nordtech

RedHat Enterprise Linux 4 turvavahendid

Lauri Jesmin
lauri.jesmin@nordtech.ee
OÜ Nordtech

nordtech

RHEL

- RHEL on RedHat Enterprise Linux
- Müüakse teenust, mitte tarkvara
- Saadaval on korraga kõik aktiivselt toetatud versioonid, praegu on need 2.1, 3 ja 4
- Peamisteks eelisteks pikk eluiga (7a) ja lai toetus erinevate tootjate poolt

nordtech

Kaitsevahendid

- ExecShield ja PIE
- Glibc ja kompilaatorite täiendused
- SELinux
- Auditeerimisvahendid
- RedHat Network

nordtech

ExecShield

- NX/XD bitt moodsates protsessorites
- Eraldatud andme/programmisegmendid
- PIE võimaluste kasutamine: ASCII Zone ja Address Space Randomization

nordtech

ExecShield

- Tulemused: 1. nov. 2003 kuni 11. august 2004 tuvastatud 16 RHEL turvaprobleemist peatatakse ExecShieldi vahenditega 12, ehk 75%

nordtech

Glibc ja kompilaatori täiendused

- Kasutakse parandatud glibc sisest veakontrolli mälukasutuse osas
- Printf funktsioonide korrektsuse kontroll
- Puhvrite suuruse kontroll

nordtech

Glibc ja kompilaatori täiendused

- Need vahendid täiendavad ExecShieldi
- Kompilaatori täiendused toimivad vaid vastavalt täiendatud programmidel
- Täiendatud glibc veakontroll toob esile seni varjatud vigu

nordtech

SELinux

- Arendatud NSA toel, sarnaseid omadusi on teistel „*trusted*“ süsteemidel
- Rakendustele antakse vähimad vajalikud õigused, õigused on lisaks tavalistele unixi õigustele
- „*Targeted Policy*“ suunatud konkreetsete deemonite turvamisele

nordtech

SELinux

- Mahukas ja uus vahend
- Täiendavat infot leiab RedHati dokumentatsionist (SELinux guide) ja RedHat Magazine arhiivist

nordtech

Auditeerimisvahendid

- RHEL 4 sisaldab auditeerimisvahendit „audit“
- Võimaldab *syscall*-ide auditeerimist ning omab ka vahendeid raportite koostamiseks

nordtech

RedHat Network

- RedHat Network on RedHati vahend uuenduste ja paranduste levitamiseks
- Vajab toimimiseks võimalust ühenduda RHN serveritega. Võimalik kasutada ka oma võrgus asuvaid Satellite või Proxy servereid
- Võimaldab servereid grupeerida, haldamist delegeerida, teavitusi jpm.

nordtech

Viiteid

- RedHati manuaalid:
  http://www.redhat.com/docs/manuals/enterprise/
- RedHat artiklid ja *whitepaper*id
  http://www.europe.redhat.com/solutions/info/
- RedHat Magazine
  http://www.redhat.com/magazine