

FileMaker® 8

Säkerhet



© 2004–2005 FileMaker, Inc. Med ensamrätt.

FileMaker, Inc.

5201 Patrick Henry Drive

Santa Clara, Kalifornien 95054, USA

FileMaker är ett varumärke som tillhör FileMaker, Inc., registrerat i USA och andra länder. ScriptMaker och logotypen för mappen är varumärken som tillhör FileMaker, Inc.

FileMakers dokumentation skyddas av lagen om upphovsrätt och det är därför inte tillåtet att mångfaldiga eller distribuera detta dokument utan FileMakers skriftliga medgivande. Dokumentationen får endast användas tillsammans med ett licensierat exemplar av FileMaker-programmet.

Samtliga personer och företag som förekommer i exempel är fiktiva och eventuella likheter med verkliga personer och företag är fullständigt oavsiktliga.

En lista över medverkande visas i dokumentet Tillskrivning som medföljer den här programvaran.

Mer information finns på webbplatsen www.filemaker.se.

Utgåva: 01

Innehåll

Kapitel 1

Databassäkerhet

Om denna handbok	5
Säkerhetsmål	5
Potentiella hot mot informationen	6
Planera säkerheten	7

Kapitel 2

Säkerhet – de 10 viktigaste punkterna

1. Förbättra den fysiska säkerheten	9
2. Förbättra operativsystemsäkerhet	9
3. Upprätta nätverkssäkerhet	10
4. Gör en plan för att skydda databasen	10
5. Begränsa dataåtkomsten med konton och behörigheter	11
6. Säkerhetskopiera databaser och andra viktiga filer	12
FileMaker Pro – filreparation	14
7. Installera, kör och uppgradera antivirusprogram	14
8. Testa säkerheten	14
9. Utvärdera och förbättra säkerheten fortlöpande	15
10. Uppgradera till FileMaker Pro 8 och FileMaker Server 8 för ökad säkerhet	15
Säkerhetsförbättringar i FileMaker Pro	15
Säkerhetsförbättringar i FileMaker Server	16

Kapitel 3

Bygga in säkerhet i lösningar

Begränsa åtkomsten med konton och behörighetsuppsättningar	17
Tips för att begränsa filåtkomst	18
Tips för att skapa effektiva lösenord	18
Att tänka på när du hanterar databaser med FileMaker Server	19
Säkerhetsöverväganden vid webbpublicering	20
Tips vid utformning av databaser för webbpublicering	20
Skydda databaser mot webbaserade intrång	22
Säkerhet på webbservern	23
Skydda data med kryptering och VPN-nätverk	23
Använda SSL-säkerhet vid webbpublicering	23
Trådlösa nätverk	23
Att tänka på vid XML-användning	24
Att tänka på vid användning av Apple Events och ActiveX	24

Kapitel 1

Databassäkerhet

Med programmet FileMaker® Pro kan du skapa databaser som kan användas individuellt, delas i serverlösa nätverk, delas med hjälp av FileMaker Server, via ODBC eller JDBC, eller delas med intranät- eller Internet-användare. Det är viktigt att fundera på vilken typ av information som ska delas, vilka sårbara punkter som finns och hur informationen och databasfilerna ska kunna skyddas.

I vissa situationer är informationen inte särskilt känslig eller kritisk för företagsverksamheten.

Själva programmet kan användas av en person på en säker plats eller i en öppen miljö där säkerhetsaspekterna är av mindre betydelse. I de allra flesta fall är dock informationen antagligen företagskritisk eller känslig på annat sätt och du måste vidta åtgärder för att skydda den. Du bör planera och införa säkerhet i alla faser av design, testning och utveckling.

Om denna handbok

- Detta dokument handlar om säkerhetsfrågor för FileMaker-versionerna 7 och 8. Om du vill veta mer om säkerhet för tidigare versioner av FileMaker Pro, hämtar du dokumenten från www.filemaker.se.
 - Om du vill ha den senaste informationen om säkerhetsfrågor för FileMaker kan du besöka supportwebbsidan för FileMaker Säkerhet på www.filemaker.se/filemakersupport, där du kan abonnera på ett nyhetsbrev om säkerhetsfrågor.
 - Stegvisa instruktioner om FileMaker Pro-funktioner, bland annat information om hur du definierar konton och behörighet för att skydda databasfiler, finns i FileMaker Pro Hjälp.
 - I FileMaker Pro-dokumentationen används uttrycket *webbpublicering*. Det refererar till databaser som användare kan komma åt via Internet eller ett intranät med hjälp av en webbläsare.
 - I denna handbok avser termen "FileMaker Pro" både FileMaker Pro och FileMaker Pro Advanced, utom när specifika funktioner i FileMaker Pro Advanced beskrivs.
- Viktigt!** Du kan hämta FileMaker 8-dokumentation i PDF-format från www.filemaker.se/fmdownloads. Uppdateringar av det här dokumentet kan du också hämta från webbplatsen.

Säkerhetsmål

När du skyddar FileMaker-databaser bör du framförallt tänka på tre saker:

- Sekretess
- Integritet
- Tillgänglighet

Sekretessbelagd information

När du utformar och distribuerar en databas, är det ditt ansvar att se till att obehöriga personer inte kan få åtkomst till informationen.

Dataintegritet

Utforma ett system som är tillräckligt öppet för att behöriga användare ska kunna skapa och uppdatera data samtidigt som det inte ska gå att göra oavsiktliga ändringar. Du måste även begränsa åtkomsten för obehöriga användare som kan försöka göra ändringar i filerna. Tyvärr finns det personer som försöker komma åt dina informationssystem och stjäla företagets tillgångar.

Tillgänglighet

Databaser bör endast vara tillgängliga för användare när det behövs. Detta är en grundläggande, men ofta förbisedd, aspekt. Databasutvecklare och nätverksadministratörer måste inte bara vidta åtgärder mot intrång från okända personer, utan också mot anställda som har större behörighet än vad som behövs. Ha som mål vid utformningen att låta användare komma åt både data och olika funktioner, men bara de användare som verkligen behöver dem. Aktivera inga delningsalternativ, till exempel webbpublicering, förrän det är nödvändigt.

Potentiella hot mot informationen

Du måste skydda dina data och databasutformningen från både oavsiktliga och avsiktliga ändringar. Någon kan försöka kopiera delar av utformningen, läsa informationen som dina användare har skrivit, förstöra systemet (kanske via någon annans användar-ID), ange falska data, förstöra dina rapporter och layouter, fördärva beräkningar eller förstöra manus.

De vanligaste hoten mot data är följande:

- Oavsiktliga hot från kända personer samt olyckor. Behöriga användare kan begå misstag, läsa information de inte bör, ta bort eller ändra poster de inte borde ha åtkomst till och ta bort eller skada filer så att systemet blir oanvändbart.
- Avsiktliga hot från kända personer. Det finns personer som vill komma åt information de inte borde se, som kan förfalska eller avsiktligt försöka förstöra informationen.
- Hot från oinbjudna personer eller hot från okända personer. Denna typ av hot är oftast Internet-baserade hot från obehöriga personer med anonym åtkomst som försöker stjäla information, orsaka skada eller göra webbsystem oanvändbara.

Det är viktigt att inse att små företag och större arbetsgrupper oftast möter samma typ av hot, särskilt på Internet. Anställda i små företag och personer med hemkontor tror ibland att de är säkra eftersom de håller en låg profil, men det stämmer tyvärr inte. Det finns obehöriga personer som använder automatiska verktyg för att söka efter och bryta sig in i sårbara system. Informationens värde brukar oftast avgöra hur mycket tid och resurser en hackare lägger ner på att försöka ta sig in i ett system. Målet med attacken är ofta att hitta ett system som kan användas för att vilseleda spåren efter en attack på ett större mål.

Små företag är vanligtvis enklare att ta sig in i, eftersom de ofta saknar ett bra skydd mot omvärlden (till exempel brandväggar som underhålls av erfarna nätverksadministratörer) och inte har några tydliga säkerhetsprocedurer för sina datorsystem (alla datorer kanske inte använder den senaste versionen av operativsystemet).

Inkräktare försöker ofta komma åt informationen i en arbetsgrupp eller ett litet företag. Ibland är målet med en attack att inaktivera systemet, men det är vanligare att man försöker komma åt känslig information, till exempelvis kreditkortsnummer eller identifieringsinformation, till exempel lösenord och personnummer. Inkräktare antas ofta befinna sig långt från arbetsgruppen och ha mycket begränsad kunskap om systemet. De använder automatiska manus för att leta upp system med välkända svagheter. Det behövs endast ett fåtal säkerhetsfunktioner för att de ska välja ett annat mål.

Planera säkerheten

Börja genom att bekanta dig med de inbyggda säkerhetsfunktionerna i FileMaker Pro: konton och behörigheter. Överväg en flexibel säkerhet i flera skikt och ett fortsatt säkerhetsarbete efter den inledande insatsen.

- Säkerhetsplanen bör vara tillräckligt flexibel för att olika åtkomstbehov ska kunna tillgodoses.
- Lägg in säkerhet på varje åtkomstnivå: lås datorer, aktivera konton och behörigheter i databaser, begränsa åtkomsten till kataloger och vidta andra åtgärder för att skydda informationen.
- Utvärdera säkerheten med jämna mellanrum för att se till att informationen fortfarande skyddas. Detta kan innebära att se till att användarna har den senaste versionen av olika program, att lösenorden ändras med jämna mellanrum, att loggfiler utvärderas och granskas och att till punkt och pricka följa uppställda säkerhetsscheman. Konfigurera och testa säkerheten när du lägger till struktur och data i filerna med tiden.

Tabellen nedan visar exempel på hur en utvecklare eller nätverksadministratör kan uppskatta risker på en arbetsplats.

Förutsättning på arbetsplatsen	Huvudsakliga säkerhetsproblem
Oerfaren datorpersonal, stor personalomsättning, nya datoranvändare	Stor risk för oavsiktliga hot som framförallt orsakas av datainmatningsmisstag och dåliga rutiner för säkerhetskopiering.
Oerfarna databasutvecklare	<ul style="list-style-type: none"> • Stor risk för oavsiktliga hot som utgörs av att personal har olämplig åtkomst till fil- och databasfunktioner. • Personal kan utgöra oavsiktliga hot genom att dela filer utan att vidta lämpliga säkerhetsmått. • Informationen blir utsatt om FileMaker Pro-konton och -behörigheter inte konfigureras så att filerna skyddas på rätt sätt.
Oerfarna nätverksadministratörer	<ul style="list-style-type: none"> • Stor risk för oavsiktliga hot som framförallt utgörs av otillräcklig operativsystemsäkerhet och dåliga rutiner för säkerhetskopiering. • Dålig nätverkssäkerhet ökar risken för avsiktliga hot, särskilt om filerna delas över Internet eller ett trådlöst nätverk. • Risker uppstår även om delade filer hämtas från filserverar i stället för den inbyggda nätverksdelningen i FileMaker Pro och FileMaker Server. Personal kan göra otillåtna kopior av filer och kan orsaka låsning av poster. Det finns även risk för skada när filerna delas på olämpliga sätt.
Dålig fysisk säkerhet	Hög risk för avsiktligt hot (stöld av datorutrustning).

Förutsättning på arbetsplatsen

Huvudsakliga säkerhetsproblem

Databasen innehåller känsliga eller värdefulla data

Ökad risk för avsiktligt hot (stöld av data), särskilt om informationen delas över Internet eller om åtkomsten till informationen inte bevakas och skyddas på lämpligt sätt.

Kapitel 2

Säkerhet – de 10 viktigaste punkterna

Se till att databasfilerna, värddatorerna, arbetsstationerna och de nätverk som använder dem är skyddade mot stöld och skada. Det här kapitlet beskriver tio säkerhetsåtgärder du kan vidta för att skydda din information och utrustning. De 10 viktigaste säkerhetsåtgärderna är följande:

- Förbättra den fysiska säkerheten
- Förbättra operativsystemsäkerhet
- Upprätta nätverkssäkerhet
- Gör en plan för att skydda databasen
- Begränsa dataåtkomsten med konton och behörigheter
- Säkerhetskopiera databaser och andra viktiga filer
- Installera, kör och uppgradera antivirusprogram
- Testa säkerheten
- Utvärdera och förbättra säkerheten fortlöpande
- Uppgradera till FileMaker Pro 8 och FileMaker Server 8 för ökad säkerhet

Var och en av dessa åtgärder beskrivs närmare i det här kapitlet.

1. Förbättra den fysiska säkerheten

Utvärdera datorerna och se till att de är fysiskt säkra:

- Värddatorn bör vara en dedicerad dator, fast förankrad vid ett bord eller fastlåst med ett lås. Datorn bör vara förankrad så att det är omöjligt att avlägsna hårddisken. Begränsa åtkomsten till datorn genom att förvara den i ett låst rum.
- Förankra arbetsstationerna som har åtkomst till databasen. Lås datorerna och begränsa åtkomsten genom att använda skärmläckare som kräver lösenord.
- Se till att säkerhetskopior som lagras på bärbara medier, till exempel band och cd-skivor, förvaras på en säker plats.

2. Förbättra operativsystemsäkerhet

Begränsa åtkomsten till viktiga data med operativsystemets säkerhetsfunktioner.

Nätverksadministratören bör endast ge behörighet åt användare som administrerar eller underhåller systemet eller FileMaker-databaserna. Nätverksadministratören bör dessutom göra följande:

- Spåra systemanvändar-ID och lösenord.
- Begränsa åtkomsten till FileMaker Pro-programmet samt till filkataloger, servrar och webbsidor.
- Granska inställningarna för fildelning och FTP vid fjärranslutning.
- Begränsa möjligheterna att överföra och hämta filer.
- Se till att alla användare har den senaste versionen av operativsystemet.

- Förenkla hanteringen genom att aktivera extern autentisering. Då används konton som har konfigurerats i Windows Domain Authentication (Windows-domänautentisering) eller Apple OpenDirectory. Mer information finns i ”Säkerhetsförbättringar i FileMaker Server” på sidan 16.
- Dela inte FileMaker Pro-filerna genom att lägga upp dem på filserverar. Använd i stället den inbyggda nätverksfunktionen i FileMaker Pro och FileMaker Server. Det förhindrar att filer kopieras på olämpligt sätt och att poster låses. Även risken för skada när filerna delas på olämpliga sätt undviks.

3. Upprätta nätverkssäkerhet

Databaser som delas i ett intranät eller på Internet använder protokollet TCP/IP. Detta protokoll kan också användas vid databasdelning i serverlösa nätverk eller med FileMaker Server. Även om TCP/IP är bra för att överföra data och låta klienter komma åt din information, lades ingen stor vikt vid säkerheten när protokollet utformades. Om du inte vidtar särskilda åtgärder kan protokollet göra det möjligt för obehöriga att komma åt datorn, serverprogrammet, databaserna och till och med andra klientdatorer i det interna nätverket. TCP/IP kan inte skydda dina data, så det är viktigt att du lägger hinder i vägen, till exempel brandväggar och SSL-datakryptering, för oinbjudna besökare. Mer information om produkter från andra företag, bland annat krypteringsprogram, finns i ”Skydda data med kryptering och VPN-nätverk” på sidan 23.

- Den vanligaste skyddsmetoden är brandväggen, som delar upp nätverket i två separata miljöer: en offentlig miljö ”utanför brandväggen” och en privat miljö ”innanför brandväggen”. Användare utanför brandväggen har endast tillgång till de TCP/IP- eller maskinvaruadresser som görs tillgängliga. Du kan koncentrera säkerheten till de serverdatorer som är utsatta, samtidigt som de datorer som befinner sig innanför brandväggen inte kräver ett lika starkt skydd.
- Användning av trådlösa nätverksenheter, till exempel Apple AirPort och andra nätverkskort enligt 802.11b-standard och basstationer, kan utgöra säkerhetshot eftersom dessa enheter kan sända nätverkstrafiken bortom kontorets väggar. Det är därför extra viktigt att kryptera nätverkssignaler från trådlösa enheter. Använd alltid den högsta nivån på signalkryptering som finns. Mer information finns i ”Trådlösa nätverk” på sidan 23.

4. Gör en plan för att skydda databasen

När du planerar utformningen av FileMaker-databasen bör du även planera hur du ska garantera säkerheten för databasfilerna. Det är mycket enklare att lägga in säkerhet i databasen redan från början, än att senare införa den.

- Skriv ned vilka områden du vill skydda, till exempel särskilda tabeller, fält, poster, layouter, värdelistor och manus. Planera hur många behörighetsuppsättningar du måste skapa för de olika nivåer av åtkomst som behövs.

- Bestäm om det behövs enskilda konton för varje användare (rekommenderas) eller om det räcker med konton som flera användare kan dela (till exempel ett konto för ”marknadsföring” och ett för ”försäljning”).

Det är möjligt att skapa ett litet antal konton som delas mellan många personer (t.ex. kontot ”Marknadsföring” eller ”Försäljning”). Kom emellertid ihåg att delade konton är en säkerhetsrisk. Om du vill ha bättre säkerhet ska du använda enskilda konton istället för delade konton. Om du ändå tänker använda delade konton, ska du se till att begränsa behörigheten för de behörighetsuppsättningar som de delade kontona använder. Ändra lösenord ibland, speciellt när vissa användare inte längre behöver åtkomst.

- Bestäm om Gästkontot ska aktiveras. Gästkontot tillåter användare att öppna filer utan att behöva logga in eller ange kontoinformation. Om du använder Gästkontot bör du tilldela det den mest begränsade behörigheten.
- Bestäm om det behövs utökad behörighet (till exempel Delning via FileMaker-nätverk eller Direkt webbpublicering) för vissa behörighetsuppsättningar.
- Skapa de konton du behöver i filen och tilldela varje konto en behörighetsuppsättning.

Fundera på att göra ett schema som visar vilka typer av användare som finns och vilka behörigheter de har:

Typ av användare	Visa poster	Lägga till poster	Ändra poster	Radera poster	Ändra manus	Köra manus	Ändra värdelistor	Menyer
Chefer	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Alla
Marknadsföring	Ja	Ja	Ja	Begränsad*	Begränsad*	Ja	Nej	Endast redigering
Försäljning	Ja	Ja	Ja	Begränsad*	Nej	Ja	Nej	Endast redigering
Personal	Ja	Ja	Ja	Ja	Ja	Ja	Nej	Alla
Juridiska	Ja	Nej	Nej	Nej	Nej	Ja	Nej	Minimum
Gäster	Ja	Nej	Nej	Nej	Nej	Nej	Nej	Minimum

*Du kan ge begränsad åtkomst till vissa funktioner, till exempel för att radera poster, genom att använda olika behörigheter för olika poster. Mer information om behörigheter för poster finns i hjälpen till FileMaker Pro.

5. Begränsa dataåtkomsten med konton och behörigheter

Konton och behörigheter är den vanligaste säkerhetsmetoden för FileMaker Pro-filer. Med konton och behörigheter kan du begränsa vad användarna ska få se och göra i en databasfil. Du kan begränsa följande:

- Filåtkomst: Användare måste ange ett kontonamn och ett lösenord för att kunna öppna en fil.
- Dataåtkomst: Gör vissa poster och fält från olika tabeller skrivskyddade eller dölj dem helt och hållet.
- Layoutåtkomst: Hindra användare från att visa och ändra layouterna i layoutläge.

- Åtkomst till värdelistor och manus: Hindra användare från att visa och ändra värdelistor och från att köra manus.
- Skriva ut/exportera data: Hindra användare från att skriva ut eller exportera data.
- Menyåtkomst: Gör endast en begränsad uppsättning menykommandon tillgängliga.

När filåtkomsten begränsas med konton, måste användaren känna till kontonamnet och lösenordet för att kunna öppna eller ansluta till en databas. Det kontonamn och lösenord användaren anger bestämmer vilka behörigheter som aktiveras, vilket i sin tur styr vad användaren kan göra i en fil. Mer information om konton och behörighetsuppsättningar finns i ”Begränsa åtkomsten med konton och behörighetsuppsättningar” på sidan 17.

Tips

- Säkerheten är bara så bra som de konton och lösenord du definierar. Mer information finns i ”Tips för att skapa effektiva lösenord” på sidan 18.
- Lämna inte ut ditt administratörskontonamn och -lösenord till någon. Om endast du har den informationen är filerna skyddade i den händelse den fysiska säkerheten, operativsystemsäkerheten eller nätverkssäkerheten kringgås.
- Du kan konfigurera FileMaker Server så att databaser kan utföra extern serverautentisering baserat på gruppnamn i stället för konton/lösenord som är lagrade i databasen. Om du vill öka säkerheten ska du inte tilldela behörighetsuppsättningen Fullständig behörighet till en kontotyp för extern server. Mer information finns i ”Säkerhetsförbättringar i FileMaker Server” på sidan 16.

Viktigt! En ny FileMaker Pro-fil är från början helt oskyddad. När användarna öppnar filer loggas de automatiskt in med administrationskontot, som har fullständig behörighet. Hindra andra från att öppna databasen med fullständig behörighet genom att ändra namn på administrationskontot och tilldela ett lösenord. Innan du delar filen med andra bör du planera säkerheten för filen och tilldela varje användare åtkomstbehörighet.

6. Säkerhetskopiera databaser och andra viktiga filer

Utveckla rutiner för återställning av data, bland annat alternativa platser och system där företagskritiska tjänster kan köras. En aktuell säkerhetskopia kan hjälpa dig att återställa systemet från en situation där någon förlorar administrationskontoinformationen för en fil eller en situation där ett användarfel (och ibland en dålig databasdesign) gör att informationen raderas eller ändras på felaktigt sätt.

Tänk på följande:

- Använd FileMaker Server som värd för databaser och gör regelbundna, automatiska säkerhetskopieringar.

Använd inte program för säkerhetskopiering från externa leverantörer på en delad FileMaker Pro-databas. Använd först FileMaker Server och gör en säkerhetskopia av din databas. Kör sedan säkerhetskopieringsprogrammet från den externa leverantören på kopian. Program för säkerhetskopiering kan förstöra öppna, delade databaser.

Du kan till exempel göra lokala säkerhetskopior av filer klockan 6:00, 9:00, 12:00, 15:00, 18:00 och 23:30 under arbetsdagar. Vid midnatt kan företagets säkerhetssystem göra en inkrementell säkerhetskopiering av hela systemet. Under fredagsnatten kan du slutligen göra en fullständig säkerhetskopiering av hela systemet. Kopiera och förvara säkerhetskopiorna på en annan plats. Om servern går ner av någon annan orsak än ett katastrofalt fel på flera enheter, kan du använda den senaste versionen av säkerhetskopian, vilket innebär att du har förlorat högst 3 timmars data. Om ett katastrofalt fel uppstår på en eller flera enheter, kan du använda föregående kvälls säkerhetskopia, vilket innebär att du har förlorat högst en dags data. Dessa rutiner kan naturligtvis skräddarsys efter olika situationer och olika informationsvärde.

- Se till att säkerhetskopiorna skyddas från skada och att de är tillgängliga. Kontrollera att de fungerar som de ska *innan* du behöver dem. Kör diagnostikprogram på hårddisken och säkerhetskopiorna med jämna mellanrum.
- Kontrollera att du kan återställa en hel uppsättning filer från säkerhetskopian.
- Skydda filerna från att skadas genom att regelbundet exportera informationen.
- Skydda själva säkerhetskopian. Förvara säkerhetskopiorna på en separat och brandsäker plats.
- Utse reservadministratörer som kan hämta filer, ifall nätverksadministratören inte är tillgänglig.
- Planera för redundans. Om det blir strömavbrott kan ett UPS-aggregat behålla strömmen i åtminstone 15 minuter, vilket ger dig tid att stänga alla filer. Om du inte kan återställa strömmen i tid, bör du överväga att använda en generator för att försörja serverna med ström. Överväg även att använda strömkällor för routrar och brandväggar. Blir kommunikationen ett problem ifall Internet-åtkomsten bryts under 48 timmar eller mer?
- Fundera på hur du ska kunna upprätthålla tjänster om ett intrång låser databasen och servern inte kan återställas till sitt föregående läge.
- Tänk dig in i fler scenarier. Vad kan hända? Hur kan du vara förberedd för olika situationer?

Nätverksadministratörer bör även granska hot mot datasystem och företagskritiska funktioner. Exempel:

- Stöld av data eller intellektuell egendom.
- Avbrott, stöld eller skada på nätverksinfrastrukturen, till exempel servrar, nätverk, datalagring och förvaring av säkerhetskopior. Skada kan orsakas av "lösenordsknäckare" eller andra typer av sabotage. De flesta skador kommer inifrån företaget eller organisationen.
- Avbrott i eller skada på företagets infrastruktur, till exempel brandväggar, miljömässiga eller biologiska risker, översvämning m.m.
- Avbrott i eller skada på den offentliga infrastrukturen, till exempel elenergi, telekommunikation (röst och data), transporter (vägar, bussar, tåg) som orsakas av miljömässiga situationer eller dåliga väderförhållanden, till exempel snöstorm eller översvämning.

Viktigt! Om ett allvarligt serverfel uppstår, till exempel ett oväntat strömavbrott, fel på hårddiskar eller fel på program, använder du säkerhetskopiorna. Alla typer av systemfel som får FileMaker Server att stängas av på fel sätt kan resultera i skadade filer, om data i cachén inte hann sparas på disk och filerna inte stängdes på rätt sätt. Även om filerna kan öppnas och du gör en kontroll eller reparation, kan dolda fel ha uppstått i filen. Filreparation är ingen garanti för att problemet har åtgärdats.

FileMaker Pro – filreparation

Använd reparationsfunktionen när en databasfil stängs på fel sätt och informationen efter den senaste säkerhetskopieringen måste återställas. Vid reparationen skapas en ny fil med ett annat namn än originalfilen eftersom det inte är tänkt att den nya filen ska ersätta den gamla. Detta är en ”rå” process som kan ta bort layouter, manus m.m. i syfte att återställa så mycket information som möjligt. Informationen bör exporteras från reparationsfilen och importeras i en ny säkerhetskopia av originalfilen.

Eftersom reparation kan ta lång tid, bör du göra lokala säkerhetskopior med jämna mellanrum, beroende på hur ofta informationen ändras.

7. Installera, kör och uppgradera antivirusprogram

Eftersom de flesta datorer har Internet-återkomst är de sårbara för virus som överförs med bifogade e-postfiler. Se till att alla anställda använder ett antivirusprogram och att de känner till de vanligaste virustecknen. Anställda bör skanna sina filer innan de kopierar eller överför dem till sina datorer. De bör aldrig öppna okända e-postbilagor, även om de kommer från någon de känner.

Obs! Kör inte program för viruskydd på öppna, delade databaser. Stäng först databasen och kör sedan programmet för viruskydd.

8. Testa säkerheten

Det är viktigt att testa alla scenarier för att vara säker på att användarkontona fungerar som förväntat med alla fildelningsmetoder.

Exempel:

- Öppna filen med olika användarkonton och testa varje behörighet som du har skapat. Se till att begränsningarna fungerar som de ska och gör eventuella justeringar.
- Testa navigering och manus med alla användarkonton. Eftersom konton har olika behörigheter kanske inte alla funktioner, som layouter, tabeller och manus, fungerar för alla användare.
- Om användare använder databasen på olika sätt, till exempel på Internet med Direkt webbpublicering, XML eller JDBC, testar du även kontona där dessa tekniker används.
- Om du publicerar filer på Internet öppnar du manus och aktiverar **Ange webbkompatibilitet**, så att du ser att alla steg stöds. Om ett manus innehåller steg som inte är webbkompatibla, kan du använda manussteget **Tillåt användaren att avbryta**, för att avgöra hur efterföljande steg ska hanteras. Mer information finns i *FileMaker Handbok för direkt webbpublicering*, som finns i mappen Elektronisk dokumentation (i mappen Svenska – Extra).
- Testa för oväntade resultat. Du kan till exempel öppna filer med olika användarkonton och försöka utföra åtgärder som användarna inte ska kunna göra. Ta bort åtkomst till behörighetsuppsättningar så långt det är möjligt.
- Be andra utvecklare försöka komma åt informationen på felaktiga sätt.
- Kör tester med jämna mellanrum, inte bara under utvecklingen, utan även efter distribuering av databasen.

9. Utvärdera och förbättra säkerheten fortlöpande

Det är viktigt att testa säkerheten fortlöpande. När nya användare till exempel använder databasen, bör du utvärdera åtkomst till informationen och till databasstrukturen, beroende på vilka arbetsuppgifter eller ansvarsområden den nya användaren har.

Ställ följande frågor till dig själv innan du utvecklar en FileMaker Pro-databas och sedan med jämna mellanrum:

- Vad är värdefullt?
- Varför är det värdefullt?
- Hur värdefullt är det?
- Hur allvarligt skulle förlust eller avslöjande av informationen vara?
- Vilken är den minsta säkerhetsnivån som behövs för att förhindra förlust eller avslöjande?
- Vilka verktyg kan jag använda för att införa den säkerheten?

Utvärdera säkerheten genom att aktivera loggfiler i FileMaker Pro och FileMaker Server och granska användarens åtgärder. Du kan även spåra åtgärder om du inkluderar manus och beräkningar som registrerar användarkontots namn, lösenord och IP-adress.

10. Uppgradera till FileMaker Pro 8 och FileMaker Server 8 för ökad säkerhet

Säkerhetsmodellen har gjorts om i FileMaker Pro 7 och FileMaker Server 7. Om du uppgraderar från en version före version 7 använder du den nya säkerhetsmodellen för att göra programmet mer robust och strömlinjeformat för användarna vid tilldelningen av konton och behörighetsuppsättningar.

Säkerhetsförbättringar i FileMaker Pro

- Den nya säkerhetsmodellen är mer intuitiv och fungerar ungefär som andra verktyg. Du kan skapa användarkonton och lösenord och dela behörigheter för flera användare och tabeller.
- FileMaker Pro stöder flera tabeller i en enda fil. Därför kan du nu skydda en databas bestående av en enda fil med flera tabeller, med hjälp av en enda uppsättning konton och behörighetsuppsättningar.
- Du kan använda funktionen Get(kontonamn) för att se vem som använder funktioner och manus. Detta banar väg för många nya möjligheter, bland annat möjligheten att skapa manus som endast kan köras av ett visst kontonamn.
- Du kan kräva att användarna anger ett nytt lösenord nästa gång de öppnar databasen eller aktivera inställningar som kräver att användarna ändrar sina lösenord efter ett visst antal dagar.
- Du kan ange att användarna måste ange ett lösenord med minst ett visst antal tecken.
- FileMaker använder en envägsalgoritm för kryptering av kontonamn och lösenord, detta förhindrar att lösenorden avkodas med verktyg för att ”knäcka lösenord”. Användarens kontonamn och lösenord verifieras på värddatorn, vilket förhindrar intrångsförsök på klientdatorn och försök att avkoda lösenordet med de körbara filerna eller temp-filerna. Du måste spara kontonamnet och lösenordet på en säker plats. Om du tappar bort kontonamnet och lösenordet måste du skapa om filerna.

Säkerhetsförbättringar i FileMaker Server

När du hanterar databaser med FileMaker Server kan du dra fördel av ett antal funktioner som gör informationen säkrare för både FileMaker Pro-användare och webbaserade klienter. Information om specifika funktioner finns i *FileMaker Server Advanced Installationshandbok för webbpublicering* och i *FileMaker Server Administratörshandbok*.

- Om du vill kryptera kontoinformationen och informationen med hjälp av FileMaker-nätverk aktiverar du **Säkra anslutningar till FileMaker Server**.
 - Om du delar filer på webbaserade klienter aktiverar du SSL-kryptering i ett webbserverprogram för att kryptera data som överförs från värddatorn till gästdatorerna på Internet. Mer information finns i ”Använda SSL-säkerhet vid webbpublicering” på sidan 23.
 - Du kan aktivera och inaktivera specifik utökad behörighet, till exempel Direkt webbpublicering, XML och XSLT för Web Publishing Engine. Om du till exempel vet att alla filer på en server kommer att delas med Direkt webbpublicering, kan du inaktivera alla andra typer av webbpublicering. Även om en fil innehåller utökad behörighet som ger åtkomst till XML-data, är åtkomsten till XML-data inte tillgänglig när filen hanteras med Web Publishing Engine. Mer information finns i *FileMaker Server Advanced Installationshandbok för webbpublicering*.
 - Om din organisation använder centralt hanterad autentisering för användare och grupper, till exempel Apple OpenDirectory eller en Windows-domän, kan du skapa konton (baserade på autentiseringsservern) som autentiserar användare. Det gör att du kan använda den befintliga servern för att styra åtkomsten till databaser utan att behöva hantera en fristående lista över konton i varje FileMaker Pro-databasfil. Mer information om autentiseringskonton med externa servrar finns i FileMaker Server Hjälp.
- Viktigt!** När en databasfil innehåller ett eller fler externa serverkonton måste du använda säkerhetsinställningarna i operativsystemet när du vill begränsa direktåtkomst till filen. Om du inte gör det kanske obehöriga användare kan flytta filen till ett annat system som replikerar miljön på din autentiseringsserver och på så sätt få åtkomst till filen. Gruppnamn för konton som autentiseras med den externa serverfunktionen lagras som textsträngar. Om gruppnamnet reproduceras på ett annat system kan obehöriga få åtkomst till den kopierade filen med samma behörigheter som medlemmarna i gruppen har, vilket innebär att data kan visas på olämpligt sätt.
- Aktivera loggfiler och funktioner för säkerhetskopiering så blir databasunderhållet enkelt och effektivt.

Kapitel 3

Bygga in säkerhet i lösningar

Utvecklare och nätverksadministratörer måste ta ansvar för säkerheten vid utveckling och distribution av sina databasfiler och att se till att säkerheten upprätthålls.

Begränsa åtkomsten med konton och behörighetsuppsättningar

Den enklaste och bästa metoden för att skydda filerna är att definiera konton och behörighet i FileMaker Pro. Det är en god idé att begränsa åtkomsten till alla filer med ett administrationslösenord som bara du känner till. Då är filerna skyddade även om andra säkerhetsåtgärder skulle kringgås.

Viktigt! Information om hur du kan konvertera säkerhetsinställningar i databaser från versioner tidigare än version 7 till den aktuella versionen av FileMaker Pro finns i *Konvertera FileMaker-databaser från tidigare versioner*. I FileMaker-hjälpen finns utförlig information och stegvisa anvisningar om kontonamn, lösenord och behörighet.

Med *konton* autentiseras användare som försöker öppna skyddade filer.

- För varje konto anges ett kontonamn och (helst) ett lösenord.
- Varje databasfil innehåller två fördefinierade konton: Admin och Gäst. Admin-kontot, som du bör ge ett annat namn för bättre säkerhet, har fullständig behörighet. Gästkotot, som du inte kan ändra namn på, tillåter användare att öppna en fil utan att ange kontonamn och lösenord. Som standard tilldelas gästkontot Endast läsbehörighet, men du kan tilldela annan behörighet i Konton och behörighet.
- Varje enskild användare bör om möjligt tilldelas ett unikt konto.

Behörighet anger en viss behörighetsnivå till en databasfil. Varje databasfil innehåller tre fördefinierade behörigheter: Full åtkomst, Endast datainmatning och Skrivskyddad åtkomst.

- Varje konto tilldelas en behörighet som anger behörighetsnivån när någon öppnar en fil med det kontot.
- Du kan skapa behörigheter för att begränsa åtkomsten till databasen. Du kan till exempel ange vilka layouter och menyer som ska vara tillgängliga och om det ska gå att skriva ut eller inte. Med behörighet kan du också begränsa åtkomsten till särskilda poster eller fält i en fil.

Med *Utökad behörighet* bestämmer du vilka datadelningsalternativ som tillåts för en viss behörighet. Du kan aktivera behörighet för tillgång till filer som delas i ett FileMaker-nätverk, via Direkt webbpublicering, Egen webbpublicering med XML eller XSLT, från ODBC- eller JDBC-klienter och FileMaker Mobile. All utökad behörighet är som standard inaktiverad.

Viktigt! För maximal säkerhet bör du skapa konton som kräver användarnamn och lösenord för alla filer. Utnyttja de nya säkerhetsfunktionerna genom att uppmana användarna att ändra lösenord efter en viss tid och genom att ange att lösenord måste bestå av ett visst antal tecken.

Tips för att begränsa filåtkomst

- Undvik automatisk inloggning med kontonamn och lösenord angivna i dialogrutan Filtillval.
- Att använda samma lösenord i varje fil är ofta praktiskt när användarna måste arbeta med flera databasfiler i en session. Detta fungerar inte längre när användarna ändrar sina lösenord (såvida de inte ändrar lösenorden i alla filer). När du skapar konton måste du skapa dem i alla databasens filer. Det är praktiskt att definiera flera tabeller i en och samma fil. Överväg att hantera filer med FileMaker Server och att använda en extern autentiseringsserver, till exempel en Windows-domän eller Apple OpenDirectory. Mer information finns i ”Säkerhetsförbättringar i FileMaker Server” på sidan 16.
- Om konton används av flera personer bör du byta lösenord med jämna mellanrum. Du bör också ändra kontonamnet och lösenordet när någon lämnar arbetsgruppen.
- Skapa en startfil som endast samverkar med kritiska filer via manus. Startfilen lagrar inga data, däremot flyttas data till mer kritiska filer via manus. Låt användarna öppna filen med sina vanliga kontonamn och lösenord som begränsar åtkomsten till känsliga data och riskabla funktioner, som att radera poster. Manusen kan utföra åtgärder som du inte skulle ge användarna behörighet att utföra, som att radera poster, genom att aktivera Kör manus med fullständig behörighet.
- Du kan ange behörighet för poster som ger användaren rätt att visa, redigera och ta bort vissa poster i varje tabell. Begränsa användarens åtkomst till vissa poster, baserat på ett antal villkor, till exempel avdelning, befattning, ansvarsområden m.m. Mer information om behörighet för poster finns i FileMaker Pro Hjälp.

Viktigt! Att begränsa åtkomsten till vissa poster kräver en mer komplicerad dataåtkomstmodell. Testa lösningen noggrant genom att logga in med olika användarkonton och utvärdera alla layouter, rapporter och manus. Dokumentera alltid särskilda villkor som måste uppfyllas, så att användarna vet vad de kan förvänta sig.

- Använd inte layouter för säkerhet. Det enda sättet att skydda filer, från till exempel CGI-anrop eller andra källor, är att begränsa åtkomsten på fält- eller tabellnivå. Mer information om hur behörigheter för layouter och poster samverkar finns i avsnittet FileMaker Pro Hjälp.
- Om du konverterar databaser från versioner tidigare än version 7.0 av FileMaker Pro ska du se till att granska alla filreferenser i din lösning och ta bort dem du inte behöver. Dialogrutan Filreferens visar information som mappplaceringar och IP-adresser. Detta kan avslöja information som du inte vill sprida. Granska loggfilen för konverteringen för att se status och om eventuella problem påträffats under konverteringen. Mer information finns i *Konvertera FileMaker-databaser från tidigare versioner*.
- Med FileMaker Pro Advanced kan du permanent ta bort behörighetsuppsättningen Fullständig behörighet och alla konton som använder den behörigheten (även Admin-kontot). Denna åtgärd kan inte ångras. Du bör endast utföra den om du är säker på att ingen behöver ha fullständig behörighet till filen igen. Mer information finns i *FileMaker Pro Advanced Utvecklingshandbok*.

Tips för att skapa effektiva lösenord

- Säkra lösenord innehåller mer än åtta tecken, både gemener och versaler och minst en siffra. Överväg att kombinera två orelaterade ord och att byta ut bokstäver mot siffror, till exempel b0tt!der (”å” har bytts ut mot en nolla och ”i” mot ett utropstecken).

- Om filer ska publiceras på webben bör kontonamn och lösenord endast bestå av utskrivbara ASCII-tecken, till exempel a-z, A-Z och 0-9. Kontonamn och lösenord som kräver större säkerhet kan innehålla skiljetecken som ”!” och ”%” men inga kolon. Om du hanterar databaser med FileMaker Server Advanced bör du aktivera SSL-kryptering.
- Lösenord är mindre säkra om de innehåller strängar som enkelt kan gissas, till exempel namn (framförallt namn på familjemedlemmar och husdjur), födelsedatum, årsdagar och ord som *lösenord*, *standard*, *huvudfil*, *admin*, *användare*, *gäst*, *klient* och liknande vanliga termer.
- Ändra lösenorden ofta, kanske efter 30 eller 90 dagar.
- Använd varje lösenord endast en gång.
- Varje enskild användare bör om möjligt tilldelas ett unikt lösenord. Om du måste dela användarkonton bör du ändra lösenordet ofta.
- Skriv inte upp lösenord i en huvudfil eller en lista, såvida inte filen eller listan är helt skyddade.
- Dela inte användarkonton med andra användare. Användare bör endast få kontonamn och lösenord från filadministratören.

Att tänka på när du hanterar databaser med FileMaker Server

Tänk på följande när du hanterar databaser med FileMaker Server:

- Om du aktiverar fjärråtkomst, se till att användare måste ange ett lösenord. Mer information finns i hjälpen till FileMaker Server.
- Lagra FileMaker Pro-filer på en lokal server (inte i nätverkskataloger). En av de viktigaste prestandafaktorerna är att snabbt kunna läsa och skriva på disken.
- Inaktivera fildelning eller se till att filerna som hanteras av FileMaker Server inte kan öppnas direkt av användarna. Om en FileMaker Pro-fil kan kopieras från en filserver, är den sårbar för attacker. Gruppnamn för konton som autentiseras med den externa serverfunktionen lagras till exempel som textsträngar. Om gruppnamnet reproduceras på ett annat system kan obehöriga få åtkomst till den kopierade filen med samma behörigheter som medlemmarna i gruppen har, vilket kan medföra att känsliga data visas för obehöriga. Mer information finns i ”Säkerhetsförbättringar i FileMaker Server” på sidan 16.
- Att dölja ett filnamn i dialogrutan Fjärröppna eller Startsidan för direkt webbpublicering är inte alternativ till att använda konton och behörighet för att skydda en fil.
- CLI-kommandon (kommandon för kommandoraden) i FileMaker Server kan innehålla kontonamn och lösenord. Se till att obehöriga användare inte via skärmen kan se lösenord som ingår i CLI-kommandon när dessa skrivs in. Begränsa åtkomsten till manus- och kommandofiler som innehåller CLI-kommandon med lösenord med hjälp av funktioner för filäggande och behörighet i operativsystemet.

Säkerhetsöverväganden vid webbpublicering

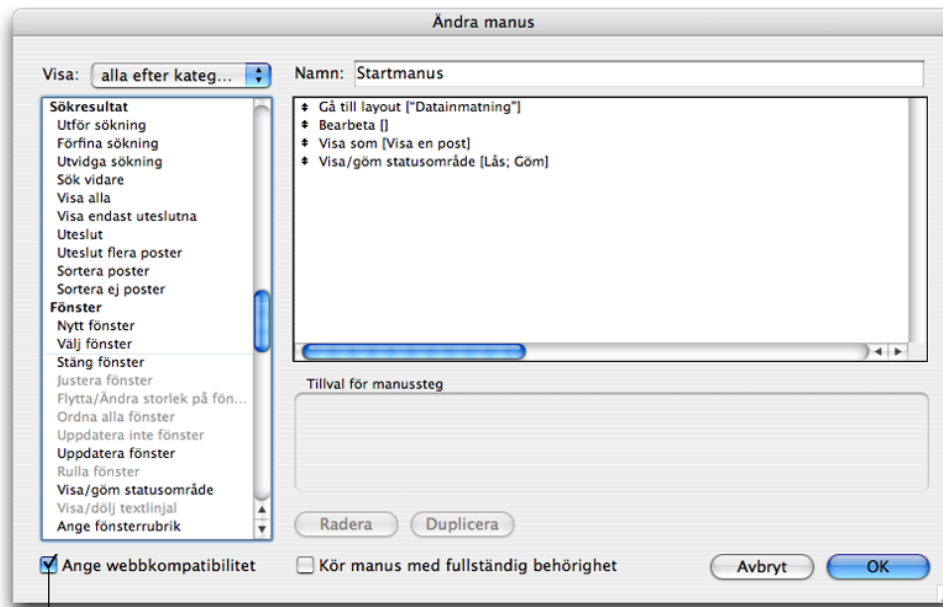
Med FileMaker Pro kan du publicera databaser på ett intranät eller Internet, där användare kan bläddra, söka i och uppdatera databaserna från en webbläsare. Detta ökar risken för intrång mer än att dela filer med andra FileMaker Pro-klienter.

Tips vid utformning av databaser för webbpublicering

1. Definiera konton och behörighet.
 - Skydda alla filer med användarnamn och lösenord. Du kan använda gästkontot som loggar in med ett förvalt användarnamn och lösenord, om det inte är praktiskt att använda unika konton för klienter. Detta gör emellertid din fil tillgänglig för vem som helst som har IP-adressen eller domännamnet till den dator som är värd för databasen.
 - Tilldela behörighet för ändring av data och databasstruktur bara när det är nödvändigt.
 - Aktivera bara de utökade behörigheter för webbpublicering som behövs. Om du till exempel använder egen webbpublicering med XSLT aktiverar du utökad behörighet för detta i motsvarande behörighetsuppsättningar, men aktivera inte utökad behörighet för andra typer av webbpublicering.
2. Om du konverterar lösningar från versioner före version 7, bör du tänka på att Web Security-databaser inte längre stöds. Du måste överföra konton, lösenord och tillhörande behörighet till de konverterade databasfilerna i FileMaker Pro. Mer information finns i *Konvertera FileMaker-databaser från tidigare versioner*.
3. I syfte att öka säkerheten kan FileMaker Pro-klienter inte längre publicera databaser via fjärråtkomst på webben. Du kan endast publicera filer på webben från värddatorn.
4. I Direkt webbpublicering är du inte längre begränsad till fördefinierade layouter när du vill visa data. Alla layouter är tillgängliga för webbanvändare, baserat på deras konton. Du kan begränsa layouter för konton med hjälp av behörighet, men du bör inte förlita dig på layouter när det gäller säkerhet. Säkerheten blir störst om du hanterar åtkomsten till data med tabeller, poster, fält, manus och värdelistor.
5. Om Direkt webbpublicering-klienter inte klickar på knappen Logga ut eller kör ett manus som innehåller manussteget Avsluta programmet, förblir anslutningen till databasen aktiv. Data kan bli tillgängliga för andra webbanvändare eller så kanske användare inte kan komma åt filen. Webbanvändare bör dessutom avsluta webbläsaren för att rensa kontoinformationen från webbläsarens cache-fil. Mer information finns i *FileMaker Handbok för direkt webbpublicering*, i mappen Elektronisk dokumentation (i mappen Svenska – Extra).
6. Välj Visa inte på startsidan för direkt webbpublicering i dialogrutan Dela databas om du vill dölja ett filnamn så att det inte visas på den inbyggda startsidan för Direkt webbpublicering. Detta är praktiskt om din lösning innehåller flera filer och du inte vill att alla filnamnen ska visas. Du bör inte använda denna funktion i stället för att definiera konton och behörighet i filer.

7. Manusresultat.

- Om ett manus innehåller ett steg för att radera poster och en webbanvändare öppnar filen med ett konto som inte tillåter radering av poster, kommer inte manussteget som raderar poster att användas. Manuset kan dock fortsätta att utföras, vilket kan ge oväntade resultat. Överväg att aktivera Kör manus med fullständig behörighet om du vill att manus ska kunna radera poster eller utföra andra begränsade åtgärder som användare normalt inte har åtkomst till med konton och behörighet. Du kan också hindra användare från att köra ett visst manus, genom att ändra deras behörighetsuppsättning och ange manus med behörigheten Ingen åtkomst för vissa användare.
- Databaser som publiceras på webben bör innehålla manus som inte har några skadliga effekter om de körs av en webbanvändare. Om du vill se vilka manussteg som inte stöds öppnar du manuset och markerar kryssrutan **Ange webbkompatibilitet** i dialogrutan Ändra manus. De manus som är nedtonade är inte webbkompatibla.
- Om ett manus innehåller steg som inte stöds, till exempel steg som inte är webbkompatibla (t.ex. Skicka e-post), eller om användare inte har behörighet att köra manuset, kan du använda manussteget Tillåt användaren att avbryta för att avgöra hur efterföljande steg ska hanteras. Mer information finns i *FileMaker Handbok för direkt webbpublicering*, i mappen Elektronisk dokumentation (i mappen Svenska – Extra).



Välj **Ange webbkompatibilitet** om du vill att manussteg som inte är webbkompatibla ska vara nedtonade

8. Lagra inte databasfiler eller känsliga data i webbappen (eller undermappar till den) i FileMaker Pro.
9. Aktivera loggfiler om du vill kunna spåra IP-adresser till användare som använder dina webbpublicerade filer (samt tid och datum för förfrågningarna liksom andra tillval).
10. Med FileMaker Pro kan du begränsa åtkomsten till de användare som använder en IP-adress som du anger i förväg. När du hanterar filer med FileMaker Server Advanced kan du ange begränsningar för klienters IP-adresser i webbserverprogrammet.

11. Om du hanterar webbpublicerade databaser med FileMaker Server Advanced, kan du vidta ytterligare säkerhetsåtgärder, till exempel SSL-kryptering som kan finnas i webbserverprogrammet. Mer information finns i ”Använda SSL-säkerhet vid webbpublicering” på sidan 23. Du kan också inaktivera de metoder för webbpublicering som du inte använder. Mer information finns i *FileMaker Server Advanced Installationshandbok för webbpublicering*.
12. Om du hanterar webbpublicerade databaser med FileMaker Server Advanced använder Web Publishing Engine vissa portar och protokoll för kommunikation med FileMaker Server Advanced och din webbserver. Det kan hända att du måste öppna portar eller tillåta protokoll på värddatorer och brandväggar. Mer information finns i *FileMaker Server Advanced Installationshandbok för webbpublicering*.
13. Om du hanterar databaser med FileMaker Server Advanced och använder egen webbpublicering med XML, kan du testa säkerheten från en webbläsare för att se vilka element som kan vara utsatta:
- Om du vill visa namnen på de databaser som publicerats på webben med XML skriver du följande adress i webbläsaren:
`http://<ip:port>/fmi/xml/fmresultset.xml?-dbnames`
 - Om du vill visa databaserna som publicerats med XSLT skriver du denna adress:
`http://<ip:port>/fmi/xsl/styleSheet_name.xml?-grammar=fmresultset&-dbnames`
 - Om du vill visa fälten för en post i databasen skriver du följande adress i webbläsaren:
`http://<ip:port>/fmi/xml/fmresultset.xml?-db=dbname&-lay=layoutname&-findany`
 - Om du vill visa manusnamnen i databasen skriver du följande adress i webbläsaren:
`http://<ip:port>/fmi/xml/fmresultset.xml?-db=dbname&-scriptnames`
 - Om du vill visa layoutnamnen i databasen skriver du följande adress i webbläsaren:
`http://<ip:port>/fmi/xml/fmresultset.xml?-db=dbname&-layoutnames`

Mer information om frågekommandon och frågeparametrar finns i *FileMaker Server Advanced Handbok för egen webbpublicering*.

Skydda databaser mot webbaserade intrång

Starta genom att gå igenom de säkerhetsprocedurer som beskrivs i det här dokumentet. Värddatorn är både din koppling till omvärlden och, om datorn inte är skyddad, även omvärldens ingång till ditt interna nätverk. Kontrollera följande:

- För lösningar som delas via webben, särskilt på Internet, bör du överväga konfigurationer med två (eller fler) datorer som avgränsar databasen från de webbpublicerande komponenterna, brandväggar, SSL och andra vanliga Internet-tekniker. Detta skyddar åtkomsten till filerna och skyddar kommunikationen mellan webbanvändarnas webbläsare och servern.
- Vidare bör inställningarna för fjärråtkomst, till exempel fildelning och FTP, ses över i syfte att begränsa möjligheten att lägga ut eller hämta filer från värddatorn, för att förhindra obehörig åtkomst till filerna.
- När du hanterar en FileMaker Pro-databas med hjälp av TCP/IP, kanske du tillåter oinbjudna besökare att komma åt värddatorn och det interna nätverket. En brandvägg är nödvändig för att avgränsa nätverket och skydda filerna ”innanför” brandväggen, vilket förhindrar att användare på ”utsidan” av brandväggen får åtkomst till TCP/IP-adresser du inte öppnat.

Säkerhet på webbservern

Webbserverprogrammet bearbetar och svarar på förfrågningar efter data när du publicerar databaser, bilder och annat innehåll på webben. När en användare skriver en webbadress i webbläsarens adressfält utgör det en begäran om att webbserverprogrammet på den adressen ska leta upp de data eller den bild som efterfrågas och skicka informationen till användarens dator där den sedan visas i webbläsaren. Webbservern har en säkerhetsfunktion som skyddar denna process. Om du hanterar databaser med FileMaker Server Advanced bör du använda ett webbserverprogram från något annat företag, till exempel Microsoft IIS (Internet Information Server) eller Apache HTTP Server, när du vill publicera filer på webben. Du kan utnyttja ytterligare säkerhetsfunktioner, till exempel SSL-kryptering, för att transportera data från värddatorn till webbklienter på ett säkert sätt.

Skydda data med kryptering och VPN-nätverk

Överväg att använda kryptering och VPN-nätverk (virtuella privata nätverk) för att skydda databaserna i ett TCP/IP-nätverk. Vid kryptering manipuleras data (klartext) på ett sådant sätt att resultatet (chiffertext) endast kan läsas av vissa program.

Du kan skydda data genom att:

- Konfigurera ett säkert VPN-nätverk för en del av nätverkstrafiken, eller all nätverkstrafik, när den överförs via ett WAN-nätverk.
- Dela databaser med FileMaker Server Advanced och konfigurera SSL-kryptering i webbserverprogrammet.
- Kombinera ovanstående.

Använda SSL-säkerhet vid webbpublicering

SSL-protokollet är en standardmetod för kryptering och autentisering av kommunikationen mellan webbservrar och klienter (webbläsare). SSL-kryptering är endast tillgänglig för databaser där FileMaker Server Advanced används som värd och den aktiveras i webbserverprogrammet, till exempel Microsoft IIS (Internet Information Server) eller Apache HTTP Server från Apache Group. Vid SSL-kryptering konverteras informationen som utväxlas mellan webbservrar och klienter till obegriplig information med hjälp av matematiska formler, så kallade *chiffer*. Dessa chiffer används sedan när informationen konverteras tillbaka till begripliga data med hjälp av *krypteringsnycklar*. Information om hur du aktiverar och konfigurerar SSL finns i dokumentationen som kom med webbservern.

Trådlösa nätverk

En annan sårbar punkt är trådlösa nätverksenheter enligt 802.11x-standard, även kallade Wi-Fi-anlutningar, som innehåller:

- en station (eller enheten för trådlös anslutning enligt 802.11x-standard), till exempel en bärbar dator
- en anslutningspunkt (trådlöst nav eller trådlös brygga) som är själva åtkomstpunkten till nätverket
- det lokala nätverket

- en autentiseringsserver, en separat enhet som kontrollerar klienter när de försöker ansluta till nätverket

Nätverksåtkomst via radiovågor lämnar nätverket öppet för avlyssning via en radiomottagare inom räckhåll för radiosändaren. Detta gör att inkräktare kan ansluta till företagsnätverk via trådlösa protokoll. Dessa intrång kan göras långt bort från den fysiska nätverksplatsen med hjälp av antennförstärkare.

Om FileMaker Server Advanced till exempel används som värd för filer, kan en inkräktare komma åt data om filerna inte skyddas av användarkonton. En inkräktare som vet hur ett WAN-nätverk styr åtkomsten kanske kan få åtkomst till nätverket, stjäla en giltig datoradress och använda dess tilldelade IP-adress. En vanlig taktik är att vänta tills den giltiga datorn slutar att använda nätverket och sedan ta över dess position i nätverket och få åtkomst till alla enheter på nätverket eller Internet.

Viktigt! När du utvärderar den fysiska säkerheten i nätverket bör du lösenordsskydda och kryptera alla trådlösa nätverkssignaler. Använd alltid den högsta nivån på signalkryptering som finns.

Att tänka på vid XML-användning

XML- och XSLT-formatmallar har blivit standard för åtkomst, distribution och presentation av data. Med funktionen egen webbpublicering i FileMaker Server Advanced kan du använda XSLT-formatmallar för att filtrera och konvertera XML-data. Du kan använda denna metod för att ta bort eller ändra metadata i XML-filer som skickas till webbanvändare (till exempel för att dölja fältnamn) eller för att statistiskt definiera parametrar för frågesträngar (till exempel databas- och layoutnamnsvärden), för att förhindra att webbanvändare visar eller ändrar dem. Mer information finns i *FileMaker Server Advanced Handbok för egen webbpublicering*.

Obs! Data som formateras i XML-format är i själva verket text. Det innebär att denna text kan snappas upp och läsas av obehöriga, såvida den inte krypteras. Varje gång du sänder data med TCP/IP och använder FileMaker Server Advanced som värd för databaser, bör du använda SSL-kryptering i webbserverprogrammet. Då blockeras paketavsökningsprogram, som övervakar nätverkstrafik och som kan extrahera FileMaker Pro-data.

Viktigt! Aktivera aldrig utökad behörighet, såvida det inte är helt nödvändigt.

Att tänka på vid användning av Apple Events och ActiveX

FileMaker Pro kan bearbeta kommandon från Apple Events i Mac OS eller från ActiveX i Windows. Detta kan ge oväntade resultat, till exempel när tiden för ett externt manus går ut och det inte bearbetar nästa kommando.

Innan du börjar använda metoder och tekniker från andra företag bör du noggrant testa alla manus och användarscenarier.