



Srebrni metak za IT bezbednost ne postoji

PRVO LOŠA VEST, a zatim još gora – godinama smo daleko od jedinstvene bezbednosne arhitekture koja će štititi sve kompanijske informacije. Razlog je jednostavan: svaka oblast informatičkih tehnologija mora da savlada različite tehničke prepreke pre nego što se uobliče sistemi

zaštite i bezbednosti. U svakoj od tih oblasti danas smo daleko od iole prihvatljive zaštite.

U februaru je kompanija Evalubase Research objavila rezultate istraživanja koje je obuhvatilo pet tehnoloških oblasti: upravljanje podacima, hardver i operativne sisteme, komunikacije i umrežavanje, razvoj aplikacija i industrijske aplikacije. Informatičari su zamoljeni da rangiraju te tehnologije po osnovu performansi, upotrebljivosti, funkcionalnosti, kompatibilnosti, održivosti i bezbednosti. Verujemo da vas neće iznenaditi podatak da je bezbednost bila na poslednjem mestu, tj. najlošije ocenjena, sem u slučaju hardvera i operativnih sistema, kao i komunikacija i umrežavanja – gde je bila preposlednja.

Lošija vest stiže od stručnjaka kompanije Coverity. Ova kompanija je specijalizovana za skeniranje izvornog koda u potrazi za greškama, od kojih većina dovodi do pojava rupa u sistemu zaštite. (Ministarstvo za nacionalnu bezbednost SAD i Univerzitet Stanford izabrali su Coverity da za njih pronalazi greške u alatkama otvorenog koda.) Njihovo istraživanje dokazuje da je matematički nemoguće eliminisati greške iz izvornog koda.

Dakle, to su te vesti – vaši podaci nisu zaštićeni i nikada to neće biti.

SVE JE RELATIVNO

NARAVNO, i bezbednost je relativan pojam. Prošlog meseca su stručnjaci kompanije Coverity objavili podatke o pronalasku grešaka u trideset jednom projektu otvorenog koda. Prosečno je bi-

lo 0,42 greške na svakih hiljadu redova izvornog koda. Programeri bi, znači, trebalo da prave jednu „glupost“ na svakih 2200 redova koda. Međutim, ako taj prosek prihvatimo kao konstantu, onda bi, primera radi, u trideset miliona redova RedHat Linuxa 7.1 bilo 12.600 prob-



lematičnih redova. Po istoj logici, u dvesta trinaest miliona redova koda Debiana 3.1 pronašli bismo 89.460 grešaka.

To ne znači da je Debian manje bezbedan kao serverski operativni sistem od Red Hata ili obrnuto, već ukazuje na vrstu informacija koje možete iskoristiti da biste smanjili rizik, odnosno na alatke kojima ćete kvantitativno proceniti rizik i nakon toga odlučiti kada, gde i da li ćete uopšte koristiti neku tehnologiju.

ZDRAV RAZUM

DA LI SU svim krajnjim korisnicima potrebni klijenti s velikim zahtevima, Windows ili Macintosh? Da li bi neki od njih svoj posao bezbednije obavljali na klijentu skromnih zahteva? Naravno da bi. Kombinacija klijenata s malim zahtevima, bez obzira na to rade li pod Windowсом ili operativnim sistemom za Macin-

toshe, i različitih serverskih sistema savršena je odbrana od mnogih poznatih propusta u sistemu zaštite. Sporedna prednost je izazivanje hakera, koji će odbranu pokušati da probiju veštinama i znanjem stečenim na Windowsu.

Neki zagovornici korišćenja isključivo jedne platforme tvrde da troškovi održavanja više operativnih sistema mogu da budu veliki u raznolikom okruženju. Možda i jeste tako, ali samo kratkoročno gledano. Troškovi koji nastaju posle probijanja sistema zaštite neuporedivo su veći. Na Univerzitetu Merilend procenjuju da vrednost kompanije koju je zadesio samo jedan upad u računarski sistem na tržištu opada za pet procenata, u odnosu na ukupan broj izdatih akcija.

POSLOVANJE = RIZIK

SVAKA FIRMA je izložena riziku čim počne da posluje. Zadatak informatičkih stručnjaka je da opasnost po podatke svedu na najmanju moguću meru. Očekivati jedno rešenje – svojevrsan bezbednosni „srebrni metak“ – nipošto nije realno. Jednosmeran pristup je dokazano opasan po sistem zaštite kada se primenjuje kao strategija jednoobrazne platforme.

Kada se ima u vidu koliko su informacije važne, čak dragocene svakoj kompaniji, možda je došlo vreme da se kompanijski podaci uvrste u završni račun kao njena imovina. Ako se to usvoji kao pravilo, rukovodstvo će sigurno insistirati da se primene najbolje moguće alatke i metodologije kako bi se smanjio rizik po te informacije. A najbolja strategija i nije da sva jaja stavite u jednu korpu. ■

Relja Jović je glavni i odgovorni urednik časopisa Mikro. Njegove uvodne reči pročitajte na adresi www.mikro.co.yu/arhiva/relja.