înainte ca sistemul de operare să fie instalat, ceea ce duce la economisirea timp, însă pot și să permită ca hard disk-ul să fie criptat imediat după instalare. Într-un astfel de proces, Windows generează singur cheia temporară pentru criptare, cu care se criptează volumul. După instalare, utilizatorii pot alege pe ce partiţie sau volum doresc să activeze BitLocker şi modalitatea în care datele vor fi blocate şi deblocate.

Metodele de deblocare a drive-urilor sunt:

- Doar cu Trusted Platform Module
- Cu TPM şi PIN în combinaţie
- Cu TPM şi cheia în combinaţie (cheia se păstrează pe USB drive)
- Doar cu cheia

Dacă drive-ul pe care îl blocaţi nu este o partiţie de sistem sau este un drive USB extern, puteţi alege şi:

- Parola
- Cardul smart

- Deblocarea automată

Windows 8 aduce o noutate atunci când vorbim de blocarea unui disk, este vorba doar de blocarea părții ocupate a discului. Astfel se obține o viteză de blocare sau deblocare mai mare. Până acum se bloca fiecare sector de pe disk, deci atât datele, cât şi sectoarele goale.

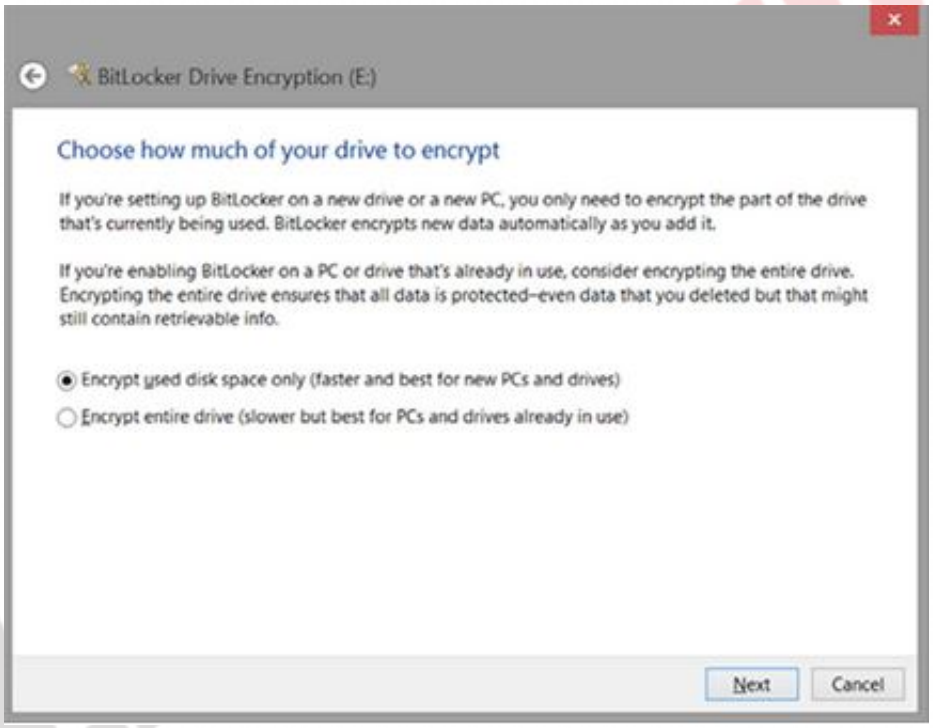

Figura 22.1 Setarea criptării BitLocker

Microsoft vă recomandă să blocaţi doar părţile ocupate ale hard disk-ului, în afară de situaţiile în care pe un hard disk aveţi mai multe partiţii cu date.

O altă funcţionalitate importantă a lui BitLocker stă în faptul că utilizatorii pot, din iniţiativă proprie, să schimbe PIN-ul pentru drive-urile de sistem şi parola pentru drive-urile cu date. Acum adminitratorii au mai puţine probleme cu setarea şi configurarea lui BitLocker pentru utilizatori, deoarece administratorul poate să activeze BitLocker şi să definească niște PIN-uri sau parole de bază, lăsând utilizatorilor posibilitatea ca la activarea lui BitLocker pe propriile

drive-uri să-și definească propriile parole unice. De asemenea, administratorul poate să reseteze parola sau PIN-ul utilizatorului care uită ce a pus.

Modul standard de a debloca drive-urile există de asemenea, ceea ce înseamnă că utilizatorul poate face acest lucru manual în timp ce pornește calculatorul. Windows 8 aduce o nouă funcţionalitate, respectiv o nouă modalitate de a debloca drive-urile, și anume deblocarea prin intermediul reţelei. Acest lucru înseamnă că administratorul poate debloca fiecare volum care este blocat cu BitLocker pe fiecare client sau server care este membru al domeniului.

Network Unlock criptează volumul folosind tot cipul TPM şi cheia care este înregistrată pe el, însă acum în loc să folosească un drive USB extern pentru a prelua cheia, aceasta este trimisă utilizatorului de către din partea serviciul Windows Deployment instalat pe un server din reţea. Transferul chei între client şi server are loc prin DHCP. Serverul care conține rolul Windows Deployment trebuie să aibă instalat suplimentul BitLocker Network Unlock pentru a răspunde la solicitările clientului.

Windows 8 BitLocker susţine noile tipuri de drive-uri hard disk care permit criptarea hardware: EHD – Encripted Hard Drive. Administrarea lui BitLocker şi EHD o puteţi face prin aceeaşi consolă: BitLocker Drive Encription Control Panel. Modurile în care se face criptarea folosind BitLocker şi folosind EHD sunt diferite:

- BitLocker protejează volumele de sistem şi non-sistem prin criptarea datelor la nivelul volumului sau la nivelul aplicaţiei.

- EHD face criptarea disk-ului complet, respectiv criptarea la nivel de hardware.

Configurarea lui BitLocker

BitLocker este disponibil doar în ediţiile Windows 8 Pro şi Windows 8

Enterprise. Acesta permite utilizatorilor să cripteze orice volum.

- Logaţi-vă pe Windows 8 folosind contul care are privilegii de administrator
- Căutaţi Bitlocker în ecranul de start şi porniţi BitLocker Drive Encryption
- Daţi un clic pe iconița Turn On BitLocker imediat lângă iconița C: BitLocker Off

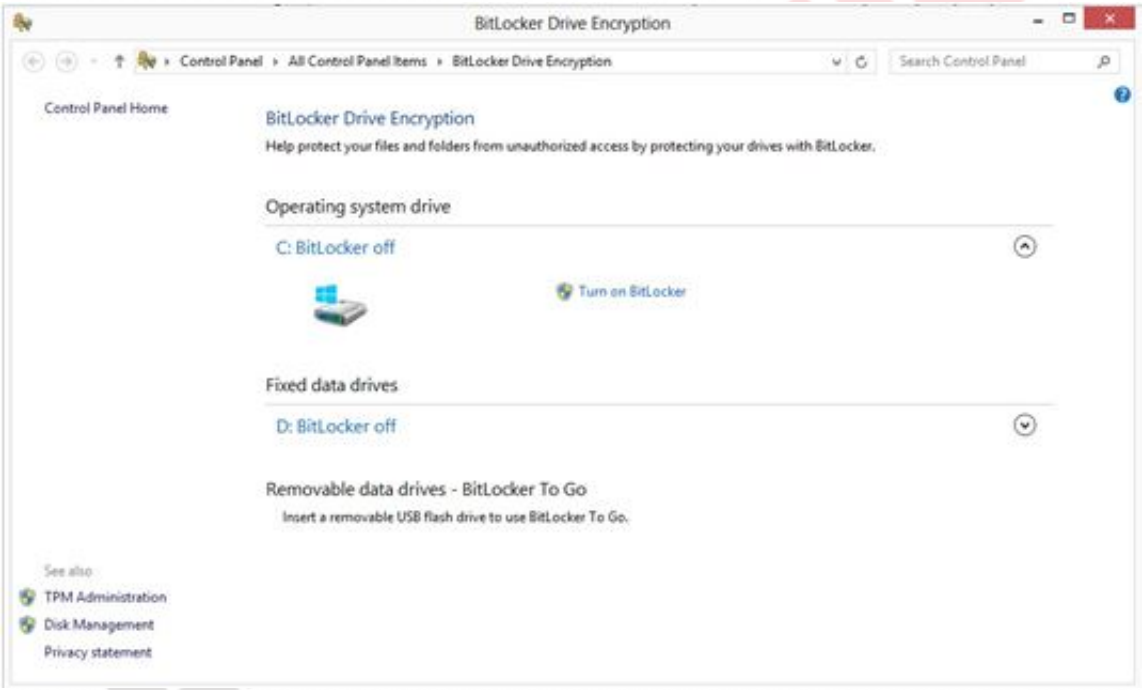

Figura 22.2 Encripția BitLocker Drive

- Dacă calculatorul posedă cipul TPM, va apărea wizard-ul pentru configurare
- Dacă calculatorul nu are cipul TPM, nu veţi putea cripta drive-ul de sistem, dar veţi putea cripta restul. În acest caz, opțiunile disponibile pentru deblocare sunt doar parola și cardul smart
- Alegeţi unde vreţi să puneţi copia cheii Recovery. Vă vor fi oferite patru opţiuni:
  - să o păstrați pe USB drive
  - să o păstrați într-un fişier pe disk-ul local

- să o printați

- Stocaţi cheia apoi alegeţi dacă se va cripta întregul drive sau doar partea care va fi ocupată
- După restartul calculatorului, BitLocker începe criptarea datelor

După ce vă logați din nou pe calculator, criptarea începe. Acest lucru poate dura de la câteva minute până la câteva ore, în funcţie de câte date aveţi pe disk. Un lucru bun este că puteţi folosi calculatorul cât timp durează procesul de criptare.

Dacă nu aveţi cipul TPM, nu veţi putea face criptarea drive-ului în întregime. Însă, Microsoft a adus şi aici ceva nou. Prin setarea opţiunilor în politicile de grup, veţi putea rezolva problema cu lipsa cipului. Pentru a începe cu setarea politicilor de grup, căutaţi gpedit.msc în ecranul de start şi porniţi editorul Group policy. Locaţia pe care se află setările este Computer Configuration \ Administrative Templates \ Windows Components \ BitLocker Drive Encryption \ Operating System Drives. Setaţi „Require Additional Authentication At Startup“.

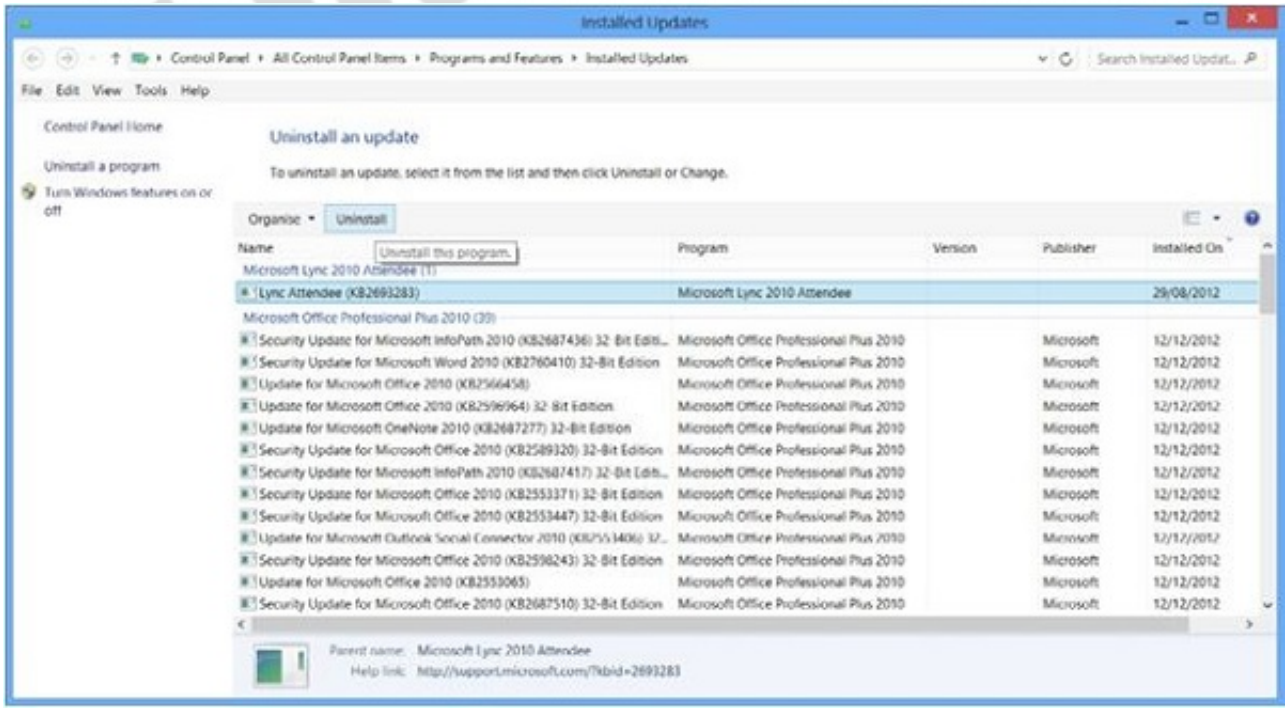

Figura 22.3 Politica de grup BitLocker

BitLocker To Go

BitLocker To Go este destinat blocării şi criptării dispozitivelor externe pentru stoarea datelor. Pentru acesta nu aveţi nevoie de cipul TPM. Datele se criptează folosind parole sau carduri smart. Utilizatorii care folosesc Windows 7 sau Windows 8 pot debloca drive-urile USB criptate numai dacă ştiu parola.

Câteva dintre setările mai importante pe care le aduce BitLocker To Go sunt:

- Este permis accesul la drive-urile externe blocate de pe sistemele de operare mai vechi
- Network Unlock poate fi folosit şi pentru drive-urile externe
- Poate fi ales mecanismul şi cheia pentru criptarea datelor
- Se poate seta lungimea minimă a PIN-ului

WIN8_22 - Windows 8

1. BitLocker-ul pentru blocarea şi criptarea datelor şi a hard disk-urilor complete foloseşte:

- a) cipul TPM
- b) cipul TDI
- c) cipul TGV
- d) cipul TLS

2. Cheia care se foloseşte de către BitLocker cu ocazia blocării şi criptării volumelor complete se numeşte Full Volume Encryption Key. Lungimea sa este de:

- a) 64 de biți
- b) 128 de biți
- c) 256 de biți
- d) 512 de biți

3. Dacă hard disk-ul care este criptat cu BitLocker este mutat pe un alt calculator cu configuraţii hardware identice, datele de pe acel hard disk vor fi:

- a) vizibile, deoarece configuraţia hardware este identică
- b) vizibile, deoarece cheia pentru decriptare se află pe hard disk
- c) blocate, deoarece cheia pentru decriptare se află pe cipul TPM al primului calculator
- d) vizibile, deoarece cheia pentru decriptare se află pe toate cipurile TPM

4. Drive-ul nu se poate bloca doar cu cheia, ci cheia trebuie combinată cu cipul TPM.

- a) adevărat
- b) fals

5. În care ediţii ale sistemului de operare Windows 8 este disponibil instrumentul BitLocker?

- [ ] a) Windows 8
- [ ] b) Windows 8 Pro
- [ ] c) Windows 8 Enterprise

6. Locaţia pe care se află setările pe care le puteţi folosi pentru a seta BitLocker prin politicile de grup este:

- ◯ a) Computer Configuration \ Windows Components \ BitLocker Drive Encryption
- ◯ b) Computer Configuration \ Administrative Templates \ Windows Components \ BitLocker Drive Encryption
- ◯ c) User Configuration \ Administrative Templates \ Windows Components \ BitLocker Drive Encryption
- ◯ d) User Configuration \ Administrative Templates \ Windows Components \ BitLocker Drive Encryption

7. Pentru blocarea drive-urilor USB ce conțin datele importante, veţi folosi instrumentul care se numeşte:

- ◯ a) BitLocker
- ◯ b) BitLocker To Go
- ◯ c) Group Policy Editor
- ◯ d) Full Volume Encryption Key

1. BitLocker-ul pentru blocarea şi criptarea datelor şi a hard disk-urilor complete foloseşte:

a

2. Cheia care se foloseşte de către BitLocker cu ocazia blocării şi criptării volumelor complete se numeşte Full Volume Encryption Key. Lungimea sa este de:

c

3. Dacă hard disk-ul care este criptat cu BitLocker este mutat pe un alt calculator cu configuraţii hardware identice, datele de pe acel hard disk vor fi:

c

4. Drive-ul nu se poate bloca doar cu cheia, ci cheia trebuie combinată cu cipul TPM.

b

5. În care ediţii ale sistemului de operare Windows 8 este disponibil instrumentul BitLocker?

b, c

6. Locaţia pe care se află setările pe care le puteţi folosi pentru a seta BitLocker prin politicile de grup este:

b

7. Pentru blocarea drive-urilor USB ce conțin datele importante, veţi folosi instrumentul care se numeşte:

b