COMPUTERWORLD

Sikkerhed i Access 2000/2003

Formålet med denne artikel er at give læseren en trin-for-trin vejledning i at sætte sikkerheden i Access op, samt gøre læseren i stand til at vurdere fordele og ulemper ved de forskellige sikkerhedsniveauer.

Skrevet den **12. May 2011** af **thomasjepsen** I kategorien **Databaser / Access** | ★★★☆☆

Vejledning i MS Access sikkerhedsopsætning

Note pr 12. maj 2011: Da sikkerheden i Access har ændret sig siden denne artikel oprindelig blev skrevet i 2004, vil de fleste metoder formentlig ikke virke i nyere versioner af Access. Artiklen vil måske blive opdateret til at omfatte nyere versioner af Access på et senere tidspunkt.

Historik
1-6-2004: Artikel frigives.
13-9-2004: Mindre stave/slåfejl er rettet, da en venlig sjæl gjorde mig opmærsom på disse. Tak for input.
12-5-2011: Advisering om, at artiklen kun henvender sig til Access 2000/2003

Formål

Databasesikkerhed - hvad enten det drejer sig om Access, SQL server, Oracle eller andre databaser - er kompliceret og kræver at man holder tungen lige i munden.

I de seneste versioner af Access har det været muligt at benytte en guide til at oprette sikkerheden, ligesom der er skrevet mange tilsvarende vejledninger. Men min erfaring gennem årene er, at dette er et af de emner, hvor folk knækker halsen og giver op eller kun får implementeret en halvfærdig sikkerhed.

Jeg mener desuden, at man får den bedste forståelse ved at lave arbejdet selv. (Det gælder også alle kontrolelement-guiderne, som findes i Access.)

Nogle vil måske mene, at denne artikel er overflødig. Men da jeg har erfaring, fra mine egne kunder, med at Access' sikkerhed er kompliceret at gennemskue, og da spørgsmålet jævnligt dukker op på eksperten.dk, så synes jeg, at det var relevant at lave denne vejledning.

Bemærk: Det skal nævnes, at menuer og funktionalitet har ændret sig fra version til version (og selvfølgelig fra sprog til sprog), hvorfor det er svært at beskrive det hele generelt. Jeg har derfor taget udgangspunkt i Access 2003 DK (for at fremtidssikre så meget som muligt). Jeg vil dog forsøge at angive forskelle i tidligere versioner.

Overvejelser

For at kunne gøre en database (applikation) sikker, er der flere perspektiver, man bør tage stilling til. I Access er det muligt at sikre et system tilnærmelsesvis 100 % (!) imod enhver ulovlig indtrængen. Det vil dog altid være muligt, hvis indtrængeren er ihærdig nok, at slette eller beskadige systemet, ligesom det også altid vil være muligt at få adgang til godkendte brugeres adgangskoder, hvis man kigger dem længe nok over skulderen eller hvis brugerne ikke er opfindsomme nok med deres adgangskoder. Imidlertid er et 100 % sikkert system lidt mere omstændigt at arbejde med. Dels skal alle brugere gå og huske på og

indtaste login-navn og adgangskode hver gang man starter en applikation. Dels skal systemet også krypteres (se senere) for at sætte prikken over i'et, og det bevirker, at Access bliver 10-15% langsommere. Der er derfor et utal af sikkerhedsgrader. Men man skal starte med at gøre sig klart, hvad man ønsker at forhindre ved at indføre sikkerhed på sin database.

Overordnet kan man sige, at der er disse forskellige sikkerhedsbehov:

- Undgå at nogen andre end jeg selv får adgang til databasen.
- Undgå at brugere "kommer til" at "pille" i opbygningen af databasen.
- Undgå at brugere (eller andre) får adgang til følsomme oplysninger.
- Undgå at brugere eller andre kan ændre/sabotere følsomme data.

Derudover kan der være et hav af variationer.

Databaseadgangskode

Den simpleste sikkerhed, man kan lægge på databasen er at angive en adgangskode, som skal indtastes hver gang databasen åbnes (Funktioner->Sikkerhed->Angiv databaseadgangskode). Men hvis ønsker at beskytte følsomme oplysninger eller have en mere avanceret styring af sikkerheden er denne metode ikke velegnet. Først og fremmest fordi, at det er relativt nemt at skrive en VBA funktion, som "prøver sig frem" indtil den rigtige adgangskode er fundet.

Access' brugersikkerhed

Den mest effektive sikkerhed, opnås ved at benytte Access' egen sikkerhedsstyring. Denne giver mulighed for at definere ret præcist hvilke tabeller, forespørgsler, formularer, rapporter og makroer en bruger må se, redigere, oprette, slette osv.
Resten af denne artikel beskæftiger sig udelukkende med opsætningen af denne sikkerhed.

1. Arbejdsgrupper

Når man skal benytte sikkerhed i Access på netværk, bør man oprette en fælles Arbejdsgruppe. I denne arbejdsgruppe gemmes (automatisk) informationer om brugere og deres adgangskoder. Der bør oprettes en ny Arbejdsgruppefil inden man begynder at oprette brugere og tilladelser.

En arbejdsgruppe oprettes ved at gå i menuen Funktioner->Sikkerhed->Arbejdsgruppeadministrator. (Fra version 2000 og tidligere, skulle man starte filen **Wrkgadm.exe**, som ligger i Office-biblioteket.)
En dialogboks dukker frem, med titlen **"Arbejdsgruppeadministrator"**. Her kan man se hvilken arbejdsgruppefil, man allerede er tilknyttet. Har man ikke ændret denne sti tidligere, vil den typisk ligge her:
C:\Documents and Settings\DitBrugernavn\Application Data\Microsoft\Access\System.mdw (denne sti er afhængig af Windows-version og -sprog)

Note: Siden Access 2000 har arbejdsgruppefilen haft .mdw som extension. Tidligere var det .mda

Man har 3 knapper i dialogboksen: **Opret**, **Tilslut** og **OK**.

[Opret]: Denne knap opretter (ganske overraskende) en ny arbejdsgruppefil på en angivet placering og tilslutter sig automatisk.

Man skal angive følgende parametre:
- **Navn** (obligatorisk)
- **Organisation** (valgfri)
- **Arbejdsgruppe-ID** (4-20 tegn. ID'en er valgfri, men kraftigt anbefalet. ID'en er case-sensitiv)

Herefter angives navn og placering af filen. Hvis flere brugere skal kobles på denne arbejdsgruppefil (hvilket er hele ideen med en "Arbejdsgruppe"), skal filen placeres på et **fælles drev**.
Pas på med at overskrive eksisterende system.mdw'er, da andre brugere kan benytte dem stadig!

Note: Arbejdsgruppe ID (Samt det tilsvarende Personlige ID, som vi kommer til senere) svarer til en mobiltelefons PUK-kode. Denne skal bruges, hvis arbejdsgruppefilen og dermed hele sikkerheden skal genskabes. ID'et skal ikke benyttes til dagligt, men bør gemmes et sikkert sted, så Arbejdsgruppefilen kan genskabes hvis den skulle blive beskadiget eller slettet (!).

[Tilslut]: Hver enkelt bruger, som skal deltage i denne arbejdsgruppe skal, fra deres egen PC, starte Arbejdsgruppeadministratoren op og vælge **[Tilslut]**, og derefter angive den nyoprettede System.mdw.

[OK]: Afslutter Arbejdsgruppeadministratoren.

2. Grupper

Når en fælles arbejdsgruppefil er oprettet på et fællesdrev, kan man begynde at oprette Brugere og Grupper.

Brugere kan have individuelle rettigheder til forskellige tabeller, formularer, rapporter og makro'er i en applikation. For at gøre administrationen af brugerne lidt lettere, kan man oprette Grupper af brugere, som ligeledes kan tildeles individuelle rettigheder.
Brugere kan tilhøre flere forskellige grupper og derved få disse gruppers rettigheder udover deres egne.

Som standard ligger der 2 grupper i Access:

- Administratorer
- Brugere

samt én bruger:

- Administrator

Man bør altid oprette sikkerheden på **gruppe-niveau**. Derved behøver man ikke at tildele rettigheder til hver bruger, men blot gøre brugeren medlem af en gruppe.

Skal man oprette en ny gruppe, åbner man menuen *Funktioner->Sikkerhed->Bruger- og gruppekonti*.
Vælg fanebladet Grupper og klik på **[Ny]**.
I dialogboksen angiver man gruppens navn efterfulgt af en **Personlig ID** (eller PID-kode). Denne kode skal bestå af mellem 4 og 20 tegn/cifre. Som tidligere nævnt, har denne Personlige ID ikke noget med adgangskode at gøre, men skal mere betragtes som en sikkerhedsnøgle, som skal bruges, hvis arbejdsgruppefilen bliver beskadiget eller slettet og efterfølgende skal genskabes.

3. Brugere

Når man skal oprette brugere foregår det på samme måde. Man bliver også her bedt om en Personlig ID. Udover det, skal man så også vælge hvilke grupper, brugeren skal tilhøre. Det er vigtigt at bemærke, at en bruger kan være medlem af flere grupper. Og at man ikke kan fravælge "Brugergruppen". Mere om dette senere.

4. Ejerskab

Inden man begynder at tildele tilladelser til brugere og grupper, er det vigtigt at man giver sin database det rette ejerskab.
Ejeren af en database, er den bruger, som har oprettet databasen i sin tid.
Alle objekter i databasen er som udgangspunkt også ejet af den bruger, som oprettede objektet. Det er dog muligt at skifte ejerskab på de enkelte objekter (*Funktioner->Skkerhed->Bruger- og gruppetilladelser->Skift ejer*) - bare ikke på selve databasen.
En bruger har altid tilladelse til at skifte rettigheder for sine egne objekter.

Og hvad betyder det i praksis?

Det betyder, at alle databaser, som er oprettet af Administratoren (standard brugeren) kan åbnes af Administrator. Man kan ganske vist fjerne alle tilladelser fra Administratoren, men Administratoren kan til hver en tid gå ind og give sig selv alle tilladelser igen - fordi han er ejer! Ligeledes har medlemmer af gruppen Administatorer mulighed for at nulstille adgangskoder for andre brugere, hvorved de kan få fri adgang.
Er brugeren Administrator derimod ikke ejer af databasen, kan han helt udelukkes fra at måtte starte databasen, hvorved han heller ikke kan nulstille adgangskoder eller tildele sig selv rettigheder.

Derfor bør man - inden man tildeler tilladelser - oprette en ny database (mens man er logget på som en ny administrator-bruger) og herefter importere alle objekter fra den gamle database. Derved er databasen 100 % ejet af den nye bruger, og man kan begynde at give tilladelser.

5. Tilladelser

Menuen Funktioner->Sikkerhed->Bruger- og gruppetilladelser er værktøjet til at styre hvem, der må hvad. Her kan man så (efter at have klikket i feltet Grupper) tildele hver gruppe de aktuelle rettigheder til hver eneste tabel, forespørgsel, formular, rapport og makro. Hver bruger, som er medlem af en gruppe får denne gruppes rettigheder.

Afhængigt af om det er en tabel, forespørgsel m.m., så er der forskellige tilladelser, som kan gives. På tabeller kan man således angive om en gruppe/bruger må:

- **Læse design** (se hvordan tabellen er bygget op i designvisning)
- **Redigere design** (ændre designet af en tabel)
- **Administrere** (alt inkl. skifte tilladelser)
- **Læse data** (åbne tabellen, men ikke redigere)
- **Opdatere data** (åbne og redigere tabellen)
- **Indsætte data** (oprette nye poster, men ikke ændre de eksisterende)
- **Slette data** (tja...)

Disse tilladelser angives for samtlige tabeller, forespørgsler, formularer, rapporter og makroer for samtlige grupper og/eller brugere. Man kan blokmarkere flere objekter af samme type for at gøre det lidt nemmere.

Er der enkelte brugere, som skiller sig ud fra de aktuelle grupper, kan han/hun tildeles individuelle rettigheder ved at klikke på Brugere. Man skal dog være opmærksom på at man ikke kan fratrække en bruger nogle rettigheder blot ved at fravælge dem i hans specifikke opsætning. En brugers tilladelser er

foreningsmængden af de grupper, som han er medlem af. Dvs. at hvis en bruger er medlem af en gruppe, som må indsætte data og en anden gruppe, som må slette data, så må brugeren altså både indsætte og slette data (men ikke redigere eksisterende data).

VIGTIGT: Hvis applikationen er delt op i frontend og backend (hvilket klart anbefales) skal tilladelser til tabeller angives i Backenden, hvorved den nedarves til frontenden. Hvis man angiver tabel-tilladelserne i frontenden, kan enhver blot åbne backenden og derved få uhindret adgang til alle data!

Når man har tildelt alle nødvendige tilladelser til alle brugere og grupper, er det tid til at lukke for adgangen for alle andre. Dette gøres ved at fjerne alle rettigheder fra brugeren Administrator og grupperne Administratorer og Brugere.

Note: Husk at fjerne Brugergruppens og Administratorgruppens rettigheder for alle objekter i databasen. Det er dog **vigtigt** at dette først gøres, når man er sikker på, alle rettigheder er overdraget til en anden bruger.

6. Adgangskode

Når man starter Access op de første gange, bliver man automatisk logget på som brugeren Admin. For at hver enkelt bruger overhovedet skal kunne logge sig på med sine egne rettigheder, skal man ændre adgangskoden for Admin. Dette gøres ved at vælge menuen *Funktioner->Skkerhed->Bruger- og gruppekonti->Skift Logonadgangskode* og derefter indtaste en ny kode i feltet Ny adgangskode og derefter bekræfte det på næste linie. Fremover vil alle som er tilknyttet den aktuelle Arbejdsgruppe blive promptet for et login-navn. Hver enkelt bruger bør så gå ind og ændre sin egen adgangskode.

Note: Hvis en bruger har glemt sin adgangskode, kan en anden bruger, som er medlem af gruppen Administratorer, **nulstille** en brugerens adgangskode. (*Funktioner->Skkerhed->Bruger- og gruppekonti->Brugere*)

7. Moduler

Hvis formålet med sikkerheden også er at forhindre andre i at få adgang til og kopiere design og funktionalitet, så er man nødt til at sætte adgangskode på moduler. Moduler er, siden Access 2000, blevet adskilt fra den generelle sikkerhedsstyring. Man kan derfor ikke give individuelle tilladelser til moduler. Man kan kun angive en adgangskode for at få adgang til modulet.

Denne adgangskode angives ved, fra VBA-editoren, at gå i menuen Tools->[databasenavn] properties->Protection. I dialogboksen sætter man kryds i feltet **Lock project for viewing**, samtidig med at man angiver en adgangskode.

Note: Hvis man kun angiver adgangskode uden at sætte kryds i **Lock project for viewing**, så skal adgangskoden kun indtastes, hvis en bruger forsøger at åbne disse properties igen.

8. Kryptering

Systemet er nu meget sikkert. Det vil dog stadig være muligt, vha. en tekst-editor, at kigge en databasen igennem og se (og måske ændre) indholdet. Det er kompliceret, men det kan lade sig gøre. Vil man også fjerne denne potentielle risiko, kan man Kryptere/kode databasen. Kryptering vil sige, at man komprimerer og koder strukturen i databasen, således at indholdet vil forekomme som volapyk ved uautoriseret adgang (f.eks. vha. tekst-editor) For at denne kryptering virker optimalt, skal den være fortaget i en **unik arbejdsgruppe**, da den ellers kan de-krypteres af enhver bruger. Kryptering sløver, som tidligere nævnt systemet ned med ca. **10-15%**.

Opbygningen af sikkerheden

Det er nyttigt at vide, hvordan Access gemmer sikkerhedsoplysningerne. Det hjælper til at forstå hvilke ting, man skal være opmærksom på.

Sikkerheden i Access gemmes i 2 filer: arbejdsgruppefilen (f.eks. System.mdw) og den enkelte database.

I **System.mdw** gemmes oplysninger om de grupper og brugere, som er oprettet. For hver gruppe og bruger gemmes **PID-kode**, **brugernavn** og **adgangskode**.
I System.mdw gemmes **ingen** oplysninger om rettigheder til de enkelte databaser.

I den enkelte **database** gemmes derimod PID-kode samt oplysninger om brugerens/gruppens **rettigheder** på de enkelte objekter.

Det betyder i praksis, at hvis man har glemt adgangskoden til systemadministratoren, men man kan huske brugernavn og PID-kode, så kan man oprette en ny arbejdsgruppefil og en ny systemadministrator-konto og derved få adgang til databasen. For databasen kender ikke og bruger ikke adgangskoden!

Konklussion

Som det forhåbentlig fremgår af artiklen, er der mange ting, man skal tage stilling til inden man vælger sikkerhedsniveau og -ambition.

Højt sikkerhedsniveau
- Meget administration
- Større besvær for brugerne
- Større chance for fejl (brugere, som får de forkerte rettigheder)
- Større chance for at noget går 'galt'

Lavt sikkerhedsniveau
- Lettere administration
- Færre fejl

Ud fra disse oplysninger, skal man således vurdere om man har brug for *Fort Knox-modellen* eller om man evt kan nøjes med et "*Databaser skal behandles med varsomhed*"*-skilt*.

Min erfaring er, at langt de fleste virksomheder i virkeligheden blot ønsker at beskytte sig mod:

- *Utilsigtet fejl fra brugerne*
- *Selvudnævnte Access-programmører blandt medarbejderne, som mener, at de 'lige kan fix'e databasen'At*

Begge disse punkter kan langt hen ad vejen forhindres vha. backup af både frontend og backend, ligesom man kan sikre sig mod meget ved at konvertere frontenden til en .mde-fil.

Først når man virkelig ønsker at beskytte fortrolige oplysninger, bør man overveje at aktivere sikkerheden på databasen. Det være sig data eller kildekode.

Lad mig komme med et par råd og advarsler omkring arbejdet med sikkerhed:

- Tag altid backup inden du begynder at pille ved sikkerhedsindstillingerne
- Skriv altid disse oplysninger ned på papir og gem dem et sikkert sted: **Brugernavn, Personligt ID (PID) samt adgangskode på systemadministratoren**
- Hav altid mere end én systemadministrator på en applikation: folk bliver syge, folk bliver sure, folk bliver fyret, folk bliver glemsomme og folk dør!
- Hvis sikkerheden er sat korrekt op, er der stort set ingen vej ind i databasen, hvis administratorkontoen 'forsvinder'.

Jeg vil slutte af med, at sige, at der mange detaljer, som ikke er blevet belyst i denne vejledning. Men det må komme i...

I næste artikel...?

Sikkerhed er rigtig mange ting i Access. I kommende artikler kunne jeg (eller andre?) finde på at tage hul på nogle af følgende issues:
- Programmering af Access-sikkerhed vha VBA
- Flere arbejdsgrupper og forskellige genveje
- Forhindre adgang bag om systemet
- Programmere sin egen sikkerhed med egen login-boks m.m.
- ???

Tak for tålmodigheden :o)
Thomas Jepsen

Kommentar af bondester d. 26. May 2007 | 1

Tror ikke den findes bedre ;-) Takker...

Kommentar af -anders- d. 09. Jul 2004 | 2

Fantastisk gennemgang af sikkerhedsmuligheder i Access, det lige før man for lyst til at forsøge sig. Glæder mig allerede til næste artikel.

aandersen
(Anders)

Kommentar af dkoclni d. 02. Jun 2004 | 3

Super artikel Thomas! En rigtig god gennemgang af sikkerhedsopsætningen - både for begyndere og de mere avancerede. Glæder mig til at læse mere af samme skuffe!

Kommentar af mikkelk d. 05. Apr 2005 | 4

En meget velskrevet artikel!

Kommentar af luzk d. 01. Jun 2004 | 5

Kommentar af sjap d. 08. Aug 2004 | 6

Kanon artikel. Meget velskrevet med mange gode pointer.
Det lykkedes mig at finde en fejl i min egen opsætning af adgang til en backend, som ellers havde fået mig til at miskreditere Access' eget sikkerhedssystem (havde gjort det fra frontenden, og derfor virkede det ikke).
Og Thomas du får lige lavet noget mere af samme skuffe - så skal jeg nok finde 5 point mere til dig :0)

Kommentar af krydset d. 27. Jul 2004 | 7

smukt skrevet. Flot formulering.

Kommentar af trer d. 01. Jun 2004 | 8

Rigtig fin grundlæggende artikel. Et forslag; En senere artikel må gerne fortælle om Access som frontend for Oracle/SQL Server og om datasikkerhed (dvs. mod tab af data).

Kommentar af stejuu d. 17. May 2005 | 9

Fin let læselig artikel!

Kommentar af simonxx d. 07. Jun 2004 | 10

Vældig god artikel

Kommentar af flemming39 d. 10. Aug 2005 | 11

Tak for en meget grundig indføring i sikkerheds mulighederne i access.

Kommentar af epimp d. 14. Jul 2006 | 12

Dette afsnit har reddet min dag. Tusind tak.

"Det betyder, at alle databaser, som er oprettet af Administratoren (standard brugeren) kan åbnes af Administrator. Man kan ganske vist fjerne alle tilladelser fra Administratoren, men Administratoren kan til hver en tid gå ind og give sig selv alle tilladelser igen - fordi han er ejer! Ligeledes har medlemmer af gruppen Administatorer mulighed for at nulstille adgangskoder for andre brugere, hvorved de kan få fri adgang.
Er brugeren Administrator derimod ikke ejer af databasen, kan han helt udelukkes fra at måtte starte databasen, hvorved han heller ikke kan nulstille adgangskoder eller tildele sig selv rettigheder."

Kommentar af charlotterj d. 22. Nov 2004 | 13

Meget velskrevet og masser af gode pointer. Tror faktisk, at de fleste kan lære af denne artikel.

Kommentar af oehre d. 22. Oct 2006 | 14

Mange centrale pointer som jeg er overbevist vil løse op for en hårdknude eller 2 - og lige til at gå til. Sjældent set sammenfald af teknisk dybde og forklaringsmæssig ligefremhed! Godt gået!

Kommentar af tascha d. 17. Oct 2007 | 15

Kommentar af palle-toft d. 27. Oct 2009 | 16

Hej Thomas,

Tusinde tak for dit hurtige svar. Jeg er muligvis specielt dum og ubegavet. Jeg har gjort alt hvad du skriver, men jeg kan stadig sætte min ACCESS til at bruge system.mdw og vupti, så har jeg adgang til hele molevitten. Ejeren står så som "Ukendt bruger".

Må jeg ringe til dig og evt. købe en af dine timer?

PALLE TOFT

Kommentar af Christian_Belgien d. 21. Jan 2010 | 17

Jeg startede med at gennemgaa denne guide, men da jeg ville proeve at tilpasse indholdet til Access 2007 gav min soegning den information at sikkerhed paa brugerniveau ikke bliver understoettet i databaser af nyere typer saasom .accdb. Kan det vaere korrekt, eller har jeg misforstaaet?

Kommentar af wanthai d. 26. Oct 2012 | 18

En super fin gennemgang af hvordan manbør sætte sikkerheden op i en database.
Har besluttet mig for at bruge denne guide fremover.
Har bare det problem lige p.t. at jeg har en fakturerings-database, som jeg gerne vil have tilføjet lidt flere funktioner, men jeg har glemt min adgangskode.
Er der en genvej eller skal jeg helt forfra for at kunne benytte deen med de ønskede muligheder?
EWr lidt på spanden, da det er mange timers arbejde der i så fald ligger forude.
Håber meget på at du, eller en anden herinde har en løsning på mit problem.