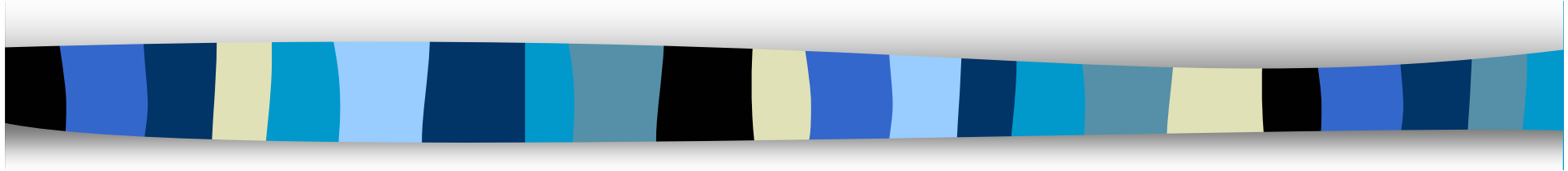


# Diplomityöseminaari



8.12.2005

Teknillinen Korkeakoulu



**Työn otsikko:** *Tekninen tiedonhankinta ja yrityksen tietojen turvaaminen*

**Tekijä:** Pekka Rissanen

**Valvoja:** Prof Sven-Gustav Häggman

**Ohjaaja:** DI Ilkka Nyman



# Sisältö

- Työn perusteet
- Ongelmanasettelu
- Tutkimusmenetelmät
- Lopputulokset
- Yhteenveto ja Johtopäätökset
- Jatkotutkimusaiheita



# Työn perusteet

- Yritysvakoilun aiheuttamat taloudelliset tappiot ovat huomattavat
- Suojattavaan yritystietoon kohdistuu lukuisia teknisiä uhkia
- Tekijänä voi olla yksittäinen henkilö, kilpaileva yritys tai valtiollinen toimija
- Vastaavaa systemaattista tarkastelua ei ole aiemmin tehty



# Ongelmanasettelu

- Selvittää ja esittää ne yritysvalvontaan tekniset tiedonhankintakeinot, jotka yritysten on tiedostettava.
- Esittää ne tavat, joilla yritykset voivat suojautua ja ennalta estää teknistä yritysvalvontaa.



# Tutkimusmenetelmät

- Työ on tehty kirjallisuustutkielmana, lähteinä:
  - kirjallisuus
  - sanomalehdet
  - aikakauslehdet
  - internet
- Käsittelevät:
  - yritysvakoilua yleisesti
  - teknisiä tiedonhankintakeinoja
  - tietotekniikkaa
  - tietoliikennetekniikka



# Lopputulokset

## ■ Uhkat

- tilatarkkailu
- teleliikenneyhteysien tarkkailu
- hyökkäykset tietojärjestelmiin
- mobiilin tietoliikenteen riskit

## ■ Torjunta

- ennalta estävä tietoturvallisuus



# Tilatarkkailu

- Tilassa tapahtuva luvaton katselu ja/tai kuuntelu
- Tilassa tallentavat laitteet
- Tarkkailujärjestelmät, jotka sisältävät siirtojärjestelmän





# Teleliikenneyhteysien tarkkailu

## ■ Luvaton

- puhelinkuuntelu
- fax-yhteyden valvonta

## ■ Liittymät

- analogiset --> väärinkäyttö helppoa
- digitaaliset --> väärinkäyttö vaikeampaa, mutta ei mahdotonta



# Hyökkäykset tietojärjestelmiin

- Tunkeutuminen tietojärjestelmään
  - julkisen verkon kautta
  - etäkäyttöyhteyden avulla
  - sisäverkon kautta
- Kohdennetut haittaohjelmat
- Keyloggerit



# Mobiilin tietotekniikan riskit

- Laitteet: matkapuhelimet, PDA:t, kannettavat tietokoneet
- Tiedostojen tai laitteiden katoaminen, varastaminen tai luvaton kopiointi
- Tietoliikenneyhteyksien heikkouksien hyödyntäminen tai väärinkäyttö
  - Bluetooth
  - WLAN
  - USB



# Ennalta estävä tietoturvallisuus

- Yrityksellä on oltava tietoturvastrategia ja siitä edelleen johdetut tietoturvaohjeet
- Eri muodoissa olevat tiedot on luokiteltava ja määriteltävä niitä vastaavat käsittelymenetelmät
- Toimitilat on myös luokiteltava, järjestettävä niitä vastaava suojaus ja käyttö
- Tietoluokituksen ja toimitilaluokituksen on oltava suhteessa toisiinsa ts.
  - Julkisia asioita voidaan käsitellä yleisissä tiloissa, mutta
  - salaisia asioita käsitellään vain niille määritetyissä tiloissa



# Ennalta estävä tietoturvallisuus

- Tietoteknisille laitteille ja tietoliikennemenetelmille on määritettävä turvalliset ja sallitut käyttötavat
- Yrityksessä on oltava vähintään nimetty henkilö vastaamassa yritysturvallisuudesta ja käytössään tarvittavat resurssit
- Turvallisuusohjeistus on koulutettava henkilöstölle, sen noudattaminen on motivoitava ja käyttöä valvottava

*Yrityksen tietojen turvaaminen ei ole pelkästään ylimmän johdon tehtävä, siihen on velvoitettu osallistumaan jokainen yksilö organisaatiossa.*



# Yhteenveto ja Johtopäätökset

- Yritysvakoilu on pysyvä ilmiö
- Pontimena kova taloudellinen kilpailu niin kansallisesti kuin kansainvälisestikin
- Suomi on korkean tason tietoyhteiskunta ja korkean teknologian osaaja --> yritysvakoilun riski kasvava
- Suurimmat uhkat kohdistuvat tietojärjestelmiin
  - suurin yksittäinen tiedon sijaintipaikka
  - yleisesti ei olla varauduttu yritysvakoilun tarkoituksessa tehtyyn tietoverkkohyökkäykseen
  - hyökkääminen mahdollista fyysisesti hyvin etäältä (internet)



# Yhteenveto ja Johtopäätökset

- Toinen uhkien painopistealue on mobiili tietotekniikka
  - uudet tekniset ratkaisut --> uudet uhkat, joita ei tiedosteta
- Uhkien torjunta on osa muuta tietoturvallisuusohjeistusta
- Suunnitelmien kulmakivi on **SUOJATTAVA TIETO**
- Suojaamismekanismit ovat määrätietoisella työllä ja suhteellisen pienillä taloudellisilla kustannuksilla järjestettävissä. Vastaavasti yritysvakoilun taloudellisten menetysten minimoinnista saatava hyöty voi olla huomattava



# Jatkotutkimusaiheita

- Radiotietä käyttävien tilatarkkailulähetteen vaimentaminen ja estäminen rakenteilla ja materiaaleilla
- Yritysvakoilun kannalta turvallisen tietojärjestelmän määrittely
- Uusien langattomien lyhyen ja pitkän kantaman tietoliikenneyhteyksien mahdolliset turvallisuusuhkat yrityskäytössä
- Internet-puheluiden turvallisuusuhkat ja niiden luvattoman monitoroinnin mahdollisuudet