Eesti Infotehnoloogia Kolledž

Kasutajate haldamine

Linux (UNIX) algajale

Edmund Laugasson
edmund.laugasson@itcollege.ee

Ohud

- igapäevane kasutamine tavakasutajana
  - isegi kui olete ise arvuti omanik
  - ka pahavaral on samad õigused kasutajaga
  - süsteemikahjustuste vältimine (kogemata kustutamine, võimalik pahavara)
- kas olete mõnel tuttaval arvutit pahavarast puhastanud?
- kas sooviksite seda tööd ka tulevikus teha?

http://www.bordercomputers.co.uk/wp-content/uploads/2013/12/computer-virus-removal.jpg

Ohud 2

- saladuste hoidmine
  - kui selgub, et üks töötaja polnud lojaalne
  - müüs firma saladused maha
  - kas on täpselt teada, mis infole tal ligipääs oli?
- minimaalsed vajalikud õigused
  - on tüütud
  - on hädavajalikud

http://1.bp.blogspot.com/-2vKcQeDIoOM/T-i5Tx-N04I/AAAAAAAAFXE/QjS2sW9HtPA/s1600/Permissions-Reset-Icon.png

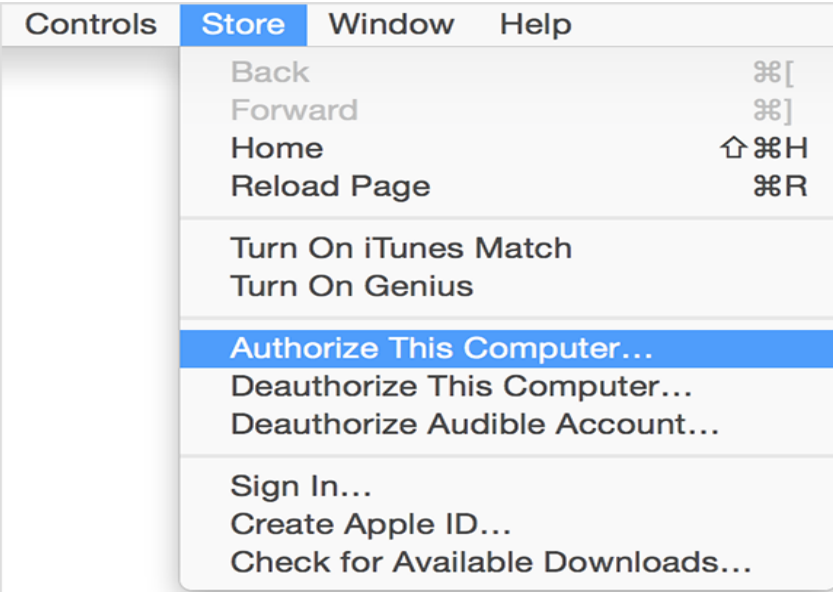
Kasutajate haldamine

- Muudatused infosüsteemis peavad jätma oma jälje
  - Kes muutis
  - Mis ajal muutis
  - Inimesed tuleb tuvastada
- Infosüsteemi andmete muutmist võivad teostada vaid volitatud isikud
  - Kasutaja õiguseid on vaja kontrollida ja reguleerida ehk rakendada pääsukontrolli

Autentimine ja autoriseerimine

- isikutuvastus e autentimine (*authentication*)
- autoriseerimine – pääsukontrolli rakendamine (*authorization*)

http://docs.oracle.com/javaee/5/tutorial/doc/figures/security-httpBasicAuthentication.gif



https://support.apple.com/library/content/dam/edam/applecare/images/en_US/mac_apps/itunes/yosemite-itunes12_store-authorize_this_computer.png

Kasutaja

- Infosüsteemi sisenev kasutaja tuvastatakse
- Kasutajale tagatakse pääs vaid neile ressurssidele, mis on tema rollile lubatud ehk kasutaja autoriseeritakse
- Infosüsteemi kasutamist ja väärkasutamist jälgitakse ehk auditeeritakse

Isikutuvastus (*authentication*)

- Kasutatakse
  - Midagi, mida kasutaja teab – salafraas (vt järgmine slaid), PIN
  - Midagi, mida kasutaja omab – kiipkaart, magnetkaart
  - Midagi, mis on kasutaja osa:) – sõrmejälg ja muud biomeetrilised vahendid

Väljakutse:
* leida turvaline paroolihaldur
  - erinevate OS'ide tugi
  - oma krüpto kasutamise võimalus
  - 2-faktoriline isikutuvastus
  - *zero access, zero knowledge*

https://everykey.com/
https://everykey.com/security/
https://www.themooltipass.com/

https://upload.wikimedia.org/wikipedia/commons/thumb/8/8f/SecureID_token_new.JPG/220px-SecureID_token_new.JPG

Salasõna -> salafraas

- Kasutaja salafraasile võib (peab) esitama nõudeid
  - peab olema raskesti äraarvatav, kuid soovitatavalt kergesti meelde jäetav – näiteks kokkukirjutatud lause, sh numbrid ja erisümbolid kuid eesti täpitähti ei soovita kasutada
  - pikkus peab olema vähemalt 8 märki, soovitavalt 20 ja rohkem (kuni 15-kohalised MS Windowsi salasõnad on murtavad alla poole tunni) – see kõik muutub arvutusvõimsuse kasvades (NB! kvantarvutid!)
  - ei tohi sisaldada sõnastikus leiduvaid sõnu
  - peab sisaldama suur ja väiketähti ning numbreid ja soovitatavalt erimärke
- salasõna ei tohi teistega jagada (kaasneb ka halduse vastutus!)
- salasõnale tuleb eelistada salafraasi, kiipkaarti, biomeetrikat vms
- võimalusel kasutada mitmeastmelist autentimist
- https://howsecureismypassword.net/ - tasub aeg-ajalt kontrollida olemasolevate salafraaside arvutuskiirust
- https://haveibeenpwned.com/ - mis on juhtunud...

Kasutaja infosüsteemis

- Uue kasutaja puhul
  - Kasutaja lisatakse vastavatesse gruppidesse või rolli
  - Kasutajale antakse identifitseerimiseks parool või kiipkaart
- Kasutaja muudab firma sees oma rolli
  - Kasutaja eemaldatakse olemasolevatest gruppidest/rollist
  - Kasutaja lisatakse uude gruppi/rolli

Kasutaja lahkub firmast

- Kasutaja lahkumisel
  - Võetakse kasutajalt ligipääs infosüsteemi ressurssidele
  - Arhiveeritakse kasutaja loodud andmed ja e-mail postkast
  - Suunatakse kasutaja e-post teise postkasti
  - Eemaldatakse kasutaja andmed süsteemist

Protsessid

- Firmas peab olema kirjalik protsess kasutajaõiguste saamiseks, muutmiseks ja kustutamiseks
- Asjad ei käi nii, et süsteemiadministraator valib ise õiguste nimekirja, mis uuele kasutajale lubatakse
- Firmas peab olema ülevaade kasutajate ja rollide õigustest

Kasutajate rollid

- kasutajad kuuluvad rollidesse, nt
  - insener
  - tootearendaja
  - administraator
  - jne
- rolle realiseeritakse sageli gruppidega
  - grupp insenerid
  - jne
- Igal rollil on omad juurdepääsureeglid infosüsteemi ressurssidele

Kasutaja ID

- Igal kasutajal on infosüsteemis oma ID
  - UNIXilaadsetes (sh Linuxis) UID – user ID
    - Näiteks 500
    - UID = 0 -> Juurkasutaja
  - Windows süsteemides SID Security Identifier
    - Näiteks S-1-5-21-domeeni_id-500
    - http://support.microsoft.com/kb/243330

Kasutaja andmed

- Linux laadsetes süsteemides hoitakse kasutaja kohta järgnevaid andmeid
  - kasutajanimi
  - salasõna (*password*) ja selle räsi (*hash*)
  - UID (User ID), GID (Group ID)
  - kasutaja kodukataloog (*/home/kasutaja*)
  - kasutaja *shell* (vaikimisi kasutatav *shell*)
  - parooli ja kasutaja aegumise andmed

Kasutajate andmed hoitakse

- Kasutajate ja gruppide andmed hoitakse kataloogides
- UNIXilaadsetes (sh Linuxis, Mac OS'is)
  - */etc/passwd* hoitakse kasutajad
    kasutaja:x:UID:GID:nimi,,tel1,tel2:/home/kodu:/bin/bash
    http://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/
  - */etc/shadow* – hoitakse salasõna räsi (*hash*) ja konto/salasõna aegumise andmeid jne, pole kõigile loetav – miks?
    http://www.cyberciti.biz/faq/understanding-etcshadow-file/
  - */etc/group* grupid
    http://www.cyberciti.biz/faq/understanding-etcgroup-file/
- AD *Active Directory*
  - Microsoft Windows süsteemides
  - ka UNIXilaadsed (sh Linux) suudavad kasutada (autentida)
- Mitme serveriga süsteemid
  - (Open)LDAP kataloogiteenus

Grupid (Rühmad)

- Kasutajal on primaarne grupp (Ubuntus sama nimega kui kasutaja) ja sekundaarsed grupid
  - Linuxis vaata käsuga *id* hetkel sisseloginud kasutaja kohta
- Näiteks võib kasutaja primaarne grupp olla users ja sekundaarsed grupid, audio, video jne
- grupikuuluvusega reguleeritakse ka ligipääsu seadmetele, kataloogidele jne
- /etc/group
- Igal grupil on oma ID ehk GID

Keskne kasutajate baas

- Suurfirmades on palju servereid
  - mitmed Unix serverid
  - mitmed Windows serverid
  - palju tööjaamu
- Probleem: kasutaja oleks vaja hoida ühes süsteemis
- Lahendus: LDAP kataloog
  - AD kujul
  - LDAP+Kerberos kujul
- juurutada on vaja neid rakendusi, mis toetavad keskset kasutajate baasi
- kui on vaja mitut kataloogi kasutajate andmete hoidmiseks, siis proovida nendevahelist sünkroniseerimist automatiseerida

Eetikast

- Süsteemiadminstraatoritel on tihti juurdepääs paljudele asjadele;
- Teil on kasutajate usaldus ja suur vastutus;
- Austage ja kaitske kasutaja privaatsust;
  - Krüpteerimata varukoopiaid võib tihti leida kõige kummalisematest kohtadest;
- See (eetika) on midagi, mida siin loengus selgeks ei saa.

Kasutajate lisamine (Linux)

- **adduser** [options] [--home DIR] [--shell|-s SHELL] [--no-create-home] [--uid ID] [--firs-tuid ID] [--lastuid ID] [--ingroup GROUP | --gid ID] [--disabled-password] [--disabled-login] [--gecos GECOS] [--add_extra_groups] **kasutajanimi**
- on olemas ka *useradd* ent ei soovita seda kasutada (vt *man useradd*)
- kasutajaprofiil võetakse */etc/skel/* - seda kujundades on võimalik uusi kasutajaid luua soovitud seadistustega.
- **Näide**
  - **adduser testkasutaja**

    https://wiki.itcollege.ee/index.php/Adduser_%26_useradd
  - http://askubuntu.com/questions/345974/what-is-the-difference-between-adduser-and-useradd

Kasutajate haldus (Linux)

- Kasutaja salasõna muutmine: **man passwd**
  - administraator muudab teiste kasutajate salasõnu:
    - **passwd [kasutaja]**
  - (hetkel sisseloginud) kasutaja muudab oma salasõna:
    - **passwd**
- Kasutaja kustutamine: **man userdel**
  - **userdel [options] kasutaja**
  - **userdel -r student –** kustutab kasutaja *student* ja tema kodukataloogi
  - kasutaja/salasõna lukustamiseks: **passwd -l kasutaja**

Kasutajate haldus (Linux) 2

- usermod [options] **kasutaja**
  - **-u UID**
  - **-g GID**
  - **-G gruppA,gruppB**
  - **-L lukustab kasutaja parooli**
  - **-U lubab kasutaja parooli**
  - **-p parool**
  - **-s shell**
  - **-l uus kasutajanimi**
  - **-c kommentaar**
  - saab muuta ka aegumist
  - vt **man usermod**

Kasutajate haldus (Linux) 3

- Paneme kasutaja lukku
  - **usermod -L <kasutaja>**
  - **usermod -L *student***
- keelame salasõna muutmise
  - **passwd -l student**
- Teeme kasutaja *student* lukust lahti
  - **usermod -U student**
- lubame salasõna muutmise:
  - **passwd -u student**

Grupid (Linux)

- Grupi lisamine: **man addgroup**
  - **addgroup** [options] [--gid ID] **grupp**
- Kasutaja lisamine gruppi: **man adduser**
  - **adduser <kasutaja> <grupp>**
  - Näiteks järgmine korraldus lisab kasutaja *student1* gruppi *students*
    - **adduser student1 students**

Info kasutaja kohta

- Kasutaja kohta saab infot korraldusega **id** (vt **man id**)

  id *<kasutajanimi>*

- Kuhu gruppi kasutaja kuulub
  groups *<kasutajanimi>*

  getent group *<kasutajanimi>*

- *man groups*
- *man getent*

Info kasutajate ja gruppide kohta

- Kasutajate nimekirja kuvamine
  getent passwd
- Gruppide nimekirja kuvamine

  getent group
- Kes on hetkel masinasse sisse loginud ja mida teeb: **w**
  (lisainfo *man w*)

Viiteid

- Kerberos protokolli lahtiseletus
  http://learn-networking.com/network-security/how-kerberos-authentication-works
- OpenLDAP seadistamise näide
  http://wiki.itcollege.ee/index.php/OpenLDAP-i_seadistamine
- Kes on arvutisse loginud ja mida teeb:
  https://wiki.itcollege.ee/index.php/K%C3%A4sklus_w
- OSadmin kasutajate haldamise spikker
  https://wiki.itcollege.ee/index.php/Osadmin_spikker#2._KASUTAJATE_HALDAMINE

Küsimused?

Tänan tähelepanu eest!