Fysiska klienter för IT-system

Egenskaper och IT-säkerhetseffekter på systemnivå

CAROLINE BILDSTEN, DANIEL EIDENSKOG,
JACOB LÖFVENBERG, IOANA RODHE

FOI-R--4701--SE
ISSN 1650-1942 December 2018

Caroline Bildsten, Daniel Eidenskog, Jacob Löfvenberg, Ioana Rodhe

Fysiska klienter för IT-system

Egenskaper och IT-säkerhetseffekter på systemnivå

Bild/Cover: Camille Orgel, Unsplash.com

Titel	Fysiska klienter för IT-system – Egenskaper och IT-säkerhetseffekter på systemnivå
Title	Physical clients for IT systems – Properties and IT security effects on system level
Rapportnr/Report no	FOI-R--4701--SE
Månad/Month	December
Utgivningsår/Year	2018
Antal sidor/Pages	43
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Cyber
Projektnr/Project no	E72727
Godkänd av/Approved by	Johan Allgurén
Ansvarig avdelning	Ledningssystem
Exportkontroll	Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen.

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bl.a. innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

Sammanfattning

Klient-server-arkitekturer tillåter en användare att nyttja data eller tjänster som erbjuds av servrar i ett nätverk. För detta krävs en klient som utgör IT-systemets gränssnitt mot användaren. Klienterna brukar delas in i tre huvudtyper baserat på deras uppbyggnad: tjocka klienter, tunna klienter och nollklienter. Tjocka klienter är väsentligen vanliga datorer där applikationerna lagras och körs i klienten. Tunna klienter är enkla datorer, med ett begränsat operativsystem, där en mjukvara för att ansluta till fjärrskrivbord används för att nå servrarna. Nollklienter är en ytterligare förenkling, där klienterna saknar operativsystem och i princip endast agerar som förlängning av användargränssnittet från serverns fjärrskrivbord.

Valet av klienttyp hänger samman med andra egenskaper i IT-systemet. Det finns sällan något självklart val utan det går ofta att använda olika klienttyper, men olika val passar olika väl samman med andra egenskaper i IT-systemet eller dess kontext. Specifikt finns det säkerhetsaspekter som hör samman med valet av klienttyp.

Det finns en marknadstrend mot systemlösningar baserade på fjärrskrivbord där konceptet med tunna klienter och nollklienter passar in väl. I marknadsmaterial och ofta även i fackpress beskrivs dessa lösningar som mycket gynnsamma, ur ett funktionellt, ekonomiskt och säkerhetsmässigt perspektiv. Vid en noggrannare analys av innehållet i dessa beskrivningar framträder en mer nyanserad bild. En del som sägs är direkt fel, en del är överdrivet, och ur Försvarsmaktens perspektiv är en del irrelevant. Även efter denna analys kvarstår dock väsentliga egenskaper som kan ge värdefulla bidrag till ett IT-system. Hur stort bidraget blir beror dock i hög grad på sammanhanget och valet av klienttyp blir en avvägning mellan olika behov.

En marknadsöversikt över tillgängliga tunna klienter och nollklienter med säkerhetsfokus visar att utbudet är magert och det är svårt att värdera tillförlitligheten i produkterna baserat på det publikt tillgängliga informationsmaterialet. Av studien som ligger till grund för denna rapport framgår dock att en säker nollklient skulle vara en värdefull komponent att ha tillgänglig i potentiella IT-systemlösningar för Försvarsmakten. I rapporten presenteras därför en tänkbar arkitektur för en nollklient som tillåter samtidig uppkoppling mot flera separata informationsdomäner för att visa den principiella möjligheten att utforma en sådan klient.

Nyckelord: tjock klient, tunn klient, nollklient, nedbantad klient

Summary

Solutions based on client-server architectures allow users to access data and services offered by a server over a network. The client terminal provides the IT system's interface for the user. Clients are usually divided into the three main categories thick clients, thin clients, and zero clients. Thick clients are essentially normal computers where applications are stored and run on the client. Thin clients are simple computers, with a limited operating system, running a remote desktop software to provide access to the servers. Zero clients are further simplified. Zero clients have no operating system and act as an extension of the user interface provided by the server's remote desktop.

The selection of client type usually involves the consideration of various properties of the IT system. There is rarely an obvious choice and it is often possible to use different client types. Nevertheless, the different types of clients do have properties that make them more or less suited as the design solution for a specific IT system. Specifically, there are security aspects associated with the choice of client type.

There is a market trend towards systems with remote desktop solutions, where the concept of thin and zero clients suits well. In marketing material, and even in the professional press, these solutions are described as very favourable, from functional, financial, and security perspectives. After a careful analysis of the content of these documents, a more balanced view of the solutions emerges. Some claims are erroneous, some are excessive, and some are, viewed from the perspective of the Swedish Armed Forces, irrelevant. After this analysis, there remain essential properties of thin and zero clients that can provide added value to an IT system. The actual value that is added usually depends on the context, and the choice of client type is usually a trade-off between different requirements.

A market overview of thin and zero clients with security certifications shows that there are only a few products available and that it is difficult to assess the reliability of these based on publicly available marketing material. However, from the results presented in this report, it emerges that a secure zero client in some cases would be a valuable component to have in IT systems used by the Swedish Armed Forces. Therefore, at the end of the report we present a possible architecture of a zero client that allows simultaneous connections to several separate information domains as an attempt to demonstrate that such a solution is possible.

Keywords: thick client, thin client, zero client

Innehåll

1 Inledning

Många IT-system baseras på klient-server-arkitekturer, där systemets funktioner fördelas mellan *servrar* som tillhandahåller olika tjänster och *klienter* som nyttjar dessa tjänster. Klient-server-arkitekturer inkluderar ett stort spann av system-arkitekturer och kan byggas på många olika sätt. Systemen kan bestå av allt från små mjukvarulösningar, där en del av mjukvaran använder tjänster som tillhandahålls av en annan del av mjukvaran, till mycket komplexa system med ett stort antal datorer och en stor mängd mjukvara. Ett exempel på ett komplext system som i stor utsträckning bygger på klient-server-arkitektur är internet, där många, globalt distribuerade klienter använder en uppsjö av olika tjänster som tillhandahålls av många, globalt distribuerade servrar.

Denna rapport handlar om klienter i en specifik betydelse, nämligen de fysiska apparater som används för att en användare ska kunna nå tjänster i ett IT-system. Fortsättningsvis är det denna betydelse hos ordet klienter som avses när det används i texten. Dessa klienter delas vanligtvis in i tre huvudkategorier – *tjocka klienter*, *tunna klienter* och *nollklienter* – beroende på deras uppbyggnad och egenskaper. För att förenkla texten kommer de två senare kategorierna att betecknas med termen *nedbantade klienter* när dessa behandlas gemensamt i rapporten. Ursprunget till dagens nedbantade klienter kan spåras tillbaka till de så kallade X-terminaler som introducerades under 1980-talet (Engberg & Porcher 1991). X-terminaler påminner mycket om dagens tunna klienter, där terminalen visar skrivbord och fönster från applikationer som körs på en annan dator.

Olika typer av klienter ger olika möjligheter och ställer olika krav på IT-systemens utformning. Valet av klienttyp är sällan en självklarhet utifrån vad systemet ska användas till, utan bestäms genom olika designval under utvecklingsarbetet. När systemarkitekten gör designvalen behöver denne en god förståelse för vilken påverkan valen ger på systemet och dess uppbyggnad. Som del i detta behöver systemarkitekten en god förståelse för de olika klienttypernas förutsättningar och egenskaper.

IT-säkerhet är en viktig fråga i systemarbetet och många designval påverkar olika säkerhetsaspekter. Genom att förstå klienttypernas övergripande egenskaper och påverkan på säkerhetsaspekterna kan kvaliteten på dessa designval höjas och därmed förhoppningsvis ge säkrare system i förlängningen.

Syftet med denna studie är att sammanställa kunskap om olika typer av fysiska klienter som används för åtkomst till IT-system. Den insamlade kunskapen är avsedd att underlätta diskussioner kring val av klienter i samband med utveckling och förvaltning av IT-system inom Försvarsmakten.

Målet med studien är att svara på följande frågor:

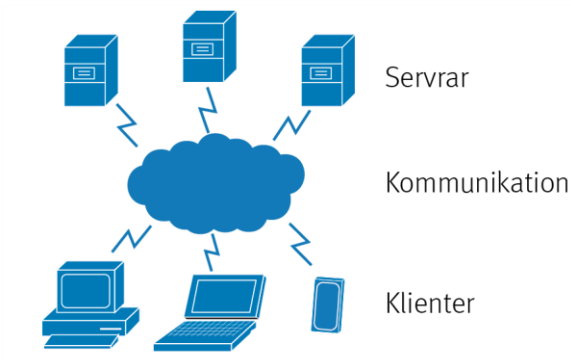
- Vilka olika typer av klienter finns det och vilka övergripande egenskaper har dessa typer?
- Vilka argument finns i marknadsföringsmaterial och liknande källor om nedbantade klienter? Håller argumenten för en kritisk granskning?
- Vilka effekter har olika klienttyper på IT-säkerheten i systemen?

Rapporten riktar sig huvudsakligen till personer som arbetar med utveckling och förvaltning av Försvarsmaktens IT-system. Studien är genomförd inom ramen för FoT-projektet *IT-säkerhetsmetoder* som är en del i FoT-området *Operationer i cyberdomänen* med beställningsnummer AF.9221516. Studien utgår från frågeställningar som prioriterats av Försvarsmaktens styrgrupp för FoT-området.

2 Bakgrund

Ett vanligt designkoncept för IT-system är klient-server-arkitekturer[1]. I sådana arkitekturer delas systemet in i *klienter* och *servrar*, där klienterna nyttjar *tjänster* hos servrarna. Konceptet med indelning i klienter och servrar används på många olika nivåer i IT-systemen, där exempelvis en mjukvarukomponent kan vara indelad i en klientdel och en serverdel med olika ansvarsområden. Servrar kan även avse de fysiska och virtuella maskiner som används för att köra server-funktioner i systemet. I detta fall utgörs klienterna av fysiska maskiner – datorer och terminaler – som nyttjas av användarna för att nå servertjänsterna i systemet. Denna rapport fokuserar på denna senare typ av klienter – de fysiska klienterna.

Figur 1 visar en generell arkitektur för klient-server-system, där fysiska klienter används för att nå fysiska och/eller virtuella servrar. Systemets användare nyttjar de fysiska klienterna för att interagera med de tjänster som systemet erbjuder. Tjänsterna kan köras såväl lokalt på klienten som på servrarna, beroende på sådant som systemets arkitektur, tjänsternas karaktär och vilken typ av klient som används.



Figur 1. Generell klient-server-arkitektur.

Det finns en stor frihet att välja hur funktionerna i systemet fördelas och vilka komponenter som används, gällande såväl mjukvara som hårdvara. Det är ofta ingen självklarhet att en viss arkitektur är signifikant bättre än andra för att lösa

[1] I engelskspråkig litteratur används både *client-server architecture* och *client-host architecture*. Orden *server* och *client* (sv. *klient*) kan avse såväl fysiska och virtuella maskiner som mjukvarukomponenter, vilket innebär att termen client-server architecture kan uppfattas som otydlig. För att underlätta förståelsen kan då termen client-host architecture användas då ordet *host* (sv. *värd*) tydligare pekar ut att det är maskiner som avses. Klient-värd-arkitektur är dock inte etablerat i svenskan, varför denna term inte används i rapporten

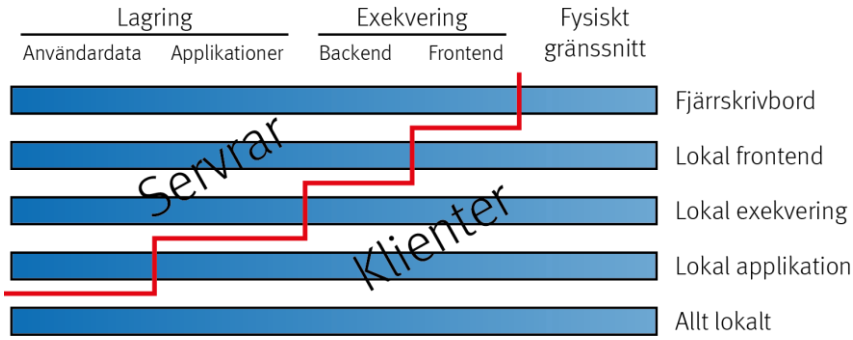
systemets uppgift. Valet bygger snarare på en mängd olika förutsättningar och krav som utvecklarna måste ta hänsyn till, exempelvis:

- systemets uppgifter
- systemets grad av centralisering (om systemet är lokalt eller distribuerat över olika platser)
- miljöfaktorer (exempelvis utrymme och klimat)
- användaraspekter (exempelvis hur ofta systemet används och om systemet används i en stridssituation)
- informations- och IT-säkerhetsaspekter.

Vissa funktioner i ett IT-system är till sin natur sådana att de passar bäst i serverdelen av systemet, exempelvis rättighetskatalogtjänster och backuptjänster. Det fysiska användargränssnittet med exempelvis bildskärm, tangentbord och mus måste befinna sig fysiskt nära användaren och hanteras därmed av klienten. De övriga funktionerna i systemet kan däremot fördelas betydligt friare mellan klient och server.

Ett exempel på hur en applikation som interagerar med användaren kan organiseras och fördelas mellan klient och server visas i figur 2. Det fysiska användargränssnittet i klienten låter användaren interagera med applikationen som körs på antingen klienten eller en server. Applikationen är uppdelad i två delar, *frontend* (användarorienterad del, presentationslager) och *backend* (dataorienterad del, datalager), där det är valbart om allt ska köras på servrar, om frontend ska köras på klienten eller om både frontend och backend ska köras på klienten. Slutligen finns möjligheten att välja var lagring av applikation och användardata ska ske.

Systemarkitekturen kan betraktas i olika perspektiv och funktionerna kan fördelas mellan olika systemkomponenter på många olika sätt. I figur 2 visas endast ett av perspektiven, där fördelningen baseras på var lagring och exekvering utförs. IT-systemen innehåller dessutom ofta flera typer av tjänster med olika krav på användarnas miljö, varför arkitekturen kan innehålla flera typer av klienter.



Figur 2. Designval avgör hur funktioner fördelas mellan klient och server.

Beroende på hur funktionerna fördelas går det att använda olika typer av klienter i systemet. När allt körs på klienten krävs en komplett dator, ofta kallad *tjock klient* (eng. thick client)[2], med ett komplett operativsystem, tillräckliga beräkningsresurser och möjlighet till lokal lagring. Ju mindre funktion som ligger hos klienten, desto tunnare kan klienten vara. I extremfallet, när endast det fysiska användargränssnittet ligger hos klienten brukar denna kallas för en *nollklient* (eng. zero client). Klienter som har en viss beräkningskraft och möjlighet att köra vissa applikationer lokalt, men mindre resurser än en normal dator brukar kallas för en *tunn klient* (eng. thin client). Tunna klienter har i regel ett lokalt operativsystem, men saknar vanligtvis lokal lagring för användardata och applikationer. Förutom operativsystemet kan tunna klienter även i viss utsträckning köra mindre krävande applikationer lokalt på klienten. I många fall används dock tunna klienter i praktiken på samma sätt som nollklienter, där klienten endast kör en applikation för att ansluta mot fjärrskrivbord. Jämfört med de tjocka klienterna så går det att se tunna klienter och nollklienter som nedbantade i fråga om exempelvis beräkningskapacitet, lagringsmöjligheter och komplexitet.

Valfriheten som exemplifieras i figur 2 begränsas ofta i någon mån av praktiska hänsyn som är specifika för varje system. Exempelvis är det inte möjligt att ha nollklienter om det inte finns en tillförlitlig kommunikation mellan klient och server. Dessa klienter kräver en slags *online*-infrastruktur, där kommunikationen alltid är igång. När så inte är fallet bygger systemet mer på en uppdelad arkitektur, där klienterna ska kunna fungera *offline*. För att samordna information i

[2] Tjocka klienter benämns även som feta klienter (eng. fat clients).

offline-arkitekturer används ofta någon form av synkroniseringstjänst på servrarna, dit klienterna ansluter för att överföra information när möjlighet finns.

När klienten endast sköter det fysiska användargränssnittet så ansluter den typiskt till så ett så kallat *fjärrskrivbord* (eng. remote desktop)[3]. Tekniken med fjärrskrivbord är inte begränsad till system med nollklienter utan kan användas oavsett klienttyp. Tunna och tjocka klienter kan komma åt dessa fjärrskrivbord genom speciella klientapplikationer, såsom Microsoft Remote Desktop[4] och Citrix Workspace[5].

Mer omfattande system med fjärrskrivbord bygger på att serverdelen byggs upp specifikt för att skapa dessa virtuella skrivbord och göra dem tillgängliga för användarnas klienter. Detta brukar kallas för en *virtuell skrivbordsinfrastruktur* (eng. virtual desktop infrastructure, VDI). VDI-lösningar kan innehålla allt från en enda server med alla relevanta tjänster för fjärrskrivbordsanslutning, till komplexa system med många virtualiserade servrar som var och en hanterar en delmängd av anslutningarna eller tjänsterna.

Servervirtualisering är en teknik som används i hög utsträckning i system med fjärrskrivbord. Virtualisering av servrar, det vill säga frikoppling av mjukvara och operativsystem som körs på servrarna från den faktiska hårdvaran, är inte enbart anpassat för fjärrskrivbord utan snarare en teknik för att hantera komplexa servermiljöer. Servervirtualisering utgör ett eget kunskapsområde, med många möjligheter och fallgropar. I en tidigare studie har FOI undersökt de IT-säkerhetsrisker som virtualiseringstekniken medför (Eidenskog & Karresand 2017).

Beroende på klienttyp finns det olika tekniker som låter användarna komma åt applikationerna. En nollklient kan förenklat ses som en förlängning av anslutningarna till användargränssnittet i form av exempelvis bildskärm, tangentbord och mus. Operativsystem och applikationer körs på servern medan användargränssnittet överförs till klienten. Nollklienten kan med denna förenklade bild kallas för en virtuell KVM-förlängare[6]. De data som skickas mellan server och klient utgörs av bild och ljud till klienten samt tangentbordstryckningar och mushändelser till servern.

[3] Fjärrskrivbord kallas även för *virtuellt skrivbord* (eng. virtual desktop). Denna term används dock även för att beteckna utökningar av en dators lokala skrivbord. I denna rapport används därför termen *fjärrskrivbord* för att undvika oklarheter om vad som avses.

[4] https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-clients [2018-11-21]

[5] https://www.citrix.se/products/citrix-workspace/ [2018-11-21]

[6] KVM är en förkortning för de engelska orden keyboard, video och mouse. Denna förkortning är vanligt förekommande för att representera det fysiska användargränssnittet på en dator. En KVM-förlängare är traditionellt sett en utrustning som kopplas mellan datorns kontakter och de fysiska I/O-enheterna för att kunna utöka avståndet mellan dem.

När tunna klienter används för att ansluta mot fjärrskrivbord blir trafiken över nätverket i praktiken densamma som om nollklienter skulle ha använts. Då tunna klienter även kan köra andra applikationer är det möjligt att exempelvis köra en lokal webbläsare för att ansluta till webbtjänster på servern eller att köra en specifik klientmjukvara som ansluter till en bakomliggande tjänst på en server. I dessa fall överförs någon form av applikationsdata över ett applikationsprotokoll, exempelvis HTML över HTTPS om det är en webbläsare och en webbtjänst som kommunicerar.

Tjocka klienter har ett operativsystem och kan i teorin köra vilka applikationer som helst, från fjärrskrivbordsanslutning till mycket komplexa programvaror. Behovet av kommunikation mellan den tjocka klienten och dess omgivning kan därmed variera mycket beroende på systemets uppbyggnad och funktion.

Smarta mobiltelefoner, surfplattor och liknande kan också användas som klienter i IT-systemen. Dessa klienter är närmast att betrakta som tjocka klienter då de såväl kan köra lokala applikationer som användas för att nå fjärrskrivbord, även om de rent fysiskt är betydligt mindre än vanliga tjocka klienter.

Användning av mobiltelefoner och liknande som klienter är relativt vanligt inom den kommersiella sfären, där det ofta talas om *bring your own device* (BYOD, sv. medtag egen apparat). Med BYOD-konceptet tillåts att de anställda ansluter till organisationens nätverk med sina egna, privata enheter för att komma åt fjärrskrivbord och andra tjänster i organisationens IT-system. Då dessa enheter är utanför organisationens kontroll så leder detta till ökade IT-säkerhetsrisker, vilket även är ett av de starkaste argumenten mot BYOD. För stora delar av Försvarsmaktens verksamheter finns i många fall ytterligare problem med att använda mobiltelefoner och liknande som klienter. Problemen kan exempelvis vara att dessa vanligtvis ansluter trådlöst till systemen och är designade för att ha ständig uppkoppling mot internet. Sådana klienter kommer inte att diskuteras vidare i denna rapport.

2.1 Klienttyper

I detta avsnitt görs en något noggrannare jämförelse av de klienttyper som introducerades ovan. Syftet är att ge en tillräckligt noggrann bild av de olika klienttypernas egenskaper för att kunna resonera om de effekter som följer när ett val görs mellan olika sorters klienter.

Det finns ingen etablerad definition att luta sig mot när man ska avgöra om en klient ska anses tillhöra den ena eller den andra typen och de relevanta egenskaperna är ofta sådana att det finns en glidande skala snarare än några få, lätt särskiljbara alternativ. Beskrivningen nedan är dock ett försök att dela in klienterna i tjocka klienter, tunna klienter och nollklienter på ett sätt som i möjligaste mån stämmer överens med det språkbruk som finns inom området.

2.1.1 Tjocka klienter

En tjock klient[7] är en dator av standardtyp som används i en klient-server-arkitektur. Den har ett operativsystem, lagringsutrymme och alla applikationer körs lokalt, vilket gör att den kan användas självständigt. En tjock klient ansluter till servern för att utbyta information, men kan däremellan utföra uppgifter självständigt. Beroende på tillämpning kan anslutningen till servern vara allt från aktiv under kortare perioder med glesa intervall, till att vara kontinuerlig. Servern sköter normalt åtminstone backup, lagring av användardata och användar-autentisering.

En variant av tjock klient som saknar lokal lagring går under namnet hybrid-klient. Hybridklienten hämtar sitt operativsystem och sin mjukvara från en server via nätverket men agerar i övrigt som en tjock klient. Bortsett från denna skillnad har hybridklienten således samma egenskaper som en tjock klient.

En fördel med hybridklienten jämfört med en vanlig tjock klient är att det kan vara lättare att säkerställa integriteten hos mjukvaran när den lagras på servern, varför klienten enkelt kan startas om för att återgå till ett känt och bra tillstånd ifall något oönskat händer. I resten av denna rapport kommer hybridklienter att anses vara en sorts tjock klient och inte behandlas separat.

2.1.2 Tunna klienter

En tunn klient (eng. thin client) är en enhet vars huvudsakliga uppgift är att erbjuda ett välfungerande gränssnitt mellan användaren och servern. På ett principiellt plan är en tunn klient som vilken dator som helst, med lagringsmedia, operativsystem och möjlighet att köra applikationer. Men eftersom uppgiften är att fungera som klient mot en server så kan den tunna klienten göras avskalad med avseende på funktion och förmåga jämfört med en tjock klient. Exempelvis behöver lagringsmediet inte vara så stort eftersom det inte är lika mycket som behöver lagras där samtidigt som processorn inte behöver vara så kraftfull eftersom servern kan stå för beräkningsprestanda. Hur avskalad klienten kan göras beror på hur uppdelningen mellan server och klient görs i det specifika fallet (jämför med figur 2 och diskussionen i anslutning till denna).

För att kunna erbjuda den önskade gränssnittsfunktionen har tunna klienter vanligtvis ett enkelt operativsystem som körs lokalt och sköter kommunikationen med servern. Operativsystemet brukar vara konfigurerat så att klienten inte erbjuder någon användaranpassning. Detta innebär att varje gång klienten startas om hamnar den i samma tillstånd. Däremot är det inte ovanligt att servern kan spara användarsessionen så att användaren kan återuppta sitt arbete från precis den punkt då det avslutades, antingen vid ett annat tillfälle eller från en annan

[7] Tjock klient kallas även fet klient, eng. thick client, heavy client, rich client.

klient. Användaren har i regel ingen möjlighet att ändra inställningar som lagras i klienten, utan detta kan endast göras av systemadministratörerna. De inställningar som finns tillgängliga för användaren berör dennes fjärrskrivbord och lagras i servern.

Tunna klienter kan variera stort i utformning och prestanda. I ena änden av spektrumet finns tunna klienter med lika hög prestanda som en kraftfull, vanlig dator. De kör avancerade applikationer själva och kan använda lokalt lagringsmedium för växlingsfiler och annan avlastning. I andra änden av spektrumet finns tunna klienter med minimal funktionalitet. Det enda den gör när den startar är att ladda operativsystem och mjukvara för fjärrskrivbordsfunktion. Spridningen i funktionalitet hos tunna klienter gör att det är svårt att ge entydiga svar på hur införandet av tunna klienter påverkar resten av IT-systemet.

2.1.3 Nollklienter

Nollklienter[8] är en vidareutveckling av tunna klienter där man har gått ett steg längre och använder sig av en mycket enkel mjukvara, ofta kallad firmware, för klientens funktionalitet. Nollklienten implementerar nätverkskommunikation med servern och erbjuder ett grundläggande grafiskt användargränssnitt. På detta sätt avkodas och presenteras visningsinformation som tas emot från servern och användarinmatning skickas tillbaka till servern. I en nollklient behövs alltså ingen beräkningskapacitet eller något fullfjädrat operativsystem. Istället kan den ses som en enhet som möjliggör att en uppsättning I/O-enheter såsom bildskärm, tangentbord och mus kan placeras på användarens arbetsplats utan att en dedikerad dator behöver finnas där.

Den enklast tänkbara nollklientlösningen är att datorn placeras på en annan plats men allt annat är lika, det vill säga att användaren kör samma program, på samma sätt som annars, på samma dator som annars (eller en motsvarande dator som har en formfaktor som är anpassad till den plats där datorn placeras). Finns det flera nollklienter kan olika serverlösningar användas. Det enklaste är att ha datorerna i en serverhall eller att använda en bladserver för att minimera utrymmesbehovet. En mer avancerad, och vanligare, lösning är att använda någon sorts VDI-lösning för att inte behöva ha lika många servrar som klienter.

Nollklienter kan ses som motsatsen till tjocka klienter, såtillvida att med en renodlat tjock klient bearbetas all data i klienten och med en nollklient bearbetas all data i servern. Allt som befinner sig mellan dessa två ytterligheter är någon form av tunna klienter.

Vilken enhet som helst som implementerar de relevanta protokollen kan användas för att ge samma funktionalitet som en nollklient. Specifikt finns det

[8] Nollklient kallas även ultratunn klient, eng. zero client, ultra thin client

inget som hindrar tjocka eller tunna klienter från att via mjukvara agera klient mot en server som är gjord för nollklienter.

2.2 Protokoll för fjärrskrivbord

När fjärrskrivbord används behövs protokoll för att strömma data från servern till klienten. Det finns väletablerade proprietära protokoll, bland annat PCoIP, ICA och RDP. De olika protokollen är utvecklade av olika aktörer, som även levererar helsystemlösningar eller samarbetar med andra leverantörer som gör det. Det finns många fjärrskrivbordsprotokoll utöver de som nämns i detta avsnitt, men dessa är i de flesta fall framtagna för att ge fjärråtkomst åt enskilda datorer snarare än att användas i större klient-server-system.

Ett av de tidigaste exemplen på fjärrskrivbordslösningar är X-protokollet som utvecklades för fönstersystemet X Window System. X Window System är ett tidigt grafiskt användargränssnitt som utvecklades för användning i stordatorvärlden i mitten av 1980-talet och som fortfarande används i stor utsträckning i Unix- och Linux-system. X Window System bygger på en arkitektur där visningen av användargränssnittet är åtskilt från applikationen genom X-protokollet, även när båda körs på samma dator. En dator med X Window System kan därför visa såväl fjärrskrivbord som enskilda fjärrfönster från andra datorer via X-protokollet.

PCoIP (PC over IP) är ett protokoll som har utvecklats av Teradici. Förutom i egna produkter så licensieras protokollet till andra företag som integrerar det i sina produkter. Ett exempel är VMware som använder PCoIP i VDI-lösningen VMware Horizon View.

ICA (Independent Computing Architecture) är ett protokoll utvecklat av Citrix. Protokollet, som inte är bundet till någon plattform, innehåller förutom själva nätverksprotokollet även mjukvara för servern och klienten. Det finns också en utökad variant av teknologin, HDX (High Definition Experience), som bland annat förbättrar möjligheten att använda fjärrskrivbord i fall med låg bandbredd eller lång fördröjning.

Microsoft har utvecklat ett protokoll som heter RDP (Remote Desktop Protocol) som, likt ICA, fungerar på de flesta plattformar och även innehåller mjukvara för klienten och servern. Servermjukvaran finns inbyggd i operativsystemet Windows vilket gör att den är väl spridd. Det finns en utökad version av protokollet som heter RemoteFX som ger en bättre grafisk användarupplevelse genom avancerad kodning av bilddata.

2.3 Leverantörernas vision

Leverantörer av nedbantade klienter, såväl tillverkare som systemintegratörer och konsulter inom området, brukar lyfta fram ett antal fördelar med att använda nedbantade klienter i IT-system. Fördelarna som lyfts fram är att nedbantade klienter påstås ge bättre ekonomi, högre säkerhet, bättre användbarhet och lägre miljöbelastning. I marknadsföringsmaterial, white papers och annan information från leverantörerna återkommer fördelarna och argumenten för dem. Detta avsnitt sammanställer fördelarna och argumenten *så som de framställs av leverantörerna*.

2.3.1 Bättre ekonomi

Tidigt i de tunna klienternas historia framhölls ekonomin som en tungt vägande faktor. En X-terminal var betydligt billigare i inköp än en Unix-arbetsstation på 1980-talet, samtidigt som de senare ofta inte utnyttjades fullt ut och därmed kunde delas av flera användare via X-terminalerna (Engberg & Porcher 1991).

Ekonomin finns kvar i dagens argumentation men fokuserar i stor utsträckning på att nedbantade klienter beskrivs som billigare än tjocka klienter över sin livscykel (så kallad total ägandekostnad, eng. total cost of ownership) (Nexterminal u.å.). De kostnadsbesparingar som leverantörerna pekar på hos klienterna inkluderar exempelvis lägre kostnad för mjukvarulicenser, längre livslängd, lägre energiförbrukning, lägre initial investering och minskad administration (DevonIT u.å.; IT-Logik u.å.; Cure Solutions 2015; Nexterminal u.å.).

Den minskade administrationen inkluderar exempelvis färre fel att avhjälpa i klientmiljön, enklare mjukvaruinstallationer, enklare uppdateringar (inklusive säkerhetsuppdateringar) och lättare hantering av rättigheter i systemet. Mycket av detta bygger på att nedbantade klienter i hög utsträckning administreras centralt, exempelvis genom hantering av klientinställningar, mjukvaruinstallationer, uppdateringar, användarkonton och rättigheter. Tjocka klienter kräver en högre grad av enskild hantering vilket leder till högre kostnad per klient (DevonIT u.å.).

Enklare administration och högre stabilitet hos de nedbantade klienterna gör att användarna mer sällan drabbas av problem och att problemen kan avhjälpas snabbare. Detta ger kostnadsbesparingar i både administrationen av IT-systemet och i verksamheten (Nexterminal u.å.).

När nedbantade klienter används så utförs nyinstallation och uppdateringar av mjukvara samt förbättringar i hårdvarans kapacitet i serverdelen. Detta sparar in arbetstid då det genomförs på ett ställe i IT-systemet istället för att kräva installation på många tjocka klienter (Nexterminal u.å.).

Leverantörerna ger den sammantagna bilden att den totala kostnaden över systemets livscykel sjunker då systemet utrustas med nedbantade klienter. En leverantör säger att den operativa kostnaden i medel går ner med 48 % vid byte till tunna klienter, men att den kan innebära besparingar på upp till 70 % (Nexterminal u.å.). En annan leverantör säger att byte till nollklienter kan leda till besparingar på upp till 95 % (vCloudPoint u.å.).

Användarnas tillgång till systemet förbättras med nedbantade klienter då klienterna är mer tillförlitliga och åtgärder av problem med dessa går snabbare. I och med den centrala administrationen är det lättare att distribuera och installera nedbantade klinter jämfört med tjocka klienter (A-Trac u.å.; VMware u.å.). Detta gör att driftsättning av nya klienter går snabbare, leder till färre problem och blir billigare. Det är även lättare att återställa en nedbantad klient om något går fel och det är lättare att ersätta klienten om den havererar. Nedbantade klienter anses ha längre livslängd då dessa saknar rörliga delar såsom hårddiskar och fläktar (A-Trac u.å.). Detta är speciellt relevant för nollklienter, där vissa leverantörer skriver att nollklienter inte kräver något underhåll alls (VMware u.å.).

2.3.2 Högre säkerhet

Nedbantade klienter beskrivs som säkrare än tjocka klienter. Enligt vissa leverantörer kan tunna klienter inte drabbas av skadlig kod medan andra menar att det endast gäller nollklienter. Det finns leverantörer som går så långt att de säger att nollklienter saknar potentiella angreppsytor och att de är ultrasäkra, vilket innebär att nollklienterna ska vara helt säkra mot IT-angrepp i form av virus och annan skadlig kod (Dell Wyse u.å.; For All IT Services 2017).

Leverantörerna anger att nedbantade klienter är signifikant säkrare än tjocka klienter när det gäller skydd av informationen i systemet. Ett återkommande argument är att informationen skyddas bättre genom att den huvudsakligen hanteras i serverdelen, snarare än att den bearbetas och lagras i klienten (Nexterminal u.å.; Kohlenberg, Ben-Shalom, Dunlop & Rub 2010). Informationen skyddas bättre då skyddet huvudsakligen hamnar hos servrarna, vilket innebär att skyddsåtgärderna kan fokuseras mer. Med tjocka klienter måste varje klient ha ett omfattande skydd för att säkra informationen i systemet (10ZiG 2017).

Nedbantade klienter gör att det blir lättare att hantera användarnas rättigheter i systemet. Exempelvis går det att sätta restriktiva regler om hur data får exporteras av användarna, vilket kan hindra att information lagras på USB-minnen eller andra lagringsmedia som ansluts till klienten. Tunna klienter innebär även att systemet kan hindra användarna från att installera obetrodd mjukvara, vilket begränsar angreppsytan mot systemet (Nexterminal u.å.; Kohlenberg, Ben-Shalom, Dunlop & Rub 2010).

Genom att nedbantade klienter saknar lokal lagring finns ingen risk att data bara sparas lokalt. Därmed blir dataförlusten obefintlig ifall en klient förkommer eller

förstörs (IT-Logik u.å.). Informationen sparas genom central lagring och backup, vilka tillsammans säkerställer att informationen finns kvar i systemet (Nexterminal u.å.).

Eftersom data inte kan sparas lokalt så undviks sekretessförlust om en klient blir stulen, då ingen information följer med i den stulna klienten. Medan tunna klienter har möjlighet att hantera informationen i ett lättillgängligt format, exempelvis ett dokument eller en webbsida, så hanterar nollklienterna endast information i form av bilddata, tangenttryckningar, mushändelser och liknande. Detta gör att det är mer komplicerat att extrahera informationen ur nollklienten.

Den centrala administrationen av nedbantade klienter gör det lättare att installera säkerhetsuppdateringar jämfört med tjocka klienter, där varje klient måste hanteras separat (Nexterminal u.å.). Från den centrala administrationen går det att trycka ut uppdateringar på många klienter samtidigt med liten arbetsinsats. Vissa leverantörer hävdar att nollklienter är säkra till sin natur och därmed inte kräver säkerhetsuppdateringar alls (For All IT Services 2017).

2.3.3 Bättre användbarhet

Nedbantade klienter påstås även ge användarfördelar då de tar liten plats, är tysta och ger låg värmeutveckling vid arbetsplatsen. Genom att ta liten plats frigörs utrymme på skrivbordet och det är möjligt att exempelvis montera klienten på baksidan av skärmen (IT-Logik u.å.; VMware u.å.). Färre saker ger mindre mängd kablar och en renare arbetsplats.

Då nedbantade klienter har färre rörliga delar, såsom fläktar och hårddiskar, så låter de mindre (Nexterminal u.å.). Detta gäller i synnerhet för nollklienter som inte har några rörliga delar alls (VMware u.å.). Minskningen i bakgrundsbuller gör att arbetsplatsen blir lugnare, vilket ger bättre förutsättningar att arbeta koncentrerat.

Den lägre effektförbrukningen hos nedbantade klienter gör att det blir svalare på arbetsplatsen, något som kan förbättra arbetsmiljön (Nexterminal u.å.). Detta är extra fördelaktigt om klienten används i miljöer där det är trångt eller där omgivningstemperaturen är hög.

2.3.4 Miljövänligare

Bland fördelarna med nedbantade klienter tas även miljöaspekter upp. Längre livslängd och enklare uppbyggnad ger lägre miljöpåverkan jämfört med tjocka klienter (Cure Solutions 2015; Citrix u.å.). I system som bygger på nedbantade klienter bestäms prestanda av serverdelen snarare än av klienterna och dessa kan därmed användas under längre tid. Genom den enklare konstruktionen med exempelvis färre mekaniska komponenter såsom fläktar och hårddiskar, så har nedbantade klienter en längre förväntad livslängd (10ZiG 2017).

Lägre energiförbrukning i drift ger en positiv miljöeffekt med nedbantade klienter. Vissa leverantörer anger att energiförbrukningen kan minska med 95–97 % vid byte från vanliga kontorsdatorer till tunna klienter (vCloudPoint u.å.; DevonIT u.å.).

Sammantaget kräver nedbantade klienter mindre naturresurser över systemets livslängd, vilket ger en lägre samlad miljöpåverkan från klienterna.

3 Analys

Detta kapitel innehåller problematiseringar av de aspekter som leverantörerna framhåller som fördelar med nedbantade klienter. Fördelarna som framhävs kan kategoriseras i följande fyra kategorier:

- ekonomi och administration
- säkerhet
- användbarhet
- miljö.

3.1 Ekonomi och administration

Detta avsnitt behandlar de fördelar som leverantörerna framhåller avseende ekonomi och administration. Beskrivningen av dessa fördelar återfinns i sin helhet i avsnitt 2.3.1.

> *Leverantörernas beskrivning: Nedbantade klienter har mindre total ägandekostnad.*

I den bild som flera av leverantörerna ger hänvisas återkommande till siffror från analysföretaget Gartner, där det exempelvis ska gå att läsa att den totala ägandekostnaden i medel sjunker med 48 % vid byte till tunna klienter.[9] Gartner har släppt flera rapporter inom området och resultatet av beräkningarna beror på de förutsättningar som väljs som utgångspunkt. En av dessa rapporter jämför total ägandekostnad för en större VDI-lösning[10] under olika förutsättningar och med olika typer av klienter. Resultatet visar bland annat att en VDI-lösning med tunna klienter i grova drag är kostnadsmässigt likvärdigt med väl nedlåsta och centralt administrerade kontorsdatorer när det gäller större IT-system. De beräkningar som utförts visar på fall med såväl besparingar som kostnads-ökningar vid användning av tunna klienter (Troni, Margevicius & Silver 2010).

En viktig aspekt i de flesta organisationer är att IT-systemen ofta är komplexa och att det inte går att begränsa sig till en typ av klient (van de Kamp 2009). Det kan exempelvis vara lämpligt för vissa användargrupper att nyttja nedbantade klienter, medan andra användargrupper kräver andra typer av klienter. Det kan exempelvis vara säljare eller supportpersonal som reser mycket och därför behöver klienter som klarar av en högre grad av mobilitet, även där det inte finns

[9] De leverantörer som nämner Gartner-rapporten har inte skrivit ut någon tydlig referens. Detta gör att det har varit svårt att identifiera vilken rapport det faktiskt rör sig om.

[10] Gartner-rapporten använder termen *hosted virtual desktop* (HVD), vilket närmast kan översättas till serverbaserade fjärrskrivbord. Beräkningarna baseras på ett system med 2 500 klienter.

tillgång till välfungerande kommunikation med servrarna. Dessa användare utrustas då lämpligtvis med bärbara datorer som används som tjocka klienter i IT-systemen.

När IT-systemen innehåller både nedbantade klienter och tjocka klienter blir den administrativa bördan på vissa sätt dubbel. Systemet kräver en administrativ organisation med tillhörande verktyg och processer för att hantera såväl de nedbantade klienterna som de tjocka klienterna (van de Kamp 2009). Om båda klienttyperna används i samma system finns risken att den totala kostnaden för systemet ökar (Igel u.å.).

En ytterligare faktor är risken för inlåsningseffekter, där organisationen bygger in ett beroende till en leverantör i sina IT-system. När organisationen vill genomföra uppdateringar eller förändringar i systemen finns det en risk att det endast är den ursprungliga leverantörens produkter som kan användas. Denna risk finns oavsett klienttyp, men är mer utpräglad med nedbantade klienter eftersom exempelvis administrativ mjukvara kan vara knuten till tillverkaren av klienten snarare än till det operativsystem som används.

Förutsättningarna för många system som Försvarsmakten använder skiljer sig från den kommersiella världen, vilket påverkar den ekonomiska kalkylen. Systemen är ofta fristående med begränsad omfattning, där systemarkitekturen är enhetlig och endast en typ av klienter används. Dessutom är det sällan som användarna ges friheten att ändra kritiska inställningar eller installera mjukvara på systemen oavsett klienttyp. Sammantaget gör detta att den faktiska skillnaden i total ägandekostnad sannolikt inte är dimensionerande faktor när det gäller klientvalet. Val av klienter görs snarare baserat på andra egenskaper såsom användbarhet samt effekt på sekretesskydd och tillgänglighet.

> *Leverantörernas beskrivning: Nedbantade klienter ger minskad och billigare administration.*

Administration av IT-system är ett omfattande område som inkluderar många arbetsuppgifter. Några av de arbetsuppgifter som ingår är installation och utbyte av utrustning, sökning och åtgärder vid fel, installation och uppdatering av mjukvara samt hantering av användare och deras rättigheter. Arbetsuppgifterna kan avse arbete med såväl klienter som servrar och annan utrustning i systemet.

Det är viktigt att se till helheten när effekterna av ett arkitekturval ska utvärderas, eftersom valet ger följdeffekter i andra delar av systemet. Exempelvis betyder introduktion av nedbantade klienter i regel att central administration blir nödvändig i någon utsträckning (Clephan 2017).

En lösning där användarna nyttjar fristående datorer, utan central administration och med minimala gemensamma funktioner, ger sannolikt en hög administrativ kostnad. Om denna lösning jämförs med en centralt administrerad och kraftigt centraliserad systemlösning med nollklienter och VDI-lösning kan resultatet bli

missvisande, då det är två system med vitt skilda egenskaper som jämförs. Alla klienttyper går att administrera centralt och det är vanligt förekommande inom större organisationer att låsa ner även tjocka klienter så att användaren inte kan installera mjukvara eller göra förändringar av kritiska inställningar. Många inställningar kan göras centralt i en katalogtjänst, exempelvis Microsoft Windows Active Directory, och propageras ut till klienterna. På liknande sätt går det att installera uppdateringar och mjukvara på klienterna.

De inställningar och mjukvaruinstallationer som behöver göras direkt på tjocka klienter kan delvis utföras genom att administratören ansluter till ett fjärrskrivbord på klienten. I kombination med centrala katalogtjänster innebär det att huvuddelen av det administrativa arbetet går att utföra utan att administratören befinner sig på samma plats som klienten.

All form av automatisering och centralisering av administrationen av IT-system innebär en investering som måste vägas mot de effekter som uppnås. Automatisering och centralisering kan i sig leda till en signifikant initial kostnad. I omfattande system med många klienter kan effekterna av investeringen ge stora besparingar i det dagliga arbetet. Det är dock inte klientvalet i sig som leder till besparingarna, snarare är det designval kring administrativa principer och hantering av klienterna på systemnivå som ger dessa effekter.

Variationen i komplexitet och storlek på Försvarsmaktens fleranvändarsystem är stor, från landsomfattande system med tusentals klienter av olika typer till små system med ett fåtal identiska klienter i ett och samma utrymme. Många av systemen är av den senare kategorin och har därmed mindre potential att ge stora besparingar. Därtill kommer hänsyn till andra aspekter såsom tillgänglighet och sekretesskydd av informationen i systemet – det kanske inte är önskvärt att ha för hög grad av centralisering av administrationen. Dessa aspekter diskuteras vidare i avsnitt 3.2.

> *Leverantörernas beskrivning: Nollklienter kräver inget eller väldigt lite underhåll.*

Nollklienterna i sig kräver rimligtvis mindre underhåll än andra klienttyper då de är enkelt uppbyggda och endast innehåller begränsad mjukvara. I och med frånvaron av ett operativsystem minskar underhållet av klienterna, men det försvinner inte helt. Det behövs säkerhetsuppdateringar även för nollklienter och det kan även komma funktionella uppdateringar som behöver installeras på klienterna. Oavsett om uppdateringarna sker ofta eller sällan behövs central administration för att det praktiskt ska gå att genomföra uppdateringarna när det rör sig om mer än några enstaka klienter (van de kamp 2009).

Nollklienter verkar typiskt i samma typ av tekniska omgivning som tunna klienter, exempelvis med en VDI-lösning i systemets serverdel. Resten av systemet kräver därmed samma mängd underhåll oavsett klienttyp.

Leverantörernas beskrivning: Nedbantade klienter leder till lägre investeringskostnad för hårdvara och lägre kostnad för mjukvarulicenser.

Klienter kan vara dyra eller billiga oavsett om de är tjocka eller nedbantade. Det är inte så enkelt att nedbantade klienter har lägre hårdvarukostnad. Nedbantade klienter kan förvisso vara billiga, men det finns även enkla och billiga vanliga datorer. På samma sätt finns dyra nedbantade klienter och dyra datorer med hög prestanda. Dessutom måste alla andra kostnader, exempelvis servrar och nätverksutrustning, räknas in när totalkostnaden beräknas. Den totala kostnaden blir därmed beroende på systemets uppbyggnad och vilka funktioner som det ska utföra.

På motsvarande sätt måste totalkostnaden för mjukvara beräknas över hela systemet, vilket gör att det inte finns något enkelt samband mellan klienttyp och mjukvarukostnad. Licensmodellerna för mjukvara kan vara ganska komplexa vilket gör att samma antal användare inte innebär samma kostnad för olika arkitekturer. I vissa licensmodeller klarar man sig med färre licenser om exempelvis inte alla användare använder en specifik mjukvara samtidigt. Vissa licensmodeller innebär högre pris per licens då den inte körs på en lokal dator. Dessutom tillkommer olika mjukvarulicenser för IT-systemets infrastruktur beroende på hur det är uppbyggt. Det kan exempelvis vara administrations-mjukvara för hantering av klienterna och mjukvara för VDI-lösningar.

Enligt beräkningarna till scenariot som beskrivs i den tidigare nämnda rapporten från Gartner blir kostnaden för mjukvara högre med nedbantade klienter jämfört med tjocka klienter. Hårdvaran beräknas dock bli billigare för de nedbantade klienterna (Troni, Margevicius & Silver 2010).

Leverantörernas beskrivning: Nedbantade klienter har längre livslängd vilket ger färre klientbyten och därmed lägre kostnad.

I teorin stämmer detta då enklare klienter bör hålla längre än mer komplexa klienter med fler komponenter. Nedbantade klienter tenderar dessutom att ha färre mekaniska komponenter, exempelvis fläktar, som riskerar att begränsa livslängden. I system som klarar sig med måttlig prestanda och har en lämplig systemarkitektur verkar det alltså finnas goda utsikter för att nedbantade klienter har en längre livslängd.

I praktiken finns dock fler parametrar att ta hänsyn till. Nya versioner av server-mjukvaran kan innebära att det tillkommer nya tekniker som påverkar klienterna. För att kunna nyttja dessa nya tekniker kan det krävas att klienterna behöver uppgraderas. Det kan även vara så att de befintliga klienterna utgör flaskhalsen när det gäller förbättringar i systemets prestanda. Det finns därmed risk att nedbantade klienter behöver bytas ut innan de är utslitna varpå de får en livslängd som är likvärdig med tjocka klienter (Bass 2012).

Leverantörernas beskrivning: Nedbantade klienter har lägre energiförbrukning vid drift vilket ger lägre driftkostnad.

Enklare klienter tenderar att förbruka mindre energi än komplexa klienter, så detta påstående stämmer. Skillnaden mellan nedbantade klienter och enklare datorer, av den typ som vanligtvis återfinns på kontor där det inte finns några speciella prestandabehov, har dock minskat då datorerna har blivit mer energieffektiva. En allt högre andel av de tjocka klienter som säljs idag är dessutom bärbara datorer, vilket ytterligare minskar gapet (Statista u.å.). Skillnaden mellan tjocka och nedbantade klienter kan därmed vara relativt liten. Nollklienter har vanligtvis låg energiförbrukning och kan ge en signifikant skillnad i förbrukning jämfört med tjocka klienter (Ibrahim, Kliazovich, Bouvry & Oleksiak 2016).

När beräkningskraften flyttas från klienten till servrarna krävs mer kraftfulla servrar, vilket drar mer energi. I större IT-system, där många klienter som var och en har relativt lågt behov av beräkningskraft delar på servrarnas kapacitet, kan besparingarna bli stora. I mindre IT-system, där ett fåtal klienter nyttjar en server, är besparingspotentialen mindre.

Då beräkningskraften och därmed energiförbrukningen koncentreras till serverhallen finns även risk att det sammantagna kylbehovet ökar. När värmeutvecklingen fördelas mellan klienterna är det möjligt att denna kan hanteras naturligt av miljön. I serverhallar behövs ofta en aktiv kylning, vilket kan kräva mycket energi om ingen naturlig källa till kyla finns tillgänglig.

I de fall där IT-systemet saknar egna servrar, exempelvis om det ansluts till någon form av molntjänst utanför organisationen, så flyttas energikostnaden för serverdriften till den kostnad som organisationen betalar för molntjänsten.

Under rätt förutsättningar kan byte till nedbantade klienter leda till stor energibesparing under drift. Detta är dock inte en självklarhet, då olika förutsättningar och designval i systemen påverkar energiförbrukningen.

3.2 Säkerhetsaspekter

Detta avsnitt behandlar de fördelar som leverantörerna framhåller avseende säkerhet. Beskrivningen av dessa fördelar återfinns i sin helhet i avsnitt 2.3.2.

3.2.1 Skydd av systemet

Leverantörernas beskrivning: Nedbantade klienter kan inte drabbas av skadlig kod. Nollklienter saknar dessutom helt angreppsytor för skadlig kod.

Där mjukvara finns, så finns alltid risk för skadlig kod. Det gäller både nollklienter och tunna klienter. Även de nollklienter som saknar operativsystem

har en mjukvara som styr de hårdvarunära funktionerna (s.k. firmware). Den mjukvaran kan också drabbas av skadlig kod och behöver uppdateras med säkerhetspatchar. Skadlig kod kan även verka dolt i arbetsminnet under tiden enheten är i drift.

En nedbantad klient är kopplad antingen till en tjock klient (som en KVM-förlängare) eller till en virtuell maskin på en server. Oavsett vilket så är den nedbantade klienten en ingångsväg till en installation av ett operativsystem. Användaren av den nedbantade klienten kan föra in skadlig kod på samma sätt som om det vore en tjock klient användaren använde, exempelvis med ett smittat portabelt media eller via smittade webbsidor (om klienten har internetaccess). Skadlig kod kan sedan spridas vidare i nätverket. Om det finns anslutna filservrar så kan skadlig kod sprida sig även via dessa.

Det finns flera exempel på sårbarheter i nedbantade klienter. Exempelvis så finns en sårbarhet i en tunn klient där en angripare kan gå förbi behörighetskontrollen och få tillgång till alla filer[11]. Det finns sårbarheter i nollklienter som möjliggör lokala användare att få högre behörigheter[12]. Ett annat exempel är en sårbarhet i VMwares ESXi, en vanlig plattform för virtuella maskiner, där sårbarheten tillåter en angripare från en virtuell maskin att köra godtycklig kod på värd-maskinen[13]. De sårbarheter som tagits upp i detta avsnitt är exempel, men det framgår ändå att nedbantade klienter inte är helt säkra eller saknar angreppsytor.

> *Leverantörernas beskrivning: Nedbantade klienter kan skyddas mot obetrodd mjukvara med hjälp av reglering av användar- och administratörsrättigheter.*

Att begränsa rättigheterna för användarna så att de inte kan installera program är en effektiv metod för att försvåra införandet av skadlig kod. För ytterligare åtgärder kan vitlistor och svartlistor införas som bestämmer vilka program som får respektive inte får köras. Dessa säkerhetsfunktioner är dock inte unika för nedbantade klienter. Det går att utföra motsvarande konfiguration i en infrastruktur med tjocka klienter då de också kan, och oftast är, administrerade centralt.

> *Leverantörernas beskrivning: Med nedbantade klienter skyddas informationen i systemet bättre då skyddet huvudsakligen hamnar hos servrarna.*

Leverantörerna framhåller att vid användning av nedbantade klienter kan skydds-åtgärderna fokuseras på de centrala servrarna. Vid användning av en infrastruktur med tjocka klienter behöver varje klient ett eget, omfattande skydd.

[11] CVE-2015-2124
[12] CVE-2015-2124, CVE-2013-2339
[13] CVE-2017-4903

En klient måste dock alltid skyddas eftersom den ger en väg in i serverdelen. Användaren kan därför föra in skadlig kod även via en nedbantad klient. En obehörig användare hindras dock från vissa typer av attacker, exempelvis extrahering av information från den lokala hårddisken i de fall klienten saknar hårddisk.

Innehållet i kommunikationen mellan klient och server förändras vid ett byte från tjocka till nedbantade klienter. Med tjocka klienter skickas paket med känslig data mellan klient och server. De kan avlyssnas och manipuleras (s.k. man-in-the-middle-attacker). Nedbantade klienter, som endast för över bild, ljud, mushändelser och tangentbordstryckningar, kan synas försvåra för en angripare men leder inte till någon väsentligt högre säkerhet. Oavsett om IT-systemet använder nedbantade eller tjocka klienter måste kommunikationen skyddas i samma grad.

Det är inte enbart tekniska aspekter som har betydelse för skyddet av informationen då även användarnas beteende är viktigt. En undersökning som Intel har utfört visar att användare med nedbantade klienter med central lagring i större utsträckning väljer att skriva ut information på papper, vilket kan leda till informationsläckage om dessa papper hamnar i orätta händer (Kohlenberg, Ben-Shalom, Dunlop & Rub 2010).

När lagring och behandling av information görs i serverdelen istället för i klienterna koncentreras de kritiska funktionerna i systemet. Därmed ökar möjligheten för en angripare att göra allvarlig skada på systemet, då angrepp mot serverdelen kan få omfattande konsekvenser. När en stor mängd information behandlas på samma ställe är värdet för angriparen stort, vilket motiverar mer resurskrävande angrepp. En ny hotbild har skapats där angriparen potentiellt skulle kunna tillgripa helt andra typer av angrepp som är betydligt mer avancerade, komplexa och långsiktiga. Dessa kan vara mycket svåra att skydda sig mot och kräva en mycket hög skyddsnivå.

> *Leverantörernas beskrivning: En nedbantad klient saknar lokal lagring och därför uppstår ingen dataförlust om klienten förloras.*

Detta är endast delvis korrekt då alla klienter har någon form av lokal lagring. Lagringsutrymmet kan vara litet, exempelvis hos nollklienter som i regel saknar hårddisk och endast har ett litet lagringsutrymme för sin egen mjukvara. Det finns dock nedbantade klienter med betydligt mer omfattande lagringsutrymme, såväl för operativsystem och applikationer som för användardata. Om intentionen med införandet av nedbantade klienter är att undvika lokal lagring så krävs ett noggrant val av lösning. När det finns behov av att säkerställa att inga användardata kan sparas lokalt, exempelvis när sekretessbelagd information behandlas, så krävs speciella åtgärder. Det kan innebära att utveckla specifika högassuransklienter eller att granska funktionen hos befintliga klienter.

Användning av klienter där ingen lagring sker lokalt får säkerhetsmässiga effekter. Om en klient blir stulen förloras ingen information vilket kan ha många fördelar för en verksamhet. I fält skulle det exempelvis innebära att data endast behöver skyddas i serverdelen för att förhindra informationsförlust eller röjande av sekretessbelagd information. I en kontorsmiljö skulle data exempelvis kunna skyddas i en låst serverhall så att kontorsplatserna inte behöver vara lika väl skyddade mot stöld eller tillgrepp. System placerade i högre informationssäkerhetsklasser kan kräva att användarna låser in sina tjocka klienter eller hårddiskar i ett säkerhetsskåp efter användning. En nedbantad klient med central lagring kan ge bättre användbarhet och förenkla regelefterlevnaden när användarna inte behöver låsa in sina datorer. Att lagra data centralt innebär dock krav på anpassade säkerhetsfunktioner för serverdelen och att kommunikationen mellan servrar och klienter skyddas. Central lagring kan även innebära en allvarligare hotbild, se diskussionen i sista stycket under föregående leverantörsbeskrivning.

Viss centralisering av data kan uppnås även vid användning av tjocka klienter. Data kan styras om så att specifika filkataloger lagras på servern, antingen exklusivt eller som spegling. Det skulle skydda mot dataförlust, men inte sekretessförlust, då spår av data kan finnas lagrad på den lokala, fysiska hårddisken i klienten. En viss nivå av skydd mot informationsstöld kan dock uppnås genom att kryptera hårddiskarna i klienterna.

> *Leverantörernas beskrivning: Med nedbantade klienter går det att skydda data i systemet genom inaktivering eller begränsning av portabelt media.*

Genom att begränsa vilka portabla medier som får användas i systemet till endast betrodda typer minskar risken att skadlig kod tar sig in i systemet från exempelvis smittade USB-stickor. För högre tilltro kan all import och export av information från portabla media inaktiveras. Det försvårar även otillåten utförsel av information ur systemet.

Att använda detta som säkerhetsfunktion är inte unikt för nedbantade klienter. Det går att begränsa och inaktivera portabla media även i tjocka klienter och med ett effektivt administrationssystem så är det lika enkelt som för nedbantade klienter.

3.2.2 Säkerhetsadministration och uppdatering

> *Leverantörernas beskrivning: Den centrala administrationen av nedbantade klienter gör att det blir lättare att installera säkerhetsuppdateringar.*

Att centraliserat skicka ut uppdateringar och säkerhetspatchar är inte unikt för nedbantade klienter. Ett centraliserat system med nedbantade klienter kan ge en enklare uppdateringshantering eftersom klientmjukvaran som körs på servern (gästoperativsystemet eller virtuella maskinen) kan uppdateras på servern när

som helst. Tjocka klienter tar istället emot uppdateringar när de är inkopplade till nätverket och måste vara igång under uppdateringsprocessen.

Användarna bör dock ändå tillfrågas när det passar med uppdateringar så att inget arbete går förlorat. En fördel med nedbantade klienter är att klienten inte behöver vara igång för uppdateringar som sker på servern. Installation kan således planeras under natten och påverkar då inte användarens produktivitet.

Att ha central administration innebär att uppdateringar snabbt kan skickas ut i systemet. Att skicka ut uppdateringar till alla klienter samtidigt är dock inte alltid bra då det finns en viss risk för att uppdateringen inte fungerar korrekt i systemet. Det kan därmed vara bättre att rulla ut uppdateringar i omgångar istället för att uppdatera alla klienter på en gång för att begränsa problemen som kan uppstå (Kohlenberg, Ben-Shalom, Dunlop & Rub 2010).

Nedbantade klienter som har ett lokalt operativsystem och lokala applikationer kräver säkerhetsuppdateringar av den lokala mjukvaran (For All IT Services 2017). Dessa uppdateringar behöver utföras på liknande sätt som i en infrastruktur med tjocka klienter, dvs. klienten behöver vara påslagen och inkopplad i nätverket för att ta emot mjukvara. Alternativt kan den installeras fysiskt på plats av lokal administratör.

> *Leverantörernas beskrivning: Nollklienter kräver inga säkerhetsuppdateringar.*

Alla typer av nedbantade klienter behöver uppdateringar. Nollklienter saknar lokalt operativsystem men har ändå en lokal mjukvara som sköter de basala funktionerna (s.k. firmware) och som behöver uppdateras. Hos nollklienter körs operativsystemet istället på en server. Oavsett var operativsystemet är lokaliserat så behöver det uppdateringar och säkerhetspatchar med jämna mellanrum. Den begränsade mjukvaran på nollklienterna innebär dock att det blir mindre mängd mjukvara att uppdatera på klienterna.

3.3 Användbarhet

Detta avsnitt behandlar de fördelar som leverantörerna framhåller avseende användbarhet. Beskrivningen av dessa fördelar återfinns i sin helhet i avsnitt 2.3.3.

> *Leverantörernas beskrivning: Med nedbantade klienter frigörs utrymme på skrivbordet. Det blir färre saker vilket ger färre kablar och en renare arbetsplats.*

Att byta från en tjock klient till en nedbantad klient innebär inte någon större skillnad vad gäller frigörande av yta på arbetsplatsen. Det krävs fortfarande en

klientmaskin med strömkabel och kabelanslutningar till skärm, mus och tangentbord. Om en nedbantad klient av typen som går att montera på baksidan av skärmen väljs så kan viss skrivbordsyta frigöras.

När det finns flera system som användaren nyttjar kan det i vissa fall vara möjligt att använda samma nedbantade klient för att ansluta till flera av dessa system. En sådan lösning, där flera klientmaskiner byts ut mot en maskin, kan frigöra betydande skrivbordsyta. Om systemen tillhör olika informationsdomäner tillkommer dock säkerhetsproblem då det ställer krav på informationsseparation.

> *Leverantörernas beskrivning: Nedbantade klienter har lägre energiförbrukning, vilket ger en svalare arbetsplats.*

På många platser i världen är hög temperatur på arbetsplatsen ett problem, särskilt under varma årstider. I en serverhall där många servrar genererar mycket värme, kan värmeproblem finnas under hela året och oavsett utomhusklimat. Hög värme innebär stress på kroppen och kan leda till försämring på mentala funktioner såsom uppmärksamhet, humör och omdöme (Arbetsmiljöverket u.å.-a). Leverantörernas beskrivning stämmer därmed överlag bra med verkligheten när det gäller klienterna, men flytten av beräkningskraft kan leda till ökade kylbehov eller sämre användarmiljö i serverhallen. Detta resonemang är relaterat till diskussionen om energiförbrukning i slutet av avsnitt 3.1.

Personal med vanligt kontorsarbete, som inte behöver datorer med hög beräkningsprestanda, har sällan problem med värmeutveckling från sina klienter oavsett typ. Personal som behöver datorer med mycket beräkningskraft kan ha klienter som ger ett besvärande värmetillskott i rummet. I sådana fall kan en nedbantad klient kopplad till en server placerad i ett annat rum minska värmeutvecklingen från klienten. Servern kräver då komponenter med mycket beräkningskraft, speciellt om det är flera användare som ska dela på serverns resurser.

> *Leverantörernas beskrivning: Nedbantade klienter har färre rörliga delar och låter därför mindre. Minskat buller ger en behagligare arbetsmiljö.*

En tystare arbetsplats ger en bättre arbetsmiljö med mindre stress (Arbetsmiljöverket u.å.-b). Klienter med passiv kylning och utan mekanisk hårddisk skulle gynna arbetsmiljön på många arbetsplatser.

Kontorsarbetare som upplever att tjocka klienter låter för mycket skulle kunna hjälpas av en passivt kyld, nedbantad klient utan rörliga delar. En tjock klient med passiv kylning och utan mekanisk hårddisk skulle dock ge samma resultat. Datorer med passiv kylning har dock generellt sämre beräkningskraft, så det kan vara svårt att uppnå både hög prestanda och låg ljudnivå i en tjock klient. Skulle detta vara nödvändigt krävs antagligen specialbyggda tjocka klienter, där komponenter med hög beräkningskraft kombinerats med tystgående fläktar eller vattenkylning.

3.4 Miljö

Detta avsnitt behandlar de fördelar som leverantörerna framhåller avseende miljö. Beskrivningen av dessa fördelar återfinns i sin helhet i avsnitt 2.3.4.

> *Leverantörernas beskrivning: Nedbantade klienter består av färre och enklare komponenter och kräver mindre resurser vid tillverkning.*

Enklare klienter ger naturligt en lägre miljöpåverkan vid tillverkning då de består av färre och i viss utsträckning enklare komponenter. Nedbantade klienter kan även vara lättare och mindre än tjocka klienter, varvid miljöpåverkan från transporter minskar.

För att bedöma den totala miljöeffekten måste hela systemet tas i beaktande då övrig utrustning såsom servrar och kommunikationsutrustning också ger miljöpåverkan. Hur det ser ut i praktiken beror således på vilka komponenter som ingår i systemet.

> *Leverantörernas beskrivning: Nedbantade klienter har längre livslängd och kräver därmed färre byten av hårdvara vilket ger lägre miljöpåverkan.*

Den faktiska livslängden hos klienterna diskuteras i avsnitt 3.1, där det noteras att livslängden inte enbart beror på den enklare tekniska uppbyggnaden hos nedbantade klienter. Under gynnsamma förutsättningar kan nedbantade klienter ha signifikant längre livslängd än tjocka klienter, men det finns även fall där skillnaden i livslängden är svårare att avgöra. I de fall där livslängden i praktiken blir längre så blir även klienternas miljöpåverkan från tillverkning, transport, etc. mindre.

> *Leverantörernas beskrivning: Nedbantade klienter har lägre energiförbrukning i drift och ger därmed lägre miljöpåverkan.*

Energiförbrukningen diskuterades i avsnitt 3.1. Gynnsamma förutsättningar kan leda till stora besparingar, men systemets uppbyggnad och förutsättningar påverkar hur stor den faktiska förbrukningen blir. Detta är återigen en fråga som måste undersökas för varje system som helhet.

4 Scenarier

I detta kapitel presenteras tre fiktiva scenarier, som är inspirerade av Försvarsmaktens olika verksamheter. Scenarierna är valda för att representera flera olika verksamhetstyper hos Försvarsmakten. De utmaningar som diskuteras i de respektive scenarierna är:

- distribuerade system med otillförlitlig bandbredd
- obehöriga användare med fysisk access
- fältmiljö med begränsad strömförsörjning och risk för fysiskt angrepp.

4.1 Distribuerade system med begränsad bandbredd

Följande scenario tar upp ett stort system med geografiskt spridda klienter, där användaren har god kontroll på sin miljö och behöver kunna använda systemet oavsett om kommunikationen till servern fungerar.

> *Ett geografiskt distribuerat system bearbetar och lagrar sekretessbelagd information. Användarna arbetar enskilt på tjocka klienter. Systemet är implementerat i geografiskt åtskilda kontorsmiljöer som alla har yttre skalskydd. Användarna har enskilda låsbara rum med säkerhetsskåp.*
>
> *Användarna delar data med varandra över ett nätverk med nationell täckning. Sammankopplingen sker via VPN-anslutning över en egen IP-tjänst. Nätverket har begränsad bandbredd och kan ibland vara otillgängligt.*

Eftersom nätverket som systemet kopplas samman över har begränsad bandbredd och tillgänglighet, så finns behov av en systemlösning som inte är beroende av att nätet är stabilt och ständigt tillgängligt.

Nedbantade klienter kräver realtidsdataöverföring mellan server och klient. Det är viktigt att nätverket är stabilt och har liten fördröjning, för att användaren ska få en bra användarupplevelse. Nedbantade klienter skulle därför inte fungera bra i detta scenario. Valet av tjocka klienter är således rimligt eftersom det minimerar realtidsberoendet av nätverket.

Användarna har tillgång till enskilda låsbara rum med säkerhetsskåp. Det gör det möjligt för varje användare att låsa in sin dator när den inte används. Risken för informationsläckage eller informationsförlust kopplad till permanent lagring i en tjock klient är därför hanterad.

4.2 Obehöriga användare med fysisk access

Följande scenario beskriver ett system som används i en typisk ledningscentral, där det förekommer flera olika IT-system med olika informationsmängder och egna operatörer.

> *Ett lokalt ledningsstödsystem hanterar och lagrar sekretessbelagd information. Användarna behöver snabbt kunna växla mellan olika arbetsuppgifter, där endast delar av arbetet innebär att ledningsstödsystemet används. I ledningscentralen där systemet används finns även andra system med andra användare. Användarna från de andra systemen är inte behöriga att ta del av informationen i ledningsstödsystemet.*
>
> *Ledningsstödsystemet är uppbyggt med nollklienter, vilket innebär att all information är lagrad i en separat serverhall. Ledningsstödsystemet är konfigurerat så att användarna inte kan använda portabelt media.*

Då det förekommer personer utan behörighet till systemet i ledningscentralen så har dessa fysisk tillgång till klienterna. Därmed finns det behov av att minimera de fysiska angreppsytorna på klienterna för att skydda den sekretessbelagda informationen i systemet. I och med att operatörerna behöver kunna växla uppgifter snabbt finns inte möjlighet att låsa in klienterna eller eventuella hårddiskar mellan användningstillfällena.

Exponeringen av information i ledningsstödsystemet minimeras genom att en nollklientlösning används istället för tjocka klienter. Detta gör att informationen inte lagras permanent i klienten vilket gör att operatören inte behöver låsa in klienten när den lämnas obevakad. Servern med all information installeras i ett låst utrymme dit endast behöriga har tillträde. Endast bild, ljud, mushändelser och tangentbordstryckningar skickas mellan klient och server. Exponeringen av informationen minimeras alltså genom att obehöriga inte kan komma åt servrarna i det låsta utrymmet. Med en sådan arkitektur hindras angripare från att extrahera sekretessbelagd information genom fysisk åtkomst till fast lagringsmedia.

Beroende på konfiguration så kan portabelt media kopplas in på nollklienten. Om användaren ska hindras från detta (exempelvis som skydd mot skadlig kod) är det viktigt att använda korrekta inställningar.

4.3 System i fält

Följande scenario beskriver ett system som används på en flyttbar stabsplats, med risk för fientliga aktiviteter och avsaknad av fast infrastruktur.

En stabsplats i fält består av ett antal containrar och stabstält. Staben använder ett IT-system som behandlar sekretessbelagd information.

Systemet är uppbyggt med ett trettiotal nollklienter med tillhörande server. Nollklienterna har ingen hårddisk och kan därför inte lagra något. Istället lagras och hanteras all sekretessbelagd information i servern. Servern är installerad i en servercontainer och nollklienterna utgör arbetsplatser i omgivande stabstält. Nätverket mellan servercontainern och omgivande stabstält har god bandbredd och tillförlitlighet.

Stabsplatsen befinner sig i en utsatt miljö. Målet, om stabsplatsen behöver överges med kort varsel, är att förlora så lite information som möjligt och minimera sannolikheten för röjande av sekretessbelagd information. Med en nollklientlösning behöver endast servern tas med, eftersom det endast är där information lagras. Beroende på assuransnivån hos den tekniska lösningen kan det räcka att ta med sig hårddiskarna från servern.

Eftersom nätverket mellan servercontainern och stabstälten har god bandbredd och stabilitet, så finns inget kommunikationstekniskt hinder för att använda nollklienter.

I en fältmiljö där strömförsörjningen kan vara begränsad, kan det vara viktigt med strömsnål utrustning. Nedbantade klienter har lägre strömförbrukning än tjocka klienter. Dock kräver nedbantade klienter en server som utför de tunga beräkningarna. Med andra ord flyttas strömförbrukningen från klienterna till servern. I ett varmt klimat kan förflyttningen av strömförbrukningen från arbetsplatserna till servercontainern vara arbetsmiljömässigt fördelaktig, eftersom det minskar värmeutvecklingen hos användarna.

Nedbantade klienter minskar också behovet av avbrottsfri kraft (UPS[14]). I scenariot räcker det sannolikt med att ha UPS för servrarna. Om en nollklient går ner är sessionen fortfarande uppe på servern och kan återupptas genom att användaren loggar in i sin session igen när strömavbrottet är över. Om det ändå bedöms nödvändigt med UPS även för nollklienterna så behövs mycket mindre kapacitet än i en lösning med tjocka klienter.

[14] Eng. uninterruptible power supply

5 Marknadsöversikt

I detta kapitel listas några kommersiella klientlösningar som har fokus på säkerhet. Produkter har identifierats genom sökningar efter *secure* och *trusted* i kombination med *thin* och *zero client*. För att lösningen ska anses ha fokus på säkerhet så har vi krävt att det ska finnas någon slags certifiering i detta avseende. Det räcker inte med att ordet *secure* ingår i beskrivningen.

Informationen som presenteras om de olika klienterna är huvudsakligen hämtad från marknadsföringsmaterial som är tillgängligt på internet. Därför presenteras ingen strukturerad beskrivning av de olika klienterna, utan informationen återspeglar istället de egenskaper som företagen själva väljer att lyfta fram. Inte heller görs någon utvärdering av säkerheten för de olika produkterna. Målet med kapitlet är istället att visa att det finns produkter som fokuserar på säkerhet och ge exempel på hur dessa ser ut. Listan med beskrivna klienter är kort eftersom det endast finns ett begränsat antal produkter som är certifierade med avseende på säkerhetsegenskaper.

5.1 Amulet Hotkey DXZ-A nollklientserie

Amulet Hotkey erbjuder nollklienter[15] som har certifierats av National Cyber Security Center i Storbritannien. Certifieringen[16] visar att produkten tagits fram enligt god, kommersiell säkerhetspraxis. Klienten gör det möjligt för användare att ansluta säkert till fysiska eller virtuella datormiljöer med fjärrskrivbord.

Om nollklienterna kombineras med KVM-switchar från Amulet Hotkey kan klienterna ges tillgång till resurser på separata nätverk i olika informations-domäner eller med olika informationssäkerhetsklasser.

Enheten är en tillståndslös klient som minimerar angreppsytan på klienten. Några funktioner är intelligent USB-avstängning och stöd för optisk nätverksanslutning. Det finns även modeller som har inbyggda smartkortläsare för att säkerställa att smartkortsdata stannar kvar i klienterna.

5.2 Raytheon Trusted Thin Client

Raytheon erbjuder en mjukvaruimplementation för tunna klienter[17] som går att installera på många kommersiellt tillgängliga tunna klienter. Mjukvaran ersätter

[15] https://www.amulethotkey.com/products/client-devices-endpoints/cpa-certified-secure-zero-clients/ [2018-12-06]
[16] https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa [2018-12-06]
[17] https://www.raytheon.com/capabilities/products/trusted-thin-clientr-remote-access-implementation [2018-12-06]

då den tunna klientens medföljande mjukvara men använder fortfarande de vanliga fjärrskrivbordsprotokollen från exempelvis Citrix, Microsoft eller VMware. Raytheons lösning är bland annat ackrediterad för att hantera information som klassificerats upp till nivån Top Secret i USA.

I lösningen ingår även en så kallad distributionskonsol (eng. distribution console) som kopplar samman klienter och servrar. Distributionskonsollen är en anslutningspunkt för klienterna och placeras typiskt i servermiljön. Klienterna kopplar upp sig till distributionskonsollen som tillhandahåller den fysiska anslutningen till ett eller flera bakomliggande nät i serverdelen. Distributionskonsollen har även uppgiften att upprätthålla separationen mellan näten.

5.3 SINA Terminal H Client III

SINA Terminal H Client III[18] är en tunn klient som är godkänd för upp till EU Secret. Den tillverkas av Secunet Security Networks AG och är en disklös klient för behandling av data från olika informationssäkerhetsklasser i upp till sex parallella sessioner. Klienten har inbyggt stöd för VPN-tunnlar som används för att skydda kommunikationen med servrarna. Klienten är skyddad mot manipulation.

[18] https://www.secunet.com/en/products-solutions/sina-terminal/ [2018-12-06]

6 En separerad nollklient

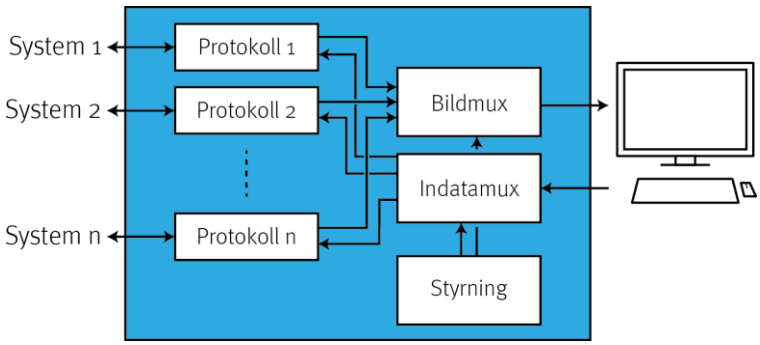
Som framgår av rapporten finns det ett antal olika aspekter som kan innebära problem när kommersiella klientlösningar används inom Försvarsmaktens IT-system. En av de mer specifika aspekterna när det gäller användning inom Försvarsmakten är behovet av separation mellan informationsdomäner. Det innebär i praktiken att IT-systemen måste vara fysiskt åtskilda för att upprätthålla separationen. I och med detta följer att användarna, som ofta behöver tillgång till flera olika informationsdomäner, även måste använda flera olika IT-system. Det i sin tur leder till att användarna måste ha klienter för alla dessa system tillgängliga samtidigt på sin arbetsplats.

Vanliga, kommersiella klienter är byggda enligt den civila marknadens krav och har inte de säkerhetsfunktioner som krävs för att skydda sekretess på högre nivåer. Exempelvis finns inga garantier för att sekretessbelagd användardata inte finns kvar i klienten när användaren loggar ut eller klienten stängs av. I kapitel 5 beskrivs klienter som har någon sorts säkerhetscertifiering, men de är inte godkända som säkerhetslösning för skydd av svensk försvarssekretess.

Ett sätt att få tillgång till en lämplig klient är att ta fram en Försvarsmaktsspecifik lösning, med de separationsmekanismer och de säkerhetsfunktioner som behövs för att uppfylla Försvarsmaktens behov. Med tanke på sekretesskraven finns det fördelar med en nollklient, då det innebär att klienten exponeras för minimalt med sekretessbelagd information. Om klienten dessutom ska användas för åtkomst till flera separata, bakomliggande IT-system i olika informations-domäner krävs att klienten upprätthåller separationen. För detta krävs att datavägarna mellan nätverket och användaren hålls åtskilda i tillräckligt hög grad.

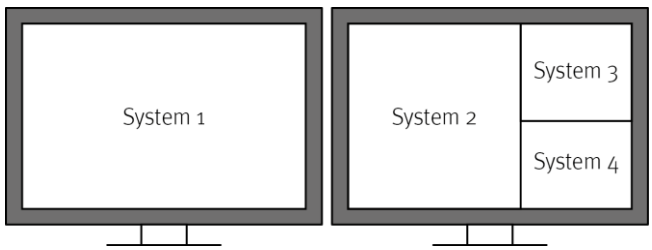
Med en Försvarsmaktsspecifik klient finns möjlighet att designa denna så att övriga säkerhetskrav uppfylls, exempelvis gällande krav kring RÖS-skydd och TEMPEST.

Figur 3 visar ett förslag på övergripande arkitektur för en separerad, säker nollklient. Ett antal fysiskt åtskilda nätverksanslutningar (betecknade *System 1–n* i figuren) ger möjlighet att ansluta klienten till flera separata, åtskilda IT-system. Trafiken på respektive nätverksanslutning hanteras av separata protokollmotorer (betecknade *Protokoll 1–n* i figuren), där respektive IT-systems klientprotokoll hanteras. Protokollen kan exempelvis vara RDP eller PCoIP men behöver inte nödvändigtvis vara samma för alla anslutna system. Protokollmotorerna extraherar bilddata från servrarna för att presentera på de lokala bildskärmarna samtidigt som de skickar användarens indata till servern för det system som användaren är aktiv i för tillfället.



Figur 3. Övergripande arkitektur för en separerad nollklient.

Från protokollmotorerna skickas bilddata vidare till en enkelriktad bildmux för att sedan presenteras på en del av en eller flera skärmar. Klienten kan visa bild från samtliga IT-system samtidigt, men tillåter endast att användaren är aktiv i ett IT-system i taget. Figur 4 visar ett exempel på hur virtuella skrivbord från fyra separata IT-system kan visas på två skärmar anslutna till samma klient.



Figur 4. Exempel på uppdelade skärmar för flera samtidiga system.

Användarens indata, exempelvis tangentbordstryckningar och mushändelser, skickas endast till det aktiva IT-systemet. Detta görs genom en indatamux som utgör den separationsmekanism i klienten som spärrar så att användarens indata endast kan nå den protokollmotor som är kopplad till det aktiva IT-systemet.

Klienten kan också ge tillgång till andra typer av anslutningar, exempelvis USB. Av praktiska skäl bör dessa anslutningar vara parallella och åtskilda hela vägen från server till individuellt fysiskt gränssnitt på klienten. Om anslutningarna delade fysiskt gränssnitt skulle användaren vara tvungen att ta bort eventuella anslutna enheter innan denne växlar aktivt IT-system i klienten.

Det är viktigt att klienten ger fullgott stöd till användaren så att denne med säkerhet vet vilket IT-system som är aktivt. I dagens lösningar, där användaren nyttjar separata klienter för olika IT-system, så vet användaren vilket system denne arbetar i utifrån vilken klient som används. När flera IT-system samsas om en klient försvinner denna distinktion och det blir nödvändigt att få till

tydligheten på ett annat sätt. Detta är en viktig fråga att hantera, men den har ingen betydelse för den tekniska säkerhetslösningens realiserbarhet.

7 Diskussion

Inom industrin finns en trend mot att centralisera IT-systemens funktionalitet och öka abstraktionsnivån genom en större frikoppling mellan fysisk maskin och funktion. Genom virtualiseringstekniken har möjligheterna att låta mjukvara definiera allt fler funktioner i IT-systemen ökat kraftigt. När funktionen frikopplas från hårdvaran blir gränserna allt mer flytande för vad som gör vad i systemen. Virtualiserade servrar kan flytta mellan fysiska maskiner i olika serverhallar via mjukvarudefinierade nätverk där topologin kan ändras utan att flytta några fysiska kablar. De fysiska klienterna utgör en viktig komponent för i stort sett alla IT-system då de utgör gränsytan mellan användarna och systemet. Nedbantade klienter är en naturlig komponent i virtualiserade IT-miljöer då mycket av klientfunktionerna flyttas från den fysiska världen – det vill säga användarens dator – till den virtuella världens servrar.

I avsnitt 2.3 beskrivs en närmast utopisk vision av hur praktiskt, effektivt och säkert ett IT-system blir om det baseras på nedbantade klienter och där servrar får stå för den största delen av funktionaliteten. I kapitel 3 görs en mer kritisk analys av denna vision och det visar sig att verkligheten inte är så bra som den bild leverantörerna utmålar. Det handlar om begränsningar på flera nivåer. Dels är lösningar som bygger på nedbantade klienter inte så bra som visionen påstår, dels behövs ofta tjocka klienter hos en delmängd av medarbetarna varför systemet ändå måste hantera tjocka klienter. I en militär kontext visar det sig dessutom att den fulla säkerhetsnyttan med nedbantade klienter inte alltid kan uppnås, då tilltron till produkternas implementation sällan är tillräcklig för att det ska gå att lita på dem fullt ut.

IT-säkerhet brukar ofta diskuteras utifrån de tre aspekterna konfidentialitet, riktighet och tillgänglighet. Klienternas egenskaper påverkar alla tre aspekterna på olika sätt beroende på ett flertal faktorer såsom systemets uppbyggnad, miljö och hotbild. Med nedbantade klienter går det att centralisera hanteringen av information till serverdelen av systemet, så att klienterna exponeras för minimalt med sekretessbelagd information. Dock går det inte att eliminera exponeringen helt, varför tilltron till klientens skydd av informationen ändå måste vara hög. Likaså påverkar klienterna riktighetsskyddet i systemet genom att de kan påverka såväl informationen i systemet som systemet i sig. Även tillgängligheten påverkas då klienterna i olika utsträckning blir beroende av systemets infrastruktur för sin funktion. Klienterna har sannolikt en mer utsatt position än övrig utrustning i systemen då de behöver vara tillgängliga i användarmiljön, vilket ofta ger en högre exponering mot potentiella angrepp.

Det krävs i regel god tilltro till klienternas implementation för att kunna lita på deras inbyggda skyddsmekanismer i så stor utsträckning som Försvarsmaktens behov innebär. Väldesignade nedbantade klienter kan vara fördelaktiga då dessa innebär mindre angreppsyta än tjocka klienter. Mindre mängd mjukvara ger

generellt sett mindre mängd allvarliga sårbarheter i produkten. Dock finns det inga klienter som helt eliminerar riskerna, varför klienterna måste ha lämpliga skydd som implementerats med tillräckligt hög tilltro.

En aspekt som är extra problematisk i Försvarsmakten är separation av informationsdomäner, där skilda mängder med sekretessbelagd information hanteras. Generellt sett kan olika informationsdomäner inte samexistera på gemensamma hårdvaruresurser, vilket gör att många systemlösningar som är praxis i den kommersiella sektorn inte kan användas i Försvarsmaktens system. Exempel på serverlösningar som sällan kan användas är samlokalisering och molntjänster. Motsvarande problem drabbar även klienterna då en och samma klient inte kan nyttjas för att nå flera system i olika informationsdomäner.

För nedbantade klienter handlar problematiken kring informationsdomäner huvudsakligen om två saker: dels måste data raderas när den inte längre behövs, dels måste separationen upprätthållas mellan IT-system i olika informationsdomäner. En knäckfråga i sammanhanget är tilltron till att klienten och dess funktioner är implementerade korrekt och därmed hanterar problematiken tillräckligt väl.

Nollklienter saknar per definition permanent lagring av användardata, men utan noggrann granskning kan det inte uteslutas att det finns något permanent minne som kan innehålla rester av sekretessbelagd information även när klienten har slagits av eller kopplats bort. För att uppnå tillräcklig tilltro till avsaknaden av permanent minne måste klienten sannolikt ha byggts specifikt för att ha denna egenskap, och den måste ha ackrediterats på vanligt sätt.

För att en nollklient ska kunna växla mellan flera olika informationsdomäner med sekretessbelagd information så måste växlingsfunktionen upprätthålla separation mellan de olika domänerna, något som är ett erkänt svårt problem. Om klienten ska kunna visa upp flera olika tjänster samtidigt blir problemet ännu svårare. Det skulle dock vara tacksamt med en nollklient vars avsaknad av permanent minne är verifierat och där det är möjligt att samtidigt vara ansluten till flera tjänster på ett sätt så att separationen upprätthålls med tillräcklig säkerhet.

Analysen i kapitel 3 visar hur svårgripbar frågan om klientval är och bredden i de faktorer som påverkar valets förutsättningar och resultat. Alla fyra områden som analysen utgår från – ekonomi, säkerhet, användbarhet och miljö – kan påverka eller vara styrande i valet. Avvägningen mellan de olika faktorerna är systemspecifik, vilket gör det svårt att ge några allmängiltiga riktlinjer om de olika klienternas lämplighet i olika situationer. För vissa system kan ett gott resultat uppnås med båda klienttyperna. För andra system kan inte alla viktiga behov tillgodoses fullt ut oavsett om tjocka eller nedbantade klienter används. I båda fallen måste olika aspekter vägas mot varandra för att välja den klienttyp som är mest lämplig med hänsyn till den totala systemlösningen.

Referenser

10ZiG (2017). *What is a thin client and what are its benefits* [blog]. https://www.10zig.com/resources/vdi-blog/what-is-a-thin-client [2018-11-29]

A-Trac (u.å.). W*hy a Business Should Consider a Thin Client Solution.* http://www.a-trac.com/documents/HP/Enterprise/datasheet/Why%20a%20Business%20Should%20Consider%20a%20Thin%20Client%20Solution_contact.pdf [2018-12-06]

Arbetsmiljöverket (u.å.-a). *Temperatur och klimat.* https://www.av.se/inomhusmiljo/temperatur-och-klimat/ [2018-11-29]

Arbetsmiljöverket (u.å.-b). *Ljud och akustik.* https://www.av.se/inomhusmiljo/ljud-och-akustik/ [2018-11-29]

Bass, S. (2012). *Why thin clients and zero clients haven't lived up to "last PC you'll ever buy" hype. (Part 1 of 2)* [blog]. https://www.brianmadden.com/podcast/Why-thin-clients-and-zero-clients-havent-lived-up-to-last-PC-youll-ever-buy-hype-Part-1-of-2 [2018-12-06]

Citrix (u.å.-a). *Six myths of zero-client computing* [white paper]. https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/six-myths-of-zero-client-computing.pdf [2018-11-29]

Clephan, S. (2017). *What Makes a Thin Client Enterprise Grade? Part 1: Management* [blog]. https://www.igel.com/technology-trends/makes-thin-client-enterprise-grade-part-1-management/ [2018-12-06]

Cure Solutions (2015). *3 reasons to consider thin clients in the workplace* [blog]. https://www.curesolutions.com/newsletter-content/3-reasons-to-consider-thin-clients-in-the-workplace [2018-11-29]

Dell Wyse (u.å.). *Dell Wyse Zero and ThinOS.* https://be01.cp-static.com/objects/pdf/5/53b/992928_1_thin-clients-blade-pcs-dell-wyse-d90d7-909654-02l.pdf [2018-11-16]

DevonIT (u.å.). *Benefits of using thin clients.* http://www.devonit.com/thin-client-education/benefits-of-using-thin-clients [2018-11-29]

Digi International Inc. (u.å.). *Zero-Client Computing* [White paper]. https://www.digi.com/pdf/wp_zeroclientcomputing.pdf [2018-11-29]

Eidenskog, D. & Karresand, M. (2017). *Risker med virtualisering av IT-system.* FOI-R--4448--SE.

Engberg, B. & Porcher, T. (1991). X Window Terminals. *Digital Technical Journal, 3(4).* ftp://ftp.linux-mips.org/pub/linux/mips/people/macro/DEC/DTJ/DTJ402/DTJ402PF.PDF [2018-11-29]

For All IT Services (2017). *Thin clients vs ultra thin clients: the difference* [blog]. https://www.forallit.nl/blog/thin-clients-vs-ultra-thin-clients/ [2018-11-29]

Ibrahim, A. A. Z. A., Kliazovich, D., Bouvry, P. & Oleksiak, A. (2016). Virtual Desktop Infrastructures: Architecture, survey and green aspects proof of concept. *Seventh International Green and Sustainable Computing Conference (IGSC)*, ss.1-8. doi: 10.1109/IGCC.2016.7892624

Igel (u.å.). *Switching from a PC environment to thin clients.* https://www.igel.com/switch-pc-to-thin-clients/ [2018-12-06]

IT-Logik (u.å.). *5 reasons why a thin client is king.* https://www.it-logik.com/5-reasons-thin-client-king/ [2018-11-29]

Kohlenberg, T., Ben-Shalom, O., Dunlop, J. & Rub, J. (2010). *Evaluating thin-client security in a changing threat landscape* [white paper]. Intel Information Technology. https://www.intel.com/content/dam/doc/white-paper/intel-it-enterprise-security-thin-client-paper.pdf [2018-11-29]

Nexterminal (u.å.). *Why use thin clients.* http://nexterminal.dk/en/why-use-thin-clients [2018-11-29]

Statista (u.å.). *Shipment forecast of tablets, laptops and desktop PCs worldwide from 2010 to 2022.* https://www.statista.com/statistics/272595/global-shipments-forecast-for-tablets-laptops-and-desktop-pcs/ [2018-12-06]

Troni, F., Margevicius, M. A. & Silver, M. A. (2010). *Total cost of ownership comparison of PCs with hosted virtual desktops, 2011 Update.* Gartner RAS Core Research Note G00209403. http://img2.insight.com/graphics/pl/gartner/article12.pdf [2018-11-29]

van de Kamp, J. (2009). *The fundamental flaws of thin clients* [blog]. https://www.brianmadden.com/opinion/The-fundamental-flaws-of-thin-clients [2018-11-29]

vCloudPoint (u.å.). *vCloudPoint Zero Client Computing.* https://www.vcloudpoint.com/zero-client-introduction/ [2018-11-29]

VMware (u.å.). *Key considerations in choosing a zero client environment for View Virtual Desktops in VMware Horizon* [white paper]. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-top-five-considerations-for-choosing-a-zero-client-environment.pdf [2018-11-29]

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se