Aspecte calitative şi cantitative ale eficienţei sistemelor de protecţie a calculatoarelor împotriva viruşilor

Prof..dr. Constantin BARON, ec. Mihai BARON,
Catedra de Informatică Economică, A.S.E., Bucureşti

Din punct de vedere teoretic, protecţia calculatoarelor împotriva viruşilor nu se poate realiza, dar eficienţa metodelor, tehnicilor şi mijloacelor folosite în prezent este suficient de bună pentru a satisface cerinţele reale şi exigenţele practice.
Nu există şi nici nu poate exista o metodă sau o tehnică unică de asigurare a protecţiei calculatoarelor împotriva viruşilor, dar există posibilitatea de folosire combinată a unor metode, tehnici şi mijloace care includ, alături de programe specializate antivirus, şi măsuri organizatorice corespunzătoare.
Într-un astfel de context, această lucrare abordează câteva aspecte generale, calitative şi cantitative mai semnificative care caracterizează, în prezent, sistemele reprezentative de protecţie a calculatoarelor împotriva viruşilor.
Cuvinte cheie: *sistem integrat de protecţie antivirus, sistem de protecţie totală antivirus, program scan, program monitor, sume de control criptografic, suprafeţe de integritate.*

Aspecte generale

Un sistem de protecţie a calculatoarelor împotriva viruşilor se poate defini ca un ansamblu de componente (mijloace, metode, tehnici, programe) interdependente, care interacţionează pentru realizarea unor obiective determinate de protecţie antivirus. În funcţie de natura obiectivelor şi de modul în care aceste componente interacţionează se disting:
a) sisteme integrate de protecţie;
b) sisteme de protecţie antivirus.
Un **sistem integrat de protecţie antivirus** are ca obiective specifice: folosirea unei diversităţi de componente (mijloace, metode, tehnici, programe); combinarea componentelor pentru folosirea cât mai eficientă a fiecăreia dintre acestea; obţinerea unui efect sinergic cât mai mare din folosirea combinată a acestor componente.
Deci, într-un sistem integrat de protecţie antivirus se pune accentul pe *aspectul sinergic* al folosirii unei diversităţi de componente.

Un **sistem de protecţie totală antivirus** are ca obiective specifice: protecţia tuturor resurselor calculatorului (fizice, logice, informaţionale) şi asigurarea unui ciclu complet de protecţie antivirus alcătuit din prevenirea infectării calculatoarelor cu viruşi, detectarea viruşilor care au pătruns în calculatoare, eliminarea viruşilor detectaţi şi refacerea resurselor calculatoarelor afectate de viruşi. Deci, într-un sistem de protecţie totală antivirus se pune accentul pe *aspectul global* al folosirii unei diversităţi de componente. Într-un context determinat, un sistem integrat de protecţie antivirus poate deveni un sistem de protecţie totală antivirus, iar un sistem de protecţie totală antivirus include implicit o diversitate de componente tipice unui sistem integrat de protecţie antivirus.

Aspecte calitative

Eficienţa sistemelor de protecţie a calculatoarelor împotriva viruşilor trebuie să fie considerată din mai multe puncte de vedere [Baron, 1996c].

• În primul rând, această eficiență trebuie să crească odată cu:
- extinderea domeniilor de activitate în care se folosesc calculatoarele electronice;
- creșterea numărului de utilizatori care posedă calculatoare personale, care folosesc sau care au acces la acestea, individual sau în rețele;
- creșterea numărului de viruși informatici și al variantelor de viruși (în prezent peste 7000, cu o creștere în medie cu câte 3-4 viruși pe zi);
- perfecționarea modului de acțiune a virușilor și de mascare a prezenței acestora în calculatoarele utilizatorilor;
- extinderea scopului acțiunii virușilor, de la scopul presupus inițial (de protecție a produselor software achiziționate în mod neautorizat) până la scopul de sabotaj, începând de la nivel de simplu calculator personal până la rețele de calculatoare deosebit de mari și de imortanță vitală (de exemplu, Internet);
- existența unor numeroase posibilități, căi și mijloace de infectare a calculatoarelor cu viruși, unele dintre acestea putând fi evitate (încărcarea sistemului de operare, sistemul de întreruperi ale microprocesoarelor, folosirea discurilor flexibile etc).

• În al doilea rând, această eficiență trebuie considerată într-un context evolutiv de forma:

1. PREVENIRE; 2. DETECTARE; 3. ELIMINARE; 4. REFACERE.

1. **PREVENIREA** infectării calculatoarelor cu viruși, ca necesitate de natură *profilactică*, implică:
a) luarea măsurilor organizatorice corespunzătoare, pentru a se evita la maxim infectarea pe diferite căi cu viruși;
b) folosirea diferitelor programe de prevenire a infectării cu viruși, selectate din cele mai cunoscute pachete de programe antivirus (VSAFE, FPROT, TBSCANX, NAV, UTSCAN, RAV etc);

2. **DETECTAREA** și identificarea virușilor care au pătruns în calculatoare pe diferite căi și prin diferite mijloace, ca necesitate de natură *terapeutică*, implică:
a) luarea măsurilor corespunzătoare pentru a evita extinderea infecției cu viruși la alte zone ale calculatoarelor, ca: renunțarea la folosirea fișierelor infectate cu viruși; resetarea la rece a calculatoarelor; deconectarea calculatoarelor de la rețeaua electrică;
b) folosirea de diferite programe de detectare și identificare a virușilor, selectate dintre cele mai cunoscute pachete de programe antivirus (SCAN, MSAV, TBSCAN, FPROT, NAV, RAV etc), pentru: detectarea și identificarea virușilor după semnături (amprente); detectarea și identificarea virușilor după intenții (acțiuni);

3. **ELIMINAREA** virușilor detectați în calculatoare prin semnături sau prin intenții, ca necesitate de natură *curativă*, implicând:
a) luarea măsurilor corespunzătoare pentru a evita întreprinderea unor acțiuni care să dăuneze și mai mult calculatoarelor, ca: utilizatorii, oricare ar fi aceștia, să nu intre în panică, deoarece unele pagube pot fi produse de către utilizatorii înșiși și nu de viruși; măsuri radicale (ca de exemplu, reformatarea discului fix) să fie adoptate ca soluții limită, atunci când alte măsuri nu mai pot fi luate;
b) folosirea de diferite programe de eliminare a virușilor detectați din cele mai cunoscute pachete de programe antivirus (CLEAN, MSAV, TBCLEAN, UTSCAN, FPROT, NAV, RAV etc);

4. **REFACEREA** zonelor (resurselor) calculatoarelor afectate de acțiunile virușilor, ca necesitate de *restabilire* a posibilităților inițiale de exploatare, implică:
a) luarea măsurilor necesare pentru reducerea la minim a pagubelor produse de viruși, ca: salvarea pe dischete a unor fișiere de date de importanță deosebită; folosirea unor copii de rezervă pentru

reinstalarea în calculatoare a programelor folosite de utilizatori;
b) folosirea de diferite metode de refacere (restabilire), în funcţie de posibilităţile lor reale, ţinând seama de modul cum au fost afectate aceste zone (resurse) de către viruşi şi anume: refacerea (restabilirea) prin folosirea unor programe din cele mai cunoscute pachete de programe antivirus (MSAV, CLEAN, TBCLEAN, UTSCAN, FPROT, NAV, RAV etc); refacerea (restabilirea) prin înlocuirea programelor distruse cu cele originale (de pe dischete sau CD-ROM-uri fără viruşi); refacerea (restabilirea) prin înlocuirea fişierelor de date distruse cu copii ale acestora (de pe dischete fără viruşi); refacerea (restabilirea) prin restaurarea sectorului de BOOT, a tabelei de partiţionare şi a configuraţiei CMOS.
Având în vedere extinderea considerabilă a utilizării calculatoarelor, atât în mod individual cât mai ales în reţele, precum şi creşterea continuă a performanţelor hardware şi software, la **mijloacele de protecţie a calculatoarelor împotriva viruşilor** reprezentate prin tetrada **PREVENIRE-DETECTARE-ELIMINARE-REFACERE,** mai pot fi adăugate şi unele constatări efectuate de utilizatorii înşişi în diferite situaţii, care interpretate corect sporesc eficienţa protecţiei antivirus [Baron, 1996].
Astfel, orice schimbare apărută în comportamentul hardware-ului şi software-ului poate fi suspectă, exceptând situaţiile când cauza acestei schimbări este cunoscută.
Dintre **schimbările suspecte** semnalate, mai importante se pot menţiona următoarele:
- spaţiul de memorie disponibilă a scăzut, ca urmare a copierii şi multiplicarii viruşilor;
- programele necesită mai mult timp pentru execuţie decât în mod normal;
- programele nu mai lucrează corect, provocând căderea sistemului sau resetarea acestuia după un anumit timp;
- datele dispar sau suferă pagube;
- dimensiunea unor programe a crescut faţă de normal, ceea ce face imposibilă lansarea lor în execuţie, cu afişarea uneori pe ecran a mesajului: "**Too big to fit în memory**";
- ecranul se comportă ciudat, în sensul că toate caracterele care se afişează se "prăbuşesc";
- nu se mai poate folosi nici o informaţie afişată pe ecran, deoarece printre informaţiile utile sunt intercalate informaţii fără vreo semnificaţie;
- emiterea unor sunete la anumite intervale de timp sau interpretarea unor fragmente de melodii (exemplu, Yankee Doodle);
- redefinirea tastelor, astfel că nu mai corespund caracterele de pe tastele apăsate cu cele afişate pe ecran;
- programul CHKDISK detectează diferite erori la controlul discului fix.
Cu cât aceste schimbări sunt sesizate mai din timp, cu atât acţiunile viruşilor sunt mai reduse şi implicit daunele produse calculatoarelor sunt mai mici.

Aspecte cantitative

Eficienţa sistemelor de protecţie a calculatoarelor împotriva viruşilor se poate exprima şi sub aspect cantitativ, comparând costurile aferente tehnicilor de protecţie (apărare) antivirus cu costurile cauzate de acţiunile viruşilor. În prezent, cele mai importante tehnici de protecţie antivirus, aflate în competiţie, sunt următoarele [Cohen, 1995]:
- protecţia antivirus bazată pe programele de tip **scan**;
- protecţia antivirus bazată pe programele de tip **monitor**;
- protecţia antivirus bazată pe **sumele de control criptografic**;
- protecţia antivirus bazată pe **suprafeţele de integritate**.
Fiecare dintre aceste tehnici se poate exprima printr-o formulă care descrie cele două feluri de costuri, pe o

anumită perioadă de timp [Cohen, 1995; Baron, 1997].

Programele de tip scan:

utilizare atacuri

$$T_s = s[cet_s + I_s + u] + a_n r_s s + a_0 r_s s + d$$

scan nou vechi

Sumele de control criptografic:

utilizare atacuri

$$T_c = s[cet_c + I_c] + [a_n + a_0] r_s o_i + d$$

verificare

Programele de tip monitor:

utilizare atacuri

$$T_m = s[I_m + u] + a_n r_s s + a_0 r_f + d$$

nou vechi

Suprafețele de integritate:

utilizare atacuri

$$T_i = sI_i + [a_n + a_0] r_f + d$$

Tabelul 1

Indicatori de costuri	
Simbol	**Denumire**
T_s	Total pentru programul scan
T_c	Total pentru suma de control criptografic
T_m	Total pentru programul monitor
T_I	Total pentru suprafața de integritate
t_s	Minute per scan
I_s	Licență pentru programul scan
I_m	Licență pentru programul monitor
a_n	Noi atacuri
r_s	Curățirea sistemului
d	Costuri de distribuție
s	Sisteme
c	Verificări/an
e	Cost angajat/min
u	Cost-distrib.*total-actualizare
t_c	Minute per verificare
I_c	Licență pentru suma de control criptografic
I_I	Licență pentru suprafața de integritate
a_0	Atacuri vechi
r_f	Curățirea fișierului
o_I	Rata de răspândire a virușilor

Notă

Cea mai mare parte a indicatorilor din tabelul 1 nu necesită explicații, exprimând costurile corespunzătoare. Costul licenței pentru sumele de control criptografic și suprafețele de integritate este un preț plătit o singură dată. Costul licenței pentru programele de tip scan și monitor este un preț plătit de fiecare actualizare periodică a acestor programe.

o_i este rata de răspândire a virușilor (apreciată la aproximativ **2** pentru un PC obișnuit, într-un mediu obișnuit și **10** pentru un PC dintr-o rețea locală).

d apare în toate formulele astfel că se poate elimina fără pierderea unor informații utile (modificarea semnificativă a rezultatelor).

Din compararea celor patru tehnici de protecție antivirus și implicit a formulelor care le descriu, se pot obține anumite concluzii deosebit de importante pe care se pot baza deciziile de protecție antivirus.

- Comparând programele de tip scan cu sumele de control criptografic, rezultă că dacă costul actualizării și refacerii în urma unor noi acțiuni (atacuri) ale virușilor depășește diferența de cost dintre timpul de realizare a sumei de control și timpul de scanare, adică dacă și numai dacă $u + a_n r_s > ce\,(t_c - t_s)$, atunci programele scan sunt mai puțin costisitoare decât sumele de control criptografic.
- Comparând programele de tip scan cu programele de tip monitor, rezultă că dacă costul total pentru programele scan depășește costul total pentru programele monitor, adică dacă și numai dacă $T_s - T_m = scet_s + a_0 r_s$, atunci scanarea periodică în căutarea virușilor cunoscuți costă întotdeauna mai mult decât "monitorizarea" în căutarea virușilor cunoscuți a fiecărui program înainte de a fi lansat în execuție.
- Comparând sumele de control criptografic cu suprafețele de integritate, rezultă că dacă costul total pentru sumele de control criptografic depășește costul total pentru suprafețele de integritate, adică dacă și numai dacă $T_c - T_i = scet_s + [a_n + a_c] r_s o_i$, atunci verificarea fiecărui program în căutarea de modificări înainte de a fi lansat în execuție este întotdeauna mai eficientă decât detectarea modificărilor în întreg sistemul prin

intermediul sumelor de control criptografic.

• Comparând suprafețele de integritate cu programele monitor, rezultă că dacă diferențele de cost al licenței anuale, la nivel de sistem, sunt mai mici în comparație cu costurile actualizării, adică dacă și numai dacă $T_m - T_i = u + a_n r_s$, atunci suprafețele de integritate sunt întotdeauna mai puțin costisitoare decât programele monitor.

Concluzii

Din aspectele prezentate anterior rezultă că intențiile producătorilor de viruși informatici sunt mult diversificate (imaginația creatorilor de programe de tip virus este prea bogată) în comparație cu posibilitățile oferite de o singură tehnică de protecție antivirus.

Un program antivirus de tip scan poate fi eficient pentru identificarea unor viruși cunoscuți (deoarece în acest scop a fost creat), dar poate fi la fel de ineficient în cazul unor viruși necunoscuți. În această situație cea mai bună tehnică (soluție) de protecție împotriva unor viruși necunoscuți în sistemul de operare MS-DOS (DR-DOS, PC-DOS, Novell-DOS) este evitarea surselor de infecție (discuri flexibile posibil purtătoare de viruși, software pirat etc).

Adoptarea unei tehnici de protecție antivirus este un studiu de compromis, deoarece nu există o astfel de tehnică care să fie de neînvins și nici o combinație de tehnici de protecție antivirus nu este eficientă, din punct de vedere al costului, în orice mediu; deci protecția antivirus "se face", nu se cumpără.

Bibliografie

[Baron, 1996a] Baron C., Zamfir G., Baron M. - *Probleme actuale privind protecția calculatoarelor împotriva viruşilor,* comunicare la Simpozionul Național de Statistică, ASE - București și CNS,25-26 aprilie 1996

[Baron, 1996b] Baron C., Baron M. - *Studiu comparativ privind sistemele de protecție a calculatoarelor împotriva viruşilor*, comunicare la Simpozionul Național de Statistică, A.S.E. - București și Comisia Națională pentru Statistică, 25-26 aprilie 1996

[Baron, 1996c] Baron C., Baron M. - *Sistem integrat pentru protecția calculatoarelor împotriva viruşilor*, comunicare la Simpozionul "Informatică de gestiune", A.S.E., București, 8.07.1996

[Baron, 1996d] Baron C., Baron M. - *Protecția împotriva viruşilor a aplicațiilor informatice în marketing,* comunicare la Sesiunea Științifică Națională "25 de ani de învățământ de marketing în România", Catedra de Marketing, A.S.E., București 25-26 octombrie 1996

[Baron, 1997] Baron C. - The efficiency of the protection systems of the computers against viruses - paper at The third International Symposium of Economic Informatics, Academy of Economic Studies, Bucharest, May, 8-10, 1997

[Cohen, 1995] Cohen F. B. - *Viruşii calculatoarelor*, traducere din limba engleză după lucrarea cu titlul original "A short course on computer viruses", Editura Teora, București, 1995.