HANDELSHÖGSKOLAN VID GÖTEBORGS UNIVERSITET

Behörighetsadministration i Windows NT
-faktorer som kan påverka säkerheten

Stefan Svensson
Institutionen för informatik

EXAMENSARBETE II, 10p
Vårterminen 1999
Handledare: Birgitta Ahlbom

Abstrakt

Syftet med uppsatsen var att undersöka de faktorer som påverkar administrering av användares rättigheter och behörigheter i Windows NT och som kan påverka säkerheten. Problem att på ett rationellt och säkert sätt tilldela rätt person lämplig behörighet kan påverka säkerheten i systemet. Det kan t.ex. resultera i att viktig information sprids eller modifieras, vilket kan ge oönskade konsekvenser för en verksamhet. Resultatet i undersökningen baseras på kvalitativa metoder såsom observation, simulering och intervjuer. Undersökningen visade att det finns delar i behörighetssystemet som inte fungerar på ett tillfredsställande sätt. Behörighetssystemet är för komplext uppbyggt, svåröverskådligt och innehåller oklara prioritetsregler. Windows NT passar därmed bäst i en relativt statisk miljö. I de fall Windows NT används i dynamiska miljöer kan man lindra problemen genom god planering, klara förutsättningar och rutiner för en konsekvent administration. Uppsatsen är skriven på Unisys Information Service i Alingsås.

Innehållsförteckning

Informationssäkerhet blir allt viktigare för näringsliv och förvaltning. Snabb teknisk utveckling skapar hela tiden nya möjligheter och problem. Den utveckling som pågått sedan den första elektroniska datorn såg dagen ljus 1942 har varit enorm. För bara tjugo år sedan sparades ofta dokument i pärmar på företagen, och i de fall som de innehöll extra viktig information användes bastanta säkerhetsskåp för förvaring. Idag blir det allt vanligare att verksamhetskritiska dokument lagras i olika datorsystem som förväntas skydda mot obehörig åtkomst.

Bakgrund

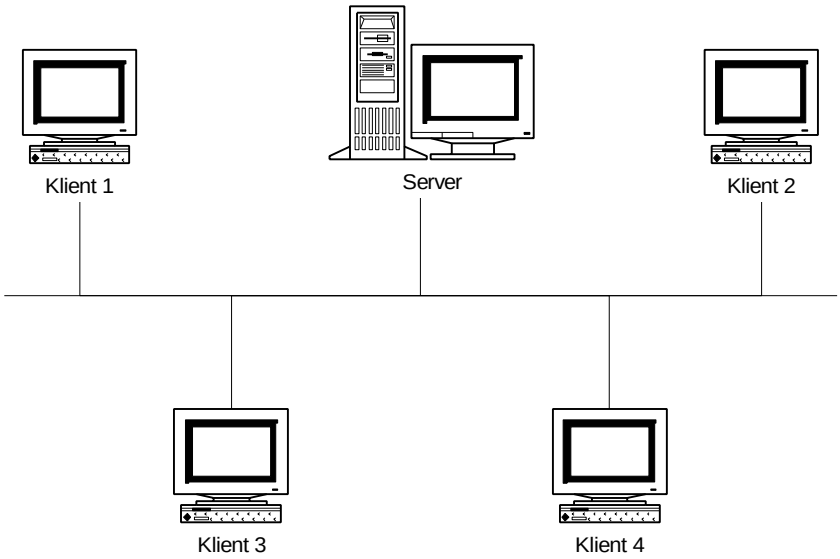
Blickar man bakåt och granskar arkitekturen hos de äldre datorsystemen och jämför dessa med dagens ser man en stor skillnad. I början stod datorerna i en egen datorhall med speciellt golv, kylanläggning och ansvarig underhållspersonal. Man använde hålkort för att köra program i en s.k. batchterminal som bestod av skrivare och hålkortsläsare. Man upptäckte efter ett tag att det var praktiskt att koppla ihop flera batchterminaler till en och samma dator. De första nätverken såg dagens ljus och bestod således av en dator med en eller flera tillhörande batchterminaler. När sedan datorerna blev mer avancerade med högre kapacitet krävdes en högre grad av dialog med användarna.

De interaktiva terminalerna utvecklades i ständig takt, man fick behov av att flera användare skulle kunna komma åt datorn samtidigt. Man anslöt ytterligare användare genom att koppla fler och fler kablar till terminalerna vilket resulterade i en situation där kabeldragningen blev en komplex uppgift med stora kabelhärvor som följd. Man löste problemet genom att låta all trafik gå genom en och samma kabel. För att detta skulle vara möjligt kopplade man närstående terminaler till en särskild kontrollenhet vars uppgift var att styra kommunikationen. Denna lösning kallas *kluster* (från engelskans cluster som betyder klunga eller anhopning). Klusterprincipen användes främst i minidatorsystem där datorkraften var centrerad till terminalservrar och terminalerna var s.k. "dumma terminaler", de kunde endast ta emot indata eller presentera utdata, d.v.s. de kunde inte bearbeta data på egen hand.

Datorernas storlek minskade samtidigt som kapaciteten ökade och så småningom uppstod arbetsstationen. En arbetsstation var ett mellanting mellan en persondator och en terminalserver. Då den hade stor kapacitet för beräkningar och hantering av grafik användes den huvudsakligen till CAD (datorstöd design) och hållfastighetsberäkningar. Dessa arbetsstationer bör inte förväxlas med de klient-datorer som ingår i dagens nätverk och som man i dagligt tal benämner just arbetsstationer (efter engelska Workstation). Arbetsstationerna tjänade i första hand en användare åt gången men så upptäckte man att genom att koppla ihop arbetsstationerna med varandra så kunde man nyttja den samlade datorkraften. Den största skillnaden mellan datornät med terminaler och datornät med arbetsstationer är att alla terminaler är underordnade terminalservern, till skillnad från arbetsstationer som har likvärdig status i nätverket. Mellantinget av dessa två alternativ är vad vi dag benämner client/server.

Client/server

Client/server-system baseras på som namnet antyder på en server och en eller flera klienter. Klienter är vanligtvis de datorer i nätverket som används som arbetsplats. En klient kan vara en godtycklig typ av dator och kallas ibland för nätdator. De har ofta lägre kapacitet och används till mindre krävande tillämpningar. Varje klient kopplas till en server. En server är en kraftfull dator vars uppgift är att hantera tunga beräkningar och lagra stora mängder information. En server har till uppgift att tillhandahålla olika tjänster nätverket. Det kan finnas en server för varje tjänst i nätverket t.ex. filserver, skrivarserver, kommunikationsserver etc. Det är idag emellertid vanligt att flera tjänster kombineras i en och samma server.



Figur 1. Exempel på nätverksarkitektur av typ client/server.

Client/server-system kan byggas kontrueras på olika sätt beroende på vilken uppgift som skall lösas. I många fall krävs en komplex samverkan mellan olika komponenter för att realisera ett client/server-system. SIG Security (1993) kategoriserar komponenterna i en fysisk, logisk, ansvarsmässig samt administrativ struktur.

Den fysiska strukturen innehåller följande komponenter:

- Klientdatorer (stationära och bärbara). Både med och utan minnesenheter.
- Nätadapter eller nätkort för anslutning till lokala nät. Modem för att ansluta bärbara klienter via telenätet.
- Nätkablage. T.ex. koaxial-, partvinnad- eller fiberkabel för att ansluta arbetsstationer till annan lokal utrustning såsom skrivare, servrar mm.
- Aktiva nätkomponenter såsom repeaters, bryggor, routers och gateways används för att koppla samman delnät till större nät.
- Serverdatorer. Utgör bearbetnings- och lagringsresurser i nätet.

Den logiska strukturen består av:

- Arbetsstationens operativsystem. Hanterar stationens hårdvara. Exempel på operativsystem är MS-DOS, MacOs, OS/2, UNIX eller Windows NT.
- Nätkommunikation. Hanterar kommunikationen mellan alla enheter som är anslutna i nätverket.
- Serverns operativsystem. Hanterar resurserna i serverdatorn. Exempel på operativsystem är MS-DOS, OS/2, UNIX, VAX/VMS och Windows NT.
- Nätoperativsystem. Innehåller funktioner för att användaren skall kunna nå filer, databaser mm utanför den lokala datorn. Exempel på nätoperativsystem är Novell NetWare, UNIX och Windows NT.

Man talar om följande ansvarsområden:

- Verkställande ledningen har det övergripande ansvaret för verksamheten.
- Samordningsansvarig ansvarar för att det finns en definierad och tillämpad strategi för hur strukturerna skall vara utformade.
- Info-systemansvarig (systemägare) har huvudansvaret för att informationssystemets aktuella ändamål uppfylls på ett korrekt sätt. Ansvarar för att systemet följer den definierade strategin.
- Informationsägare. Ansvarar för att informationen i systemet samlas in, skapas och används på ett korrekt sätt.

De administrativa rollernas uppgifter är:

- Informationsadministration. Planera långsiktigt för informationstillgång och försörjning.
- Nätadministration. Omfattar dagliga uppgifter såsom skapa, underhålla och övervaka kommunikationsvägar.
- Serveradministration. Definiera nya nätadresser, underhålla nätoperativsystem mm.
- Databasadministration. Innebär underhåll, och behörighetsadministration inom databasprodukterna.
- Administration av arbetsstationer. Omfattar stöd till användare t.ex. anslutning, konfigurering, uppgradering mm.
- Behörighetsadministration. Hanterar användarnas behörighet i nätoperativsystemet. Lägger till, tar bort och modifierar användarkonton.

Hedemalm (1998) anger att fördelarna med client/server-system bl.a. är:

- Möjlighet att köra gemensamma tillämpningar från servern.
- Enklare handhavande vid uppgraderingar och systemunderhåll.
- Information kan lagras på gemensam plats, säkerhetskopieringen blir därmed enklare.
- Dela gemensamma resurser såsom skrivare, scanners och annan kringutrustning.
- Ökande möjligheter till spridning av intern information och elektronisk kommunikation.

Denna teknik har en potential att till en relativ låg kostnad tillåta en flexibel fördelning av bearbetnings- och lagringskapacitet i utrustningar. Nu börjar informationen spridas mellan olika servrar, och gränserna mellan olika delsystem börjar suddas ut. Idag sitter användarna vid kraftfulla arbetsstationer, kopplade till en eller flera servrar som i sin tur sitter anslutna till andra.

Programvaror

Även programvarorna skiljer sig väsentligt från förr. I SIG Securitys årsbok (1999) finns fakta som visar på den snabba utvecklingen inom detta område. Där anges att förr var programvaror förhållandevis små och antalet programrader räknades i till tusentals rader kod. Ett helt Unix-system t.ex. bestod i mitten av 80-talet av ca 25.000 rader kod. Idag har antalet rader i programvarorna formligen exploderat och programmen har blivit gigantiskt stora och komplexa. Antalet programrader anges istället i miljontals (Windows NT 5/ Windows 2000 uppges innehålla runt 25 miljoner rader).

Vad blir då följderna av denna utveckling? Programvarorna kommer med stor sannolikhet fortsätta att växa, nätverken kommer att breda ut sig och allt mer kritiska applikationer byggs in i företagens infrastruktur. Men för att detta skall fungera krävs kvalitet och detta åstadkoms genom att högre krav ställs på både utvecklare, leverantörer och integratörer. Dessutom måste man börja ställa krav på företagen som använder tekniken. Säkerhet är ett kvalitetsattribut och någon form av certifiering (som ISO 9000 eller BS 7799) kommer att krävas från exempelvis aktieägare och andra intressenter anser SIG Security.

Administration

Även säkerhetsarbetet har förändrats oerhört mycket, framför allt under 90-talet. Säkerhetsarbetet har utvecklats från att vara inriktat på fysiska driftsgöromål till att skydda värdefull information från obehörig manipulering eller spridning. Det handlar inte längre endast om fungerande rutiner för säkerhetskopiering så att man slipper göra om några vekors arbete om hårddisken skulle krångla. Nu handlar det ofta om att skydda databaser eller register av betydande värde. Säkerhetsadministration och behörighetsregistrering har successivt vuxit till egna funktioner med förgreningar över hela företaget. Målet är att förse medarbetare med tillgång till rätt information i sitt dagliga arbete. Otvivelaktigt är det också så att säkerhetsarbetet kommer att fortsätta förändras mycket även de närmaste åren. Man behöver inte gå så långt som till börser eller banker för att hitta verksamheter där tillgången till datorsystemen är kritiska. Sjukvård, offentlig förvaltning, försäkringsbolag och även vanliga företag som sysslar med försäljning har hela sin verksamhet datoriserad. Nu för tiden existerar knappt prislistor, kundregister, lagerregister mm i pappersform.

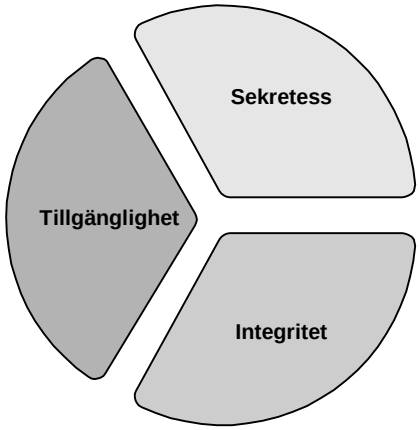
Säkerhet är i nuläget viktigare än någonsin. I SIG Security (1999) jämför man företag utan uttalad säkerhetspolicy och utan målmedvetet säkerhetsarbete med företag som saknar dörrlås eller brandskydd. God säkerhet är redan och kommer att bli ett allt viktigare konkurrensmedel.

Säkerhet, hotbild och konsekvenser

Vad är säkerhet?

Det finns egentligen inte någon enhetlig eller officiellt antagen definition av säkerhet. SIG Security (1999) hänvisar till följande definition från Information Technology Security Evaluation Criteria [ITSEC]. Säkerhet är:

- *"Sekretess. Att hålla information och resurser otillgängliga för obehöriga.*
- *Integritet. Förhindrande av otillåten modifiering av information och resurser.*
- *Tillgänglighet. Att hålla information och resurser tillgängliga för behöriga."* (s. 9)



Figur 2 Ingående delar i definitionen av säkerhet enligt [ITSEC].

SIG Security har också en egen informel definition av säkerhet som kan vara lättare att ta till sig:

- *"Säkerhet: Egenskap eller tillstånd som innebär skydd mot okontrollerad insyn, förlust eller påverkan, oftast i samband med medvetna försök att utnyttja eventuella svagheter, eller*
- *Ett system är säkert om man kan lita på det och om det alltid beter sig som förväntat."* (s. 9)

Man delar upp begreppet säkerhet i tre olika typer: Fysisk säkerhet. Handlar, som namnet antyder, om att skydda systemet mot fysiska angrepp som stöld eller åverkan. Det kan röra sig om lås, passerkort, brandlarm, korrekt back-up-tagning skapande av en alternativ driftmiljö etc. Logisk säkerhet. Innefattar alla mekanismer och all den teknik som tas till hjälp för att lösa säkerhetsproblemen som uppstår i organisationen. Organisatorisk säkerhet. Handlar om hur systemet ska administreras och hur drift och underhåll av systemet ska ske. I princip inbegriper detta all mänsklig interaktion med systemet och omfattar de krav man måste ställa på användare och driftspersonal.

Hotbild

Intrångssäkerhet och "hackare" är ständigt i fokus i säkerhetsdebatten. Men minst lika viktig är den interna säkerheten. Dåligt utbildade medarbetare kan ställa till en hel del, och än mer förstås den som är illvilligt sinnad. Problemet ligger i att systemen faktiskt ska vara lättillgängliga för de anställda**.** Intern säkerhet handlar om att skydda sina system mot inre hot, oavsett om de grundar sig i slarv eller om det är kriminella handlingar. Warman (1993) skriver:

> *"Another example is the myth that a great dela of technical knowledge is required in order to commit a computer crime. In fact, the evidence that has been collected tends to suggest the opposite. Actual cases indicate that computers are also misused by people with minimal technical knowledge, bur who are authorized to process data in a particular way."* (s. 77)

Det finns goda skäl att se över säkerheten kring användningen av datorer och digitalt lagrad information. Riskerna går i regel att spåra till interna situationer snarare än externa. De helt avgörande riskerna med datasäkerhet bottnar i den mänskliga faktorn. I publikationen IEEE (Instsitute of Electrical and Electronics Engineers) Spectrum (Aug/91) (citerad i Galli & AlfaNet Communications (1992)) anges att de förluster som orsakas av bristande säkerhet kan delas in i tre riskgrupper:

- Angrepp från individer utanför organisationen 3%
- Misstag från egen personal 65%
- Avsiktliga handlingar av egen personal 31%

Om vi lägger ihop misstag och avsiktliga handlingar från egen personal så är det interna hot det i särklass största problemet. Den snabba utvecklingen av Internet på senare år har säkerligen inneburit en kraftig ökning för de yttre hoten, men är fortfarande inte i närheten av andelen interna brott. Snarare är det så att interna brott antagligen är större än vad statistiken visar. Warman (1993)

> *"In practise, howewer, we cannot say whit any certainty that computer security violation are predominantly caused by insiders. What we can say is that of those violations which are detected, admitted by the organization, and the the instigator identified; the majority seem to be caused by insiders."* (s. 78)

Konsekvenser

Konsekvenserna av ett dataintrång är ofta mycket dyrbart. Det beror inte endast på de direkta och uppenbara skador som intrånget förorsakar. Bratt (1998) anger att det dessutom alltid en finns risk att den som tagit sig in i systemet även gjort annat som kan ge skador vid ett senare tillfälle och som sprider sig till andra delar av systemet.

Därmed blir det nästan alltid nödvändigt att stänga av den del av systemet som drabbats direkt och de delar som inte kan uteslutas är eller kan bli skadade. Avstängningen av system på detta sätt medför enligt Bratt ofta betydande kostnader för verksamheten i form av stillestånd och låg produktivitet. Blir intrånget dessutom känt extern kan kostnader för minskad tilltro till verksamheten tillkomma.

Företagsbeskrivning

Uppsatsen är skriven hos Unisys Information Service i Alingsås som ingår Unisys inc. Företaget Unisys består av mer än 33.000 anställda föredelade över 100 länder. I Sverige finns 170 medarbetare. Prioriterade marknadssegment är Bank & Finans, Telekommunikation, Offentlig sektor, Transport och Publishing. Unisys Information Service är i huvudsak inriktade på outsourcing av stordatordrift och hotell för servrar. Verksamheten omfattar datakommunikation på avancerad nivå såsom nätverksintegration, fjärrhantering av nätverk, utveckling, drift, underhåll och support. Kundkretsen utgörs av medelstora och stora företag.

Syfte och frågeställningar

Syfte

Syftet med denna uppsats är att för Unisys räkning undersöka de faktorer som påverkar administrering av användares rättigheter och behörigheter i Windows NT och som i förlängningen kan påverka säkerheten.

En klar och koncis administration av användare kompletterad med en utarbetad strategi där man vet vilka säkerhetsmässiga brister och styrkor lösningarna i behörighetsadministrationen innehåller är mycket värdefullt för Unisys. Genom att skapa en bild över problemområdet kan man utifrån den vidta åtgärder för att uppnå en erforderlig säkerhet.

Jag vill med studien för egen skull fördjupa mig inom ämnet och få en större kunskap om Windows NT i allmänhet och problematiken kring behörighetsadministration i synnerhet.

Rapporten vänder sig även till de som arbetar med säkerhetsfrågor eller med införande och användning av client/server -tillämpningar inom ett företag eller annan organisation. T.ex. administratörer, säkerhetsansvariga, systemutvecklare och nätanvändare. Rapportens innehåll kan också vara av intresse för dem som arbetar med distribuerad databehandling, kommunikationsnät mm, utan för den skull implementera client/server-system.

Problem

Mycket av de resurser som leverantörer och användarföretag lägger ned på säkerhetsmekanismer i system gäller behörighetskontroll, d.v.s. möjligheten att reglera vem som kan använda en systemresurs samt på vilket sätt detta kan ske.

Den ökande decentraliseringen av ansvar för drift och utveckling, som möjliggörs med client/server-tekniken och som ofta kan vara ett mål i sig, innebär en risk för att säkerhetsfrågorna inte får en tillräcklig genomlysning och blir allt svårare att administrera.

Ur en administratörs perspektiv måste de funktioner som skall användas ge en klar överblick över vilka resurser som skyddas, vilka användaridentiteter som definierats, vilka rättigheter en viss identitet har, vem som kommer åt en given resurs mm.

Om det innebär svårigheter att på ett rationellt och säkert sätt tilldela rätt person lämplig behörighet så kan det påverka säkerheten i systemet. Det kan t.ex. resultera i att viktig information sprids eller modifieras vilket kan ge oönskade konsekvenser för verksamheten.

Frågeställning

- Vilka faktorer påverkar behörighetsadministrationen i Windows NT?
- Kan de i förlängningen påverka säkerheten i systemet?
- Vad bör man tänka på vid behörighetsadministration för att trots dessa faktorer erhålla en acceptabel säkerhetsnivå?

Avgränsning

Client/server är ett mycket omfattande begrepp. Uppsatsen fokusera på system där man använder klienter och Servrar med Windows NT som nätoperativsystem. Arbetet behandlar administration av användare på en övergripande nivå och inte hur man går tillväga rent praktiskt. Då uppsatsen i första hand fokuserar på användare i systemet begränsas hotbilden att gälla interna hot. När termen säkerhet används i uppsatsen baseras den på definition av ITSEC. Framför allt sekretess och integritet.

Studien avser i första hand de problem som relateras till behörighetsadministration i nätstrukturer där domänmodeller med förtroendeförhållanden används. Den behandlar således inte strukturer grundade på arbetsgrupper. Ingen hänsyn tas heller till komplementprodukter från tredje part utan inriktas på Windows NT i sin grundversion.

Metod

Huvudsyftet med en vetenskaplig rapport är att redovisa ett utfört forskningsarbete på ett så klart och koncist sätt som möjligt. I en akademisk uppsats bör en allmänt erkänd metod användas för att undersöka problemområdet med anknytning till en teori- och modellvärld. Detta kapitel avser att ge en förklaring till vald metod. För att läsaren skall kunna följa resonemangen och förstå hur det föreliggande arbetet har gått till beskrivs det totala tillvägagångssättet.

Rapportens disposition

För att rapporen skall bli så lätt att läsa som möjligt beskrivs strukturen i rapporten. Den består av följande fem kapitel: Introduktion, Metod, Teoretiskt ramverk, Resultat, Diskussion och slutsats. I Introduktion introduceras läsaren i bakgrunden till problemområdet samt får frågeställning och syfte presenterat. I nästa kapitel, Metod, beskrivs förfarandet i undersökningen kopplat till den vetenskapliga undersökningsmetod som ligger till grund för arbetet. I kapitlet Teoretiskt ramverk redogörs för de begrepp och termer som arbetet baseras på. Därefter presenteras resultatet från observation, simulering och intervjuer i kapitlet Resultat, vilket följs av avslutande diskussion med slutsats. I slutet av rapporten finner man slutligen en lista med referenser. I Bilaga medföljer bilagor innehållande Windows NT:s olika objekts rättigheter, säkerhetsmodellen i Windows NT samt de intervjufrågor som låg till grund för intervjuerna.

Undersökningsmetod

Den typ av rapport som vanligtvis förknippas med forskning är resultatet av ett empiriskt arbete, d.v.s. ett material har på något specificerat sätt samlats in varefter det bearbetats

Ämnet Informatik omfattar både teknik och människa samt hur de samverkar. Det handlar Inte bara hur man bygger system utan också hur man använder dem och hur de påverkar organisationer. Följande arbetsdefinition av området informatik föreslås av Le Duc (1998):

> *"…Informatics is the discipline concerned with information technology and its use. Information technology per se is not exclusively in focus in the field of informatics. The boundary of informatics is wider, namely a combination of knowledge on IT design with knowledge on the use of IT. Informatics requires thus both technical knowledge and knowledge of the human use of technology. Furthermore, informatics is not only descriptive - it has a normative dimension comprising heuristic rules of thumb on how to design and adapt information systems with the most appropriate technology for a given user context. "* (s. 97)

När man gör en undersökning är det viktigt att man använder sig av lämpliga metoder för problemområdet. Inom Informatik är det extra viktigt då ämnet fokuserar på både människa ock teknik samt framför på samspelet däremellan. Man talar om två olika sätt att utföra en undersökning. Deduktion är den klassiska vetenskapliga metoden där man utifrån en referensram, t.ex. en teori eller en modell, formulerar hypoteser som testas mot verkligheten. Med induktion går man åt det motsatta hållet, nämligen från observationer i verkligheten till generalisering inom en teoretisk referensram.

Validitet och reliabilitet

Det är av stor vikt att undersökningen uppfattas som pålitlig d.v.s. att det inte var en tillfällighet som gjorde att det redovisade resultatet uppnåddes. Pålitlighet uppnås genom att undersökningen utförs med ett verktyg som har förmåga att undersöka det som är avsikten. Det är viktigt att den valda metoden är reliabel och lämplig för att skapa en valid modell. Utan en valid och lämplig modell får man ingen validitet i sitt arbete trots att man använder sig av en inom forskningen accepterad och vedertagen metod. Det samma gäller även det motsatta förhållandet, man inte får en valid modell om man inte använder sig av en lämplig metod

Man skiljer normalt på två metoder då man skall samla information. Kvalitativa och kvantitativa metoder. Le Duc (1996, s 42): hänvisar till följande tabell från Holme & Solvang (1991, s. 86).

Tabell 1. Jämförelse mellan kvantitativa och kvalitativa metoder.

Kvantitativa metoder	Kvalitativa metoder
1. Precision: forskaren eftersträvar en maximalt god avspegling av den kvantitativa variationen.	1. Följsamhet: forskaren eftersträvar bästa möjliga återgivning av den kvalitativa variationen.
2. Ringa information om många undersökningsenheter; går på bredden.	2. Riklig information om få undersökningsenheter; går på djupet.
3. Systematiska och strukturerade observationer, t ex. enkät med fasta svarsalternativ.	3.Osystematiska och ostrukturerade observationer, t ex. djupintervju eller intervjumall utan fasta frågor eller svarsalternativ.
4. Man intresserar sig för det gemensamma, det genomsnittliga eller representativa.	4. Man intresserar sig för det säregna, det unika eller det eventuellt avvikande.
5. Avstånd till det levande: insamlingen av information sker under betingelser som skiljer sig från den verklighet man vill undersöka.	5. Närhet till det levande: insamlingen av information sker under betingelser som ligger nära den verklighet man vill undersöka.
6. Man intresserar sig för åtskilda variabler.	6. Man intresserar sig för sammanhang och strukturer.
7. Beskrivning och förklaring.	7. Beskrivning och förståelse.
8. Åskådare eller manipulator: forskaren iakttar fenomenet utifrån och strävar efter en roll som observatör. Variationen för variabler kan manipuleras fram.	8. Deltagare eller aktör: forskaren observerar fenomenet inifrån. Han vet om att han påverkar resultaten genom det faktum att han är närvarande. Han kan även deltaga som aktör.
9. Jag-det-relation mellan forskaren och den undersökte.	9. Jag-du-relation mellan forskaren och den undersökte.

Kvantitativa metoder

För det kvantitativa perspektivet är huvudargumenten: reliabilitet, representativitet, reproducerbarhet, kumulativitet, verifierbarhet och inte minst tillgången till klart angivna metodregler. En kvantitativ metod är formaliserad och strukturerad. Metoden grundar sig på beräkningar och absoluta resultat. Man samlar in stora mängder av data utifrån kriterier som styrs av frågeställningarna. Oftast sker insamling av data genom något sorts formulär med en begränsad mängd svarsalternativ. Därefter analyseras datan utefter färdiga statistiska tekniker, och man får i slutändan ett resultat i procent och tabellform. Den kvantitativa metoden kan man t.ex. använda då man vill ta undersöka hur många i en population som tycker eller beter sig på ett speciellt sätt. Kvantitativa resultat är ofta generaliserande, vilket betyder att man kan överföra slutsatserna i resultatet på en större population än den man har undersökt.

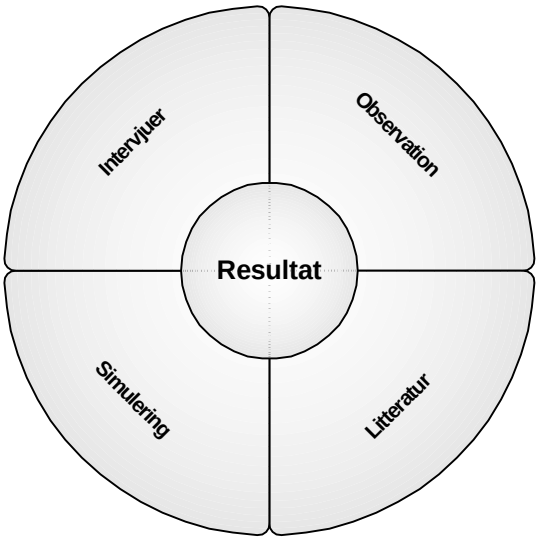
Kvalitativa metoder

För den kvalitativa metoden är huvudargumenten: förståelse, intersubjektivitet, teorigenerering, validitet, upptäckt, variation och kanske framför allt nyfikenhet. Styrkan med den kvalitativa metoden är möjligheten att se förändrelseprocesser, att förstå människors egentliga åsikter, förmåga att adoptera till nya frågeställningar och idéer som uppstår i den miljö som forskningen pågår i samt att bidraga till utformningen av ny teorier. En risk vid kvalitativa undersökningar är att man låter sina egna förutfattade meningar styra tolkningen av insamlat material. Det kan ofta vara svårt att dra generella slutsatser utifrån resultaten av kvalitativ forskning. Av det resultat man erhållit kan man bara uttala sig om den specifika situation man undersökt. Den del av resultatet man kan använda för att dra generella slutsatser är den som inte är specifik för situationen.

I denna undersökning har en kvalitativ metod använts då den lämpar sig bäst när man vill undersöka bakomliggande faktorer och förstår hur saker och ting fungerar. Det fanns ett behov av att erhålla en djupare insikt om problemet. Det var också viktigt att undersöka hur helheten påverkas. Vad som orsakar vad och varför det gör det. Undersökningen är därmed till högre grad fokuserad på djup än på bredd.

Använda metoder

Insamlande av data i undersökningen gjordes på med hjälp av fyra olika metoder: observation, litteratur, simulering, intervjuer.



Figur 3. Använda metoder för att nå resultatet i undersökningen.

Studien är kopplat till ett speciellt projekt hos Unisys. Kopplingen till ett projekt har valts eftersom jag strävar efter att kombinera teorierna bakom behörighetsadministrationen med det praktiska användandet av metoder och tekniker som användningen i en skarp miljö innebär. På så sätt hoppas jag få en djupare förståelse. Backman (1998) belyser fördelen med fallstudier:

> *"Fallstudier anses vara särskilt tillämpliga i utvärderingar, där studieobjekten ofta är mycket komplexa. Man söker exempelvis förklara, förstå eller beskriva stora företeelser, organisationer eller system, som inte enkelt låter sig undersökas med annan metodik."* (s. 49)

Observation

Till viss del baseras materialet i undersökningen av egen erfarenhet då jag under sommaren 1998 var trainee på Unisys. Jag fick då inblick i verksamheten och förståelse för problematiken i projektet som fallstudien grundar sig på.

Deltagande observation innebär att observatören både påverkar och påverkas av det som observeras, men endast inom bestämda gränser. Ett antal praktiska problem finns som gör att deltagarobservation ibland är svårt att genomföra. För att kunna delta och utföra ett arbete som de anställda i en verksamhet krävs att man behärskar arbetet.

Komplexiteten i det aktuella projektet gjorde det dock i princip omöjligt att kunna delta fullt ut på grund av på den korta tid som stod till förfogande. Ren observation är då betydligt enklare att genomföra. Observationer är ett bra komplement till intervjuer eftersom man kan inrikta sig på vad som övergripande sker i verksamheten och man erhåller då större förståelse för problemområdet.

Man skiljer mellan systematiska och osystematiska observationer. En systematisk observation utföres efter en plan, över vad som skall observeras, när och hur ofta observationerna skall göras, samt hur de skall registreras och dokumenteras. Man bestämmer sig för ett schema med ett tillräckligt antal observationer. Data bör registreras på ett tillförlitligt sätt. En osystematisk observation är friare i olika avseenden, jämfört med de systematiska observationerna.

Min tid som trainee kan om möjligt klassas som osystematisk observation. Jag var vid den aktuella tidpunkten inte medveten om att den verksamhet som jag var en del av skulle ingå i min undersökning. Av den anledningen resulterade inte tiden som trainee i de resultat som det skulle vid en medveten observation. Observationen gav mig istället en introduktion till hur projektet var uppbyggt och insikt om de problem som uppstod. Tiden gav mig därmed en stabil bakgrund för vidare observationer.

Litteratur

Syftet är att generera kunskap om problemområdet och att i litteraturavsnittets förklara det teoretiska ramverket som ligger till grund för uppsatsen. Det är särskilt viktigt i ämnet informatik att noggrant utföra definitionsarbete eftersom området utvecklas i en rasande takt där ständigt nya fenomen och begrepp dyker upp. Branschen har också en hög "hypefaktor" där ständigt nya termer myntas och sprids. Backman (1998) skriver:

> *"I exempelvis utredningsarbeten där man vänder sig till lekmän, måste stort utrymme ägnas åt att föra in läsaren i området, att förklara och definiera begrepp och företeelser, att motivera vetenskaplig och/eller samhällelig betydelse etc."* (s. 37*)*

Litteraturstudien bestod av att samla in litterärt material i syfte för individuell självstudie Sökning efter litteratur skedde företrädesvis på bibliotek och på Internet. Sökning efter information på Internet skedde med hjälp av befintliga sökrobotar, främst användes Alta Vista och Infoseek. De sökord som användes var: "Windows NT", "säkerhet", "administration", "användare", "user" och "security" i olika mixade konstellationer. När intressant information påträffades söktes efter ytterligare publicerat material från författaren och/eller via eventuellt rekommenderade länkar. Tiden som avsattes till självstudier uppgick till ungefär två veckor.

Då majoriteten av litteraturen var på engelska angavs vissa facktermer på engelska. I de fall det fanns en lämplig översättning till svenska så användes även den. Detta kan dock ge ett intryck av att termerna inte är konsekvent behandlade i rapporten.

Simulering

För att få praktisk erfarenhet sattes ett testnätverk upp. Nätverket bestod av två datorer installerade med Windows NT Server. En av dem var konfigurerad som en primär domänkontrollant och den andra som en sekundär domänkontrollant. I nätverket fanns också två datorer med Windows NT Workstation för att simulera användarnas miljö.

Simulering gick till så att då det uppstod oklarheter orsakade av observationen, litteraturen eller intervjuerna återskapades situationen i de fall det var möjligt. På detta sätt blev det möjligt att koppla ihop teori med praktisk förståelse för hur det fungerade i en skarp miljö.

Intervjuer

Intervju är en teknik som nästan kan sägas vara självskriven när man gör en kvalitativ studie, och är troligen den metod som de flesta människor anser ”vara” kvalitativ metod. Intervjuer kan genomföras på flera sätt, t ex strukturerat eller ostrukturerat. Att använda sig av en helt ostrukturerad intervju är svårt. Le Duc (1996) skriver:

> *"Det kan verka lockande för oerfarna utredare att börja samla in data m h a informella intervjuer utan större förberedelser. Informella intervjuer ska dock användas endast i speciella sammanhang såsom förstudier. Induktiva och utforskande studier som inte använder frågeformulär så mycket kräver också noggranna förberedelser för att leda till användbara resultat."* (s. 53)

I undersökningen användes därför halv-strukturerade intervjuer baserade på en frågemall. Syftet med intervju är inte enbart för att skapa förståelse om något, utan också för att slutligen kunna föreslå en lösning eller diskutera eventuella problem.

Urval

Det är viktigt att man väljer ut urvalet med värderingar lämpliga för den metod man använder i undersökningen. Man bör således inte använda kvalitativa kriterier i urvalet när undersökning är av kvantitativ art eller vice versa. Man skiljer på slumpmässigt och målstyrt urval. Patton (1990) utvecklar nedan förhållandet mellan slumpmässigt och målstyrt urval:

> *"The logic of purposeful sampling is quite different from the logic of probability sampling. The problem is, however, that the utility and credibility of small purposeful samples are often judged on the basis of the logic, purpose, and recommended sample sizes of probability sampling. What should happen is that purposeful samples be judged on the basis of the purpose and rationale of each study and the sampling strategy used to achieve the study's purpose. The sample, like all other aspects of qualitative inquiry, must be judged in context-the same principle that undergirds analysis and presentation of qualitative data. Random probability samples cannot accomplish what in-depth, purposeful samples accomplish, and vice versa."* (s. 184)

För att koma fram till vilka personer som skulle intervjuas användes urvalprincipen som Patton benämner ”criterion sampling” vilken går ut på att man väljer de fall som möter vissa ställda kriterier. Urvalet för intervjun grundade sig i huvudsak på två kriterier. För att få bästa förståelse hur behörighetsadministrationen i Windows NT fungerar rent funktionsmässigt var det viktigt att få tillgång till personer med hög teoretisk kompetens inom området. Det var också önskvärt att personerna skulle också ha god erfarenhet om behörighetsadministration i verksamheter som använder Windows NT d.v.s. hur funktionerna tillämpas praktiskt i verkligheten. Urvalet bestod således av fyra anställda på Unisys som samtliga uppfyllde de båda kriterierna. De innehar följande befattningar: en nätverksspecialist och en driftstekniker med vardera sex års erfarenhet samt två nätverkstekniker varav en med fyra års erfarenhet och en med två års erfarenhet. Tillsammans ansvarar de för implementeringen och den kontinuerliga administrationen av nätverksdelen i projektet som studien grundar sig på.

Intervjufrågor

Eftersom intervjuerna baserades på användningen av en intervjumall går det inte exakt att redogöra för alla de frågor som ställdes under intervjun. Ett antal punkter användes dock att diskutera kring. Frågorna arbetades fram utifrån erfarenheter från observation och litteraturstudier. Från observationen erhölls en överblick av problemområdet och från fysiskt och virtuella litteraturstudier erhölls teoretisk kunskap. Tillsammans bildade de en grund av förståelse för problemområdet. Utifrån denna grund identifierades olika problem vilket resulterade i att en frågemall formulerades. Le Duc (1996) belyser vikten ett frågeformulärs utformning:

> *"Man måste därför strukturera formuläret så att det stämmer så bra som möjligt med de teoretiska utgångspunkter och resonemang som ligger till grund för arbetet. Frågeformuläret är den slutgiltiga operationaliseringen av ens teoretiska frågeställning. Därför måste detta till form, struktur och innehåll stämma så bra överens som möjligt med de teoretiska förutsättningarna."* (s. 54)

Frågemallen (bilaga 3) bestod av tolv stycken frågor, varav de fyra första var personliga, d.v.s. de handlade om personens bakgrund såsom ålder, erfarenhet, meriter mm. Resterande åtta frågor var kategoriserade i två olika områden. Det första området berörde behörighetssystemets olika funktioners begränsningar och möjligheter i Windows NT. Det andra behandlade de intervjuades syn på behörighetsadministration ur ett vidare perspektiv.

Tillvägagångssätt

Tid bokades för ett personligt möte med personerna i urvalet. De intervjuade erhöll skriftligt intervjufrågorna några dagar i förväg för att de skulle kunna förbereda sig.

Vid intervjutillfällena informerades de om att de inte behövde följa frågorna i kronologisk ordning utan det gick bra att tala fritt för att på så sätt få en helhetsbild. För att dokumentera intervjun spelades svaren på frågorna in med diktafon under mötets gång. Intervjun sammanställdes och skrevs därefter ut i sin helhet så snabbt som möjligt. Anledningen var att få med så många minnesbilder, intryck och uppslag som möjligt.

Patton (1990) förordar att trots arbetsinsatsen skriva ut hela de bandade intervjuerna av följande skäl:

> *"At the Minnesota Center for Social Research, we found that the ratio of transcribing time to tape time was typically 4:1 on the average, it took four hours to transcribe one hour of tape. Despite these costs, full transcriptions are the most desirable data to obtain. Transcripts can be enormously useful in data analysis and later in replications or independent analyses of the data."* (s. 349)

Ett problem när man gör intervjuer på det här löst strukturerade sättet, till skillnad från ett kvantitativt formulär där det finns begränsade frågor och svar, är att man inte alltid får raka svar på de frågor man ställer. I en kvalitativ intervju skall intervjuobjektet i största möjliga mån själv få utforma sina tankar och åsikter på ett naturligt sätt. Syftet är att förmedla komplett information till intervjuaren för att därmed skapa så djup förståelse som möjligt. Resultatet blir att diskussionerna ofta går in i varandra. När man sedan analyserar svaren finner man att vissa frågor endast är besvarades delvis eller inte alls. Detta är ett problem man får acceptera och tackla bäst det går i en kvalitativ undersökning.

I resultatet redovisas s.k. rådata i forma av citatblock från intervjuerna. På det viset får läsaren själv en uppfattning om vad som har sagts med de intervjuades egna ord och hjälper därmed till att skilja på data och tolkning av data.

Teoretisk referensram

I detta avsnitt presenteras de teoretiska termer som är centrala i uppsatsen. Den teoretiska referensramen ska ge läsaren en inblick i teorin som uppsatsen grundar sig på och ge en förståelse för problemområdet som uppsatsen behandlar. Delen som beskriver de olika funktionerna i behörighetskontrollsystemet i Windows NT är disponerat så att avsnittet om en funktion baseras på avsnittet innan där föregående funktion förklaras. På så tillämpas en logisk ordning för att förbereda läsaren inför kommande läsning. Det finns dock avsnitt innehållande funktioner som grundar sig på varandra. I de fall är avsnitten placerade i den ordning jag anser vara lämpligast för att kunna förstår behörighetssystemet på lättast sätt. Det kan dock resultera i att läsaren måste alternera mellan avsnitten.

Behörighetsadministration

Syftet med behörighetsadministration är enligt SIG Security (1993) att nyttja behörighetskontrollerna så att:

> *"Behöriga användare alltid kommer åt den information och de bearbetnings- och kommunikationsresurser som krävs för ett effektivt fullgörande av sin arbetsuppgift. Samtidigt bör användarna kunna förhindras från åtkomst till resurser som de inte behöver för sitt arbete. "* (s. 59)

Behörighetskontrollsystem

I grunden har alla användare tillgång till praktiskt taget samma information och resurser i ett nätverk, men det är i långt ifrån de flesta fall som det är lämpligt att samtliga skall kunna nyttja alla delarna på ett likvärdigt sätt. En person skall t.ex. kunna ändra i ett dokument, en annan endast läsa informationen medan en tredje inte ha rätt att öppna dokumentet. För att skydda information och program mot obehörig förändring eller spridning i en datoriserad verksamhet krävs funktioner för behörighetskontroll. För att administrera behörighetskontrollen används att ett behörighetssystem (BKS). I en publikation av Dataföreningen i Sverige (1997) finns definitionen:

> *"System för behörighetskontroll innebär de administrativa och tekniska åtgärder för tilldelning och kontroll av användarens identitet, styrning av användarens behörighet att använda systemet och dess resurser samt för registrering av denna användning."* (s. 111)

Ett BKS omfattar alla erforderliga säkerhetsfunktioner i ett IT-system, som tillsammans ska tillgodose att verksamhetens säkerhetsregler för IT-systemet kontinuerligt uppfylls. Enligt Dataföreningen i Sverige (1997) så utgör grunderna för ett fungerande BKS av följande samverkande delar:

- Det aktuella operativsystemet.
- Funktioner i operativsystem vars huvudsakliga uppgift är att styra behörighetskontrollen.
- Behörighetsfunktioner i tillämpningsprogram.
- Administrativa rutiner.

Ett BKS skall vidare:

- Skydda verksamhetens mot avsiktlig eller oavsiktlig intrång vilket kan resultera i förändringar eller obehörig användning av själva systemet.
- Skydda informationen i systemet mot obehörig åtkomst så att den inte kopieras, förändras eller förstörs.
- Skydda medarbetare mot att oavsiktligt göra något otillåtet för att verkan inte skall bli såsom i någon av de två ovanstående punkterna eller som i nedanstående punkt.
- Förhindra att den anställde hamnar i en situation där denne kan bli oskyldig misstänkt för obehörig användning av själva systemet eller information i det.
- Möjliggöra uppföljning och kontroll av de funktioner som finns i system.

Dataföreningen i Sverige anser därför att ett BKS bör ha följande funktioner inbyggda:

- Identifiering av användaren och certifiering av den föregivna identiteten. För att verifiera en individ kräva t ex lösenord, aktiva kort (smartcard) eller användning av biometriska metoder.
- Reglering av åtkomsträttigheter dvs vem får göra vad, hur och när.
- Tilldelning av resurser t ex nätverksenheter, skivminne, skrivare, program etc.
- Registrering av användarens aktiviteter i systemet, vilka ofta benämns loggning.

Ett system för kontroll av användarens behörighet kan vara antingen manuellt eller automatiskt. En hierarkisk uppbyggnad av BKS är önskvärd eftersom det medför att det är möjligt att definiera grupper av användare och ge särskilda rättigheter till nätadministratör, gruppansvariga etc.

Behörighetssystemet i Windows NT

Windows NT (New Technology) är Microsofts mest avancerade operativsystem. Det är anpassat för att användas i såväl fristående miljö som nätverksmiljö. Det finns i två olika utföranden, Windows NT Server respektive Workstation. Microsoft Corporation (1999) skriver om sitt operativsystem:

> *"Security in any system is a combination of technology and policy. The Microsoft® Windows NT® operating system has a robust security model that enforces granular access control on all resources and facilitates the consistent use of policies to leverage the technological safeguards."*

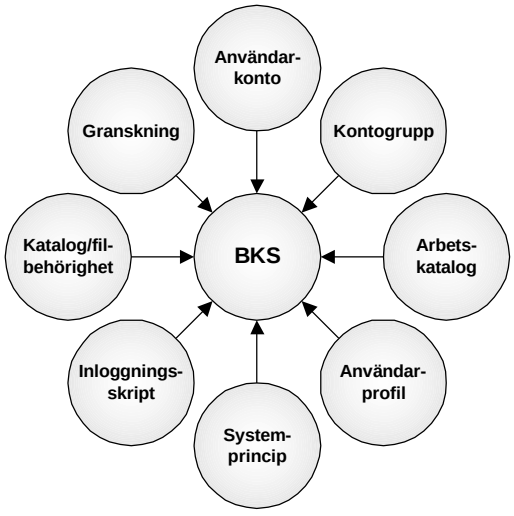
Det finns en utvärderingsmodell för att bestämma hur säkert ett operativsystem. Den heter Trusted Computer Security Evaluation Criteria (TCSEC), även känd som The Orange Book, vilken publicerades 1983 av US Department of Defence (DoD). Den innehåller regler och kriterier för att fastställa hur säkert ett system är. De olika säkerhetsnivåerna i Orange Book är:

- D.
- C1 - C2.
- B1 - B3.
- A1.

Där nivå D är den lägsta och nivå A1 den högsta. Windows NT är certifierat för nivå C2. Det är inte helt lätt att förklara vad det innebär eftersom Orange Book är en djungel av regler och förordningar, men för att ha något att jämföra med så ligger UNIX i sitt grundutförande (det kan byggas ut) ungefär på C1-nivå vilket är något lägre. MS-DOS, som helt saknar säkerhet är klassat på den lägsta nivån D. Det var den amerikanska versionen av NT 3.5 (med Service Pack 3) som fick C2-stämpeln. Säkerhetsmodellen i NT 3.5 (bilaga 2) skiljer sig dock inte i någon större utsträckning från den i NT 4.0. Mitrovic (1997) beskriver kortfattad säkerhetsmodellen:

> *"Första komponenten är själva inloggningsprocessen. Varje användare måste först logga in på en NT-server för att kunna få tillgång till de delade resurserna. Nästa komponent är LSA (Local Security Authority), som har till uppgift att kontrollera om användaren har tillgång till resursen som efterfrågas. SAM (Security Account Manager) är en databas som innehåller information om alla användarkonton. Slutligen har vi (SRM) Security Refernce Monitor som kontrollerar om användaren har rättigheter har rättigheter till begärda resurser och utför de begärda kommandona om så är fallet."* (s. 34)

Windows NT skyddar systemet genom att endast tillåta att auktoriserade användare får tillgång till systemet. För att en person skall kunna logga på Windows NT krävs att personen har ett användarkonto. Inte ens när auktoriserade användare loggar på har de obegränsad tillgång till systemet. Användaren kan bara utnyttja de delar av systemet som han har rättighet till. Användaren kan dessutom bara utnyttja de resurser i systemet som han har behörighet att använda.



Figur4. Samverkande funktioner i Windows NT:s behörighetssystem.

Rättigheter (User Rights)

En rättighet tillåter en användare att utföra vissa åtgärder i systemet. Utan korrekta rättigheter kan dessa åtgärder inte utföras. Rättigheter gäller systemet som helhet och är inte detsamma som behörighet, som gäller enskilda objekt. Det kan vara lite förvirrande då rättigheter ibland kan upplevas vara samma som behörigheter. Rättigheter kan tilldelas både enskilda användarkonton och gruppkonton. Rättigheter kopplade till användarkonton och gruppkonton förser användarna med varierande grad av restriktioner och privilegier (bilaga 1) beroende på organisationens krav .

Behörigheter (Permissions)

Behörighet är regler som specificerar vilka användare som kan komma åt olika specifika objekt såsom filer, kataloger, skrivare etc. Ägaren till ett objekt anger vilka användare/grupper som skall erhålla behörighet till objektets. Behörighet specificeras på ett objekt istället för på en användare eller grupp. Tilldelningen sker således bakvänt jämfört med rättigheter, där man reglerar vad användaren har tillåtelse att utföra.

Användarkonton (User Accounts)

Varje person som vill använda Windows NT måste ha ett användarkonto. Ett användarkonto består av unik information om en viss användare såsom användarnamn, lösenord och olika befogenheter på systemnivå. Användaren loggar in i datorn med användarnamnet och tillhörande lösenord. Användaren erhåller då de rättigheter och befogenheter som är kopplade till respektive konto. Under användningen övervakar och kontrollerar Windows NT att användaren endast får rättighet att utföra de funktioner som överensstämmer med de givna restriktionerna i användarens konto. Användarkonton kan vara av två olika typer: lokala och globala användarkonton.

Lokala användarkonton (Local User Accounts)

Ett lokalt konto innebär att kontot endast är registrerat på en specifik dator. Ett användare som har ett lokalt konto kan bara logga in på den aktuella datorn där kontot är registrerat. Användaren kommer därför endast åt resurserna på den datorn.

Globala användarkonton (Global User Accounts)

Ett globalt konto däremot lagras globalt på en server i nätverket vilket medför skillnaden att användaren inte är hänvisad till en speciell dator utan hon/han har möjligheten att logga på flera av datorerna i nätverket. Användarens möjligheter att nyttja resurser är därför inte begränsade till den datorn där kontot är registrerat. Det bör också påpekas att en användare inte är begränsat till bara en typ av konto. En användare kan mycket väl ha både flera lokala och globala konton.

I Windows NT finns flera inbyggda konton. Ett inbyggt konto är ett användarkonton som är fördefinierat. I Windows NT finns två grundläggande konton, Administratör och Gäst. Kontot Administratör tillhör gruppen Administratörer och används för att hantera övergripande inställningar på systemnivå i Windows NT. Den person som har ett administratörskonto har fullständig kontroll över NT och är därför det viktigaste kontot i ett NT-baserat datorsystem. Kontot Gäst är praktiskt taget motsatsen till administratörskontot. Gäst tillhör gruppen Gäster och är det kontot som har minst privilegier i NT. En användare med gästkonto har därför mycket begränsad tillgång i systemet.

Man kan själv skapa ytterligare konton med alla tänkbara mellanliggande privilegier. Ett användarkonto kan som nämnts tidigare ha olika rättigheter kopplat direkt till sig, men vanligare är att det görs genom att man ansluter kontot till en viss kontogrupp.

Kontogrupper (Group Accounts)

Med användarkonton kan man tilldela olika användare rättigheter och privilegier. Då man hanterar många användare så är det troligt att åtminstone några använder samma resurser och erhåller liknande rättigheter i systemet. Genom att samla de användarkonton som skall ha samma rättigheter och privilegier tillsammans i en kontogrupp kan man styra användarna på ett effektivare sätt. Antag t.ex. att alla användare på en ekonomiavdelning inom ett företag behöver komma åt samma bibliotek på serverns hårddisk. Istället för att då ge varje enskilt användarkonto behörighet att komma åt informationen så kan man bevilja behörigheten till en speciell grupp. Man gör därefter de berörda användarna till medlemmar i gruppen. De erhåller då gruppens rättigheter och behörigheter. På så sätt blir det betydligt enklare att hantera stora skaror av användare. En användare kan vara medlem i mer än en grupp. Det är dock viktigt att påpeka att det inte finns någon prioritetsordning mellan olika grupper. Grupper har inte heller högre prioritet än konton. Windows NT har två typer av grupper: lokala grupper och globala grupper.

Figur 5. Användare med olika rättigheter grupperade i olika kontogrupper.

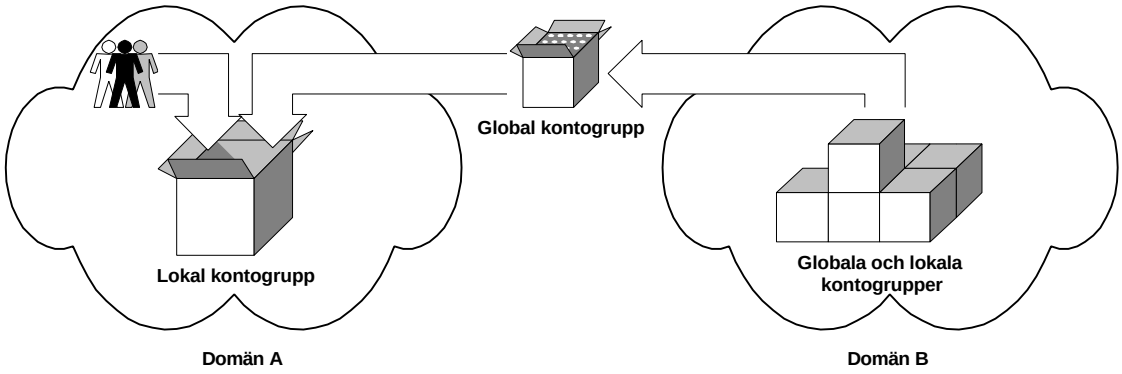
Lokala grupper (Local Group Accounts)

Används lokala grupper på en klient eller en fristående server (stand alone server) så erhåller de konton som ingår i gruppen bara rättigheter på den lokala maskinen. Medan en lokal grupp som är skapad på en domänkontrollant (domain controller) skapas på alla domänkontrollanter i domänen och erhåller då rättigheter i hela nätverket. En lokal grupp kan också innehålla globala grupper från både den egna domänen och från andra domäner, lokala grupper kan alltså ha både enskilda konton och globala grupper som medlemmar. Däremot kan inte en lokal grupp vara medlem i en annan lokal grupp.

Globala grupper (Global Group Accounts)

En global grupp å andra sidan har endast konton tillhörande den egna domänen som medlemmar. Globala grupper kan bara skapas och administreras på domänkontrollanter. En global grupp kan inte innehålla lokala grupper, andra globala grupper eller konton från en annan domän. De globala grupperna har generellt i ingen makt utan görs till medlemmar i lokala grupper där rättigheter och privilegier specificeras.

Trots detta spelar de en viktig roll när man delar ut lokala rättigheter och behörigheter på fristående servrar och klienter. I en typisk Windows NT-konfiguration är användarkonton medlemmar i en global grupp. Den globala gruppen är i sin tur medlem i en eller flera lokala grupper där premisser och restriktioner har angivits. Globala grupper fungerar alltså i huvudsak som en konteiner innehållande användarkonton för att sedan grupperas i lokala grupper.



Figur 6. Lokal kontogrupp innehållande användare från den egna domänen och en global kontogrupp med användare från en annan domän.

I Windows NT finns ett flertal fördefinierade kontogrupper med olika rättigheter. Uppsättningen inbyggda grupper i Windows NT (bilaga 1) beror på om datorn är konfigurerad som en domänkontrollant eller inte.

Kontoprinciper (Account Policies)

Kontoprinciper anger vilka regler som gäller för samtliga användarkontons lösenord i systemet. Man kan t.ex. definierar längsta och kortaste giltighetstid för lösenord, minsta längd på lösenord mm. Reglerna anger även när eventuell utelåsning från systemet skall ske. Om utelåsning är aktiverad kan ett användarkonto inte användas efter ett antal misslyckade inloggningsförsök inom en viss tid. Ett låst konto är och förblir låst tills en administratör har låst upp kontot eller en reglerad tid har förflutit.

Arbetskatalog (Home Directory)

En arbetskatalog innehåller användarnas filer och program. Det kan tilldelas en vald användare eller delas av många användare tillsammans. En Arbetskatalog bildas automatiskt när man skapar ett nytt användarkonto men den kan också skapas manuellt. Den kan användas både lokalt på en enskild arbetsstation eller globalt på en server. Arbetskatalogen gör det lättare för användaren och administratören att hålla reda på användarens filer då de förvaras på en specificerat plats i nätverket. Det gör det också möjligt för systemansvariga att hindra användaren från att komma åt systemfiler eller filer som hör till andra användare.

Användarprofiler (User Profiles)

En användarprofil består av information om hur gränssnitt och funktioner i Windows NT skall konfigureras för användaren. En användares konfigurationsinformation kan specificeras separat och sparas i användarens personliga profil. När en användare loggar på systemet läses användarprofilen in och användarens arbetsmiljö i Windows NT konfigureras enligt inställningarna i profilen. Information rör de användarespecifika inställningarna av Windows NT-miljön.

Carter (1997) anger följande inställningar som kan anges i en profil:

- Inställningar i Windows NT Explorer, Notepad, Paint, Hyperterminal, Klockan, Kalkylatorn och andra inbyggda applikationer.
- Inställningar för gränssnittet inkluderat skärmsläckare, bakgrundsfärg, bakgrundsmönster och andra skärminställningar.
- Inställningar i applikationer skapade för Windows NT.
- Inställningar för nätverks- och skrivarkopplingar.
- Inställningar för Startmenyn, inkluderat programgrupper, program och nyligen använda dokument.

En användarprofil kan gestaltas i tre olika typer:

Lokal användarprofil (local user profile) skapas automatiskt när användaren loggar på Windows NT första gången. Den lagras som namnet antyder lokalt vilket medför att inställningarna endast gäller för den aktuella datorn. För varje användare är den personliga profilen åtkomlig varje gång hon/han hädanefter loggar på den just den klienten.

Global användarprofil (roaming user profile) är en användarprofil som lagras centralt på en server. Detta medför att användaren erhåller sin personliga profil oavsett vilken dator hon/han loggar på i nätverket. När användaren loggar på kopieras profilen till användarens dator från servern i de fall den är nyare än den lokala profilen. Om inte så frågar Windows NT vilken profil användaren vill ladda, den lokala eller den globala. Både profilen på den lokala datorn och på servern uppdateras sedan när användaren loggar ur systemet.

Obligatorisk användarprofil (mandatory user profile) är en global profil som efter den har blivit tilldelad en användare inte kan ändras av användaren. Användaren kan fortfarande ändra sina inställningar när hon/han är inne i systemet men den obligatoriska profilen uppdateras inte när användaren loggar ur. Nästa gång användaren loggar på NT igen så återgår inställningarna till de givna kriterierna i profilen.

Systemprinciper (System Policies)

Systemprinciper liksom obligatorisk profil gör det möjligt för en administratör att kontrollera arbetsmiljön för en användare i ett nätverk. När en användare loggar på Windows NT så laddas först användarens profil och sedan användarprinciperna. Med systemprinciper erhåller dock administratören mycket mer konfigurerbara alternativ än med obligatorisk profil. Systemprinciper innebär en kraftfullare funktion för att styra en användare än vad profiler gör. Systemprinciperna i Windows NT består av användare-, grupp- och datorprinciper. Systemprinciperna begränsar användarens möjligheter att utföra uppgifter på datorerna i nätverket. Då systemprinciper omfattar användare, grupper och datorprinciper så kan de gälla för samtliga användare och datorer, eller bara för individuella användare, grupper eller datorer.

En användareprincip består av ett flertal inställningar som begränsar användarens program och nätverksmöjligheter. Inställningarna är kopplade till användarens konto vilket medför att de gäller på samtliga datorer som användaren kan logga in på.

En grupprincip appliceras på en grupp. Alla användare som är medlem i gruppen påverkas av principerna med undantag av de användare som har individuell användarprincip. En användare är ofta medlem i mer än en grupp och varje grupp kan ju ha sina speciella principer. Vissa grupprinciper kan i vissa fall motverka varandra. För att då veta vilka principer som gäller måste administratören gruppera principerna beroende på vilken prioritet de skall ha.

Datorprinciper är principer som påverkar en lokal dators konfiguration. Denna konfiguration gäller sedan för alla användare som logar på den aktuella datorn.

Inloggningsskript (Logon Script)

Ett inloggningsskript är en exekverbar fil (bat-, cmd- eller exe-fil) som är kopplat till användarens konto. Filen laddas varje gång en användare loggar in. Användningen av inloggningsskript möjliggör för administratören att skräddarsy systemet för varje enskild användare eller grupp. Administratören kan konfigurera nätverksinställningar så att en användare t.ex. kan dela filer och andra resurser över ett nätverk.

Ett inloggningsskript kan också användas till att starta applikationer. Inställningar och kopplingar sker automatiskt när skriptet laddas. Administratören kan skapa ett unikt skript till varje användare eller använda ett gemensamt till flera användare.

Katalog- och filbehörighet (Directory and File Permission)

Windows NT skyddar automatiskt de filer och kataloger som lagras på en partion med filsystemet NTFS (New Technology File System). På en NTFS-partition kan man kontrollera vem som skall ha tillgång till filer eller kataloger samt hur dessa kan användas av användare och grupper. NTFS tillåter endast andra användare att komma åt en filen/katalog i de fall hon eller han har behörighet. Denna funktion kallas Discretionary Access Control (DAC). Det finns ett flertal nivåer på behörighet som man kan ange (bilaga 1).

Granskning (Auditing)

I Windows NTs behörighetssystem inkluderas en funktion som benämns granskning. När granskning används producerar Windows NT en förteckning (logg) över specificerade händelser och aktiviteter som uppstår i systemet. Specifika användaraktiviteter kan sedan spåras genom granskning av händelserna i säkerhetsloggen. Flera olika typer av händelser kan lagras (bilaga 1), t.ex. en användare som loggar in eller ett försök av en användare att läsa en fil. Både lyckade och misslyckade försök kan lagras.

Nätverksorganisation

Domän eller arbetsgrupp (Domain or Workgroup)

I en arbetsgrupp delar alla lika på resurserna. Eftersom det inte finns någon primär server kallas modellen för peer-to-peer network. Varje ingående NT server eller arbetsstation upprätthåller en lokal kopia av användare och grupper. För de användare som ska dela på resurser som finns på flera datorer gäller att deras användarkonton måste vara registrerade på respektive dator.

En domän är ett samlingsnamn för en grupp av servrar och klienter som delar på resurser, konton och den säkerhet som är uppsatt kring komponenterna. Servrar och klienter delar på en databas med domänkonton och globala kontogrupper. Detta medför att man kan logga in med ett användarkonto och få tillgång till delade filer och andra resurser datorerna inom domänen. Microsoft Corporation (1996) skriver om domäner:

> *"A domain is a logical grouping of network servers and other computers that share common security and user account information. Within domains, administrators create one user account for each user. Users then log on once to the domain, not the individual servers in the domain."* (s. 2)

En domän i Windows NT baseras på tre grundelement:

Domänkontrollant (domain controller) som består av en dator med Windows NT Server och stor kapacitet. Domänkontrollanten upprätthåller en databas med samtliga användarkonton som gäller inom domänen.

Andra Servrar som hör till domänen. Dessa delar databasen med domänens användarkonton som kontrolleras av domänkontrollanten. Dessa servrar har således inga egna databaser med användarkonton.

Klienter med Windows NT Workstation. Lokal datorer med Windows NT har egna databaser med användarkonton. När en lokal dator ansluts till en domän kompletteras domänkontrollantens användardatabas med uppgifter från den lokala datorns databas.

Doyle (1996) menar att fördelarna med en domänstruktur är:

- *"Single Logon Procedure.*
- *Network users can connect to multiple servers by logging on to a single network*
- *Universal Resource Access.*
- *The user needs only one domain user account and password to use network resources.*
- *Centralized Network Administration."* (s. 81)

Domänkontrollanter (Domain Controllers)

Microsoft Corporation (1996) förklarar en domänkontrollants funktion och innebörd med följande definition:

> *"Within a domain, domain controllers manage all aspects of user-domain interactions. Domain controllers are computers running Windows NT Server that share one directory database to store security and user account information for the entire domain; they comprise a single administrative unit. Domain controllers use the information in the database to authenticate users logging on to domain accounts."* (s. 3)

Casey Doyle (1996) förklarar de två olika typerna av domänkontrollanter i Windows NT:

- Primär domänkontroll (Primary Domain Controller, PDC) spårar ändringar i domänens konton och sparar dem i kontodatabasen SAM (Security Account Manager). När en användare loggar in i domänen så kontrolleras dennes identitet mot SAM. Det kan endast finnas en PDC per domän.

- Sekundär domänkontrollant (Back up Domain Controller, BDC) upprätthåller en kopia av kontodatabasen. Anledningen är att domänen inte skall slås ut och alla behörigheter försvinna om PDCn slutar att fungera. Skulle det hända så finns en kopia på respektive BDC i domänen. Kopian uppdateras med jämna intervaller med information från den primära domänkontrollantens kontodatabas. Det kan finnas mer än BDC per domän.

Fristående servrar (Stand Alone Server)

Alla servrar i en domän behöver inte vara dedikerade till domänkontrollanter (PDC eller BDC). Datorer som kör Windows NT Server kan istället konfigureras till en fristående server. Denna server kopierar inte kontodatabasen från den primära domänkontrollanten och kan därför inte autentisera användare i nätverket. Servrar av denna typ används ofta för speciella ändamål såsom stora databaser eller andra resurskrävande applikationer.

Förtroenderelationer (Trust Relationship)

Microsoft Corporation (1996) skriver om användningen av förtroenderelationer:

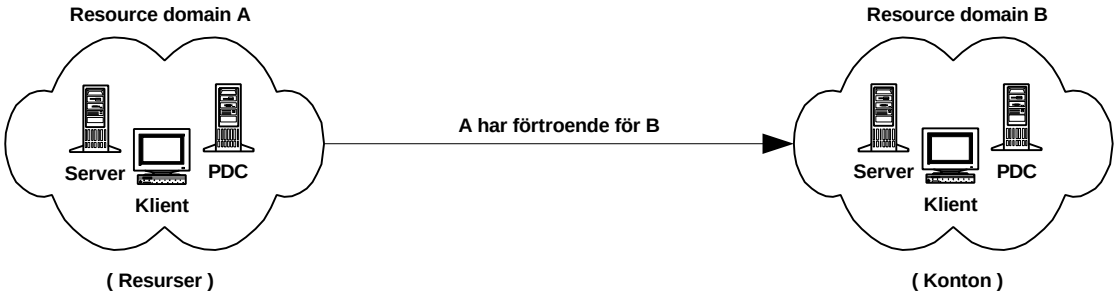
> *"Windows NT Server Directory Service provide security across multiple domains through trust relationship. A trust relationship is a link that combines two domains into one administrative unit that can authorize access to resources on both domains."* (s. 5)

Definitionen av en förtroenderelation mellan två domäner är således att en förtroenderelation utgör en länk för att infoga domänerna i en administrativ enhet. För att grupper och användare ska kunna få tillgång till de resurser som finns i en annan domän så måste det först skapas ett förtroendeförhållande mellan domänerna.

Om inte förtroenderelationer finns mellan domänerna så måste användare och grupper som vill nyttja resurser i en andra domäner också ha konton i dem. Detta medför att administrationen blir mer utspridd och svårhanterlig. Skall t.ex. en användare få andra rättigheter så är administratören tvungen att justera samtliga domäner där användaren har ett konto registrerat. För att undvika multipla användarkonton och för att centralisera administrationen så används istället förtroenderelationer. En förtroenderelation beskrivs genom att låta en pil peka från domänen som har förtroende till domänen som får förtroendet.

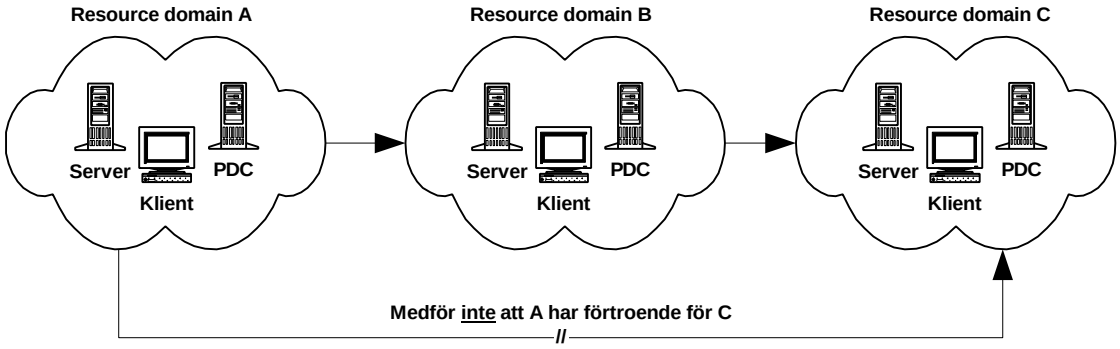
Genom att en domän som har resurser att dela med sig ger ett förtroende till en domän innehållande de användare som vill har tillgång till resurserna så uppstår en förtroenderelation. En domän som ger ett förtroende till en annan domän kallas för trusting domain d.v.s. den litar på den andra domänen. En domän som får förtroende kallas för trusted domain.

Ett förtroende kan vara både enkelriktat och dubbelriktat. Ett dubbelriktat förtroende mellan två domäner medför att användarna kan komma åt resurserna i respektive domän. Ett dubbel förtroende består i själva verket av två enkla förtroenden och beskrivs med två pilar pekande i var sin riktning.



Figur 7. Envägs förtroenderelation mellan två domäner.

Förtroenden är icke transitiva vilket bäst förklaras med ett exempel: Om domän A litar på domän B som i sin tur litar på domän C så medför det inte (som man kanske tror) att domän A automatiskt litar domän på C. Man alltså inte skapa ”förtroendekedjor” mellan domäner (i kommande version av Windows NT, Windows 2000 är dock detta möjligt) .



Figur 8. Begränsningar av förtroenderelationer i följd.

När ett förtroende har skapats, så kan trusting domain känna igen alla globala kontongrupper och alla användarkonton ifrån trusted domain. Förtroenderelationer används ofta i Wide Area Network (Wan).

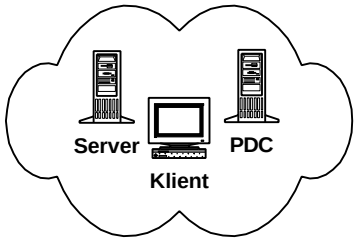
Domänmodeller

Carter (1997) specificerar fyra typer av teoretiska domänmodeller: Single Domain, Single Master Domain, Multiple Master Domain och Complete Trust Domain Model.

Single Domain Model

Single Domain Model består av en domän. Alla användarkonton, kontogrupper och resurser ligger inom samma domän. Förtroenderelationer behöver därför inte användas.

En Single Domain Model är ett lämpligt val för en organisation som kräver en centraliserad administration av användare.

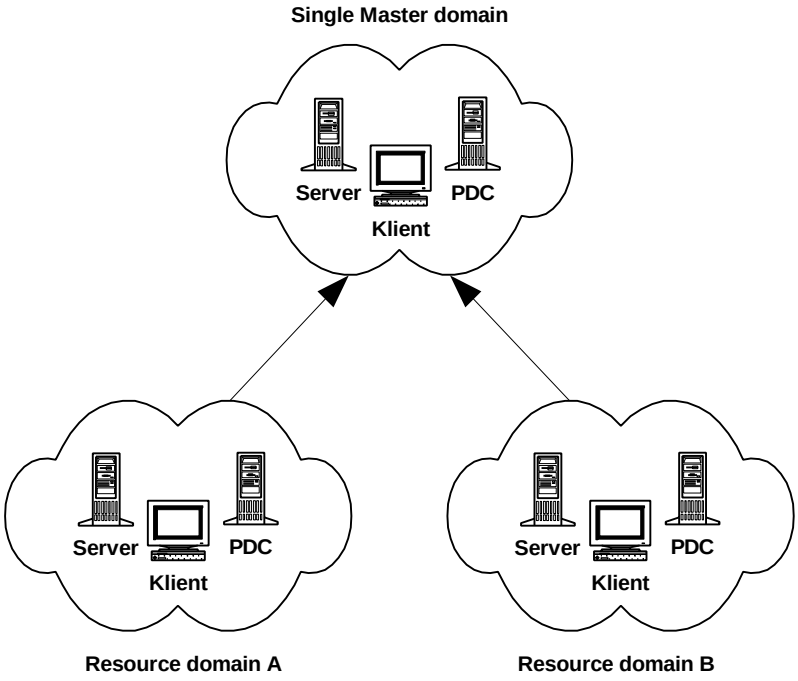


Figur 9. Single Domain model.

Ett bekymmer med den här modellen är att hantering inte är lämplig när nätverket växer. Ju fler användare och resurser som läggs till desto mer oöverskådligt blir det att administrera. Som administratör måste man då hantera långa listor av konton och grupper för att hitta rätt.

Single Master Domain Model

Single Master Domain Model består av en master domain som innehåller alla konton samt en eller flera domäner som innehåller delade resurser. Master domain agerar som en central administrativ enhet för användarekonton och grupper. I denna arkitektur används envägs förtroenden. Domänerna med resurserna litar på master domain med användarkonton och kontogrupper. På så sätt kommer användarna åt resurserna i domänerna. Single Master Domain är lämplig när man vill ha en centraliserad hantering av användare och grupper med en decentraliserad hantering av resurser. T.ex. lokala administratörer i varje domänen som ansvarar för resurserna i sin egna domän.

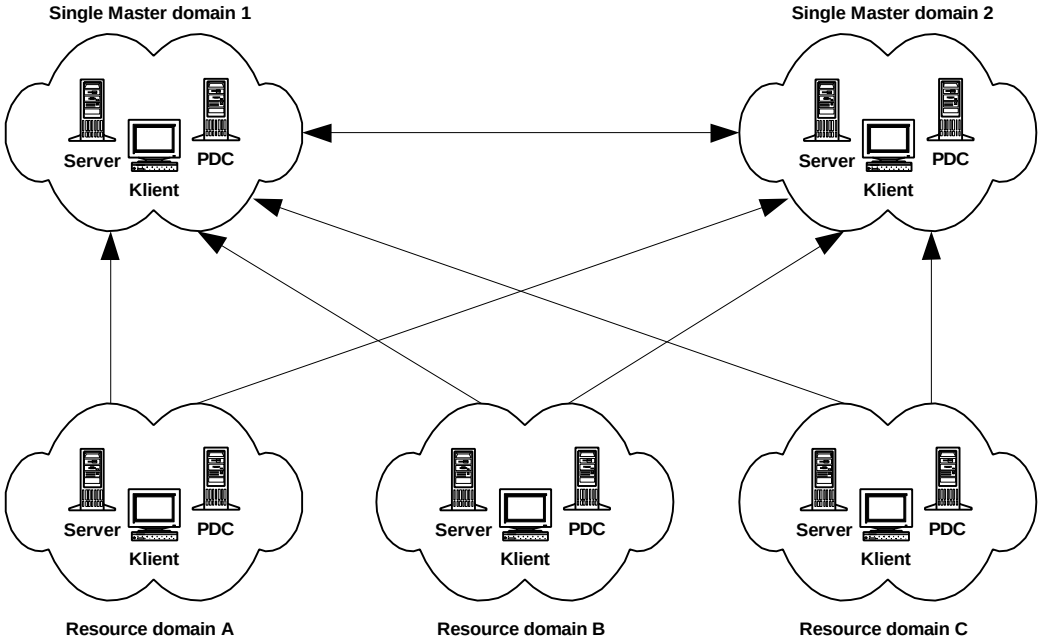


Figur 10. Single Master Domain model.

Servrarna i resource domain skickar alla inloggningsförfrågningar till domänkontrollanten i master domain. Nackdelen är om det finns många användarkonton definierade, det kan då bli långa svarstider från servern i master domain.

Multiple Master Domain Model

Multiple Master Domain Model består av två eller flera master domains innehållande konton och en eller flera domäner som innehåller delade resurser. I detta fall används tvåvägs förtroenden mellan varje master domain och envägs förtroenden från varje resource domain till varje master domain. På grund av tvåvägs förtroende mellan de bägge master domains kan administrationen av användare centraliseras eller distribueras mellan flera administratörer. Förutom samma fördelar som finna i Singel Master Domain så är Master Domain Model lämplig för organisatorisk eller geografisk indelning. Ofta får verksamhetens organisationsschema styra nätverkets utseende. T.ex. när man återspegla olika avdelningar i ett företag. Där det finns fjärrlänkar sätts nya domäner upp. Genom det här upplägget kan användare ur valfri master domain komma åt resurser i valfri resource domain.

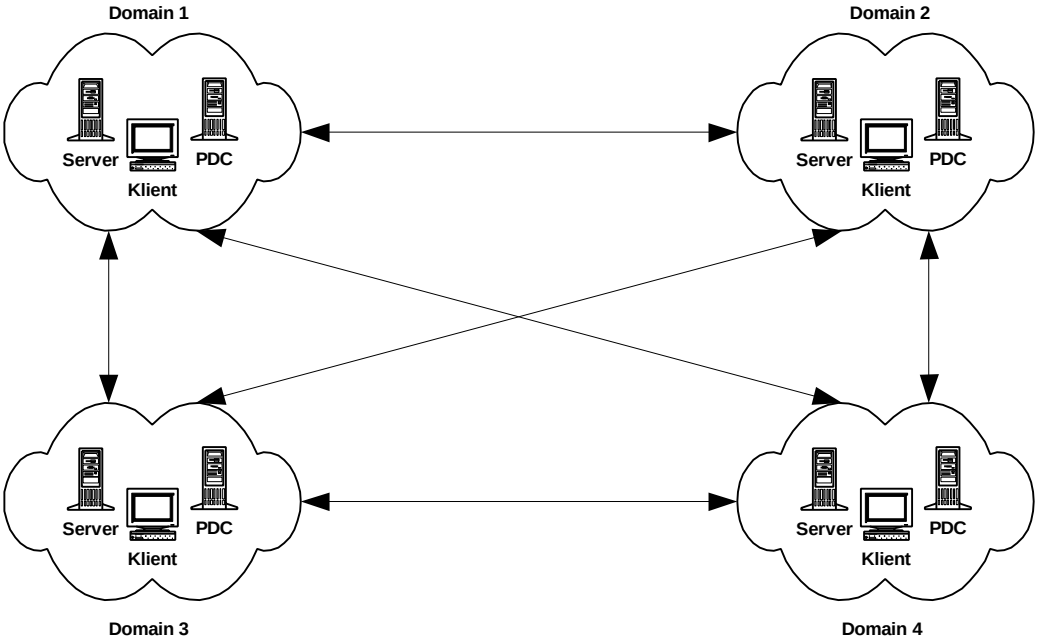


Figur 11. Multiple Master Domain Model.

Nackdelen med den här modellen är att grupper ibland måste läggas till flera gånger för olika domäner, det blir lätt många släktskap att hålla reda på och användaradministrationen kan bli svårare då användare förekommer i flera domäner.

Completet Trust Domain Model

Complete Trust Domain Model är en decentraliserad modell som består av två eller flera domäner som innehåller användarkonton och delade resurser. Mellan varje domän används tvåvägs förtroenden. Denna modell uppfattas vid första anblicken att vara lätt att administrera. Användare och resurser kan grupperas logiskt i de olika domänerna. Alla domäner litar på varandra och kommer åt varandras resurser. Organisationer som strävar efter decentraliserad användaradministration och resurshantering kan använda denna modell.



Figur 12. Complete Trust Domain model.

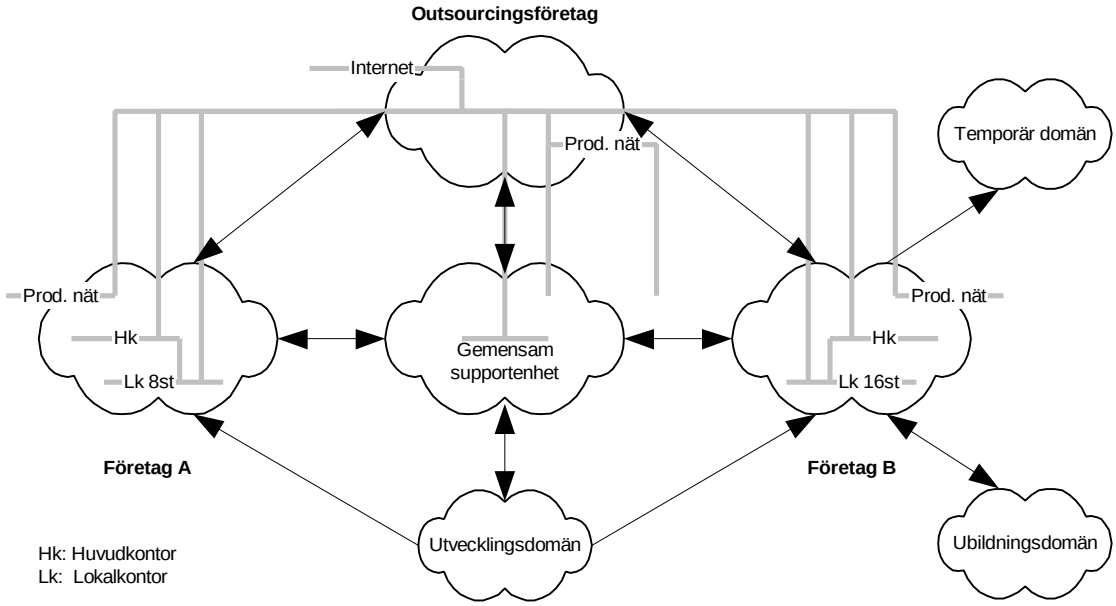
Den största faran med den här modellen ligger i en ohanterbar mängd släktskap då antalet domäner växer. För varje domän som ingår i modellen ökar antalet förtroenden med formeln: n * (n-1), där n är antal domäner. Detta medför att i en modell där det ingår t.ex. fyra domäner krävs tolv stycken tvåvägs förtroenden

Resultat

I detta avsnitt presenterar jag vad som har framkommit i undersökningen. Resultatet är disponerat så att jag först beskriver det projekt på Unisys som studien är kopplad till. Därefter presenterar jag de intervjuer som gjordes med personerna som ingick i urvalet.

Projektbeskrivning på Unisys

Projektet som fallstudien grundar sig på omfattar två företag i södra Sverige. Företag A består av ett huvudkontor och åtta stycken lokalkontor. Företag B består av ett huvudkontor och sexston stycken lokalkontor. Tillsammans har de bildat ett gemensamt företag vars uppgift är att tjäna som supportenhet till de båda.



Figur 13. Översikt av nätarkitektur med domänmodell i studien

Domänmodellen i projektet kan beskrivas som en avancerad forma av Complete Trust Domain Model. Den kan beskrivas som en kombination av en Complete Trust Domain Model och två stycken Single Master Domain Models. Modellen innehåller sju domäner. För att hålla ihop domänerna används sammanlagt tio stycken förtroenderelationer varav sju stycken är dubbelriktade och tre är enkelriktade.

Förutom två företagsdomäner, en supportdomän och outsourcingföretagets domän (Unisys) existerar det tre övriga domäner. Den första är en utvecklingsdomän som fungerar som supportenhetens konsultdomän, den andra är en utbildningsdomän till företag B och den tredje är en temporär domän som inte kommer att existera i framtiden.

Kvantiteten användare och resurser i outsourcingdomänen hos Unisys är fördelade så att ca 95% utgör resurser och resterande 5 % är användare. I de övriga domänerna är förhållandet det motsatta, 5% är resurser och 95% är användare. Detta betyder att majoriteten av användarna i projektet använder resurser i outsourcingdomänen och att personalen på Unisys tillsammans med supportenheten ansvarar för administration av alla användarna i de övriga domänerna.

Nätverksarkitekturen är också relativt komplex. Till vardera företagsdomänerna går det tre stycken nätverksförbindelser från Unisys. Två av dem har olika uppgifter i kommunikationen och det tredje är ett produktionsnätverk som tjänar som testnätverk under utvecklingsfasen. Det finns även en förbindelse mellan respektive företags huvudkontor och dess lokalkontor. Till supportenheten finns det två stycken förbindelser varav ett används för kommunikation och det andra för produktion och tester. I arkitekturen ingår också en koppling till Internet.

Administratörerna i outsourcingdomänen skall kunna komma åt resurser och administrera användare i samtliga domäner. Användarna i företag A,B och supportenheten skall ha tillgång till resurserna i outsourcingdomänen. Supportenhet skall också kunna komma åt resurser i de båda företagen. Däremot skall inte användare i företag A och B få tillgång till det andra företagets resurser eller kunna administrera användare och resurser i den egna domän. Om man refererar till de teoretiska modellerna som beskrivs i föregående kapitel framstår denna modell som minst sagt komplext uppbyggd

Intervjuer

De svar som presenteras nedan baseras i huvudsak på de intervjuades erfarenheter i det aktuella projektet. Resultatet av intervjuerna redovisas i den ordning som intervjumallen är strukturerad. Först behandlas de olika delar som behörighetssystemet i Windows NT består av. Därefter återges svaren på frågor som övergripande rör behörighetsadministration.

Behörighetssystemets ingående funktioner

Konton

När det gäller hanteringen av användarkonton i Windows NT så var samtliga intervjuade överens om att det är relativt enkelt så länge som man hanterar ett begränsat antal användare. När man däremot skall hålla reda på en större skara användare så blir det svårare. Det blir problem när alla användare ligger i en enda stor lista. Det är inte svårt att se vilka grupper en utvald användare är medlem men det är desto mer problematiskt att se vilka rättigheter användaren har på enkelt och överskådligt sätt. Det svårt att få information om vilka användare som har en speciell rättighet t.ex. vilka i systemet kan ändra systemtiden.

Exempel på kommentarer:

- *"Enkelt i stort sätt, men alla användare skulle inte ligga i en enda stor hög, man skulle på något sätt kunna dela upp listan när den innehåller många konton."*

- *"Problemet är att man inte kan se genom kontodatabasen. Vem är vad i kontohanteringen, den är ej överblickbar."*

Grupper

Kontogrupper är till för att förenkla administrationen av användare som fullgör liknande uppgifter i datorn och därmed bör ha samma rättigheter. De intervjuade ansåg att det i stora drag fungerade bra med den premissen att man verkligen höll sig till de riktlinjer som Microsoft förespråkar Problemet är att det är svårt att i hålla sig till teoretiska riktlinjer i praktiken. Det kan t.ex. komma önskemål från kunden som inte var påtänkta från början. De ansåg dessutom att en stor brist i hanteringen av grupper är att det inte på ett enkelt och överskådligt sätt går att söka ut de grupper som har en speciell rättighet. De hade också synpunkter på uppdelningen av lokala och globala grupper och dess funktioner.

Exempel på kommentarer:

- *"Det är inte bra när man skiljer på globala och lokala grupper. Man kan inte lägga en global grupp i en annan global grupp eller en lokal grupp i en lokal grupp, det skulle underlätta."*

- *"Svårt att hålla tänkt standard när kunden i efterhand kommer och vill ändra förutsättningarna, i ett fall ville de t.ex. minska antalet grupper."*

- *"Överblickbarheten, att få en bild av hur det ser ut. Dåliga verktyg för att t.ex. söka alla de grupper som innehar en speciell rättighet i systemet."*

- *"Det skulle finnas flera nivåer av grupper i en hierarkisk ordning"*

Arbetskataloger

En arbetskatalog är en katalog i datorn som reserveras för en viss användare. När användaren loggar in i Windows NT blir denna katalog användarens aktuella katalog. På frågan om vad administratörerna tyckte att denna lösning så tyckte de att hanteringen med användares arbetskataloger var enkel så länge man följde standard men det finns ändå vissa brister.

Exempel på kommentarer:

- *"Jag tycker att det finns för många sätt att skapa arbetskataloger på."*

- *"Om man låter Microsoft skapar katalogen så hamnar alla användare i en hög. Då blir det jobbigt för användaren att se sin katalog bland 200 användare."*

- *"Man kan inte utan tredjepartsprodukt begränsa hur mycket Hårddiskutrymme en användare skall få, om t.ex. en användare tar back up på sin lokala hårddisk så minskar utrymmet på servern snabbt och kapaciteten i systemet kan minska."*

- *"Ok om man följer Microsofts standard, svårare att administrera om man har speciallösningar."*

Användarprofiler

Syftet med användarprofiler är att varje användare skall kunna skräddarsy datorns inställningar för eget bruk. Det ger också administratören möjlighet att kontrollera användarens datormiljö. På denna fråga ansåg personerna i undersökningen att profilens största fördel är att man kan styra användarna till ett gemensamt gränssnitt men att det inte passade i alla situationer.

Exempel på kommentarer:

- *"Fungerar ganska bra faktiskt,, är svåradministrerat, men användarmässigt bra då det ger upphov till ett enhetligt gränssnitt gentemot användarna."*

- *"Med en statiskt miljö och klara förutsättningar, så fungerar det bra."*

- *"Bra när man vill ha samma profil för alla, men när kunden ändrade sig i projektet och ville att vissa skulle kunna ändra vissa inställningar så resulterade det i det problem."*

Systemprinciper

Systemprinciper innebär för administratören att hon/han får ett kraftigt verktyg att begränsa användares möjligheter i systemet. Samtliga var överens om att funktionen innehåller många inställningsbara restriktioner på olika nivåer som administratören kan använda för att styra användarna i systemet. Det finns dock en funktion som orsakar förvirring. I inställningarna finns ett tredje alternativ som komplement till status på en inställning som vanligtvis endast kan vara aktiverad eller avaktiverad. Detta ovanliga alternativ innebär något i stil med "oförändrade inställningar". Det betyder att man låter inställningarna vara som de är i nuläget. Detta upplevs ovanligt krångligt då det i långt ifrån alla situationer går att avgöra vilka inställningar som faktiskt är aktuella. De ansåg också att systemprinciperna lämpade sig bäst i verksamheter som inte är så dynamiska.

Exempel på kommentarer:

- *"Mycket bra restriktioner av användare. Det finns många inställningar."*

- *"Jag föredrar att kontrollera policy med skript, då det är omöjligt att genomföra en skräddarsydd miljö med endast system policy. Jag tycker inte att policy kan ersätta skript."*

- *"Ok om det är en statisk miljö och klara förutsättningar finns. Om utopin existerar där kundens krav är densamma från början till slut."*

- *"Det är speciellt svårt med följdkonsekvenser när man arbetar med principer. Man skapar en princip utifrån en arbetsstation, hur miljön skall se ut för användaren. Så kommer de i efterhand och vill ändra, Då måste man ha kvar grundförutsättningarna, om man då inte har de på grund av att man har ändrad i ett tidigare skede, t.ex. ytterligare installationer av program så måste man skapa grundförutsättningarna på nytt. Missar man då något så vet man inte alls vilka konsekvenser det får."*

Inloggningsskript

Inloggningsskript är en annan metod att för skräddarsy systemet för en enstaka användare eller en grupp av användare. När en användare loggar in med ett konto så körs det eventuella skript som är kopplat till kontot. Intervjun gav bilden av att användningen av inloggningsskript fungerar relativt smärtfritt. Det upplevs däremot att tillvägagångssätt att skapa själva skripten är något förlegat. Lösningen är mest användbar när flera användare laddar samma skript. I de situationer man är tvungen att skapa personliga skript för varje användare så leder det i de fall man har en större mängd användare till ett mycket tidskrävande arbete. Man nämnde även en säkerhetslucka i skripthanteringen som rör åtkomst och laddning av skirpt. En Skriptfil sparas i katalogen Netlogon. Problemet är att eftersom varje konto måste ha åtkomst till filen för att kunna ladda den vid inloggning så kan man inte spärra filen för läsning. Följden blir att även användaren kan öppna filen och ta del av informationen. I de fall som viktiga inställningar sker i skriptfilen är detta olämpligt då användaren erhåller information som inte var avsedd att visas.

Exempel på kommentarer:

- *"Ett fritt verktyg men det känns lite uråldrigt, jag skulle gärna se mer av de mallar och snabba wizards som Microsofts använder på andra ställen."*
- *"Fungerar ok i de fall man har en enhetlig struktur för samtliga användare."*
- *"Nödlösningar hamnar tyvärr ofta i skriptet. Det som man inte kan lösa på annat sätt."*
- *"Skriptet sparas i Netlogon och kan där läsas av användaren som då kan erhålla information om nätverket som igentigen inte skall komma ut."*

Katalog och fil-behörigheter

Med standardbehörigheter för filer och kataloger kan man styra vilka som skall ha tillgång till filen/katalogen samt på vilket sätt. Majoriteten i undersökningen anser att säkerhetsnivån på filer och kataloger i Windows NT är bra men de upplever det svårt att realisera behörigheterna då det ibland är oklart vilka behörigheter som till slut gäller på t.ex. en fil när olika restriktioner är specificerade på olika nivåer i katalog- och filstrukturen . Ett annat problem som upplevs är att det går att på ett enkelt sätt få information om en användares eller grupps sammanlagda behörigheter på alla objekt.

Exempel på kommentarer:

- *"Jag tycker att NTFS förser administratören med det ultimata verktyget och grundlägger såväl säkerheten som driftsäkerhet i just den biten."*
- *"Det är svårt att veta vad som till slut gäller om man t.ex. sätter behörigheter på en fil som man sedan sparar i en katalog som har annorlunda behörigheter."*
- *"Det finns luckor i NTFS, t.ex. när ägaren till en fil inte ger behörighet till någon så kan ända en annan person med hjälp av Kommandotolken (Dos-läge) radera filen."*

Domäner med förtroenderelationer

När två eller flera domäner delar på samma nätverk kan de ställas in för att ”lita” (trust) på varandra. Det gör det möjligt för datorer som hör till en viss domän att ta emot användare som har konton i en annan, förvaltat domän. På frågan hur administration av domäner med förtroenderelationer upplevs är de inblandade av samma åsikt. Förtroenden mellan domän är svårhanterliga, ju fler domäner som skall samverka desto värre. Lösningen upplevs som väldig oflexibel i situationer där man har utgått från vissa premisser och i efterhand blivit tvungna att definiera om förtroenderelationerna.

Exempel på kommentarer:

- *"Jag tycker att användningen av truster är en plåga, särskilt när man blir tvungen att arbeta med en struktur som har fler än två domäner."*

- *"Enkelt att implementera, svårare att administrera när man har komplexa trustförhållanden."*

- *"Väldigt lätt att göra fel och sedan mycket svårt att ändra när man redan har implementerar trusten."*

Behörighetsadministration ur ett vidare perspektiv

Då intervjun övergick från att handla om behörighetssystemets olika funktioner till att behandla behörighetsadministrationen på ett övergripande plan framgick det att de merparten av problemen är baserade på att behörighetssystemet i Windows NT är svåröverblickbart och oflexibelt.

Det är svårt att veta vilka restriktioner som till slut gäller för en användare. Det finns för många delar i behörighetssystemet där man kan definiera rättigheter och behörigheter. Man kan styra användaren genom att sätta rättigheter och behörigheter i användarkonton, kontogrupper, arbetskataloger, användarprofiler, systemprinciper, inloggningsskript, kataloger, filer och i viss mån genom förtroenderelationer. Man ansåg också att det finns för många sätt som man kan skapa dessa restriktioner på. Ofta går restriktionerna in i eller överlappar varandra.

Exempel på kommentarer:

- *"Överblickbarhet, svårt att få reda på övergripande status på en användare."*

- *"Jag har ingen total bild av hur det här fungerar, det har jag verkligen inte."*

De intervjuade berättade att då man kontinuerligt måste göra ändringar som inte var med i de ursprungliga premisserna i kombination med tidsbrist så resulterar det ofta i en situation där administrationen blir komplex och svårhanterad. Man hade klara föresatser från början då man satt och gjorde en planering hur man ville bygga en säker struktur med en så lätthanterlig administration som möjligt.

Sedan dess har förutsättningarna i projektet ändrats flera gånger. T.ex. kom kunden i efterhand med önskemål om att användaren skall kunna byta färg i gränssnittet och ändra upplösning på skärmen. Man blev då tvungen att ändra redan planerad och implementerad administration.

Exempel på kommentarer:

- *"Man läser hur mycket som helst om att förarbetet och studierna innan man implementerar är a och o för att få ett fungerande system. Om man sedan ändrar på förutsättningarna när man redan är i drift slår man undan benen på sig själv."*

- *"Hade man haft rätt förutsättningar från början så hade lösningen kanske blivit bra. Nu är den inte bra på grund av att vi har satt upp systemet efter helt andra förutsättningar än vad vi har nu."*

Det blir en oerhört tidskrävande och komplex uppgift att felsöka. När man inte har en överskådlig bild av behörighetsstrukturen och sedan är tvungen att ändra något är risken stor att man får följdkonsekvenser som inte var planerade. Det intervjuade menade också att det lätt resulterar i att man tar en genväg och löser problemet för stunden. Detta sker ofta på ett sätt som inte är lämpligt, man ger t.ex. en användare för mycket rättigheter istället för att försöka lösa problemet med minimala ändringar av inställningar. Detta i sin tur resulterar i att användarbehörigheten blir ännu mer svåradministrerad och att säkerheten påverkas.

Exempel på kommentarer:

- *"Det finns tillfällen då man är säker på att det man har ändrat inte skall ge några biverkningar någon annanstans vilket det på ett konstigt sätt ändå blir till slut."*

- *"Bekvämlighet och tidsbrist gör det enkelt att ge någon tillfälliga administrationsrättigheter som egentligen inte skall ha det och sedan kanske glömma bort det."*

Kontentan blir idag att man administrera ett system på ett sätt som det inte var tänkt från början. Ett system som är ett resultat av för många ändringar i ett redan planerat systemet. Då man måste ta hänsyn till krav och önskemål som inte var planerade i strukturen från början kräver det ofta i speciallösningar. Då man därefter skall installera nya program eller byta version på befintliga program så vet man inte hur de kommer anpassa sig till en okänd miljö.

Exempel på kommentarer:

- *"Att jag idag är tvungen att administrera NT som det aldrig var tänkt att användas, detta får följdkonsekvenser och kostar tid och pengar, dessutom kan man tänka sig att kompabiliteten vid framtida implementeringar/uppgraderingar av systemet kan ge magsår."*

Under slutet av intervjuerna berördes förslag på åtgärder och önskemål som syftar till att realisera en säker användarmiljö baserad på en fungerande behörighetsadministration.

Exempel på kommentarer:

- *"Följ den standard som Microsoft förespråkar i de fall det är möjligt."*
- *"Lägg rättigheter på gruppnivå så långt det är möjligt."*
- *"Hålla nere antalet domäner och förtroenderelationer så mycket det går. Mycket planering innan"*
- *"Använd överskådlig namnstandard."*
- *" Att Stenhårt följa överenskomna principer och riktlinjer."*
- *"Tydligt uttryckta önskekål hur användaren skall kunna använda systemet."*
- *"Att hellre sänka rättigheter än att höja då det uppstår önskemål eller krav från användare, viktigt att våga stå på sig även om det kan resultera i tvister."*
- *"Håll nere antalet administratörer. Lös aldrig problemet genom att ge administratörsbehörighet till användaren, definiera hellre om användarens rättigheter även om det är tidsödande och krångligt."*

Slutligen fick de intervjuade svara på frågan: Anser du att det går att samtidigt få god säkerhet och enkel administration av användare? På denna fråga talar ett exempel på en kommentar för sig själv:

- *"Ja i teorin."*

Diskussion

Uppsatsens syfte har varit att undersöka de faktorer som påverkar administrering av använda Uppsatsens syfte har varit att undersöka res rättigheter och behörigheter i Windows NT och som i förlängningen kan påverka säkerheten i systemet. Diskussionen kommer att föras utifrån den teoretiska referensramen i kombination med resultaten från intervjuerna.

Behörighetssystemets olika funktioner

Säkerhetsfunktionerna i Windows NT skall skydda datorn och dess data genom att kontrollera vilka som kan använda datorn och hur de använder den. Groves (1993) skriver att en av de viktigaste målsättningarna med Windows NT var att göra operativsystemet så säkert som möjligt utan att för den skull göra det avsevärt svårare att använda detta. Säkerhetsfunktionerna har varit i åtanke från början och under hela arbetet med att utveckla systemet. Groves anser att resultatet har blivit att säkerheten är lika lätt att hantera som alla andra delar av NT

Har Microsofts verkligen lyckats med föresatsen? Stämmer Groves uppfattning med verkligheten? Av intervjun framgick att säkerhetsadministrationen i Windows ofta inte upplevs så enkel och komplett som det anges i litteraturen om Windows NT.

Konton

När det gäller själva behörigsystemets uppbyggnad och olika komponenters funktionalitet så anger Microsoft Corporation (1996) att hanteringen av konton och grupper visserligen kräver planering men att själva proceduren för att administrera konton är enkel och lätthanterlig. I undersökningen framgår det att hanteringen av konton fungerar bra så länge som man har ett mindre antal användare men i de fall man skall administrera ett större antal användare så uppstår problem. Det saknas ett funktionellt och överblickbart verktyg för att utröna en användare sammanlagda rättigheter, vilket knappast kan ersättas med grundlig planering. Detta medför en risk när ett konto skall modifieras. Man kan då missa information om användarens rättigheter. Följden kan bli att modifieringen av rättigheterna tillsammans med den missade information ger användaren rättigheter långt över den tänkta.

Grupper

Enligt Microsoft (1996) är syftet med grupper att förenkla administrationen av användare som har liknande rättigheter och privilegier i systemet. Microsoft skriver att användningen av grupper medför en enkel hantering när man skall förse ett set användare med lämpliga befogenheter. Det stämmer om man jämför med att inte använda grupper överhuvudtaget. Men då Microsoft uppenbarligen har försökt möjliggöra en enklare hantering av konton är jag förundrad över att Microsoft inte har utvecklat konceptet med grupper mer än vad som är gjort. De har skapat grupper för att förenkla kontohanteringen men har inte förenklat själva grupphanteringen. De har flyttat en del av problemen som tillhör kontohanteringen till att istället gälla hanteringen av grupper. Det finns en klar avsaknad av möjligheten att kunna ordna grupper hierarkiskt. Microsoft har också utvecklat användningen med lokala och globala grupper onödigt krångligt. För det första är det inte ens logiska namn på grupperna.

Jag förstår inte hur man kan använda benämningen: lokala grupper och globala grupper när man kan göra en global grupp som medlem i en lokal grupp men inte tvärt om. Vore det inte mer logiskt att byta namn på grupperna? Eller framför allt att konstruera om lösningen med grupper. För det andra upplevs arbetssättet med globala grupper som används över domängränser onödigt svårhanterligt. Vore det inte betydligt enklare att endast använda en sorts grupper och göra det möjligt att använda gruppen för att ge användare tillgång till resurser i andra domäner ? Detta problem har antagligen uppmärksammats av Microsoft. I kommande version av Windows NT (Windows 2000) finns inte längre denna konstruktion. Bristen av ett bra sökverktyg för att t.ex. se vilka grupper som har en speciell rättighet kopplad till sig medför att samma risk som påpekades i kontohanteringen gäller även i hanteringen av grupper. Faktum är att det i administrationen föreligger en ännu högre risk då man ofta sätter merparten av rättigheter på just gruppnivå vilket medför att biverkningarna kan bli större.

Arbetskataloger

Att ge en användare en arbetskatalog skall göra det lättare för dels användare och dels administratören att hålla reda på användarens filer genom att de koncentreras till en specificerad plats. Denna hantering fungerar i stora drag tillfredsställande. De intervjuade hade i och för sig synpunkter på att det finns för många sätt att skapa arbetskataloger. Jag anser att det inte är något problem så länge de hanteras konsekvent. I de fall där det inte är möjligt kan det emellertid vara ett problem. En funktion som dock saknas i systemet är en rutin för att begränsa det utrymme som en arbetskatalog kan ta i anspråk. Detta problem kan väl i och för sig inte påstås påverka säkerheten. Möjligen kan en illvillig användare fylla utrymmet på servern och därmed till slut orsaka att systemet blir obrukbart. Användaren kan däremot inte ta del av eller modifiera information som hon/han inte har tillåtelse att göra. Ett annat problem som inte heller det kan anses påverka säkerheten är när Windows NT själv skapat arbetskatalogen för användarna. I de fall då man har många användare blir det svårt för användaren att hitta sin katalog bland alla de andra. Detta problem har emellertid en lösning. Man ansluter (mappar) katalogen som en enhet till t.ex. användarens "H:" med hjälp av ett inloggingsskript. Denna lösning medför att användaren ser sin arbetskatalog som en egen logisk enhet.

Användarprofiler

Om användarprofiler skriver Groves (1993) att Windows NT har utformats för att på ett enkelt sätt låta flera användare i tur och ordning använda samma dator. När ett konto skapas för en användare håller NT reda på dennes användarinställningar. Man kan som administratör också använda den här funktionen för att skräddarsy datorns inställningar till varje användares krav och behov.

Användningen av profiler fungerar riktigt bra så länge man arbetar med en relativt statisk miljö med klara förutsättningar. Funktionen fungerar dock inte lika bra om man vill standardisera användarnas miljö i en dynamisk situation. Jag anser dock att detta problem inte orsakas av själva arbetssättet med användarprofiler. Lösningen bygger ju på att man antingen ger användarna friheten att skapa sina egna inställningar eller att man försäkrar sig om att man inte får en dynamisk situation där man kontinuerligt är tvungen att göra ändringar i konfigurationen. I de fall man har en föränderlig miljö och ändå är tvungen att styra användarnas inställningar så medför det med rätta stora problem.

Jag har svårt att se hur Microsoft skulle kunna konstruera en lösning som är så flexibel att man kan styra användarna med standardiserade inställningar och samtidigt ge dem frihet att utforma sina egna arbetsmiljöer. Det låter som en paradoxal uppgift.

Systemprinciper

Med systemprinciper kan man kontrollera en användares arbetsmiljö och handhavande. Restriktionerna kan specificeras för en enskild användare eller en grupp av användare. Man kan också konfigurera varje dator i nätverket. Microsoft har av någon anledning konstruerat tre alternativ för varje inställning; aktiverad, avaktiverad och oförändrad. Anledningen till denna lösning har jag i skrivandets stund inte lyckats utröna. I litteraturen anges inte heller någon förklaring till konstruktionen. Jag antar att tanken bakom kanske är att det skall förenkla på något sätt. I teorin låter det ju bra att kunna behålla inställningarna som de är och komplettera med en liten ändring. Klart är däremot att den i vissa situationer kan ge upphov till komplikationer vid praktisk tillämpning. Det är inte alltid som man är medveten om vilka inställningar som för nuvarande gäller. Ofta vet man bara att arbetsmiljön fungerar. Detta kan resultera i svårigheter när man upprepande gånger ändrar systemprinciperna. Då man från gång till gång inte vet vad inställningarna innebär kan det i slutändan resultera i att man har konfigurerat en princip med ett speciellt syfte, som i själva verket beter sig på ett annorlunda sätt. Detta medför att man inte vet gällande status i systemet vilket för en administratör är något av det farligaste som finns. Denna risk borde egentligen inte existera. Jag anser att ett sådant här kraftigt verktyg skall kunna användas i en verksamhet där man ibland ändrar premisserna i systemet.

Det finns också en mer konkret risk när man använder datorprinciper. Ett princip laddas när en användare loggar in i Windows NT. Då man använder datorprinciper så laddas principen från den domän som användaren loggar på. Detta medför att om användaren loggar på en annan domän som hon/han är behörig i men som inte använder samma datorprinciper så gäller inte de restriktioner som är specificerade i den ursprungliga domänen. Följden bli att användaren kan få tillgång till applikationer och funktioner som det inte är tänkt användaren att skall ha och därmed påverkas säkerheten. Det är därför viktigt att implementera en enhetlig konfiguration av datorprinciper i samtliga domäner som användaren är behörig i.

Inloggningsskript

Inloggningsskript kan användas till att konfigurera en användares arbetsmiljö genom att skapa nätverkskopplingar och starta applikationer. Groves (1993) anser att inloggningsskript är en enkel och praktisk metod för att skräddarsy systemet för en enstaka individ eller grupp av användare.

Utifrån intervjuer och litteratur är jag beredd att hålla med, men det finns två nackdelar. Det första rör själva tillvägagångssättet vid skapandet av skriptet. Det uppfattas som något förlegat. Man är i Windows van vid att man anger inställningar i antingen fördefinierade dialogrutor eller med hjälp av inbyggda wizards. Denna nackdel påverkar knappast systemet såvida man inte skriver felaktiga kommandon i skripet. Man får helt enkelt hoppas att administratören är tillräcklig kompetent och noggrann så det inte inträffar. Den andra nackdelen påverkar däremot i högre grad säkerheten i systemet. En användare kan öppna skriptfilen och läsa den information som är angiven där. Informationen kan t.ex. bestå av nätverksinställningar mm.

Användaren kan då få information om hur nätverket är strukturerat etc. vilket självklart inte är lämpligt ur säkerhetssynpunkt. Detta problem kan mildras något genom att administratören specificerar en granskning (Audit) på skriptfilen. Händelsen registreras i en säkerhetslogg, men risken är när administratören väl blir medveten om att någon har tagit del av informationen i skriptet kan det redan vara försent.

Katalog och fil- behörigheter

På en partition som är formaterad med NTFS kan man sätta katalogbehörighet och filbehörighet som anger vilka användare eller grupper som är behöriga samt på vilka nivåer de är det. Jag anser att Windows NT förser användare och administratörer med goda möjligheter att styra vilka som skall ha behörighet till kataloger och filer. Det uppstår dock snabbt ett problem då man använder sig av olika nivåer av restriktioner för olika användare och grupper. Det saknas en funktion för att på ett överskådligt sätt utröna vilka objekt en användare eller en grupp har behörighet till och vilken nivå av behörighet. Detta problem belyses av Sheldon (1996):

> *"To check permissions on folders and other resources, you must go to each resource individually to review which users and groups have permissions. This can be a bewildering task."*

Det är troligt att Microsoft inte anser det vara värt eller att det är för kostsamt att utveckla ett verktyg som söker igenom katalogstrukturen och specificerar vilka filer och kataloger en användare har behörighet till samt vilken grad av behörighet. Jag tycker att det är beklagligt då ett sådant verktyg verkligen skulle underlätta administrationen.

Det är också krångligt att hålla reda på vilken behörighet som i slutändan gäller för ett objekt som ligger längst ner i hierarkin om olika behörigheter är satta på högre instanser. Detta medför att man får en svårhanterlig administration av behörigheter på kataloger och filer vilket kan resultera i att säkerheten blir lidande då man inte alltid vet status. Somarsoft (1994) skriver att ett vanligt fel när filer och kataloger får felaktiga behörigheter baseras på skillnaden när ett objekt kopieras och flyttas. Kopieras filen ärver filen rättighterna från katalogen den kopieras till medan en fil som flyttas i katalogstrukturen behåller sin behörighet. Här blir det uppenbart vilka krångliga regler behörighetsadministrationen baseras på. Jag får känslan av att Microsoft i sin iver att konstruera ett säkert filsystem har satsat på en alltför stark kombination av hög säkerhet och flexibilitet, vilket har resulterat i att administrationen av filer och kataloger har blivit alltför svårhanterlig.

Den säkerhetslucka som anges i resultatet av intervjuerna och som går ut på att man i NTFS-Dos kan radera en fil trots att man inte har någon som helst behörighet till den kan motverkas med användning av systemprinciper. Man spärrar då Kommandotolken så att användaren inte kommer åt den.

Granskning

Granskning är en funktion som fungerar riktigt bra, jag anser att den till viss mån täcker en del av missarna i konstruktionerna av de övriga delarna i behörighetssystemet. Då angivna händelser registreras i säkerhetsloggen har administratören möjlighet att övervaka och spåra användare och gruppers aktiviteter. För att denna funktion skall ha någon nytta krävs självklart att administratören kontinuerligt undersöker säkerhetsloggen.

Det som vore önskvärt och som Microsoft har missat i konstruktionen är ett meddelandesystem så att administratören blir uppmärksam så fort något har inträffat i systemet. Detta har uppmärksammats av andra mjukvarutillverkare vilket har resulterar i att det finns en uppsjö av tredjepartsprogram som kan sköta om denna uppgift.

Domäner med förtroenderelationer

Med följande citat lovordar Microsoft Corporation (1996) användningen av förtroenderelationer mellan domäner:

> *"Trust realationship move the convenience of centralized administration from the domain level to the network level. By establishing trust relationships between the domains on your network, you enable user accounts and global groups to be used in domains other than the domain where theses accounts are located. You need to create each user account only once, and because directory service enable syncronization of all security data in the database, the account can be given access to any computer on your network – not just the computers in one domain."* (s. 37)

Det går inte att komma ifrån att man uppnår en hel del fördelar med domäner. För nätverk med en domän eller en master domain är det inga större bekymmer att använda Windows NT. Det finns dock en baksida av ovanstående citat som ger sig tillkänna från intervjuerna och ingående litteraturstudier. Skall man ha flera master domains och resource domains eller en så kallad Complete Trust Domain Model blir det ett konststycke att bygga ett bra nätverk. Mitrovic (1997) skriver att den största nackdelen med Windows NT som nätoperativsystem framför allt gäller implementationen av domäner och behovet av släktskap. Det finns enligt Mitrovic många företag som har låtit bli att använda Windows NT just på grund av domänmodellen. Det som är väsentligt är vad NT kostar att installera, administrera och att utveckla i förhållande till andra system.

När man har en komplex domänstruktur med många förtroenderelationer är det svårt att ändra i strukturen på grund av att den ofta är väldigt låst. I de fall man har en dynamisk verksamhet medför det mycket extra arbete. Säkerheten i systemet påverkas i regel inte såvida man inte använder nödlösningar istället för att komma till rätta med problemet på rätt sätt. Det kräver dock mycket tid och energi som skulle kunna användas för andra ändamål. Det verkar dock som om att Microsoft har uppmärksammat svårigheterna. I Windows 2000 är konstruktionen med domäner och förtroenderelationer modifierade och har inte samma innebörd som i nuvarande version.

Behörighetsadministration ur ett vidare perspektiv

Enligt Olofsson (1996) beror grundproblemet på komplexiteten i client/server-systemen. I och med att resurserna i nätet distribueras blir det svårt för administratörer att hålla reda på exakt vilken hård- och mjukvara som finns i nätverket och vilka användare som ska ha behörighet till vad. Administrationen av användarnas behörigheter riskerar därför att bli krånglig. De som ansvarar för och arbetar med säkerheten i ett client/server-system måste kunna anlägga en helhetssyn, så att en erforderlig skyddsnivå kan bibehållas. Kan man inte det är det svårt att vara konsekvent i sitt arbete med att administrera användares rättigheter och behörigheter.

Enligt SIG Security (1993, s29) är ofta den interna säkerheten i systemet baserad på bristande administrativa funktioner så att administratörer inte ges tillräcklig överblick över vidtagna åtgärder och deras effekt.

I Windows NT består problemet i behörighetssystemet av två faktorer. Det första är att behörighetssystemet består av för många olika delar. På grund av denna spridning av funktioner är det svårt att få en bild av vilka rättigheter och restriktioner en användare har i systemet. Man skulle lösa en del av problemet genom att konstruera lätthanterliga verktyg för att lättare kunna överblicka administrationen. Då Microsoft ständigt påpekar säkerheten i Windows NT är det förvånande att man inte har satsat resurser på detta problem. Då det tyvärr inte utan tredjepartsprodukter existerar applikationer för detta ändamål är risken stor att man får oönskade konsekvenser vid administrationen. Groves (1993) tar upp vikten av att veta vad en modifiering i systemet innebär:

> *"Kom ihåg att varje rättighet innebär ett möjligt kryphål i datorns säkerhetssystem. Eftersom okritisk tilldelning kan underminera datorsäkerheten……Befogenheten att tilldela andra användare rättigheter bör utövas försiktigt och bara av användare som inser konsekvenserna av det"* (s.108)

Felsökning beroende på konsekvenserna blir ett komplex och tidskrävande arbete. Det resulterar ofta i att man istället försöker lösa problemet tillfälligt. Här kolliderar kravet på rationell och snabb hantering med kravet på hög säkerhet. Då detta arbetssätt kontinuerligt fortskrider får man en behörighetsstruktur som allt mer baseras på nödlösningar av olika slag. Detta i sin tur resulterar i att man till slut ”målar in sig i ett hörn” och uppgiften att administrera användare konsekvent och effektivt blir allt mer komplex. Sakta men säkert undermineras därmed säkerheten i systemet.

Den andra faktorn är att de specificerade restriktionerna i funktionerna i många avseenden överlappar varandra. Det är svårt att skilja på var en rättighet slutar och en annan börjar. De regler som anger vilken prioritet rättigheterna har i förhållande till varandra beror i för hög grad på i vilken situation rättigheterna nyttjas. Det är svårt att dra generella slutsatser från en struktur till en annan vilket medför att det är krångligt att tillämpa reglerna generellt.

För att ändå motverka en situation som ovan kan man i vissa fall kompensera med olika åtgärder när ett client server-system skall utformas. De säkerhetsmässiga kraven måste analyseras på ett tidigt stadium. Redan i en förstudie bör kraven på tillgänglighet, riktighet och sekretess kartläggas. Detta gäller både den befintliga situationen och en framtida situation.
Marcey & Wendall (1997) förklarar i klartext:

> *"NT provides the ability to have a highly secure system only with the correct configuration and object access controls. Operating systems don’t make security problems go away. There is not an operating system available today that can provide you with a complete security solution."*

Det är således oerhört viktigt att man planerar innan man implementerar systemet. Det finns också viktiga punkter att ta hänsyn till när systemet är i drift. SIG Security (1993) skriver att administratörer skall ha givna rutiner för en konsekvent tilldelning av rättigheter. De måste också ha tillräckligt med tid för att utföra sitt arbete som behörighetsadministratörer samtidigt som det skall finnas en överordnad uppföljning av administratörsarbetet.

Vid den dagliga hanteringen av rättigheter och behörigheter bör man alltid ta hänsyn till regeln om minsta möjliga privilegier. Hedemalm (1998) förklarar innebörden:

> *"En bra idé är att inte använda mer säkerhet (och därmed krångel) än vad som behövs. Allt som känns som en komplikation riskerar att kringgås eller leda till förvirring. Nätverket bör liksom andra organisationsfrågor, vara ett ständigt informationsämne."* (s. 28)

Slutsats

Några av problemen som upplevs i undersökningen härrör från att det i projektet har tillkommit ändringar i ett system som från början var tänkt att vara ovanligt styrt och standardiserat. Dock kvarstår det faktum att det inte går att bortse ifrån att det finns delar i behörighetssystemet som inte fungerar på ett tillfredsställande sätt. Undersökningens resultat att visar behörighetssystemet är för komplext uppbyggd och svåröverskådligt och innehåller oklara prioritetsregler. Svårigheter i behörighetsadministrationen kan därför påverka säkerheten i system. Windows NT passar bäst i en relativt statisk miljö. I de fall Windows NT används i dynamiska miljöer kan man lindra problemen genom god planering, klara förutsättningar och rutiner för en konsekvent administration.

Kritik

Kritik som kan anföras mot den använda metoden är att även om syftet är att observera förutsättningslöst så är det i princip omöjligt att vara helt objektiv mot det man undersöker. Det är därför troligt att mina egna tankar och uppfattningar om undersökningsområdet har präglat uppsatsen. Resultatet har säkerligen också formats av syftet med undersökningen. Om syftet t.ex. är att belysa vilka problem som finns i en verksamhet kan det medföra att varje tänkbart blir till ett verkligt problem. Även om man försöker ta hänsyn till detta tror jag att man ofta omedvetet gör detta misstag.

Fortsatt arbete och framtida forskning

Snart kommer nästa version av Windows NT. Flera betaversioner har redan släppts. Vad vore intressantare än att undersöka den och göra en jämförelse mellan versionerna? Man kan också tänka sig en jämförelse med ett annat nätoperativsystem såsom Novell eller Unix.

Referenser

Böcker

Backman, J. (1998). *Rapporter och uppsatser*. Lund: Studentlitteratur.

Carter, A. R. (1997). *Windows NT 4.0 MSCE Study Guide.* Foster city, CA: IDG Books.

Casad, J., Dalton, W., & Tate, S. (1997). *MSCE Training guide: Windows NT Server 4* (4th ed.). Indianapolis: New riders.

Dataföreningen i Sverige. (1997). *Steg för steg mot bättre IT-säkerhet*. Stockholm: DF.

Doyle, C. (1996). *Windows NT Server networking guide*. Washington, DC: Microsoft Press.

Galli, P., & AlfaNet Communications ab. (1992). *Informationssäkerhet*. Linköping: Affärslitteratur.

Groves, J. (1993). *Boken om Windows NT*. Stockholm: Liber Utbildning.

Hedemalm, G. (1998). *Nätverk från grunden*. (3:e rev uppl.). Sundbyberg: Pagina.

Le Duc, M. (1998). *Introduktion till begrepp och metoder inom Informatik med Systemvetenskap i samband med uppsatsarbete*. Institutionen för Ekonomi och Informatik, Stockholm University.

Le Duc, M. (1996). *Constructicvist Systemics. Theoretical Elements and Applications in Environmental Informatics*. Doctorsavhandling. School of Business, Stockholm University.

Microsoft Corporation (1996). *Windows NT server 4: Concepts and planing*. Washington, DC: Microsoft press.

Mitrovic, P. (1997). *Microsoft NT 4 & Intranetware*. Stockholm: IDG.

Patton, M. Q. (1990). *Qualitative Evaluation and Research Methods*. (2nd ed.). Newbury Park: Sage.

SIG Security. (1999). *Säkerhetsarkitekturer*. Lund: Studentlitteratur.

SIG Security (1993). *Client/server och säkerhet*. Lund: Studentlitteratur.

Internet

Bratt, H. I. (1998). *ITfacts*. [online document 1999-04-09]. URL http://www.itfacts.com.sida.asp?nr=161

Marcey, K., & Wendall, M. (1997). *Windows NT Network Security A Manager's Guide*. [online document 1999-04-17]. URL http://ciac.llnl.gov/index/documents.html

Microsoft Corporation .(1999). [www document1999-05-02]. URL http://www.microsoft.com/ntserver/security/default.asp

Olofsson, K. (1996*). Komplicerad säkerhet i client-serversystem*. [online document 1999- 05-02]. Computer Sweden nr 63 1996 i avdelningen Nätverk. URL http://domino.idg.se/cs/artikel.nsf/e8a76acf828e0088c12566d70055dfe6/ff3f0c1f97e9b0b2c12564e4004fd6d3?OpenDocument

Sheldon, T. (1996). *Steps for Evaluating the Security of a Windows NT® Installation.* [online document 1999-04-13].URL http://www.ntresearch.com/ntchecks.htm

Somarsoft, Inc. (1994). *Windows NT Security Issues.* [online document 1999-04-13]. URL http://www.somarsoft.com/security.htm

Bilaga 1 Rättigheter och behörigheter i Windows NT.

Tabell 1. Beskrivning av användares olika rättigheter i Windows NT, Carter (1997).

Rättighet	Avancerad	Beskrivning
Åtkomst till den här datorn från nätverket	Nej	Låter en användare ansluta till datorn över nätverket.
Agera som en del av operativsystemet	Ja	Används normalt inte av administratörer. Används av de som programmerar applikationer i Windows NT.
Koppla klienter till domänen	Nej	Låter användaren rättighet att koppla klienter till domänen
Ta back up filer och kataloger	Nej	Låter en användare ta back up på filer och kataloger i datorn. Denna rättighet åsidosätter katalog- och filbehörigheter.
Kringgå bläddringskontroll checking	Ja	Låter användaren rättighet att ändra kataloger och söka igenom katalogträd även om inte användaren inte har behörighet till katalogerna.
Ändra systemtiden	Nej	Låter användaren rättighet att ändra tiden på datorns interna klocka.
Skapa Swap-fil	Ja	Används normalt inte av administratörer. Används av de som programmerar applikationer i Windows NT.
Skapa ett token objekt	Ja	Används normalt inte av administratörer. Används av de som programmerar applikationer i Windows NT.
Skapa permanenta delade objekt	Ja	Används normalt inte av administratörer. Används av de som programmerar applikationer i Windows NT.
Debug programs	Ja	Används normalt inte av administratörer. Används av de som programmerar applikationer i Windows NT.
Fjärravsluta Windows NT	Nej	Denna rättighet är för närvarande inte implementerad. Den är reserverad för framtida användning.
Generera Säkerhets audits	Ja	Används normalt inte av administratörer. Används av de som programmerar applikationer i Windows NT.
Öka quotas	Ja	Används normalt inte av administratörer. Används av de som programmerar applikationer i Windows NT.
Öka prioritet på scheduling	Ja	Används normalt inte av administratörer. Används av de som programmerar applikationer i Windows NT.
Ladda och stänga ner drivrutiner	Ja	Låter en användare ladda och ta bort drivrutiner dynamiskt.
Låsa sidor i minnet	Ja	Används normalt inte av administratörer. Används av de som programmerar applikationer i Windows NT.
Logga på som ett batch jobb	Ja	Används normalt inte av administratörer. Används av de som programmerar applikationer i Windows NT

Logga in som en tjänst	Ja	Låter en process registreras som en tjänst i systemet. Det här är en avancerad användarrättighet.
Logga Lokal inloggning på lokalt	Nej	Låter användaren rättighet att logga på lokalt på den dator.
Hantera granskning och säkerhetslogg	Nej	Låter användaren rättighet att se och ändra säkerhetsloggen. Gör det möjligt för användaren att konfigurera auditing på filer, kataloger och skrivare.
Modifiera miljövariabler	Ja	Används normalt inte av administratörer. Används av de som programmerar applikationer i Windows NT.
Profilera enkel process	Ja	Används normalt inte av administratörer. Används av de som programmerar applikationer i Windows NT.
Profilera system	Ja	Används normalt inte av administratörer. Används av de som programmerar applikationer i Windows NT.
Byta ut en process token	Ja	Används normalt inte av administratörer. Används av de som programmerar applikationer i Windows NT.
Återställ filer och kataloger	Nej	Låter en användare återställa filer och kataloger i datorn. Denna rättighet åsidosätter fil- och katalogbehörigheter.
Stänga ner systemet	Nej	Låter användaren stänga ner Windows NT.
Bli ägare till filer och andra objekt	Nej	Låter en användare ta över ägande av filer, kataloger och andra objekt i datorn.

Tabell 2. Beskrivning av inbyggda grupper på en domänkontrollant i Windows NT, Carter (1997).

Fördefinierad grupp	**Grupp**	**Beskrivning**
Administratörer	Lokal	Har fulla administrativa rättigheter och behörigheter att administrera en domän. Innehåller inledningsvis den globala gruppen domänadministratörer
Back up Operatörer	Lokal	Har behörighet att ta back up och återskapa filer och kataloger i alla domänkontrollanter i en domän
Gäster	Lokal	Har i grundutförandet inga behörigheter. Innehåller inledningsvis den globala gruppen Domängäster
Replikator	Lokal	Används av tjänsten katalogreplikator i Windows NT
Användare	Lokal	Har i grunden inga behörigheter. Innehåller den globala gruppen Domänanvändare
Konto Operatörer	Lokal	Kan skapa, radera och modifiera användarkonton, lokala grupper och globala grupper med undantag av grupperna Administratörer och Server Operatörer .
Skrivare Operatörer	Lokal	Kan initiera och hantera skrivare på varje domänkontrollant i domänen.
Server Operatörer	Lokal	Har behörighet att ta back up och återskapa filer och kataloger på alla domänkontrollanter i domänen.
Domän Administratörer	Global	Har i grunden inga behörigheter. Innehåller inledningsvis det fördefinierade kontot Administratör
Domän Användare	Global	Har i grunden inga behörigheter. Innehåller inledningsvis det fördefinierade användarkontot Administratör. När nya konton skapas ingår de automatiskt i denna grupp.
Domän Gäster	Global	Har i grunden inga behörigheter. Innehåller inledningsvis det fördefinierade kontot Användare.

Tabell 3. Beskrivning av inbyggda grupper på en fristående server i Windows NT, Carter (1997).

Fördefinierad grupp	**Grupp**	**Beskrivning**
Administratörer	Lokal	Har fulla administrativa rättigheter och behörigheter att administrera datorn. Innehåller inledningsvis det fördefinierade kontot Administratör
Back up Operatörer	Lokal	Har behörighet att ta back up och återskapa filer och kataloger på datorn.
Gäster	Lokal	Har i grundutförandet inga behörigheter. Innehåller inledningsvis det fördefinierade kontot Gäst
Replikator	Lokal	Används av tjänsten katalogreplikator i Windows NT
Användare	Lokal	Har i grunden inga behörigheter. När ett nytt användarkonto skapas blir det automatiskt medlem i denna grupp.
Makt Användare	Lokal	Kan skapa och modifiera användarekonton och grupper med undantag av kontot Administratör och gruppen Administratörer. Kan dela ut kataloger och skrivare

Tabell 4. Beskrivning av granskningsbara händelser i Windows NT, Carter (1997).

Händelse	**Beskrivning**
In- och utloggning	En användare loggade in eller ut på arbetsstationen eller upprättade en nätverksanslutning.
Fil- och objektåtkomst	En användare använde en katalog eller fil som granskas eller sände ett utskriftsjobb till en skrivare som granskas.
Utnyttjande av rättigheter	En användare utnyttjade en rättighet (annan än de rättigheter som gäller för inloggning och utloggning).
Hantering av användare och grupper	Något av följande hände: Ett användarkonto eller en grupp skapades, ändrades eller togs bort. Ett användarkonto bytte namn, inaktiverades eller aktiverades. Ett lösenord angavs eller ändrades.
Ändringar i säkerhet	En ändring gjordes av Rättigheter eller Granskning.
Omstart, avstängning och händelser som påverkar säkerheten	En användare startade om eller stängde av datorn, eller också påverkade en händelse systemets säkerhet eller säkerhetslogg.
Processpårning	Dessa händelser ger detaljerad spårningsinformation för vissa händelser, t ex programstart, indirekt åtkomst av ett objekt och processavslut.

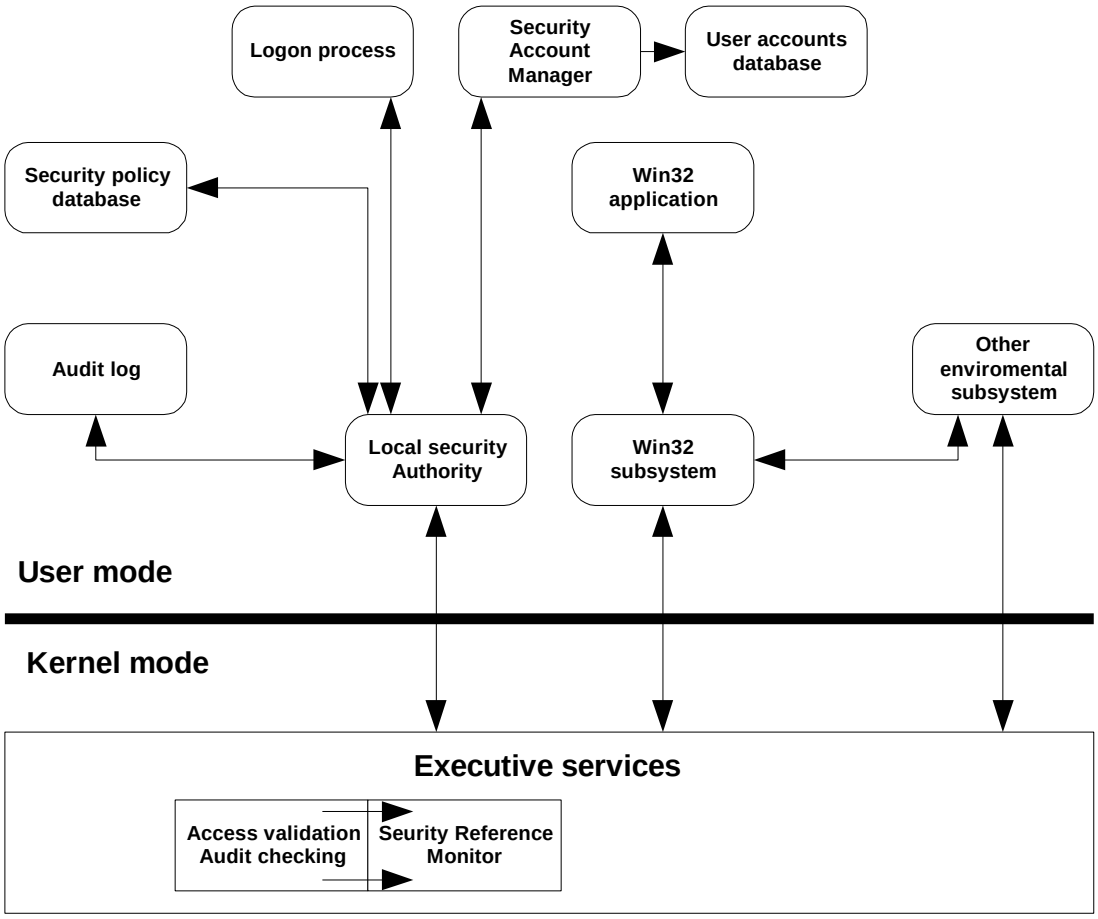
Tabell 5. Beskrivning av definierbara behörigheter på kataloger i Windows NT, Casad & Dalton & Tate (1997).

Behörighet	**Beskrivning**
Ingen åtkomst	Förhindrar all åtkomst till katalogen och dess filer. När du anger Ingen åtkomst för en användare förhindras åtkomst även om användaren tillhör en grupp som har åtkomst till katalogen.
Lista	Gör det möjligt att: Visa filnamn och namn på underkataloger och Ändra katalogens underkataloger. Du kan inte: Ansluta till filer, om inte åtkomst ges av annan katalog- eller filbehörighet.
Läsa	Gör det möjligt att: Visa filnamn och namn på underkataloger. Ändra katalogens underkataloger. Visa data i filer och köra program.
Lägga till	Gör det möjligt att: Lägga till filer och underkataloger i en katalog. Du kan inte: Ansluta till filer, om inte åtkomst ges av annan katalog- eller filbehörighet.
Lägga till och läsa	Gör det möjligt att: Visa filnamn och namn på underkataloger. Ändra katalogens underkataloger. Visa data i filer och köra programfiler. Lägga till filer och underkataloger i en katalog.
Ändra	Gör det möjligt att: Visa filnamn och namn på underkataloger. Ändra katalogens underkataloger. Visa data i filer och köra programfiler. Lägga till filer och underkataloger i en katalog. Ändra data i filer. Ta bort katalogen och dess filer.
Fullständig behörighet	Gör det möjligt att: Visa filnamn och namn på underkataloger. Ändra katalogens underkataloger. Visa data i filer och köra programfiler. Lägga till filer och underkataloger i en katalog. Ändra data i filer. Ta bort katalogen och dess filer. Ändra behörighet för katalogen och dess filer. Överta ägarskap av katalogen och dess filer.

Tabell 6. Beskrivning av definierbara behörigheter på filer i Windows NT, Casad & Dalton & Tate (1997).

Behörighet	**Beskrivning**
Ingen åtkomst	Förhindrar all åtkomst till katalogen och dess filer. När du anger Ingen åtkomst för en användare förhindras åtkomst även om användaren tillhör en grupp som har åtkomst till katalogen.
Läsa	Gör det möjligt att: Visa data i filer. Köra filen (om det är en programfil).
Ändra	Gör det möjligt att: Visa data i filer. Köra filen (om det är en programfil). Ändra data i filen. Ta bort filen.
Fullständig behörighet	Gör det möjligt att: Visa data i filer. Köra filen (om det är en programfil). Ändra data i filen. Ta bort filen. Ändra behörighet för filen. Överta ägarskap av filen.

Bilaga 2 Säkerhetsmodellen i Windows NT.



Figur 1. Figuren härstammar ursprungligen från Mitrovic (1997,s 35) och visar hur säkerhetsmodellen i Windows NT är uppbyggd.

Bilaga 3 Intervjumall.

PERSONLIGT

1. Vilken är benämningen på din nuvarande anställning inom företaget?
2. Vad är din nuvarande arbetsuppgift?
3. Vilka är dina tidigare meriter (anställningar/utbildningar mm) inom dataområdet?
4. Hur länge har du arbetat med uppgifter relaterade till nätverk?

WINDOWS NT / UPPBYGGNAD

5. Hur upplever du att det är att arbeta med (fördelar/nackdelar):
    - Konton (User Account)?
    - Systemprinciper (System Policy)?
    - Grupper (Group Account)?
    - Profiler (User Profile)?
    - Arbetskataloger (Home Directory)?
    - Inloggningsskript (Loggon Script)?
    - Katalog- och filbehörigheter (Directory and File Permission)?
    - Förtroenderelationer (Trust Relationship)?

ADMINISTRATION I SIN HELHET

6. Är det något du anser fattas vid administration i Windows NT Server?
7. Är det något du anser fattas vid administrationen i Windows NT Workstation?
8. Vad anser du att man skall tänka på när administrerar användare?
9. Vilka övergripande problem upplever du vid administration av användares behörighet och rättigheter?
10. Vad anser du vara de största "fällorna" inom behörighetsadministrationen?
11. Anser du att det går att samtidigt få en hög säkerhet och enkel administration?
12. Vad vore önskvärt vid administrationen?