COLEGIUL TEHNIC „VICTOR UNGUREANU”
CÂMPIA TURZII

PROIECT

PENTRU OBŢINEREA CERTIFICATULUI DE CALIFICARE
PROFESIONALĂ NIVEL 4

TEHNICIAN OPERATOR TEHNICĂ DE CALCUL

ABSOLVENT:
PĂCURARIU E.A. REBECA-ANA-MARIA

COORDONATOR:
prof. ARION LOREDANA

2019 – 2020

Protejarea sistemelor de calcul împotriva virușilor informatici

CONŢINUT

ARGUMENT

Henry Kissinger a spus odată:
"Chiar şi un paranoic
are câţiva duşmani reali".

Oricine utilizează un calculator are ceva de care se teme: pornind de la bandele josnice de hackeri, crackeri şi fabricanţi de viruşi până la companiile care doresc să ne urmărească obiceiurile de navigare pe Internet. Cu toate acestea, nu trebuie să fim paranoici: avem nevoie doar de câteva instrumente optime pentru protejarea sistemului de calcul.

Nu este suficientă instalarea unui sistem de operare, dacă în timp, nu sunt eliminate vulnerabilităţile care apar. Aceasta se face prin instalarea de patch-uri (programe sau secvenţe de program care „acoperă" ameninţarea). De obicei, patch-urile sunt puse la dispoziţia utilizatorilor de cei care vând sistemul de operare. Actualizarea cu regularitate va duce la un sistem mai sigur şi mai stabil.

O importanţă deosebită trebuie acordată si aplicaţiilor pe care le descarcă şi le instalează utilizatorii. Aceste aplicaţii, dacă nu au fost testate îndeajuns, pot crea spaţii prin care intruşii vor putea să pătrundă în sistem. De aceea, nu trebuie instalat un program sau o aplicaţie, fără acordul administratorului de sistem.

Politica de securitate trebuie să dezbată si problema monitorizării sistemului. Orice sistem de operare de generaţie nouă are inclus un program de monitorizare, unde sunt evidenţiate toate erorile de sistem sau de încărcare a aplicaţiilor.

I. INTRODUCERE

- Ce este un virus şi ce este un program antivirus -

I.1. VIRUŞII

Viruşii reprezintă programe adăugate în aplicaţii care se multiplică singure în alte programe din spaţiul rezident de memorie sau de pe discuri. Apoi fie saturează complet spaţiul de memorie/disc şi blochează sistemul de operare, fie, după un număr fixat de multiplicări, se autoactivează şi intră într-o fază distructivă (care de regulă este exponenţială);

Bomba software este o procedură sau parte de cod inclusă într-o aplicaţie "normală" care este activată de un eveniment predefinit (de exemplu ziua de 13). Autorul bombei anunţă producerea evenimentului, lăsând bomba să explodeze adică să producă acţiunile distructive programate;

Viermii au efecte similare cu cele ale bombelor şi viruşilor. Principala diferenţă faţă de aceştia este aceea că nu au o localizare fixă (pe disc sau în memorie) sau nu se multiplică singuri. Viermii se mută în permanenţă, ceea ce îi face dificil de detectat. Cel mai renumit exemplu este *viermele internetului*, care a scos din funcţiune o mare parte din utilizatorii Internet în noiembrie 1988;

Trapele reprezintă accese speciale, frauduloase, la sistem. În mod normal accesele la sistem sunt rezervate pentru proceduri de încărcare de la distanţă, de întreţinere sau pentru dezvoltatorii unor aplicaţii. Trapele permit atacatorilor accesul neautorizat la sistem, prin eludarea procedurilor uzuale de identificare.

Calul Troian este o aplicaţie modificată astfel încât, pe lângă funcţia normală să mai execute, pe ascuns, o altă funcţie. Calul Troian nu creează copii, ceea ce îl face mai greu de depistat. De exemplu, un hacker poate înlocui codul unui program normal de control "login" cu un alt cod care face acelaşi lucru, dar, adiţional, copiază într-un fişier numele şi parola pe care utilizatorul le tastează în procesul de autentificare. Ulterior, folosindu-se de datele stocate în acest fişier, hackerul va avea acces facil la sistem.

I.2. PROGRAMELE ANTIVIRUS

Programele antivirus contribuie la protejarea computerelor împotriva viruşilor, viermilor, cailor troieni precum şi a altor "invadatori" care pot ataca un computer. Însă, în acest caz, e mai grav decât o simplă răceală. Viruşii, viermii şi ceilalţi asemenea lor se dedau deseori la acţiuni răuvoitoare, cum ar fi ştergerea de fişiere, accesarea de date personale sau utilizarea computerului pentru a ataca alte computere.

De ce trebuie să utilizăm un program antivirus?

Se poate preveni "îmbolnăvirea" unui computer prin "injectarea" unui program antivirus. Să reţinem doar că, asemenea dozelor de vaccin, deseori nu este suficientă o singură administrare. Este necesară administrarea regulată a unor doze auxiliare. În situaţia de faţă, acest lucru înseamnă pur şi simplu actualizarea regulată a programului antivirus. Aceste actualizări se oferă în general pe baza unui abonament la distribuitorul de produse antivirus.

Antivirusul - sistemul imunitar al computerului

Un nivel superior de securizare îl reprezintă softurile de securizare ale sistemelor de operare, ***antiviruşii***. Astfel utilizarea unui antivirus (client, în cazul unui computer personal sau server/client în cazul unei reţele) ne protejează de posibilii viruşi care pot pătrunde în reţeaua noastră şi ne pot crea atâtea "neplăceri".

În ultimul timp **viruşii** dau tot mai multă bătaie de cap utilizatorilor şi administratorilor de reţea. Pentru a înlătura riscul de a fi "infectaţi" trebuie să se instaleze pe computer un client de antivirus. Este absolut obligatoriu ca sistemul sau reţeaua să fie apărate de un program antivirus.

Dar după instalarea lui nu înseamnă că am scăpat de grijă în privinţa viruşilor ce se răspândesc cu atâta rapiditate prin Internet.

Asiguraţi-vă că aveţi clientul de antivirus actualizat la zi, verificând pe site-ul producătorului respectivului antivirus. În cazul conexiunii permanente la Internet puteţi seta actualizarea automată a antivirusului, scăpând astfel de grijă de a-l actualiza manual. Majoritatea clienţilor de antivirus se pot configura periodic (la interval de o zi sau la câteva ore), să verifice pe site-ul de origine dacă există actualizări pentru el. Lăsaţi antivirusul să monitorizeze on-line traficul de date şi de mail-uri (primite sau expediate), astfel veţi fi notificaţi în cazul în care un virus încearcă să pătrundă în computerul dumneavoastră, fie pe cale directă, fie prin intermediul mail-urilor virusate. În cazul în

care veţi primi un mail virusat, antivirusul îl va devirusa sau pur şi simplu va şterge attachamentul mail-ului respectiv şi vă va informa asupra faptului că acel mail a fost virusat şi vi s-a blocat accesul la attachmentul respectiv. Cu toate acestea trebuie să fiţi foarte atenţi la ataşamentele din mail-urile primite, deoarece uneori virusul poate fi foarte nou, iar antivirusul să nu îl detecteze. În cazul în care un mesaj vi se pare dubios, iar fişierul ataşat are o extensie pe care nu aţi mai întâlnit-o, nu deschideţi respectivul fişier.

Cum ne apărăm împotriva viruşilor

Pornind de la conceptul bine experimentat că este mai puţin costisitor să previi decât să tratezi, este necesar să se acorde o atentie deosebită problemei viruşilor. Într-o formă simplistă, lupta împotriva viruşilor s-ar putea rezuma la o singură frază: trebuie îmbunătăţite programele si curăţate dischetele înaintea introducerii lor în unitatea centrală.

Există astăzi mai multe organizaţii internaţionale care se ocupă cu problemele viruşilor pe calculator. Una dintre acestea se numeşte CARO - Computer Anti-virus Researcher Organisation, şi este o organizatie constituită din cei mai reputaţi experţi din lume care se ocupă cu standardizarea şi clasificarea viruşilor.

Încă din anul 1990 a fost înfiinţată o instituţie specializată în acest domeniu, numită EICAR - Institutul European pentru Cercetarea Programelor Anti-Virus. Această organizaţie s-a bucurat de un real succes, mai ales în întâlnirile cu vânzătorii de programe.

În decembrie 1990, firma Symantec a lansat produsul Norton Anti-Virus Software, astăzi foarte la modă. Tot în acelasi an, dar în luna aprilie, firma Central Point Anti-Virus a lansat produsul CPAV.

Există mai multe publicaţii internaţionale pe această temă, iar Internet-ul abundă de materiale şi informaţii. Cea mai importantă revistă internaţională dedicată raportării şi analizei viruşilor se numeşte Virus Bulletin. De la lansarea sa în iulie 1989, revista a monitorizat noile dezvoltări din domeniul programării viruşilor şi a evaluat cele mai actualizate instrumente si tehnici pentru combaterea ameninţării reprezentate de viruşi.

În lupta împotriva viruşilor este necesar să se cunoască cele mai importante şi eficiente mijloace, metode si tehnici care pot fi utilizate în acest scop. Pentru aceasta, este nevoie să ne familiarizăm cu câteva noţiuni şi concepte specifice.

Suma de control (Checksum) este o valoare numerică obţinută din biţi individuali ai unui fişier. Împreună cu data creării, mărimea si atributele DOS ale fişierului, suma de control este memorată în fişiere de tip listă de control. De obicei, are lungimea de 32 sau 64 biţi.

Un alt termen des utilizat este *CRC*. Acronimul lui "Cycled Redundancy Check", în traducere - "Control Redundant Ciclic", el reprezintă o metodă matematică folosită pentru verificarea integrităţii datelor. Este o formă de sumă de control, care se bazează pe teoria polinoamelor de lungime maximă. Desi este mai sigură decât cea bazată pe o simplă sumă de control, metoda CRC nu oferă totuşi o adevărată securitate criptografică.

O secvenţă de biţi sau, mai general, o combinaţie de secvenţe variabile, prin care programele antivirus încearcă să identifice viruşii se numeşte *semnătura* unui virus (virus signature).

Operaţia prin care se elimină un virus dintr-un fişier sau dintr-un sistem se numeşte *dezinfecţie* (clean). Desigur, contaminarea unui calculator cu un virus informatic se numeşte *infecţie* (infection).

Tehnica prin care se adaugă unui program executabil o porţiune de cod, pentru a se asigura autoverificarea sa, în aşa fel încât suma sa de control să fie verificată înainte ca programul propriu-zis să se execute, se numeşte *imunizare* (immunization). Orice modificare făcută programului poate fi deci verificată si execuţia refuzată. Această tehnică poate provoca multe probleme deoarece ea intră în conflict adesea cu programul pe care încearcă să-l protejeze.

Atunci când se generează o *amprentă* (o informaţie de control) pentru un fişier spunem că s-a efectuat o *inoculare* (inoculate). Este suficient apoi să se compare această amprentă cu alta calculată ulterior pentru a detecta alterarea eventuală a fişierului de către un virus.

Un program antivirus care caută fişiere infectate, analizând secvenţe identificabile ca aparţinând unor viruşi cunoscuţi (aşa numitele "semnături" de virus) se numeşte *program de scanare* (scanner). Programele de scanare au diverse limitări, printre care, cea mai importantă este faptul că ele nu pot căuta decât viruşi deja identificaţi sau cunoscuţi.

Un *software antivirus* (anti-virus software) reprezintă un produs program utilizat pentru a identifica şi deseori pentru a furniza mijloacele necesare eliminării viruşilor de pe sistemele infectate. Acest proces este denumit frecvent "curăţare" sau "dezinfectare".

Un *software de dezinfecţie* (desinfection software) nu este altceva decât un program care încearcă să îndepărteze viruşii de pe discurile infectate, astfel încât să restaureze elementele infectate la starea lor anterioară. Dat fiind faptul că adesea viruşii sunt polimorfi (schimbaţi de o manieră subtilă), software-ul de dezinfectare poate să facă greşeli cu consecinţe potenţial catastrofale pentru integritatea datelor. Detecţia viruşilor sectorului de încărcare este cu mult mai fezabilă decât cea a

fişierelor executabile, iar utilizarea programelor de sistem (DEL, SYS, FDISK şi FORMAT) reprezintă adesea o soluţie preferabilă.

Vaccinul este un program pe calculator realizat pentru a oferi o protecţie împotriva viruşilor de calculator. Adăugând un cod scurt la fişiere, se declanşează o alarmă atunci când un virus încearcă să modifice fişierul. Vaccinurile mai sunt numite şi programe de imunizare.

Autorii răuvoitori de viruşi ai calculatoarelor ştiu de existenţa programelor de vaccinare şi antivirus şi unii dintre ei se ocupă cu crearea de noi viruşi care să le contraatace. Dacă folosiţi calculatorul pentru afaceri sau aplicaţii profesionale vitale, protejaţi datele introducând în calculator numai copii noi, care nu au fost deschise, de programe obţinute direct de la producători.

Din activitatea programelor anti-virus pot rezulta şi alarme false. O monitorizare a procesului de dezinfectare este deseori foarte utilă.

O metodă de detectare a fişierelor virusate constă în compararea periodică a fişierului cu cel original, din dată, oră şi dimensiune. Aceste teste nu prezintă totală încredere deoarece atât data si ora, cât si dimensiunea fişierelor pot fi manipulate convenabil, fără a ne putea da seama dacă s-a umblat în fişierul original şi dacă acesta a fost alterat.

Există şi alte elemente care pot fi verificate, cum ar fi sumele de control (check sum), mai de încredere, dar nu totală, prin care datele dintr-un fişier sunt însumate şi trecute printr-un algoritm specific, rezultând un fel de semnătură pentru acel fişier. Sumele de control funcţionează pentru verificarea integrităţii unui fişier în cazul transferului dintr-un punct în altul. Pentru protecţie, lista sumelor de control este necesar a fi păstrată pe un server separat, chiar pe un mediu separat accesibil doar de administrator si de utilizatorii de încredere. Totuşi această tehnică este insuficientă când sunt atacuri sofisticate împotriva integrităţii fişierelor, existând pericolul ca la destinaţie să ajungă un fişier necorespunzător.

Pe Internet se găsesc însă suficiente materiale referitoare la modul în care pot fi învinse sistemele care folosesc sume de control, multe dintre ele chiar prin acţiunea viruşilor. Multe dintre utilitarele antivirus folosesc o analiză a cifrei de control pentru a identifica activităţi de virusare.

Există tehnici satisfăcătoare bazate pe calcularea unei amprente digitale (digital fingerprint) sau semnătură pentru fişiere. Algoritmii care realizează acest lucru fac parte din familia MD, cea mai cunoscută implementare fiind MD5. Aceasta este o funcţie neinversabilă (one-way) care generează semnătura digitală pentru un fişier prin intermediul unui algoritm de condensare a mesajului (message digest). Algoritmul preia la intrare un mesaj de o lungime arbitrară şi produce un rezultat pe 128 biţi denumit amprentă (fingerprint) sau rezumat (message digest). Algoritmul se bazează pe

un concept conform căruia este imposibil prin prelucrare să se producă două mesaje cu acelaşi rezumat sau să se reconstituie un mesaj pornind de la un anumit rezumat. Algoritmul MD5 este proiectat pentru aplicaţii bazate pe semnături digitale, în care un fişier de dimensiuni mari trebuie comprimat într-un mod sigur înainte de a fi criptat cu o cheie privată (secretă).

Un produs care utilizează algoritmul MD5 este S/Key dezvoltat de Bell Laboratories pentru implementarea unei scheme de parole unic valabile (one-time), care sunt aproape imposibil de spart, deşi parolele sunt transmise în clar, dar datorită faptului că parola fiind de unică valabilitate, nu mai este de nici un folos pentru un eventual intrus.

O tehnică foarte interesantă aplicată în combaterea viruşilor se bazează pe utilizarea programelor automodificabile (self-modifying program). Acestea sunt programe care îşi schimbă deliberat propriul lor cod, cu scopul de a se proteja împotriva viruşilor sau copierilor ilegale. În acest mod devine foarte dificilă validarea prin mijloace convenţionale.

II. UTILIZAREA PROGRAMELOR ANTIVIRUS

Programele antivirus sunt programe create special pentru a efectua următoarele operaţiuni:

- să detecteze viruşii prin verificarea conţinutului fişierelor si semnalarea prezenţei semnăturii unui virus cunoscut sau a unor secvenţe suspecte in interiorul lor

- să dezinfecteze sau să şteargă fişierele infestate de viruşi cunoscuţi

- să prevină infectarea prin supravegherea acţiunilor din memorie si semnalarea întâlnirii unor anumite acţiuni că ar putea fi generate de existenţa in memorie a unui virus.

Exista doua feluri de antiviruşi după modul in care acţionează:

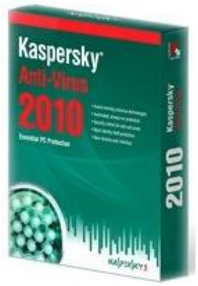
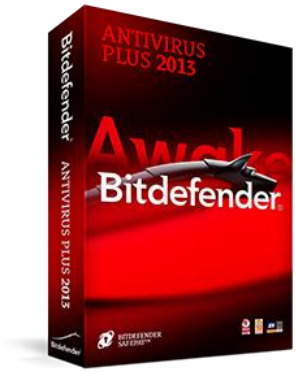
1. Programe care după ce au fost lansate ce rămân în memoria calculatorului şi supraveghează fiecare aplicaţie lansată în execuţie.
2. Programe care sunt lansate de către utilizator numai atunci când el doreşte să verifice calculatorul

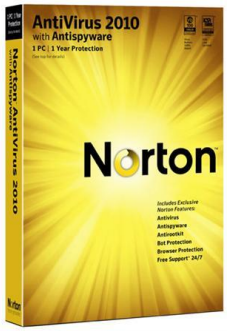
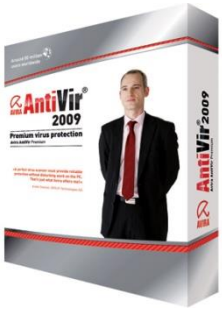
In următoarele condiţii are loc devirusarea:

- → **Scanarea** = citirea fişierelor şi a memoriei şi identificarea viruşilor cunoscuţi de programul antivirus respectiv
- → **Devirusare** = extragerea virusului sau ştergerea fişierului infectat

→ **Monitorizare** = este operaţia prin care un antivirus existent in memorie verifică si semnalează sistematic eventuala apariţie a unui virus

II.1. Exemple de programe antivirus

	**Kaspersky Anti-Virus** vă protejează calculatorul de viruşi troieni, spyware, rootkits fiind o protecţie reală împotriva tuturor tipurilor de malware. Asigură protecţie pentru programele de mesagerie instantanee (ICQ, MSN). Metodele reactive de detecţie sunt combinate cu tehnologii proactive pentru a asigura securitate efectivă, în timp ce update-ul automat ne asigură protecţie neîntreruptă şi fără a interveni în activitatea noastră.
	**Bitdefender Antivirus Plus 2013** foloseşte tehnologia de securitate nr. 1 pentru oprirea ameninţărilor informatice, securizarea tranzacţiilor online şi protecţia datelor confidenţiale în reţelele de socializare. • Cea mai bună apărare împotriva viruşilor şi a programelor spion • Protejarea datelor confidenţiale pe Facebook şi Twitter • Detectează site-urile riscante • Protejează împotriva furtului de identitate • Certificat Windows 8
	**ESET Smart Security** este primul reprezentant al noii abordări de securitate cu adevărat integrată a computerului. Produsul foloseşte viteza şi precizia ESET NOD32 Antivirus, care este garantat de cea mai recentă versiune a motorului de scanare ThreatSense, combinat cu modulele personalizate de protecţie firewall şi antispam. Rezultatul este un sistem inteligent, mereu în alertă pentru atacuri şi software dăunător, care vă pun computerul în pericol. ESET Smart Security Business Edition poate fi instalat atat pe servere cât şi pe staţiile de lucru din cadrul unei reţele (varianta Home Edition poate fi instalată numai pe staţii de lucru). Cu ESET Smart Security Business Edition controlaţi şi administaraţi de oriunde, indiferent de distanţa, sistemul de

	securitate ales folosind ESET Remote Administrator. Acesta reprezintă o necesitate atât pentru afacerile care au mai multe puncte de lucru cât şi pentru administratorul de sistem care are o munca flexibila (călătoreşte sau lucrează de la distanţă). Licenţa este de tip electronic.
	**NORTON ANTIVIRUS 2010.** Protecţie extraordinară împotriva viruşilor, programelor spyware şi altor programe software rău intenţionate.
	**Avira AntiVir Premium** este un program antivirus fiabil care vă protejează împotriva tuturor ameninţărilor:viruşi, viermi, troieni, rootkits, phishing, adware, spyware, roboţii şi periculoase "drive-by" download-uri. Licenţa este de tip electronic. Modalitatea de licenţiere este online.
	**Panda Global Protection 2010** Această soluţie este cea mai completă soluţie de securitate de la Panda Security. Este tot ce are nevoie un utilizator, asigurând protecţie împotriva viruşilor, spyware, rootkits, hackerilor, fraude online, furtul de identitate.
	**Avira AntiVir Mobile** este o protecţie profesională împotriva viruşilor şi malware-ului care ataca un terminal mobil,Pocket PC sau SmartPhone.

<table>
<tr>
<td>  </td>
<td>F-Secure Mobile Security asigură securitatea smartphone-ului nostru atunci când dăm telefoane, trimitem mesaje multimedia, navigăm pe Internet, verificăm e-mailul sau ne plătim facturile. Pachetul de securitate completă include protecţie antivirus, antispyware, firewall şi un modul de control anti-furt care protejează informaţiile chiar dacă smartphone-ul este pierdut sau furat. F-Secure este pioner în securitatea mobilă, ceea ce face ca această aplicaţie să fie uşor de instalat şi uşor de folosit fără a afecta perfomanţă smartphone-ului.</td>
</tr>
<tr>
<td>  </td>
<td>Microsoft Security Essentials

Security Essentials, soluţia de securitate furnizată gratuit de către Microsoft, a ajuns la versiunea 4.0.
Microsoft Security Essentials 4.0 rulează pe sistemele de operare Windows XP / Vista / 7. Printre noutăţile pe care le aduce menţionăm interfaţa grafică îmbunătăţită şi motorul de scanare în timp real cu o rată de detecţie mai bună.
Merită spus că suita de securitate Microsoft include şi un modul de carantină îmbunătăţit (ce vizează viruşii, troienii şi viermii cu grad ridicat de periculozitate. Pe toţi aceştia îi va muta automat în carantină, fără a solicita intervenţia utilizatorilor.
Odată instalat, Microsoft Security Essentials păstrează un modul rezident în memoria RAM a calculatorului, capabil să asigure protecţie permanentă împotriva aplicaţiilor periculoase. Baza de date cu semnături antivirus este actualizată în mod automat.
Ca şi în cazul versiunilor precedente, Microsoft Security Essentials 4.0 poate fi instalat (fără "artificii tehnice") doar pe calculatoare cu Windows original.</td>
</tr>
<tr>
<td></td>
<td>AVG Antivirus a evoluat mult de la utilitarele cu funcţii simple din primii ani. Pentru a proteja calculatorul de viruşi în ziua de astăzi este nevoie de mult mai mult decât de un simplu program software. AVG însa, dovedeşte zi de zi că reprezintă un serviciu cuprinzător.
Premii câştigate:
VB100% în testul Virus Bulletîn din Noiembrie 2003 pe platforma Windows 2003 Server.
rata de detectie de 100% a lui AVG Anti-Virus System este continuu certificată de către laboratoarele ICSA.</td>
</tr>
</table>

III. PROTECŢIA IMPOTRIVA SPYWARE

Calculatoarele conectate la internet sunt bombardate în mod constant, cu viruşi de tip troian, spyware, malware etc. Astfel ca utilizatorii acestor calculatoare, instalează softuri de protecţie contra lor. Conturile de e-mail sunt bombardate constant de mesaje nefolositoare de publicitate (spamm) astfel ca, utilizatorii instalează programe de protecţie anti-spam. Când consideri că ai lucrurile sub control, de fapt te trezeşti că ai sistemul de calcul invadat de sute de viruşi tip spyware şi adware, care rulează silenţios, monitorizând şi raportând activitatea calculatorului tău. Spyware şi Adware monitorizează şi urmăresc navigarea voastră pe internet, astfel încât, companiile care cercetează navigarea pe internet şi comportamentul utilizatorilor să-şi poată focaliza cu precizie eforturile de marketing. Astfel ca, în funcţie de paginile de internet vizitate si de comportamentul vostru pe internet veţi primii în căsuţa de e-mail oferte de marketing tot mai personalizate. De obicei astfel de informaţii în legătură cu obiceiul utilizatorilor de sisteme de calcul se vând către firme şi/sau persoane fizice de obicei pe sume considerabile. Multe tipuri de spyware merg chiar mai departe de simpla monitorizare a navigării pe internet furând parole, seriile numerele şi numele deţinătorilor cărţilor de credit, etc.

Cum vă puteţi proteja de asemenea programe? În mod ironic, mulţi utilizatori sunt de acord cu instalarea lor. De fapt, ştergerea câtorva spyware şi adware poate face anume programe gratuite sau programe care se folosesc o anumita perioada de timp (shareware), nefolositoare. Voi enumera mai jos cinci paşi, prin care te poţi proteja de spyware şi adware.

Fii atent de unde descarci aceste programe - Programele suspecte vin de pe site-uri suspecte. Daca te uiţi după programe cu folosinţă gratuită sau cu folosinţă pentru o anumită perioadă de timp (shareware) instaleaza-le de pe pagini de internet cu o reputaţie foarte bună (tucows.com, download.com, softpedia.com).

Nu descărcaţi programe de pe pagini de internet care oferă programe furate (programe care de obicei au licenţa comercială iar acele site-uri de internet le dau gratuit împreuna cu cheile de decodare - aşa numitele keygen-uri.). Programele luate din aceste surse sunt „injectate” de obicei cu o mare cantitate de viruşi extrem de periculoşi.

Citiţi cu foarte mare atenţie licenţele de acord ale utilizatorilor - În engleza se numeşte „End User Licence Agreement” (E.U.L.A) Este o specificaţie tehnică foarte lunga adesea de neînţeles plină cu tot felul de chichiţe juridice care se termină cu 2 butoane pe care scrie „Nu. Nu sunt de acord” şi „Da! Am citit şi sunt de acord cu termenii şi condiţiile”. Majoritatea oamenilor bifează că

sunt de acord cu aceşti termeni fără să fi citit nici un cuvânt. Aceasta licenţă este un acord legal intre utilizator şi creatorul acelui program. Fără să citeşti eşti de acord (fără să vrei) să instalezi programe de tip spyware sau alte tipuri de programe maliţioase care nu fac bine sistemului tău de calcul. De aceea, este bine să citeşti această licenţă, şi dacă interesele tale o cer, să nu te sfieşti să nu fi de acord cu acea licenţă.

Citeşte înainte să dai click. Câte odată, când vizitezi o pagină de internet, vă apare o căsuţă de text. Ca şi licenţa de utilizare, mulţi utilizatori consideră în necunoştinţă de cauză că trebuie doar să apese pe „Yes" sau „OK". Făcând acest lucru fără să citiţi ce conţine acea licenţă, a-ţi putea spune: „Da! Sunt de acord să-mi instalez programul vostru spyware pe calculatorul meu.". De aceea este bine să vă opriţi şi să citiţi acea licenţă.

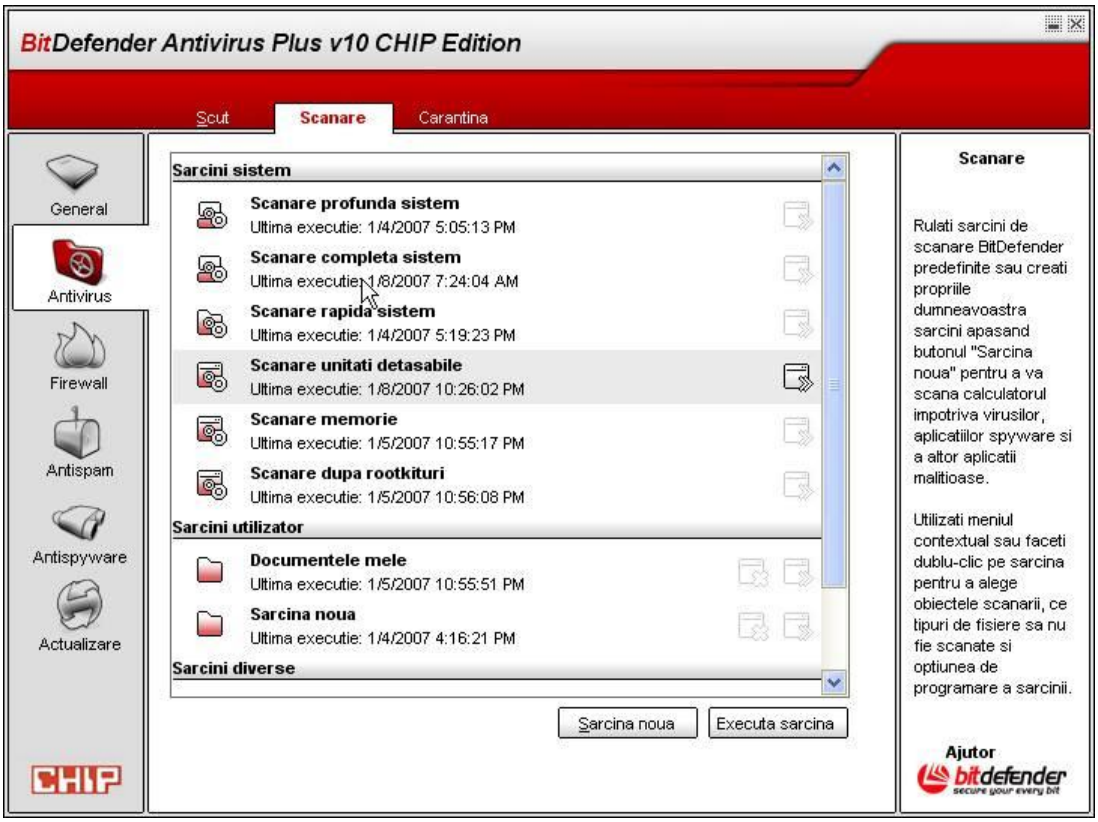
Protejează-ţi sistemul - Poţi să-ţi protejezi sistemul cu multe programe antivirus apărute pe piaţa în ziua de astăzi. O mare parte din firmele care vând calculatoare că au sistem de operare Windows au şi programe antivirus instalate pe aceste calculatoare. Este bine ca cel puţin odată pe saptamîna să faceţi o actulaizare pentru antivirus. Dacă produsul vostru antivirus nu detectează şi nu blochează spyware puteţi încerca, produse tip Adware (program special de detecţie a acestor tipuri de viruşi) care vă protejează sistemul de spyware sau adware în timp real.

Scanează-ţi sistemul - Chiar dacă programele antivirus, firewall şi alte măsuri de protecţie îţi monitorizează sistemul de calcul, tot este indicat să scanezi periodic tot sistemul.

IV. INSTALAREA ŞI CONFIGURAREA UNUI PROGRAM ANTIVIRUS

În era viruşilor şi a viermilor este necesară instalarea unui antivirus înainte de conectarea la internet. Pe fondul numeroaselor vulnerabilităţi din Internet Explorer, este suficientă apelarea unei pagini web pentru a permite accesul unui program dăunător în sistem. Pe lângă numeroase alte produse comerciale, utilizatorii particulari se pot baza şi pe utilitare gratuite. Un astfel de exemplu este AntiVir. AntiVir Personal Edition poate fi descărcat de la adresa http://www.avira.com/en/avira-free-antivirus. Singura problemă este faptul că aplicaţia AntiVir nu verifică şi mesajele cu ataşamente de prezenţa programelor dăunătoare. După instalare, antivirusul este integrat automat în centrul de securitate al Windows XP, iar starea acestuia este monitorizată permanent.

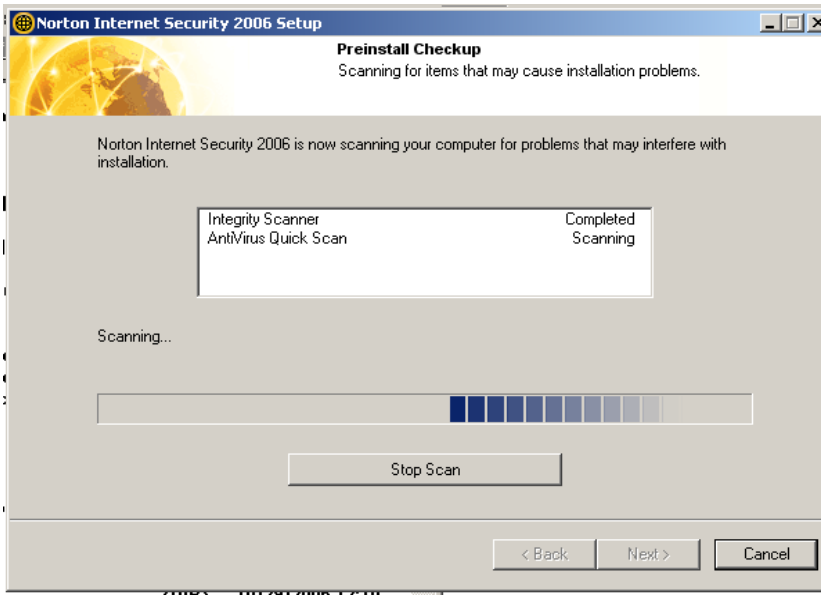
Dacă în sistem este descoperit un virus, aplicaţia indică acest lucru printr-o informare acustică şi/sau vizuală. De multe ori se întâmplă însă ca viruşii să fie îndepărtaţi din sistem, dar să se reîncarce imediat în memoria de lucru, prin intermediul unui script. În acest caz este necesară o repornire, urmată de verificarea sistemului în Safe Mode. Prin acţionarea tastei [F8] în timpul pornirii şi alegerea modului Safe Mode sunt încărcate numai driverele necesare, iar viruşii nu au nici o posibilitate de a se încărca în memorie. Dacă virusul găsit este recunoscut corect, însă nu poate fi eliminat din sistem, căutaţi pe internet informaţii despre acesta. Producătorii de programe antivirus oferă aceste informaţii pe paginile lor de internet şi, în plus, veţi găsi sfaturi preţioase despre cum poate fi îndepărtat virusului respectiv sau despre diverse utilitare speciale. Un alt exemplu de program antivirus este BitDefender Plus Chip Edition (se poate obţine o versiune gratuită cu revista Chip)



Multe componente de calculator, cum ar fi plăcile de bază, sunt livrate cu soluţii software antivirus. Poate fi deci util să aruncăm o privire asupra conţinutului CD-ului cu driverele de instalare al componentelor achiziţionate. De asemenea majoritatea firmelor producătoare de programe antivirus pun la dispoziţia clienţilor versiuni de evaluare care sunt funcţionale un interval de timp limitat. Aceste versiuni demo pot fi totuşi utile în caz de urgenţă.

Să vedem în continuare cum se instalează şi cum se configurează o aplicaţie antivirus. Am ales spre demonstraţie aplicaţia Norton Intenrent Security al firmei Symantec pentru că pe lângă aplicaţia propriu zisă de antivirus are incluse toate module suplimentare foarte utile în timpul navigării pe internet cum ar fi un Firewall configurabil respectiv un modul pentru e-mail, spam, adware şi spyware şi în al doilea rând pentru că a fost inclus în pachetul de utilitare primite împreună cu driverele plăcii de bază folosit de autor, deci îl putem folosi legal.

După lansarea aplicaţiei de instalare (de obicei setup.exe sau instal.exe) acesta va solicita utilizatorului o pre-scanare a sistemului. Este bine să acceptăm această „oferta" având în vedere că există posibilitatea ca să existe deja o infecţie cu viruşi activi în memoria calculatorului caz în care acesta ar putea compromite chiar programul antivirus. Putem renunţa la aceasta presacanare doar în situaţia în care urmează să instalăm aplicaţia pe un calculator care tocmai a fost configurat şi pe care sa instalat pe „curat" sistemul de operare folosindu-se un kit de instalare din surse sigure. (Atenţie ! Chiturile de instalare piratate de cele mai multe ori sunt virusate, generatoarele de chei sau patch-urile care „sparg" protecţia antipiraterie nu sunt gratuite, le primim cu cai troieni. Aviz amatorilor.). Se recomandă de asemenea instalarea programului antivirus imediat după instalarea şi configurarea sistemului de operare dar înainte de a ne conecta la internet. Prima conexiune la internet ar trebuii să fie actualizarea listei de viruşi recunoscuţi de programul nostru antivirus de pe site-ul producătorului.

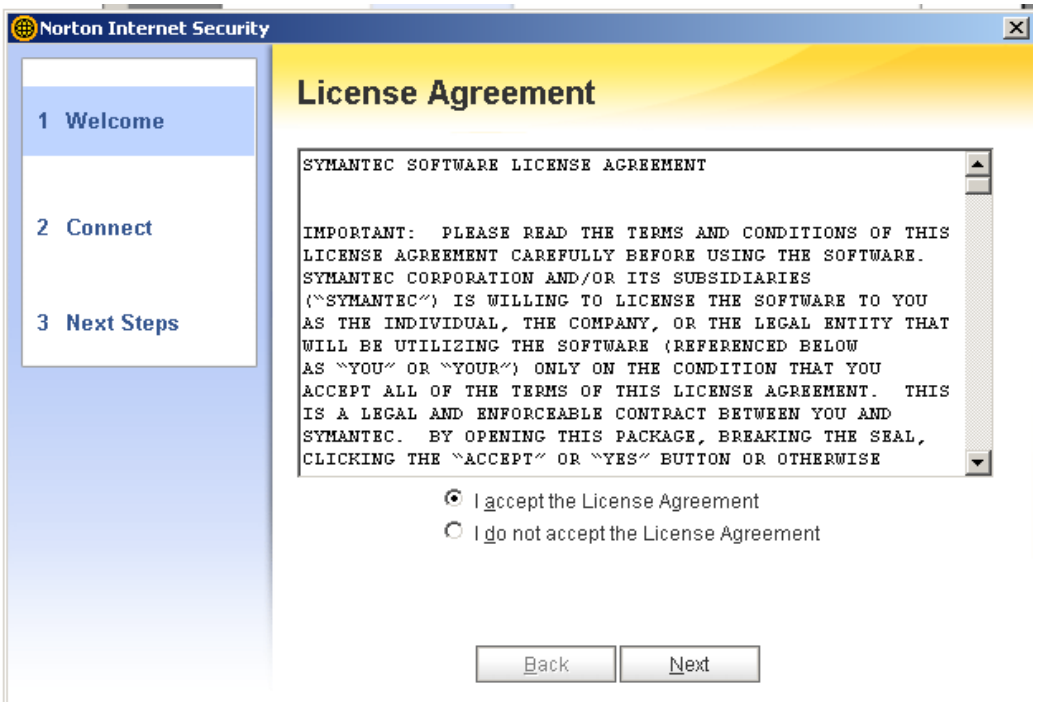


După ce scanarea are loc cu succes, adică fără să se semnaleze prezenţa vreunui virus se trece la instalarea propriu zisă a aplicaţiei (Atenţie ! În această fază de prescanare programul va căuta doar în memoria calculatorului şi în aplicaţiile care rulează în acel moment pe PC şi putând

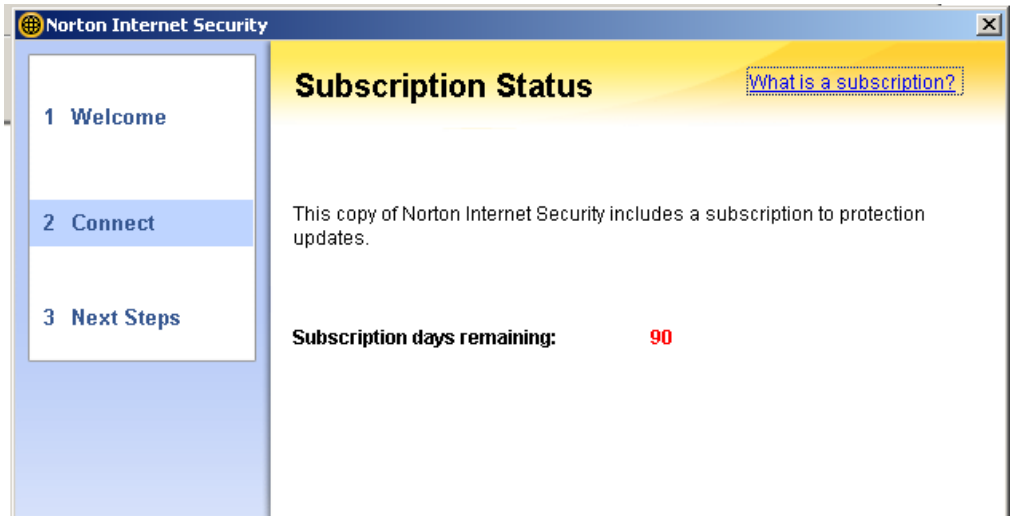
recunoaşte doar viruşii incluşi în lista de viruşi până la data emiterii chitului de instalare care de multe ori este depăşit chiar cu câţiva ani).

În pasul următor trebuie să ne alegem tipul de instalare în funcţie de numărul de utilizatori care au acces la calculator. Astfel pentru o mai bună protecţie şi pentru a permite configurări mai ample am ales a doua modalitate cel care permite configurarea setărilor pentru mai mulţi utilizatori. Chiar dacă folosiţi calculatorul doar acasă este bine ca să creaţi un cont de utilizator cu drepturi limitate numai pentru a naviga pe internet ceea ce înseamnă implicit instalarea aplicaţiei antivirus cu opţiunea de configuraţii mai complexe **Install with acounts and parental Control**.

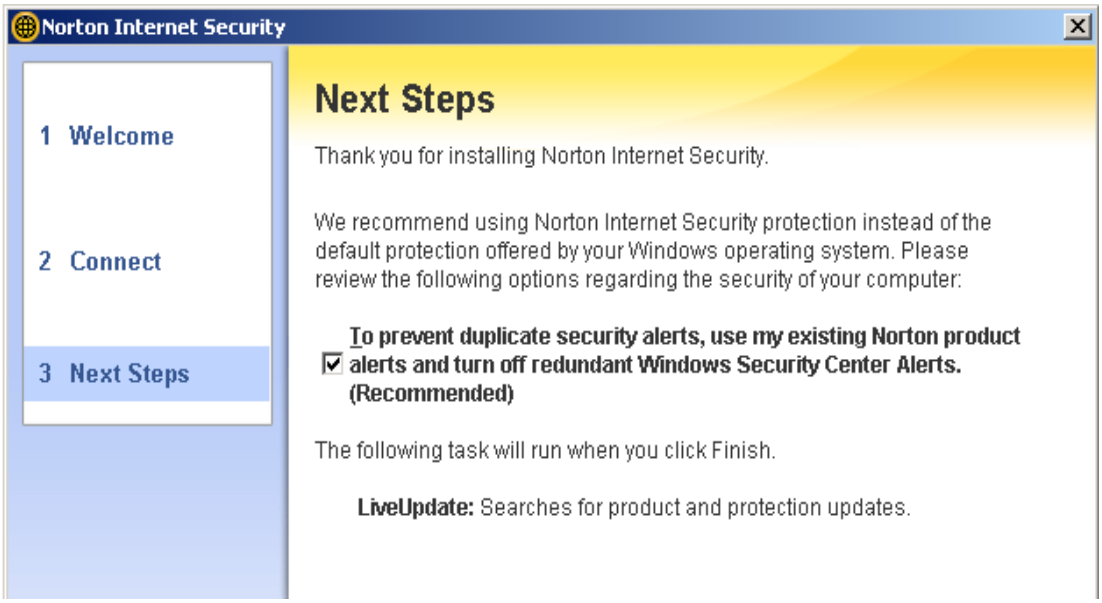
În pasul următor are loc instalarea propriu zisă a aplicaţiei adică copierea pe hard discul calculatorului a fişierelor programului precum adăugarea la regiştrii a informaţiilor necesare funcţionării programului antivirus. La finalizarea instalării trebuie să repornim calculatorul astfel încât aplicaţia antivirus să se “integreze” în sistemul de operare, repornire solicitată chiar de modulul de instalare al programului. După repornirea calculatorului aplicaţia este automat lansat în execuţie şi pentru început afişează câteva informaţii utile despre program cum ar fi drepturile de utilizare,



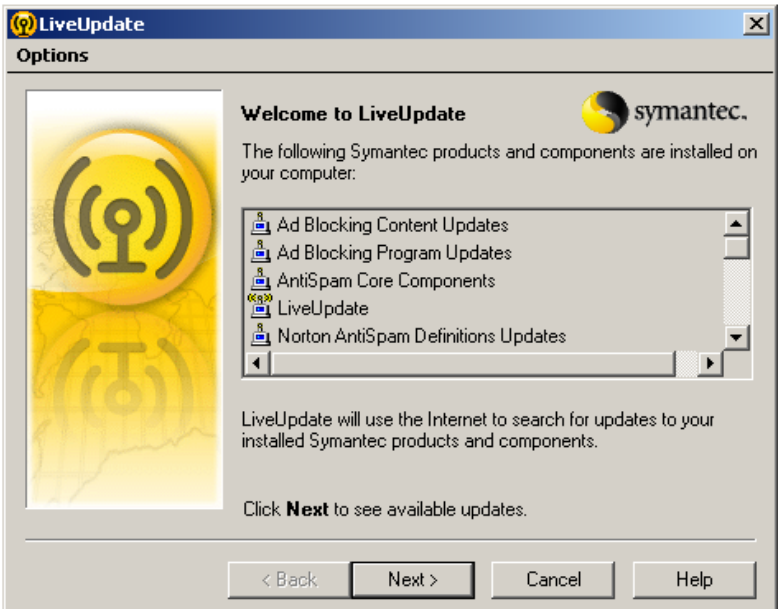
perioada de subscriere (anunţare a programului la producător sau perioada cât putem descărca gratuit actualizările de viruşi).



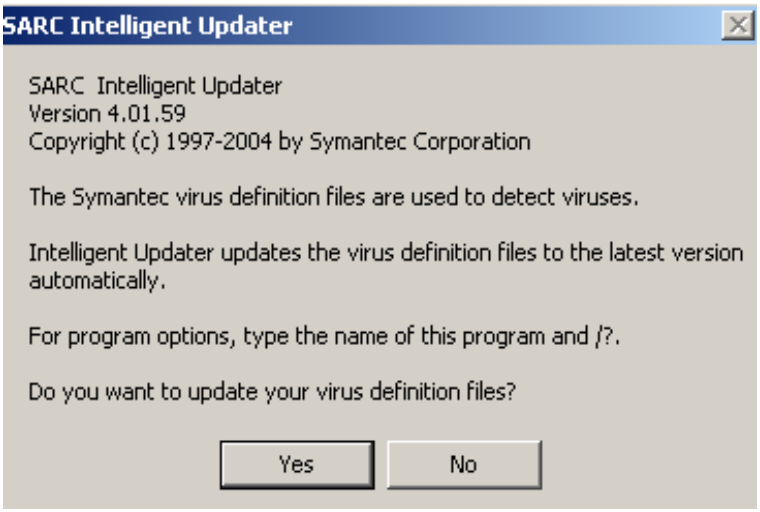
Programul ne va cere acordul pentru a dezactiva celelalte aplicaţii de securitate (în speţă Windows security) este nevoie de acest lucru dat fiind faptul că anumite aplicaţii de securitate pot intra în conflicte care pot duce la blocarea calculatorului. Este posibil de exemplu ca nu program antivirus să găsească semnăturile unor viruşi în baza de date al unui alt program antivirus şi să declanşeze operaţiile de eliminare a virusului astfel al doilea program antivirus poate deveni inoperaţional.



După ce trecem de aceste elemente informative urmează faza în care aplicaţia va iniţia legătura cu site-ul producătorului pentru a descărca ultimele liste de viruşi şi eventualele componente îmbunătăţite ale programului. Evident pentru această operaţiune trebuie să fim conectaţi deja la internet. Dacă nu suntem conectaţi la internet putem face totuşi cea mai importantă operaţie, anume actualizarea listei de viruşi, folosind un fişier descărcat recent de pe site-ul producătorului de pe un alt calculator conectat la internet. Firma Symantec pune la dispoziţia utilizatorilor noi liste de viruşi cu o regularitate de 10-14 zile.



Actualizare automată



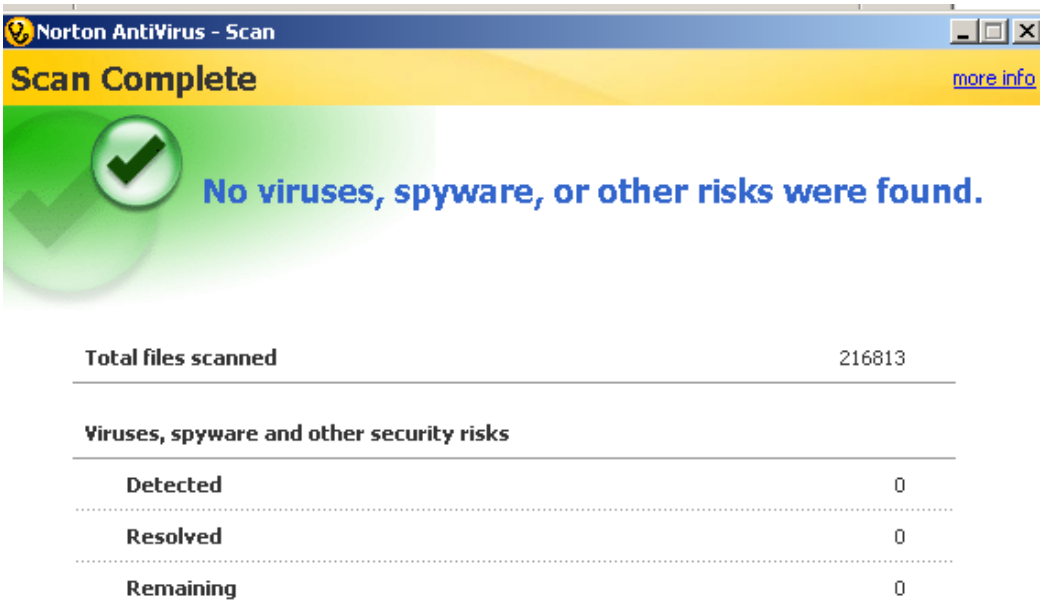
Actualizare manuală

După ce actualizările au fost efectuate programul este gata de acţiune. Atenţie putem sări peste etapele de actualizare dar nu se recomandă acest lucru.

Abia acum putem spune că am terminat instalarea aplicaţiei. Este afişat o fereastră de unde putem vedea starea diferitelor componente ale aplicaţiei. Ne interesează acele elemente care sunt marcate cu semnul exclamării. Dacă instalarea a decurs normal şi sau făcut actualizările singurul asemenea element este cel legat de scanarea completă a sistemului. Presupunând că nu a existat un alt program antivirus pe sistem este posibil să avem fişiere virusate care în etapa de prescanare nu au fost găsite aceştia nefiind activi în memorie. Urmează deci să realizăm o scanare completă a sistemului. Pentru acesta dăm clic pe elementul marcat cu semnul de exclamare şi deschidem informaţiile detailate (Detailed Status). Va apărea o nouă fereastră unde putem observa ca în dreapta stării **Full System scan** avem mesajul **Not completed** .

Pentru a remedia această problemă vom da clic pe textul Full System Scan iar aplicaţia va începe scanarea tuturor fişierelor de pe discurile calculatorului. În funcţie de cantitatea de fişiere stocate pe calculator această operaţie poate dura de la câteva minute până la câteva ore. Se recomandă ca la scanarea calculatorului să nu se facă şi alte operaţii pe calculator, deşi pe calculatoare suficient de puternice scanarea va putea rula liniştit în fundal fără să afecteze semnificativ viteza de rulare a celorlalte aplicaţii.

După terminarea scanării dacă avem noroc vom avea următoarea fereastră care ne informează despre rezultatele scanării:



BIBLIOGRAFIE

1. Dabija George, *Securitatea sistemelor de calcul*, auxiliar curricular elaborat în cadrul proiectului *Învăţământul profesional şi tehnic în domeniul TIC,* proiect cofinanţat din Fondul Social European în cadrul POS DRU 2007-2013
2. D.W. Davies, W.L. Price, "*Security for Computer Network*", John Wiley & Sons 1989.
3. Angheloiu A, Gzorfi E, Patricu V, Securitatea şi protecţia informaţiei in sistemele electronice de calcul, ed. Militara, Bucureşti 1986.
4. Incze Arpad, *Securitatea în Internet. Ameninţări, atacuri, viruşi*, Curs Universitatea „1 Decembrie 1918" Alba Iulia
5. ro.wikipedia.org