## Sikkerhet - ikke bare virus-kontroll og passordbeskyttelse

Foredrag av:
Knut Soelberg

Norsk Regnesentral
Tlf 22 85 26 23
E-post: knuts@nr.no

Innhold
- Datadrevne angrep
- Elektroniske spor
- Sårbarhet i nettverks-tjenester og operativsystem
- Hvordan beskytte seg



## Sikkerhetsproblematikk

- Åpne nett (Internett)
  - Fritt tilgjengelig
  - Stoler ikke på brukerene
  - Fare for
    - avlytting
    - innbrudd
    - vandalisme
    - elektroniske spor
- Lukkede nett bedriftsinterne nett - intranett
  - Stoler på brukerene
  - Andre type farer domminerer
    - menneskelige feil



## Datadrevne angrep

- E-post med vedlegg
- World Wide Web
- Distribuerte kodesnutter
  - Java
  - Nettverks OLE



## Elektronisk post med vedlegg

- Muligheter
  - Kan legge ved dokumenter, regneark, presentasjoner
  - E-post programmer kan vise vedleggende automatisk
  - Word, WP, Exel el. startes opp med dokumentet
- Farer
  Dokumentene kan inneholde
  - makrovirus
  - makroer som endrer oppsett
  - makroer som sender e-post



## Elektronisk post med vedlegg

- Tiltak for å beskytte seg
  - Ikke sett opp e-post program til automatisk å vise vedlegg
  - Ikke se på (word) dokumenter ol. fra ukjente



## World Wide Web

- Nettlosen (web-browseren) kan settes opp til å starte eksterne programmer for å vise dokumenter
- Dokumentene kan inneholde aktiv kode
  - postscript
- Vær forsiktig med å la nettlosen starte opp eksterne programmer

## Java

- Generelt objektorientert programmeringsspråk
- Godt egnet for distribuerte applikasjoner
- God integrasjon mot Web
- Java applets
  - Kodesnutter som hentes over nettet
  - "Kjører" inni nettlosen
  - Gir meget store muligheter for nye spennende web-applikasjoner



## Java - sikkerhet

- Sikkerhet: sentralt i design av
  - programmeringsspråk
  - miljø (javatolken innebygget i nettlosen)
- Problemer/hull avdekket til nå skyldes
  - implementasjonsfeil
- Ledende kompetanse personer er skeptiske
- Behov for
  - sikker autentisering av java applets
  - stoler vi på applets fra X?



## Andre typer aktiv kode

- Javascript
  - Har noen fellestrekk syntaksmessing
  - Har ingen til felles med Java ang.
    design
    implementasjon
    sikkerhetsfunksjonalitet
- VBScript, Oracle Basic
- ActiveX (nettverks OLE)
  - Sannsynligvis kun tilgjengelig for Microsoft operativsystmer
  - Vet svært lite om sikkerhetsfunksjonalitet
  - Generelt meget skeptisk



## Elektroniske spor

- Hva legger du (ubevist) igjen av informasjon
  - navn og e-post adresse (e-post, news, web)
  - maskinnavn (web, ftp, telnet)
- Hvor blir slike spor liggende
  - i e-post meldinger, news artikler
  - i logger til web og ftp-tjenester
- Hvem har tilgang til å avlese dine spor



## Sårbarhet i nettverkstjenester og operativsystemer

- Ikke tenkt for mye teknologi og "duppe ditter"
- Enkel system konfigurasjon
  - hold oversikten
- Ha et (mest mulig) feil fritt system
  - rett alle feil i konfigurasjon og programvare
- Beskyttelse mot virus er sunn livsførsel
  - ikke (først og fremt) virus-sjekk programmer



## System- og tilstandsovervåkning

- Hva bør sjekkes?
  - Vanlige potensielle sikkerhetshull
  - Gammel programvare
  - Mangelfull og feilaktig konfigurering
  - Passordbruk
  - Nettverkstjenester
    - Fjern alle nettverkstjenester som ikke er i bruk
- Følg med på CERT-lister, info fra produsent
  - Noen er flinke til å varsle om feil, sårbarhet, sikkerhetshull
  - Andre ikke

## Intervett-regelene for Telenor

- Utarbeidet av Øystein Graf, Telenor IT
  - Vær ikke en smittebærer
  - Sørg for at du ikke lekker
  - Vær ikke en tyv
  - Ha respekt for arbeidsgivers tid
  - Husk at du representerer Telenor
  - Vis god folkesikk
  - Kjør ikke traktor i rush-trafikken



## Oppsummering

- Nedfell behovet for sikkerhet i en sikkerhetsstrategi
- Utarbeid enkle rutiner og bevistgjør
  - brukere og driftspersonale
- Teknologier som Java
  - gir helt nye utfordringer relatert til sikkerhet
- Sikkerhetshull og sårbarhet
  - varsles i noen miljøer/produsenter
  - dysses ned i andre
- "Security by obscurity"
  - billig på kort sikt
  - kanskje katastrofe på lang sikt