Linux sigurnost

Zaštita lokalnog računala (2)

Osim što Linux računalo može biti napadnuto "izvana", moramo se pobrinuti da i "unutarnje" stvari ne kompromitiraju sustav. Osim fizičke zaštite, to ćemo napraviti kontrolom korisnika i dodatnom softverskom zaštitom

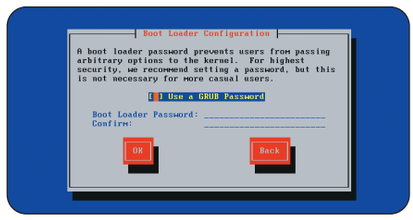
Piše: Ivan Capan

Nakon što smo u prošlom nastavku saznali nešto više o tome tko bi nam i zašto pokušao napraviti nešto loše, red je da ga i pokušamo spriječiti u tome. Više je pristupa tom problemu, ovisno o načinu na koji je računalo izloženo problemima (preko mreže ili od strane lokalnih korisnika). Iako lokalni problemi mogu biti ozbiljniji, najviše ipak trebamo paziti na one druge, jer su češći i zlоćudnijih namjera. Sigurnost ćemo graditi iznutra prema van, tj. prvo moramo biti sigurni da je računalo fizički zaštićeno i da korisnici ne mogu zbog neznanja ili loših namjera napraviti ništa loše, pa ćemo ga tek onda spojiti na mrežu i štititi ga od nje.

Fizička zaštita računala

Prvi stupanj sigurnosti trebao bi biti nedostupnost kućišta iza zaključanih vrata i pod osiguranjem. Kako to često nije moguće, a i osjetno smanjuje funkcionalnost, treba vidjeti što se

▲ ***Screensaver*** **može zaključati ekran ako korisnik neko vrijeme nije za računalom**



▲ **Ponekad se već pri instalaciji omogućuje postavljanje lozinke u *boot loader***

može napraviti na softverskom nivou. Ukoliko netko pokrene računalo s *boot* diskete ili CD-a, nije mu nikakav problem promijeniti *root* lozinku pa je to najčešće prvi (i jedan od najuspješnijih) pokušaja ulaska. Protiv toga se moramo zaštititi postavljanjem lozinke na BIOS ili čak i fizičkim uklanjanjem CD-ROM-a i disketne jedinice. Nažalost, još uvijek vrijedi opcija otvaranja kućišta i resetiranja BIOS-a, ali bar znamo da smo nekome malo otežali posao. Neki proizvođači ugrađuju *default* lozinke tako da sve to pada u vodu. Od krađe diska i kopiranja podataka u drugom računalu možemo se štititi kriptiranjem cijelog datotečnog sustava, ali onda kod svakog resetiranja moramo biti nazočni i upisati lozinku, inače će disk biti potpuno nečitljiv.

Za pokretanje OS-a koriste se *boot loaderi* poput LiLo-a ili GRUB-a. Njihova fleksibilnost omogućuje pokretanje *root* ljuske iz početnog izbornika (*linux init=/bin/sh*). Takva loša praksa može se ograničiti korištenjem opcija "password" i "restricted" u LiLo konfiguraciji, odnosno "password" i "lock" u GRUB-u.

Nakon što se računalo pokrenulo, potencijalni napadač imat će manje mogućnosti jer ga već štiti operacijski sustav. Možda će pokušati resetirati računalo, što mu se može otežati odspajanjem tipke *Reset* na kućištu i komentiranjem retka odgovornog za kombinaciju *Ctrl - Alt - Del* u datoteci /etc/inittab. Neobično je bitno da korisnici (a pogotovo *root*!) ne ostavljaju svoj *desktop* dostupnim kad neko vrijeme nisu za računalom. To se može riješiti automatskim *screensaverom* (xlock) koji će usput i zaključati ekran.

Korisnici i njihove lozinke

Ne mora se posebno naglašavati koliko je nužno imati kvalitetne lozinke za svakog korisnika. Korisnici ne vole previše pamtiti pa tako odabiru lozinke temeljene na broju telefona, datumu rođenja ili nekom obiteljskom imenu, a kao kuriozitet drže ga na komadu papira nalijepljenom na monitor. Dobra lozinka trebala bi se sastojati od barem osam znakova, od kojih su dvije znamenke, a ostatak slučajno odabrana slova, a nikako ne neka postojeća riječ iz bilo kojeg konteksta. Naime, postoje programi koji