Securitatea este un lucru foarte important. Fiecare îşi doreşte să aibă libertate, dar în acelaşi timp să aibă şi sentimentul de siguranţă că bunurile pe care le deţine nu-i pot fi substrase ilegal. De asemenea, securitatea informaţională este foarte importantă. Nimeni nu vrea să-i fie atacat calculatorul, iar datele să-i fie furate sau şterse.

Windows 8 vine cu noi îmbunătăţiri ale sistemelor de securitate, de care numeroşi utilizatori nu sunt conştienţi. De exemplu, Secure Boot, care ajută la soluţionarea problemelor cauzate de atacurile rootkit. Producerea unui nou sistem de operare care să poată rezista la piaţa actuală de hackeri şi programe maliţioase este o sarcină foarte dificilă, iar ceea ce a făcut Microsoft cu sistemul de operare Windows 8 a fost să creeze un sistem care poate să crească şi să se dezvolte în timp şi să se adapteze la noile modificări care apar.

SecureBoot

Cel mai mare pericol pentru calculatoare şi date îl reprezintă programele maliţioase care se extind pe Internet: viruşi, viermi, cai troieni etc. Aplicaţiile antivirus luptă şi protejează mai mult sau mai puţin sistemele de operare împotriva acestor programe. Rootkit este însă o aplicaţie care se încarcă înaintea sistemului de operare, aflându-se cu un nivel sub acesta, motiv pentru care programele antivirus nu o pot găsi şi înlătura. Windows Vista conţine instrumente care pot să blocheze scrierea în locurile care sunt bune pentru a ascunde rootkit-uri. Windows 7 a venit cu instrumentul BitLoker care verifică fişierele de sistem şi doar acestora le permite să se iniţieze în timpul pornirii sistemului de operare.

Odată cu sistemul de operare Windows 8 vine şi Unified Extensible Firmware Interface (UEFI), noul standard internaţional prezentat ca înlocuitor pentru BIOS. Cu ajutorul său, Microsoft a ridicat nivelul de protecţie împotriva pornirii şi încărcării rootkit-urilor la cel mai înalt nivel posibil. Suplimentul care face posibil acest lucru se numeşte Secure Boot.

UEFI este încă o noutate şi doar câţiva producători de plăci de bază au implementat acest nou standard în produsele lor. Majoritatea foloseşte în continuare BIOS-ul. Pentru a putea folosi opţiunea Secure Boot, trebuie să aveţi UEFI.

De asemenea, Secure Boot solicită ca disk-ul pe care se află sistemul de operare şi sectorul boot să fie setate ca GPT (GUID Partition Table), şi nu ca MBR (Master Boot Record), aşa cum se obişnuia până acum. Cu ocazia instalării sistemului de operare Windows 8 pe calculatoarele cu UEFI, procesul de instalare converteşte disk-ul în GPT şi creează patru partiţii necesare pentru lucrul cu Secure Boot.

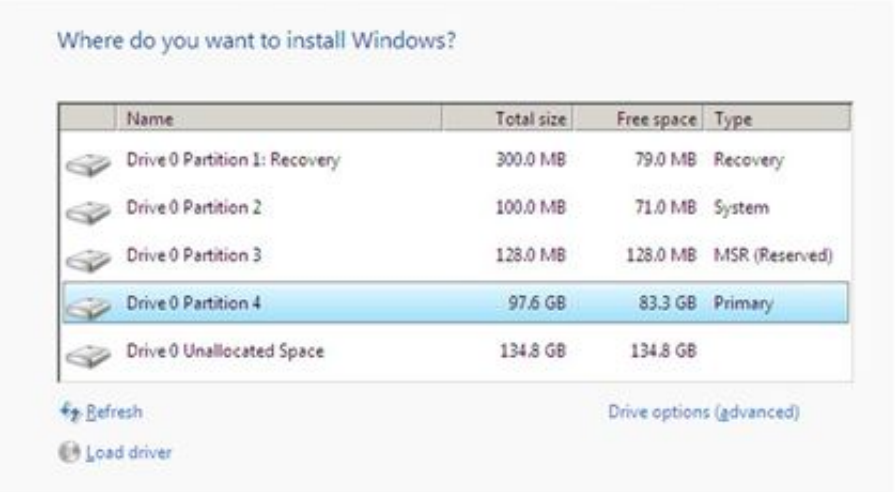

Figura 17.1 Partiţionarea disk-ului

Windows PowerShell 3.0 aduce noi comenzi pentru lucrul cu Secure Boot. După ce instalaţi Windows 8, porniţi consola PowerShell şi tastaţi confirm-SecureBootUEFI pentru a verifica dacă Secure Boot este activ.

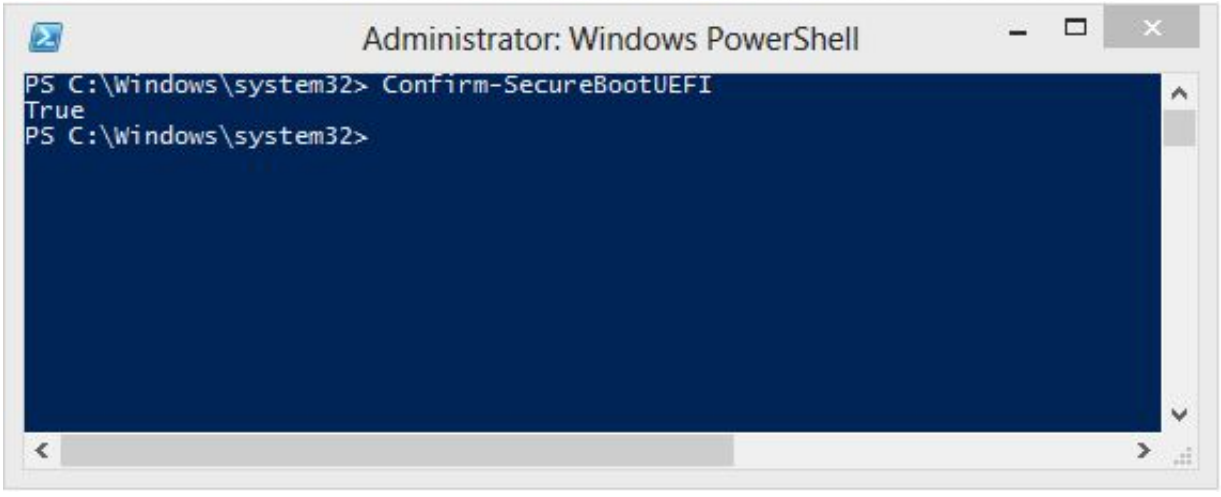

Figura 17.2 PowerShell SecureBoot

Secure Boot vă permite să vă protejaţi împotriva pornirii aplicaţiilor neautorizate, dar vă va face probleme dacă doriţi să aveţi instalatpe calculator Windows 8 şi încă un sistem de operare mai vechi sau unul care nu este Microsoft. În astfel de situaţii, va trebui să dezactivaţi SecureBoot şi să reinstalaţi Windows 8. Dezactivarea lui SecureBoot o puteţi face doar din consola UEFI. Singura situaţie în care nu se poate dezactiva SecureBoot şi în care sunteţi obligaţi să folosiţi sistemul de operare Windows 8 sunt calculatoarele cu platforma ARM. Calculatoarele bazate pe cipurile ARM lucrează cu UEFI şi folosesc SecureBoot, dar utilizatorii nu pot accesa consola UEFI, nu pot face modificări şi nu pot dezactiva SecureBoot.

Smart Screen filter

Filtrul Smart Screen este un supliment al sistemului de operare Windows 8 care monitorizează constant aplicaţiile şi le găseşte pe acelea necunoscute şi neacceptate de către Microsoft. De asemenea, găseşte site-urile web cu probleme şi le opreşte din funcţionare, ajutându-vă să scăpaţi de posibilele probleme. Filtrul afişează mesajul că aplicaţia pe care o iniţiaţi sau site-ul pe care îl vizitaţi poate fi periculos sau maliţios.

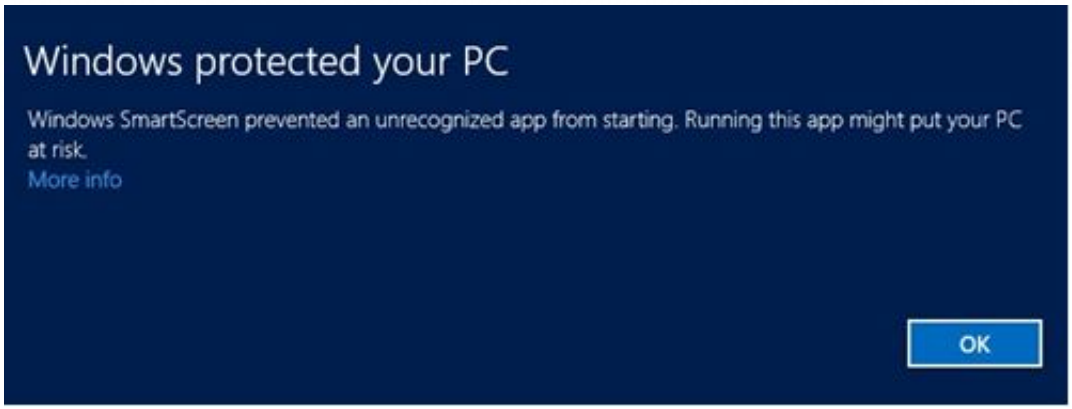

Figura 17.3 Smart Screen

Dacă utilizatorul dă clic pe OK, aplicaţia sau site-ul nu va porni. Dacă se ştie că aplicaţia este legitimă şi utilizatorul vrea să o pornească, deşi Windows 8 nu este de acord, trebuie să daţi clic pe linkul More info, apoi pe opţiunea care permite activarea aplicaţiei.

Deşi aplicaţia este activatăîn mod standard, aceasta se poate bineînţeles dezactiva. Acest lucru nu este însă recomandabil. Dezactivarea o faceţi în secţiunea Change SmartScreen Settings pe care o puteţi accesa căutând-o în ecranul de start. Deschideţi accest instrument şi selectaţi una dintre opţiunile oferite:

- Get Administrator Approval Before Running An Unrecognized Application From The Internet – o opţiune foarte bună atunci când vorbim despre calculatoarele corporative, deoarece este nevoie de acordul dvs. pentru a activa orice aplicaţie potenţial periculoasă.
- Warn Before Running An Unrecognized Application, But Dont Require Administratore Approval – Obţineţi un avertisment, dar totuşi vă este permis să porniţi aplicaţia.
- Dont Do Anything – SmartScreen este dezactivat.

Figura 17.4 Setarea Smart Screen

UAC – User Account Control

Odată cu apariţia sistemului de operare Windows Vista, a fost introdus şi instrumentul pentru controlul accesului - UAC, care permite utilizatorilor să gestionezeîn cel mai simplu mod conturile de utilizator autorizate.

Delogarea de pe calculator şi logarea cu un cont de administrator autorizat numai pentru a instala o anumită aplicaţie sau pentru a modifica vreo setare poate fi o procedură extrem de neconvenabilă. Din acest motiv, pentru calculatoarele lor de acasă, numeroşi utilizatori şi-au adăugat contul de utilizator în grupul de administrarelocal. Acest lucru a rezolvat problema cu instalarea, dar a creat o breşă de securitate. De fiecare dată când vă logaţi pe calculatorul dvs., numele dvs. de utilizator şi parola rămân în memoria calculatorului. Dacă cineva obţine aceste date, poate să le folosească în scopuri maliţioase şi să stabilească o conexiune nelegitimă. Aici intră în acţiune UAC, care vă permite să rămâneţi logaţi ca un utilizator obişnuit, iar de fiecare dată când doriţi să faceţi o sarcină administrativă, să introduceţi numele de utilizator şi parola contului autorizat. În acest caz, acreditările de utilizaotr nu rămân salvate în calculator.

Figura 17.5 User Account Control

Figura 17.6 Introducerea acreditărilor User Account Control

Sistemul de operare Windows 8 a schimbat puţin modul în care aplicaţiile sunt iniţiate. Indiferent dacă sunteţi logat ca un utilizator obişnuit sau ca administrator, aplicaţiile sunt iniţiate fără drepturi de administrare. Microsoft a evaluat că peste 95% dintre aplicaţii nu solicită drepturi de administrator pentru a funcţiona, de aceea se şi pot porni cu cele mai puţine autorizaţii posibile. Abia când apare nevoia ca aplicaţia să introducă sau să modifice ceva legat de stările de sistem,, apare şi nevoia de a utiliza drepturi suplimentare. În aceste situaţii, atât utilizatorii obişnuiţi, cât şi administratorii primesc un avertisment că aplicaţia încearcă să facă ceva ce poate dăuna sistemului şi solicită administratorului să fie de acord cu acest lucru, iar utilizatorilor obişnuiţi le cere să introducă numele de utilizator şi parola de administrator.

Unele instrumente din Command Prompt sunt protejate cu UAC, deoarece se consideră că modificarea lor necontrolată poate cauza probleme în funcţionarea sistemului de operare sau a reţelei.

Figura 17.7 Setarea timpului şi a datei

Microsoft a adăugt în sistemul de operare Windows 8 şi culori pentru avertismente. Acum fundalul are diferite culori în funcţie de motivul pentru care este pornit UAC.

- Fundalul roşu cu iconiţa roşie sub formă de scut – Aplicaţia este blocată prin politica de grup sau din cauza faptului că producătorul este blocat.

- Fundalul albastru cu iconiţa albastră aurie sub formă de scut - Aplicaţia aparţine grupului de aplicaţii administrative ale sistemului de operare Windows 8 sau face parte din Control Panel

- Fundalul albastru cu iconiţa albastră sub formă de scut – Aplicaţia este semnată cu Authenticode şi Windows 8 are încredere în ea.

- Fundalul galben cu iconiţa galbenă sub formă de scut – Aplicaţia nu este semnată sau este, dar Windows 8 încă nu o consideră de încredere.

De fiecare care dată când este pornit UAC, iar desktop-ul se întunecă şi nu aveţi posibilitatea să folosiţi nicio altă aplicaţie până nu închideţi fereastra UAC, selectaţi dacă acceptaţi riscul, introduceţi numele de utilizaotr şi parola sau renunţaţi.

Setarea nivelului până la care UAC va controla calculatorul cu privire la aplicaţiile şi acţiunile dvs. o puteţi face folosind instrumentul User Account Control Settings pe care îl puteţi accesa căutând „UAC“ în ecranul de start.

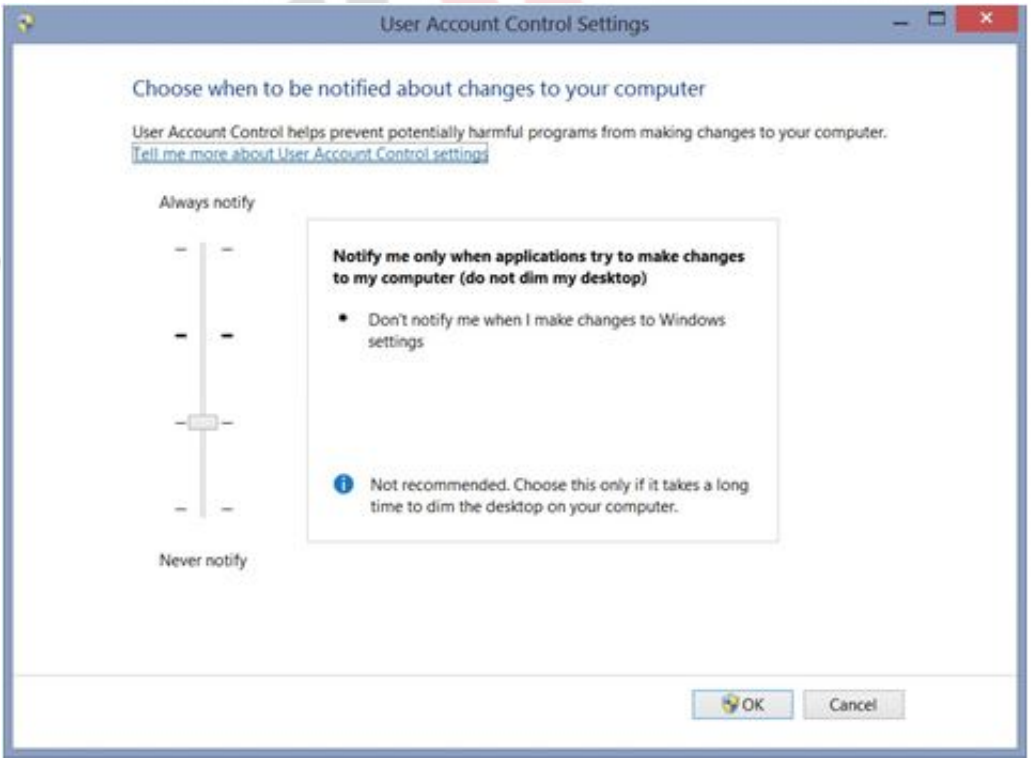

Figura 17.8 Setarea lui UAC

- High – dacă puneţi glisorul pe Always Notify, sistemul îl va atenţiona pe utilizator de fiecare dată este pornită instalarea unei aplicaţii sau o acţiune care va modifica setările sistemului de operare.

- Medium – glisorul se află aici prin default, iar UAC îl va atenționa pe utilizator dacă acțiunea încearcă să instaleze aplicația, dar nu și dacă vor avea loc modificări ale setărilor sistemului de operare Windows.
- Low – atenționeată utilizatorul atunci când acțiunea încearcă să facă modificări pe calculator, dar nu întunecă desktop-ul și îi permite utilizatorului să lucreze chiar și dacă UAC este încă activ.
- Never Notify – nu-l atenționează pe utilizator niciodată, dar lasă serviciul UAC activ.

UAC-ul din cadrul sistemului de operare Windows 8 a fost evaluat ca fiind mult mai stabil şi un isntrument mai puţin iritant. Nu este atât de zgomotos ca înainte, iar setările sale le puteţi face mai detaliat. Astfel, utilizatorii au devenit mai relaxaţi şi sunt tot mai puţini cei care folosesc conturile autorizate pentru logarea pe calculator.

WIN8_17 - Windows 8

1. Noul standard internaţional, prezentat ca înlocuitor pentru BIOS, poartă acronimul:

- a) UEFI
- b) IEFI
- c) UFO
- d) UEFO

2. SecureBoot solicită ca disk-ul pe care se află sistemul de operare şi sectorul boot să fie setat ca:

- a) MBR
- b) NTFS
- c) GPT
- d) FAT

3. Pentru a verifica dacă Secure Boot este activ, utilizaţi comandlet-ul PowerShell:

- a) confirm-SecureBootUEFI
- b) set-SecureBootUEFI
- c) confirm-SecureBoot
- d) set-SecureBoot

4. Aplicaţia care împiedică pornirea aplicaţiilor care nu sunt aprobate de Microsoft şi filtrează traficul de pe Internet blocând site-urile problematice se numeşte:

- a) SmartFilter
- b) SmartScreen
- c) IPFilter
- d) SecureBoot

5. UAC este prescurtarea de la:

- a) Union Account Control
- b) User Access Control

- ◯ c) User Account Continuity
- ◯ d) User Account Control

6. Dacă aplicaţia este blocată prin politica de grup şi din acest motiv nu poate fi pornită, iconiţa UAC va fi:

- ◯ a) roşie cu fundal roşu
- ◯ b) albastru-verzui cu fundal albastru
- ◯ c) albastră cu fundal albastru
- ◯ d) galbenă cu fundal galben

7. Opţiunea SmartScreen a sistemului de operare Windows 8 nu o puteţi dezactiva nicicum.

- ◯ a) adevărat
- ◯ b) fals

1. Noul standard internaţional, prezentat ca înlocuitor pentru BIOS, poartă acronimul:

a

2. SecureBoot solicită ca disk-ul pe care se află sistemul de operare şi sectorul boot să fie setat ca:

c

3. Pentru a verifica dacă Secure Boot este activ, utilizaţi comandlet-ul PowerShell:

a

4. Aplicaţia care împiedică pornirea aplicaţiilor care nu sunt aprobate de Microsoft şi filtrează traficul de pe Internet blocând site-urile problematice se numeşte:

b

5. UAC este prescurtarea de la:

d

6. Dacă aplicaţia este blocată prin politica de grup şi din acest motiv nu poate fi pornită, iconiţa UAC va fi:

a

7. Opţiunea SmartScreen a sistemului de operare Windows 8 nu o puteţi dezactiva nicicum.

b