

Biztonsági szolgáltatások a Red Hat Enterprise 4-ben



A Red Hat Enterprise Szerver felépítése azt bizonyítja, hogy „a kevesebb sokszor több” – különösen egy jól megvalósított SELinux révén.

Ebben a hónapban véget ér a biztonsági lehetőségekről szóló három részes disztribúció-áttekintő sorozatunk. *SUSE Linux 10.0*-val kezdtem, majd *Debian GNU/Linux 3.1*-gyel folytattam, végül ebben a részben a *Red Hat Enterprise Linuxról (RHEL)* lesz szó. A *Red Hat Enterprise Linux* egy általános célú *Linux* disztribúció, amely a szerverek és az asztali gépek piacát is megcélozza. Amint a nevéből is látszik, az *RHEL* igen robusztus kíván lenni, stabil és skálázható; más szóval: egy nagyvállalat igényeinek is meg akar felelni, éles környezetben. Ez nem is meglepő, hiszen az *RHEL* arról híres, hogy minden tekintetben a csúcson teljesít. A *SUSE Linux*hoz hasonlóan az *RHEL* is futtatható az *IBM eServer z-Series mainframe* nagygépeken is. A kiválasztott szoftvercsomagokra vonatkozóan a *Red Hat* (a *SUSE Linux*nál sokkal inkább, de a *Debian*-nál is jobban) ragaszkodik ahhoz a megközelítéshez, hogy „a kevesebb sokszor több”. Míg egy teljes *Debian* rendszer 15000-nél is több csomagból áll, a *SUSE* is 4000 felett tartja a csomagot számát, az *RHEL* megelégszik 1730-cal (beleértve az *RHEL* alkalmazásszervert és az extra csomagokat is, melyek nem részei a szigorú értelemben vett operációs rendszernek).

Egyáltalán nem eufémizmus azt mondani, hogy ezt az irányválasztást jól védhető. A hivatalosan támogatott csomagok számának korlátozásával a *Red Hat* jóval kisebb támadási felületnek van kitéve (nem is beszélve a segítségnyújtó alkalmazottaktól elvárt ismeretekről). A kevesebb csomag kevésbé bonyolult rendszert eredményez, ez pedig nagyobb stabilitást és biztonságot jelent (legalábbis elméletben).

Ennek a tervfilozófiának azért hátrányai is vannak. Korlátozottabb módon lehet válogatni az eszközök közül (hálózati kiszolgálók és háttérprogramok, titkosítási és egyéb eszközök terén), kisebb a rendszer rugalmassága; megnő annak a valószínűsége, hogy kénytelen lesz a felhasználó egy harmadik féltől származó csomagot telepíteni; esetleg saját magának kell lefordítania egy-egy programot közvetlenül a forrásból.

Ahogy azt már többször említettem korábbi cikkeimben, alapvetően nincs semmi gond a házilag fordított programokkal, különösen akkor, ha ez bizonyos összetevők „bele nem fordítását” (azaz kizárását) jelenti, hatékonysági vagy biztonsági megfontolásokból. De semmi sem kelhet versenyre a disztribúció által támogatott bináris csomagokkal az automatizált biztonsági frissítések terén. A *Gentoo*-

n kívül egyetlen nagyobb disztribúciónak sincsenek automatikus eszközei olyan programok biztonsági frissítésére, amelyeket a helyi gépen közvetlenül forráskódból fordítottak.

Ezen kívül, ahogy arra majd rá fogok mutatni, az *RHEL ES (Enterprise Server) 4* a *SELinux*tól eltekintve (*SELinux = Security Enhanced Linux, megerősített biztonságú Linux*) különösen is csínján bánik azokkal a programokkal, melyek kifejezetten a biztonság megerősítését vagy a biztonsági rések pártázását szolgálják. Ez nem azt jelenti, hogy az *RHEL*-t alacsonyabb biztonságúnak gondolnám; a kisebb támadási felülete és a kitérő *SELinux* támogatása egyaránt kimagasló színvonalú. Ez inkább azt jelenti, hogy más, nagyobb disztribúciókkal összehasonlítva kevesebb választásunk van egy *RHEL*-alapú biztonságos szerver vagy asztali gép kialakításának módját illetően, illetve még kevesebb választásunk van arra nézve, hogy hogyan használjuk a biztonsági alkalmazásokat.

A RHEL ES 4 telepítése

A *Red Hat Enterprise Linux* igen egyszerűen használható grafikus telepítővel rendelkezik, amely – az alap operációs rendszer telepítése mellett – lehetővé teszi számos további programcsomag kiválasztását,

1. táblázat *Néhány biztonsági programcsomag az RHEL ES 4-ben*

Csomag neve	Leírása
bind-chroot	Beállítja a BIND-alapú DNS szerveret chroot jail-ben (átállított gyökérkönyvtárú, nagy biztonságú operációs rendszer-részben) való futtatásra.
dovecot	Biztonságos futásra kihegyezett IMAP szerver (levélkézbeszítő).
freeradius	RADIUS hitelesítési szolgáltatás hálózati eszközök számára
krb5-server	Kerberos hitelesítési és titkosítási szerver.
splint	Eszköz C nyelvű programkódok ellenőrzésére, különös tekintettel a biztonsági sebezhetőségeket rejtő hibákra.
vsftpd	Nagy biztonságú FTP kiszolgáló. Ez az RHEL egyetlen FTP szervere – kitűnő választás.
cryptsetup	Titkosított fájlrendszer létrehozását teszi lehetővé (virtuális blokkeszközökként).
ethereal, tcpdump	Klasszikus protokollelemzők (azaz csomagkémlelő).
gnupg	E-mail titkosító eszköz (általános célú titkosításra is alkalmas).
ipsec-tools	IPSEC VPN alagút kiépítését segítő eszközök.
nc	Netcat, sokoldalú IP-csomag átirányító.
nmap, nmap-front end.	Nmap portszkener és a hozzá tartozó grafikus felület.
openldap-clients, openldap-servers	OpenLDAP címtár és hitelesítési rendszer.
openssh	A legnépszerűbb szabad "Secure Shell" szerver és kliens.
openssl	Általános célú SSL/TLS titkosítási könyvtárak és eszközök.
policycoreutils, setools, setools-gui	SELinux házirend-beállító és -kezelő eszközök.
selinux-doc	Alapértelmezetten nincs telepítve, de hasznos lehet a SELinux dokumentációja.
postfix-pflogsumm	Naplóösszegző a Postfix levélküldőhöz.
spamassassin	Népszerű SPAM/UCE (kéretlen reklámlevél) szűrő.
stunnel	Általános célú SSL/TLS csomagoló (wrapper) TCP alkalmazásokhoz.
sudo, usermode	Programok rendszergazdai jogosultsággal történő futtatásának lehetővé tétele nem-rendszergazda felhasználók számára.
tcp_wrappers	Egyszerű IP alapú hozzáférés-szabályozást tesz lehetővé különböző TCP alkalmazások számára.
up2date, up2date-gnome	A Red Hat automatikus (hálózati) szoftverfrissítője.

a rendszergazda jelszavának megadását, a hálózat beállítását, egy egyszerű helyi tűzfal-házirend kialakítását, valamint a *SELinux* használatának bekapcsolását. Az első újratöltés után a telepítő további módosításokat eszközöl: beállítja a *Red Hat* hálózati előfizetést, segít létrehozni az első nem-adminisztrátori felhasználói fiókot és beállítani az *X Window* rendszert. Én személy szerint nem sokat szoktam foglalkozni a *Red Hat* telepítőprogramjának csomagkiválasztó részével. Ez a választólista ugyanis nem fedi le még a telepítőlemezen található programokat sem (nem is beszélve az internetes gyűjteményekről). Pontosabban az volt a tapasztalatom, hogy

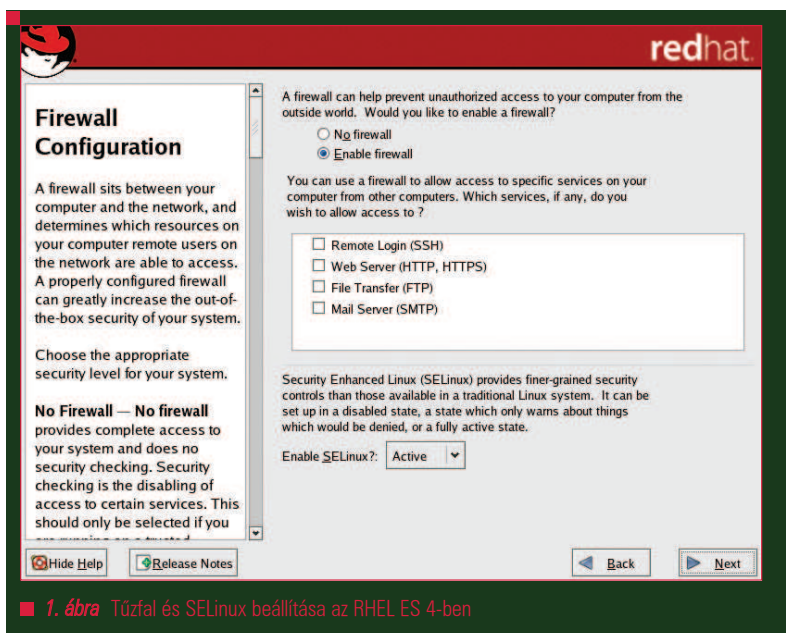
volt néhány csomag, melynek létezésében biztos voltam (például a *gnupg*), mégsem találtam őket, egyszerűen azért, mert olyan kategória alá voltak eltemetve, amelyre álomban sem gondolnék. A csomagkiválasztó által felajánlott programokra vonatkozóan sajnos nem látunk részletes leírást, és a merevlemez-igényére nézve sem kapunk információt. Ráadásul a függőség-kezelő funkciója is szándékoltan primitív. Ha a telepítő nem talál valamit, amire szüksége van, egyszerűen hibát ad; semmilyen megoldást nem kínál fel a probléma megoldásának érdekében (megadhatná a hiányzó csomag helyére vonatkozó információt, vagy felajánlhatná

a gondot okozó, függőségben álló csomagok kiválasztásának vagy ki nem választásának lehetőségét stb.) Bár az egyszerűség dicséretes erény lehet, ez a korlátozott funkcionalitás nem versenyezhet a *Debian aptitude* csomagkezelő eszközével vagy a *SUSE YaST* adminisztrációs központjával. Ha ezt a csomagkiválasztó modult a telepítés után újra használni szeretnénk, megkereshetjük a *GNOME Alkalmazások* menüpontja alatt a *Rendszerbeállításokon* belül: *Alkalmazások telepítése/törlése*. Véleményem szerint azonban sokkal inkább javunkra szolgál, ha a szoftvertelepítéseket az *up2date* segítségével, vagy éppen a jó öreg *RPM*-mel oldjuk meg.

Tehát milyen biztonsággal kapcsolatos csomagok érhetőek el az *RHEL ES 4*-ben? Az 1. Táblázat felsorolja a legtöbbjüket. Röviden, ha biztosítani akarjuk a helyi rendszert, akkor ehhez lényegében elegendő a *SELinux* használata és a helyi tűzfal-házirend beállítása. Ha más rendszerek biztonságát szeretnénk elemezni, auditálni, akkor ehhez az *RHEL ES 4*-ből szinte csak az *Nmap* programot tudjuk használni. Ez a gyűjtemény tisztességesen átfogja szinte az összes lényeges biztonsági eszközt. Néhány hiányzó programot azonban meg kell említeni:

- Jó volna valamiféle fájl-integritás (sérülésmentesség) vizsgáló, mint pl. a Tripwire vagy az AIDE.
- Ideje volna átváltani a *Syslog-NG*-re, ami egy igen hatékony rendszernaplózó, szemben a régi *syslogd*-vel, amire az *RHEL* épít.
- Kellene valamiféle virtualizációs környezet (*Felhasználói Módú Linux*, *Bochs*, *Xen* stb.).
- A mindenütt jelenlévő behatolásérzékelő és csomagnaplózó *Snort* is hiányzik.
- Webes biztonsági eszközökre is szükség lenne, mint például a *squidguard*, a *mod_security* stb.

Természetesen mindenki szabadon megteheti, hogy ezen eszközök bármelyikének forráskódját letölti és manuálisan lefordítja. De az ily módon elkészített programokat nem lehet majd az *up2date* automatikus frissítéseivel naprakészen tartani. Így tehát elmondható, hogy az *RHEL* meglehetősen prózai, mind az elérhető biztonsági csomagok, mind a programtelepítő vonatkozásában. Dicséretére legyen mondva, hogy a telepítő egy másik modulját, melyben a tűzfal és a *SELinux* állítható be, igen kedvelem (1. ábra). A tűzfal is, és a *SELinux* funkcionalitás is be van kapcsolva alapértelmezetten, és a képernyő baloldali keretében látható sűgőszöveg minden beállítási lehetőséget részletesen elmagyaráz. Ha a tisztelt felhasználónak még sohasem volt dolga *SELinux*-szal, választha-



1. ábra Tűzfal és SELinux beállítása az RHEL ES 4-ben

tó egy olyan beállítás is, mely szerint a kernel csak egy figyelmeztetést ad az olyan esetekben, amikor sérül a helyi *SELinux* házirend, de nem gátolja meg a jelzést okozó esemény futását. Alapértelmezetten azonban a *SELinux* aktív állapotban van, és érvényesít egy alapvető házirendet – ez némileg korlátok közé szorítja az *Apache (httpd)*, a *bind*, a *NIS (ypbind)*, a *dhcpcd*, a *mysqld*, az *ntpd*, a *portmap*, a *postgresql*, az *snmpd*, a *squid* és a *syslogd* működését.

Még egyet érdemes tudni a *Red Hat Enterprise Linux* telepítőjéről: sem a kezdeti beállításoknál (amikor megadható a rendszergazda jelszava), sem pedig az első nem-rendszergazda felhasználók jelszavának beállításakor nincs semmi olyan jelszóerősség-vizsgálat, mint amelyet például a *SUSE* telepítője használ, vagy amelyet – meglehetősen egyszerű szöveges ablakban – a *Debian* telepítésekor is láthatunk.

Ez elég szerencsétlen megoldás. Jelszótörő és nyers erőre építő támadások nap mint nap érnek bennünket. Örömmel láttam azonban, hogy az *XScreenSaver* képernyővédő úgy van beállítva, hogy bekapcsolásakor jelszóval zárja le az *X* munkameneteket. Már akkor is boldogabb lennék, ha csak ezektől az *XScreenSaver* által használt jelszavaktól közvetelné meg a rendszer, hogy tartalmazzon kis- és nagybetűket, középpontozást és számokat.

Automatikus frissítések up2date-tel

Rendszerünk naprakészen tartása, azaz a legfrissebb biztonsági frissítések letöltése és alkalmazása alapvető fontosságú minden *Linux* rendszerben. A *Red Hat* volt az egyik úttörő az automatikus frissítések felkínálásában, amikor néhány éve az *up2date* segédprogrammal együtt bevezette a *Red Hat* hálózati szolgáltatásokat; ez a rendszer egyre kiforrottabban működik.

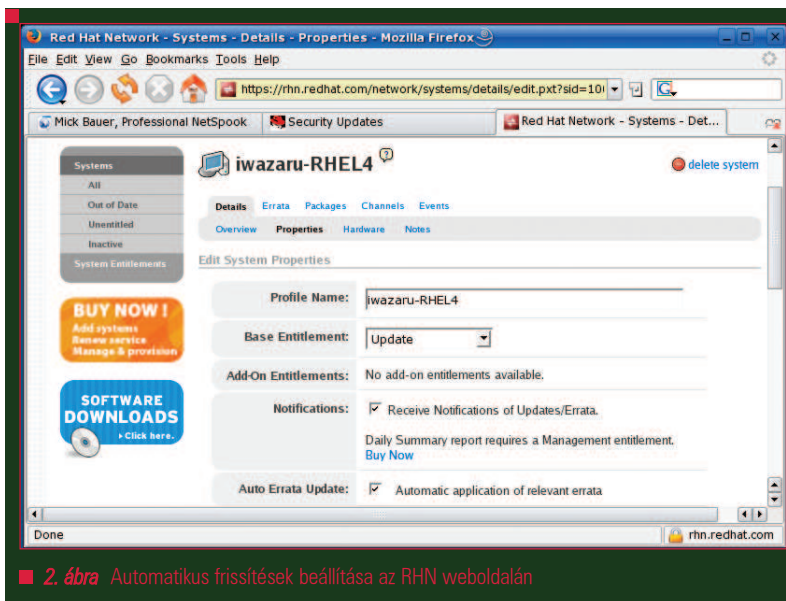
Működésének módja, hogy minden frissen feltelepített *Red Hat* rendszer első újratöltése után felajánlja a lehetőséget a *Red Hat* hálózati szolgáltatások beállítására. Minden *Red Hat* termék magában foglalja az „*RHN (N = Network, hálózati) frissítési felhatalmazásra*” való előfizetést. Amikor kéri a rendszer, be lehet írni egy felhasználónevet és jelszót, amelyet használni szeretnénk a későbbiekben, valamint egy előfizetői számot, amely a telepítési médiummal érkező „aktiválja előfizetését” kártyára van nyomtatva. Ugyanaz a felhasználói fiók használható egyegy előfizetéshez tartozó több rendszer kezelésére.

Míndezek „mellékhatásaként” tehát lesz egy aktív előfizetésünk a *Red Hat* hálózati szolgáltatásokra, ezen belül egy rendszerprofilunk, amely megfelel az aktuális *Red Hat* rendszerünknek; valamint egy *RHN* frissítési felhatalmazásunk, amely révén rend-

szerünk automatikusan ellenőrizheti és letöltheti a megvásárolt *RHEL* verzióhoz tartozó szoftvercsomagok legfrissebb változatait.

A biztonsági frissítések ellenőrzésének és alkalmazásának legegyszerűbb módja, ha a *GNOME* asztalon levő „Red Hat hálózati riasztások” ikonra mért jobb egérgattintással kiválasztjuk a „Frissítések ellenőrzése”-t, majd lefuttatjuk az *up2date*-et, ha szükséges. Az említett ikon sugárzó piros felkiáltójelet tartalmaz, amennyiben a rendszer nem naprakész – ellenkező esetben kék pipa jelzi a friss rendszerállapotot.

Automatizálni is lehet a frissítéseket: a megfelelő *RHN* igazolvánnyal bejelentkezve a Red Hat weboldalra (www.redhat.com/en_us/USA/rhn az amerikai felhasználók számára) a „Systems” („Rendszerek”) fülre kattintva kiválasztható a saját rendszerprofilunk. A „Properties” („Tulajdonságok”) menüpontban kattintsunk az automatikus hibajavítás melletti jelölőnégyzetre (2. ábra). Ilyen frissítési módra nyilván semmi szükség magas rendelkezésre állású vagy változásvezérelt rendszerek esetén, hiszen a szoftverfrissítések mindig hozhatnak újabb hibákat vagy ütközéseket. Az *up2date/RHN* páros érett és sok lehetőséget kínáló megoldás, különösen nagy szervezeteknél, melyek részéről megvan az igény és a fizetőképesség a számítógép-hálózat ilyen módon történő kezelésére és naprakészen tartására. Egyszerű *Linux* felhasználóként azonban számomra ez bonyolultabb, mint a *Debian apt* programrendszere (amely talán bizonyos tekintetben spártaibb, de sokkal egyszerűbb szkripteket írni hozzá), sőt a *SUSE YOU* („Yast Online Update”) frissítőjénél is komplikáltabb (ezt sokkal egyszerűbb konfigurálni). Furcsamód úgy tűnik, hogy (az *RHEL* sok más összetevőjéhez hasonlóan) az *up2date* opcióinak beállításához több grafikus felületet is végig kell nézni (beleértve a Red Hat weboldalát) – ha csak nem parancssorból állunk neki a beállításnak (ezen esetben ugyanis elegendő csak a */etc/sysconfig* szerkesztése). Ha a beállítandó Red Hat rendszerünk egy szerver (amin, megfelelő szigorúságú házirend esetén talán nincs is telepítve az *X Window* rendszer), vagy egyszerűen sze-



2. ábra Automatikusan frissítések beállítása az RHN weboldalon

reti valaki a parancssort, akkor biztos vagyok abban, hogy az *up2date* és a többi Red Hat funkcionalitás megtanulása nem okoz komolyabb nehézséget. Ironikusan úgy fogalmazhatnék, hogy az *RHEL* adminisztrációjának grafikus felületei (amelyek elvileg azért születtek, hogy egyszerűbbé tegyék a felhasználók dolgát) inkább összezavarnak. De az is lehet, hogy ez csak számomra van így.

SELinux a Red Hat Enterprise Linuxon

Amint láthattuk, az *RHEL* az operációs rendszer biztonságát illetően igen erősen támaszkodik a *SELinuxra*. Ez aligha mondható hanyagságból vagy szellemi tunyaságból eredő döntésnek; a *SELinux* átfogó és aprólékosan beállítható hozzáférés-szabályozási rendszert biztosít a rendszer felhasználói, az alkalmazások, a folyamatok és a fájlok számára. Ahogy már említettem az előzőekben, az alapértelmezett *SELinux* házirend szabályozza a leggyakrabban használt alkalmazásokat, azok hozzáférési jogosultságait. Ez az alapértelmezett házirend megváltoztatható a *GNOME* „Alkalmazások/ Rendszerbeállítások/ Biztonsági szint” menüpontjával (3. ábra); itt egyúttal megadható egy egyszerű helyi tűzfal-házirend is. Az *RHEL ES 4* által megvalósított *SELinux* jó szívvel ajánlható az egyszerűsége miatt; nem is beszélve arról

a fontos tényről, hogy már alapértelmezetten be van kapcsolva. Ez a jó hír. A rossz pedig az, hogy egy egyéni *SELinux* házirend létrehozásához (amely bővíti vagy szűkíti az alapértelmezett megszorításokat, vagy amely más alkalmazásokat is meghív) szükséges némi dokumentáció-olvasgatás. A legcélszerűbb a „Red Hat Enterprise Linux 4 Red Hat SELinux Bevezető”-vel kezdeni, ami a www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/selinux-guide címen érhető el (angolul).

Valószínűleg szükség lesz még néhány egyéb grafikus eszközre is, nevezetesen a *setools* és a *setools-gui* csomagokra. Ezekben a csomagokban találhatóak például a *sepcut*, az *apol*, a *seaudit* és a *seuserx* programok, melyek használatára vonatkozóan lásd a */usr/share/doc/setools-1.5.1* könyvtárbeli dokumentációt (természetesen a névbeli számok tükrözhetnek más verziót is).

RHEL Tűzfal beállítása

Említettem az imént a *GNOME* „Alkalmazások/ Rendszerbeállítások/ Biztonsági szint” segédprogramot. A *SELinuxszal* ellentétben ez a program nem ad lényegesen több lehetőséget a helyi tűzfal konfigurálásához annál, mint amire már a telepítéskor lehetőség nyílt. Ez a házirend engedélyez minden olyan hálózati műveletet, ami „kifelé” irányul, azaz a helyi rendszerből ered, és letilt minden „be-

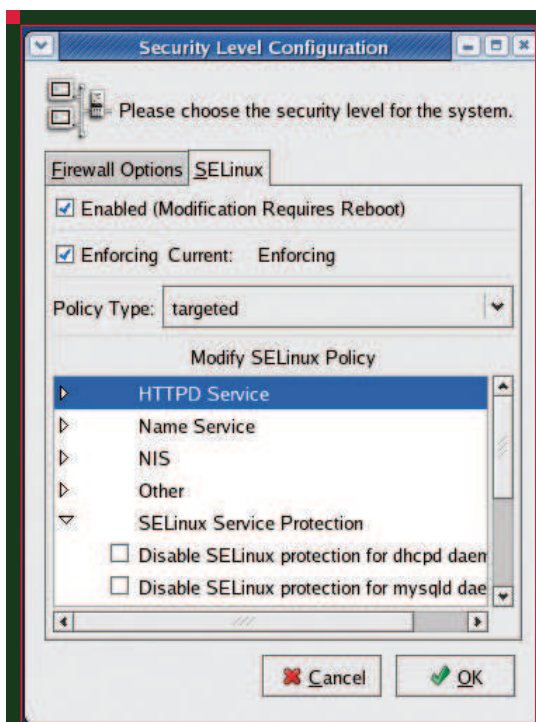
felé” jövőt (ami a helyi rendszert célozná meg), kivéve az ezek közül kiválasztottakat: *Red Hat telepítő, HTTP, FTP, Telnet, mail (SMTP)* és *SSH*. A „Biztonsági szint” segédprogrammal megadható néhány port és protokoll is, mégpedig [port #]: [protokoll] formában, például *689:tcp, 53:udp, 53:tcp*. Ha ezeknél egzotikusabb beállításokra van szükség, akkor a kívánt *iptables* parancsokat manuálisan kell megírni. Szerencsére ez egyszerűen megtehető a */etc/sysconfig/iptables* fájl szerkesztésével (vagy újabb sorok beszúrásával). További információk az *iptables* kézikönyv (*man*) oldalain és a *Red Hat Enterprise Linux* biztonsági útmutatójában (*Security Guide*) találhatóak.

Címtárszolgáltatások, Nyilvános Kulcsú Infrastruktúra (PKI)

Említést érdemel, hogy a *Red Hat* nemrégiben megvásárolta a *Netscape Címtárkiszolgálót (Netscape Directory Server)*, majd átdolgozta és átnevezte *Red Hat Directory Server* névre; ezzel az *OpenLDAP* és a *Sun* által kiadott „*Java System Directory Server*” kereskedelmileg támogatott alternatívája kíván lenni. Bár ez nem része az *RHEL*-nek (külön vásárolható meg hozzá), jó tudni arról, hogy ez a *Red Hat* biztonsági koncepciójának kulcsfontosságú összetevője. Az *RHEL* egyébként teljes mértékben támogatott *OpenLDAP* csomagokat is tartalmaz. Ugyanebben a csapásirányban haladva – szintén ráadásaként megvásárolható módon – a *Red Hat Hitelesítési Rendszer (Red Hat Certificate System)* kereskedelmileg támogatott *PKI* megoldást is biztosít. Az *OpenSSL* természetesen része az *RHEL*-nek, de minden egyéb konfigurációs eszköz (mint amilyen például a *TinyCA*) nélkül.

Zárszó

Vegyes érzelmeket váltottak ki bennem a *Red Hat Enterprise ES 4*-ben található biztonsági összetevők. Egyrészt jóval kevesebb biztonságot



3. ábra A biztonsági szint beállítását lehetővé tevő alkalmazás

erősítő szoftveres eszköz található az *RHEL*-ben, mint a *Debian GNU/Linuxban* vagy a *SUSE Linuxban*. A biztonsági eszközök (más, nagyobb disztribúciókban bőségesen képviselt) teljes kategóriái hiányoznak: fájlok épségét vizsgáló alkalmazások, behatolásérzékelők, virtualizációs környezetek stb. Másrészt a *Red Hat* teljes disztribúciója szelvében-hosszában példátlan ellenőrzési szintet hozott létre. Nehéz döntéseket hozott meg a támogatandó és karbantartandó, illetve az elhagyandó programokat illetően; ez erőteljesen lecsökkenti a *Red Hat* rendszerek támadási felületét. Semmi kétség, a napvilágra jutó sebezhetőségek kijavítására a *Red Hat* biztonsági csapata számára egyszerűbb tartani a rövid válaszidőt az *RHEL 1730* csomagját illetően, mint a *Debian* biztonsági csapat számára, mely disztribúciójának 15000 feletti csomagjéért felelős. Azzal, hogy az *RHEL 4*-be felvette a *SELinuxot*, sőt használatát alapértelmezettnek tekinti, a *Red Hat* igen merész lépést tett. A *SELinux* által biztosított kernelszintű kötelező hozzáférés-szabályozás nagymértékben hozzájárul az olyan biztonsági rések csökkentéséhez, amelyeket a különbö-

ző hozzáadott alkalmazások célba vennének. Ezen kívül azzal, hogy ez a védekező technológia a nem kívánt működés megelőzését szolgálja, már önmagában sokkal erősebb, mint bármiféle behatolásérzékelő, fájl-integritás ellenőrző és egyéb *utólagos* „lyukfoltozó” technológiák; bár igazán megtehetné a *Red Hat*, hogy mindkettőt használja (az előrettekintő eszközöket és a visszatekintő méréseket is), hiszen a *SELinux* sem kikezdehetetlen.

A tisztelt Olvasó *Linuxra* irányuló igényeitől függően tekinthető az *RHEL* erősnek és lényegre törőnek, avagy korlátoznak és esetlennek. A magam részéről bizonyos okokból nem rajongok annyira az *RHEL*-ért, mint amilyen szívesen használok a *Debian* és a *SUSE Linuxot* a munkámhoz: biztonsági szakértő és tanácsadó vagyok. Többnyire olyan eszközöket használlok, melyek nagy részét az

RHEL feleslegesnek ítélte a megcélzott piac (feltehetően a vállalati *IT* szakértők) számára. Ezzel együtt úgy vélem, hogy ha egy *RHEL* alatt futtatott webszervert kellene biztonságossá tennem (*SELinuxszal* vagy anélkül), akkor manuálisan telepíteném a *mod_security*, a *Squidguard*, a *Syslog-NG* programokat és más olyan eszközöket is, melyeket az *RHEL* jelenleg nem tartalmaz.

Linux Journal 2006., 146. szám



Mick Bauer
(darth.elmo@wiremonkeys.org)
az Egyesült Államok egyik legnagyobb bankhálózatában felelős a hálózati biztonságért. Ő a szerzője az O'Reilly által kiadott *Linux szerverek biztonsága, Linux Server Security* c. mű második kiadásának. (Korábban a *Biztonságos szerverek építése Linuxon, Building Secure Servers With Linux* címet viselte a könyv.) Időnként előad információ-biztonsági konferenciákon. Ő a szerzője a „Hálózatmérnöki Polkának” („*Network Engineering Polka*”).