Veileder
for bruk av tynne klienter

Dette dokumentet er en veileder for bruk av terminaltjener/klient (tynne klienter) for å skille samtidige brukerrettigheter i åpne og sikre soner.

April 2005



Datatilsynet

Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Org.nr:	Hjemmeside:
Postboks 8177 Dep 0034 OSLO	Tollbugt 3	22 39 69 00	22 42 23 50	974 761 467	www.datatilsynet.no

Innhold

Del I Innledning 3
1 Definisjoner 3
2 Formål 3
3 Konfigurering av soner og sikkerhetsbarrierer 3

Del II Trusler og sikkerhetskrav 4
4 Trusler 4
5 Sikkerhetskrav og akseptkriterier 4

Del III Konfigurering 6
6 Nettverksmessig oppsett 6
7 Konfigurasjon av terminaltjener 7
8 Protokoll mellom tjener og klient 7

Del IV Sikkerhetsvurdering 8
9 Krav relatert til sikkerhetsbarriere 8
10 Krav til terminaltjeneren 8
11 Krav relatert til operativsystemet 9

Del I Innledning

1 Definisjoner

Det vises til ”veiledning i informasjonssikkerhet for kommuner og fylker” for definisjoner.

2 Formål

Denne veilederen beskriver bruk av tynne klienter for samtidige brukerrettigheter mot intern/sikker sone. Veilederen er et bidrag for å møte de akseptkriterier som personopplysningsloven legger opp til. Det er i dag flere leverandører av tynnklientløsninger. Disse har forskjellige egenskaper og varierer i funksjon og pris.

3 Konfigurering av soner og sikkerhetsbarrierer

Soner benyttes som et grunnleggende prinsipp i sikkerhetsarkitekturen. En sone utgjør en del av et informasjonssystem og deles for eksempel opp etter behov for skjerming av ulike personopplysninger. Soner opprettes også basert på behovet for tilgangstyring og segmentering av brukere. For å begrense tilgangen til personopplysninger, kan det være hensiktsmessig å benytte følgende soner internt i en virksomhet:

- sikret sone; hvor sensitive personopplysninger behandles (ved behov opprettes flere sikrede soner i virksomheten, for eksempel dersom dette bedre understøtter taushetsplikt). Den enkelte sikrede sone er teknisk atskilt fra resten av det interne nettverk og eventuelle andre sikrede soner, foruten mot eksterne nettverk.
- intern sone; hvor ”ikke-sensitive” personopplysninger behandles. Denne kan også omfatte andre opplysninger i virksomheten som ikke skal eksponeres eksternt.

Mellom eksternt nettverk og sikret sone hvor sensitive opplysninger behandles skal det være flere sikkerhetsbarrierer. Sikkerhetsbarrierene skal inneholde funksjoner for:

- nettverkskontroll; som regulerer informasjonsflyten mellom eksternt nettverk og virksomhetens ulike soner, herunder hvilke nettverks- og applikasjonsprotokoller som kan benyttes
- tilgangskontroll; som muliggjør kontroll og begrensning på applikasjonsnivå med det formål å:
  - verifisere at det er den tillatte tjenesten som faktisk benyttes
  - hindre at tjenesten benyttes for initiering av aktiviteter som ikke er tillatt og ikke er del av tjenesten selv
  - kontrollere og begrense funksjonaliteten i tjenestene etter behov
  - forhindre utnyttelse av kjente svakheter i tjenestene
  - kontrollere og filtrere ut komplekse datastrukturer slik at datadrevne angrep og tilstedeværelse av ødeleggende program hindres (for eksempel uønsket Active-X komponenter, uønsket Java og Java-script, virus)
  - ivareta autentisering og autorisering av brukeren før tjenesten aktiveres
  - motstå "denial of service"-angrep, det vil si uautorisert nedkjøring av tjenester.

Trafikk fra sikker sone skal alltid være initiert fra innsiden av barrieren.

Del II Trusler og sikkerhetskrav

4 Trusler

Følgende trusler er identifisert ved bruk av terminaltjener for å oppnå samtidige brukerrettigheter i åpne og sikre sesjoner:

1. Overføring av informasjon fra sikker til intern sone ved e-post
2. Overføring av informasjon fra sikker til intern sone ved direkte lagring
3. Overføring av virusinfisert informasjon, trojanske hester eller annen uønsket programvare fra intern til sikker sone ved direkte lagring
4. Overføring av informasjon fra sikker til intern sone ved mellomlagring (harddisk, diskett, USB-penn eller annet medium)
5. Brukere på sikker sone overstyrer oppsett i egen arbeidsstasjon
6. Brukere på sikker sone overstyrer oppsett i terminaltjener
7. Eksterne brukere overstyrer oppsett i terminaltjener
8. Fiendtlig programvare som kan brukes til å kompromittere sensitiv informasjon er installert på klientmaskin
9. Fiendtlig programvare som kan brukes til å penetrere sikker sone er installert på terminaltjener
10. Brukere på intern sone overstyrer oppsett i terminaltjener
11. Oppsett på terminaltjener for sikker bruker gir potensiell åpning for brukere på intern sone til å få tilgang til sikre soner, det vil si gå mot lovlig trafikk
12. Utskrift fra sikker sone blir sendt til printer som er definert til bruk av intern terminalsesjon

5 Sikkerhetskrav og akseptkriterier

En anbefalt løsning for systemteknisk sikkerhet, inkludert implementering av sikkerhetsbarriere er gitt av Datatilsynet i *"Veiledning i informasjonssikkerhet forkommuner og fylker"* [2]. Det er en forutsetning at de prinsippene som beskrives blir fulgt. Dokumentet er tilgjengelig fra Datatilsynets websider: http://www.datatilsynet.no under menyvalget "Informasjonssikkerhet".

Datatilsynet anbefaler disse overordnede akseptkriteriene for en løsning med nettverksforbindelse mellom sikre og interne soner:

- Det må benyttes et operativsystem eller 3. part sikkerhetsløsning som tilfredsstillende skiller mellom brukeres rettigheter til henholdsvis intern og sikret sone. Dette må skille mellom brukere og brukergruppers (identitet/passord) rettigheter til system og nettverksressurser.

- Brukere i sikret sone må konfigureres med to alternative brukerprofiler hvis tilgang til eksterne nettverk skal gis til disse brukerne. De to brukerprofilene kan ha følgende tilgjengelige tjenester:
  - kun tilgang til tjenester og informasjon i sikret sone
  - kun tilgang til tjenester og informasjon i eksterne nettverk, inkludert eventuell tilgang til intern sone.

• Teknisk sikkerhetsløsning hos brukeren skal bidra til å hindre uautorisert utlevering av sensitive personopplysninger ved utilsiktet overføring av data mellom program, eksempelvis ved bruk av "klipp og lim"-funksjon.

• Hvis bruker i sikret sone også skal ha tilgang til tjenester i den interne sonen eller tjenester i eksternt nettverk, må det ikke være mulig å lagre ukrypterte sensitive personopplysninger lokalt på arbeidsstasjonen.

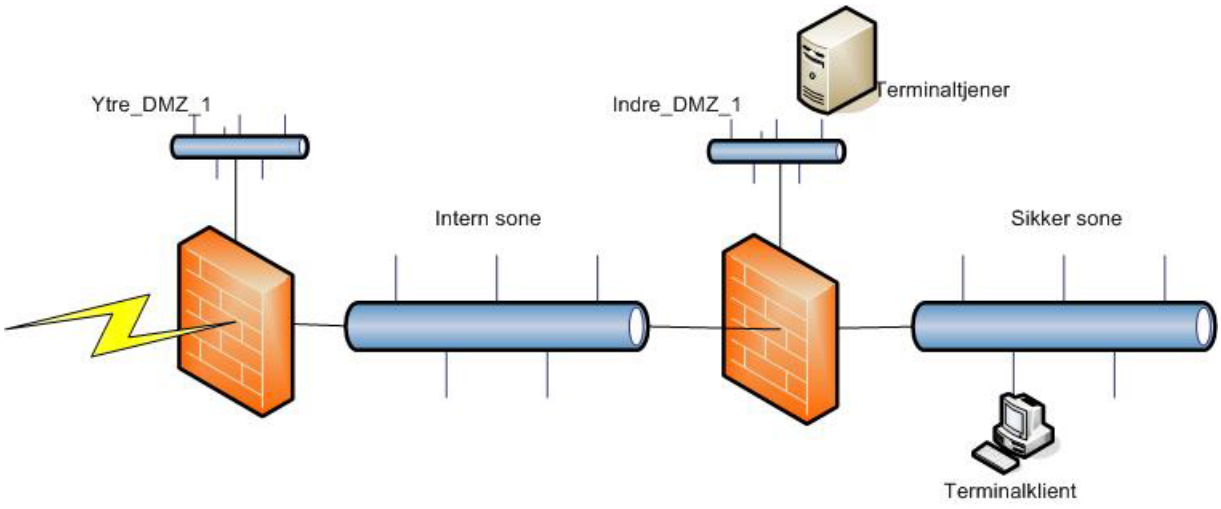
For å håndtere samtidige brukerrettigheter i åpne og sikre sesjoner ved bruk av terminaltjener, må kravene nedenfor oppfylles. Tabellen viser også hvilke trusler de enkelte krav imøtekommer.

- Vedlegg til e-post må ikke kunne hentes fra sikker sone og sendes ut i intern sone
- Bruker må ikke ha tilgang til lokale lagringsmedier fra terminalsesjonen
- Bruker må ikke ha tilgang til å endre oppsettet av terminalklienten på lokal maskin
- Mellomlagret sensitiv informasjon (for eksempel minne og mellomlagring) må ikke gjøres tilgjengelig for intern sesjon
- Utskrift fra terminalsesjon til sikker sone skal ikke håndteres via Netbios protokoll, men via protokoll for terminaltjener
- Lokal bruker må være "lavnivå brukere" uten noen administrative rettigheter
- Terminaltjeneren må plasseres på en egen sone, tilknyttet indre barriere, uten brukere
- Terminaltjeneren skal være dedikert for denne bruk uten annen programvare
- Indre sikkerhetsbarriere mot sikker sone skal ikke tillate trafikk initiert utenfra
- Indre sikkerhetsbarriere mot sikker sone skal bare tillate terminalklienten tilgang til terminaltjeneren
- Administratorkonto på terminaltjeneren må sikres ved hjelp av mekanismer tilgjengelige i operativsystemet
- Brukernes rettigheter på terminaltjeneren må begrenses slik at brukeren ikke kan foreta endringer av oppsett
- Eksterne brukere skal ikke få tilgang til terminaltjeneren
- Anonyme brukere eller "gjest"-brukere skal ikke tillates på terminaltjeneren
- Tekst fra sikker sone må ikke kunne klippes og limes inn i intern e-post
- "Klipp og lim"-funksjonen må være utilgjengelig mellom terminalsesjon og sikker sesjon
- Indre sikkerhetsbarrierer mellom terminaltjeneren og intern sone skal bare tillate trafikk initiert fra terminaltjeneren
- Det må ikke være mulig å styre utskrifter av sensitiv informasjon

Del III Konfigurering

6 Nettverksmessig oppsett

Figuren nedenfor viser hvordan terminaltjener settes opp i nettverk hvor det er gjennomført soneinndeling med bruk av to nivåer med brannmur.



FIGUR 1: Soneinndeling med bruk av to nivåer med brannmur

Beskrivelse av soner:
- Ytre_DMZ_1: Maskinene i Ytre_DMZ_1 foretar kontroll av trafikk mellom Internett og de interne nettverkene. Nettverket kan omfatte maskiner for videresending av e-post, kontroll av innholdsbaserte trusler og proxy for WEB.

- Indre DMZ_1: Egen sone på den indre sikkerhetsbarrieren bare til bruk for terminaltjener.

- Sikker sone: Sone hvor det behandles sensitive personopplysninger. Det kan etableres flere atskilte sikre soner hvor terminalklienter betjenes fra den samme terminaltjeneren.

– **Intern sone:** Sone hvor virksomhetens øvrige informasjon behandles.

Terminaltjeneren må legges i et eget grensesnitt, ”sikker tjener”-sone, på den indre sikkerhetsbarrieren. Terminaltjeneren vil da være på et segment uten brukere og uten direkte tilgang fra Internett. Alle klienter fra sikker sone som ønsker å få tilgang til Internett (sende e-post eller benytte WEB tjenester), eller til intern sone, gjør dette via en terminaltjener

Den indre sikkerhetsbarrieren må for å beskytte terminaltjeneren, konfigureres slik at det kun er terminalklienter fra sikker sone som kan nå terminaltjeneren. Terminaltjeneren plasseres i indre DMZ for å oppnå konfigurasjonskontroll over nettverkstrafikken. Den indre DMZ vil fungere som en ”sluse” for trafikken. På denne måten er det terminaltjeneren som når internsone eller ytre nett på vegne av brukeren i sikker sone.

Terminalklienten kopler seg opp mot en terminaltjener. Her må brukeren logge seg på for å få tilgang til Internett eller intern sone. Brukeren skal autentiseres mot intern sone, og få tilhørende rettigheter i intern sone. Det skal være mulig for brukere fra sikker sone å kjøre applikasjoner i intern sone (for eksempel timeregistrering, tekstbehandling eller andre vanlige applikasjoner) via terminaltjeneren. Brukeren skal også ha tilgang til å lagre informasjon fra disse applikasjonene i intern sone. Ekstern e-post mottas i postkontor i ytre DMZ og må hentes inn av virksomheten ved hjelp av POP eller IMAP slik at gjennomgående forbindelser ikke opprettes. E-posten hentes til interne postkontor på intern eller sikker sone:

– Åpen e-post (ikke sensitiv) skal hentes til postkontor i den interne sonen
– Der hvor sensitive personopplysninger skal mottas via e-post, må den aktuelle sikrede sone som skal motta e-posten ha et eget postkontor hvor denne posten blir dekryptert og sjekket for virus.

Brukere på den sikre sonen får tilgang til postkontor på intern sone for sending og mottak av ekstern åpen e-post via terminaltjeneren. Eventuell sensitiv e-post håndteres i den sikre sonen.

7 Konfigurasjon av terminaltjener

Terminaltjeneren må konfigureres slik at terminalklienten ikke skal få tilgang til lokale ressurser. ”Klipp og lim”- funksjonen må deaktiveres slik at informasjonen ikke skal kunne kopieres fra applikasjon i sikker sone.

Terminaltjeneren må konfigureres slik at den bare har tilgang til bestemte, forhåndsdefinerte tjenester.

Tilgangen til applikasjoner må defineres slik at gruppekonti (”Gjest”, ”N-avdeling” og lignende) ikke tillates å starte applikasjonene. Alle brukere / terminalklienter må logge seg på terminaltjener med individuelle brukernavn og passord for å kunne starte en applikasjon.

8 Protokoll mellom tjener og klient

Protokollen som benyttes mellom terminaltjener og -klient skal ikke kunne anvende andre funksjoner enn de som er nødvendige for klienten. Aktuelle funksjoner er overføring av informasjon fra tastatur og mus, informasjon for å oppdatere skjermbilder, samt nødvendige funksjoner for å kontrollere forbindelsen mellom klient og tjener. For utskrift fra applikasjoner i intern sone må protokollen også tilby funksjon for overføring av utskriftsdata til skriver i sikker sone.

Siden protokollen bare vil overføre intern informasjon som er tilgjengelig fra intern sone, vurderes ikke kryptering som et nødvendig tiltak.

Del IV Sikkerhetsvurdering

9 Krav relatert til sikkerhetsbarriere

Dersom trafikk initieres mot sikker sone utgjør dette en risiko. Dette kan resultere i at uønsket programvare blir installert i sikker sone og kan kompromittere informasjon.

For å redusere denne risikoen må den indre sikkerhetsbarrieren konfigureres slik at trafikk ikke kan initieres fra terminaltjener mot sikker sone. Som en følge av dette kan ikke autentisering av brukere ved pålogging til terminaltjener skje via Netbios eller IP tilbake til en domenekontroller i sikker sone. Autentisering må enten skje lokalt i terminaltjeneren eller mot annen domenekontroller utenfor sikker sone.

Terminaltjeneren må beskyttes slik at den ikke kan kompromitteres av brukere fra sikker sone eller av brukere fra intern sone. Dersom tjenermaskinen blir kompromittert, kan oppsettet av terminaltjeneren endres, og dette kan føre til at sensitiv informasjon kan bli kompromittert.

For å redusere denne risikoen må den indre sikkerhetsbarrieren konfigureres slik at den bare tillater trafikk initiert av terminalklientene mot terminaltjener. Ingen annen trafikk skal tillates initiert fra intern sone mot terminaltjener.

10 Krav til terminaltjeneren

Sensitiv informasjon må beskyttes slik at den ikke kan bli sendt til intern sone og dermed bli kompromittert. Brukerne må også forhindres i å lagre informasjon hentet fra for eksempel Internett på harddisk. Slik informasjon kan inneholde virusinfisert informasjon, trojanske hester eller annen uønsket programvare, og kan kompromittere sensitiv informasjon. Brukerne må derfor ikke, fra en terminalsesjon, få tilgang til sensitiv informasjon lagret på egne lagringsmedier. Terminaltjeneren må kunne konfigureres så en slik tilgang blir forhindret.

Bruk av ”klipp og lim”- funksjonen gir mulighet til å kompromittere sensitiv informasjon, og denne funksjonen må derfor deaktiveres. Dette må også gjelde for ”print screen”-funksjonen.

Mellomlagring, det vil si lagring som ikke er brukerinitiert, men som blir håndtert automatisk av applikasjoner eller operativsystem, utgjør en mulig risiko for kompromittering av sensitiv informasjon. Dersom sensitiv informasjon mellomlagres må ikke denne være tilgjengelig for en intern sesjon.

Alle publiserte programmer vil kjøre på terminaltjeneren og mellomlagringsfiler blir lagret på denne, i for eksempel nettleseren. Dette anses ikke som en trussel fordi disse filene bare vil inneholde ikke-sensitiv informasjon.

Ukontrollert stans av operativsystemet hos terminalklienten resulterer i at informasjon dumpes til harddisken. Fordi klienten ikke skal ha tilgang til lokal harddisk vurderes ikke dette som noen trussel.

Det er mulig å skrive ut ikke-sensitiv informasjon fra terminalsesjoner. Printere som er tilgjengelige bestemmes av brukerprofilen ved oppstart av terminalklienten, der brukeren blir

autentisert. Dersom dette er en printer beregnet for ikke-sensitiv informasjon, kan sensitiv informasjon kompromitteres dersom den sendes til denne printeren fra en samtidig sikker sesjon. Dette vurderes ikke som noen risiko, fordi printere er definert i operativ systemet sammen med brukerprofilen. Printervalgene for sikker og intern bruker (terminalklient) vil derfor være helt atskilt.

Utskrift fra en terminalsesjon som eksekverer på tjeneren må ikke initiere trafikk inn mot sikker sone (se under krav relaterte til sikkerhetsbarriere). Siden utskrifter fra terminalsesjonen sendes via den dedikerte protokollen vil dette ikke initiere noe trafikk inn mot sikker sone.

For å beskytte terminaltjeneren mot uautorisert tilgang skal ikke anonyme brukere tillates å kjøre applikasjoner på denne. Bare brukere som er eksplisitt definert i tjeneren skal kunne kjøre programmer slik for eksempel som terminalklienten. Terminaltjeneren må derfor konfigureres slik at Anonym/"Gjest"-brukere ikke kan starte publiserte applikasjoner.

11 Krav relatert til operativsystemet

Brukerne kan, dersom de har nødvendige rettigheter, endre sikkerhetskonseptet på lokal maskin. Dette kan resultere i at sikker sone blir kompromittert ved at uønsket programvare installeres og eksekveres.

Brukerens rettigheter på egen arbeidsstasjon må defineres slik at brukeren ikke har mulighet, enten bevisst eller ubevisst, til å overstyre sikkerhetskonseptet som er definert for terminalklienten. Dette tilsier at operativsystemet på klientmaskinen må være et som gir mulighet for begrensning av brukeres rettigheter.

Terminaltjeneren er en av de mest kritiske delene av sikkerhetskonseptet, fordi tjeneren opererer som en "agent" på vegne av brukere på sikker sone. Dersom konfigurasjonen av terminaltjeneren endres, vil det kunne påvirke hele sikkerhetskonseptet, se kapittel 7 for nødvendig konfigurasjon av terminaltjeneren.

Terminaltjeneren må konfigureres etter "need-to-know" prinsippet. Terminalklientene skal ikke ha flere rettigheter enn det som er nødvendig for å kjøre de programmene som er bestemt. Resten av systemet må beskyttes slik at det ikke bevisst eller ubevisst kan gjøres endringer i oppsettet av andre enn systemadministrator.

Ved å starte en nettleser, for eksempel Internett Explorer, vil terminalklienten kunne utforske terminaltjeneren og eksekvere de applikasjonene som den har tilgang til. Denne muligheten er tilstede selv om terminaltjeneren er konfigurert slik at klientene bare skal kunne eksekvere publiserte (forhåndsdefinerte) program. Dersom tilgangsrettighetene på terminaltjeneren er satt slik at klientenes tilgang er begrenset til de oppgavene de skal utføre, vil ikke dette utgjøre noen sikkerhetstrussel.

Det må gjøres periodisk integritetssjekk på terminaltjeneren for å oppdage uønskede endringer i konfigurasjon eller applikasjoner.