Sikkerhed
i et
dokument management system
(ELO Professional 5)

Martin Lind

Hørsholm 2007
IMM-B.ENG-2007-28

Forord

Denne rapport handler om, hvad ELO[1] har gjort for at sikre deres system mod angreb fra en hacker. ELO Professional 5 er et dokument management system, som også har indbygget workflow for filerne i systemet. ELO Professional 5 består af arkiver med en SQL database til hvert arkiv. Databaserne indeholder metadata til hver af de filer, som er i arkivet, f.eks. datoen hvor filen blev lagt i arkivet, stien til filen og det navn som bliver vist i ELO osv. ELO vil med deres produkter skabe en slags rygrad, hvor alle virksomhedens filer kan ligge i. Med denne rygrad vil de skabe større sporbarhed, i virksomhedens arkiver, således at filer nemt kan findes. ELO's mål er at integrere så mange programmer som muligt, så det er muligt at anvende ELO til at arkivere filer fra de programmer man anvender. Af de programmer som allerede er integreret i ELO, kan nævnes; Microsoft Office pakken, SAP, Navision og BAAN. Målet er at alle virksomhedens filer i sidste ende skal være i ELO arkiver og ikke bare i mapper i Windows, hvor sporbarhed er lav, og sikkerheden kan være svær at få styr på fordi brugerne selv opretter en masse mapper.
I rapporten gennemgås de Windows funktioner som ELO bruger til at beskytte data med i arkiverne. Derudover gennemgås hvad ELO programmet gør for at beskytte data, og hvilke foranstaltninger der er foretaget for at hindre brugere i at se og ændre filer, som ikke er relevante for netop dem.
I forbindelse med dette eksamensprojekt er der blevet udviklet et program, med henblik på at understøtte og sikre at den nuværende sikkerhedsopsætning af ELO, er så fejlfri som muligt.

Jeg takker min vejleder Jens Thyge Christensen for at komme med kritiske kommentarer og forslag til rapporten. Jeg vil også gerne takke ELO Digital Office og deres danske afdeling med Bent Okholm i spidsen for at give mig muligheden for at udarbejde denne opgave og give mig spændende udfordringer.

Martin Lind
S022336

[1] Elektronische Leitz Ordner

Indholdsfortegnelse

Indledning

Hvor der er en vilje er der en vej.

Det er med dette gamle ordsprog for øje, at jeg vil analysere sikkerheden i ELO Professional 5, som er et dokument management system. Jeg er af den overbevisning, at hvis en person vil have fat i nogle fortrolige oplysninger, er dette muligt, så længe personens vilje opvejer besværet ved at skaffe oplysningerne.

Jeg mener at IT-sikkerhed, altid maximalt vil være 99.9% sikkert, da man altid, som minimum, vil kunne bryde ind via et brugernavn og kodeord. Det har utallige gange vist sig, at folk vælger kodeord som er nemme at gætte, og skulle det ikke være sådan, kan man bruge brute force[2] til at finde frem til kodeordet. Brute force kan tage lang tid, før den giver resultat, hvis den skal gennemløbe alle muligheder, men med et godt gennemtænkt brute force program og lidt detektiv arbejde, kan man skære den tid det tager at bryde ind i et system drastisk ned.

For at forstå sikkerhed i computerterminologi er det vigtig at forstå dem, som prøver at bryde ind, de såkaldte hackere.

Der findes to slags hackere: whitehats og blackhats. Whitehats kalder man dem, som prøver at bryde ind for at afsløre svagheder i systemer, for derefter at gøre virksomheden/producenten opmærksom på at de har et sikkerhedsbrud. Disse whitehats arbejder ofte i sikkerhedsvirksomheder, og udfører ofte et bestillingsarbejde fra virksomheden/producenten. Men der findes også amatør whitehats, som prøver at hjælpe virksomheder/producenter med at gøre deres systemer mere sikre. Problemet med disse amatør whitehats er, at det kan være svært at skelne mellem, en der vil oplyse dig om et problem med dit system, og en der praler med at han er kommet ind i dit system. Derfor tør amatør whitehats som oftest ikke at kontakte virksomheden/producenten, direkte af frygt for at de skal blive anmeldt for indbrud.

Den anden type hacker er blackhats, disse er modsat whitehats kun ude på at gøre skade eller at fremme deres rygte. De mest almindelige motiver som blackhats har er [1]:

- Notorisk omdømme, anerkendelse og ego
- Finansiel gevinst
- Udfordring

[2] Se afsnittet om brute force for en forklaring på hvad brute force er.

- Aktivisme
- Hævn
- Spionage
- Informationskrigsførelse

Listen er sorteret efter den fare de udgør. En person der hacker som blackhat, og gør det for at få anerkendelse, er derfor mere tilbøjelig til at gøre skade, da dette beviser han har været der. Hvorimod en der spionerer helst ikke vil blive opdaget, og vil oftest lade systemet være som det var, så der ikke er noget der vækker mistanke.

Både whitehats og blackhats kan deles ind i 3 underkategorier: Begynder, mellem og avanceret. Disse tre kategorier repræsenterer hver tre forskellige farer.
Begyndere er nemme at beskytte sig imod, men skulle det ske, at de kommer forbi sikkerhedsforanstaltningerne, er det denne gruppe der oftest forårsager mest skade. Det er ikke altid, fordi de med vilje vil lave skade, men da de ikke helt ved, hvad de laver, kommer de ofte til at forårsage skader på systemet. Begyndere vil for det meste bruge programmer, der udnytter et sikkerhedshul. Programmerne er lavet af personer, der forstår at programmere og har dybere indsigt i IT-sikkerhed aspekter.
Mellemniveaus hackere har forståelse for programmering, og kan iværksætte systematiske angreb. De kan bryde ind i de fleste systemer, hvis de har tid nok. Men forståelsen for sikkerhed i denne gruppe er ikke så stor, så de vil oftest blive opdaget, når de forsøger at bryde ind.
Det avancerede niveau er professionelle hackere. Disse personer vil man oftest finde i sikkerhedsfirmaer eller efterretningstjenester. De vil være interesseret i at arbejde i skyggen, så de ikke bliver opdaget og derfor vil fareniveauet for et angreb fra denne gruppe mod ens data være lavt. Medmindre man skjuler noget, som de så gerne vil have fat i at de laver et angreb, som kompromitterer sikkerheden og muligvis ødelægger data.

Det er vigtig at huske, at whitehats og blackhats findes overalt, også internt i virksomheden. Mange IT-administratorer glemmer oftest, at et angreb kan komme fra en person, der er ansat i virksomheden, hvorfor det også er vigtigt at beskytte data mod ansatte i virksomheden.

Problemformulering

I min praktikperiode er jeg blevet bekendt med et dokument management system kaldet ELO. ELO er udviklet i tre niveauer, som hver er produceret til at håndtere data efter virksomhedens størrelse (stor virksomhed – stor datamængde; lille virksomhed – lille datamængde). Virksomheder har som oftest et større eller mindre krav til sikkerheden når de vælger at håndtere deres data digitalt.
Således er der i ELO´s mindste produkt til ikke lagt stor vægt på sikkerheden. Til en undersøgelse af sikkerhedsniveauet i ELO´s nyeste produkt, ELO-Enterprise, har det været umuligt at få materiale, da dette netop lige er færdigudviklet her i marts 2007. Derfor er valget faldet på produktet "ELO Professional 5", hvis sikkerhedsopbygning vil blive vurderet i forhold til de standarder der er anerkendt indenfor IT-sikkerhed i dag.

Derudover vil programmets sikkerhedsopsætning blive gennemgået, som den fremstår på nuværende tidspunkt, med henblik på at sikre data i arkiverne på forskellige sikkerhedsniveauer i forhold til brugerne af systemet eksempelvis, hvordan de holdes adskilt fra data som ikke har relevans for dem. Herunder vil programmets sikkerhedsfunktioner blive vurderet i forhold til de standarder der i dag gælder indenfor IT-sikkerhed.

For at sikre om opsætningen af ELO Professional 5 til enhver tid i en virksomhed er fejlfri vil det blive forsøgt at udviklet og implementeret et testprogram, Elektronische Leitz Ordner Security (ELOS). Programmet skal give mulighed for at rette på opsætningen, hvis der findes fejl i denne.

Projektet har således tre formål: 1) At klarlægge hvilke sikkerhedsniveauer der er udnyttet i ELO Professional 5, og 2) om programmet kan opbygges med flere forskellige sikkerhedsniveauer og endelig 3) at forsøge at udvikle og implementere et program der kan anvendes med ELO Professional 5 for at sikre en korrekt opsætning.

Sikkerhed

I dette afsnit vil jeg gennemgå nogle af de begreber, som bliver brugt i forbindelse med IT-sikkerhed. Først gennemgås hvad kryptering er og hvordan vi er endt ved de krypteringsalgoritmer, som benyttes i dag. Derefter kort gennemgang af begrebet brute force, og til sidst gives et overblik over, hvad den menneskelige faktor betyder i forhold til IT-sikkerhed.

Begrebet sikkerhed inden for IT

Enhver virksomhed har selvfølgelig en mængde forskellige krav til sikkerhed, og måden, hvorpå disse krav skal implementeres, vil også variere fra virksomhed til virksomhed. Der vil kunne laves en rapport til hver virksomhed med en analyse af deres sikkerhed og mulige forbedringer. Det vil derfor ikke være muligt at gennemgå alle sikkerhedsspørgsmål i denne rapport, hvorfor jeg har valgt kun at berøre dem, som er relevante for ELO.
I 2000 udgav Scott Culp ti love for brugere og ti love for administratorerer omkring sikkerhed. Disse 20 love er udarbejdet i et forsøg på at hjælpe med at forstå problemerne indenfor sikkerhed.
De 10 love for brugerer [1 s10-11]:

1. If a bad guy can persuade you to run his program on your computer, it's not your computer anymore.
2. If a bad guy can alter the operating system on your computer, it's not your computer anymore.
3. If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.
4. If you allow a bad guy to upload programs to your Web site, it's not your Web site anymore.
5. Weak passwords trump strong security.
6. A machine is only as secure as the administrator is trustworthy
7. Encrypted data is only as secure as the decryption key.
8. An out-of-date virus scanner is only marginally better than no virus scanner at all.
9. Absolute anonymity isn't practical, in real life or on the Web.
10. Technology is not a panacea.

De 10 love for administratorer [1 s12-13]:

1. Nobody believes anything bad can happen to them, until it does.
2. Security only works if the secure way also happens to be the easy way.
3. If you don't keep up with security fixes, your network won't be yours for long.
4. It doesn't do much good to install fixes on a computer that was never secure to begin with.
5. Eternal vigilance is the price of security.
6. There really I someone out there trying to guess your password.
7. The most secure network is a well-administered one.
8. The difficulty of defending a network is directly proportional to its complexity.
9. Security isn't about risk avoidance; it's about risk management.
10. Technology is not panacea.

Disse love belyser de konkrete problemer, som ofte opstår, fordi IT-medarbejdere tager visse ting for givet, og ikke er sat ordentlig ind i, hvordan man sikrer et system mod angreb. Lovene til brugerne viser tydeligt, at man skal understrege overfor brugerne, at de kun skal bruge programmer som er godkendt af IT-afdelingen, og at de skal være påpasselige med at låse deres computer, når de forlader den, også selvom det bare er for at hente kaffe. Brugerne skal også instrueres i at vælge sikre kodeord.
Men vil disse ting for at øge sikkerheden være mulige i det virkelige liv. Kan IT-afdelingen automatisere noget af dette, eller er det en risiko, enhver IT-afdeling er nødt til at leve med? En IT-afdeling har mulighed for at lukke ned for brugernes rettigheder, så de ikke har mulighed for at installere et hvilket som helst program. Dette er en god løsning, hvis følgende er opfyldt: En vis mængde af små programmer såsom MSN Messenger[3], Skype osv. skal være tilgængelige i den godkendte programpakke fra IT-afdelingen. Hvis de ikke er det, vil brugere overtale administrator til at installere små programmer eller selv finde programmer, som kan lægges på maskinen uden om diverse installationsbegrænsninger, og derved er der lige pludselig ikke styr på, hvilke programmer der er installeret, og hvilken indflydelse disse måtte have på andre programmer. Det virker måske som en underlig ting at sørge for, men man skal ikke undervurdere menneskets behov for at være socialt. Jeg har ved selvsyn set en virksomhed, som har en meget stram politik omkring installation af programmer. De havde en

[3] MicroSoft Network Messenger

smukt styret programpakke med en masse programmer, og styr på hvilke brugere der havde adgang til hvilke programmer. Men når man var ude hos brugerne, kunne man gang på gang se, at de havde overtalt personer fra IT-afdelingen til at få installeret et lille program. Enkelte havde endda evner nok til at slippe uden om installationsproblemet ved bare at installere programmet på en åben maskine og derefter flytte filerne over på en anden maskine og så køre programmet på den maskine. Jeg må ikke fortælle virksomhedens navn på grund af tavshedspligt, men jeg kan sige, at vi snakker om en større virksomhed med ca. 1000 ansatte og en milliard omsætning. Dette viser, at det ikke bare er et problem, som mindre virksomheder har, men at der i den grad er et problem hos større virksomheder.
Problemet med at hindre personer fra at få ubegrænset fysisk adgang til en maskine er noget sværere at håndtere. Hvis man skal bruge en automatisk pauseskærm med kodeord, skal man tage stilling til, hvor længe der skal gå, før den skal aktiveres, for er tiden sat for lavt, vil den blive aktiveret for tit og irritere brugeren, og hvis den er sat for højt, kan hackeren nå at komme hen til maskinen før pauseskærmen aktiveres. En anden mulighed er at bede brugerne om at sætte kodeord på hver gang de forlader maskinen. Men så opstår problemet med brugeren som bare lige skal hente kaffe eller bare lige skal hente noget, osv. En tredje mulighed er at sætte adgangskort til maskinerne. Dette giver dog hurtigt samme problem som før, da det er for besværligt og brugerne vil lade kortet ligge på bordet eller sidde i maskinen, selv om de går. Altså kort sagt er det besværligt, og brugerne vil undgå så tit, de har mulighed for det. Jeg mener, at den bedste metode her er den første med pauseskærmen kombineret med en god kontrol af sine ansatte. Dette burde minimere risikoen, og som lov nr. ni for administratorerne siger, er det ikke muligt at undgå risici, man kan kun prøve at begrænse risiciene.
I problemet med at kodeord er for lette at gætte, er der muligheder for at komme uden om dette. Man kan blandt andet oprette en regel i ens domæne politikker på ens Domain-controller, om at der skal være visse krav opfyldt, for at kodeordet kan accepteres. Man kan desuden efteruddanne en medarbejder i at teste, om kodeord er sikre nok. Så kan personen prøve at bryde ind i systemet et par gange om året. Dette sætter dog krav til medarbejderens loyalitet, idet denne får kompetencer, som kan misbruges. En uddybning af dette emne gennemgås i afsnit: Den menneskelige faktor.

Sikkert i dag! Sikkert i morgen?

”Sikkert i dag! Sikkert i morgen?” er nok noget alle sikkerhedseksperter tænker over hele tiden. Vil det vi bruger i dag også være sikkert i fremtiden og hvis ikke, hvor lang tid vil det så være sikkert at bruge. Det er et meget svært spørgsmål at svare på, og ofte findes der ikke noget klart svar på det. Der bliver hele tiden udviklet nye teknologier, og nye algoritmer bliver implementeret, og disse kan være med til at komme med nye sikkerhedsmetoder eller destabilisere gamle sikkerhedsmetoder. En måde at nærme sig et svar på dette spørgsmål er ved at gennemgå det vi ved i forvejen og tage ved lære af historien.

Kryptering

En måde at beskytte sine data på er at kryptere dem. Kryptering beskytter data ved at oversætte ens klartekst (plaintext) til ciphertekst (ciphertext) ved hjælp af en krypteringsalgoritme. Den eneste måde at få klarteksten tilbage er så at køre en dekrypteringsalgoritme med den rigtige nøgle. Hvis der bruges et forkert kodeord skal dekrypteringsalgoritmen generere volapyk.
For at forstå kryptering er det vigtigt at starte fra starten af. De første spor vi har af kryptering stammer fra antikken. En populær form for kryptering i Romerriget var at erstatte bogstaverne i ens klartekst med bogstaver et præcist antal længere henne i alfabetet. Antallet af pladser som bogstaverne forskydes kaldes nøglen. Hvis man har en nøgle på 5 vil ens ciphertekst-alfabet komme til at se sådan ud:

Klartekst alfabet	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Æ Ø Å
Cipher alfabet	F G H I J K L M N O P Q R S T U V W X Y Z Æ Ø Å A B C D E

Det betyder at en besked som hed: ”Vi angriber ved daggry”, efter en kryptering med ovenstående algoritme vil se sådan ud: Æn fslwngjw æji ifllwa. Ved første øjekast ser dette ud som volapyk, men algoritmen er ikke så svær at knække. Ved brug af det danske alfabet er der 28 mulige nøgler, den 29. nøgle kan ikke bruges da cipher alfabetet, er det samme som klartekst alfabetet. I antikken har denne form for kryptering været tilstrækkelig, da de fleste af Romerrigets fjender ikke var på samme teknologiske niveau som romerne selv.

Forskellige afarter af denne algoritme blev brugt frem til mellemkrigstiden mellem de to verdenskrige. Her blev det klart, at man blev nødt til at udvikle nye algoritmer til at beskytte statshemmeligheder og militære kommandoer, da disse blev sendt med den tids nye teknologier, telefonen og radiobølger. De nye teknologier gjorde det muligt hurtigt at give kommandoer over lange afstande, men alle med en antenne kunne lytte med. For at udnytte den nye teknologi var det nødvendigt at opfinde en kryptering-algoritme, som man ikke lige kunne gætte. Dette resulterede i maskiner som Enigma. Enigma-maskinen virker ved, at man trykker på det bogstav, som man vil have krypteret, dette resulterer i, at en elektrisk impuls bliver sendt igennem tre rotorer. Hver rotor krypterer bogstavet ved, alt efter hvordan rotoren er bygget op, at sende impulsen ud et andet sted på den næste rotor. For enden af de tre rotorer sidder en reflektor, som sender impulsen tilbage gennem de tre rotorer og ud på Enigma's display. Rotorerne og reflektoren skal være opbygget på sådan en måde, at et bogstav aldrig kan krypteres til sig selv, forstået på den måde at A aldrig må krypteres til A. Efter en elektrisk impuls har været igennem systemet, rykker den første rotor en plads fremad. Når den første rotor er nået en omgang, rykker den anden rotor en plads fremad. Sådan forsætter det indtil beskeden er færdig [2].

I 1948 sker der et kæmpe gennembrud for kryptering, da Claude E. Shannon publicerede sin artikel "A Mathematical Theory of Communication". Dette er første gang, det bliver foreslået, at man kan beskrive billeder, lyd og bogstaver i form af bits. Dette giver helt nye muligheder for at lave krypteringsalgoritmer.

Den amerikanske regering blev i starten af 70'erne opmærksom på at der var behov for at udvikle en standardalgoritme, som alle kunne bruge. Det var nødvendigt at udvikle en algoritme, som kunne være offentlig kendt, uden at det kompromitterede sikkerheden. Den eneste mulighed for at dekrypterer skulle være at bruge den rigtige nøgle, så det eneste mulighed for at angribe krypteret data er med brute force, og det skulle tage lang tid, før en computer fandt den rigtige nøgle. Det var nødvendigt at udvikle en ny algoritme, da der på det tidspunkt var en masse algoritmer på markedet, men de arbejde ikke sammen og nogen af dem var slet ikke sikre og kunne nemt brydes. Den første officielle krypteringsalgoritme var DES[4], som blev gjort offentlig tilgængelig i 1975. DES bruger en 56 bits nøgle, hvilket betyder at der er 2^{56} mulige nøgler, eller skrevet fuldt ud: 72.057.594.037.927.936.

[4] Data Encryption Standard

DES virker ved, at man deler sine data op i 64 bits blokke. Hver af disse 64 bits blokke bliver så krypteret hver for sig. I selve krypteringen bliver en 64 bits blok delt op i to 32 bits blokke. De to blokke bliver først permuteret (IP i fig. 1) og derefter sendt igennem 16 runder. Efter de 16 runder bliver de to blokke igen permuteret (FP i fig. 1), disse to permutationer ophæver hinanden, og var oprindelig kun med, for at algoritmen kunne kører flydende på hardware fra denne tid. I hver runde bliver den ene af de to blokke sendt uændret igennem og den anden krypteret med nøglen. Krypteringen forgår i en Feistel funktion. Blokken med de 32 bits bliver først ekspanderet til 48 bits ved hjælp af en permutation (E i fig. 1). Når dette er gjort, bliver blokken krypteret ved at bruge en XOR-funktion, med en nøgle på 48 bits, som er udledt af den oprindelige 56 bits nøgle. Til hver af de 16 runder er der forskellige 48 bits nøgler, men de er alle udledt af den oprindelige 56 bits nøgle. XOR er en ”eksklusiv eller”-funktion. Dette betyder at de to blokke bliver sammenlignet, og hvis de begge på samme bit-plads har samme værdi bliver værdien 1, og hvis det er forskellige værdier vil værdien blive 0.

Eksempel: To 16 bits blokke som bliver kørt igennem en XOR.

1010011111000001

100101010100110

110011010011000

Resultatet af XOR-funktionen bliver delt op i otte 6 bits dele, som hver bliver sendt igennem en S-boks (S(1-8) i fig. 1). S-boksene laver de 6 bits om til 4 bits ved at bruge en ikke lineær transformation, derfor er S-boksene meget vigtige for DES-algoritmen, for uden dem ville algoritmen være lineær og dermed triviel at bryde. Til sidst bliver den krypterede blok kørt igennem en permutation, for derefter at blive samlet med den anden 32 bits blok med en XOR-funktion.

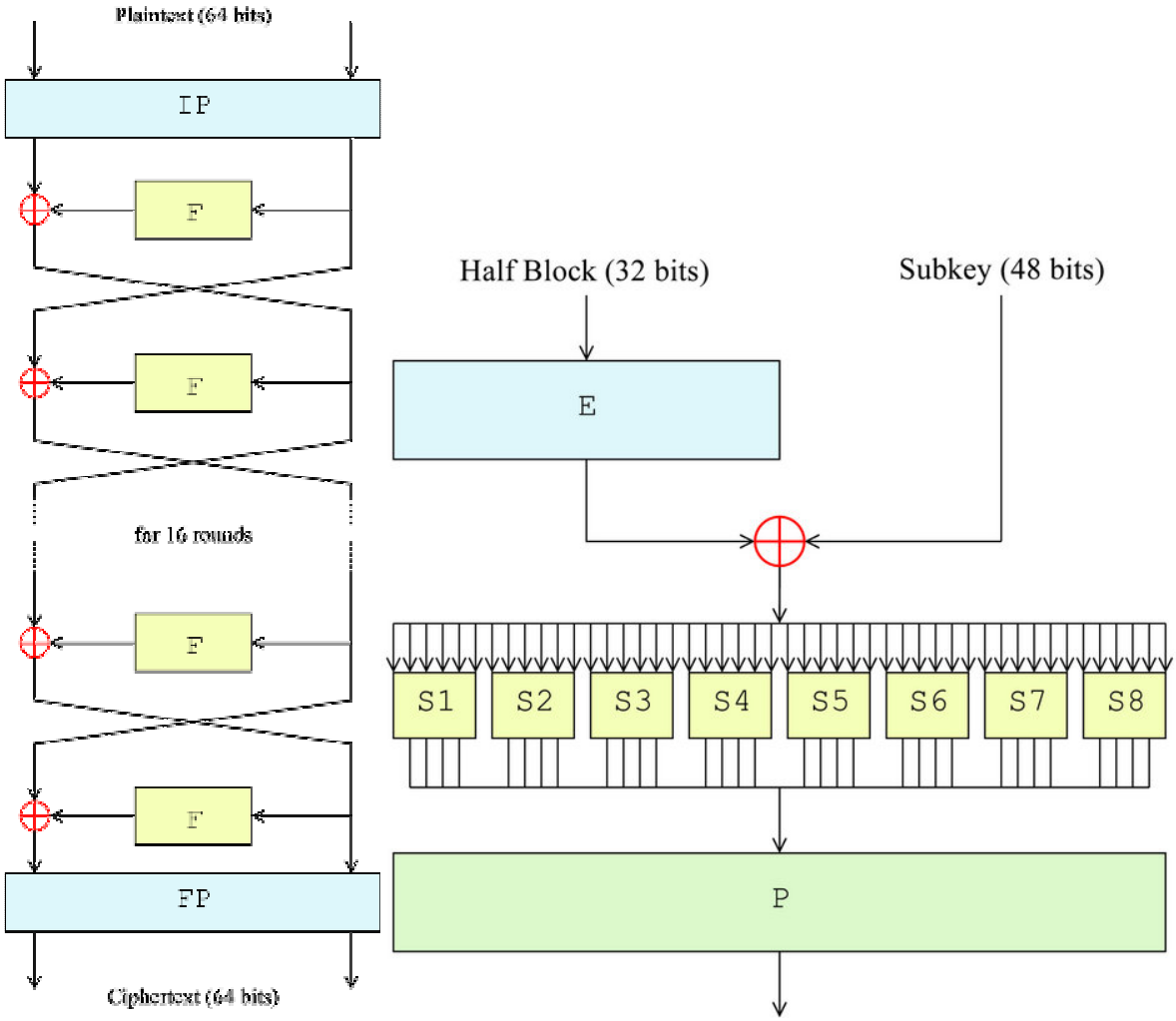

Fig. 1 Den venstre del af billedet viser det overordnet gennemløb i DES-algoritmen. Den højre del viser Feistel funktionen som er hjertet i DES-algoritmen. Denne funktion er markeret med et F i venstre del af billedet. [3]

DES standarden var sikker i mange år, men til sidst indhentede teknologien den. 22 år efter at den var udgivet lykkes det ”DESCHALL Project[5]” for første gang at bryde DES-krypteringen i et officielt forsøg. I 1998 forsøgte ”Deep Crack[6]” at bryde en DES-kryptering. Det tog dem 56 timer at bryde den. Året efter forsøgte ”Deep Crack” i samarbejde med ”distributed.net” at bryde en DES-kryptering igen, og på blot 22 timer og 15 minutter brød de krypteringen. Dette betød, at der var behov for at udvikle en ny algoritme, som var mere sikker. For at gøre DES sikker igen mens en ny algoritme blev udviklet, begyndte man at bruge 3DES[7]. 3DES er bare DES kørt tre gange med forskellige nøgler i hver af de tre DES [3]. Men efterfølgeren til DES

[5] Det samlede navn for alle de frivillige der var med til at prøve at bryde DES-krypteringen.
[6] En maskine bygget af Electronic Frontier Foundation specielt til at bryde DES-krypteringen.
[7] Tripel Data Encryption Standard

var allerede opfundet i 1998 af to belgiske forskere, Joan Daemen and Vincent Rijmen. Den blev omdøbt fra Rijndael til AES[8], og i 2001 blev den officielt anerkendt som afløseren til DES. Ved den seneste opdatering af statistikker omkring AES i 2006 var der endnu ingen der havde lykkes med at bryde en AES-kryptering. Til AES algoritmen kan man bruge 128, 192 eller 256 bits nøgler. Det giver et maximalt nøgleantal på 2^{256} [4].

Hash-algoritmer

Hvis man vil beskrive en fil med en unik værdi udfra dens data, kan man bruge hash-algoritmer. Princippet bag hash-algoritmer er at enhver fil vil få et unikt id. Dette bruges f.eks. til at se om der er dubletter i ens arkivsystem. Det har dog endnu ikke været muligt at designe en hash-algoritme der kan lave 100% unikke hash-værdier. Dette er ikke muligt, fordi der med alle kendte hash-algoritmer er den teoretiske mulighed for, at to forskellige filer har den samme hash-værdi. I de hash-algoritmer der anvendes i dag, er denne mulighed så lille, at den i praksis aldrig vil forekomme.

Brute Force

Brute force blev brugt om det arbejde kryptograferne under anden verdenskrig udførte. De var nødt til at prøve alle de mulige nøgler for at dekryptere tyskernes koder. Derfor sagde man, de brugte brute force. Dette udtryk er siden hen blevet en måde at fortælle, hvor sikker en algoritme er. Mange af de hackerprogrammer, der findes, bygger på brute force metoder. Disse programmer virker ved, at de prøver alle de kodeordskombinationer, som findes indenfor det interval, man vælger der skal prøves. En anden brute force metode er at prøve alle mulige nøgler. Forskellen på kodeord og nøgler, er at kodeord er en måde at vise nøgler, så vi forstår dem.
Brute force, er specielt indenfor de senere år, blevet en meget større trussel mod IT-sikkerheden, fordi det er blevet billigt og nemt at bygge store supercomputere. Disse supercomputere har så stor kapacitet, at de nemt kan knække kodeord, der er for svage, blot ved at prøve alle muligheder.

[8] Advanced Encryption Standard

Den menneskelige faktor

Nu har jeg gennemgået en del om sikkerhedsbegreber og principper. Men det er vigtigt at huske at ligegyldig hvor mange penge eller hvor megen tid man lægger i beskyttelsen af sit netværk er det mennesker, der skal administrere det. Den menneskelige natur indeholder mere eller mindre svagheder, som kan lede til, at et systems sikkerhed kan blive kompromitteret.

- Dovenskab – dette kan medføre, at netværket ikke bliver opdateret, når der er tilgængelige opdateringer, eller kodeord er svage og lette at gætte.
- Hævn – dette kan medføre, at personen ødelægger visse dele af netværket eller lader huller i netværket være åbne.
- Griskhed – dette kan medføre, at personen er mere tilbøjelig til at modtage penge for at lade huller i netværket stå åbne.
- Forelskelse – dette kan medføre, at personen kan lade sig overtale til at lade huller i netværket stå åben.
- Social anerkendelse – dette kan medføre, at personen kommer til at udlevere oplysninger om netværket, som en hacker kan udnytte.

Ovenstående kan til tider lyde, som var det taget ud af en film, men det forekommer i den virkelige verden. Nogen af disse historier vil man næppe høre om, fordi personerne synes de er for pinlige, eller fordi de aldrig bliver opdaget.

For at illustrere at disse kan forekomme, vil jeg henvise til en undersøgelse, der blev fortaget i andet halvår af 2006 i England. En journalist stillede sig op på gaden, og spurgte folk, der gik forbi om deres kodeord, så han kunne lave en statistik over hvilke ord, der blev mest brugt. Et andet eksempel på dette er da radioavisen på P3 d. 11/4 2007, bragte en reportage, om at danskerne bruger svage kodeord, og reporteren spurgte personer på gaden om deres kodeord, hvorefter personerne fortalte deres kodeord. Dette virker uskyldigt nok, men det overraskende var, at folk rent faktisk fortalte den engelske journalist og den danske reporter, hvad deres kodeord var. Journalisten fik sin statistik og reporteren sin historie, men de overså det egentlige problem, ved det de havde gjort. Dette i sig selv virker ikke så farligt, men så tænk over dette scenario:

Man fremskaffer nogle brugernavne ved at kikke på mailadresser for nogle ansatte i det firma man vil angribe. Brugernavne kan man nemt få fat i, idet de fleste firmaer anvender brugernavnet før @ i mailadressen. Når dette er gjort, stiller man sig udenfor virksomheden eller et sted, hvor man ved, at en større del af virksomheden ofte kommer, og laver den

samme undersøgelse som journalisten. Nu har man en række brugernavne og kodeord, og så er det eneste, der mangler at finde et brugernavn og kodeord der hører sammen, så har man adgang til virksomheden. Denne fremgangsmetode vil nok kun have en ringe chance for at lykkes, men hackere har mange andre mere sofistikerede metoder, som meget nemt giver resultater.
En af de egenskaber mennesket har, har jeg undladt at sætte på listen, da jeg synes, den skiller sig lidt ud. Egenskaben er nysgerrighed. Grunden til at jeg ikke har sat den på listen, er at i alle tilfældene på listen, er personen helt klar over, at han gør noget forkert. Men med nysgerrighed er der stor chance for, at personen kommer til at ødelægge noget, uden at vedkommende er sig det bevist. Dette aspekt må ikke glemmes, når man fastlægger sikkerhedspolitikken for virksomheden, da det kan medføre katastrofale fejl i systemet. Det er derfor vigtigt, at man som administrator låser sit netværk ned, så hver bruger kun har præcis adgang til netop det, han skal bruge og ikke mere.

ELO Digital Office

ELO Digital Office udsprang fra Leitz[9] i 1996, da man indså at der var et marked for at lave en digital udgave af ringbindet. ELO Digital Office producerer tre produkter:

Office

Office er deres mindste produkt, med maximalt fire arkiver med 200.000 filer i hvert arkiv. I denne udgave er der ikke lagt særlig meget vægt på sikkerheden. Den eneste sikkerhed der er i dette produkt, er Windows's styring af mappeadgang til de forskellige brugere når man kører over netværk og ELO programmets interne styring af brugerne [5].

Professional

Professional er det produkt, jeg har valgt at fokusere på. Der er her lagt vægt på sikkerheden, da det er lavet til større firmaer, som ofte stiller store krav til sikkerheden. I denne udgave kan man have 20 arkiver med op til 4,2 mia filer per arkiv. I denne versionen findes der også et workflow modul og mulighed for at sætte flere moduler til, så man kan integrerer flere programmer [5].

[9] Opfandt ringbindet i 1871.

Enterprise

Enterprise er deres nyeste produkt. Modsat de to andre produkter sætter dette produkt ikke krav til hvilket styresystem, der bliver brugt, da man har programmeret det i Java, men ellers ligner det på mange punkter Professional udgaven. Det eneste den kræver, er at Apache Tomcat er installeret. Denne udgave kan i princippet have uendelig mange arkiver med 4,2 mia. filer per arkiv. Denne udgave har også en helt speciel opbygning når det gælder sikkerhed. Grunden til at jeg ikke har valgt at skrive om dette produkt, er at det først blev præsenteret for offentligeheden til Cebit-messen i Tyskland i marts 2007. Jeg har derfor ikke haft mulighed for at skaffe materiale om programmet, og jeg har heller ikke haft mulighed for at sidde og arbejde med programmet. Derfor har jeg valgt at koncentrere mig om professional udgaven [5].

ELO-sikkerhed

ELO har valgt at benytte Windows sikkerhedsprincipper, når det drejer sig om at beskytte filerne fra angreb udenom ELO. Disse vil jeg beskrive i afsnittet ”Microsoft Network Technology-sikkerhed”. I dette afsnit gennemgås de principper, ELO bruger i programmet til at adskille brugere fra de filer de ikke må se og hackere fra at bryde ind.
ELO Professional består af to programmer, et server program og et klient program. Tanken er så, at serverprogrammet har fuld adgang til arkiv-strukturen og hele databasen. Klient programmerne kan så bede om adgang til forskellige dele af arkivet og alt efter rettighederne i ELO, kan brugeren så få adgang eller blive nægtet adgang. Dette begrænser så muligheden for angreb til det brugernavn og kodeord som serverprogrammet benytter. Derfor anbefaler ELO, at det kun er personen der installerer ELO, samt enkelte fra IT-afdelingen, der kender disse to ting. Efter installation af ELO skriver man brugernavn og kodeord ned på et stykke papir, og anbringer det i et pengeskab, så oplysningerne kan genfindes, hvis der skulle ske noget, som kræver at brugernavn og kodeord skal anvendes.

Brugere

Brugere af ELO Professional 5 kan få tildelt rettigheder til systemet direkte eller via brugergrupper. Man vil gerne videreføre principperne bag tildeling af rettigheder fra Windows system, og derfor anbefaler ELO Digital Office, at man ikke tildeler rettighederne direkte til brugeren, men at brugeren får de rettigheder, der skal anvendes, igennem de

brugergruppen, som brugeren er medlem af. Både brugere og brugergrupper har, som en grundsten, en unik identifikator så de aldrig kan forveksles med andre brugere eller brugergrupper af systemet.

Nøgler

Til at adskille brugere fra filer eller dele af arkivet som de ikke har adgang til, benytter ELO såkaldte nøgler. Det er muligt at knytte mange forskellige nøgler til hver fil, med forskellige rettigheder. De fire rettigheder man kan tildele med nøgler er: læse, skrive, slette og kørsel og har brugeren bare én af disse rettigheder, kan man se filerne, ellers er filerne skjult for brugeren.

Kryptering

ELO Proffesional 5 anvender twofish til at kryptere med. Denne krypteringsalgoritme var blandt de fem finalister til at blive valgt til AES, men som nævnt var det Rijndael algoritmen der blev valgt. Twofish anvender 128, 192 eller 256 bits nøgler til at kryptere med, og er opbygget med en Feistel struktur, ligesom DES er. Twofish bliver anset som en sikker krypteringsalgoritme, idet denne algoritme var højt placeret i konkurrencen til AES, da der var høje krav til algoritmen for at komme i betragtning. Shiho Moriai og Yiqun Lisa Yin har dog publiceret en artikel i 2000, der hævder at krypteringen teoretisk kan brydes, og at det vil kræve ca. 2^{51} specielt udvalgte klartekster, for at få de data der er nødvendig for at bryde krypteringen. Shiho Moriai og Yiqun Lisa Yin er kommet frem til dette, ved at anvende matematiske regneregler, og har ikke forsøgt at bryde krypteringen i praksis. Der er ingen, der officielt har forsøgt at bryde towfish i praksis, eller påstår at det har lykkes for dem at bryde twofish [6].

Arkiver i ELO

Et arkiv i ELO består af to ting, en mappe på en harddisk til fysisk at placere filerne der bliver gemt i ELO og en database, som indeholder oplysninger og rettigheder omkring hver fil. Helt præcist bliver hver fil pakket ind i en maske. Disse masker kan man selv designe i ELO, så de har mulighed for at indeholde netop de metadata, man mener, er nødvendige til den type fil. En maske har dog felter som er obligatoriske. Den skal have et felt, hvor dens navn i ELO kan indtastes, et felt med den dato hvor filen er oprettet og et felt med den dato hvor filen er lagt ind i ELO. Disse masker bruges når man skal søge efter en fil, da det er hurtigere at søge

igennem den metadata der er i maskerne end at starte en fuldtekst søgning, hver gang man skal finde en fil. ELO Professional har dog mulighed for at fortage en fuldtekst søgning hvis det skulle være nødvendigt.
I ELO bruges MD5[10] til at lave de hash-værdier, der bruges, når ELO skal se om den fil, man prøver at lægge ind i ELO, eksisterer i arkivet i forvejen. MD5 har ligesom de andre hash-algoritmer den svaghed, at der teoretisk kan forekomme ens hash-værdier. For at imødekomme dette problem har ELO valgt at begrænse pladsen i hvert arkiv. Dette vil igen gøre den teoretiske mulighed for forskellige filer med ens hash-værdier endnu mindre [7].
Når man tilføjer en fil i ELO, bliver der først lavet en hash-kode af filen, for at se om filen allerede findes i arkivet. Hvis dette er tilfældet, vil man blive spurgt, om man vil lave en reference til den fil, som er i arkivet, eller om man vil indføre den nye fil i arkivet.
Ligegyldigt om man vælger at oprette en reference eller en ny fil, eller hvis filen ikke er i arkivet, vil man blive bedt om at vælge en maske herefter. I masken kan der være felter, som skal udfyldes når filen lægges ind i ELO. Når alle felter er udfyldt, vil filen blive overført til det fysiske arkiv.
Når det drejer sig om at slette en fil i ELO, er der indlagt ekstra sikkerhed. Ønsker man at slette en fil i ELO, bliver den i første omgang ikke fysisk slettet, men der bliver derimod sat en variabel i databasen ved filens indtastning, om at den ikke skal vises i ELO. For fysisk at slette filer fra ELO, skal man være administrator. Hvis man er dette, kan man aktivere en funktion i ELO, som gør at man kan se de filer, som er blevet slettet af bruger og derpå vælge, om de skal slettes fysisk fra harddisken.

Microsoft Network Technology-sikkerhed

Dette afsnit omhandler Microsoft NT[11]-sikkerhed omkring brugere, brugergrupper og fil/mappeadgang. Det er dette område som ELO udnytter til at beskytte sine arkiver mod indtrængning udenom ELO. Dette gør denne del af Windows systemet til en væsentlig del af sikkerheden i ELO og bør derfor gennemgås for at se hvilken sikkerhed det tilbyder.
Derfor vil der blive gennemgået, hvordan brugere og brugergrupper har deres egen unikke identifikationsmetode, så der ikke opstår tvivl i systemet om hvilken bruger eller

[10] Message-Digest algorithm version 5
[11] Network Teknologi

brugergruppe, man har med at gøre. Teorien bag at samle bruger i brugergruppe vil blive gennemgået, og Windows mulighed for at begrænse adgang til mapper til udvalgte brugere og brugergrupper bliver beskrevet.

SID[12] (Brugere)

Enhver bruger eller brugergruppe i Windows har en SID, som Windows anvender til at skelne de forskellige brugere fra hinanden. En SID er bygget op af 5 dele:

S-<revision>-<identifier authority>-<subauthorities>-<relative identifier>

1 2 3 4 5

Et eksempel på et SID er: S-1-5-21-833815213-1531848612-156796815-1105.[13]

1 2 3 4 5

- Revision
  Dette tal angiver, hvilken version af SID der bliver brugt. Der bliver indtil videre kun brugt 1 i Windows server 2003, Windows 2000 og Windows XP. Men hvis der i fremtiden bliver behov for at udvide eller lave om på SID opbygningen, har Microsoft gjort klar til, at dette nemt kan gøres blot ved at tallet efter S'et ændres til noget andet.
- Identifier authority
  Dette tal bestemmer hvilken autoritet SID'et har. I eksemplet er det 5, og det er Windows NT Authority
- Subauthorities
  Denne række tal er unikke for det domæne, hvori SID optræder. Denne talrække bliver af mange også kaldt "domain identifier"
- Relative identifier
  Det sidste tal i SID'et er den unikke identifikation af brugeren eller brugergruppen. I eksemplet er det 1105.

Det smarte ved at bruge SID er at det bliver meget sværere at udgive sig for at være en anden, end den man er. På grund af den næstsidste del af SID'et skulle det ikke være praktisk muligt, at have to brugere på forskellige netværk der har samme SID.

[12] Security IDentifier
[13] I Windows Security Ressource Kit 2 kan man finde en liste med nogen af de mest kendte SID'er

Brugergrupper

Ligesom en bruger har en brugergruppe en SID, som gør brugergruppen unik overfor sine omgivelser. Brugergrupper bruges til at samle brugere i store grupper, så det er nemmere at dele adgang og rettigheder ud til dem. I stedet for at man skal tildele en masse brugere den samme rettighed en efter en, kan man tilføje alle brugerne i en brugergruppe og så tildele rettigheden til brugergruppen. En udbredt metode for at hindre at brugere skal opnå for mange rettigheder, er at brugerne får tildelt alle sine rettigheder ud fra de brugergrupper, brugeren er med i. ELO bruger to grupper i deres programopsætning, en ELO administratorgruppe og en ELO brugergruppe. Disse bruges til at begrænse adgangen til ELO's mapper og arkiver. ELO har valgt denne metode da den sikrer høj gennemskuelighed, og gør det nemt for IT-afdelingen at fjerne eller tilføje rettigheder, uden at skulle ændre direkte ved brugerens opsætning.

Fil-/Mappeadgang

Et af hovedpunkterne i ELO Professional 5's beskyttelse af data, er windows fil- og mappeadgangskontrol. Til ethvert objekt på en NTFS formateret harddisk er der tilknyttet et sikkerhedsbeskrivelseselement.
Dette element indeholder, foruden en header, en SID til ejeren og en SID til den primære gruppe som ejeren tilhører, samt en Discretionary Access Control List (DACL) og en System Access Control List (SACL).

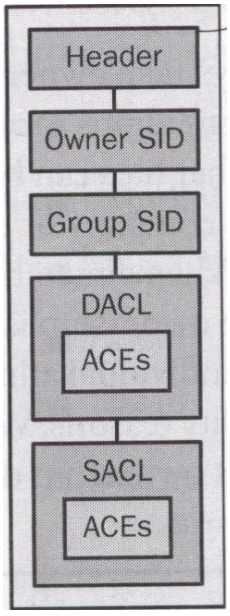

Fig. 2 Billedet viser opbygningen af et sikkerhedsbeskrivelses element. [1 s. 139]

Forskellen på disse to, er at i DACL kan enhver, som har ”Take ownership”, ”Change permission” eller ”Full control” til objektet, ændre på de elementer som er i DACL. Det er i disse to lister adgangskontrollen styres, nærmere betegnet fra Generic deny ACE[14]s og Generic allow ACEs listerne. Hver ACE indeholder en Security IDentifier (SID). Når en bruger forsøger at få adgang til et objekt bliver DACL gennemgået for at se om brugerens SID eller en af dens sikkerhedsgruppers SID passer til en i DACL.
Når windows søger igennem en DACL kikker den efter ACE med denne prioritet:

1. ”Explicit deny”
2. ”Explicit allow”
3. ”Inherited deny”
4. ”Inherited allow”

Hvis der f.eks. findes en ”Explicit deny” på brugeren, vil denne altid være den gældende også selvom der findes en af de andre. Dette betyder at ”Explicit” altid overskriver ”Inherited”. Det er derfor ligegyldigt hvor mange ”Inherited allow”, man har, så længe man bare har en ”Inherited deny” eller ”Explicit deny”. Hvis brugeren ikke har mindst et SID, som passer i DACL vil brugeren automatisk blive afvist.

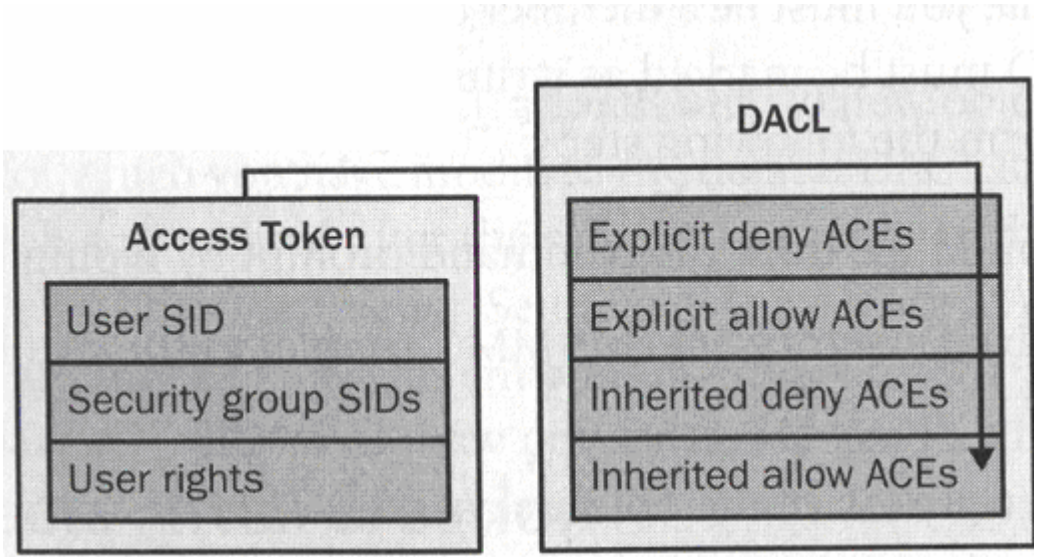

Fig. 3 Billedet viser hvordan der søges om brugeren har adgang. Først søges der efter brugeren SID i DACL listen og derefter efter de grupper som brugeren er medlem af i DACL listen. Til sidst ses der om brugeren har specielle rettigheder som giver adgang [1 s. 95].

[14] Access Control Entry

Både DACL og SACL indeholder foruden ACE'er, en række elementer; en header som indeholder metadata, som tilhører de forskellige ACE'er i DACL, en SID til ejeren og en SID til den primære gruppe som ejeren tilhører.
Princippet bag denne adgangskontrol er meget enkel, men der er dog visse faldgrupper. En af disse, er når der skal kopieres eller flyttes objekter. Når et objekt kopieres, oprettes der et nyt objekt under det nye forældre objekt. Når dette sker, nedarver objektet tilladelser fra det nye forældre objekt, og dette kan jo være anderledes i forhold til det gamle forældre objekt. Alle "Explicit" tilladelser forsvinder, da det er et nyt objekt. Når et objekt flyttes, bliver objektet fysisk, hvor det er, men referencen til objektet bliver ændret. Sikkerhedstilladelserne bliver først ændret, når der bliver ændret i forældre objektet's eller objektet's sikkerhedstilladelser. Når dette sker, vil de nedarvede tilladelser blive opdateret, men alle "Explicit" tilladelser vil stadig være de samme.

Microsoft SQL sikkerhed

ELO Professional 5 bruger en SQL-database til at gemme de oplysninger, som den anvender, som f.eks. masker med tilhørende data fra felterne i masken, nøgler, brugernavne, osv. Men det er ikke alle SQL-servere der bliver anbefalet af ELO, da sikkerhedsprincipperne i SQL-servere kan variere meget. En af de SQL-servere ELO anbefaler er Microsoft SQL 2005 (MS SQL 2005).
MS SQL 2005 bliver anbefalet, fordi Microsoft sætter sikkerhed meget højt, og fordi MS SQL 2005 er integreret i Windows, så man kan udnytte de sikkerhedsprincipper, som er i Windows, blandt andet fil-/mappeadgang, som også er vigtigt for ELO Professional 5.
Der er to måder at komme ind til SQL databasen. Man kan enten bryde ind i selve SQL-severen eller man kan stjæle database-filen og åbne den på en anden SQL-server. Hvis man skal bryde ind i en MS SQL 2005-server kræver det, at man skaffer et brugernavn og kodeord. Det er derfor vigtigt, at man lige efter man har installeret MS SQL 2005-server ændrer kodeordet for den standard oprettede system administrator (sa) konto i MS SQL 2005-serveren. Man skal desuden kun tillade en bruger at ændre i ELO's database og begrænse brugernes adgang og privilegier til et minimum, så skulle en anden bruger blive kompromitteret får dette ikke indflydelse på ELO.

For at forhindre at en bryder ind og stjæler database filen, kan man udnytte Windows fil/mappeadgangskontrol. Når man installerer MS SQL 2005 bliver der automatisk oprettet en sikkerhedsgruppe til alle de brugere, som bliver oprettet i MS SQL 2005. Den standard mappe som bliver oprettet til databasefiler, bliver låst ned så kun administrator og medlemmer af denne sikkerhedsgruppe kan få adgang. Dette sikrer at ikke hvem som helst kan få adgang til databasefilerne. Skulle man ønske at sikre denne mappe endnu mere kan man fjerne administrator gruppen og kun tilføje præcist de administratorer som skal have adgang til denne mappe.

Analyse

Denne analyse del har jeg valgt at opdele i tre afsnit. Det første vil omhandle en fiktiv virksomhed, som efter en række fejl har store huller i sin opsætning af ELO. Fejlene gennemgås i detaljer, samt hvordan de er opstået, og hvilke opgaver der skal udføres for at rette op på dem. Yderligere gennemgås, hvordan man kan komme fejlene i forkøbet. Andet afsnit omhandler, hvor mange led i sikkerhedskæden der kan briste, før end hele ELO opsætningen er kompromitteret. Jeg vil se på, om der er nogle områder, som skal have mere opmærksomhed end andre, da de er vigtige i sikkerhedsøjemed. Det tredje afsnit beskriver den perfekte opsætning af ELO, og dernæst en analyse af om denne opsætning så lever op til de sikkerhedskrav, der normalt bliver stillet af virksomheder i dag.

Det totale nedbrud af sikkerhed (ELO i Jensens virksomhed)

Hr. Jensen ejer en mindre entreprenør-virksomhed. For 5 år siden besluttede Hr. Jensen, at hans virksomhed skulle have mere styr på deres kontrakter, tilbud, arkitekttegninger fakturaer o.lign. Valget faldt på ELO Professional 5, da dette program kunne tilbyde de funktioner og det sikkerhedsniveau, som der blev krævet. Da Hr. Jensen sætter sikkerheden meget højt blev installationen og opsætningen af ELO fortaget af ELO Digital Office selv.
Fem år senere har Hr. Jensen et problem med, at en af hans konkurrenter bliver ved med at komme med tilbud på kontrakter, som er billigere end Hr. Jensens virksomhed tilbyder. Desuden har han lagt mærke til, at der forsvinder data fra ELO-arkivet, og at flere af virksomhedens ELO-workflows har de forkerte personer som modtagere af data. Han

mistænker derfor sikkerheden i ELO for at være brudt. Han hyrer herefter et uafhængigt firma, som har specialiseret sig i sikkerhed, til at gennemgå sikkerheden omkring ELO, og se om det er muligt for udestående at komme ind i ELO-arkiverne.
Firmaet starter med at kikke på den rapport, som ELO Digital Office har lavet i forbindelse med opsætningen af ELO i Hr. Jensens virksomhed for fem år siden. Ud fra denne rapport laver de en rapport over sikkerheden i en optimal ELO opsætning (Se afsnit ”Den perfekte ELO opsætning”). Derefter går de i gang med at undersøge, om opsætningen stadig svarer til den oprindelige opsætning.
Den første fejl i forhold til den oprindelige opsætning de opdager, er opstået i forbindelse med, at Hr. Jensens virksomhed har udskiftet den server, hvorpå ELO arkiverne ligger. Fejlen er opstået, fordi IT-afdelingen ikke var opmærksom på hvilke regler Windows bruger, når man kopierer mapper. Da IT-afdelingen havde sat den nye server op, flyttede de ELO arkiver fra den gamle server til den nye. Når man flytter fra en server til en anden server, svarer det til at kopiere filerne og derefter at slette dem. Det er derfor reglen om nedarving ved kopieringer, der gælder i dette tilfælde. Hvis filerne bare var blevet flyttet internt på harddisken på den gamle server, var det en anden regel som gjaldt. Ved kopiering bliver mappeadgangen nedarvet fra det nye forældre objekt, og alle direkte tildelte mappeadgange bliver slettet. Det nye forældreobjekts opsætningen gav fuld adgang for alle brugere og brugergrupper, hvorved alle ELO arkiver blev frit tilgængelig for alle. Dette betyder at alle der har adgang til virksomhedens netværk, frit vil kunne se alle de filer, som er gemt i ELO og derfor have mulighed for at manipulere med dem. Løsningen på dette problem er meget enkel. Det eneste der skal gøres er at åbne mappeadgangsvinduet og fortælle at den øverste ELO arkivmappe ikke må nedarve fra sit forældre objekt. Derefter sætter man fuld adgang for ELO administrator gruppen, og ingen andre skal have adgang til denne mappe. Det er vigtigt at ingen andre end ELO-administratorgruppen får adgang til ELO arkiverne, idet sikkerheden ellers kompromitteres.

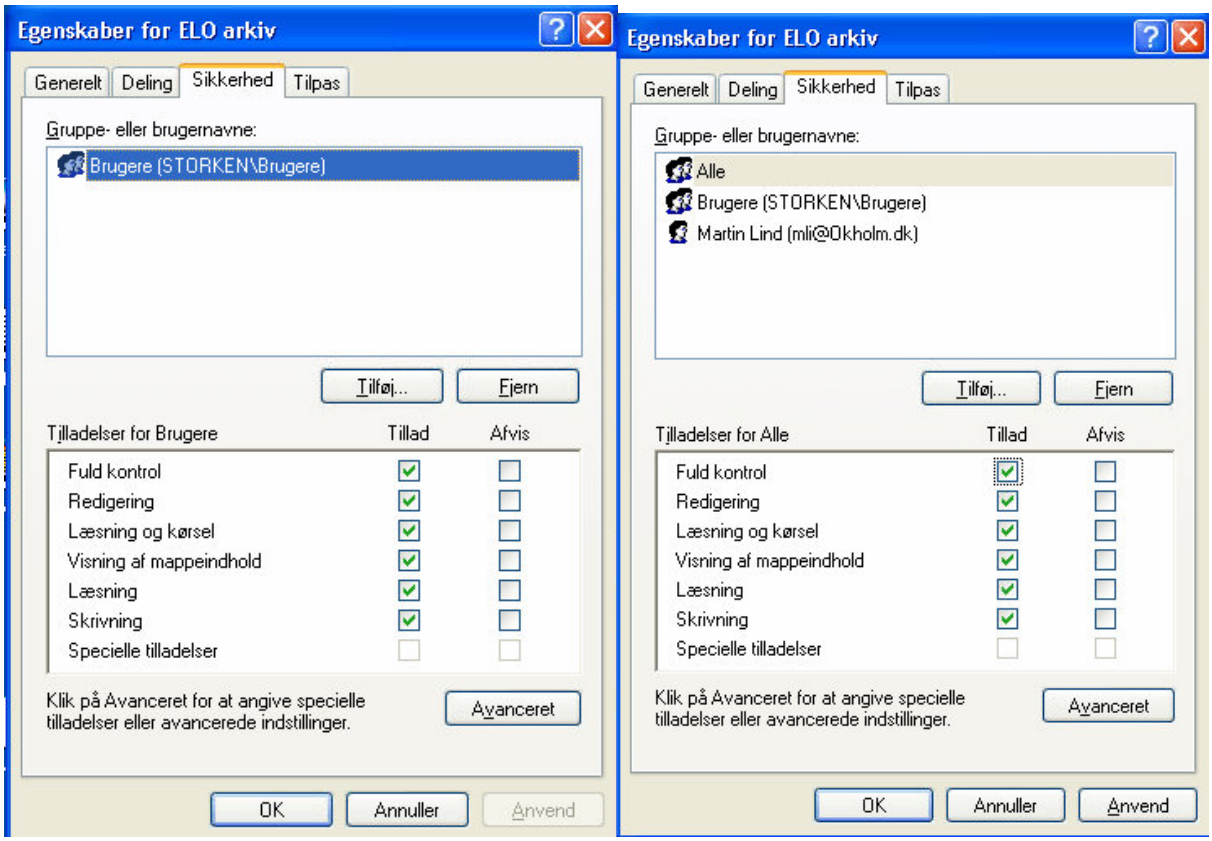

Fig. 4 Den venstre del af billedet viser en korrekt opsætning af en ELO arkiv mappe, hvorimod i den højre del er der alt for mange brugere der har adgang til mappen i om med at gruppen Alle indeholder alle brugere i hele systemet.

I forbindelse med flytningen af arkiverne havde man også flyttet ELO's database fra den gamle server til den nye server. Dette har samme virkning for databasen, som det havde for arkiverne, alle vil få rettigheder til at se og ændre i databasen.

Disse to fejl alene vil gøre at alle med en minimal forståelse for hacking, ville kunne læse og manipulere data udenom ELO programmet. Det kræver dog stadig, at man har adgang til netværket enten internt i virksomheden eller via virksomhedens forbindelse til internettet.

Efter at sikkerhedseksperterne havde undersøgt ELO opsætningen i Windows miljøet, gik sikkerhedsfirmaet i gang med at se på opsætningen inde i ELO. For at undersøge tildelingen af nøgler og brugerrettigheder.

Ved en nærmere undersøgelse viste det sig, at i en af de interne ELO brugergrupper var der krydset af i den rettighed, som giver lov til at ignorere alle andre rettigheder. Dette betød, at alle der var i den brugergruppe kunne gøre lige, hvad der passede dem i ELO. Denne rettighed fandt sikkerhedsfirmaet skødelsesløs, da denne rettighed kan være yderst kompromitterende for sikkerheden i ELO, idet den blot var placeret midt mellem de andre rettigheder uden nogen form for ekstra advarsel. Det kræver ikke mere end en uopmærksom IT-medarbejder,

før end denne rettighed er givet til en bruger, som så kan udnytte den. Hr. Jensens virksomhed havde valgt at begrænse adgang til forskellige mapper i ELO ved, at bruge den nye funktion i ELO Professional 5; nemlig at låse mapper ved hjælp af brugergrupperne i ELO. I versioner før version 5 havde det kun været muligt at låse ved hjælp af ELO nøgler. Disse nøgler blev så tildelt de brugere, der skulle have rettigheder til at se de mapper, der er låst med nøglen. Her fandt sikkerhedsfirmaet ingen problemer, men de fandt ud af, at hvis en bruger havde den før omtalte rettighed, ville den tilsidesætte låsningen af mapper, og brugeren ville have fri mulighed til at se og ændre filer placeret i mapper, som burde være låst for brugeren.

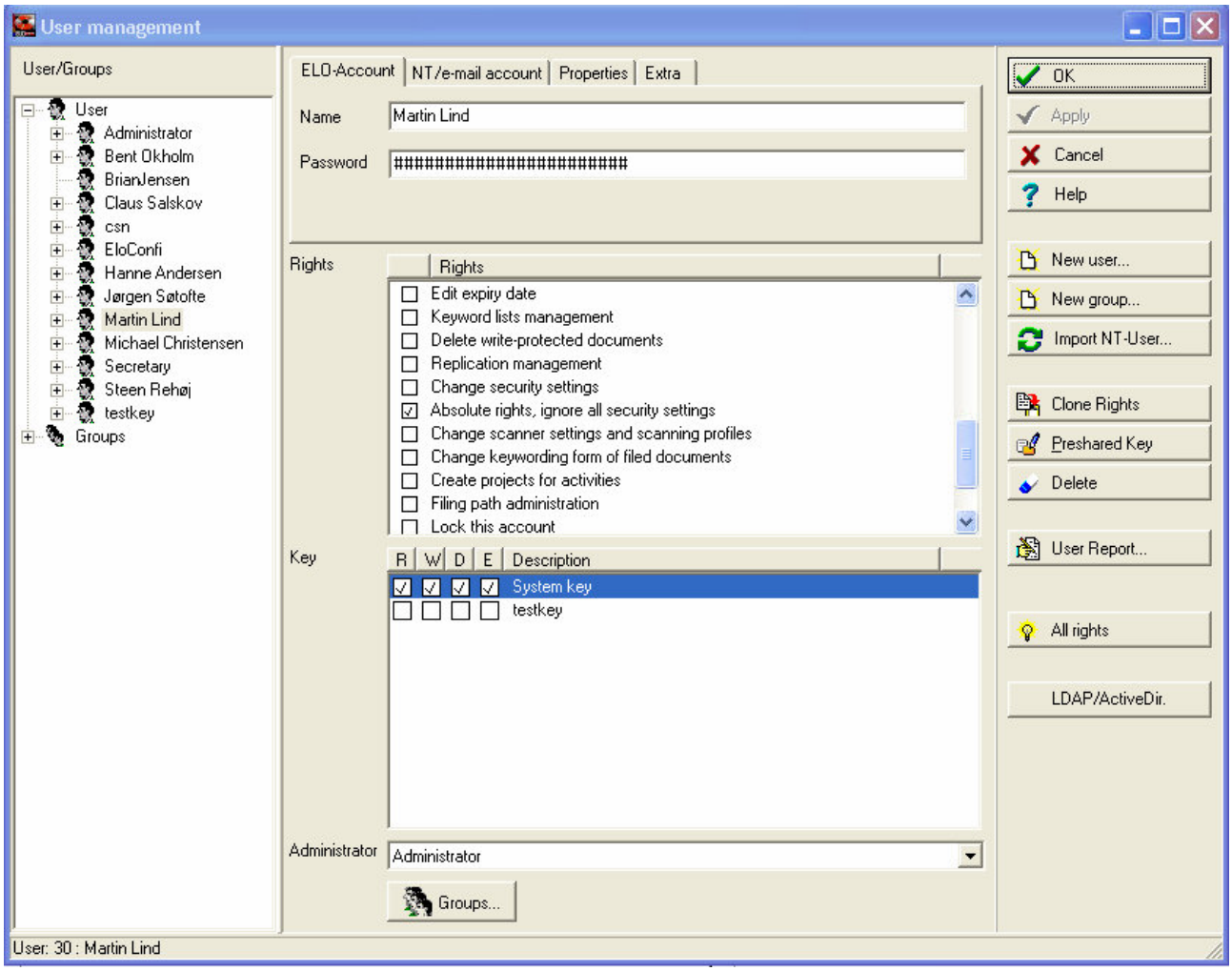

Fig. 5 Billedet viser interfacet fra ELO, hvor man kan styrer brugernes rettigheder og hvilke nøgler der er tildelt til brugeren. At brugeren her har fået den udvidede rettighed som overskriver alle andre rettigheder kan ses ved flue benet udfor rettigheden.

Efter en længere undersøgelse af Hr. Jensens virksomhed og dennes IT-miljø fandt man frem til, at en bruger havde modtaget bestikkelse af det konkurrerende firma, for at videregive oplysninger om tilbud. Denne bruger havde adgang til de tilbud, som lå i ELO, også selv om

der ikke havde været de føromtalte fejl på opsætningen af ELO. Undersøgelsen viste yderligere, at de problemer, der havde været med forsvundne filer, skyldes nysgerrige brugere, der havde været inde i arkivet og prøvet sig frem, uden de havde vidst hvad de havde lavet. Problemet med de forkerte workflows var også fremkaldt af brugere, der havde testet deres kunnen i ELO, og da de havde fået den rettighed som tilsidesatte alle andre, kunne de forårsage mere skade end ellers.
Sikkerhedsfirmaet anbefalede, at man sendte IT-afdelingen på efteruddannelse hos ELO Digital Office, så fejlene ikke ville gentage sig, og at ELO Digital Office gennemgik opsætningen igen, så den levede op til de oprindelige krav, som var opsat ved installationen af ELO. Sikkerhedsfirmaet forslog også, at IT-afdelingen skulle være med på sidelinien, når rettelserne til opsætningen blev fortaget, hvorved de lærte, hvordan det skulle se ud, og hvilke faldgrupper der er. Sikkerhedsfirmaet mente ikke, at ELO på nogen måde var skyld i de problemer, der havde været, da problemerne var grundet i en forkert opsætning af programmet, som var kommet efter virksomheden havde skiftet server. Sikkerhedsfirmaet mente dog at rettigheden, som tilsidesatte alle andre rettigheder skulle gøres mere synlig, så den ikke blev tildelt ved en fejl.

Antal led før kæden brister

Hvor mange fejl skal der egentlig være på ELO opsætningen, før det hele falder samme og en hacker har frit spil i arkiverne. Hvis fil/mappeadgangen bare er sat forkert på enten SQL serverens databasemappe eller på arkivmappen, vil der være fri adgang for en hacker. Det er vigtig at pointere her, at hackeren skal have adgang til virksomheden netværk enten via en bagdør eller ved at fysisk sidde på netværket med en computer for at kunne se mapperne. En forkert opsat adgang til Global mappen vil ikke i første omgang true arkiverne, men en hacker kan lave ravage i brugernes ELO postbokse og globale indstillinger.
Hvis mappeadgangen på arkivmappen er forkert opsat, vil en hacker frit kunne bevæge sig rundt i arkiverne, og den eneste hindring er at filerne er navngivet af ELO, og er derfor ikke sigende for hvad filerne indeholder. Dog kan hackeren, hvis han har brug for mere tid til at finde dét han søger, bare kopiere arkiverne til sin egen maskine og her, i fred og ro, søge i arkiverne til han finder det, han skal bruge. Er hackere kun ude på at ødelægge er han rimelig

ligeglad med hvordan filerne er navngivet. I denne situation ødelægges data bare ved at slette eller modificere disse med inkorrekt data.
Hvis en hacker får fri adgang til ELO's SQL database, kan han finde frem til brugernavne og kodeord, men da kodeordene er maskeret, kræver det, at han kan finde ud af at bryde maskeringen for at opnå adgang til ELO. En anden hindring i dette tilfælde er, at hackeren skal have adgang til klientprogrammet for at logge ind, og når han er inde skal han benytte en ELO administrator konto for at kunne lave alvorlig ravage.

Den perfekte ELO opsætning

For at opnå maksimal sikkerhed i ELO-opsætningen skal følgende kriterier være opfyldt: Mappen som indeholder ELO arkiverne skal kun medlemmer af ELO-administratorgruppen have fuld adgang til. Derudover skal mappen som indeholder ELO-klient-programmet kun give medlemmer af ELO-brugergruppen ret til at se og afvikle klientprograminstallationen, dette er ikke et krav fra ELO, men det er med til at øge sikkerhden. ELO-brugergruppen skal desuden have ret til at læse og afvikle i Global-mappen, og ELO-administratorgruppen skal have fuld adgang i Global-mappen, som indeholder deres postboks og globale indstillinger. Mappen med SQL-databasen skal kun brugeren, som afvikler SQL-programmet, og den brugergruppe, som blev oprettet under installationen af MS SQL 2005, have fuld adgang til. Alle andre brugere skal ikke tildeles nogen form for adgang til disse mapper. Det er desuden vigtigt, at man begrænser medlemmerne af ELO-administratorgruppen til kun at indeholde den bruger, som afvikler ELO-server-programmet, og den bruger, som afvikler backup-programmet. Det er vigtigt at der ikke er for mange der får adgang til arkiverne, da disse er det vigtigste i et dokument management system. Grunden til at man begrænser adgangen til Global-mappen, er for at personer, der ikke har fået adgang til ELO, ikke skal have mulighed for at pille i brugernes globale indstillinger og postbokse.
Man kan sige, at ELO udnytter Windows til at lave en mur omkring ELO, hvor den eneste mulighed for at komme ind er at have et gyldigt Windows brugernavn og kodeord, samt et brugernavn og kodeord til ELO. Ved at bruge Windows på denne måde sikrer ELO, at skylden for eventuelle indbrud vil ligge hos Microsoft eller internt hos virksomheden. Skylden vil være Microsofts, hvis en angriber udnytter en bagdør, som findes i Windows, til at opnå adgang til ELO's arkiver.

Skylden vil ligge intern i virksomheden, som anvender ELO, hvis angriberen har opnået adgang via brugernavn og kodeord. Dette kan forekomme, hvis brugerne i virksomheden har en sløset omgang med deres kodeord, eller hvis kravene til kodeordene ikke er sat højt nok. En virksomhed vil stå i et dilemma, når der skal tages stilling til en kodeordspolitik. Hvis kravene til kodeordet er for lavt, vil det være for let at gætte eller finde frem til det via brute force. Et eksempel på hvor let det kan være, at knække et kodeord kan være, at hvis kravene er at et kodeord skal være 6 bogstaver, og der må kun bruges bogstaver. Det giver ca. 308 millioner mulige kodeord, hvis man kun benytter små bogstaver. Dette lyder måske af meget, men det vil kun tage et program specielt designet til at teste kodeord 2 min og 40 sekunder at prøve alle mulige kombinationer. Hvis kodeordskravet udvides til både brug af store og små bogstaver når man op på 19 mia. mulige kombinationer[8]. Dette betyder at kodeordet kan knækkes på lige lidt over en uge. En tidligere hacker fortæller i sin blog om, hvor let det er at finde frem til folks kodeord på forskellig vis. Han har desuden lavet en tabel, der viser hvor lang tid det vil tage at knække et kodeord[9][10]:

Kodeords længde	Alle typer tegn	Kun små bogstaver
3 tegn	0.86 sekunder	0.02 sekunder
4 tegn	1.36 min	0.046 sekunder
5 tegn	2.15 timer	11.9 sekunder
6 tegn	8.51 dage	5.15 sekunder
7 tegn	2.21 år	2.23 sekunder
8 tegn	2.10 århundreder	2.42 dage
9 tegn	20 årtusinder	2.07 måneder
10 tegn	1,899 årtusinder	4.48 år
11 tegn	180,365 årtusinder	1.16 århundreder
12 tegn	17,184,705 årtusinder	3.03 årtusinder
13 tegn	1,627,797,068 årtusinder	78.7 årtusinder
14 tegn	154,640,721,434 årtusinder	2,046 årtusinder

Det bliver derfor anbefalet, at man som minimum anvender nedenstående krav, når man laver sit kodeord [11]:

- Eight to 14 characters
- One or more punctuation marks
- One or more digits
- A leading letter
- A trailing letter
- A mix of upper and lower case

- No repeating letters
- No use of forward slash
- No use of words related to my name

Hvis kravene bliver for høje vil brugerne begynde at have en sløset omgang med sine kodeord, idet disse bliver svært at huske, samtidig med at det af sikkerhedsmæssige grunde skal skiftes hver 3-6 måned. Det betyder at brugerne skriver deres kodeord ned på et stykke papir, og har det papir liggende i skuffen ved siden af computeren. En undersøgelse underbygger dette, idet den viste at en tredjedel af alle medarbejder har deres kodeord nedskrevet på en seddel nær deres computer [12].
En nærliggende tanke for et angreb er at lave et man-in-the-middle angreb. Dette angreb virker ved, at en hacker sidder imellem brugeren og serveren, og udgiver sig overfor brugeren for at være serveren og overfor serveren at være brugeren. Fordelen ved at lave sådan et angreb er, at det kan være meget svært at bevise, at der har siddet en imellem brugen og serveren, men bagsiden ved denne form for angreb er, at det kræver stor ekspertise at udføre. Jeg spurgte Mr. Thiele, som er chef for ELO's udviklingsafdeling, om det var muligt at lave et man-in-the-middle angreb på ELO Professional 5, imellem dennes klient og server program. Til det svarede han, at det ikke var muligt at lave, da ELO har metoder til at sikre, at det er den rigtige bruger, der sender forespørgslerne. Det var dog ikke muligt at få en beskrivelse af de metoder, der bliver brugt i denne sammenhæng.

Nyudviklet sikkerhedsprogram

Jeg har valgt at udvikle programmet i C# og bruge funktioner fra .NET. Derfor kræver mit program at minimum .NET version 2.0 er installeret.
Da den primære beskyttelse mod at uvedkommende får adgang til ELO's arkiver, er at begrænse adgang ved at bruge Windows fil/mappeadgangsstyring. Derfor har jeg valgt at fokusere mit program på at teste om opsætningen af adgangen til arkiverne og Global-mappen, er sat rigtigt. Skulle opsætningen være forkert, kan man få programmet til at sætte indstillingerne rigtigt.

Programmets GUI[15] kan ses i fig. 6. Der er indsat tal i felterne, som der vil blive refereret til i teksten, når funktionen beskrives. Når der refereres til knapperne i GUI'en vil jeg skrive deres tekst i anførselstegn.

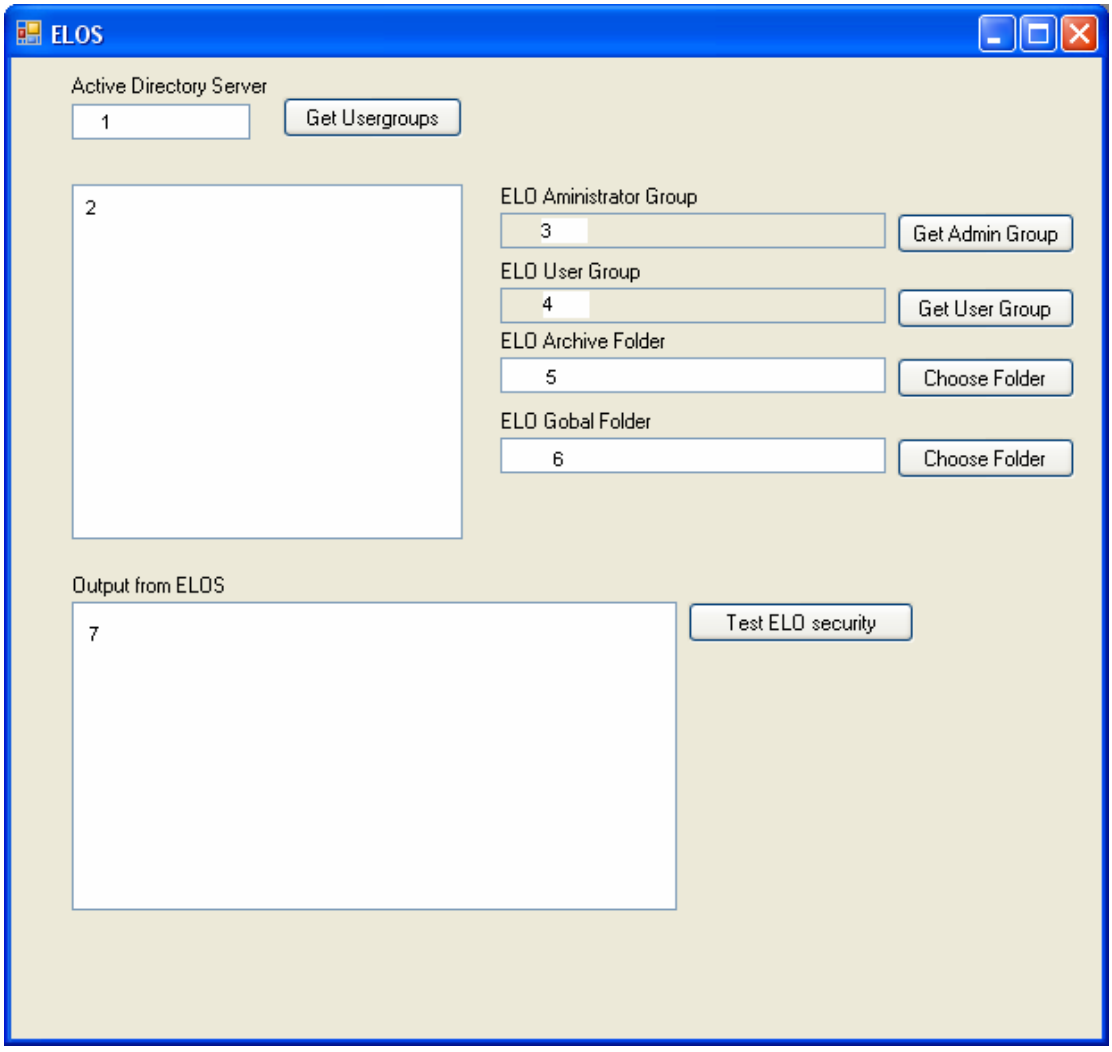

Fig. 6 GUI fra det ny udviklede program.

For at bruge programmet skal man først indtaste navnet på serveren, som kører Active Directory (AD) i felt 1, herefter trykkes på "Get Usergroups". Programmet laver nu et kald til AD'en med en forespørgsel efter alle brugergrupperne, som findes i AD'en. Resultatet af forespørgselen bliver vist som en list i felt 2. Herefter markeres ELO's administratorgruppe fra listen i felt 2 og der trykkes på "Get Admin Group". Navnet på gruppen bliver vist i felt 3, og gruppens SID bliver gemt i en intern variabel i programmet. Derefter vælges ELO's brugergruppe fra listen i felt 2 og der trykkes på "Get User Group". Herefter bliver navnet på gruppen vist i felt 4, og gruppens SID bliver gemt i en intern variabel i programmet. Som det

[15] Grafic User Interface

ses i fig. 6 er felt 3 og 4's baggrund grå, hvilket betyder at de er låst mod skrivning fra brugeren. Denne låsning er anvendt, fordi mit program kræver at de to gruppers SID er sat i de interne variable, for at den kan kører. Det kan derfor ikke nytte noget, at brugeren indtaster navne på grupper direkte i felterne, for da bliver de to variable med SID ikke sat.
Herefter skal man vælge ELO's arkiv mappe, og for at gøre dette kan man enten indtaste stien til mappen, eller man kan få et vindue frem (se fig. 7), hvor man kan vælge mappen, ved at trykke på "Choose Folder". Hvis man bruger "Choose Folder" bliver stien til mappen automatisk indsat i felt 5. Det samme gælder for stien til ELO Global mappen, her kan man også selv indtaste stien i felt 6 eller blot vælge mappen via "Choose folder".

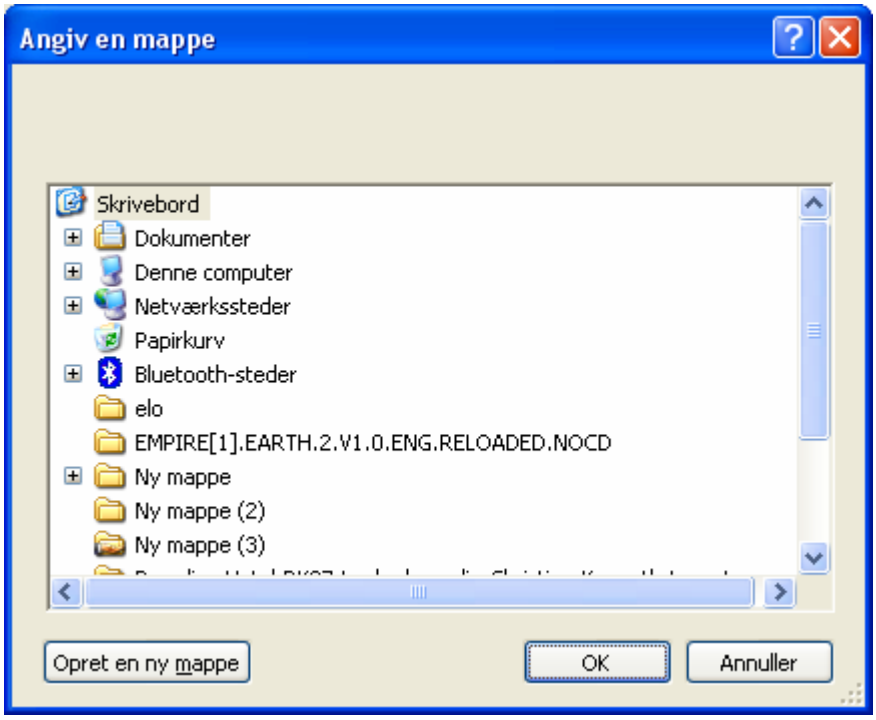

Fig. 7 Vinduet der kommer frem når der trykkes på "Choose Folder"

Nu har programmet tilstrækkelig information til teste opsætningen af ELO Proffesional 5. Dette gøres ved at trykke på "Test ELO Security". Når der trykkes på denne knap vil programmet først se om de to mapper, der er angivet i felt 5 og 6 findes. Findes de af programmet, hentes først adgangslisten fra ELO's arkiv mappe, og denne liste bliver gennemgået af programmet, for at se om det kun er ELO's administratorgruppen i den, og at gruppen har fuld kontrol. Derefter bliver adgangslisten for ELO's Global mappe hentet, og denne vil også blive gennemgået, for at se om det kun er ELO's administratorgruppe og ELO's brugergruppe, som er i listen, og at administratorgruppen har fuld kontrol, og brugergruppen kun har læs og kørsel adgang. Resultatet af denne kontrol bliver lagt i en liste

som en talværdi. De mulige værdier, som kan blive skrevet i listen, og beskederne de svarer til, kan ses i fig 8. Disse værdier bliver oversat til tekst og skrevet i felt 7. Skulle der være fejl i opsætningen, bliver en ny knap vist med teksten: ”Correct ELO settings”. Værdien 1 til 10 er reserveret til fejl med ELO’s arkiv mappe. Værdier mellem 11 og 20 er reserveret fejl ved ELO’s Global mappe, og værdier mellem 100 og 110 er beskeder om korrekt opsætningen. De mulige beskeder man kan få fra programmet med tilhørende værdi er vist i fig. 8.

Værdi	Besked	Vises korrektions knappen
1	ERROR: There are to many groups and users assigned to ELO's archive.	Ja
2	ERROR: ELO Admin-group does not have the correct access.	Ja
3	ERROR: The group assigned to the ELO archive is not the selected ELO Admin group.	Ja
11	ERROR: There are to many groups and users assigned to ELO's Gobal-folder.	Ja
12	ERROR: The group assigned to the ELO Gobal-folder is not the selected ELO Admin group.	Ja
13	ERROR: The group assigned to the ELO Gobal-folder is not the selected ELO user-group.	Ja
14	ERROR: ELO Admin-group does not have the correct access.	Ja
15	ERROR: ELO User-group does not have the correct access.	Ja
100	CORRECT: ELO arhive has the correct setup.	Nej
101	CORRECT: ELO Gobal-folder has the correct setup for the Admin-group.	Nej
102	CORRECT: ELO Gobal-folder has the correct setup for the User-group.	Nej

Fig. 8 Viser de forskellige værdier som programmet kan sætte i resultat listen og den tilhørende tekst som bliver skrevet i felt 7 i fig. 6, samt om værdien aktivere ”Correct ELO settings”.

Når man trykker på ”Correct ELO settings”, bliver ELO’s arkiv mappens adgangsliste rettet til, at den valgte administratorgruppe har fuld kontrol, og ingen andre har adgang, hvis værdien i listen er mellem 1 og 10. Er der en værdi i listen mellem 11 og 20, bliver ELO’s

Global mappes adgangsliste rettet, så kun ELO's administratorgruppe har fuld kontrol, og ELO's brugergruppe har læs og kørsel adgang. Ved alle andre værdier skal der ikke ændres noget i opsætningen, og " Correct ELO settings" vil ikke blive vist.
Med hensyn til mulige udvidelser til dette program er det nærliggende, at tænke på at man kunne lave et modul til den, som kunne teste styrken af brugernes kodeord, da den eneste vej ind i arkiver nu er gennem ELO Professional 5. Det kan derfor ikke nytte noget, hvis brugernes kodeord er for svage, og derfor nemt kan gættes. For at lave et sådanne modul kræver det, at man skal have programmet til at kommunikere med ELO's login menu eller finde frem til den måde ELO kommunikere mellem serverprogrammet og klientprogrammet.

Konklusion

Efter at have undersøgt ELO Professional 5, må jeg konkludere at sikkerheden generelt er meget god. Det er ikke bare et halvhjertet forsøg på at give indtryk af, at systemet er sikkert. Folkene i ELO Digital Office har tænkt over tingene og formået at udnytte den indbyggede sikkerhed, der findes i Windows til at data sikres i arkiverne. Ved at bruge fil/mappe adgangskontrollen på arkiv mapperne og Global mappen sikrer ELO effektivt, at man skal gennem deres program for at komme ind til arkiverne.
Det er faktisk i selve ELO Professional 5 programmet der er størst grund til bekymring. Som nævnt tidligere er der midt mellem rettighederne placeret en rettighed, der trumfer alle andre rettigheder, og giver fuld adgang til hele arkivet. Det er min mening at denne rettighed, på en eller anden måde skal gøres mere synlig, så man ikke kommer til at tildele rettigheden til nogen, som ikke skal have den. Mit forslag er at man flytter rettigheden op i toppen af listen, og gør skriften fed, så den skiller sig ud fra de øvrige rettigheder. Bortset fra denne ene mulige fejlkilde giver ELO Professional 5 rig mulighed for at begrænse adgang for brugerne til forskellige dele af arkivet. Det er nemt at tildele brugergrupper eller nøgler adgang til dele af arkivet og derefter tildele disse til brugerne. I udviklingen af ELO Professional 5 har ELO gennemtænkt dette aspekt godt. De har ved implementeringen gjort sådan, at tildeling af en nøgle ikke umiddelbart betyder, at man har ubegrænset adgang til de dele af arkivet, som åbnes med nøglen. Det kommer helt an på, hvor mange af de fire nøglerettigheder brugeren får tildelt med nøglen. De fire rettigheder der følger med nøglen er: læse, skrive, slette og afvikling. Har brugeren fået tildelt bare én af disse rettigheder, vil han altid kunne se filerne.

ELO har yderligere indført den smarte funktion, at det kun er administratorer der kan slette filer permanent. En bruger vil, hvis han har rettigheder til at slette, kunne slette filer, men filen bliver ikke slettet fysisk fra harddisken. Dette betyder at IT-afdelingen ikke skal ud og have fat i backup'en, hvis en bruger kommer til at slette noget forkert, men blot kan fjerne den markering som brugeren satte da filen blev slettet i ELO, hvorefter filen igen er synlig i ELO. Programmet der er blevet designet til netop dette projekt, kan se om opsætningen på arkiver og Gobal-mappen er korrekt opsat ved at lave forespørgsler til adgangslisten på mapperne og her sammenligne resultaterne med de valgte brugergrupper. Programmet kan, i tilfælde af fejl, rette fejlen ved opsætningen, således at opsætningen kan leve op til de ønskede krav, ELO har for at deres system er sikkert.

Kilder

[1] Microsoft Windows Security Ressource Kit, Second Edition
Ben Smith, Brian Komar og Microsoft Security Team
Microsoft Press
2005

[2] http://en.wikipedia.org/wiki/Enigma_machine

[3] http://en.wikipedia.org/wiki/Data_Encryption_Standard

[4] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[5] http://www.elo-digital.com/

[6] http://en.wikipedia.org/wiki/Twofish

[7] http://en.wikipedia.org/wiki/Md5

[8] http://rf-web.tamu.edu/security/SECGUIDE/V1comput/Password.htm

[9] http://onemansblog.com/2007/03/26/how-id-hack-your-weak-passwords/

[10] http://ekstrabladet.dk/nyheder/samfund/article289944.ece

[11] http://www.symantec.com/enterprise/security_response/weblog/2006/06/passwords.html

[12] http://epn.dk/teknologi/internet/article4899.ece

Derudover er anvendt:

”Installation Training Module” fra ELO Digital Office. (Appendiks B)

”ELO Professional 5 Client manual” (Appendiks D)

Brute Force
Matt Curtin
Copernicus Books
2005

Security in Computing, third edition
C. P. Pfleeger & S. L. Pfleeger
Prentice Hall
2003.

Windows Server 2003 Resource Kit

The Microsoft Windows Server Team

Microsoft Press

2005

Appendiks indholdsfortegnelse

Appendiks A

Nyudviklet programs kode.

Dette appendiks indeholder alt koden til programmet som blev udviklet i dette projekt.
Programmet består af følgende filer:
Program.cs
ELOS.cs
ELOS.Designer.cs
Resources.Designer.cs
Settings.Designer.cs
AssemblyInfo.cs

Programmet findes også på den vedlagte cd, i form af et Microsoft Visual Studio Project.

Program.cs

```
using System;
using System.Collections.Generic;
using System.Windows.Forms;

namespace ELOS
{
    static class Program
    {
        /// <summary>
        /// The main entry point for the application.
        /// </summary>
        [STAThread]
        static void Main()
        {
            Application.EnableVisualStyles();
            Application.SetCompatibleTextRenderingDefault(false);
            Application.Run(new ELOS());
        }
    }
}
```

ELOS.cs

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Text;
using System.Windows.Forms;
using System.DirectoryServices;

namespace ELOS
{
    public partial class ELOS : Form
    {
        // Variabls being used by the program.
        List<string> SID = new List<string>();
        string ELOAdminSID = "";
        string ELOUserSID = "";
        int count = 0;
        List<int> fouls = new List<int>();
        bool visibelcorret = false;

        public ELOS()
        {
            InitializeComponent();
        }

        // Function started if there is a click on button "Get Usergroups"
        private void getGroups_Click(object sender, EventArgs e)
        {
            listBox1.Items.Clear();
            // Test if anything is entered in the ADServer field.
            if (ADServer.TextLength == 0)
            {
                listBox1.Items.Add("Please enter the name on the AD-
server");
            }
            else
            {
                // The try is here in case the the AD-server is not found
and a
                // exeption i casted.
                try
                {
                    ADGrouplist.Items.Clear();
                    SID.Clear();
                    // Call to the AD-server to get all user-groups and
their SID.
                    DirectoryEntry ADentry = new DirectoryEntry("LDAP://" +
ADServer.Text);
                    DirectorySearcher ADsearch = new
DirectorySearcher(ADentry);
                    ADsearch.Filter = ("(objectclass=group)");
                    foreach (System.DirectoryServices.SearchResult ADresult
in ADsearch.FindAll())
                    {
```

```
ADGrouplist.Items.Add(ADresult.GetDirectoryEntry().Name.ToString());
                        SID.Add(new
System.Security.Principal.SecurityIdentifier((byte[])ADresult.GetDirectoryE
ntry().Properties["objectSid"][0], 0).Value.ToString());
                    }
                }
                catch (Exception exp)
                {
                    listBox1.Items.Add("The servername entered is not
correct or");
                    listBox1.Items.Add("there is no connection to the
server");
                    listBox1.Items.Add("Message from windows:
"+exp.Message.ToString());
                }
            }
        }
        // Function started if there is a click on button "Get Admin Group"
        private void getAdmin_Click(object sender, EventArgs e)
        {
            // Sendes the name of the Admin group to the ELOAdmin-field if
one is selected.
            try
            {
                ELOAdmin.Text = ADGrouplist.SelectedItem.ToString();
                ELOAdminSID = SID[ADGrouplist.SelectedIndex].ToString();
            }
            catch
            {
                ELOAdmin.Text = "No group selected.";
            }
        }
        // Function started if there is a click on button "Get User Group"
        private void getUser_Click(object sender, EventArgs e)
        {
            // Sendes the name of the User group to the ELOUser-field if
one is selected.
            try
            {
                ELOUser.Text = ADGrouplist.SelectedItem.ToString();
                ELOUserSID = SID[ADGrouplist.SelectedIndex].ToString();
            }
            catch
            {
                ELOUser.Text = "No group selected.";
            }
        }
        // Function started if there is a click on button "Choose folder"
(ELO archive folder)
        private void Choosefolder1_Click(object sender, EventArgs e)
        {
            // Startes a browser dialog window and sets the path to the
fólder
            // selected in the ELOArchive-field
            folderBrowserDialog1.Reset();
            DialogResult foldersucces = folderBrowserDialog1.ShowDialog();
            if (foldersucces == DialogResult.OK)
            {
```

```
                ELOArchive.Text = folderBrowserDialog1.SelectedPath;
            }
        }
        // Function started if there is a click on button "Choose folder"
(ELO Global folder)
        private void Choosefolder2_Click(object sender, EventArgs e)
        {
            // Startes a browser dialog window and sets the path to the
fólder
            // selected in the ELOGlobal-field
            folderBrowserDialog1.Reset();
            DialogResult foldersucces = folderBrowserDialog1.ShowDialog();
            if (foldersucces == DialogResult.OK)
            {
                ELOGlobal.Text = folderBrowserDialog1.SelectedPath;
            }
        }
        // Function started if there is a click on button "Test ELO
security"
        private void test_Click(object sender, EventArgs e)
        {
            listBox1.Items.Clear();
            fouls.Clear();
            bool status = true;
            // See if all the required fields have data in them.
            if (ELOAdmin.TextLength == 0)
            {
                status = false;
                ELOAdmin.Text = "Error no group selected";
            }
            if (ELOUser.TextLength == 0)
            {
                status = false;
                ELOUser.Text = "Error no group selected";
            }
            if (ELOArchive.TextLength == 0)
            {
                status = false;
                ELOArchive.Text = "Error no folder selected";
            }
            if (ELOGlobal.TextLength == 0)
            {
                status = false;
                ELOGlobal.Text = "Error no folder selected";
            }
            if (ELOAdminSID.Length == 0)
            {
                listBox1.Items.Add("Error in selecting admin-group.");
                listBox1.Items.Add("Please select group via the group-
list.");
            }
            if (ELOUserSID.Length == 0)
            {
                listBox1.Items.Add("Error in selecting user-group.");
                listBox1.Items.Add("Please select group via the group-
list.");
            }
            if (status == true)
            {
```

```
                try
                {
                    // See if the to selected paths exists.
                    if (System.IO.Directory.Exists(ELOArchive.Text) &&
System.IO.Directory.Exists(ELOGlobal.Text))
                    {
                        // Get the AccessControl related too the ELO
archive folder.
                        System.Security.AccessControl.DirectorySecurity
ArchiveSec = System.IO.Directory.GetAccessControl(ELOArchive.Text);

System.Security.AccessControl.AuthorizationRuleCollection AccessRules =
ArchiveSec.GetAccessRules(true, true,
Type.GetType("System.Security.Principal.SecurityIdentifier"));
                        // Test the archive folder fore errors.
                        if (AccessRules.Count > 1)
                        {
                            fouls.Add(1);
                        }
                        else
                        {
                            if
(AccessRules[0].IdentityReference.ToString().Equals(ELOAdminSID))
                            {
                                count = 0;

System.Security.AccessControl.FileSystemAccessRule[] rule = new
System.Security.AccessControl.FileSystemAccessRule[AccessRules.Count];
                                foreach
(System.Security.AccessControl.FileSystemAccessRule rule2 in AccessRules)
                                {
                                    rule[count] = rule2;
                                    count++;

                                }
                                if (rule[0].FileSystemRights ==
System.Security.AccessControl.FileSystemRights.FullControl)
                                {
                                    fouls.Add(100);
                                }
                                else
                                {
                                    fouls.Add(2);
                                }
                            }
                            else
                            {
                                fouls.Add(3);
                            }
                        }

                        // Get the AccessControl related too the ELO Global
folder.
                        ArchiveSec =
System.IO.Directory.GetAccessControl(ELOGlobal.Text);
                        AccessRules = ArchiveSec.GetAccessRules(true, true,
Type.GetType("System.Security.Principal.SecurityIdentifier"));
                        // Test the Global folder fore errors.
                        if (AccessRules.Count > 2)
```

```
                        {
                            fouls.Add(11);
                        }
                        else
                        {
                            if
(AccessRules[0].IdentityReference.ToString().Equals(ELOAdminSID))
                            {
                                if
(AccessRules[1].IdentityReference.ToString().Equals(ELOUserSID))
                                {
                                    count = 0;

System.Security.AccessControl.FileSystemAccessRule[] rule = new
System.Security.AccessControl.FileSystemAccessRule[AccessRules.Count];
                                    foreach
(System.Security.AccessControl.FileSystemAccessRule rule2 in AccessRules)
                                    {
                                        rule[count] = rule2;
                                        count++;

                                    }
                                    if (rule[0].FileSystemRights ==
System.Security.AccessControl.FileSystemRights.FullControl)
                                    {
                                        fouls.Add(101);
                                    }
                                    else
                                    {
                                        fouls.Add(14);
                                    }
                                    if (rule[1].FileSystemRights.ToString()
== System.Security.AccessControl.FileSystemRights.ReadAndExecute.ToString()
+ ", " +
System.Security.AccessControl.FileSystemRights.Synchronize.ToString())
                                    {
                                        fouls.Add(102);
                                    }
                                    else
                                    {
                                        fouls.Add(15);
                                    }

                                }
                                else
                                {
                                    fouls.Add(13);
                                }
                            }
                            else if
(AccessRules[1].IdentityReference.ToString().Equals(ELOAdminSID))
                            {
                                if
(AccessRules[0].IdentityReference.ToString().Equals(ELOUserSID))
                                {
                                    count = 0;

System.Security.AccessControl.FileSystemAccessRule[] rule = new
System.Security.AccessControl.FileSystemAccessRule[AccessRules.Count];
```

```
                                    foreach
(System.Security.AccessControl.FileSystemAccessRule rule2 in AccessRules)
                                    {
                                        rule[count] = rule2;
                                        count++;

                                    }
                                    if (rule[1].FileSystemRights ==
System.Security.AccessControl.FileSystemRights.FullControl)
                                    {
                                        fouls.Add(101);
                                    }
                                    else
                                    {
                                        fouls.Add(14);
                                    }
                                    if (rule[0].FileSystemRights.ToString()
== System.Security.AccessControl.FileSystemRights.ReadAndExecute + ", " +
System.Security.AccessControl.FileSystemRights.Synchronize.ToString())
                                    {
                                        fouls.Add(102);
                                    }
                                    else
                                    {
                                        fouls.Add(15);

listBox1.Items.Add(rule[0].FileSystemRights.ToString());
                                    }

                                }
                                else
                                {
                                    fouls.Add(13);
                                }
                            }
                            else
                            {
                                fouls.Add(12);
                            }
                        }
                    }
                    else
                    {
                        listBox1.Items.Add("The folders entered does not
exits.");
                    }
                    /* Foul 1-10 is ELO archive error messages
                     * Foul 11-20 is ELO program error messages
                     * Foul 100-110 is correct messages
                     */
                    visibelcorret = false;
                    foreach (int foul in fouls)
                    {
                        if (foul == 1)
                        {
                            listBox1.Items.Add("ERROR: There are to many
groups and users assigned to ELO's archive.");
                            visibelcorret = true;
                        }
```

```
                        if (foul == 2)
                        {
                            listBox1.Items.Add("ERROR: ELO Admin-group does
not have the correct access.");
                            visibelcorret = true;
                        }
                        if (foul == 3)
                        {
                            listBox1.Items.Add("ERROR: The group assigned
to the ELO archive is not the selected ELO Admin group.");
                            visibelcorret = true;
                        }
                        if (foul == 11)
                        {
                            listBox1.Items.Add("ERROR: There are to many
groups and users assigned to ELO's Gobal-folder.");
                            visibelcorret = true;
                        }
                        if (foul == 12)
                        {
                            listBox1.Items.Add("ERROR: The group assigned
to the ELO Gobal-folder is not the selected ELO Admin group.");
                            visibelcorret = true;
                        }
                        if (foul == 13)
                        {
                            listBox1.Items.Add("ERROR: The group assigned
to the ELO Gobal-folder is not the selected ELO user-group.");
                            visibelcorret = true;
                        }
                        if (foul == 14)
                        {
                            listBox1.Items.Add("ERROR: ELO Admin-group does
not have the correct access.");
                            visibelcorret = true;
                        }
                        if (foul == 15)
                        {
                            listBox1.Items.Add("ERROR: ELO User-group does
not have the correct access.");
                            visibelcorret = true;
                        }
                        if (foul == 100)
                        {
                            listBox1.Items.Add("CORRECT: ELO arhive has the
correct setup.");
                        }
                        if (foul == 101)
                        {
                            listBox1.Items.Add("CORRECT: ELO Gobal-folder
has the correct setup for the Admin-group.");
                        }
                        if (foul == 102)
                        {
                            listBox1.Items.Add("CORRECT: ELO Gobal-folder
has the correct setup for the User-group.");
                        }
                        Correct.Visible = visibelcorret;
                    }
```

```
                }
                catch (Exception EXP)
                {
                    listBox1.Items.Add(EXP.Message.ToString());
                }
            }
        }
        // Function started if there is a click on button "Correct ELO
settings"
        private void Correct_Click(object sender, EventArgs e)
        {
            foreach (int foul in fouls)
            {
                if (foul > 0 && foul < 11)
                {
                    // Gets the AccessControl fore the archive folder and
deletes all the accessrules.
                    System.IO.DirectoryInfo ArchiveInfo = new
System.IO.DirectoryInfo(ELOArchive.Text);
                    System.Security.AccessControl.DirectorySecurity
ArchiveSec = ArchiveInfo.GetAccessControl();

System.Security.AccessControl.AuthorizationRuleCollection AccessRules =
ArchiveSec.GetAccessRules(true, true,
Type.GetType("System.Security.Principal.SecurityIdentifier"));
                    foreach
(System.Security.AccessControl.FileSystemAccessRule rule in AccessRules)
                    {
                        ArchiveSec.RemoveAccessRule(rule);
                    }
                    // Adds the correct accessrules to the AccessControl
and loads the AccessControl
                    // to the archive folder
                    ArchiveSec.AddAccessRule(new
System.Security.AccessControl.FileSystemAccessRule(new
System.Security.Principal.SecurityIdentifier(ELOAdminSID),
System.Security.AccessControl.FileSystemRights.FullControl,
System.Security.AccessControl.InheritanceFlags.None,
System.Security.AccessControl.PropagationFlags.InheritOnly,
System.Security.AccessControl.AccessControlType.Allow));
                    ArchiveSec.AddAccessRule(new
System.Security.AccessControl.FileSystemAccessRule(new
System.Security.Principal.SecurityIdentifier(ELOAdminSID),
System.Security.AccessControl.FileSystemRights.FullControl,
System.Security.AccessControl.InheritanceFlags.ContainerInherit,
System.Security.AccessControl.PropagationFlags.InheritOnly,
System.Security.AccessControl.AccessControlType.Allow));
                    ArchiveSec.AddAccessRule(new
System.Security.AccessControl.FileSystemAccessRule(new
System.Security.Principal.SecurityIdentifier(ELOAdminSID),
System.Security.AccessControl.FileSystemRights.FullControl,
System.Security.AccessControl.InheritanceFlags.ObjectInherit,
System.Security.AccessControl.PropagationFlags.InheritOnly,
System.Security.AccessControl.AccessControlType.Allow));
                    ArchiveInfo.SetAccessControl(ArchiveSec);

                }
                if (foul > 10 && foul < 21)
                {
```

```
                    // Gets the AccessControl fore the Global folder and
deletes all the accessrules.
                    System.IO.DirectoryInfo ArchiveInfo = new
System.IO.DirectoryInfo(ELOGlobal.Text);
                    System.Security.AccessControl.DirectorySecurity
ArchiveSec = ArchiveInfo.GetAccessControl();

System.Security.AccessControl.AuthorizationRuleCollection AccessRules =
ArchiveSec.GetAccessRules(true, true,
Type.GetType("System.Security.Principal.SecurityIdentifier"));
                    foreach
(System.Security.AccessControl.FileSystemAccessRule rule in AccessRules)
                    {
                        ArchiveSec.RemoveAccessRule(rule);
                    }
                    // Adds the correct accessrules to the AccessControl
and loads the AccessControl
                    // to the Global folder
                    ArchiveSec.AddAccessRule(new
System.Security.AccessControl.FileSystemAccessRule(new
System.Security.Principal.SecurityIdentifier(ELOAdminSID),
System.Security.AccessControl.FileSystemRights.FullControl,
System.Security.AccessControl.InheritanceFlags.None,
System.Security.AccessControl.PropagationFlags.InheritOnly,
System.Security.AccessControl.AccessControlType.Allow));
                    ArchiveSec.AddAccessRule(new
System.Security.AccessControl.FileSystemAccessRule(new
System.Security.Principal.SecurityIdentifier(ELOAdminSID),
System.Security.AccessControl.FileSystemRights.FullControl,
System.Security.AccessControl.InheritanceFlags.ContainerInherit,
System.Security.AccessControl.PropagationFlags.InheritOnly,
System.Security.AccessControl.AccessControlType.Allow));
                    ArchiveSec.AddAccessRule(new
System.Security.AccessControl.FileSystemAccessRule(new
System.Security.Principal.SecurityIdentifier(ELOAdminSID),
System.Security.AccessControl.FileSystemRights.FullControl,
System.Security.AccessControl.InheritanceFlags.ObjectInherit,
System.Security.AccessControl.PropagationFlags.InheritOnly,
System.Security.AccessControl.AccessControlType.Allow));
                    ArchiveSec.AddAccessRule(new
System.Security.AccessControl.FileSystemAccessRule(new
System.Security.Principal.SecurityIdentifier(ELOUserSID),
System.Security.AccessControl.FileSystemRights.ReadAndExecute,
System.Security.AccessControl.InheritanceFlags.None,
System.Security.AccessControl.PropagationFlags.InheritOnly,
System.Security.AccessControl.AccessControlType.Allow));
                    ArchiveSec.AddAccessRule(new
System.Security.AccessControl.FileSystemAccessRule(new
System.Security.Principal.SecurityIdentifier(ELOUserSID),
System.Security.AccessControl.FileSystemRights.ReadAndExecute,
System.Security.AccessControl.InheritanceFlags.ContainerInherit,
System.Security.AccessControl.PropagationFlags.InheritOnly,
System.Security.AccessControl.AccessControlType.Allow));
                    ArchiveSec.AddAccessRule(new
System.Security.AccessControl.FileSystemAccessRule(new
System.Security.Principal.SecurityIdentifier(ELOUserSID),
System.Security.AccessControl.FileSystemRights.ReadAndExecute,
System.Security.AccessControl.InheritanceFlags.ObjectInherit,
```

```
System.Security.AccessControl.PropagationFlags.InheritOnly,
System.Security.AccessControl.AccessControlType.Allow));
                    ArchiveInfo.SetAccessControl(ArchiveSec);
                }
            }
            Correct.Visible = false;
        }
    }
}
```

ELOS.Designer.cs

```
namespace ELOS
{
    partial class ELOS
    {
        /// <summary>
        /// Required designer variable.
        /// </summary>
        private System.ComponentModel.IContainer components = null;

        /// <summary>
        /// Clean up any resources being used.
        /// </summary>
        /// <param name="disposing">true if managed resources should be
disposed; otherwise, false.</param>
        protected override void Dispose(bool disposing)
        {
            if (disposing && (components != null))
            {
                components.Dispose();
            }
            base.Dispose(disposing);
        }

        #region Windows Form Designer generated code

        /// <summary>
        /// Required method for Designer support - do not modify
        /// the contents of this method with the code editor.
        /// </summary>
        private void InitializeComponent()
        {
            this.ADServer = new System.Windows.Forms.TextBox();
            this.label1 = new System.Windows.Forms.Label();
            this.ADGrouplist = new System.Windows.Forms.ListBox();
            this.getGroups = new System.Windows.Forms.Button();
            this.ELOAdmin = new System.Windows.Forms.TextBox();
            this.getAdmin = new System.Windows.Forms.Button();
            this.getUser = new System.Windows.Forms.Button();
            this.ELOUser = new System.Windows.Forms.TextBox();
            this.label2 = new System.Windows.Forms.Label();
            this.label3 = new System.Windows.Forms.Label();
            this.ELOArchive = new System.Windows.Forms.TextBox();
            this.ELOGlobal = new System.Windows.Forms.TextBox();
            this.label4 = new System.Windows.Forms.Label();
            this.label5 = new System.Windows.Forms.Label();
            this.folderBrowserDialog1 = new
System.Windows.Forms.FolderBrowserDialog();
            this.Choosefolder1 = new System.Windows.Forms.Button();
            this.Choosefolder2 = new System.Windows.Forms.Button();
            this.test = new System.Windows.Forms.Button();
            this.listBox1 = new System.Windows.Forms.ListBox();
            this.label6 = new System.Windows.Forms.Label();
            this.Correct = new System.Windows.Forms.Button();
            this.SuspendLayout();
            //
            // ADServer
```

```
            //
            this.ADServer.Location = new System.Drawing.Point(34, 26);
            this.ADServer.Name = "ADServer";
            this.ADServer.Size = new System.Drawing.Size(100, 20);
            this.ADServer.TabIndex = 0;
            //
            // label1
            //
            this.label1.AutoSize = true;
            this.label1.Location = new System.Drawing.Point(31, 9);
            this.label1.Name = "label1";
            this.label1.Size = new System.Drawing.Size(116, 13);
            this.label1.TabIndex = 1;
            this.label1.Text = "Active Directory Server";
            //
            // ADGrouplist
            //
            this.ADGrouplist.FormattingEnabled = true;
            this.ADGrouplist.HorizontalScrollbar = true;
            this.ADGrouplist.Location = new System.Drawing.Point(34, 71);
            this.ADGrouplist.Name = "ADGrouplist";
            this.ADGrouplist.Size = new System.Drawing.Size(219, 199);
            this.ADGrouplist.TabIndex = 2;
            //
            // getGroups
            //
            this.getGroups.Location = new System.Drawing.Point(152, 22);
            this.getGroups.Name = "getGroups";
            this.getGroups.Size = new System.Drawing.Size(101, 23);
            this.getGroups.TabIndex = 3;
            this.getGroups.Text = "Get Usergroups";
            this.getGroups.UseVisualStyleBackColor = true;
            this.getGroups.Click += new
System.EventHandler(this.getGroups_Click);
            //
            // ELOAdmin
            //
            this.ELOAdmin.Location = new System.Drawing.Point(274, 87);
            this.ELOAdmin.Name = "ELOAdmin";
            this.ELOAdmin.ReadOnly = true;
            this.ELOAdmin.Size = new System.Drawing.Size(216, 20);
            this.ELOAdmin.TabIndex = 4;
            //
            // getAdmin
            //
            this.getAdmin.Location = new System.Drawing.Point(496, 87);
            this.getAdmin.Name = "getAdmin";
            this.getAdmin.Size = new System.Drawing.Size(100, 23);
            this.getAdmin.TabIndex = 5;
            this.getAdmin.Text = "Get Admin Group";
            this.getAdmin.UseVisualStyleBackColor = true;
            this.getAdmin.Click += new
System.EventHandler(this.getAdmin_Click);
            //
            // getUser
            //
            this.getUser.Location = new System.Drawing.Point(496, 129);
            this.getUser.Name = "getUser";
            this.getUser.Size = new System.Drawing.Size(100, 23);
```

```
            this.getUser.TabIndex = 6;
            this.getUser.Text = "Get User Group";
            this.getUser.UseVisualStyleBackColor = true;
            this.getUser.Click += new
System.EventHandler(this.getUser_Click);
            //
            // ELOUser
            //
            this.ELOUser.Location = new System.Drawing.Point(274, 129);
            this.ELOUser.Name = "ELOUser";
            this.ELOUser.ReadOnly = true;
            this.ELOUser.Size = new System.Drawing.Size(216, 20);
            this.ELOUser.TabIndex = 7;
            //
            // label2
            //
            this.label2.AutoSize = true;
            this.label2.Location = new System.Drawing.Point(271, 71);
            this.label2.Name = "label2";
            this.label2.Size = new System.Drawing.Size(117, 13);
            this.label2.TabIndex = 8;
            this.label2.Text = "ELO Aministrator Group";
            //
            // label3
            //
            this.label3.AutoSize = true;
            this.label3.Location = new System.Drawing.Point(271, 113);
            this.label3.Name = "label3";
            this.label3.Size = new System.Drawing.Size(85, 13);
            this.label3.TabIndex = 9;
            this.label3.Text = "ELO User Group";
            //
            // ELOArchive
            //
            this.ELOArchive.Location = new System.Drawing.Point(274, 168);
            this.ELOArchive.Name = "ELOArchive";
            this.ELOArchive.Size = new System.Drawing.Size(216, 20);
            this.ELOArchive.TabIndex = 10;
            //
            // ELOGlobal
            //
            this.ELOGlobal.Location = new System.Drawing.Point(274, 213);
            this.ELOGlobal.Name = "ELOGlobal";
            this.ELOGlobal.Size = new System.Drawing.Size(216, 20);
            this.ELOGlobal.TabIndex = 11;
            //
            // label4
            //
            this.label4.AutoSize = true;
            this.label4.Location = new System.Drawing.Point(271, 152);
            this.label4.Name = "label4";
            this.label4.Size = new System.Drawing.Size(99, 13);
            this.label4.TabIndex = 12;
            this.label4.Text = "ELO Archive Folder";
            //
            // label5
            //
            this.label5.AutoSize = true;
            this.label5.Location = new System.Drawing.Point(271, 197);
```

```
            this.label5.Name = "label5";
            this.label5.Size = new System.Drawing.Size(93, 13);
            this.label5.TabIndex = 13;
            this.label5.Text = "ELO Global Folder";
            //
            // Choosefolder1
            //
            this.Choosefolder1.Location = new System.Drawing.Point(496,
168);
            this.Choosefolder1.Name = "Choosefolder1";
            this.Choosefolder1.Size = new System.Drawing.Size(100, 23);
            this.Choosefolder1.TabIndex = 14;
            this.Choosefolder1.Text = "Choose Folder";
            this.Choosefolder1.UseVisualStyleBackColor = true;
            this.Choosefolder1.Click += new
System.EventHandler(this.Choosefolder1_Click);
            //
            // Choosefolder2
            //
            this.Choosefolder2.Location = new System.Drawing.Point(496,
213);
            this.Choosefolder2.Name = "Choosefolder2";
            this.Choosefolder2.Size = new System.Drawing.Size(100, 23);
            this.Choosefolder2.TabIndex = 15;
            this.Choosefolder2.Text = "Choose Folder";
            this.Choosefolder2.UseVisualStyleBackColor = true;
            this.Choosefolder2.Click += new
System.EventHandler(this.Choosefolder2_Click);
            //
            // test
            //
            this.test.Location = new System.Drawing.Point(379, 305);
            this.test.Name = "test";
            this.test.Size = new System.Drawing.Size(127, 23);
            this.test.TabIndex = 16;
            this.test.Text = "Test ELO security";
            this.test.UseVisualStyleBackColor = true;
            this.test.Click += new System.EventHandler(this.test_Click);
            //
            // listBox1
            //
            this.listBox1.FormattingEnabled = true;
            this.listBox1.HorizontalScrollbar = true;
            this.listBox1.Location = new System.Drawing.Point(34, 305);
            this.listBox1.Name = "listBox1";
            this.listBox1.Size = new System.Drawing.Size(339, 173);
            this.listBox1.TabIndex = 17;
            //
            // label6
            //
            this.label6.AutoSize = true;
            this.label6.Location = new System.Drawing.Point(31, 289);
            this.label6.Name = "label6";
            this.label6.Size = new System.Drawing.Size(93, 13);
            this.label6.TabIndex = 18;
            this.label6.Text = "Output from ELOS";
            //
            // Correct
            //
```

```
            this.Correct.Location = new System.Drawing.Point(380, 454);
            this.Correct.Name = "Correct";
            this.Correct.Size = new System.Drawing.Size(126, 23);
            this.Correct.TabIndex = 19;
            this.Correct.Text = "Correct ELO settings";
            this.Correct.UseVisualStyleBackColor = true;
            this.Correct.Visible = false;
            this.Correct.Click += new
System.EventHandler(this.Correct_Click);
            //
            // ELOS
            //
            this.AutoScaleDimensions = new System.Drawing.SizeF(6F, 13F);
            this.AutoScaleMode = System.Windows.Forms.AutoScaleMode.Font;
            this.ClientSize = new System.Drawing.Size(611, 550);
            this.Controls.Add(this.Correct);
            this.Controls.Add(this.label6);
            this.Controls.Add(this.listBox1);
            this.Controls.Add(this.test);
            this.Controls.Add(this.Choosefolder2);
            this.Controls.Add(this.Choosefolder1);
            this.Controls.Add(this.label5);
            this.Controls.Add(this.label4);
            this.Controls.Add(this.ELOGlobal);
            this.Controls.Add(this.ELOArchive);
            this.Controls.Add(this.label3);
            this.Controls.Add(this.label2);
            this.Controls.Add(this.ELOUser);
            this.Controls.Add(this.getUser);
            this.Controls.Add(this.getAdmin);
            this.Controls.Add(this.ELOAdmin);
            this.Controls.Add(this.getGroups);
            this.Controls.Add(this.ADGrouplist);
            this.Controls.Add(this.label1);
            this.Controls.Add(this.ADServer);
            this.Name = "ELOS";
            this.Text = "ELOS";
            this.ResumeLayout(false);
            this.PerformLayout();

        }

        #endregion

        private System.Windows.Forms.TextBox ADServer;
        private System.Windows.Forms.Label label1;
        private System.Windows.Forms.ListBox ADGrouplist;
        private System.Windows.Forms.Button getGroups;
        private System.Windows.Forms.TextBox ELOAdmin;
        private System.Windows.Forms.Button getAdmin;
        private System.Windows.Forms.Button getUser;
        private System.Windows.Forms.TextBox ELOUser;
        private System.Windows.Forms.Label label2;
        private System.Windows.Forms.Label label3;
        private System.Windows.Forms.TextBox ELOArchive;
        private System.Windows.Forms.TextBox ELOGlobal;
        private System.Windows.Forms.Label label4;
        private System.Windows.Forms.Label label5;
```

```
        private System.Windows.Forms.FolderBrowserDialog
folderBrowserDialog1;
        private System.Windows.Forms.Button Choosefolder1;
        private System.Windows.Forms.Button Choosefolder2;
        private System.Windows.Forms.Button test;
        private System.Windows.Forms.ListBox listBox1;
        private System.Windows.Forms.Label label6;
        private System.Windows.Forms.Button Correct;
    }
}
```

Resources.Designer.cs

```
namespace ELOS.Properties
{


    /// <summary>
    ///   A strongly-typed resource class, for looking up localized
strings, etc.
    /// </summary>
    // This class was auto-generated by the StronglyTypedResourceBuilder
    // class via a tool like ResGen or Visual Studio.
    // To add or remove a member, edit your .ResX file then rerun ResGen
    // with the /str option, or rebuild your VS project.

[global::System.CodeDom.Compiler.GeneratedCodeAttribute("System.Resources.T
ools.StronglyTypedResourceBuilder", "2.0.0.0")]
    [global::System.Diagnostics.DebuggerNonUserCodeAttribute()]
    [global::System.Runtime.CompilerServices.CompilerGeneratedAttribute()]
    internal class Resources
    {

        private static global::System.Resources.ResourceManager
resourceMan;

        private static global::System.Globalization.CultureInfo
resourceCulture;


[global::System.Diagnostics.CodeAnalysis.SuppressMessageAttribute("Microsof
t.Performance", "CA1811:AvoidUncalledPrivateCode")]
        internal Resources()
        {
        }

        /// <summary>
        ///   Returns the cached ResourceManager instance used by this
class.
        /// </summary>

[global::System.ComponentModel.EditorBrowsableAttribute(global::System.Comp
onentModel.EditorBrowsableState.Advanced)]
        internal static global::System.Resources.ResourceManager
ResourceManager
        {
            get
            {
                if ((resourceMan == null))
                {
                    global::System.Resources.ResourceManager temp = new
global::System.Resources.ResourceManager("ELOS.Properties.Resources",
typeof(Resources).Assembly);
                    resourceMan = temp;
                }
                return resourceMan;
            }
        }
```

```
        /// <summary>
        ///   Overrides the current thread's CurrentUICulture property for
all
        ///   resource lookups using this strongly typed resource class.
        /// </summary>

[global::System.ComponentModel.EditorBrowsableAttribute(global::System.Comp
onentModel.EditorBrowsableState.Advanced)]
        internal static global::System.Globalization.CultureInfo Culture
        {
            get
            {
                return resourceCulture;
            }
            set
            {
                resourceCulture = value;
            }
        }
    }
}
```

Settings.Designer.cs

```
namespace ELOS.Properties
{


    [global::System.Runtime.CompilerServices.CompilerGeneratedAttribute()]

[global::System.CodeDom.Compiler.GeneratedCodeAttribute("Microsoft.VisualSt
udio.Editors.SettingsDesigner.SettingsSingleFileGenerator", "8.0.0.0")]
    internal sealed partial class Settings :
global::System.Configuration.ApplicationSettingsBase
    {

        private static Settings defaultInstance =
((Settings)(global::System.Configuration.ApplicationSettingsBase.Synchroniz
ed(new Settings())));

        public static Settings Default
        {
            get
            {
                return defaultInstance;
            }
        }
    }
}
```

AssemblyInfo.cs

```
using System.Reflection;
using System.Runtime.CompilerServices;
using System.Runtime.InteropServices;

// General Information about an assembly is controlled through the
following
// set of attributes. Change these attribute values to modify the
information
// associated with an assembly.
[assembly: AssemblyTitle("ELOS")]
[assembly: AssemblyDescription("")]
[assembly: AssemblyConfiguration("")]
[assembly: AssemblyCompany("Lind")]
[assembly: AssemblyProduct("ELOS")]
[assembly: AssemblyCopyright("Copyright © Lind 2007")]
[assembly: AssemblyTrademark("")]
[assembly: AssemblyCulture("")]

// Setting ComVisible to false makes the types in this assembly not visible
// to COM components.  If you need to access a type in this assembly from
// COM, set the ComVisible attribute to true on that type.
[assembly: ComVisible(false)]

// The following GUID is for the ID of the typelib if this project is
exposed to COM
[assembly: Guid("23296c74-a23b-4917-a9c8-d3dfc4a053d9")]

// Version information for an assembly consists of the following four
values:
//
//      Major Version
//      Minor Version
//      Build Number
//      Revision
//
[assembly: AssemblyVersion("1.0.0.0")]
[assembly: AssemblyFileVersion("1.0.0.0")]
```

Appendiks B

Installation ELOprofssional 5.0 Server

(På tysk)

Dette appendiks indeholder en gennemgang af, hvordan man skal installere og opsætter ELO Professional 5´s serverdel.

Dauer dieser Unit

120 Minuten

Unit 1

Installation ELO*professional* 5.0 Server

In dieser Unterrichtseinheit lernen Sie

- Vorbereitungen vor der Installation.
- Installation und Konfiguration des Microsoft SQL Servers.
- Einrichten und Vorbereitung einer Datenbank
- Installation des **ELO***professional* Server Programms
- Registrierung des **ELO***professional* Server Dienstes
- Einrichten von NT Security
- Konfiguration der **ELO***professional* Server Einstellungen und Registry Einträge

Inhaltsverzeichnis

1 ELO*professional* Installation Vorbereitungen

1.1 Verteilung der Server

ELO*professional* kann mit allen Komponenten auf einen Server installiert werden, hier kommt es nicht gegenseitig zu irgendwelchen Störungen. Im anderen Extrem kann jeder ELO Dienst einen eigenen physikalischen Server erhalten. Wie diese Aufteilung im konkreten Projekt zu erfolgen hat wurde während der Projektierungsphase festgelegt und muss bei der Installation beachtet werden.

Beachten Sie bitte, dass bei einer Verteilung der ELO Server auf unterschiedliche Computer sichergestellt sein muss, dass sich alle Dienste untereinander ansprechen können und nicht durch Netzwerkeinschränkungen oder eine zu eng eingestellte Firewall getrennt werden dürfen. Insbesondere wenn Sie den Internet-Gateway vom Rest der Installation mit einer zusätzlichen Firewall trennen wollen, sollten Sie bedenken, dass Windows die NamedPipe Verbindungen über RPC realisiert.

1.2 Anwender und Gruppen einrichten

ELOprofessional benutzt die NT Security zum Schutz seiner Dokumente und Konfigurationsdateien. Aus diesem Grund müssen vor der Installation zwei Gruppen und ein Dienstkonto angelegt werden die dann von ELO verwendet werden können. Beachten Sie, dass Sie zum störungsfreien Betrieb ein Domänennetzwerk oder ein Active Directory Netzwerk benötigen. Andernfalls handeln Sie sich einen extrem erhöhten administrativen Aufwand ein.

- **EloAM** : Ein Domänen-Anwenderkonto welches als Dienstkonto für die ELO Serverkomponenten verwendet wird. Dieses Konto sollten Sie mit einem Passwort belegen und die Voreinstellung "Passwort läuft nie ab" aktivieren.

  Vorteile von Domänenanwendern und globaler Gruppe:
  - Module und Funktionsbausteine (Volltext, Internetgateway, etc...) von **ELO***professional* können auf das Netzwerk verteilt werden, nicht einzig nur auf dem **ELO***professional* Server.
  - Archivdateien bzw. Archivpfade können auf andere Rechner ausgelagert werden, bei Installation mit NT Security
  - Mit Administrationsrechten haben Sie überall im Netzwerk Zugriffsmöglichkeiten auf interne **ELO***professional* Systemdateien
- **GrpEloAdmin**: Ein globales Domänenkonto in das alle NT Anwender aufgenommen werden, die Vollzugriff auf ELO Dokumente benötigen. Auch Administratoren sollten keinen leichtfertigen Zugriff auf ELO Dokumente haben, daher sollte einzig das EloAM Konto und das Anwenderkonto, das die Datensicherungen übernimmt, hier aufgenommen werden. Falls ein Administrativer Zugriff auf die geschützten Bereiche notwendig wird, können Sie das entsprechende Konto bei Bedarf temporär in die GrpEloAdmin aufnehmen.
  Während der Installation muss auch das Konto unter dem installiert wird Mitglied in dieser Gruppe sein.
- **GrpEloUser**: Ein globales Domänenkonto in das alle NT Anwender aufgenommen werden die ELO Anwender sind. Hier sollten auch die Anwender aus der GrpEloAdmin nochmals mit aufgeführt werden.

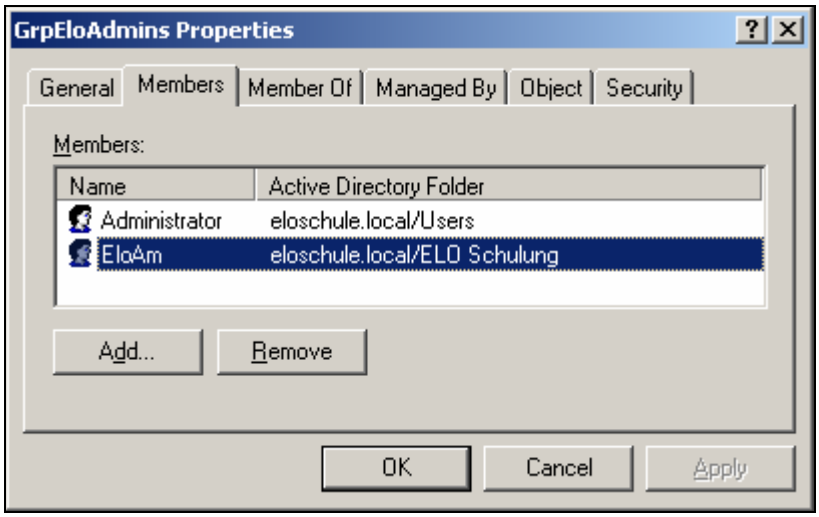

Bild 1: GrpEloAdmin Mitglieder

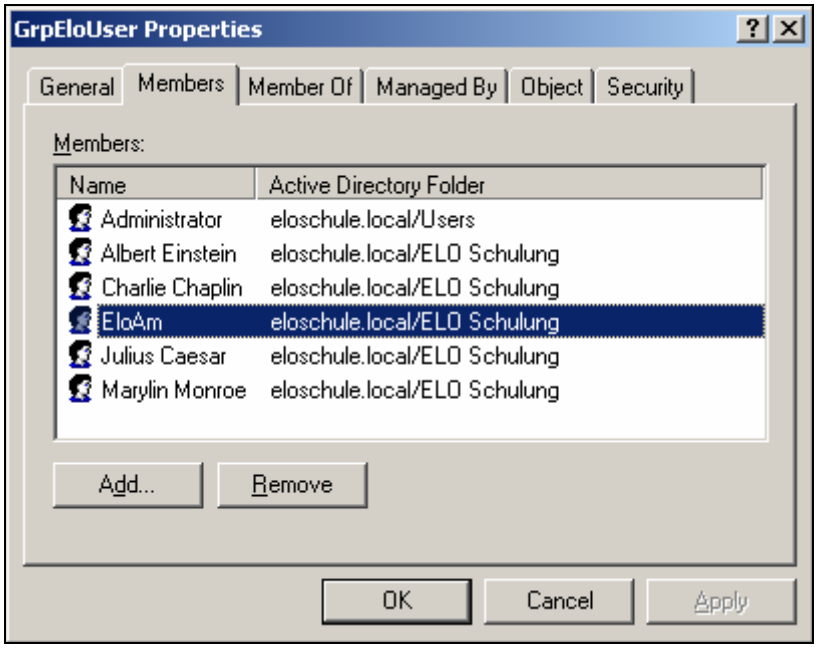

Bild 2: GrpEloUser Mitglieder

Merke:
Ab Windows XP brauchen Dienstkonten ein Passwort. Der Dienst startet nicht mit einem leeren Passwort

Hinweis:
Sie benötigen mindestens "lokale" Administrationsrechte zum Installieren von ***ELO***professional.

Sie benötigen Domänenadministrationsrechte zum Installieren von ***ELO***professional *mit NT Security*

1.3 Sicherheitsrichtlinien (security policy)

Folgende Anwenderrechte werden benötigt:

EloAm: "Als Dienst anmelden" – dieses Recht wird immer benötigt

EloAm: "Lokal anmelden" – wenn Sie das **ELO***professional* Internetgateway einsetzen an einem Domainencontroller. Das Windows Konto (wenn es kein Administrationskonto ist) der anonymen Anmeldung am IIS braucht zusätzlich das Recht der lokalen Anmeldung. Das haben an einem Domänencontroller nur die Administratoren.

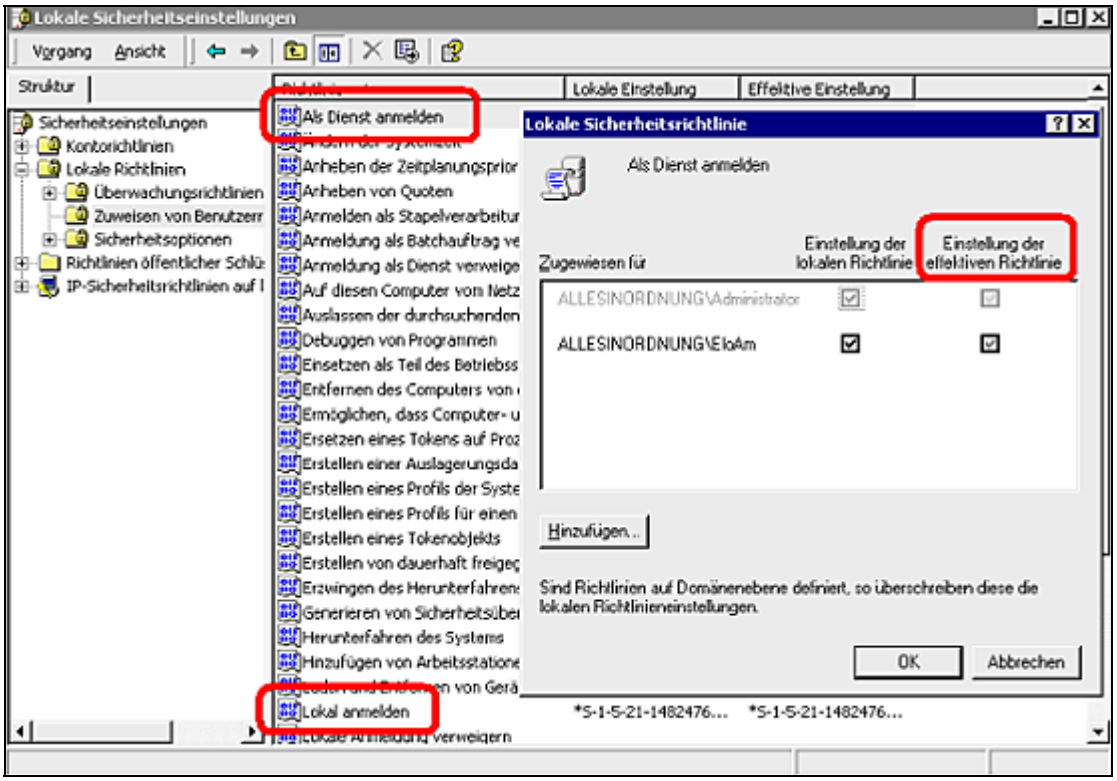

Bild 3: Benutzerrechte

Hinweis:
Achten Sie auf die "Einstellung der effektiven Richtlinie"! Domänenrichtlinien überlagern die lokalen Sicherheitseinstellungen. Wird ***ELO***professional *in einer Domäne auf einem "Nicht-Domänencontroller" (Mitgliedserver) installiert, so müssen Sie das Recht "Als Dienst anmelden" auch in den Sicherheitsrichtlinien für Domänen und Domänencontroller hinterlegen. Andernfalls starten die ELO Dienste nicht mehr nach einem Neustart.*

Hinweis:
Das Recht "lokale Anmeldung" soll nur gesetzt werden, wenn das Internetgateway auf einem Domänencontroller installiert wird (unüblich). Hinterlegen Sie das nur in der Richtlinie für Domänencontroller. Sollten Sie fälschlicherweise das Recht in der Richtlinie für die Domäne hinterlegen einzig für das Konto EloAm, dann kann sich anschliessend kein normaler Anwender mehr in der Domäne anmelden!

1.4 Windows 2003 Vorbereitung

Wenn Sie **ELO***professional* auf einem Windows 2003 Server installieren wollen, dann sollten Sie das Verzeichnis "ELOprof" vorher manuell anlegen und mit den richtigen Berechtigungen ausstatten, weil ab Windows 2003 nur noch Administratoren per Default Vollzugriff auf neu erstellte Objekte haben.

Der ELO Dienst unter dem Konto "EloAm" hat normalerweise keine Administrationsberechtigungen, und damit hat er keinen Vollzugriff auf die beim Setup erstellten Verzeichnisse. Der ELO Server Dienst mit dem Konto "EloAm" wird nicht starten können, wenn er keinen Vollzugriff auf "seine" Verzeichnisse bekommt.

- Erstellen Sie das Verzeichnis ELOprof von Hand und geben Sie Vollzugriff für die Gruppe GrpEloAdmin und lesenden/ausführenden Zugriff für die Gruppe GrpEloUser

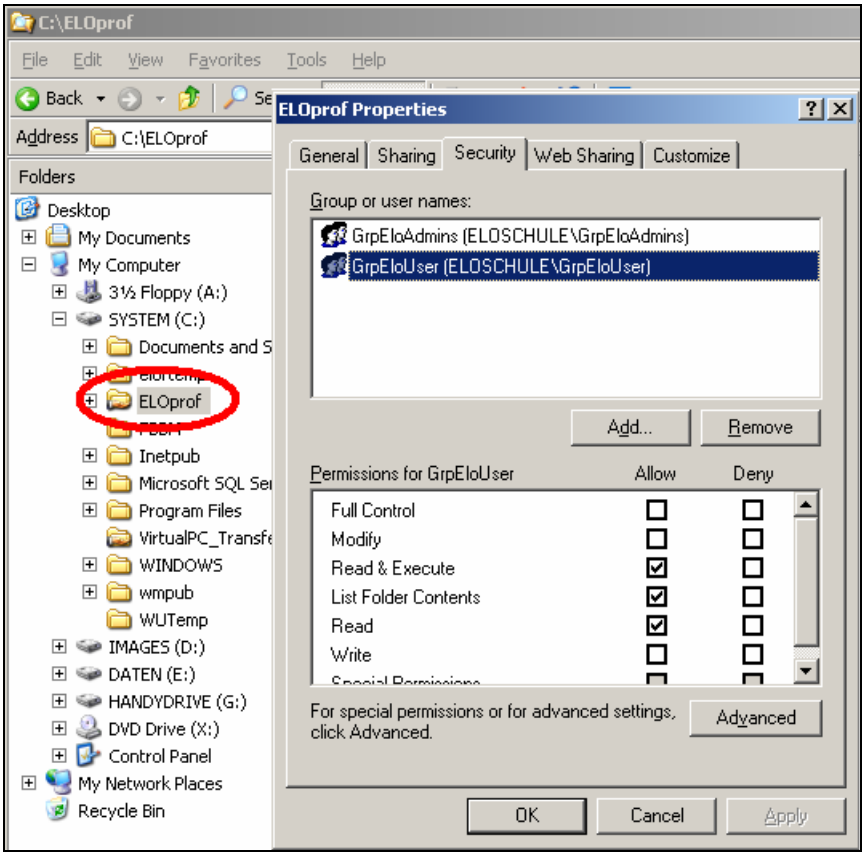

Bild 4: Vollzugriff GrpEloAdmin und lesender Zugrif für GrpEloUser auf das ELOprof Wurzel-Verzeichnis

Hinweis:
Diese oben angegebene Berechtigungsempfehlung ist nur eine von vielen Möglichkeiten. Es obliegt Ihnen im weiteren Verlauf der Installation und bei Installation von Modulen auf die dort jeweils benötigten NT-Security Einstellungen zu achten, um korrektes und sicheres Funktionieren zu gewährleisten

Merke:
Wenn Sie einem Windows Verzeichnis Rechte entzogen oder hinzugefügt haben, weiss das das angemeldete Konto erst nach einem Neu-Anmelden in Windows!

1.5 Grobstruktur der ELO*professional* Datenbanken und Archivdaten

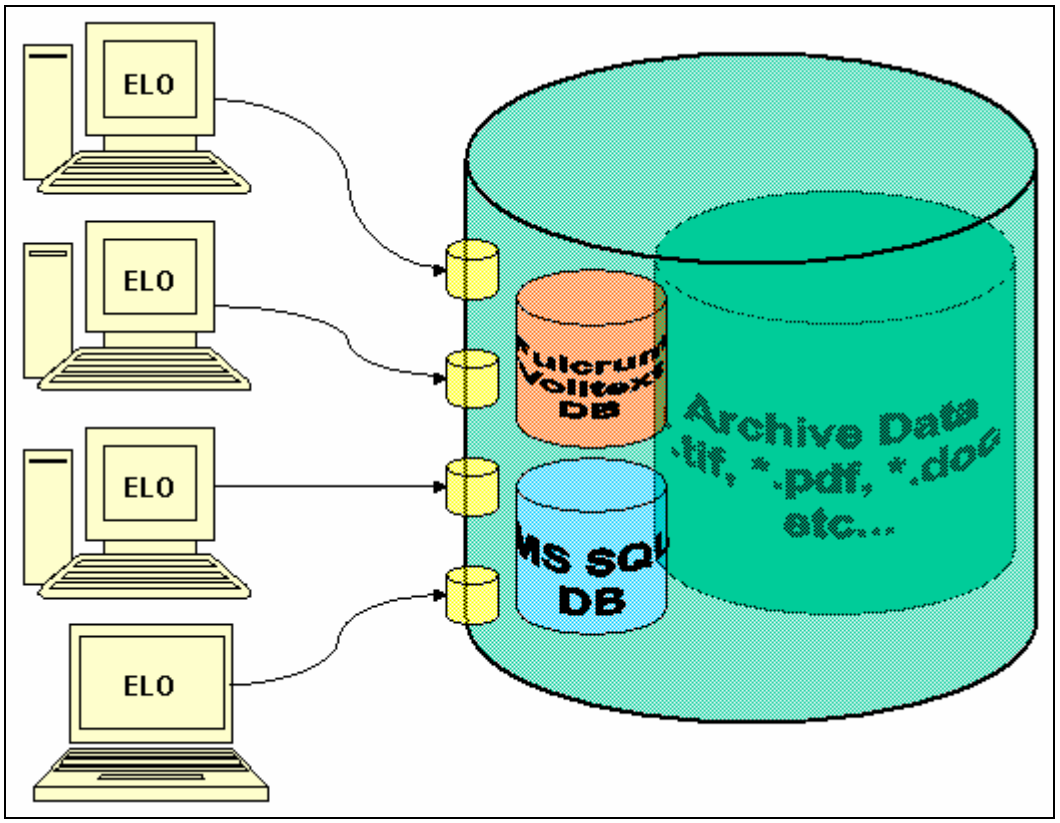

*Bild 5: **ELO**professional Grobstruktur – persönliche Postboxen, Datenbanken und Dokumentenpool*

1.6 Checkliste und Passwortliste verwenden

Verwenden Sie für jede Installation immer die aktuellen Checklisten aus dem Internet!

Merke:
Die Checklisten helfen Wichtiges nicht zu übersehen, sind eine Art Leistungsnachweis, lassen Entscheidungen leichter nachvollziehen und extrem hilfreich, wenn die Verantwortlichkeiten wechseln im Verlauf eines Projektes!

1.7 Microsoft Office Sicherheitseinstellungen

Hinweis:
Überprüfen Sie vor jeder manuellen Client Installation die Sicherheitseinstellung aller MSoffice Produkte (Word, Excel, Powerpoint...). Wir können bis einschliesslich MS Office 2003 die ELO Makros immer installieren, auch entgegen der Microsoft Sicherheitseinstellungen. Aber funktionieren tun die Makros ab MS Office 2003 nur, wenn nicht die höchste Sicherheitsstufe eingestellt ist.

2 MS SQL Server Installation

Vor der Installation kontrollieren Sie bitte ob Sie den von der aktuellen Serverversion geforderten Stand im Bezug auf Service Packs und zusätzliche Komponenten erreicht haben.

- Windows NT 4.0: mindestens erforderlich ist das Service Pack 4 und der Internet Explorer 4, Service Pack 1.
- Windows 2003 Server: mindestens erforderlich ist für den MS SQL 2000 das Service Pack 3

Merke:

Der SQL Server 7.0 ist nicht mehr verwendbar auf einem Windows 2003 Server. Er bringt das Active Directory zum Stillstand.

Hinweis:
Kontrollieren Sie sorgfältig, ob Sie eine Vollversion oder eine 120 Tage Testversion installieren. Eine MS SQL Testversion kann später nur über den Umweg der Deinstallation und Neuinstallation zur Vollversion gemacht werden.

2.1 Performance Tuning

Trennung von Datenbank und ELO Dokumenten

- Bei identischen Rahmenbedingungen bringt eine Auftrennung der Datenbank und der Dokumentenablage auf unterschiedliche Festplatten gegenüber der Speicherung auf einer gemeinsamen Festplatte in unserer ELO-Testumgebung ein Geschwindigkeitsvorteil von 50%. Dieses Ergebnis bestärkt unseren Projektierungsvorschlag, dass die Datenbank ein eigenes Medium (normale Festplatte oder RAID 1) erhalten sollte.

2.2 Installation Komponenten MS SQL 2005

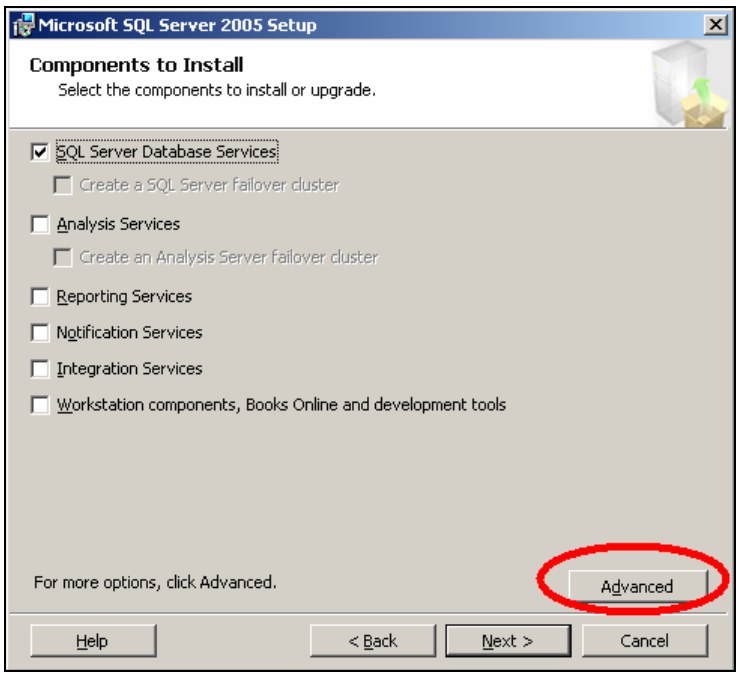

Bild 6: Schaltfläche "Advanced" für zusätzliche zu installierende Komponenten und Installations Pfad

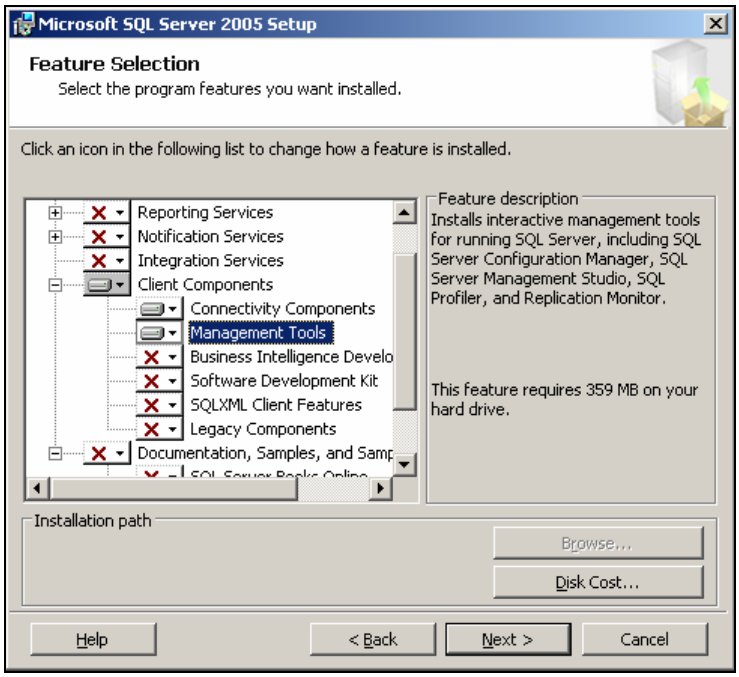

Bild 7: Installations Pfad und Detailbeschreibung der Komponenten

- Connectivity Components: "Installs components for communication between clients and servers, including network libraries for ODBC and OLE DB."
- Management Tools: "Installs interactive management tools for running SQL Server, including SQL Server Configuration Manager, SQL Server Management Studio, SQL Proviler, and Replication Monitor."

2.3 Anmeldekonto für Start des MS SQL Dienstes

Der Microsoft SQL Server wird per default unter dem System Dienstkonto (local system account) installiert. Das ist prinzipiell auch akzeptabel. Wenn Sie es selbst entscheiden können, empfehlen wir für das Starten des MS SQL Dienstes ein eigenes "nicht-Administrationskonto" zu verwenden. Idealerweise das Konto EloAm.

Zwei Wege bieten sich hier an:

1) Der SQL Server wird unter dem EloAM Konto installiert. Er gehört dann zur GrpEloAdmin und besitzt Vollzugriff auf das Archivdataverzeichnis.

2) Falls der SQL Server bereits installiert ist oder das MS SQL Dienste-Konto nicht geändert werden soll, empfehlen wir Ihnen die ELO Archivdatenbank in das Standard Datenbankverzeichnis des SQL Servers zu legen. Dort wo der SQL Server seine Master Datenbank hat (master.mdf).

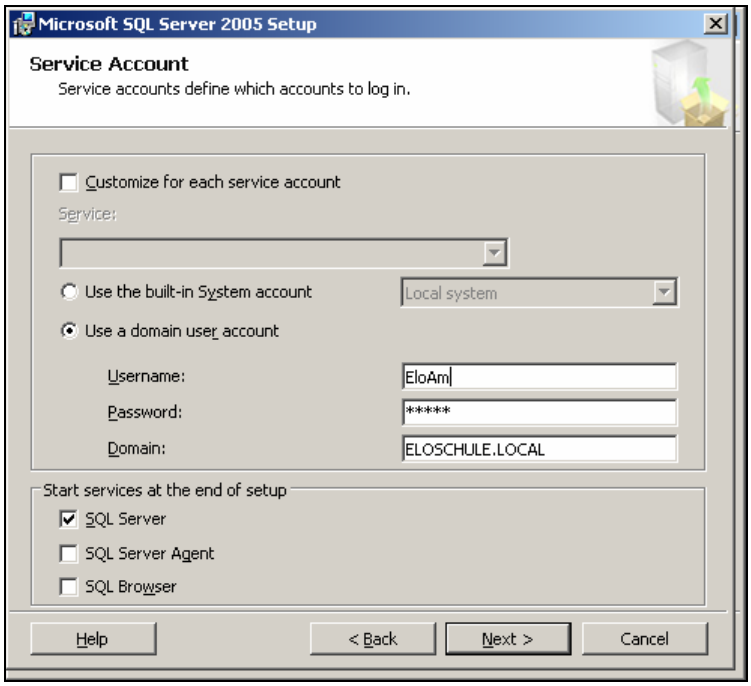

Bild 8: Anmeldekonto des MS SQL Dienstes

2.4 Authentifizierungsmodus (MS SQL2005)

Wählen Sie bei der Installation den Authentifizierungsmodus "Gemischter Modus" Modus (Windows-Authentifizierung und SQL Server-Authentifizierung), ansonsten lässt sich später die "EloDB" Anmeldung nicht korrekt einrichten.

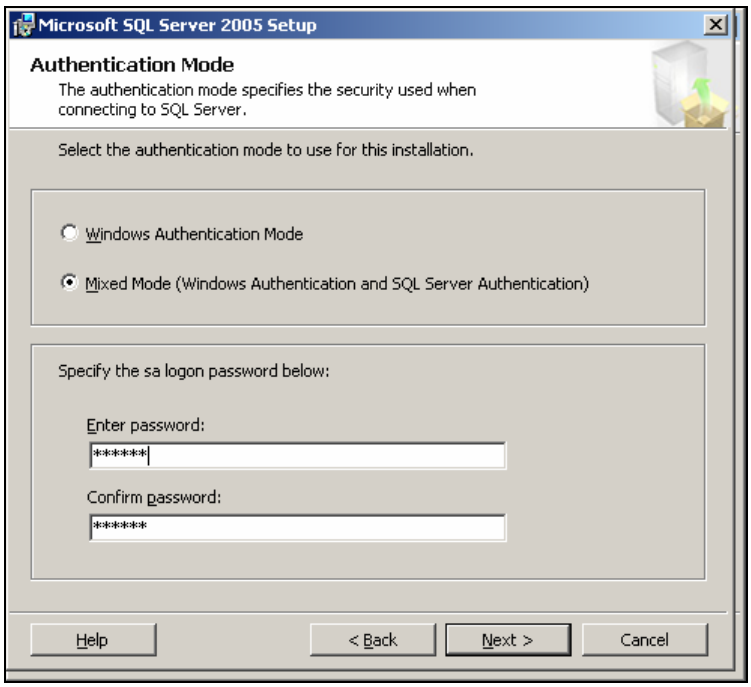

Bild 9: Gemischter Modus

Hinweis:
Die Verwendung der "SQL Server Authentifizierung" ist ein zusätzliches Sicherheitsplus. Kein Windows Anwender kann sich per ODBC mit der Datenbank ohne ELO verbinden, es sei denn er kennt Anwender und Passwort für die Datenbank.

2.5 MS SQL Anwender EloDb anlegen

MS SQL User EloDb für den Zugriff auf ELO Datenbanken anlegen und mit einem Passwort versehen.

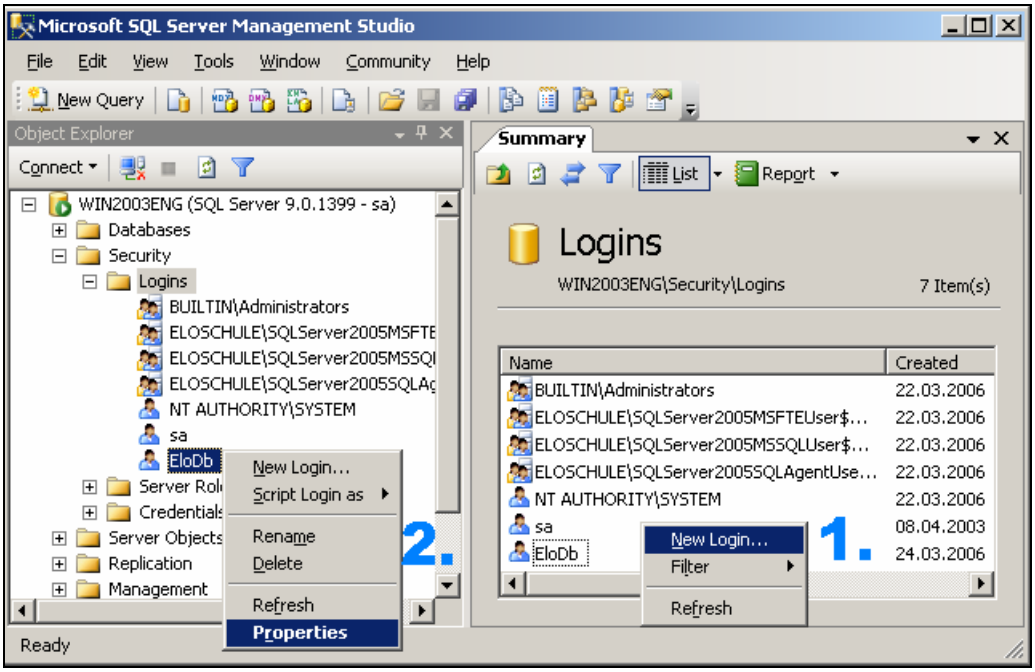

Bild 10 MS SQL Server Management Studio

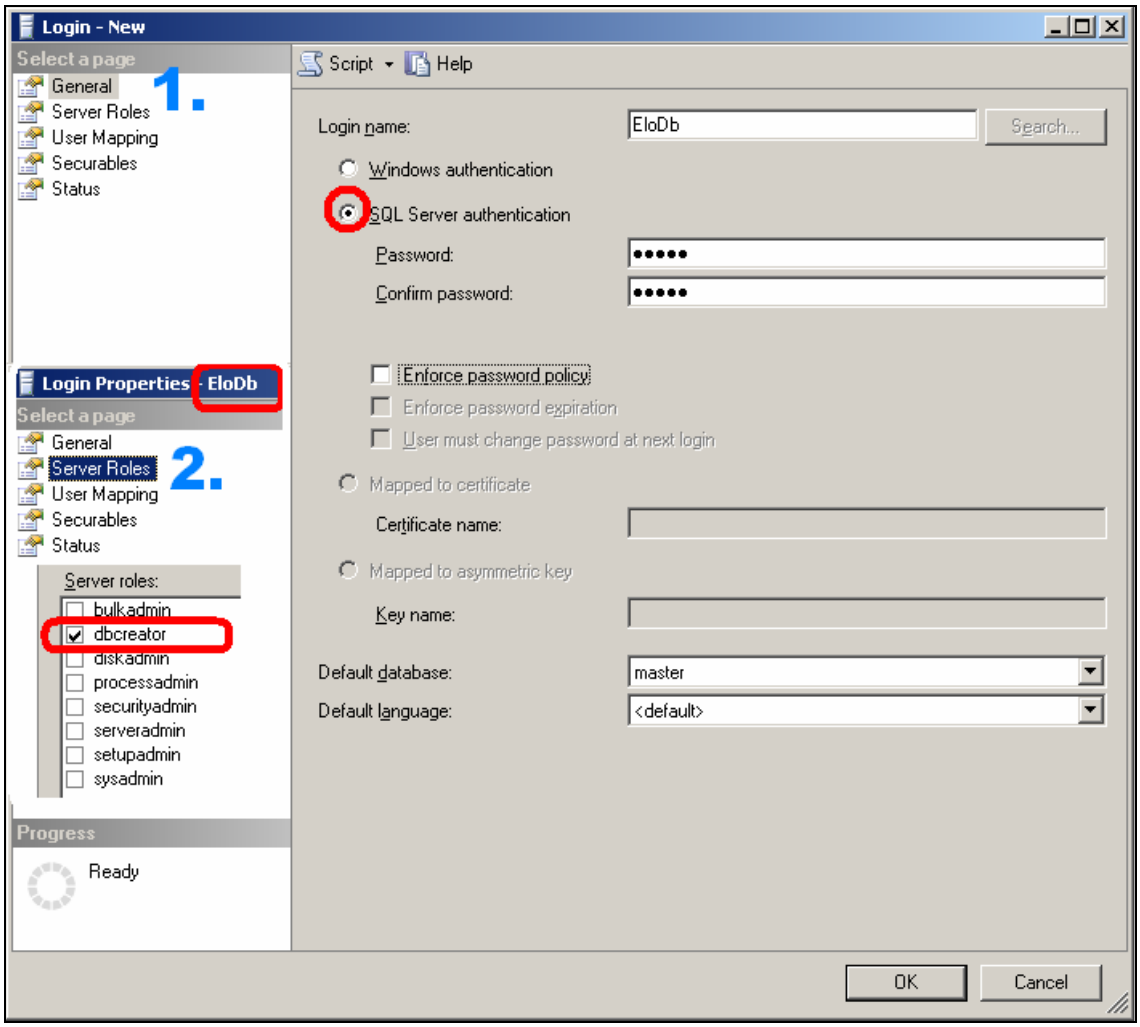

Bild 11: Anlegen des MS SQL Datenbank Anwenders EloDb

Teilen Sie dem EloDB Anwender einzig das Recht "Database Creators" zu. Wenn Sie das vergessen können Sie keine ELO Archive anlegen.

Merke:
Vergeben Sie auch dem Datenbankanwender Administrator "sa" ein Passwort!

3 ELO*professional* Server Installation

3.1 Sprachversion

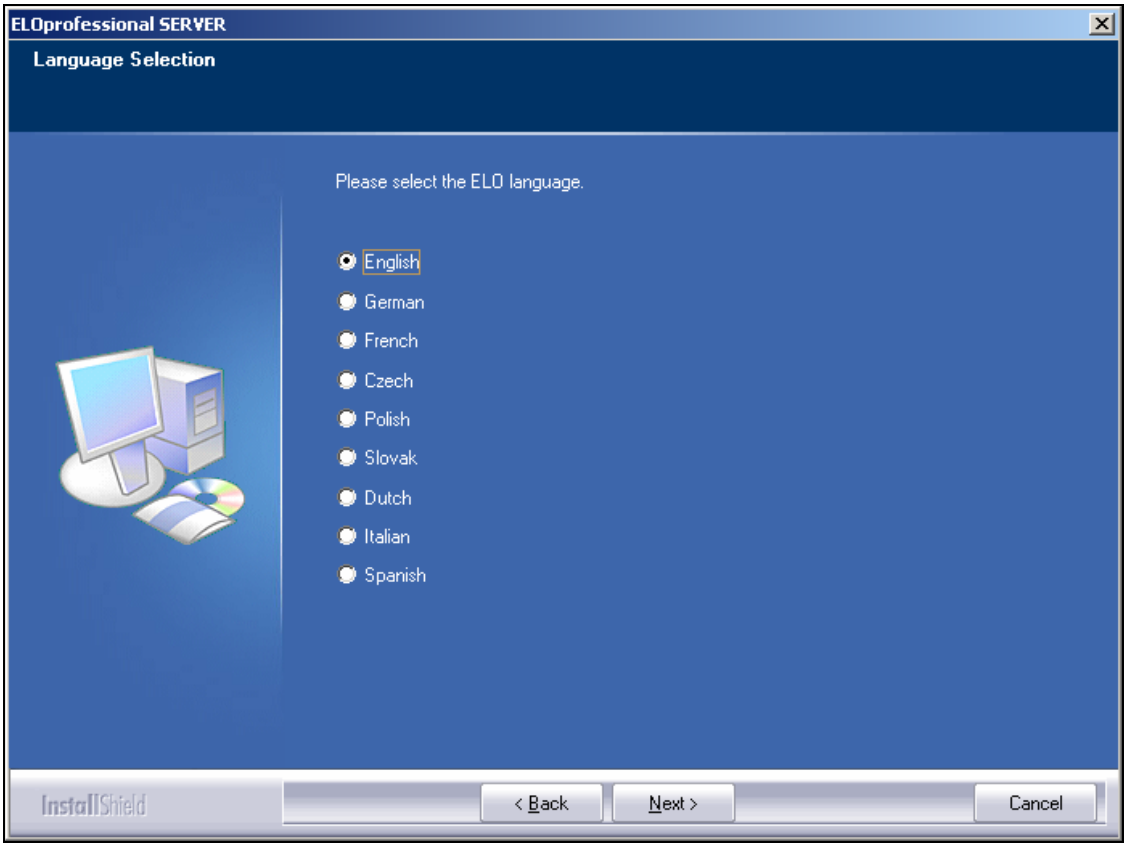

Bild 12: zu diesen Sprachen existieren Serverdateien.

Hier wählen Sie die Sprachversion Ihrer künftigen ELO-Installation aus. Allerdings ist die Menüsprache von ELO Server Komponenten immer Englisch, egal was Sie hier konfigurieren.

Die auswählbare Sprache bezieht sich auf die EloMdb*.TXT Datei, deren Auswirkung sich bemerkbar macht in:

- Benamung der ELO Schriftfarben
- Benamung der ELO Ablagemasken
- Benamung der ELO Projekte und Aktivitäten
- U.a. wie z.B. "standard Workflow" etc...

Weiter auf die Datei "Syslog.esp" mit Auswirkung auf:

- Benamung "Systemschlüssel"
- Benamung Default User und Gruppen

Hinweis:
*Wenn Sie den **ELO**professional Client in einer dieser Sprachen installieren wollen, dass müssen Sie momentan noch sicherstellen, dass Sie eine dieser Landesprache entsprechende Installations CD einsetzen*

3.2 Server Installation

Die gesamten **ELO***professional* Programme einschliesslich der Archivdaten werden normalerweise anfangs in ein Verzeichniszweig installiert. Wir raten nicht dazu davon abzuweichen. Falls das aus irgendwelchen Gründen doch einmal notwendig wird müssen Sie die benötigten Netzwerkfreigaben vor der Installation manuell erzeugen.

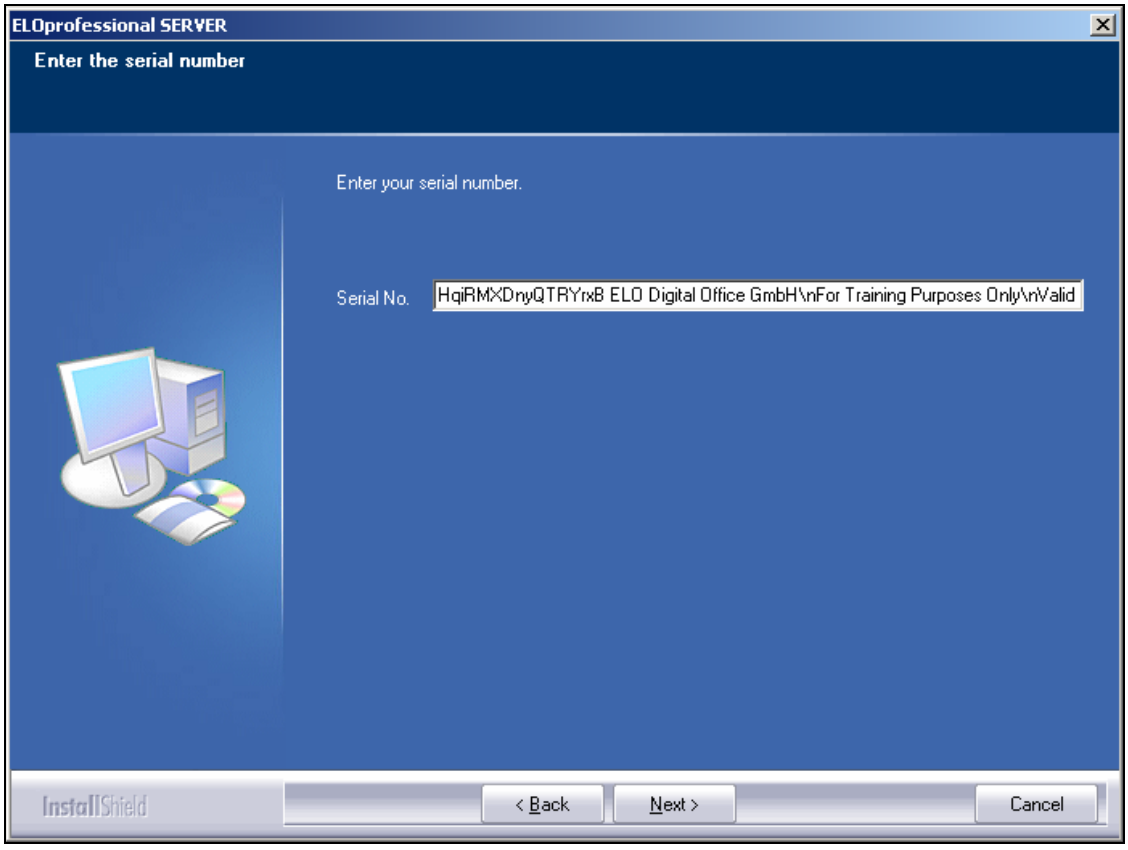

Bild 13: Eingabe Ihrer persönlichen Seriennummer

Zum Begin der Installation wird die Seriennummer abgefragt. Sie erhalten diese Normalerweise mit der Bestellung per Email. Beachten Sie bitte, dass diese Nummern personalisiert sind. Zur Bestellung geben Sie den Kundennamen und Ort an. Sie erhalten dann zu diesen Angaben eine Seriennummer, die auch nur für diesen Kunden gültig ist. In der Seriennummerneingabe müssen Sie deshalb auch den kompletten Eintrag incl. Name und Ort angeben, andernfalls wird die Nummer ungültig. In diesem Fall wird der AccessManager nicht starten und Sie finden im AccessManager Report einen Hinweis auf eine ungültige Seriennummer.

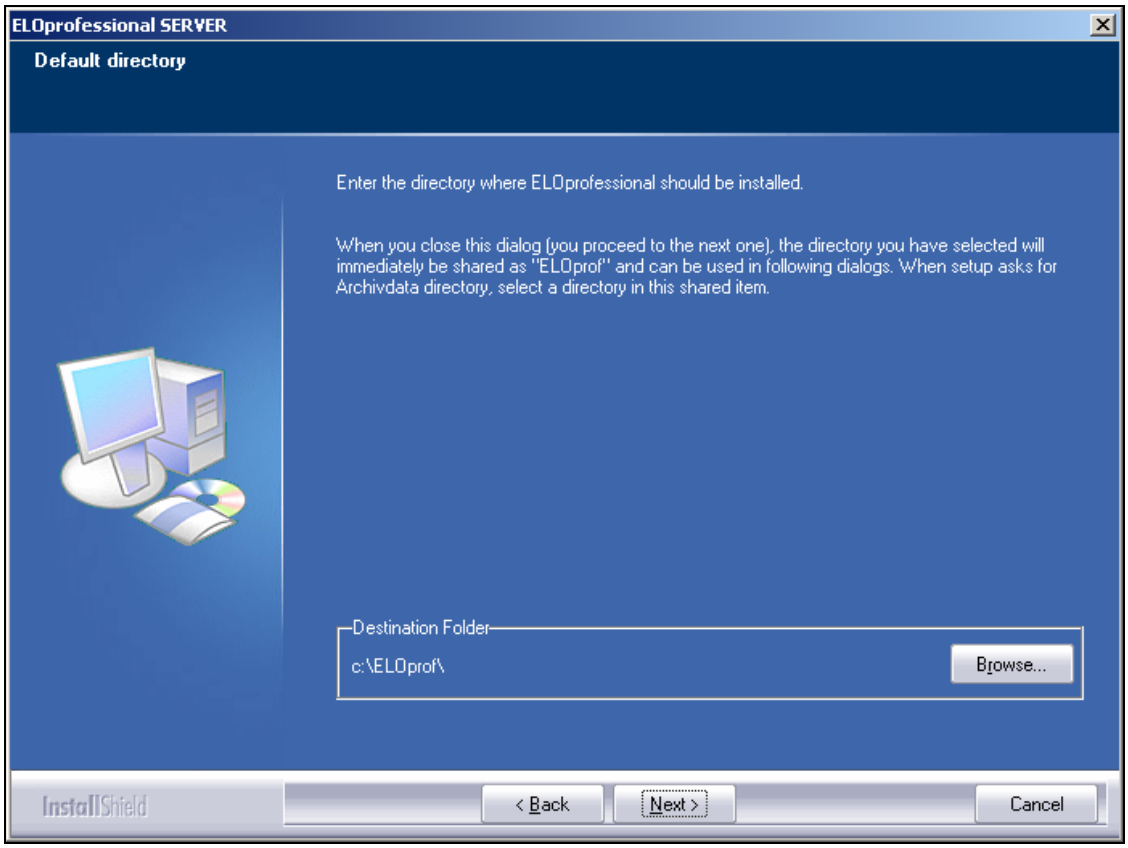

Bild 14: ELO Installationsverzeichnis

Unterhalb dieses "Standard-Installationsverzeichnisses" wird das Setup die komplette ELO Installation ablegen. Auch die Netzwerkfreigabe hierzu wird automatisch erzeugt werden. Auch wenn die folgenden Dialog ein einigen Stellen die Möglichkeit geben hiervon abzuweichen, sollten Sie im Normalfall bei den vorgeschlagenen Werten bleiben.

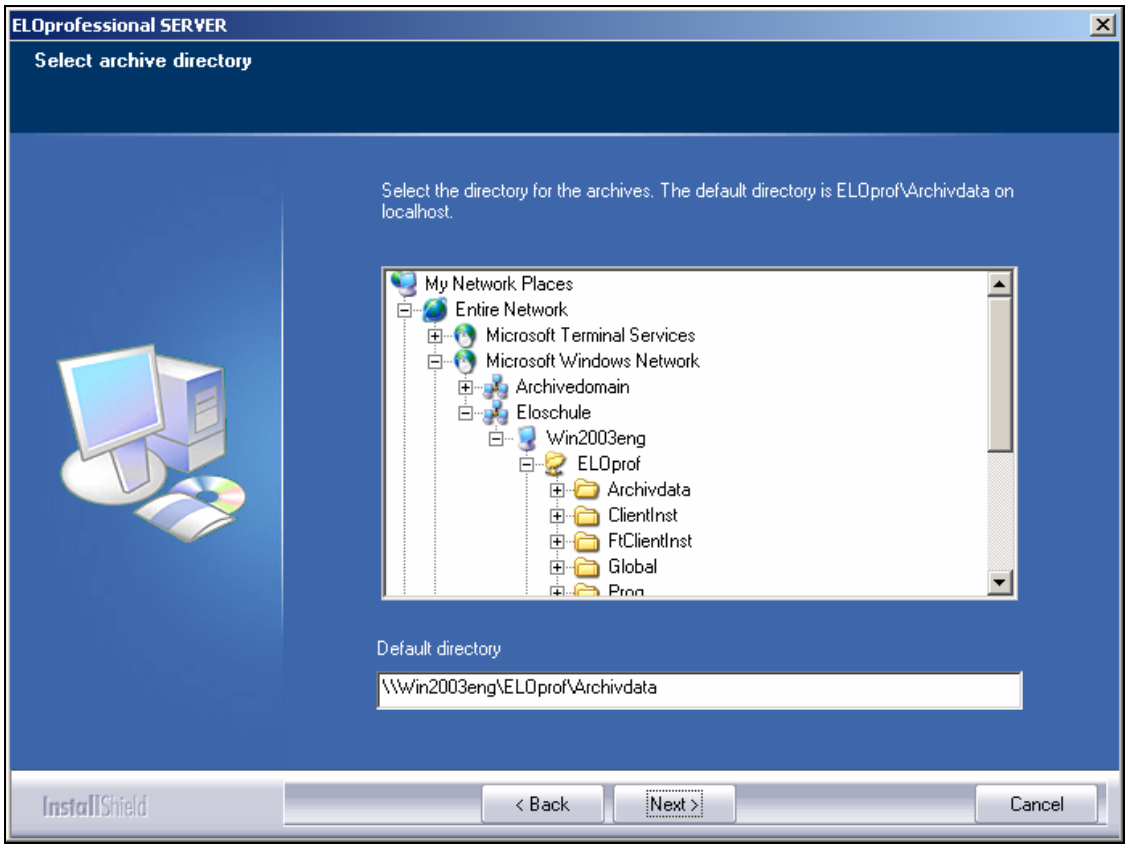

Bild 15: ELO Archiv Verzeichnis

Zu diesem Verzeichnis hat das Setup Programm nun eine Netzwerkfreigabe erzeugt. Diesen Wert sollten Sie unverändert akzeptieren. Wenn Sie hier einen anderen Wert benötigen, müssen Sie die dazu passende Freigabe manuell anlegen.

Hinweis:
Legen Sie das Verzeichnis Archivdata dort hin, wo auch der ELO Server Dienst installiert ist. Dokumente können später besser über Dokumentenpfade im gesamten Netzwerk gestreut werden.

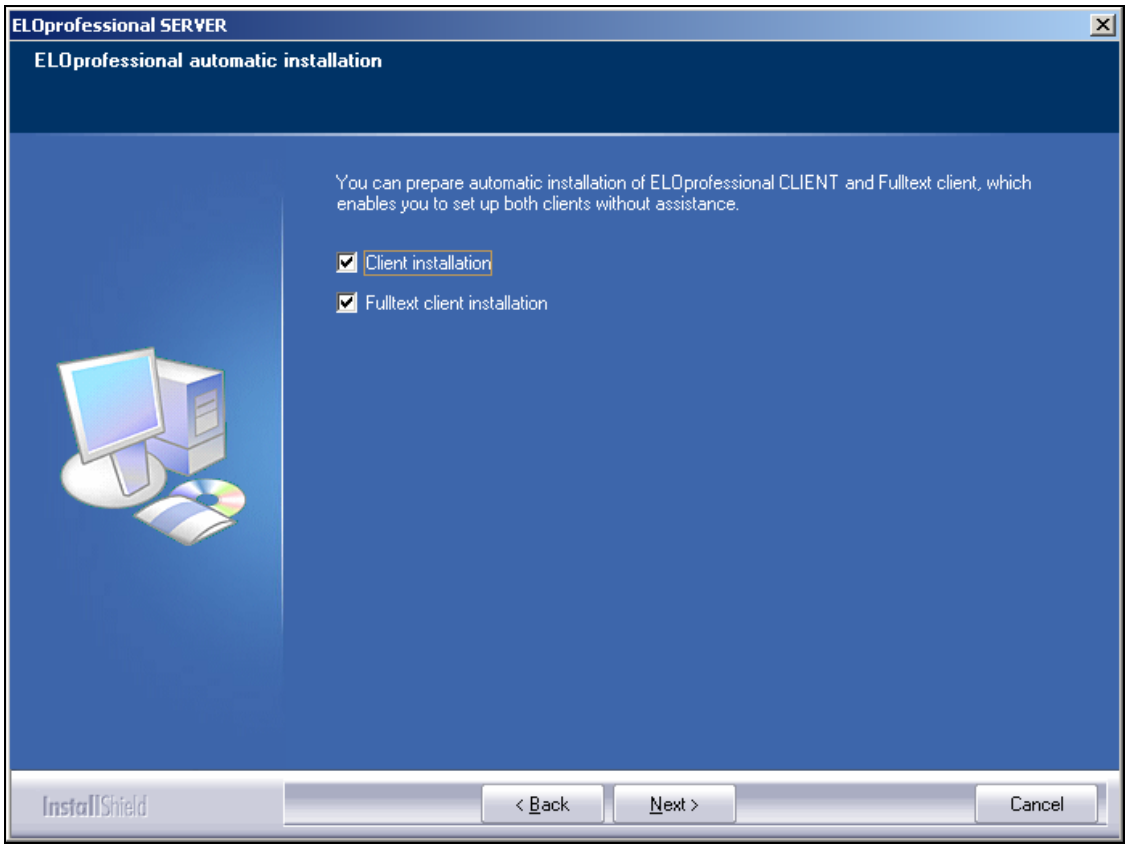

Bild 16: Verzeichnisse erstellen für automatisches Client Setup

Sie können auf dem Server ein vorbereitetes Image für die Client Installation hinterlegen. Das ermöglicht dann auf dem Client eine automatische Installation ohne CD und weitere Benutzereingaben. Falls Sie dieses Image nicht wünschen entfernen Sie die beiden oben aufgeführten Optionen.

Zur Client Installation das Setup Programm im Ordner "ClientInst" des Freigabe-Verzeichnisses ELOprof von einem Client aus ausführen.

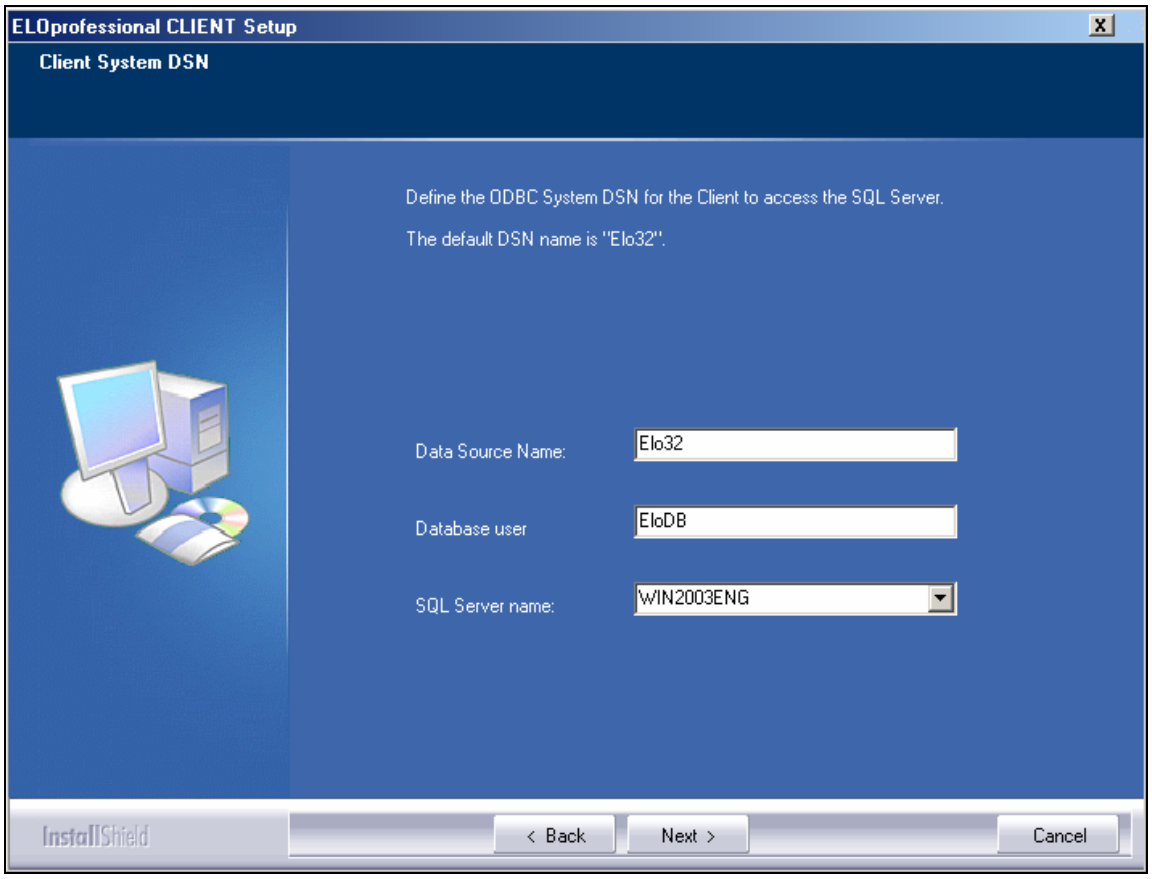

Bild 17: System DSN zur Archivdatenbank einrichten

Im folgenden werden die Standardparameter für die Client Installation eingegeben:

- Data Source Name : ist immer Elo32, diesen Eintrag sollten Sie unverändert lassen.
- Datenbank-Anwender: normalerweise EloDB. Hier geben Sie den Anwender ein den Sie zuvor im Enterprise Manager für den ELO Zugriff eingerichtet haben.
- SQL-Servername: Hier geben Sie den Computernamen des SQL Servers an.

3.3 Server Konfiguration

Hinweis:
Jede Änderung an einer AccessManager Option erfordert einen Neustart des AccessManager Dienstes! Erst danach ist die Änderung wirksam.

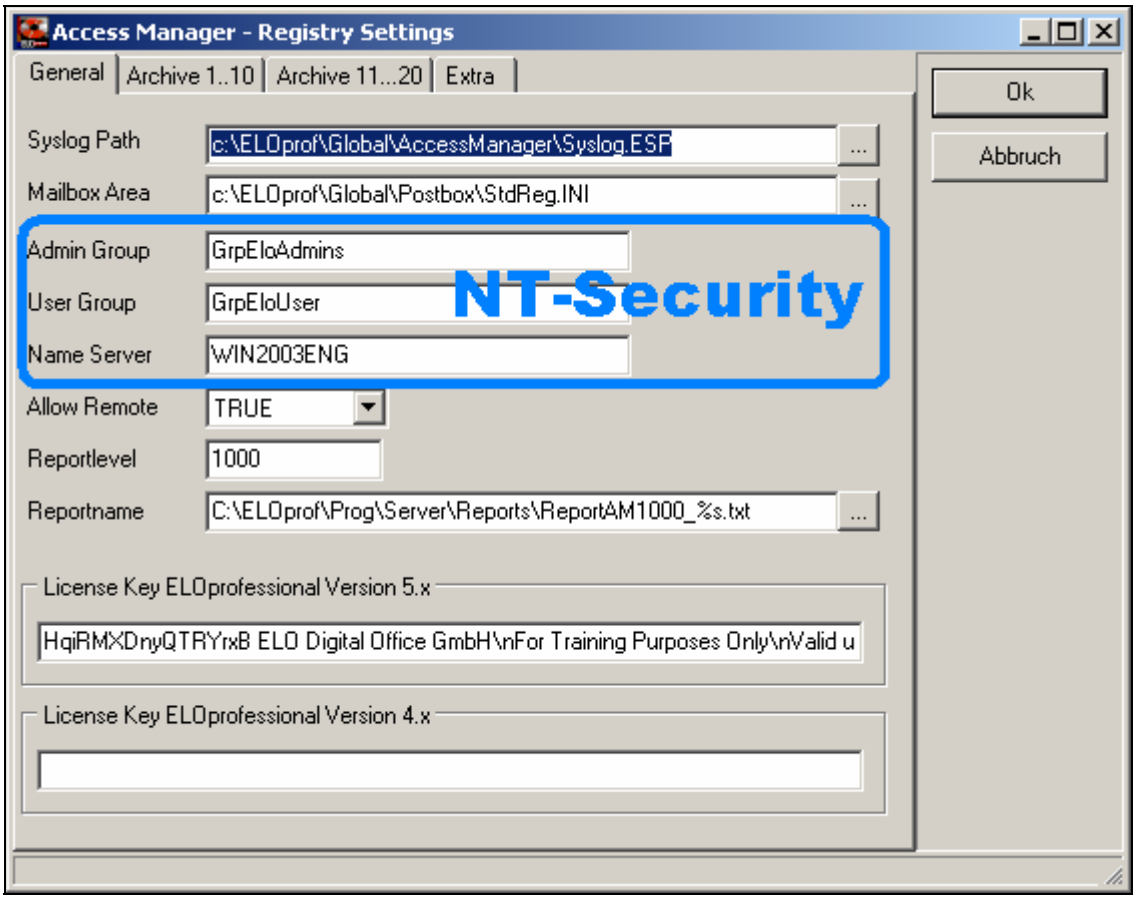

Bild 18: AccessManager Optionen - Konfiguration von NT-Security

Hinweis:
wenn Sie kein Domänennetzwerk betreiben oder aus anderen Gründen auf die NT Security verzichten wollen, dann lassen Sie die Felder "Admin Gruppe", "Anwendergruppe" und "Namensserver" leer. Beachten Sie bitte, dass ELO dann keinerlei Dokumentenschutz einrichten kann.

- "SYSLOG Path" nicht verändern.
- "Mailbox Area" sollte auf einen Netzwerkspfad (UNC Schreibweise) umgesetzt werden, insbesondere wenn **ELO***mobile*, **ELO***replikation* oder das Internetgateway zum Einsatz kommen. Lassen Sie sich nicht daran stören, dass es ab **ELO***professional* 5.0 keine Datei StdReg.INI mehr in diesem Verzeichnis gibt. Es kommt einzig und allein auf den UNC Pfad am Anfang dieser Zeile an!

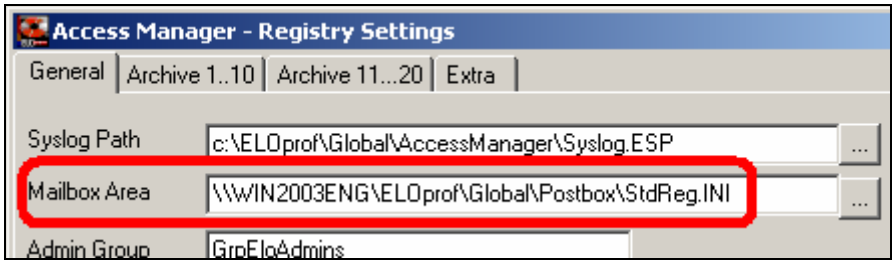

Bild 19

- NT Security Option "Admin Group": die Windows NT Gruppe GrpEloAdmin eintragen
  - In diese Gruppe kommen alle Windows Domänenbenutzer hinein, die Zugriff auf die Dokumente im Dateisystem haben. Normalerweise wären das der Anwender EloAm und der Datensicherungsaccount. Während der Installation kann auch noch der Domänenadministrator aufgenommen werden, damit wenigstens die vom ELO Accessmanager eingestellten Berechtigungen überprüft werden können.
- NT Security Option "User Group": die Windows NT Gruppe GrpEloUser eintragen.
  - In diese Gruppe kommen alle Windows Domänenbenutzer hinein, die mit ELO arbeiten können sollen. Nur diese Anwender haben Zugriff auf ELO Systemdateien im Netzwerk
- NT Security Option "Name Server": Namensserver , der die NT Domänenbenutzerdatenbank enthält (i.d.R. PDC)
  - Der ELO Accessmanager benötigt einen Rechnernamen, an dem er die NT Domänenbenutzer security-seitig identifizieren kann (SID). Im Idealfall ist dies der Domänencontroller (PDC).
  - Als Namensserver setzen Sie normalerweise den PDC Ihrer Domäne an. Falls das nicht möglich ist können Sie auch den lokalen Rechnernamen einsetzen. In diesem Fall sind aber ein paar Besonderheiten in der Namensauflösung in NT Netzwerken zu beachten die zu Funktionseinschränkungen beim ELO Administrator Anwender führen können. Da bei einer lokalen Namensauflösung die lokalen Anwender eine höhere Priorität besitzen als die Domänenanwender, wird das Administrator Konto und alle Domänen Konten zu denen es einen gleichnamigen lokalen Anwender gibt, überdeckt. Sie können das zwar manuell in der Anwenderkonfiguration (siehe Client Handbuch) korrigieren, haben aber einen erhöhten administrativen Aufwand.
- "Allow Remote" auf TRUE
  - Damit kann mit ELO Administrationsrechten von jedem ELO Client im Netzwerk der Reportlevel und der Reportdateiname temporär geändert werden, bis zum nächsten Neustart des Accessmanagers.
  - Änderungen am Reportlevel werden sofort berücksichtigt, es ist kein Neustart des Accessmanager-Dienstes notwendig
- "Reportlevel" auf 1000 – während der weiteren Installation. Nach erfolgreicher Beendigung der gesamten ELO Installation wieder auf "10" zurückstellen!
  - Reportlevel 10: Standardeinstellung für den normalen Betrieb
  - Reportlevel 1000: Im konkreten Fehlerfall, um die Ursache ausführlich zu protokollieren und ggf. diesen Report zum ELO-Digital Support zu schicken. Kein Dauerbetrieb mit Reportlevel 1000! Das drückt sehr stark auf die Performance und erzeugt in kürzester Zeit eine sehr grosse Datei – die dann wiederum selbst zu Fehlern führen kann.
- Den Lizenzschlüssel sollten Sie unverändert lassen. Lediglich wenn Sie sich im Setup Programm vertippt haben oder nach einer Funktionserweiterung von uns einen neuen Schlüssel erhalten, sollten Sie hier eingreifen.

3.3.1 Accessmanager Report

Der AccessManager kann ab Server Version 3.368 (22.Juli 2002) so konfiguriert werden, dass er automatisch jeden Tag eine neue Reportdatei anfängt. In dieser Betriebsart sollten Sie natürlich ein eigenes Verzeichnis für die Reportdateien vorsehen. Eingericht wird dieses indem Sie im Reportdateinamen ein %s angeben (das s bitte klein schreiben, sonst wird es nicht erkannt), also z.B. Das Zielverzeichnis müssen Sie vorher anlegen, ELO erzeugt es nicht selber.

Bild 20: Report Datei - für jeden Tag eine eigene

3.4 Archive einrichten

Unter den Archive-Registertabs können Sie die AccessManager Archive einrichten. Änderungen an dieser Stelle werden erst nach einem Neustart des AccessManagers aktiv. Sie können bis zu 20 Archive anlegen.

Als Vorgabe wird immer ein "Archiv1" eingerichtet. Im Normalfall sollten Sie diesen Namen gegen einen "sprechenden" Namen austauschen, bevor Sie den AccessManager zum ersten Mal starten.

Sie können die Archive sowohl mit UNC-Pfad wie auch mit einer Laufwerkskennung eintragen. Da dieser Pfad beim Erzeugen des Archivs auch gleich als Vorschlagswert für den Basispfad verwendet wird, hat ein UNC-Pfad den Vorteil, dass gleich ein gültiger Basispfad generiert wird. Allerdings hat der UNC-Pfad auch den Nachteil, dass der AccessManager bei Netzwerkstörungen die Verbindung zu seinen Archivdateien verliert und der Dienst neu gestartet werden muss. Aus diesem Grund ist die Verwendung von Laufwerksbasierenden Pfaden zu den Archiven zuverlässiger. Sie müssen in diesem Fall dann aber anschließend im Client unter „Systemverwaltung“ – „Dokumentenpfade“ den Basispfad auf einen UNC-Pfad umstellen oder mit geschützten Pfaden arbeiten (in diesem Fall greift der Client niemals auf den Archivdata-Bereich zu, die Dokumente werden vom AccessManager aktiv an den Client übertragen).

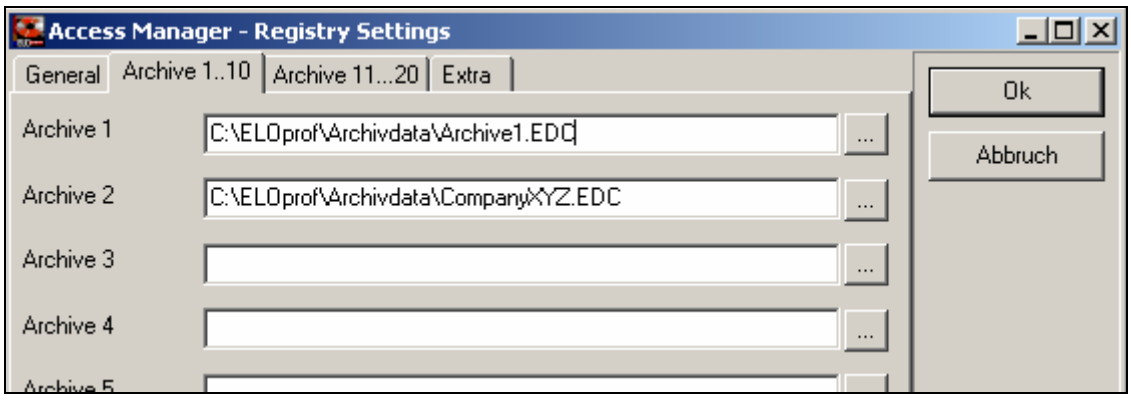

Bild 21: für jedes neue Archiv eine neue Zeile

Hinweis:
Beschränken Sie sich auf Buchstaben und Ziffern. Verwenden Sie keine Leerzeichen, Bindestriche und Sonderzeichen. Der Name darf nicht länger als 16 Zeichen sein und der Archiv Name muss mit einem Buchstaben beginnen

Merke:
Verwenden Sie hier (Bild 21) Laufwerksbuchstaben!! Es erhöht die Stabilität. Verwenden Sie dagegen für die Postbox den UNC Pfad, im speziellen wenn Sie das ***ELO***professional *Internetgateway betreiben (Newsletter #50)..*

3.4.1 Verdeckte Archive

Ab der Version **ELO***professional* 3.00.454 gibt es eine Möglichkeit Archive zu "verstecken". Nur Anwender mit Hauptadministrationsrechten können diese Archive dann sehen/auswählen.

Der Archivname muss dabei folgender Konvention folgen:

ELOLK_Archivname

"Archivname" ist frei wählbar. Ins Summe dürfen 16 Zeichen nicht überschritten werden und die anderen Einschränkungen aus obigem Hinweis gelten nach wie vor.

Um solch ein Archiv auszuwählen muss man mit Hauptadministrationsrechten angemeldet sein. Wenn Sie dann ELO beenden und wieder starten, erst dann können Sie die "verdeckten" Archive sehen.

3.5 AccessManager Registry Einstellungen

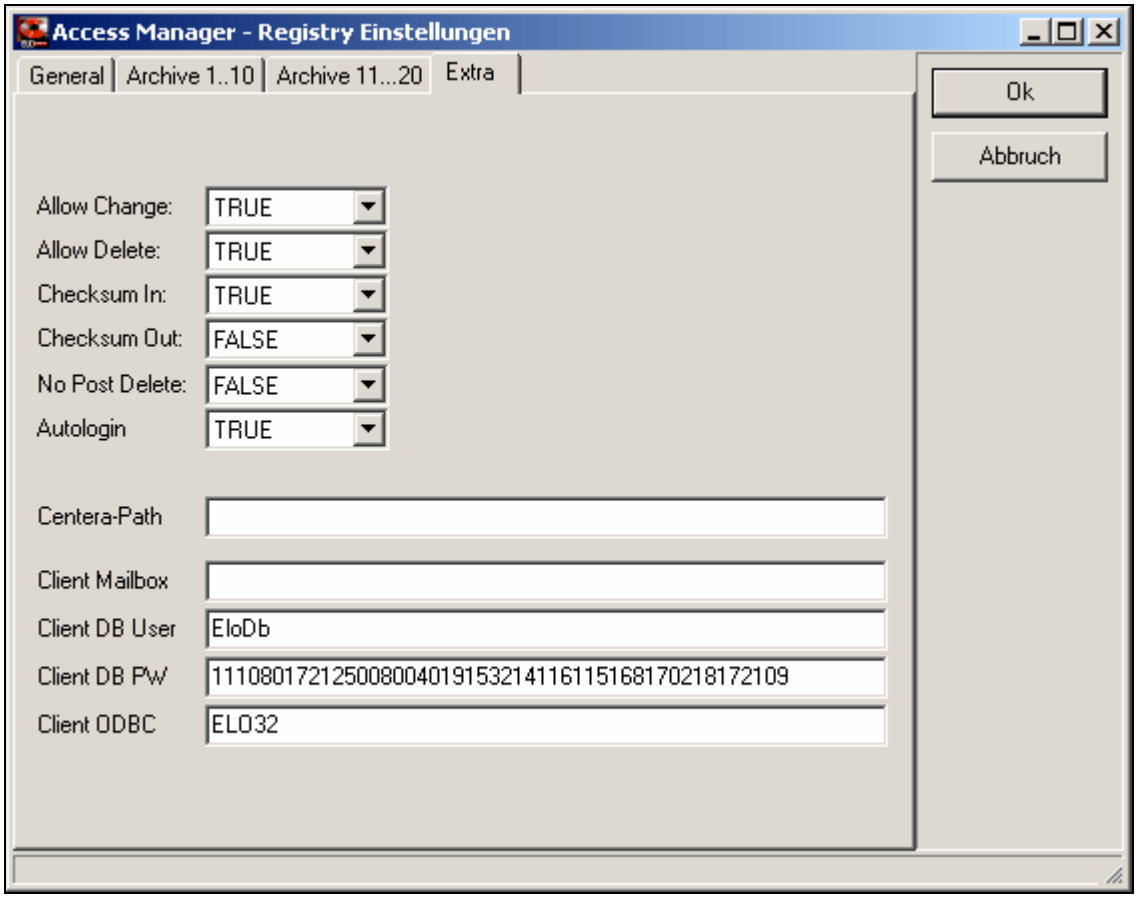

Bild 22: AccessManager Registry Einstellungen

Wenn Sie hier keine Änderungen vornehmen (Bild 22), dann verwendet **ELO***professional* interne Standard Voreinstellungen, die im Normalfall sinnvoll sind, ohne dass diese hier explizit angezeigt werden.

Erst wenn Sie hier Einstellungen vornehmen, werden Registrierungseinträge geschrieben, die dann die getroffene Einstellung auch anzeigen.

1) Allow Change

   Wenn Sie das Feld AllowChange auf "FALSE" umstellen akzeptiert der AccessManager keine Veränderung an Dokumenten mehr. Dokumente mit dem Dokumenten Status "Freie Bearbeitung" können nicht mehr geändert werden. Nur noch die Option "Versionskontrolliert" lässt ein Bearbeiten von Dokumenten zu, wo jede Änderung zu einer neuen Version wird.

2) Allow Delete

   Wenn Sie in ELO Dokumente löschen und dauerhaft entfernen lassen, wird im Archivdata Bereich die original-Dokumentendatei gelöscht. Wenn Sie das unterbinden wollen (z.B. aus Sicherheitsgründen oder weil der Archivdatenbereich ein WORM Medium ist) sollten Sie den Eintrag "AllowDelete" auf "FALSE" umstellen. Der ELO Client kann jetzt nach wie vor Dokumente löschen. Diese werden aber nur aus der Datenbank nicht aber aus dem AccessManager Bereich entfernt. Beachten Sie, dass es sich hier nicht um einen Ersatz der Datensicherung handelt. Es bleibt zwar die Dokumentendatei erhalten aber die Verschlagwortung und DMS Information geht verloren.

3) Checksum In

   Über die Option "Checksum In" können Sie in ELO den MD5 Mechanismus aktivieren. Hierbei wird zu jedem abgelegten Dokument ein MD5 Hash erzeugt und abgespeichert. Falls das Dokument irgendwie am ELO vorbei manipuliert wurde, kann das dann vom Client aus über die Option "Checksumme prüfen" erkannt werden. Sie können diese Option jederzeit nachträglich aktivieren. Allerdings werden nur für neu abgelegte Dokumente dann die Checksummen ermittelt. Für die älteren, bereits vorhandenen Einträge meldet der ELO Client dann nur, dass er die Checksumme nicht prüfen kann weil er keine Informationen dazu gespeichert hat. **Dieser Eintrag wird auch vom Client für die automatische Dublettenprüfung benötigt**. Wenn Sie ihn erst nachträglich aktivieren, ist im Archiv für alle vorher abgelegten Dokumente keine Checksumme für den Vergleich vorhanden. Sie sollten ihn deshalb prinzipiell auf „true“ setzen, auch wenn Sie die Checksummenprüfung nicht benötigen.

4) Checksum out

   Als Erweiterung der Checksum In Funktion dient die "Checksum Out" Option. Hier wird bei jeder Dokumentenanforderung die Checksumme des Dokuments geprüft bevor der Server das Dokument freigibt. Falls die Checksumme nicht korrekt ist gilt das Dokument als verloren ("besser gar kein Dokument als ein verfälschtes Dokument"). Beachten Sie, dass diese Option natürlich eine deutliche zusätzliche Serverlast erzeugt. Sie sollten Sie nur aktivieren, wenn Sie wirklich benötigen. Sie können diese Einstellung jederzeit ändern, sie wird aber nur nach einem Neustart des AccessManagers aktiv.

5) No Post Delete

   Mittels der Option "NoPostDelete" können Sie verhindern, dass Postbox Dokumente gelöscht werden. Jedes mal wenn der Anwender ein Löschen der Postbox veranlasst werden die Einträge in eine anderes Verzeichnis (DELETED) verschoben und nicht gelöscht solange diese Option aktiv ist.

6) Autologin

   Über die Option "Autologin" können Sie steuern ob Sie den Anwendern einen automatischen Systemeinstieg ermöglichen wollen. In der Einstellung "FALSE" ist immer ein explizites Login am ELO Client notwendig. Wenn dieser Wert auf "TRUE" steht kann ein Anwender das Archiv ohne extra ELO Login betreten sofern folgende Bedingungen erfüllt sind:
   - ELO ist mit der Option NT-Security eingerichtet
   - Der Client hat unter "Systemverwaltung – Optionen – Allgemein" die Checkbox "Automatischer Systemeinstieg" aktiviert.
   - Zu dem aktuellen NT Konto ist ein passender ELO Anwender konfiguriert.

7) Centera Path

- ohne Bedeutung für die **ELO***professional* 5.0 Grundlagenschulung -

8) Client Mailbox

- ohne Bedeutung für die **ELO***professional* 5.0 Grundlagenschulung -

9) Client DB User

Voreinstellung für den Anmeldenamen am SQL Server. Gegenüber früheren **ELO***professional* Versionen hat diese Konfigurationsmöglichkeit den Vorteil, dass das SQL Anmeldepasswort und der SQL Username geändert werden können, ohne dass das bei jedem Client nachregistriert werden muss.

10) Client DB PW

Voreinstellung für das Anmeldepasswort von **ELO***professional* am SQL Server. Gegenüber früheren **ELO***professional* Versionen hat diese Konfigurationsmöglichkeit den Vorteil, dass das SQL Anmeldepasswort und der SQL Username geändert werden können, ohne dass das bei jedem Client nachregistriert werden muss.

Das Passwort selbst kann im Klartext eingegeben werden (nicht empfohlen) oder dessen verkrypteten Wert (Registry).

11) Client ODBC

Voreinstellung des DSN-Names, mit dem sich dieser ELO Client an welchem SQL Server anmelden soll.

Hinweis:
Hinweis: Nahezu alle Änderungen in den Optionen erfordern einen Neustart des AccessManagers (nicht des gesamten Server PCs) um aktiv zu werden. Die einzige Ausnahme hiervon sind die Einstellungen zur Reportdatei und dem Reportlevel wenn die Option "AllowRemote" gesetzt ist. Diese Änderungen werden dann sofort und ohne Neustart übernommen.

Merke:
Vor einem Neustart (bzw. dem ersten Start) des Accessmanagers überprüfen Sie noch die Windows Registry Berechtigungen (Kapitel 3.7, Seite 26)

3.6 Registrierung des AccessManager Dienstes

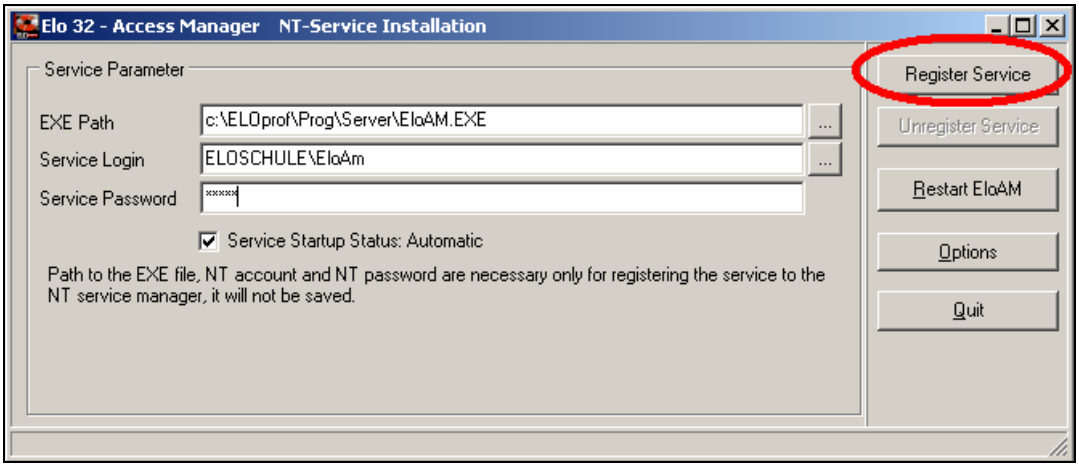

Bild 23: AccessManager Dienst anmelden/registrieren

Zum Abschluss der Serverinstallation wird automatisch das AccessManager Konfigurationsprogramm gestartet. Hier müssen Sie zuerst den ELO Server beim Windows NT Dienstmanager anmelden. Tragen Sie deshalb im Feld "NT Konto" den Namen des ELO Dienstkontos ein (normalerweise EloAM) und unter "NT Passwort" das dazu gehörende Passwort. Anschließend betätigen Sie die Schaltfläche "Dienst registrieren".

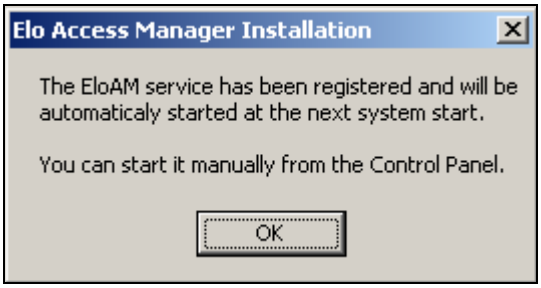

Bild 24: AccessManager Dienst ist installiert

Nachdem der AccessManager beim NT Dienstmanger angemeldet worden ist können Sie in den Optionen Dialog wechseln (Schaltfläche "Optionen").

Hinweis:
Einstellungen hier in Bild 23 werden festgelegt durch Betätigen der "Installieren" Schaltfläche. Änderungen hier am Login erfordern daher ein "Deinstallieren" (Dienst abmelden) unter Beibehalt der Registrierungseinträge und ein erneutes "Installieren" (Dienst registrieren). Alternativ können Sie die Änderungen auch direkt über die Microsoft Dienste-Verwaltung (Systemsteuerung – Dienste) vornehmen.

3.7 Windows Registry Berechtigungseinträge

Start – Ausführen – REGEDT32

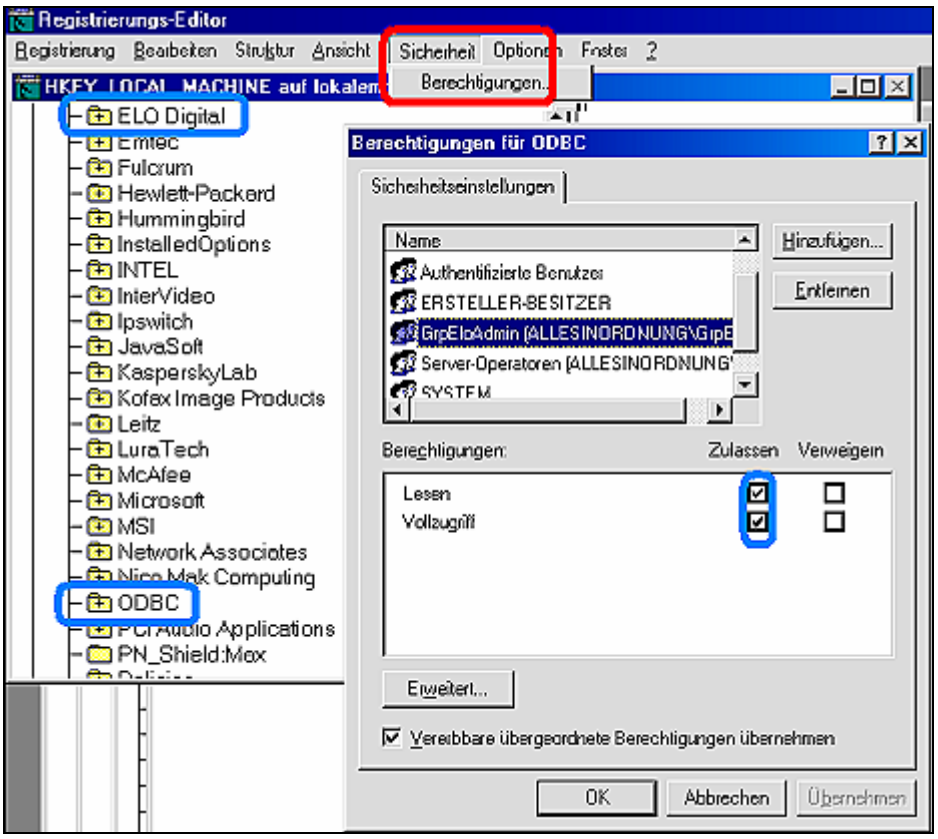

Bild 25: GrpEloAdmin Vollzugriff auf Registry Zweige – HKEY_LOCAL_MACHINE

3.8 Abschluss der ELO Server Installation

Nachdem der Server installiert und konfiguriert worden ist, können Sie ihn über die Schaltfläche "Neustart AM" starten.

Das Konfigurationsprogramm sollte daraufhin in der Statuszeile die Meldung "Service EloAM gestartet" ausgeben. Falls nicht werden Sie statt dessen eine Fehlermeldung vorfinden. Der häufigste Fehler an dieser Stelle sind falsche Konfigurationsdaten in der NT Security. Kontrollieren Sie bitte sorgfältig nochmals alle Passwörter, Anwender- und Gruppennamen. Weiterhin liefert die Statusmeldung ergänzende Fehlerhinweise. Falls Sie danach den Fehler immer noch nicht lokalisieren können, sollten Sie zuerst in den Windows NT Dienstmanager wechseln und die Starteigenschaften des ELO AccessManager Dienstes kontrollieren (hier werden Sie von Windows NT explizit auf ein evtl. falsch eingetragenes Passwort hingewiesen). Wenn Sie damit immer noch nicht weiter kommen sollten Sie den AccessManager Report ansehen. Hier werden Sie weitere Gründe für die Fehlfunktion vorfinden.

Im folgenden ein Beispiel für eine falschen Eintrag in der Admin Gruppe:

```
# SetEloAMSID
Security-ID für Accessmanager-Account GrpEloAdmin ermitteln
Accessmanager-Account GrpEloAdmin unbekannt beim (LookupAccountName)!
```

Hier wurde aufgrund eines Tippfehlers der Eintrag GrpEloAdmin mit einem doppelten N geschrieben, der NT Anwender konnte deshalb nicht ermittelt werden.

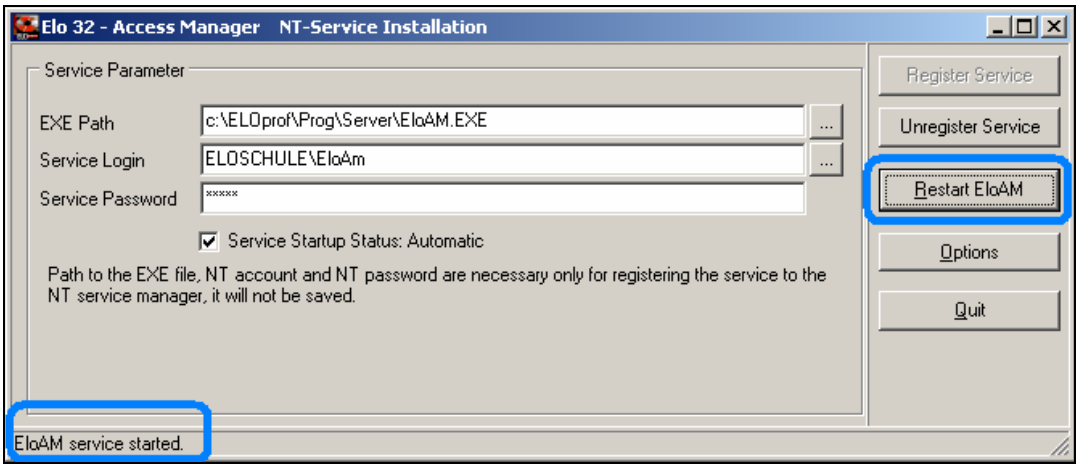

Bild 26: Neustart des AccessManagers

3.9 Verschiedenes

3.9.1 Notebook Installationen

Auch Standalone PCs (z.B. Notebooks) brauchen für eine **ELO***professional* Installation ein Netzwerk. Ist kein Netzwerk vorhanden, dann kann eine MS Loopbackadapter Installation helfen, der ein Netzwerk simuliert.

Obwohl es Software ist, unter Windows finden Sie den Loopbackadapter unter "Systemsteuerung – Hardware – Hardware hinzufügen".

Hinweis:
Das Thema "Loopbackadapter" ist bei Windows von Version zu Version und auch innerhalb von Service Packs unterschiedlich. Prinzipiell braucht ELO keinen Loopbackadapter. Mangels ausreichenden Windowskenntnissen kann er aber machmal ganz hilfreich sein.

Ein Auszug aus dem Newsletter #31 von Herrn Thiele:

```
...nur alle UNC Pfade im AccessManager ( Syslog Datei, Postboxen, Archive)
und im Client ( Postbox, Dokumentenpfade) auf Laufwerkspfade umstellen.
Zudem hat der Client unter "Systemverwaltung – Optionen – Allgemein" noch
den Namen des AccessManagers eingetragen, diesen tauschen Sie einfach
gegen einen Punkt aus. Mit dieser Konfiguration können Sie ELO auch in
einer "defekten" Windows Umgebung betreiben.
```

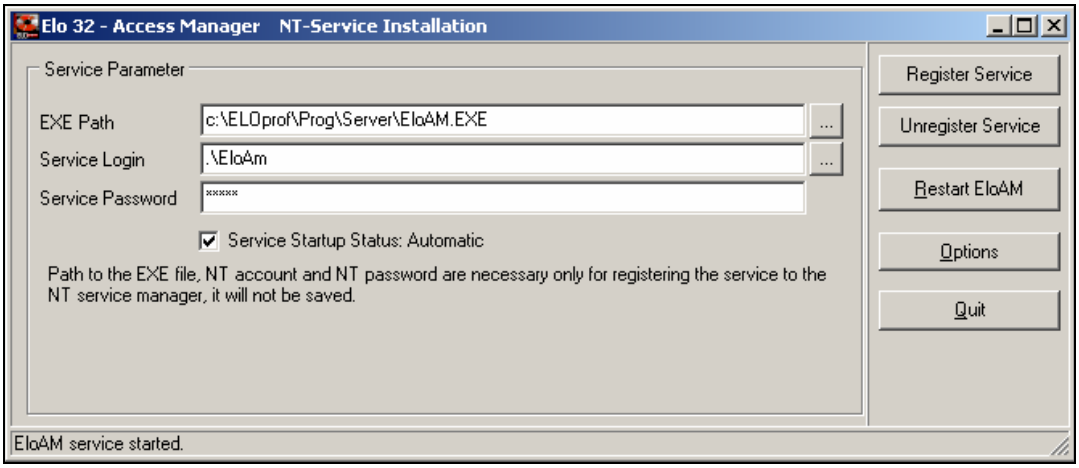

*Bild 27: Accessmanager Eintrag bei **ELO**professional ohne Netzwerk*

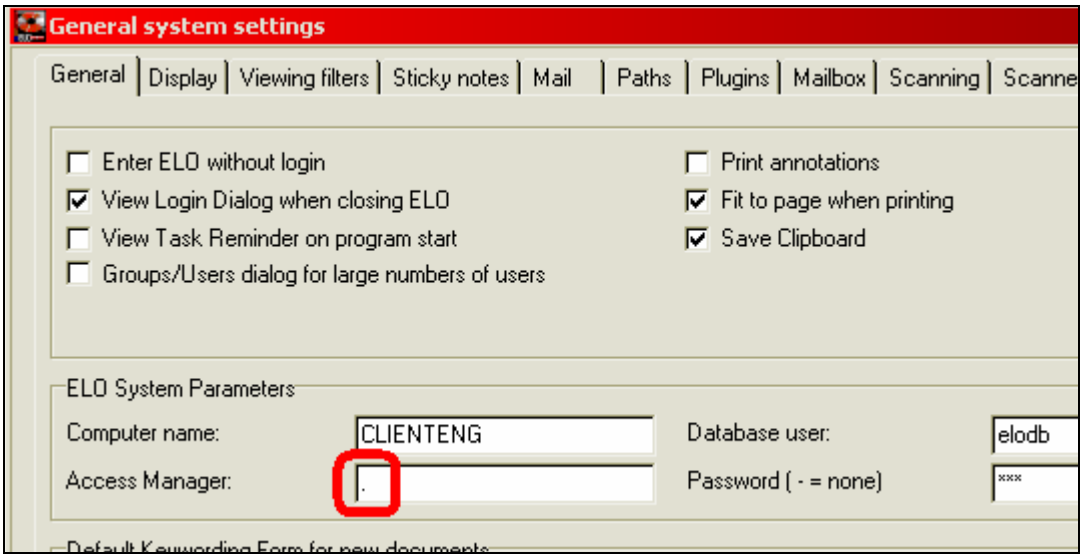

*Bild 28: Accessmanager Eintrag beim **ELO**professional Client eines Laptops (Standalone PC)*

3.9.2 Zeitsynchronisation im Netzwerk

Zeitsynchronisation empfiehlt sich in jedem Falle, da Sie ansonsten bei Dokumentenversionen riskieren, dass nicht die neueste Version angezeigt wird. Auch in den Reports von Ereignissen kann ein Durcheinander entstehen.

Sekundengenaue Zeitsynchronisation im Netzwerk ist unverzichtbar, wenn **ELO***professional* mit den Modulen "Replikation" oder "Mobil" betrieben wird.

Auszug aus dem Newsletter #32 von Herrn Thiele:

```
Die korrekte Funktion der Replikation hängt auch davon ab, dass alle
beteiligten PCs eine korrekte Uhrzeit verwenden. Innerhalb eines
Netzwerkes kann man das relativ leicht über eine Batchdatei

net time \\<Servername> /set /yes

im Autostart aller Clients sicherstellen. Voraussetzung ist natürlich,
dass der Server die korrekte Uhrzeit besitzt.

Falls mehrere Netze durch die Replikation betroffen sind, bieten sich
Zeitserver im Internet zur automatischen Synchronisierung an. In der
aktuellen c't (19/2002) finden Sie einen Artikel, der hierzu
Basisinformationen vermittelt.
```

3.9.3 Berechtigungseinstellungen NT Security

Falls Berechtigungseinstellungen geändert wurden, im Newsletter #32 von Herrn Thiele wird beschrieben, wie Sie die Berechtigungseinstellungen auf Dateisystem Ebene wieder in den Originalzustand versetzen:

Wenn Sie die Berechtigungen manuell korrigieren wollen oder müssen (z.B. nach einer Serverumstellung), dann sollten Sie für jeden Ablagepfad folgendermaßen vorgehen:

1) Das Basisverzeichnis auswählen (default unter: ...\EloProf\Archivdata\<Archivname>) und über die Rechteeinstellung "GrpEloAdmin Vollzugriff" für ALLE Unterverzeichnisse und ALLE Unterdateien einstellen. Mit diesem Schritt werden die Dokumenteneinstellungen korrigiert, anschließend sind aber die Verzeichnisse zu hart eingeschränkt.

2) Diese Einschränkung wird nun in einem zweiten Schritt korrigiert indem die Berechtigung für das Verzeichnis auf "GrpEloAdmin Vollzugriff und GrpEloUser Read/Execute" eingestellt wird. Die Vererbung wird auf ALLE Unterverzeichnisse und KEINE Dateien eingestellt.

3) Nun noch den AccessManager neu starten, da er in seinem internen Cache die von Ihnen geänderten Werte nicht kennt und somit nicht alle angeforderten Dokumente neu freischaltet.

3.9.4 Versionsinformtationen

Auszug aus dem Newsletter #39 von Herrn Thiele:

Der Client ab **ELO***professional* **3.00.510** schreibt bei jedem Programmstart seinen aktuellen Versionsstand in die Registry (unter **HKCU\Software\ELO Digital\Versions**). Hierüber kann jederzeit die aktuelle ELO Version ausgelesen werden, auch dann, wenn der Client nicht aktiv ist oder aufgrund eines Fehlers nicht aktiviert werden kann.

Wir werden diese Funktion in den kommenden Wochen für alle relevanten ELO Module einführen, so dass sich der Support jederzeit leicht Überblick über die installierten Programmversionen verschaffen kann. Hierzu erstellen wir auch ein kleines Programm, welches die Versionsstände auflistet und audrucken kann (im Tools-Bereich).

Ich möchte an dieser Stelle alle Partner, welche ELO Erweiterungen programmieren, ermutigen diesen Paremter ebenfalls einzutragen. Hierzu fügen Sie in dem aufgeführten Pfad einfach eine Zeichenkette ein, welche als Namen Ihre Modulbezeichnung trägt. Der Inhalt der Zeichenkette besteht aus der Versionsnummer und optional einem @ Symbol und einem weiteren kurzen Infotext.

4 Datensicherung

Auszug aus dem Newsletter #47 von Herrn Thiele:

```
++++++++++++++++++++++++++++++++++++++++++++++++++
Inkonsistenzen in der Datensicherung
++++++++++++++++++++++++++++++++++++++++++++++++++

Während der Datensicherung sollten innerhalb von ELO keine Aktivitäten
stattfinden, andernfalls ist es schwierig eine konsistente Datensicherung
zu erzeugen. Im Allgemeinen wird das durch eine entsprechende
Verfahrensanweisung während der Sicherung erzwungen (z.B. ELO Dienste
während der Sicherung beenden).

In einem 24 Stunden, 7 Tage pro Woche System ist das aber nicht möglich.
In diesem Fall kann man auch keine vollständig konsistende Datensicherung
erzeugen. Allerdings kann man die Störungen durch eine geeignete
Sicherungsreihenfolge minimieren. Zudem muss man sich im klaren darüber
sein, dass das Sicherungsvolumen durch den Startzeitpunkt der Sicherung
und nicht durch das Ende beschränkt wird.

1. Sichern Sie die Datenbank VOR den AccessManager Daten. Hierdurch
erreichen Sie, dass es zu jedem logischen Dokument in der Datenbank auch
wirklich eine Dokumentendatei im AccessManager Bereich gibt. Die
Inkonsistenz beschränkt sich in diesem Fall darauf, dass es im
AccessManager "verwaiste" Dokumentendateien gibt, die keinem logischen
Dokument zugeordnet sind. Aus Kostengründen ist das im Allgemeinen
sicherlich kein Problem, falls doch, können diese Dateien über den
Menüpunkt "Archiv" - "Reports" - "Systemdiagnose" ermittelt werden und
manuell entfernt werden.

2. Sichern Sie die AccessManager Konfigurationsdateien (*.EDC, *.EPT) NACH
den Dokumentendateien. Hierdurch kann es zwar vorkommen, dass in der EDC
Datei ein Dokument eingetragen wird, welches als Datei in der Sicherung
nicht vorhanden ist - dieses Dokument ist aber in der Datenbank ohnehin
nicht vorhanden und kann deshalb niemals angesprochen werden. Falls Sie
die EDC Datei VOR den Dokumentendateien sichern, dann kann es passieren,
dass es zu einer neuen Dokumenten-nummer bereits eine Datei gibt, der
folgende Ablage-vorgang wird dann scheitern. Diese Inkonsistenz können Sie
allerdings sehr leicht manuell reparieren, entweder über den Menüpunkt
"EDC-Datei neu" oder durch löschen der zusätzlichen Dateien über den
Explorer.

3. Stellen Sie sicher, das WÄHREND der Rücksicherung keine Aktivitäten im
System durchgeführt werden können. Insbesondere wenn Sie mit
incrementellen Sicherungs-datensätzen arbeiten oder bei der Rücksicherung
irgend-welche Probleme auftreten, kann es passieren, dass im ELO bereits
neue Dokumente abgelegt werden, während die Rücksicherung noch nicht
abgeschlossen ist. Achten Sie unbedingt darauf, dass der
Replikationsdienst während dieser Zeit deaktiviert ist!
```

4. Wenn Sie ein Restore durchgeführt haben, führen Sie UNBEDINGT eine sorgfältige Systemkontrolle durch bevor wieder die Arbeit aufgenommen wird. Falls die Rücksicherung nicht vollständig oder fehlerhaft durchgeführt wurde, erhalten Sie durch die weitere Arbeit ein System welches kaum mehr kontrollierbar ist. Sie sollten auch bedenken, dass die Ursache für den Restorevorgang (z.B. eine unzuverlässige Festplatte, eine Virusinfektion...) auch bereits die letzte Datensicherung beeinflußt haben könnte. In diesem Fall müssen Sie evtl. noch manuelle Reparaturen am System durchführen oder auf eine ältere Sicherung zurückgreifen. Da solche Schäden nicht unbedingt sofort sichtbar werden, sollten Sie in den Tagen (oder Wochen) nach einem Restore das System sorgfältiger beobachten.

Dokumente sollten während dieser Zeit unbedingt aufgehoben werden, Vorgänge sorgfältig protokolliert werden. Diese Hinweise finden Sie im Wesentlichen bereits in dem über 2 Jahren alten Dokument zur ELO Daten-sicherung im Internet (Dokumente Bereich). Falls die Punkte für Sie nicht selbstverständlich waren, sollten Sie sich das gesamte Dokument nochmals ansehen (als Auffrischung).

Appendiks C

Dubletkontrol

(På tysk)

En kort gennemgang af hvordan dubletkontrollen virker i ELO. Den bliver forklaret hvordan ELO anvender MD5 til at lave hashkoder af filerne som bruges til dubletkontrol.

Dublettenfreie Archivablage

In den meisten Archivumgebungen stellen Dubletten nur ein untergeordnetes Problem dar, da nur ein sehr kleiner Teil der Dokumente versehentlich oder absichtlich mehrfach abgelegt werden. In einigen speziellen Bereichen kann es aber auch zu einer sehr hohen Anzahl von Mehrfachablagen kommen, so dass Dubletten einen großen Teil des verfügbaren Speichers belegen. In diesen speziellen Fällen kann es durchaus sinnvoll sein erhöhten Aufwand zur Vermeidung der Dubletten in Kauf zu nehmen.

Zur Dublettenkontrolle gibt es zwei unterschiedliche Ansätze:

1. Aktive Dublettenvermeidung durch Informationshinweise und Referenzen
2. Passive Dublettenvermeidung durch einmalige Speicherung der Datei

Beide Ansätze haben ihre spezifischen Vor- und Nachteile. ELOprofessional 4.0 unterstützt die aktive Dublettenvermeidung von Anfang an, die passive ab der Version 4.00.088 in einer pre-Release Form welche noch nicht in Produktivarchiven eingesetzt werden sollte.

1 Aktive Dublettenvermeidung

Bei der aktiven Dublettenvermeidung wird auf dem Client bei der Ablage geprüft, ob es dieses Dokument bereits gibt. Wenn es schon vorhanden ist, erhält der Mitarbeiter einen entsprechenden Hinweis mit der Auswahl, ob er das Dokument trotzdem ablegen möchte, eine Referenz auf das Vorhandene Dokument verwenden möchte oder den Ablagevorgang ganz abbrechen möchte.

Diese Vorgehensweise hat den Vorteil, dass Mehrfachablagen transparent werden. Der Anwender sieht, wo das Dokument bereits hinterlegt worden ist und kann entscheiden, ob er mit einer eigenen Version weiterarbeiten möchte. Da diese Dubletten aktiv wahr genommen werden, besteht hier zudem die Möglichkeit Probleme in den Geschäftsabläufen zu erkennen und zu verbessern. Weiterhin besteht der Vorteil, dass die Mehrfachablage über Referenzen letztendlich auf ein Dokument und eine Verschlagwortung zeigt und es so nicht vorkommen kann, dass unterschiedliche oder gar widersprüchliche Informationen zu einem Dokument abgelegt werden.

Allerdings hat diese Form auch Einschränkungen. Aus Sicherheitsgründen können die Referenzen nur zur Dokumenten angeboten werden, auf die der Anwender auch Zugriffsrechte besitzt. Wenn eine Dokumentendatei bereits im System gespeichert ist, der Anwender aber keine Zugriffsberechtigung hierauf besitzt, wird auch keine Dublettenwarnung angezeigt. Das ist deshalb notwendig, da allein die Bestätigung der Existenz eines Dokuments einen unzulässigen Geheimnisverrat darstellen kann. Zudem besitzt die Verkettung über eine Referenz nur eine Verschlagwortung, die dem zusätzlichen Ableger nicht immer sichtbar gemacht werden kann oder soll.

2 Passive Dublettenvermeidung

Bei der passiven Dublettenvermeidung wird jedes Dokument zur Ablage akzeptiert. Der Client legt auch für jede Datei eine eigene Verschlagwortung an, es entsteht also ein vollwertiges logisches Dokument. Auf der Serverseite wird allerdings jede neue Datei darauf hin geprüft, ob sie bereits vorhanden ist. Wenn sie schon da ist, dann wird sie nicht noch mal neu gespeichert, es wird statt dessen die vorhandene Version mit verwendet.

Diese Vorgehensweise hat den Vorteil, dass bei Dubletten jedes Dokument mit einer eigenen Verschlagwortung (und eigenen Sicherheitseinstellungen) versehen werden kann. Die einzelnen Anwender merken keinen Unterschied zwischen der Ablage der Dublette und einer normalen Ablage.

Dieser Vorteil stellt aber gleichzeitig auch einen Nachteil dar. Der Anwender bekommt keinen Hinweis darauf, dass es das Dokument im Archiv bereits gibt. Die erneute Ablage erzeugt ein völlig eigenständiges logisches Dokument, lediglich der Speicherplatz für die Dokumentendatei wird nur einfach belegt. Wenn das Dokument im Dateiinhalt oder in der Verschlagwortung ergänzt wird, dann wird eben nur die Version verändert, in der die Aktion ausgelöst wurde.

3 Welche Form sollte man verwenden?

Es gibt keine einfache Antwort, welche der beiden Formen besser ist. Diese Auswahl hängt von dem jeweiligen Projekt und den Rahmenbedingungen ab. Die aktive Dublettenvermeidung ist im Allgemeinen besser, wenn es darum geht, Dubletten aufzuspüren und zu vermeiden (z.B. um unterschiedliche Planungsstände zu vermeiden, die durch unterschiedliche Fortschreibung aus der mehrfachen Ablage eines Plans entstanden sind. Die passive Dublettenvermeidung ist günstiger, wenn es nur um den belegten Speicherplatz der Dokumentendateien geht und keine organisatorische Kontrolle gewünscht ist.

4 Technische Aspekte bei der passiven Dublettenvermeidung

Die aktive Dublettenvermeidung ist in der Version ELOprofessional 4.0 von Anfang an vorhanden und freigegeben. Die passive Vermeidung ist ab der Version 4.00.088 in einer Testversion implementiert und ist nur bedingt für den Produktivbetrieb zu verwenden. Sie sollten diese Funktion nur dort einsetzen, wo auch nachträglich noch ein Zugriff auf die Originale möglich ist, so dass bei einer Fehlfunktion keine Daten verloren gehen.

4.1 Allgemeine Hinweise

Die passive Dublettenkontrolle wird durchgeführt, indem für jede Datei ein 128 Bit MD5 Hash gebildet wird. Dieser Hash wird in Form einer 32-stelligen Zeichenkette als Dateiname verwendet. Dateien mit identischen Inhalt erzeugen den gleichen MD5 Hash und erhalten somit bei der Ablage den gleichen Dateinamen. Die Datei muss deshalb nur einmal gespeichert werden.

Diese MD5 Dateien werden in einer Verzeichnisstruktur abgelegt, die aus 4096 Unterverzeichnissen besteht (12 Bit). Diese Unterverzeichnisse sind von 000, 001, 002 ... FFF durchnummeriert. Das Zielverzeichnis für eine Datei ergibt sich aus den drei letzten Stellen des Dateinamens (ohne Extension), die Datei 012345....0123456789ABCDEF.TIF wird also im Verzeichnis MD5_DEF abgelegt. Aus dem verwendeten Ablagepfad und dem Dateinamen können Sie also leicht das tatsächliche Ablageziel ermitteln.

4.2 Installation

Zur Installation wird ein ganz normales ELOprofessional 4.0 System vorausgesetzt. Den Client müssen Sie auf die Version 4.00.088 oder neuer setzen, den AccessManager auf die Version 4.00.040 oder neuer. Änderungen in der Datenbank sind für die passive Dublettenkontrolle nicht notwendig, diese Aktionen finden ausschließlich auf dem AccessManager statt.

4.3 Konfiguration

Wenn Sie die Archivablage um die passive Dublettenkontrolle erweitern wollen, dann müssen Sie einen Dokumentenablagepfad mit der Strukturinfo „MD5 Ablage“ verwenden. Bei einem bestehenden Archiv dürfen Sie auf keinen Fall die Strukturinfo des Basispfades umstellen, dann würden die alten Dokumente nicht mehr gefunden werden. In diesem Fall müssen Sie einen neuen, zusätzlichen Pfad als MD5 Pfad einrichten und in den Optionen (und bei Bedarf in den einzelnen Ablagemasken) als Basispfad eintragen. Die Dublettenkontrolle funktioniert prinzipiell nur, wenn Sie im AccessManager die Ermittelung des MD5 Hash bei der Ablage (Registry-Option Checksum In) aktiviert haben.

Der AccessManager kann beim dauerhaften Löschen von Dokumenten nicht feststellen, ob so ein Dokument möglicherweise noch von anderer Stelle aus verwendet wird. Deshalb wird ein Dokument aus einem MD5 Pfad nur dann gelöscht, wenn es ein Backup davon gibt. Sie sollten so einen MD5 Pfad also nur dann verwenden, wenn Sie mit Spiegelpfaden oder einem Backupserver arbeiten. Wenn ein Dokument ohne Backup gelöscht werden soll, wird die Dokumentendatei nicht entfernt und verbleibt im Dateisystem.

4.4 Systemeinschränkungen

Prinzipbedingt gibt es bei der MD5 Ablage ein paar Einschränkungen, die beachtet werden müssen:

1. Da die logische Dokumentennummer bei diesen Dateien nicht mehr Teil des Dateinamens ist, können solche Pfade nicht mehr per „EDC-Datei neu aufbauen“ ausgelesen werden. Es muss also sichergestellt werden, dass die EDC Datei des AccessManagers zuverlässig in die Datensicherung aufgenommen wird.
2. Die Identifikation über einen 128 Bit MD5 Hash kann theoretisch dazu führen, dass zwei unterschiedliche Dateien als identisch angesehen werden. Eine der beiden Versionen wird dann verloren gehen. Die Wahrscheinlichkeit für dieses Ereignis ist allerdings extrem gering, sie liegt etwa bei 1 zu 100000000000000000000000000000000000000. Es ist meines Wissens noch kein Fall bekannt, wo es tatsächlich zu so einem Konflikt gekommen ist.
3. Dokumente in der freien Bearbeitung erzeugen bei jedem Speichervorgang eine neue Datei (wenn sie verändert worden sind). Deshalb belegen Sie genauso viel Speicher wie die versionskontrollierten Dokumente, dieser wird beim Löschen dann auch nicht mehr freigegeben. Aus diesem Grund sollten Sie Dokumente aus der freien Bearbeitung nicht in MD5 Pfade ablegen.
4. Beim Löschen eines Dokuments aus dem MD5 Pfad kann es vorkommen, dass auch andere Dokumente diese Datei benötigen. In diesem Fall wird beim nächsten Zugriff automatisch ein Restore (ohne Nachfrage beim Client) ausgeführt. Sie sollten den MD5 Pfad deshalb nur mit Backup-Lösungen betreiben, die einen dauerhaften Zugriff auf den Spiegelpfad erlauben. Solange keine Dokumente aus dem MD5 Pfad dauerhaft entfernt werden, ist dieser Punkt allerdings nicht relevant. Vor dem dauerhaften Entfernen von Dokumenten aus dem ELO Client heraus sollte man sicherstellen, dass alle Dokumente über den Backupdienst gesichert worden sind (d.h. der Backupdienst meldet nach einem aktuellen Lauf „nothing to do“).
5. Die passive Dublettenprüfung erfolgt nur innerhalb eines Ablagepfades. Wenn Sie mit mehreren Pfaden arbeiten, ist jeder für sich Dublettenfrei, zwischen den unterschiedlichen Pfaden kann es aber doppelte Einträge geben. Wenn Sie nur den Basispfad mit einem MD5 Pfad, den Spiegelpfad aber mit einem normalen Ablagepfad betreiben, dann ist nur der Basispfad Dublettenfrei, im Spiegelpfad sind die Dokumentendateien mehrfach enthalten. Eine zusätzliche Sicherheit erhalten Sie hierdurch nicht, da die Quelle für den Spiegelpfad immer die gleiche Datei aus dem Basispfad ist.

Appendiks D

ELO Professional 5 Client manual

Dette appendiks indeholder hele ELO Professional 5 klient manualen. Denne fylder 800 sider, som er vedlagt på cd'en i pdf-format. Filen er navngivet uk-client5.pdf.