

## Internett brannmur Administrasjon

Foredrag av:  
Knut Soelberg

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

### Innhold

- Analyse av behov
- Krav til løsning
- Behov for ansvarsforhold og administrasjon

Norsk Regnesentral

1

## Organisasjonens utgangspunkt

- Behov for ekstern kommunikasjon
  - Beskrives i IT- strategien
- Behov for sikring av informasjon og ressurser
  - Avklares og beskrives i sikkerhetsstrategien
  - Behov for brannmur og dens sikkerhetsnivå avklares
  - Ansvarsforhold avklares

Norsk Regnesentral

2

## Se på helheten

- Ikke installer en ståldør i hovedinngangen når kjøkkendøra står på vidt gap
  - Ikke glem at tilkoblingen til Internett kun er en av mange trusler
  - Vurder også krav til sikkerhet ved tilkobling til andre nett
  - Vurder også krav til konvensjonell dokumentdistribusjon

Norsk Regnesentral

3

## Dilemma

- Større krav til sikkerhet medfører større begrensninger og mindre brukervennlighet for brukerne
- Brukervennlighet kontra grad av sikkerhet må vurderes før valg av løsning

Norsk Regnesentral

4

## Valg av type brannmur

- Avgjør hva du ønsker å oppnå
  - Blokkere alle innkommende sesjoner eller noen
  - Stoler du på dine egne brukere, kan de gjøre hva de vil?
  - Blokkere for den tilfeldige "hacker'n"
  - Tilby sikre forbindelser med sterk autentisering og kryptering

Norsk Regnesentral

5

## Konfigurering og administrasjon

- Kommerielle løsninger kan ofte tilby
  - Grafiske brukergrensesnitt
  - Terminalbasert som gir mulighet for automatisering
- For brukervennlige grensesnitt kan føre til falsk trygghet

Norsk Regnesentral

6

## Konfigurasjon av bastion host

- ◆ Benytt det operativsystemet du kjenner best
- ◆ Fjern unødvendig programvare og tjenester
- ◆ Sørg for et høyt sikkerhetsnivå
- ◆ Sørg for utstrakt bruk av logging & varsling
- ◆ Kommersielle løsninger er dog ofte en "black box"

Norsk Regnesentral

7

## Konfigurasjon av DNS

- ◆ DNS navnetjeneste kan by på problemer
- ◆ Valg
  - Operere med en egen uavhengig navnetjeneste med egne rootjenere
  - Skjule navn på interne noder
  - La navn på interne noder være kjent

Norsk Regnesentral

8

## Leverandører

- ◆ De fleste har kun en type løsning
- ◆ Varierende kompetanse om
  - produktet
  - brannmur og sikkerhet generelt
- ◆ Ofte kun en sentral kompetanseperson
- ◆ Velg ikke første og beste produkt og leverandør

Norsk Regnesentral

9

## Leverandører - tjenester

- ◆ Basis tjenester
  - Sette opp og konfigurere løsningen
  - Opplæring
  - Skreddersydd dokumentasjon for installasjonen
- ◆ Tilleggstjenester mange kan tilby
  - Utarbeide sikkerhetsstrategi
  - Outsourcing

Norsk Regnesentral

10

## Kontinuerlige endringer

- ◆ Dynamisk organisasjon
  - Nye behov
- ◆ Internett er i en rivende utvikling
  - Nye tjenester

Norsk Regnesentral

11

## Applikasjonsgateway Hva med nye tjenester?

- ◆ En proxy for hver tjeneste
  - Ny tjeneste => behov for ny proxy
- ◆ Hva med
  - Realaudio (udp-basert)
  - Nye betalingstjenester
- ◆ Brannmurprodusenter vil utvikle proxier for nye tjenester
  - men proxien vil alltid komme i ettertid

Norsk Regnesentral

12

## Plug and Play?

- ♦ Mange kommersielle brannmurer har
  - lettfattelig grafisk brukergrensesnitt
    - forenkler installasjon og konfigurasjon
- ♦ alt du trenger i en enhet for
  - sikker tilkobling til Internett
  - å tilby web-, ftp-tjenester mm. ut på Internett
- ♦ Lav brukerterskel
  - løsningen "er på lufta" med et museklikk

Norsk Regnesentral

13

## Tilfredstillende totalløsninger krever

- ♦ Oppsett & konfigurasjon basert på din organisasjons sikkerhetspolitikk
- ♦ Tilfredstillende drift og vedlikehold
  - Må forstå konsekvensene av en endring
- ♦ Gode rutiner for endringshåndtering
- ♦ Klare ansvarsforhold og koordinering
- ♦ Brannvegger er **ikke** plug 'n play!

Norsk Regnesentral

14

## Endringshåndtering

- ♦ En ansvarshavende for totalløsningen
  - bastion host, screening routers og programvare
- ♦ Ingen endringer (hardware og software)
  - uten konsekvensvurdering og klarsignal fra ansvarshavende
- ♦ Prosedyrer for de vanligste endringene
- ♦ Oppdater dokumentasjon etter hver endring

Norsk Regnesentral

15

## Sikkerhet på brukernivå

- ♦ Bevisstgjør brukeren om å være påpasselig med hva de sender hvor av informasjon
- ♦ Retningslinjer for bruk av lokale og internettressurser
- ♦ Tilrettelegg for å unngå virusproblemer mm
  - La frivillige vedlikeholde kataloger med populær fritt tilgjengelig programvare

Norsk Regnesentral

16

## Oppsummering

- ♦ Ikke la en brannvegg bli falsk trygghet
- ♦ Ha klare ansvarsforhold og gode retningslinjer
- ♦ Ikke tro at brannveggen er sikker bare teknologien er på plass
  - En tilfredstillende brannvegg totalløsning:
    - 20% teknologi
    - 80% administrasjon

Norsk Regnesentral

17