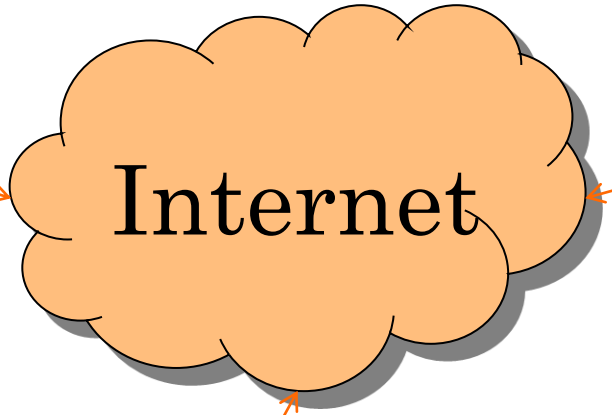
Tietoturva

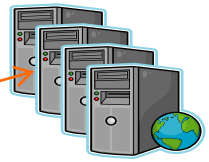
Miten suojaudun haittaohjelmilta

Tietoverkon rakenne

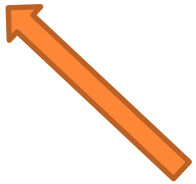
Koti

Reititin
tai
modeemi





Palvelimet
- Pankki
- S-posti
- Lehdet
- Tv / elokuvat
- Sosiaaliset mediat
- Ym.



Roisto

Pari hyökkäyksestä

- DOS = Denial Of Cervice = palvelunesto
  - Monta kaapattua tietokonetta muodostaa ISON ryhmän
  - Kaappaaja kontrolloi ryhmää ja voi kohdistaa hyökkäyksen yhteen palvelimeen
    - Palvelin ylikuormittuu eikä kykene palvelemaan
- Tietojen kaappaus
  - Tietokoneen ja palvelimen (esim. Pankki) välinen yhteys kaapataan
  - Kaappaaja voi kontrolloida liikennettä
  - TK => kaappaaja => pankki => kaappaaja => TK
  - Tili tyhjenee muiden sitä huomaamatta

Tietoturva tarkoittaa, että …

- Tieto on
  - Saatavilla tarvittaessa
  - Ajan tasalla
  - Totuudenmukaista
  - Palautettavissa esim. kiintolevyrikon sattuessa
  - Suojassa tietomurroilta
  - Suojassa haittaohjelmilta
- Tietoväline on
  - Suojassa varkauksilta
  - Suojassa vahingoilta
    - Tulipalo
    - Luonnon katastrofit

Yleissäännöt 1/2

- Haittaohjelmilta voi suojautua
  - Pitämällä ohjelmat ajan tasalla päivittämällä ne uusimpaan versioon
  - Lataamalla aina virusten torjuntaohjelman päivitykset
  - Ei avaa sähköpostissa tuntemattomilta tulevia viestejä eikä varsinkaan liitetiedostoja
    - Vain avattu liite tai linkki voi saastuttaa koneen
  - Myös virallisilta vaikuttavat (esimerkiksi pankit) viestit ja linkit ovat vaarallisia
    - Esim. pankit eivät koskaan lähetä linkkejä tai kehota paljastamaan tunnuslukuja
  - Varmistamalla, että salasana on käytössä ja riittävän hyvä
    - Tarkasta salasanan suojaavuus täältä

Yleissäännöt 2/2

- Haittaohjelmilta voi suojautua (jatkoa…)
  - Ei käynnistä tuntemattomista lähteistä saatuja ohjelmia
    - Skannaa AINA tiedostot ajan tasalla olevalla viruskanneriohjelmalla ennen käynnistämistä
  - Ei avaa kuvatiedostoja (myös tunnetuista lähteistä varauksin)
    - Skannaa AINA tiedostot ajan tasalla olevalla viruskanneriohjelmalla ennen avaamista
  - Käyttämällä virtuaalikonetta epäselvissä tapauksissa
    - Avaa epäilyttävän internetsivun
    - Asentaa ohjelman, joka voi olla saastunut
    - Avaa epäilyttävät tiedostot (kuvat, tekstit yms)
  - Ottamalla käyttöön useita käyttäjätunnuksia: useita peruskäyttöä varten ja yksi asennuksia varten
    - Jokaisella käyttäjällä olisi hyvä olla oma tunnuksensa ja salasanansa
    - Varsinainen käyttö vain peruskäyttötunnuksilla

Viruskannerit

- Käy läpi systeemin tiedostot ja parhaat jopa kiintolevyn käynnistysalueet
- Tarjolla lukemattomia hyviä ohjelmia
  - F-Secure
  - Symantec (Norton)
  - Avira
  - Panda
  - Microsoft Security Essentials
- Pilvessä toimiva ratkaisu on parhaiten ajan tasalla
  - Käytettävissä aina ajan tasalla oleva kuvaustiedosto
  - Ei toimi, jos ei yhteyttä Internetiin – eikä tarvitse!
  - Vain muutamalla (maksullisella) toimiva ratkaisu
- Jotkut skannerit käynnistettävä erilliseltä CD:ltä
  - Vaikeat tapaukset

Palomuurit

- Estää ei-toivotut yhteydenotot tietokoneeseen
- Nykyisin mukana jo käyttöjärjestelmässä
  - Esim. Microsoft Windows
- Mukana suurimmassa osassa maksullisia turvaohjelmistoja
  - Ei tarvetta, koska jo olemassa oleva on täysin riittävä
- Tarjolla myös erillisiä laitteita
  - Yleensä firmoille tarkoitettuja
  - Jos ”nurkissa pyörii” vanha laite, voi sen ottaa käyttöön palomuuriksi (Linux –pohjainen ohjelma)

Virtuaalikoneet

- Virtuaalikone toimii eräänlaisena ”koneena koneen sisällä” ja käyttää isäntäkoneen resursseja (levy, verkko, näyttö, hiiri, oheislaitteet)
- Eristää käyttöjärjestelmät toisistaan
  - Virusten torjuntaohjelmisto on asennettava myös virtuaalikoneeseen, vaikka sellainen olisi jo isäntäkoneessa
  - Käyttöjärjestelmä voi olla mikä tahansa, mikä on tuettu
- Helposti siirrettävissä toiseen koneeseen
- Helppo ottaa varmuuskopio (= monistaa alkuperäinen asennus)

Virtuaalikoneet (jatkoa …)

- Tarjolla
  - VMWare
    - Pisimpään markkinoilla
    - Tuote sekä jo olemassa olevan käyttöjärjestelmän muuttamiseen virtuaaliseksi että virtuaalikoneen käyttämiseen
    - Myös valmiita järjestelmiä (suuri osa maksullisia)
  - VirtualBox
    - Oraclen tuote
  - VirtualPC
    - Microsoftin tuote
- Kaikki ilmaisia
- Automaattinen varmuuskopiointi

Salasanat

- Salasanan on oltava
  - Tarpeeksi pitkä
    - Vähintään 6 merkkiä
  - Merkit sellaisia, että järjestelmä ei sekoa
    - Ei skandeja, erikoismerkkejä, välilyöntejä
    - Isot ja pienet kirjaimet, alaviiva, numerot sallittuja
  - Ei lemmikkien, lasten tai puolison nimeä
  - Ei osoitetta, syntymäpäiviä tms.
  - Ei löydettävissä suoraan sanakirjasta
- Oivallinen rakenne on salasana, joka on helppo muistaa, mutta sekaisin
  - Esim. sininen => 5in1heh
- Oheisista linkeistä neuvoja
  - Problematiikka
  - Salasanageneraattori
- Salasanoja voi säilyttää Password safe –ohjelmalla

Muut turvallisuustekijät

- Tietokoneen on oltava turvallisessa tilassa varkauksien varalta
  - Autossa ei näkyvillä
  - Kahvilassa ei poissa valvovan silmän ulottuvilta
- Varmistuksien oltava kunnossa ja ajan tasalla
  - Tärkeän tiedon olisi hyvä olla monessa paikassa oman koneen kiintolevyn lisäksi
    - CD (CD-R tai CD-RW)
    - Muistitikku
    - Pilvi (Dropbox, Sugarsync)
    - Toinen tietokone
    - Verkkokiintolevy
  - Varmistusohjelmia saatavilla ilmaiseksi Internetistä
    - Helpointa varmistaa automaattisesti ulkoiselle tietovälineelle (esim. verkkokiintolevy tai muistitikku)

Muut turvallisuustekijät (jatkoa …)

- Pilvipalveluita on käytössä yllättävän paljon
  - Ilmainen sähköposti
    - Ei arkaluontoisia viestejä, salasanoja, käyttäjätunnuksia
  - YouTube, Facebook, LinkedIn, Dropbox, SugarSync, Verkkoposti …
  - Pilvessä tieto on toisilla palvelimilla muissa maissa
- Internettiin viety tieto on pysyvästi julkista
  - Harkittava tarkkaan, mitä tietoa antaa
    - Laki, moraali, henkilöiden suoja
  - Poistaminen mahdotonta