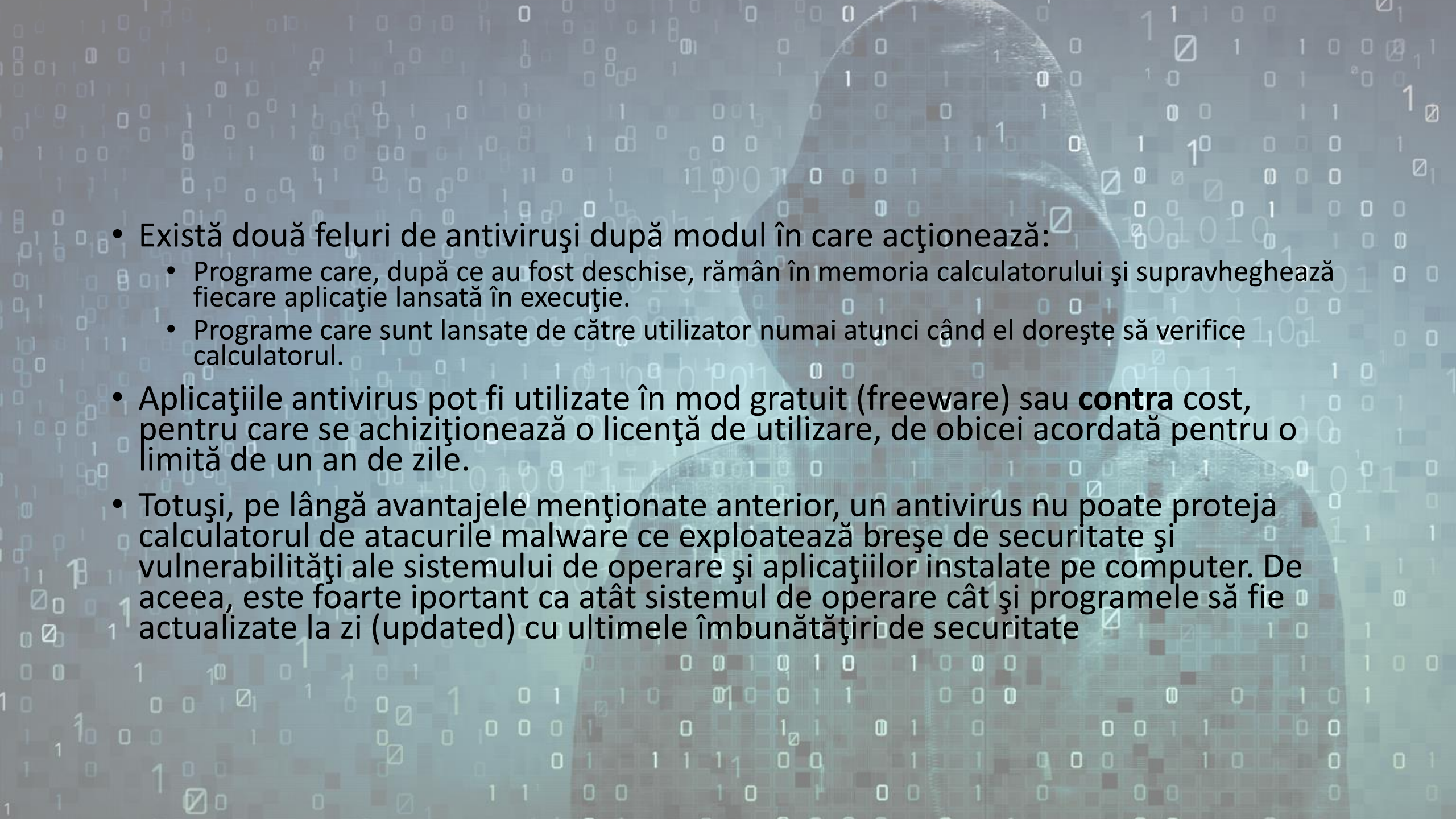
Malware

2.3. Protecție

2.3.1. Înţelegerea modului de funcţionare a unei aplicaţii antivirus şi a limitărilor sale

- programele ce ne pot ajuta să protejăm computerul de viruşi se numesc antiviruşi şi au ca scop principal scanarea calculatorului, identificarea şi blocarea programelor malware.
- Acţiunile care pot fi aplicate la **identificarea** viruşilor pot fi de **blocare** şi **eliminare** a acestora sau de izolare într-o zonă sigură, numită **carantină**, în cazul în care virusul nu poate fi eliminat.
- Identificarea viruşilor se realizează cu ajutorul unei **baze de date** conţinută de aplicaţia antivirus, în care sunt înglobate diferitele tipuri de viruşi (semnături malware).
- trebuie să înţelegem este faptul că, deşi antivirusul poate fi o unealtă eficientă, acesta este limitat la semnăturile despre viruşii existenţi.

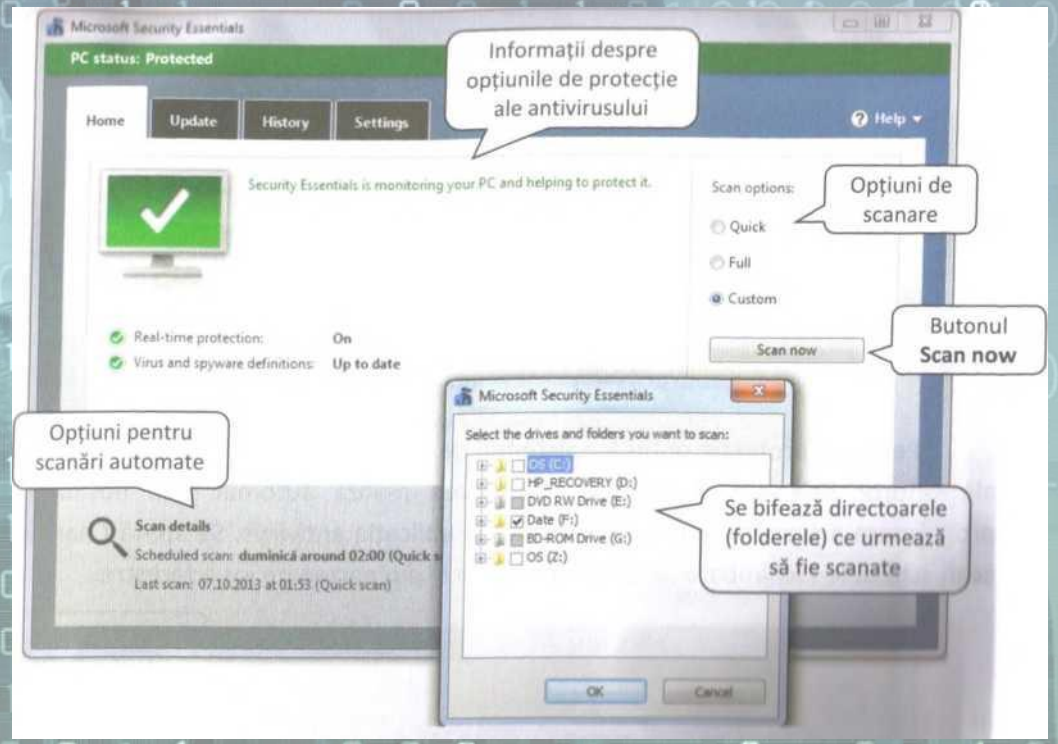


- Există două feluri de antiviruşi după modul în care acţionează:
  - Programe care, după ce au fost deschise, rămân în memoria calculatorului şi supravhegheză fiecare aplicaţie lansată în execuţie.
  - Programe care sunt lansate de către utilizator numai atunci când el doreşte să verifice calculatorul.
- Aplicaţiile antivirus pot fi utilizate în mod gratuit (freeware) sau **contra** cost, pentru care se achiziţionează o licenţă de utilizare, de obicei acordată pentru o limită de un an de zile.
- Totuşi, pe lângă avantajele menţionate anterior, un antivirus nu poate proteja calculatorul de atacurile malware ce exploatează breşe de securitate şi vulnerabilităţi ale sistemului de operare şi aplicaţiilor instalate pe computer. De aceea, este foarte iportant ca atât sistemul de operare cât şi programele să fie actualizate la zi (updated) cu ultimele îmbunătăţiri de securitate

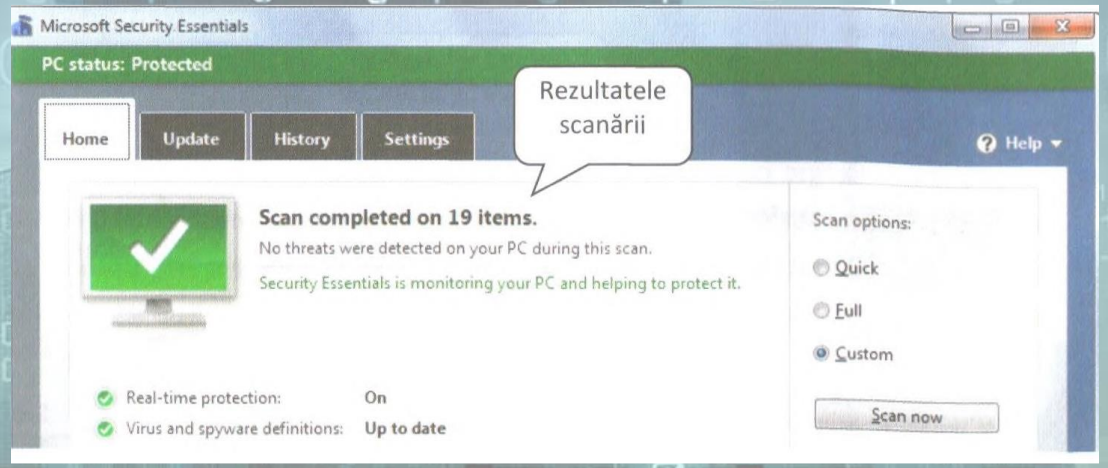
2.3.2. Scanarea partiţiilor, directoarelor, fişierelor cu o aplicaţie antivirus. Programarea scanărilor cu ajutorul unei aplicaţii antivirus

- Modul de lucru cu un antivirus este asemănător pentru toate aplicaţiile antivirus. Vom exemplifica în cele ce urmează lucrul cu programul Microsoft Security Essentials, un program antivirus dezvoltat de compania Microsoft, ce poate fi utilizat în mod gratuit.
- Există două variante pentru a lansa comanda de scanare a unui director, fişier au aplicaţie:
  - Prima variantă constă în deschiderea aplicaţiei prin dublu click pe iconiţa afişată în zona de sistem sau prin click stânga pe scurtătura **Microsoft Security Essentials** meniul de **Start**.
  - În fereastra aplicaţiei se selectează opţiunea **Custom** (Personalizat) şi se apasă butonul **Scan Now**. Apare fereastra cu structura de directoare unde se bifează directoarele de se doresc a fi scanate.

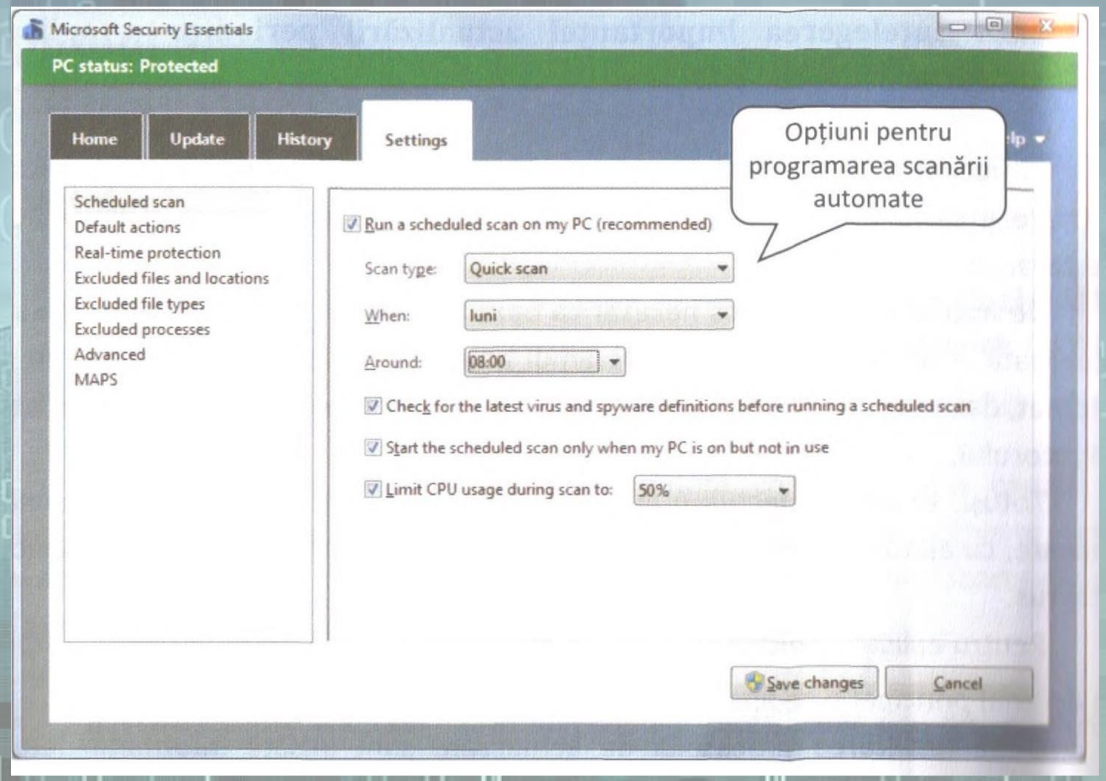
- A doua variantă utilizează comanda de scanare existentă în meniul contextual. Astfel, se execută click dreapta pe obiectul dorit (director, fişier sau aplicaiţie) şi se selectează opţiunea **Scan with Microsoft Security Essentials.**
- După finalizarea scanării, apare fereastra unde sunt prezentate rezultatele procesului de scanare.



- Pentru o protecţie optimă a sistemul de calcul se recomandă scanări periodice ale tuturor fişierelor. Acest lucru se poate realiza automat prin opţiunea de programare a scanării, pusă la dispoziţie de aplicaţia antivirus.
- Se apasă **Change my scan schedule** (Schimbare program de scanare) din partea de jos a ferestrei.



- În fereastra **Settings** (Setări) se stabilesc opţiuni pentru tipul de scanare, ziua şi ora și se apasă butonul **Save changes** (Salvare modificări).



2.3.3. Înțelegerea termenului de carantină și efectul de introducere în carantină a fișierelor infectate / suspecte

- Termenul de **carantină** se referă la o zonă securizată, gestionată de antivirus unde sunt izolate fișierele infectate sau suspecte. Aceasta elimină riscul de infectare a sistemului de calcul și permite trimiterea acestor fișiere spre analiză, către compania producătoare a antivirusului.
- Fișierele aflate în carantină, sunt scanate automat la fiecare actualizare a bazei de date cu semnături malware iar dacă sunt curățate, sunt mutate automat la locul lor inițial.
- Utilizatorul are la dispoziție opțiuni de ștergere, restaurare sau trimitere a fișierelor spre analiză. Se poate specifica de asemenea, intervalul de timp după care fișierele din carantină pot fi șterse automat, dacă devirusarea acestora nu se poate realiza.

2.3.4. Înţelegerea importanţei actualizării periodice a aplicaţiei antivirus

- În fiecare zi apar noi ameninţări malware care constituie un pericol ridicat de infectare a calculatorului, dacă programul antivirus nu e la curent cu semnăturile acestora.
- De aceea, este imperios necesar ca baza de date cu semnături malware să fie actualizată zi de zi. Din fericire, programul antivirus realizează actualizarea în mod automat, dacă există o conexiune la Internet, fără să mai necesite o acţiune din partea utilizatorului.
- Totuşi, se poate efectua o actualizare manuală a bazei de date cu semnături malware, cu ajutorul opţiunii **Update** (Actualizează) disponibilă în interfaţa aplicaţiei antivirus.
- Pentru aplicaţia **Microsoft Security Essentials** se selectează tab-ul (fila) **Update** meniul principal şi se apasă butonul **Update.**
- După finalizarea procesului de actualizare sunt afişate informaţii detaliate înspre data verificării şi baza de semnături malware.