Linux sau Windows?

de Eugen Secmerean

Am pus o întrebare dificilă. Am pus această întrebare pentru că orice construcție în domeniul protejării unei infrastructuri informatice trebuie să plece de la premisa de bază: ce platformă foloseşti. Apoi, aplici elemente indispensabile precum politica de securitate, firewall-uri şi antiviruşi. Cu nuanțele de rigoare, balanța a cam înclinat în favoarea Linux, cu amendamentul că nu oricum şi nu pentru oricine.

Cel mai echilibrat răspuns la spinoasa întrebare mi s-a părut a fi cel dat de Mihai Ianciu, de la UTI Systems: „nu cred că pot fi făcute judecăți absolute şi apriorice... este ca şi cum ai întreba care este cea mai sigură maşină. Probabil că dacă ai investi miliarde de euro într-un vehicul, ar putea fi realizat de nu ştiu câte ori mai sigur decât altul, dar merită să investeşti miliarde de euro într-o maşină numai pentru că poți intra frontal, cu 300 km/h, într-un perete de beton, fără să mori? Depinde. Dacă eşti o mică firmă care desfăşoară o activitate informatică medie, normală, fără documente ultrasecrete, atunci un grad de protecție suficient şi bun este dat de Windows sau orice altă platformă echivalentă. Eu cred că Windows oferă o securitate suficientă pentru mediile obişnuite, la prețul corect. Dacă începem să nu mai ținem cont de resursele şi de eforturile necesare, ci doar de gradul de securitate de atins, probabil că există soluții cu care poți obține această securitate superioară celei oferite de Windows".

La rândul său, Bogdan Olteanu, CIO al GeCAD Net, este şi mai prudent: „nu consider, în acest moment, o platformă mai sigură decât cealaltă. Este adevărat că apar vulnerabilități, cu o frecvență supărător de mare mai ales la Windows, însă cred, ca specialist, că este vorba de ceea ce americanii ar numi «The Big Dog». Microsoft este fenomenul cel mai important astăzi şi atunci comunitatea hackerilor şi a tuturor celor ce fac rău vor încerca să atace şi să afecteze platfomele Microsoft. Probabil că peste câțiva ani, ținta favorită va fi alta".

Avira, o companie de securitate fondată de specialişti în RAV (antivirusul cumpărat de Microsoft în 2003), vede lucrurile destul de diferit. Mugurel Tudor, responsabil cu securitatea companiei, spune că platformele Linux sunt mult mai sigure decât platformele Windows, din diverse motive: Windows încearcă să fie cât mai prietenos de folosit, ceea ce se traduce prin foarte mult cod scris, iar când ai multe linii de cod, invariabil ai şi multe buguri, ceea ce înseamnă probleme de securitate. Microsoft a luat însă în serios problema securității abia recent, ceea ce presupune, poate, numeroase probleme de securitate în codul său sursă mai vechi". Pe de altă parte, integrarea foarte strânsă între diversele aplicații Microsoft este o armă cu două tăişuri: foarte uşor de găsit, înseamnă în acelaşi timp că poți profita de o vulnerabilitate într-o aplicație pentru a exploata o cu totul altă aplicație (spre exemplu execuție de cod din Internet Explorer).

Şi pentru că în discuție a apărut problema bug-urilor, Tudor Galoş, segment marketing manager, Microsoft România, explică despre ce este vorba: „bug-uri apar în toate aplicațiile şi sistemele de operare. Un bug este o eroare de cod care cauzează defecțiuni în funcționarea software-ului, sau comportamente neaşteptate şi are mai multe cauze: lipsa de testare a unor scenarii de funcționare lasă unele bug-uri nedescoperite; apariția unor noi scenarii de funcționare; presiuni de timp pe echipele de dezvoltare; schimbări în echipele de dezvoltare etc.". Microsoft a impus însă echipelor sale de dezvoltare un proces numit „engineering excelence", prin care echipele de testare nu semnează un release de software dacă nu trece prin multiple faze de eliminare a bug-urilor. Astfel, înainte de a intra în faza RTM (release-to-manufacturing), orice este acum testat de terțe părți pentru indentificarea bug-urilor. De asemenea impunerea procedurilor din cadrul inițiativei „trustworthy computing" a limitat foarte mult numărul bug-urilor.

Şi atunci, care ar fi problema cu vulnerabilitățile din Windows? „Un bug se tratează în două modalități, după ce este identificat: se scoate un patch, care, în funcție de severitatea problemei, este inclus într-un buletin lunar de securitate, sau este pus spre download imediat.

În paralel, pentru cei care nu pot aplica patch-ul, se creează unul sau mai multe scenarii de evitare a efectelor exploit-urilor de bug-uri (se numesc mitigation techniques); de exemplu, la Sasser exista patch-ul de demult, însă cei care nu au aplicat patch-ul şi au activat Internet Connection Firewall nu au avut nici un fel de problemă" - detaliază Tudor Galoş.

Potrivit lui Mugurel Tudor, de la Avira, premisa de la care trebuie pornit este că nu există software fără buguri, ci doar software pentru care încă nu au fost găsite buguri. Un bug poate fi considerat orice greşeală de programare care ar putea duce la o funcționare anormală a aplicației. Cauzele apariției lui sunt foarte complexe: uneori vina nu este exclusiv a programatorului respectivei aplicații - spre exemplu, dacă un bug este prezent într-o bibliotecă de funcții, el va fi prezent în toate aplicațiile care vor folosi acea bibliotecă.

Oricum, putem considera că, în general, cauza apariției unui bug este o greşeală de programare, iar respectiva greşeală de programare poate izvorî dintr-o slabă cunoaştere a limbajului de programare, din neatenție, din insuficientă analiză asupra problemelor, dintr-un design greşit etc. În momentul în care astfel de probleme sunt detectate, ele sunt (în general) reparate, iar felul în care aceste rezolvări sunt făcute depinde de gravitatea lor şi de politica firmei producătoare: pentru cele mai puțin grave, probabil se va aştepta lansarea unei noi versiuni de program, iar pentru cele foarte grave probabil vor fi lansate patch-uri pentru repararea fişierelor binare afectate (sau instalarea noilor versiuni „sigure" disponibile). Pratica patch-urilor pentru fişiere binare este prezentă în exclusivitate în lumea aplicațiilor comerciale. Pe platformele open source, în general sunt publicate patch-uri la surse, iar utilizatorii sunt încurajați să recompileze noile versiuni (sau să instaleze direct noua versiune gata compilată - astfel de update-uri de securitate sunt furnizate foarte rapid de către distribuțiile de Linux).

Problema rămâne însă la costurile de aplicare a patch-urilor: pentru că, de obicei, un patch serios, instalat pe o maşină Windows, are nevoie de reboot, este de părere Mihai Dincă, de la UTI Systems. „Pentru un ISP, spre exemplu, un reboot care provoacă un down-time de ordinul minutelor este aproape inacceptabil. Peste Linux, instalarea de patch-uri se poate face, în majoritatea cazurilor, fără repornirea întregului sistem. În cazul Code Red, de exemplu, care a afectat serverele IIS, costurile suplimentare pentru aplicarea patch-urilor au fost considerabile. Şi această diferență este, la rândul ei, cauzată de diferența în arhitectura celor două platforme: fiind modular, Linux poate fi patch-uit pe bucăți, fără a avea nevoie să fie reboot-at" - detaliază Dincă. Pe un desktop, un reboot nu este atât de critic, dar pe un server, lucrurile pot fi mult mai complicate. Trebuie adăugat însă că programul de update/patch-uri de la Microsoft este net superior față de cele pentru distribuțiile majore RedHat şi SuSE. Acesta este confirmat chiar şi de certificările acordate de organizații de specialitate precum SANS, care a clasat pe primul loc programul pus la dispoziție de Microsoft.

Şi atunci, cum stăm?

Foarte multe companii au început să rezolve problema într-un mod mult mai radical: au renunțat la sursa problemei. Costin Burdun şi Mihai Dincă, specialişti în securitatea informațiilor în cadrul UTI Systems, consideră că „din toate companiile cu care au lucrat, comparând organizațiile care funcționau pe Microsoft şi cele pe Open Source, balanța, în zona serverelor şi aplicațiilor critice, se înclină în favoarea nu neapărat a Linuxului, ci şi a Unixului, a sistemului Solaris, BSD... foarte în general şi foarte la prima vedere, credem că pe primul loc se situează Unix şi distribuțiile de Linux Red Hat şi SuSe, implementările de BSD şi Solaris fiind destul de rare. Apoi, urmează Microsoft. Linux este mai facil, de aceea este preferat, Unix fiind renumit, de altfel, pentru aplicații enterprise şi critice. În plus beneficiază de acreditări de securitate specifice şi mai ales cerute în mediile guvernamentale. Totuşi, eforturile pe care Microsoft le-a depus pentru îmbunătățirea securității sunt evidente pentru informaticieni. Rețelele omogene în tehnologie Microsoft au câştigat şi continuă să câştige teren".

Dar cel care pune punctul pe „i" este Mihai Dincă: „din punct de vedere al securității, analiza este extrem de complexă, fiind foarte mulți factori ce trebuie cântăriți. Serios vorbind, principalul avantaj al Linux este însuşi conceptul care a stat la baza creării sale: arhitectura modulară. Microsoft, adică platforma Windows, spre exemplu, este construit monolit. Îi dai drumul, faci click dreapta, îi porneşti serviciile şi aştepți să funcționeze. Aceasta poate fi considerată un avantaj: uşurința în instalare şi configurare la Microsoft este extrem de benefică. Linux permite un control mult mai avansat, dar costurile în termen de timp şi personal sunt evident mai ridicate.

Tot în comparație cu Microsoft, partea de rețea din Linux este concepută mult mai corect, folosește implementările standard de protocoale, nu are elemente proprietare, are suport pentru toate mecanismele de securitate, remote access-ul pe Linux este mult mai sigur. Windows, la rândul său, folosește un protocol specific RPC (Remote Procedure Call), care, prin definiție, aduce un risc potențial de securitate major. RPC poate fi apelat de către o mașină pentru a comanda unei alte mașini din rețea să execute anumite lucruri. Deci, un executabil instalat pe un desktop poate comanda, prin acest RPC, resetarea unei stații de lucru din celălalt departament.

Această abordare este cauzată de faptul că Microsoft a marjat mult pe facilități şi uşurință în utilizare, iar pentru apermite aceste caractetistici, a implementat asemenea funcționalități, precum RPC". La rândul său, Costin Burdun detaliază: „este o chestiune de percepție: Linux a început de la a implementa serviciile de bază cât mai corect şi cât mai conform RFC (Request For Comments, standardele în domeniu), fără a se ține cont foarte mult de un potențial utilizator care nu ar şti prea multe.
Totul a fost făcut în primul rând cu respectarea regulilor, ceea ce a rezultat într-o platformă fundamental corectă. În Windows practic s-a pornit cumva invers, dinspre utilizator, creându-se apoi mecanismele interne de lucru. Şi tocmai plecând de la această diferență în abordare apare şi diferența în numărul şi gradul de periculozitate a vulnerabilităților ce sunt identificate în cele două platforme. Astfel, vulnerabilitățile Microsoft sunt mai puține ca număr, dar mai grave, ca efecte - cele din Linux sunt mai numeroase, dar mai puțin critice".

Bogdan Olteanu are experiența lucrului în străinătate. El spune că, de multe ori, responsabilul de aplicarea de patch-uri nu are timpul suficient pentru a testa aceste remedii înainte de a le instala - ceea ce, potrivit regulilor internaționale, nu este recomandat.
„În principiu, fiecare companie care are resursele necesare şi suficiente ar trebui să dispună de un mediu de testare - ceea ce înseamnă practic o dublare a tuturor sistemelor critice, pentru a se putea testa orice noutate în condiții identice celor din activitatea curentă.
În termeni financiari, înseamnă o investiție dublă. Spre exemplu, bursa din New York rulează trei medii de testare în paralel cu sistemul curent, principiul de lucru fiind acela de preluare a sarcinilor în caz de defecțiune" - explică Bogdan Olteanu.
Nu putem vorbi de eficiență pentru programele antivirus dacă acestea nu se bazează pe sisteme de operare pe care se aplică actualizări şi patch-uri la zi. S-a ajuns ca în termen de şapte zile de la publicarea unei vulnerabilități să apară şi exploit-ul respectiv. Şi aceasta este o medie, pentru că de multe ori, exploit-urile apar şi mai rapid. Şi atunci, lucrând cu un antivirus chiar neactualizat de o săptămână, te expui pericolului de virusare.

Potrivit lui Costin Burdun, „o politică de securitate trebuie să prevadă ca pentru componentele critice ale sistemului, să existe un mediu de testare a patch-urilor înainte de a fi instalate în rețea. Soluțiile noastre vin şi cu o platformă de testare, care ajunge să coste, în medie, între 20% şi 30% din valoarea totală a bugetului implementării. Aceasta pentru că nu este neapărat nevoie să creezi mediu de testare pentru întreaga infrastructură, ci numai pentru componentele ei critice".

Dar, este oare chiat atât de importantă platforma? Gheorghe Dobre, fondatorul companiei de training Intelprof, relevă că „până în urmă cu un an chiar, când spuneai securitate, toată lumea se gândea la antivirus şi ia firewall. Acum, lucrurile au evoluat în sensul că organizațiile au înțeles că au nevoie de politici de securitate care să nu se refere numai la nişte măsuri marginale. Trebuie să ştie cum să facă o evaluare de risc, să ştie ce oameni să angajeze atunci când nu dispun de competențele necesare, să înceapă să crească pe plan intern competențele. Pe de altă parte, preocupările au devenit tot mai profunde -numai anul acesta, am ținut deja de patru ori un curs dificil, de implementare a autorităților de certificare cu chei publice (PKI) şi am constatat că este un subiect care preocupă atât integratori, cât şi utilizatori. La fel de solicitate sunt şi cursurile despre configurarea amănunțită a firewall-urilor, cele despre diverse unelte".

Punctul de vedere al trainer-ului este important din cauză că oglindeşte fidel şi imediat nevoile de moment ale utilizatorilor din mediul de afaceri. „Cea mai mare pierdere, din punct de vedere al securității, măsurată în bani, suferită de companiile care au răspuns la un studiu pe această temă, a fost pierderea informației proprietare - nu viruşii, nu alte probleme, ci pierderea informației proprietare a creat cea mai mare pagubă financiară, provocată de cele mai multe ori de cauze interne - distrugere accidentală sau premeditată, furt. Atacurile de tipul ingineriei sociale sune tot mai frecvente - ce multe lucruri poți obține cu o bere! De fapt, utilizatorii nu au de ce să ştie cum se fac setările la un firewall - ci trebuie să cunoască şi să respecte un cod de conduită" - spune Gheorghe Dobre. Indiferent dacă este vorba de Linux sau Windows, am spune noi. ■