



# Aktualisierung auf FileMaker 8:

Einsatz des neuen,  
erweiterten Sicherheitsmodells

## Über dieses technische Briefing

Ziel dieses technischen Briefings ist es, dem erfahrenen FileMaker Entwickler zu einem besseren Verständnis des neuen, erweiterten Sicherheitsmodells von FileMaker 8 zu verhelfen. Dieses Dokument wird Ihnen bei der Einschätzung der Hauptmerkmale und Vorzüge des neuen Sicherheitsmodells helfen sowie bei der Planung, Vorbereitung und Implementierung Ihrer Strategie bei der Migration zu FileMaker Pro 8. Das Dokument wurde von Steven Blackwell verfasst, FileMaker Solutions Alliance Partner und Präsident und CEO von Management Counseling Services. Es ist Bestandteil einer Reihe technischer Briefings, die Entwicklern bei der Migration zur neuen FileMaker 8 Produktfamilie helfen soll.

Weitere technische Unterlagen finden Sie in den gedruckten und elektronischen Handbüchern und der Online-Hilfe, die zum Lieferumfang von FileMaker Pro 8, FileMaker Server 8 und FileMaker Server 8 Advanced gehören.

**Bitte beachten Sie:** Dieses technische Briefing ist relevant für FileMaker 8 und FileMaker 7 Produkte.

## Einführung

Wir leben in einer digitalen Welt, in der das Internet nicht nur die Hauptverkehrsstraße darstellt, sondern auch den Zustand der Gesellschaft als Ganzes reflektiert. Das Internet und seine Dienste sind entscheidend für Unternehmen jeglicher Art und Struktur. Ob es eine Universität ist, die Zugriff zu Datenbanken mit Forschungsergebnissen bietet, ein Paketzustelldienst, der seine Lieferungen erfasst, eine überregionale Handelsvereinigung, die eine Online-Datenbank ihrer Mitglieder führt, eine kleine Firma, die Ein- und Ausgangsrechnungen festhält, oder ein Industrieunternehmen, das seine Abnehmer über den Status von Bestellungen auf dem Laufenden hält – all diese Firmen verlassen sich auf rasch zugängliche und kontinuierlich aktualisierte Informationsquellen.

Wir erwarten, dass uns online alle Möglichkeiten offenstehen, die auch die reale Welt bietet, und gehen davon aus, diese Aktivitäten mit einem hohen Maß an Sicherheit ausführen zu können.<sup>1</sup> Die Realität aber sieht anders aus; das Internet wird immer unsicherer und seine Nutzung riskanter. Effektiv gesehen sind die Grenzen der Sicherheit die Grenzen des Internets – und diese gelten auch für FileMaker Pro® Systeme und für ihre Entwickler und Benutzer.

Entwickler von Software-Produkten sollten sich darauf verlassen können, dass ihr geistiges Eigentum sicher und geschützt bleibt. Firmen sollen erwarten dürfen, dass ihre eigenen Daten nicht Unbefugten gegenüber offengelegt werden und dass nur autorisierte Personen die Möglichkeit haben, Informationen innerhalb ihrer Systeme hinzuzufügen, zu verändern oder zu löschen. Sicherheit ist also sehr wichtig. Aber was wollen wir eigentlich schützen? Was ist angreifbar? Allgemein gesehen, sollte sich Datenbanksicherheit um drei spezielle Bereiche kümmern:

- Schutz des geistigen Eigentums
- Vertraulichkeit von Daten
- Unverletzlichkeit von Daten

Im weiteren Sinne ist Sicherheit auch Teil eines Plans für geschäftliche Kontinuität, der die fortgesetzte Fähigkeit eines von Daten abhängigen Unternehmens beschreibt, seine Tätigkeit auch angesichts mehrerer Ausfälle weiterzuführen. Dieses Thema reicht über den Umfang dieses technischen Briefings hinaus; es ist aber von großer Bedeutung.



Dieses Dokument behandelt fünf Themen, die für Entwickler von FileMaker Pro Lösungen und für IS/IT/DBA-Manager, die mit FileMaker Pro und FileMaker Server arbeiten, von größter Bedeutung sind:

- ein kurzer Abriss des FileMaker Pro 6 Sicherheitsmodells und einiger damit verbundener Probleme;
- ein Überblick der Hauptmerkmale des neuen Sicherheitsmodells von FileMaker Pro 8 / FileMaker Server 8;
- eine Beschreibung mehrerer signifikanter Probleme bei der Sicherheitsverwaltung, die das neue Modell beseitigt;
- mehrere signifikante Probleme in struktureller und entwicklungstechnischer Hinsicht bei Dateien, die Entwickler von früheren Versionen zu FileMaker Pro 8 konvertieren; und
- die Auswirkungen, die das neue Modell sowohl auf die Arbeitsweise als auch auf die geschäftlichen Aktivitäten der drei hauptsächlichen FileMaker Pro Anwendergruppen hat: *Entwickler kommerzieller Lösungen, selbständige Entwickler und IS/IT/DBA-Manager, speziell in unternehmensweiten Arbeitsgruppen.*

## Inhaltsverzeichnis

Über dieses technische Briefing .....	1
Einführung.....	1
Es war einmal... ..	3
FileMaker Pro 8: Ein neuer Ansatz.....	3
Konten und Passwörter: Berechtigungsnachweise .....	3
Berechtigungen .....	6
Erweiterte Zugriffsrechte.....	8
Planung und Reihenfolge des Sicherheitsschemas .....	8
Neue Funktionen für die Sicherheitsverwaltung.....	9
Feinabstufung des Zugriffs.....	9
FileMaker Server 8.....	11
Web-basierter Zugriff: Das vereinheitlichte Sicherheitsmodell.....	14
FileMaker Pro 8 beseitigt wesentliche Probleme bei der Sicherheitsverwaltung.....	17
Verwaltung von Konten .....	17
Verschlüsselter Netzwerkverkehr.....	19
Auslesen von Passwörtern.....	19
Andere beseitigte Probleme .....	19
Probleme bei der Konvertierung früherer Versionen .....	20
Auswirkungen auf Geschäftsmodelle und Abläufe bei Entwicklern und IS/IT/DBA-Managern .....	21
Fazit.....	22
Über den Autor .....	23
Endnoten.....	23
Bibographie.....	25



### Es war einmal...

Frühere Versionen der FileMaker Produktfamilie stellten den Client in den Mittelpunkt und verließen sich auf ein Trusted Client Modell für die Authentifizierung und Passwortannahme<sup>2</sup>. Dies sorgte für beträchtliche Probleme, die bisweilen umfangreiche provisorische Lösungen erforderlich machten. In den meisten Fällen sorgten diese Provisorien eher für weniger als für mehr Sicherheit. Ebensovienig wurde der Netzwerkverkehr verschlüsselt. All dies hat sich jetzt geändert. Diese Änderungen sind umfassend, dramatisch und gewaltig. *Als Entwickler haben wir die einmalige Gelegenheit, die Vorteile zu nutzen, die dieser Wechsel bietet.*

### FileMaker Pro 8: Ein neuer Ansatz

Das neue FileMaker Pro 8 Sicherheitsmodell setzt voraus, dass Entwickler und IS/IT/DBA-Manager das Thema Sicherheit ernst nehmen. Ein neues Modell nützt wenig, wenn seine Funktionen nicht eingesetzt werden. **Hauptzweck des neuen Sicherheitsmodells ist die Durchsetzung der erforderlichen Regeln und Abläufe – die sich von Fall zu Fall unterscheiden können –, um den Schutz des geistigen Eigentums zu gewährleisten und die Vertraulichkeit und Unverletzlichkeit der Daten zu garantieren.**

Das neue FileMaker Pro 8 Sicherheitsmodell ist eine eigene Ebene der Datenbankarchitektur. Es ist nicht mehr Bestandteil des Datenbankschemas, der Ebene, in der Objekte wie Tabellen, Felder, Dateiverweise und Beziehungen definiert werden. Die Folgen dieser Trennung sind beträchtlich. Entwickler können Klassen von Benutzern {Superuser genannt} erlauben, Konten und Passwörter zu löschen, zu aktivieren, zu deaktivieren und zurückzusetzen, sogar während die Dateien geöffnet sind und von FileMaker Server 8 oder FileMaker Server 8 Advanced bereitgestellt werden. Änderungen treten sofort in Kraft und werden durch das gesamte System weitergegeben. Außerdem benötigen Superuser zur Verwaltung von Sicherheitseinstellungen keine Zugriffsrechte auf das Datenbankschema, was vor allem Entwicklern kommerzieller Lösungen den wirksamen Schutz ihres geistigen Eigentum ermöglicht.

#### Konten und Passwörter: Berechtigungsnachweise

Das FileMaker Pro 8 Sicherheitsmodell basiert auf Konten. Es authentifiziert die *Berechtigungsnachweise* der Benutzer, um ihnen Zugriff auf die Datenbank mit vom Entwickler definierten *Berechtigungen* zu geben. Berechtigungsnachweise besitzen zwei Komponenten: einen Kontonamen und ein Kontopasswort oder, bei externer Authentifizierung, einen Gruppennamen<sup>3</sup>. Wurde der Berechtigungsnachweis eines Benutzers korrekt authentifiziert und er selbst als legitim und gültig identifiziert, kann er sich beim System mit einer bestimmten Zugriffsebene anmelden, die durch die Berechtigung festgelegt ist. Abb. 1 verdeutlicht diesen Vorgang.

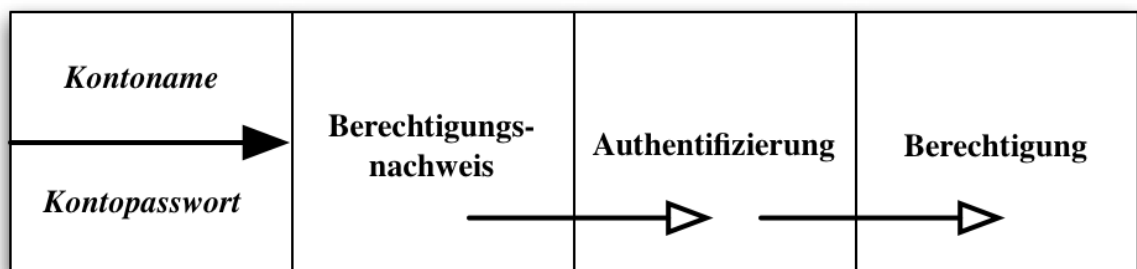


Abb. 1. Das zentrale Konzept des Sicherheitsmodells.



Es gibt wichtige Regeln für die Erstellung von Berechtigungsnachweisen. *Kontonamen müssen eindeutig sein, unterscheiden aber nicht Groß- und Kleinschreibung.* Beim Einrichten eines Kontos in mehreren Dateien sollten Entwickler darauf achten, den Kontonamen exakt gleich zu schreiben. So entsteht keine Verwirrung und das System ist eindeutig strukturiert. *Passwörter unterscheiden Groß- und Kleinschreibung, müssen aber nicht eindeutig sein.* Man könnte glauben, dass dies fehleranfällig ist; dem ist jedoch nicht so, wie ich später erläutern werde. Beachten Sie, dass sich dieses Modell vollständig von dem früherer Versionen unterscheidet. Der Entwickler kann für das Passwort eine Mindestlänge und eine Gültigkeitsdauer festlegen. Vergisst ein Benutzer sein Kennwort (was sicherlich passieren wird), kann ein Administrator mit entsprechender Berechtigung das Konto neu anlegen, das Passwort zurücksetzen usw. und den Benutzer dann auffordern, ein neues Passwort festzulegen.

Entwickler definieren Konten und Passwörter im Menü *Ablage* (Mac) bzw. *Datei* (Windows); sie können außerdem *Superusern* das Recht zur Kontenverwaltung einräumen, was später in diesem Dokument beschrieben wird. Nach Auswahl von [Definieren-Konten und Zugriffsrechte] erscheint ein Dialogfeld ähnlich dem Folgenden:

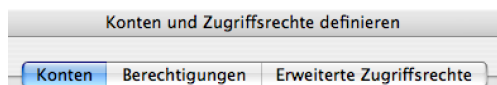


Abb. 2. Reiter im Dialogfeld „Konten und Zugriffsrechte definieren“

Durch Klicken in „Konten“ erscheint ein Fenster für Kontodefinition und Authentifizierungsoptionen:

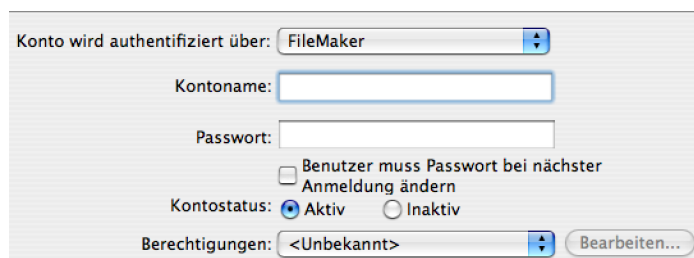


Abb 3. Bereich zur Bearbeitung von Konten.

Hier gibt der Entwickler einen Namen und ein Passwort für das Konto ein. Er kann durch Markieren der entsprechenden Option festlegen, dass der Benutzer bei der nächsten Anmeldung das Passwort ändern muss.

Im Allgemeinen wird die Sicherheit erhöht, wenn der Benutzer die Verantwortung für den Besitz des Passworts übernehmen muss. Zwar kann der Administrator das Passwort zurücksetzen, falls der Benutzer es vergessen hat (was garantiert passieren wird), aber das System ist sicherer, wenn nur der jeweilige Benutzer selbst sein Passwort kennt. Sorgfalt sollte auch bei der Definition des Kontonamens angewandt werden. Viele Unternehmen verwenden ein standardisiertes Verfahren zur Benennung von Kontonamen; z. B. könnte SchmidtA oder Schmidt\_a ein Standard-Kontoname für den Benutzer Anton Schmidt sein. Auf diese Weise lässt sich ein Kontoname relativ mühelos erraten, was ein Sicherheitsrisiko darstellt. Vom Benutzer selbst festgelegte Kontonamen verringern dieses Risiko, ebenso wie Namensvarianten, z. B. SchmidtA#\$. Starke Passwörter sind mindestens acht Zeichen lang und kombinieren alphanumerische und Sonderzeichen<sup>4</sup>. Sie sind leicht zu merken,



aber nur schwer zu erraten. FileMaker Pro 8 unterstützt Passwörter oder Passphrasen mit bis zu 100 Zeichen, einschließlich Leerzeichen. Ein Beispiel für eine Passphrase wäre die Adaptation einer leicht zu merkenden, aber schwer zu erratenden Gedichtzeile oder eines Zitats: *Verweile doch, du bist so schön*.

Erstellt ein Entwickler eine neue FileMaker Pro 8 Datei, wird ein Standardkonto namens *Admin* angelegt, das kein Passwort besitzt und die Berechtigung [Voller Zugriff] erhält, (s. Abb 4). FileMaker Pro 8 erstellt außerdem eine automatische Anmeldung<sup>5</sup> mit dem Kontonamen „*Admin*“ und einem leeren Passwort. Das ermöglicht dem Entwickler, mit der Datei zu arbeiten. Ich empfehle jedem Entwickler, als erstes diesem Konto einen anderen Namen als *Admin* zu geben und ihm ein Passwort zuzuweisen. Andernfalls verbleibt der Standardname, der leicht zu erraten ist und somit unbefugten Zugriff auf die Datei ermöglicht. Entwickler sollten die Berechtigungsnachweise für Berechtigungen mit [Voller Zugriff] sicher aufbewahren. Geht das Passwort verloren oder wird es vergessen, kann es nicht wiederhergestellt werden, auch nicht von FileMaker Inc.

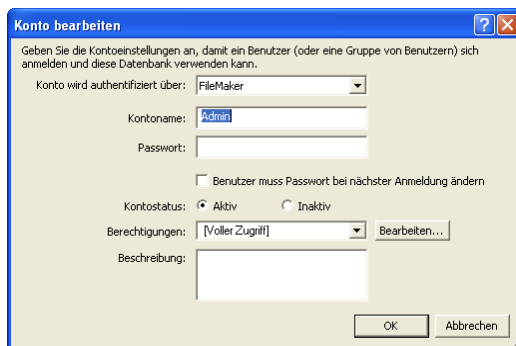


Abb. 4. Das Standardkonto „Admin“ mit der Berechtigung [Voller Zugriff].

Im Bereich „Konto bearbeiten“ wählt der Entwickler auch die Authentifizierungsmethode: *FileMaker* oder *Externer Server*. Wählt der Entwickler die zweite Option, ändert sich das Fenster, wie in Abb. 5 gezeigt.

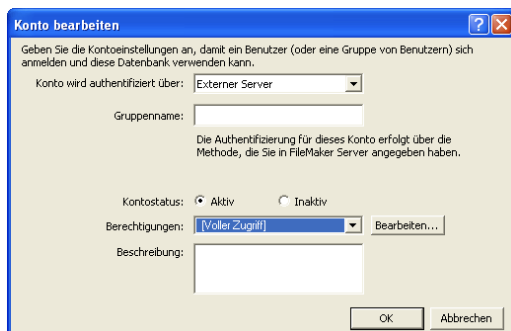


Abb. 5. Bereich „Konto bearbeiten“ mit Optionen für die externe Authentifizierung.



Beachten Sie, dass „Kontoname“ zu „Gruppenname“ geworden ist. Hier wird der Name einer Gruppe der externen Domain eingetragen,<sup>6</sup> und FileMaker Server 8 verwaltet die Authentifizierung jetzt extern. Hier einige wichtige Anmerkungen zur Kontodefinition und den Authentifizierungsoptionen:

1. Jede Datei benötigt mindestens ein intern (von FileMaker Pro) authentifiziertes Konto mit [Voller Zugriff].<sup>7</sup>
2. Ich rate davon ab, Konten mit der Berechtigung [Voller Zugriff] durch externe Mechanismen authentifizieren zu lassen. Fällt eine physische Kopie der Datei in falsche Hände, kann das Domain-System nachgebildet und so das Domain-Konto ausgetrickst werden, was uneingeschränkten Zugriff auf die Dateien erlaubt.
3. Gute Sicherheitspraxis fordert, dass Kontennamen für *Einzelbenutzer* bestimmt sind. **Benutzer dürfen ihre Berechtigungsnachweise nicht weitergeben oder offenlegen.** Individualität ist von zentraler Bedeutung in einem System, das die drei Grundpfeiler der Sicherheit durchsetzt: Schutz des geistigen Eigentums, Vertraulichkeit und Unverletzlichkeit von Daten.

Wann sollte man die eine Authentifizierungsmethode der anderen vorziehen? Manchmal werden Entwickler die interne FileMaker Authentifizierung nutzen, weil die Lösung in einem Umfeld ohne Domain-Struktur eingesetzt wird. In vielen anderen Fällen aber werden sowohl beratende als auch firmeninterne Entwickler die externe Authentifizierung verwenden, um bestehende IS/IT-Ressourcen zu nutzen und Konten und Lösungsverfahren zu vereinheitlichen. Bei externer Authentifizierung werden die Domain-Berechtigungsnachweise des Benutzers dazu verwendet, auf einer bestimmten Berechtigungsstufe Zugriff zur FileMaker Pro Datenbank zu geben. Beachten Sie, dass eine Datei sowohl intern als auch extern authentifizierte Konten besitzen kann. In FileMaker Server 8 kann der Server-Administrator wählen, welche Option benutzt werden soll: *Nur FileMaker Konten* oder *FileMaker und Externe Server Konten*. Wir werden dies später in diesem Dokument behandeln.

Die Option für die externe Authentifizierung bedeutet, dass FileMaker Pro 8 im Zusammenspiel mit FileMaker Server 8 die „Einmalanmeldung“ erlaubt, auch „Anmeldung mit universeller Authentifizierung“ genannt. Dies ist eine bei IS/IT System- und Netzwerkverwaltung weit verbreitete Technik. Man geht davon aus, dass der Aufwand für die Verwaltung von Berechtigungsnachweisen verringert wird, wenn der Benutzer für den Zugriff auf Netzwerk- und digitale Ressourcen nur einen einzigen Nachweis merken muss. Obwohl dies wahrscheinlich zutrifft, wird dadurch die Sicherheit der Datenbank einer Instanz außerhalb von FileMaker Pro überantwortet. Daher sollten Entwickler mit den Themen Netzwerksicherheit und Authentifizierung allgemein vertraut sein.<sup>8</sup>

## Berechtigungen

Hat der Entwickler eine neue FileMaker Pro 8 Datei angelegt, kann er jedes vom Entwickler erstellte Konto einer der Standard-Berechtigungen zuweisen. Es gibt zwei Arten von Berechtigungen: [Voller Zugriff] und alle anderen, die *nachgeordnet* sind. Nachgeordnete Berechtigungen, ob standardmäßig vorhanden oder vom Entwickler angelegt, besitzen bestimmte Einschränkungen. Ein Entwickler **kann keine** Berechtigung mit [Voller Zugriff] anlegen; nur die Standard-Berechtigung ist verfügbar. Es gibt neben [Voller Zugriff] noch zwei weitere Standard-Berechtigungen: [Nur Dateneingabe] und [Nur Lesezugriff]. Beide sind nachgeordnet. Entwickler sollten die Komponenten dieser beiden nachgeordneten Berechtigungen sorgfältig untersuchen, bevor sie diese einem Konto zuweisen. Oft umfassen sie trotz ihrer Namen eine andere Berechtigungsstufe als diejenige, die der Entwickler dem Konto wirklich zuweisen will. Aus diesem Grund wird ein Entwickler bei manchen Konten,



die „Nur zur Dateneingabe“ und „Nur zum Lesen“ bestimmt sind, selbst erstellte Berechtigungen verwenden.

Entwickler können und werden individuelle nachgeordnete Berechtigungen erstellen, denn erst sie bringen die volle Leistungsstärke und Flexibilität des neuen Sicherheitsmodells zur Geltung. Berechtigungen sind im neuen Sicherheitsschema von FileMaker Pro 8 von zentraler Bedeutung. Sie bestimmen innerhalb einer Datei und für alle Tabellen dieser Datei, welche Berechtigungen ein Benutzer besitzt und welche Aktionen er durchführen darf.

In *Konten und Berechtigungen definieren* {Abb. 6} erscheint nach Auswahl des zweiten Registers „Berechtigungen“ ein Dialogfeld ähnlich Abb. 7, in dem der Entwickler individuelle untergeordnete Berechtigungen erstellt.

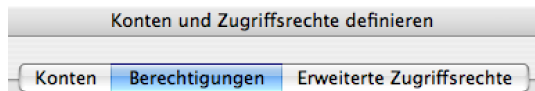


Abb. 6. Register „Berechtigungen“ im Dialogfeld „Konten und Zugriffsrechte definieren“

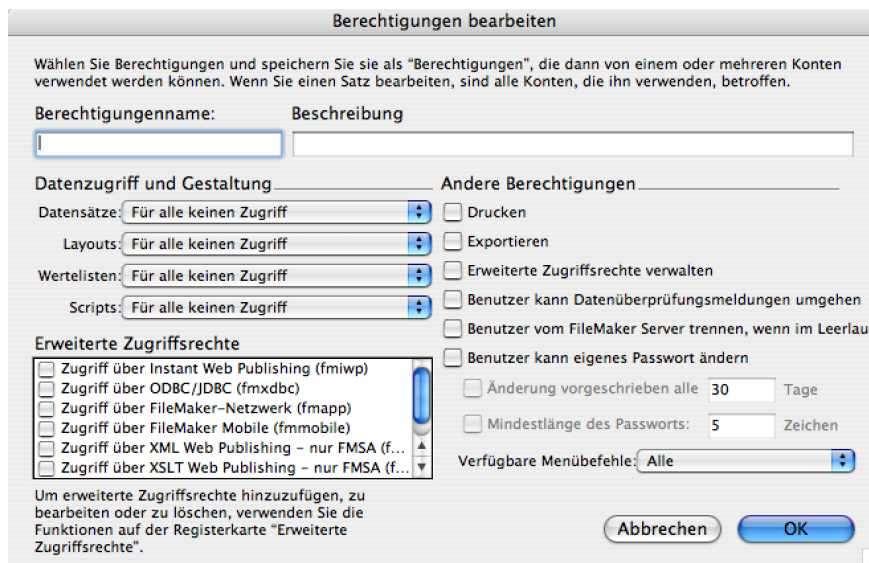


Abb. 7. Dialogfeld „Berechtigungen bearbeiten“.

Im Fenster „Berechtigungen bearbeiten“ fällt zuerst auf, dass die meisten Optionen standardmäßig *deaktiviert* sind. Dies ist ein großer Unterschied gegenüber früheren Versionen, in denen die meisten Optionen aktiviert waren und einzeln explizit deaktiviert musste. In FileMaker Pro 8 sind alle Optionen standardmäßig deaktiviert, und der Entwickler muss den Zugriff auf eine Vielzahl von Objekten und Funktionen ausdrücklich gewähren.

Jedem Konto ist *eine, und nur eine*, Berechtigung zugewiesen. Eine bestimmte Berechtigung kann jedoch mehreren Konten zugewiesen sein. Auch dies ist eine deutliche Änderung gegenüber früheren Versionen, in denen Passwörter unterschiedlichen Gruppen zugewiesen werden konnten. Beachten Sie die verschiedenen Bereiche im Dialogfeld „Berechtigungen bearbeiten“: *Datenzugriff und Gestaltung*, *Erweiterte Zugriffsrechte* und



*Andere Berechtigungen.* Im folgenden Abschnitt, der die Feinabstufung des Zugriffs behandelt, werden wir diese Bereiche ausführlicher behandeln. Beachten Sie auch das Textfeld „Beschreibung“, in dem sich ein Kommentar oder eine Beschreibung zum Zweck dieser Berechtigung eintragen lässt. Diese neue Option ist sehr hilfreich bei der strukturellen Verwaltung und der technischen Dokumentation von Lösungen.

### Erweiterte Zugriffsrechte



Abb. 8. Das Register „Erweiterte Zugriffsrechte“.

Abb. 8 zeigt das letzte Register im Dialogfeld *Konten und Berechtigungen definieren*. Durch Anklicken erscheint ein Fenster, in dem sich erweiterte Zugriffsrechte zu diversen Berechtigungen und somit auch zu den zu dieser Berechtigung gehörenden Konten zuweisen lassen. Die meisten dieser erweiterten Zugriffsrechte sind Optionen für den Netzwerkzugriff, wie FileMaker Server, Instant Web Publishing, Custom Web Publishing über die neue Web Publishing Engine in FileMaker Server 8 Advanced und Datenbankverbindungen per ODBC/JDBC oder FileMaker Mobile. Außerdem können Entwickler hier eigene erweiterte Zugriffsrechte für die Verwendung mit diversen externen oder internen Modulen anlegen.

### Planung und Reihenfolge des Sicherheitsschemas

Das neue Sicherheitsschema von FileMaker Pro 8 verlangt vom Entwickler, die Sicherheit auf andere Art als bisher zu planen. Dies ist ein sehr komplexes Thema, zu dem erst weitere Erfahrungswerte gesammelt werden müssen, bevor sich beste Praktiken empfehlen lassen.

Es könnte sich als einfacher erweisen, nach Festlegung der Lösungsspezifikationen während der Entwicklung zu Testzwecken mehrere individuelle, nachgeordnete Berechtigungen zu erstellen und ihnen leicht erkennbare Kontonamen und Passwörter zuzuweisen<sup>9</sup>. Das erlaubt nicht nur eine Optimierung der Berechtigungen, sondern auch, falls erforderlich, die korrekte Zuweisung von Berechtigungen zu Objekten in sehr feinen Abstufungen.

Komplexe Lösungen – und auch solche mit weitaus geringerer Komplexität – profitieren aber davon, wenn ihre Spezifikationen einen Abschnitt enthalten, der speziell auf diese Zugriffsrechte eingeht. Die Definition dieser Berechtigungen kann eine Herausforderung sein. Wie sollte ein Entwickler am besten die effektive Nutzung des neuen Sicherheitssystems planen? Es gibt mehrere klare, anerkannte Methoden für die Zugriffsverwaltung:

- Obligatorische Zugriffssteuerung;
- Freigestellte Zugriffssteuerung (jetzt umfassend in FileMaker Pro 6 Dateien verwendet);
- Regelbasierte Zugriffssteuerung; und
- Rollenbasierte Zugriffssteuerung.

Beim rollenbasierten Ansatz erstellt der Entwickler für jede identifizierte Rolle innerhalb der Datenbank eine individuelle, nachgeordnete Berechtigung und weist dieser Berechtigung dann so viele Konten zu, wie es Mitarbeiter in dieser Rolle gibt.<sup>10</sup>



## Neue Funktionen für die Sicherheitsverwaltung

FileMaker Pro 8 besitzt eine Anzahl neuer Funktionen für die Sicherheitsverwaltung, die Informationen über das Konto zurückgeben, das für den Zugriff auf die Datei benutzt wird. Es handelt sich um „Hole“-Funktionen, die die „Status“-Funktionen ersetzen. Hierzu gehört HOLE (KONTONAME)<sup>11</sup>, HOLE (DATEI BERECHTIGUNGEN) und HOLE (DATEI BERECHTIGUNGEN ERWEITERT). HOLE (PROGRAMMBENUTZERNAME) wurde von älteren Versionen übernommen, aber Einsatzmöglichkeiten und Nutzen sind verringert<sup>12</sup>. Außerdem gibt es Funktionen zur Prozessor- und Netzwerkabfrage, die sicherheitsrelevant sein können, wie HOLE (SYSTEM NICADRESSE) und HOLE (SYSTEM IPADRESSE). Die zurückgegebenen Resultate können in Scripts, Formeln, Zugriffstests auf Datensatzebene und ähnlichen Bereichen genutzt werden, um Konten zu identifizieren und auf Basis dieser Identifikation weiter zu verfahren.

## Feinabstufung des Zugriffs

*Feinabstufung* bezieht sich auf die abgestufte Zugriffssteuerung, die das Sicherheitsmodell für eine Vielzahl unterschiedlicher Objekte und Funktionen von FileMaker Pro ermöglicht:

### Objekte

Tabelle
ScriptMaker™ Script-Erstellung
ScriptMaker Script-Zugriff
Wertelisterstellung
Wertelistenzugriff
Layout-Erstellung
Layout-Zugriff
Datensatz
Feld

### Funktionen

Drucken
Exportieren
Verwalten des eigenen Passworts
Optionen für die Datenbankfreigabe, einschließlich Netzwerk, ODBC/JDBC, Instant Web Publishing, Custom Web Publishing und FileMaker Mobile
Trennen bei Inaktivität
Schemazugriff unter kontrollierten Bedingungen
Kontoverwaltung
Externe API-Bearbeitung
Verwaltung Erweiterter Zugriffsrechte

Die *Verwaltung* der erweiterten Zugriffsrechte, wie in einem vorherigen Abschnitt angemerkt, sollte von den erweiterten Zugriffsrechten selbst unterschieden werden. Verwaltung bezieht sich auf die Fähigkeit, erweiterte Zugriffsrechte aktivieren oder deaktivieren zu können sowie darauf, neue individuelle Zugriffsrechte anlegen, löschen und bestimmten Berechtigungen zuweisen zu können bzw. diese Zuweisung wieder rückgängig zu machen. Ich werde später in diesem Dokument noch näher auf die erweiterten Zugriffsrechte eingehen.



Für Entwickler, die eine derart genaue Feinabstimmung nicht benötigen, bietet FileMaker Pro 8 wie seine Vorgänger eine Anzahl unterschiedlicher Standardeinstellungen für die Sicherheit, die eine rasche Zuweisung der Zugriffsoptionen zu eigenen nachgeordneten Berechtigungen ermöglichen. Abb. 9 zeigt hierfür ein Beispiel:

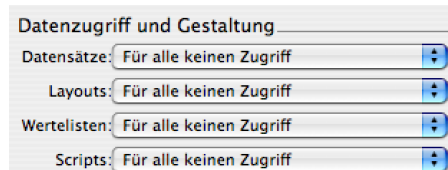


Abb. 9. Standardmäßige Zugriffsoptionen.

Die Feinabstufung ist ein sehr wichtiges Konzept, und seine umfassende Nutzung verleiht dem Entwickler viele Möglichkeiten zur Steuerung des Zugriffs auf Objekte und Funktionen in der Datei und somit zur Durchsetzung der drei Grundpfeiler der Sicherheit: Schutz geistigen Eigentums, Vertraulichkeit von Daten und Unverletzlichkeit von Daten. Für diese Objekte und Funktionen gibt es mindestens **vier Zugriffsstufen**, die objektweise oder für eine gesamte Kategorie vergeben werden können. Dies erfolgt einzeln für jede selbsterstellte, nachgeordnete Berechtigung, was eine weitere Abstufung darstellt. Die einzelnen Stufen sind:

- *Erstellen*, außer bei Tabellen, Felder und Beziehungen; diese lassen sich jedoch unter kontrollierten Bedingungen erstellen.<sup>13</sup>
- *Bearbeiten*, einschließlich Löschen.
- *Anzeigen*, bzw. bei Scripts: Nur ausführbar.
- *Kein Zugriff*.

Bei dieser Zuweisung kann zwischen Objekten unterschieden werden, die der Entwickler angelegt hat, und Objekten, die Benutzer oder der Administrator nachträglich erstellen. **Dies bedeutet, dass der Entwickler einem Administrator oder sogar einem Endbenutzer die Möglichkeit geben kann, neue Layouts, Scripts, und Wertelisten zu erstellen, ohne bestehende Objekte dieser Art zu verändern.**

Die Möglichkeit, einem Administrator das Erstellen neuer Scripts zu erlauben, ohne jedoch die vom Entwickler erstellten verändern zu dürfen, birgt bedeutende Implikationen. Eine solch fein abgestufte Kontrolle schützt das geistige Eigentum des Entwicklers, vor allem bei kommerziellen Lösungen. Sie schützt aber auch interne Geschäftsabläufe vor Störungen, während ein Administrator zusätzliche Funktionen implementieren kann.

Scripts besitzen eine besondere Funktionalität, wie es ihrer zentralen Bedeutung für FileMaker Pro Abläufe entspricht. Der Entwickler kann für jede einzelne individuelle, nachgeordnete Berechtigung ein Script als *Veränderbar* angeben, d. h. der Benutzer kann es bearbeiten. Das Script kann aber auch als *Nur ausführbar* markiert werden, so dass der Benutzer es zwar sehen, aber weder die Ablauflogik noch die einzelnen Schritte sehen oder verändern kann. Die letzte Möglichkeit lautet *Kein Zugriff*. Das heißt, dass der Benutzer das Script weder sehen kann noch weiß, dass es existiert. Es erscheint nicht in der Liste der Scripts, auch nicht, wenn ScriptMaker™ geöffnet ist. Derselbe Benutzer kann neue Scripts erstellen, aber nicht diejenigen sehen, die für die zu seinem Konto gehörende Berechtigung als *Kein Zugriff* markiert sind.



Abb. 10 zeigt die Optionen für Scripte zusammen mit der Option *Eigene Berechtigungen*. Damit können die Zugriffsoptionen für jedes Script einzeln festgelegt werden. FileMaker Pro 8 besitzt für die meisten anderen Objekte ähnliche Abstufungen, wie die obenstehende Tabelle verdeutlicht.

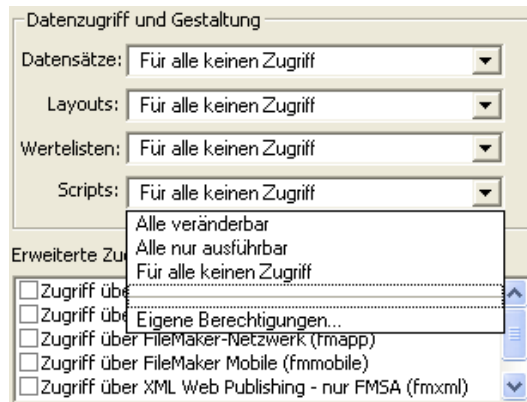


Abb. 10. Die Optionen für den Script-Zugriff lassen sich sehr fein abstufen.

## FileMaker Server 8

FileMaker Server 8 und FileMaker Server 8 Advanced spielen im neuen Sicherheitsmodell eine wichtige Rolle innerhalb drei entscheidender Bereiche: Authentifizierung, Dateifilterung und Datenverschlüsselung.

Sowohl die Mac OS X Version als auch die Windows 2000 Server/Windows 2003 Server Version von FileMaker Server 8 besitzen integrierte Authentifizierungsmechanismen, die beim Zugriff auf den Daemon oder den Dienst die Sicherheit kontrollieren. Die Verwaltung dieser Objekte wird in einem separaten technischen Briefing zu FileMaker Server 8 ausführlicher beschrieben, aber beide können so eingestellt werden, dass für Zugriff und Verwaltung eine Authentifizierung bei der Anmeldung erforderlich ist. Die physische Sicherheit des Computers, auf dem FileMaker Server 8 läuft, sowie der für den Zugriff bereitgestellten Dateien ist sehr wichtig. Sicherheitsvorkehrungen wie das Deaktivieren von File Sharing auf Betriebssystemebene, das Aufstellen des Computers in einer geschützten und gesicherten Umgebung und das korrekte Erfassen der Aufbewahrungsorte aller Sicherungskopien der Dateien können in beträchtlichem Maße zu einer Verbesserung der Sicherheit beitragen. Außerdem besitzt FileMaker Server 8 umfangreiche Protokollfunktionen<sup>14</sup>, sowohl für das Programm selbst als auch für die bereitgestellten Dateien; dies ist eine große Hilfe bei den wichtigen Funktionen der Prozess- und der Zugriffsüberwachung.



Die Abbildungen 11a und 11b zeigen das Register „Sicherheit“ in FileMaker Server 8 unter Mac OS X bzw. Windows 2000 Server/2003 Server.

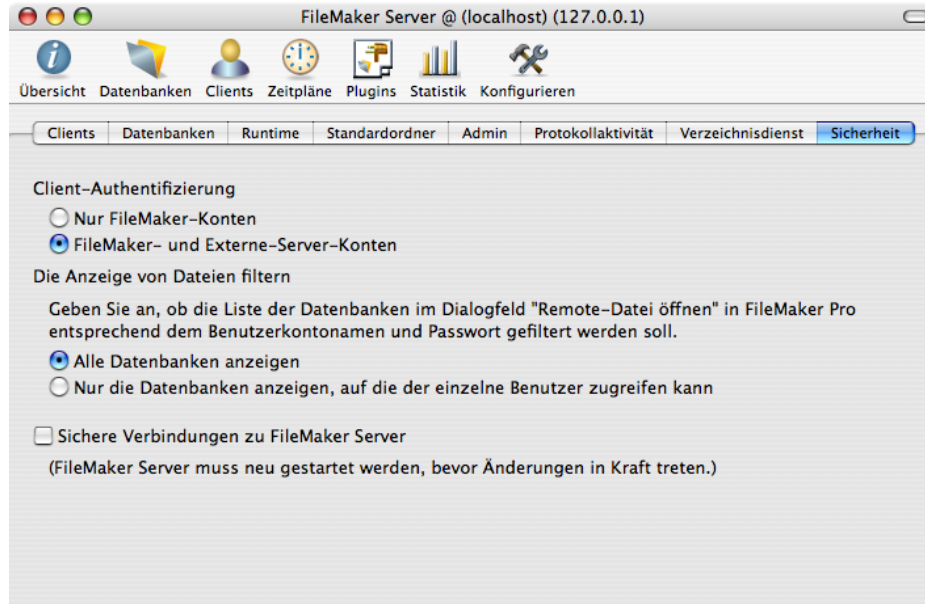


Abb. 11a. Das Register „Sicherheit“ in FileMaker Server unter Mac OS X.

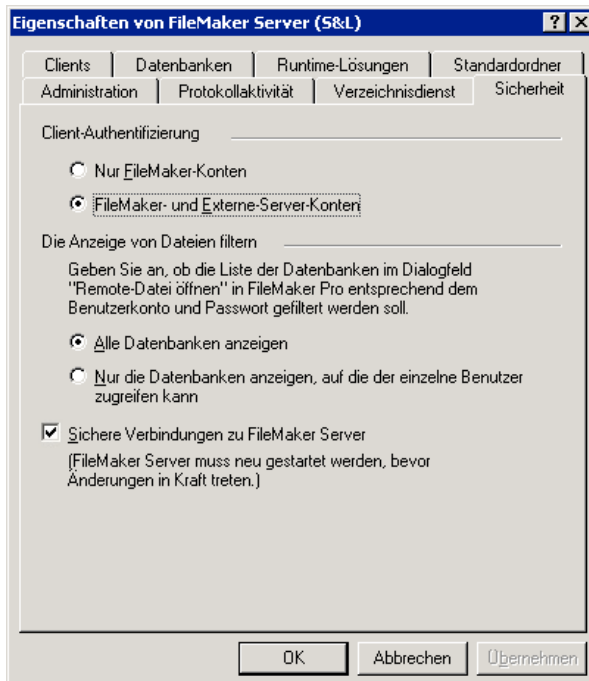


Abb. 11b. Das Register „Sicherheit“ in FileMaker Server unter Windows 2003 Server.



Wenn FileMaker Pro 8 Datei ein Konto besitzt, das extern authentifiziert werden soll, führt FileMaker Server 8 diese Aufgabe durch, wie vorhin gesehen. Beachten Sie die Option *Client Authentication*. Bei beiden Versionen kann der Server-Administrator *Nur FileMaker Konten* oder *FileMaker und Externe Server-Konten* wählen.

Es gibt mehrere Aspekte hinsichtlich Struktur und Einsatz, die Entwickler und IS/IT/DBA-Manager bedenken sollten, wenn sie die externe Authentifizierung einsetzen. Erstens deaktiviert die Auswahl der Option *Nur FileMaker Konten* nur die extern authentifizierten Konten in einer bestimmten FileMaker Pro 8 Datenbankdatei.

Zweitens gehören Benutzer in firmenweiten Domains normalerweise zu mehreren Domänen-Gruppen<sup>15</sup>. Damit stellt sich die Frage, mit welcher Gruppe der Benutzer für den Zugriff auf die Dateien authentifiziert werden soll. Die Benutzerin *Jane Smith* könnte Mitglied der Gruppen *FileMaker*, *Entwickler* und *FSA Partners* sein. Jede dieser Gruppen besitzt ein Konto in der Datenbankdatei und jedes dieses Konten hat völlig unterschiedliche Zugriffsrechte. Wie wird der Zugriff bestimmt? Die Antwort lautet, dass der Entwickler die Authentifizierungsreihenfolge im Register *Konten* des Dialogfelds *Konten und Berechtigungen definieren* der Datenbank festlegt. Das in der Reihenfolge der Authentifizierungs **erste** übereinstimmende Konto, bestimmt die Berechtigungen. Abb. 12 verdeutlicht dieses Konzept. Es zeigt, dass *Jane Smith* bei externer Authentifizierung die Verbindung mit dem Konto *FSA Partners* mit der Berechtigung *Superuser* herstellt. Entwickler müssen gemeinsam mit den IS/IT/DBA-Managern entsprechende Vorkehrungen treffen, um sicherzustellen, dass bei Benutzern, die Mitglied in mehreren Gruppen sein können, der Zugriff mit der erwarteten Zugriffsebene erfolgt. Solche Benutzer können bei Bedarf natürlich auch mit interner Authentifizierung auf die Dateien zugreifen.



Abb. 12. Die Authentifizierungsreihenfolge bestimmt, welches Konto und welche dazugehörige Berechtigung der externen Authentifizierung gewählt wird, wenn ein Benutzer zu mehreren Domain-Gruppen gehört.

Betrachten Sie noch einmal in den Abbildungen 11a und 11b die zweite Option *Sichere Verbindungen zu FileMaker Server*. Diese Option ist binär – sie ist entweder aktiviert oder deaktiviert. Ist sie aktiviert, wird der Datenverkehr zwischen FileMaker Pro 8 Clients und FileMaker Server 8 verschlüsselt, ebenso wie der Datenverkehr zwischen FileMaker Server 8 und der neuen Web Publishing Engine, sowohl bei Instant Web Publishing als auch bei Custom Web Publishing. Weitere Informationen zu den Auswirkungen dieser Option bei Web-basiertem Zugriff finden Sie im folgenden Abschnitt zum vereinheitlichten Modell.

Die dritte Option von FileMaker Server 8, die in den Abb. 11a und 11b gezeigt wird, bezieht sich auf die Anzeige der Dateinamen im Menübefehl *Remote öffnen* [Ablage/Datei - Remote öffnen...] in FileMaker Pro



8. In der einfachsten Stufe sorgt diese Option dafür, dass alle Datenbanken, deren Namen angezeigt werden sollen, erscheinen, wenn die Option *Alle Datenbanken anzeigen* markiert ist. Wählt der Administrator aber die Option *Nur die Datenbanken anzeigen, auf die der einzelne Benutzer zugreifen darf*, muss für den Benutzer in der Datenbank ein authentifiziertes Konto bestehen, damit er überhaupt darauf zugreifen kann.

Will ein Benutzer eine Verbindung zum Server herstellen, während diese Filterung wirksam ist, versucht FileMaker Pro 8 die für den betreffenden Benutzer gespeicherten Informationen zu verwenden. Unter Mac OS X wird hierzu der Schlüsselbund verwendet, unter Windows 2000 Professional und Windows XP Professional die Berechtigungsnachweise des Benutzers. Gibt es keine gültigen Übereinstimmungen, erscheint ein modaler Dialog, in dem der Benutzer einen Berechtigungsnachweis eingeben muss {Kontoname und Kontopasswort}, um die vom Server bereitgestellten Datenbanken sehen zu können. Dieser Dialog kann auch aufgerufen werden, indem der Benutzer die WAHL-Taste unter Macintosh OS X oder die SHIFT-Taste unter Windows 2000 Professional bzw. Windows XP Professional gedrückt hält, während er den Server-Namen im Menübefehl *Remote öffnen...* wählt. Macht der Benutzer ungültige Angaben, erscheint ein weiteres modales Dialogfeld, in dem er gebeten wird, sich mit anderen Berechtigungsnachweisen erneut beim Server anzumelden.

### **Web-basierter Zugriff: Das vereinheitlichte Sicherheitsmodell**

Die FileMaker Pro 8 Sicherheitsfunktionen gelten im vereinheitlichten Modell auch für Benutzer, die per Browser auf Datenbanken zugreifen. Der Entwickler kann Web-basierten Benutzern erlauben, eigene Konten anzulegen, und diese dann in die Datenbank einfügen. Hierfür gibt es zahlreiche Verwendungen, z. B. eine Online-Registrierung. Einer selbsterstellten Berechtigung kann das Konto eines Web-Benutzers genauso zugeordnet werden wie jedes andere Konto auch. Die Zugriffsrechte einer bestimmten Berechtigung gelten auch für Web-Benutzer, sowohl via Instant Web Publishing als auch via Custom Web Publishing. Hat ein LAN-Benutzer die Erlaubnis, per Browser auf eine Datei zuzugreifen, gelten die Berechtigungen des FileMaker Pro Clients im LAN auch für den Web-basierten Zugriff. Dadurch lassen sich auf Basis einzelner Konten und Tabellen sehr robuste Zugriffsregeln festlegen. Die Einstellungen für Dateifilterung gelten ebenfalls für den Web-basierten Zugriff.

Administratoren können auch in LAN-basierten FileMaker Pro Lösungen auf die Dateien über Web-Oberflächen zugreifen, falls die Berechtigungen so strukturiert sind, dass diese Funktion zulässig ist. Eventuell existieren interne Richtlinien, die dagegen sprechen; möglich ist es aber.

Web-basierte Benutzer können die neuen Verschlüsselungsfunktionen von FileMaker Server 8 nutzen. Das Aktivieren der Verschlüsselung erstellt einen verschlüsselten Kanal zwischen FileMaker Server 8 und den FileMaker Pro 8 Clients, ebenso wie zur Web Publishing Engine. Entwickler und IS/IT/DBA-Manager finden weitere Informationen zur Konfiguration der Web Publishing Engine in den technischen Briefings zu FileMaker Server und FileMaker Web Publishing. Sowohl Apache als auch Microsoft IIS unterstützen SSL-Verbindungen von modernen Browsern. Damit muss innerhalb des gesamten Datenleitung nur noch die Verbindung von der Web Publishing Engine zu Apache bzw. IIS geschützt werden. Hierzu existieren zahlreiche Ansätze.<sup>16</sup>

Damit FileMaker Server 8 und FileMaker Server 8 Advanced Web-basierte Verbindungen erlauben, muss der Server angewiesen sein, diese Verbindungen zuzulassen, und den entsprechenden Lizenzschlüssel besitzen. Lesen Sie hierzu die technischen Briefings zu FileMaker 8 Web Publishing und zu FileMaker Server 8. Ähnlich ist es bei



ODBC/JDBC-Verbindungen, bei denen die Annahme solcher Verbindungen ausdrücklich im Register *Clients* von FileMaker Server 8 und FileMaker Server 8 Advanced aktiviert werden muss. Zusätzlich muss der Entwickler, oder in manchen Fällen ein *Superuser*, für Verbindungen über Instant Web Publishing, Custom Web Publishing und ODBC/JDBC die entsprechenden erweiterten Zugriffsrechte in der bereitzustellenden Datei aktivieren. Diese erweiterten Zugriffsrechte können für jede Berechtigung einzeln konfiguriert werden.

Betrachten wir noch einmal den Bereich des Dialogfelds „Berechtigungen bearbeiten“, das wir in Abb. 7 gesehen haben. Abb. 13 zeigt diesen Bereich, in dem die Verwaltung der vier erweiterten Zugriffsrechte erfolgt.

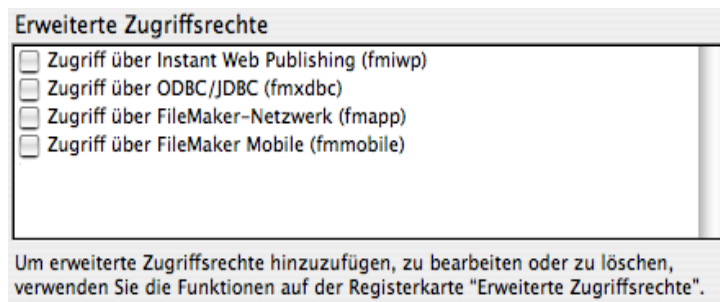


Abb. 13. Die standardmäßig vorhandenen „Erweiterten Zugriffsrechte“

Entwickler würden die Optionen für Instant Web Publishing (Schlüsselwort *fmiwp*) und ODBC/JDBC (*fmxdbc*) für diejenigen Berechtigungen markieren, denen sie dieses Zugriffsrecht einräumen wollen, einschließlich der Berechtigung [Voller Zugriff]. Danach können alle Konten, die dieser Berechtigung zugewiesen sind, auf diese Weise auf die Datei zugreifen, wenn sie von FileMaker Server 8 bereitgestellt wird. Doch dazu – um es deutlich zu sagen – muss eine komplette Abfolge von Sicherheitskontrollen durchlaufen werden:

- Erweiterte Zugriffsrechte aktiviert für eine bestimmte Berechtigung;
- Authentifizierte Berechtigungsnachweise {Kontoname und Kontopasswort} für das dieser Berechtigung zugewiesene Konto; und
- FileMaker Server mit korrekter Lizenzierung und Konfiguration für Verbindungen über Instant Web Publishing, Custom Web Publishing und ODBC/JDBC.

Schlägt eine dieser Kontrollen fehl, z. B. für das erweiterte Zugriffsrecht, kann auf die Datei von keinem Konto zugegriffen werden, das dieser Berechtigung zugewiesen ist, auch wenn die Datei von FileMaker Server bereitgestellt wird. Will ein Entwickler den Zugriff auf eine Datei per Custom Web Publishing erlauben, muss er zwei individuelle erweiterte Zugriffsrechte mit den Schlüsselwörtern *fmxml* und *fmxmlt* anlegen, je nach Art des gewünschten Custom Web Publishing Zugriffs.<sup>17</sup> In Abb. 14 sind diese Zugriffsrechte aktiviert, ebenso wie das für Instant Web Publishing.



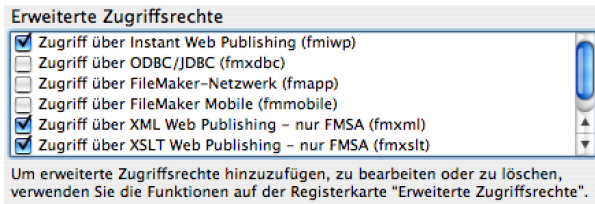


Abb. 14. Erweiterte Zugriffsrechte für Custom Web Publishing, zusammen mit dem erweiterten Zugriffsrecht für Instant Web Publishing.



Abb. 8 zeigte das Register „Erweiterte Zugriffsrechte“. Hier sehen Sie es noch einmal.

Nach Anklicken dieses Registers sieht das Dialogfeld ähnlich aus wie in Abb.15 gezeigt. Hier kann ein Entwickler oder ein *Superuser* mit entsprechenden Berechtigungen neue erweiterte Zugriffsrechte anlegen und sie den verschiedenen Berechtigungen zuweisen. Damit sind sie für alle Konten verfügbar, die zu diesen Berechtigungen gehören. Abb. 7 zeigt die Option *Erweiterte Zugriffsrechte verwalten* im Bereich *Andere Berechtigungen*, die das Recht zum Verwalten erweiterter Zugriffsrechte für eigene nachgeordnete Berechtigung erteilt. Jeder Benutzer mit einem authentifizierten Konto, das zu dieser Berechtigung gehört, kann erweiterte Zugriffsrechte verwalten.

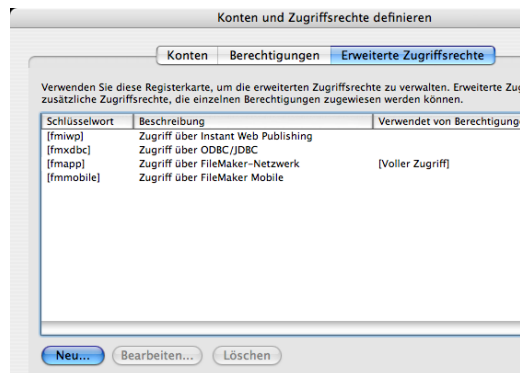


Abb. 15. Dialogfeld „Konten und Zugriffsrechte definieren“ für die erweiterten Zugriffsrechte

Klickt der Entwickler oder *Superuser* in *Neu...* oder *Bearbeiten...*, erscheint ein Dialogfeld wie das in Abb. 16 zeigte. Hier können neue, eigene erweiterte Zugriffsrechte angelegt und Berechtigungen zugewiesen werden. Entwickler, die Benutzern Zugang zu diesem Dialogfeld gewähren, sollten bedenken, dass hier auch erweiterte Zugriffsrechte von allen Konten in der Datei entfernt werden können, einschließlich derjenigen, die



zu Berechtigungen mit [Voller Zugriff] gehören. Offensichtlich ist dies nur selten erwünscht. Der Entwickler muss genau abwägen, welche Auswirkungen das Erteilen dieser Berechtigung hat. In firmenweiten Installationen werden aber wohl mindestens der Administrator oder einige *Superuser* die Berechtigung haben müssen.

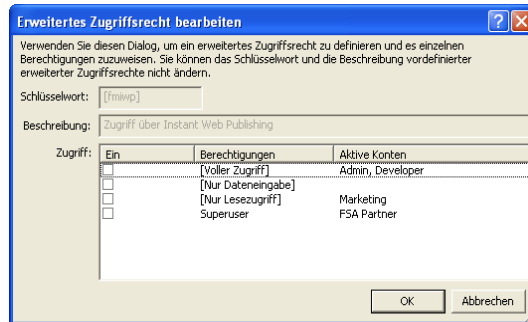


Abb. 16. Bearbeiten und Zuweisen der Erweiterten Zugriffsrechte.

## FileMaker Pro 8 beseitigt wesentliche Probleme bei der Sicherheitsverwaltung

Das neue FileMaker Pro 8 Sicherheitsmodell verbessert die Funktionen früherer Produktversionen. Hier sind in erster Linie zu nennen: Zugriffskontrolle, Abfangen des Netzwerkverkehrs, fein abgestufte Zugangssteuerung zu Objekten und Funktionen, Auslesen von Passwörtern und Manipulation von FileMaker Pro Dateien in Texteditoren.

### Verwaltung von Konten

In früheren Versionen von FileMaker Pro war es für Entwickler und Administratoren sehr aufwändig, mehrere Passwörter und Gruppen zu verwalten, vor allem in Mehr-Dateien-Lösungen. Im neuen FileMaker Pro 8 kann eine Datei mehrere Tabellen umfassen. Auf den ersten Blick scheint dies die Probleme der Sicherheitsverwaltung bei Mehr-Dateien-Lösungen zu beseitigen. Manche Entwickler werden einfach eine Mehr-Dateien-Lösung zu einer Mehr-Tabellen-Lösung *in einer einzigen Datei* zusammenfassen, in der sich alle Sicherheitsoptionen zentral verwalten lassen. Obwohl es viele Fälle gibt, in denen die geeignete Architektur *eine Datei und mehrere Tabellen* erfordert, gibt es wahrscheinlich ebenso viele Fälle, in denen Struktur und geschäftliche Abläufe Lösungen mit *mehreren Dateien und mehreren Tabellen* erfordern. Darüber hinaus ergibt die Konvertierung einer FileMaker Pro 6 Lösung mit mehreren Dateien zu FileMaker Pro 8 eine FileMaker Pro 8 Lösung mit mehreren Dateien, bei der das Sicherheitsschema noch immer in *mehreren Dateien* verwaltet werden muss.

Entwickler können jetzt Administratoren oder anderen *Superusern* erlauben, die Konten geöffneter Dateien zu verwalten. Dabei vorgenommene Änderungen treten sofort in Kraft. Ein *Superuser* kann neue Konten anlegen, bestehende Konten löschen, deaktivieren oder aktivieren und Kontopasswörter zurücksetzen. Beim letztgenannten Vorgang kann der *Superuser* ein neues Kontopasswort festlegen oder festlegen, dass der Benutzer bei der nächsten Anmeldung ein neues Passwort wählen muss.

**Diese Fähigkeit kann sich auf alle Dateien einer Lösung erstrecken. Der Superuser benötigt keinen Zugriff auf das Datenbankschema, also Tabellen, Felder und Beziehungen, um Konten verwalten zu können.** Entwickler kommerzieller Lösungen können somit in ihre Lösungen Funktionen zu Kontenverwaltung integrieren, die helfen, das geistige Eigentum des Entwicklers zu schützen.



Anders als der Entwickler, der Kontonamen und Passwörter über das Menü *Ablage/Datei* [Ablage/Datei - Definieren - Konten und Berechtigungen] definiert, verwaltet der *Superuser* Kontonamen, Kontopasswörter und Kontostatus über Scripts. Die erforderlichen Schritte befinden sich in der neuen ScriptMaker Kategorie *Konten*. Über die Eingabefelder des Scriptschritts *Eigenes Dialogfeld anzeigen* kann der Administrator oder *Superuser* an andere Scriptschritte Variablen weitergeben, z. B. *Konto hinzufügen*. Dies funktioniert bei jeweils einem Konto.

Will der *Superuser* aber fünfzig neue Konten in einer oder mehreren Dateien *gleichzeitig* anlegen, können die entsprechenden Variablen von einer Datei zur nächsten weitergereicht und die entsprechenden Aktionen in einer Datei nacheinander und für ein Konto nach dem anderen ausgeführt werden. Dies klingt komplex und zeitaufwändig, ist es aber nicht. Mit dieser automatisierten Methode war es möglich, in weniger als zwei Minuten 1.000 neue, eindeutige Konten in einer einzigen Datei anzulegen. Dieser automatisierte, per Script ablaufende Vorgang reicht einfach die erforderlichen Variablen für *Kontoname* und *Kontopasswort* nacheinander von einer Steuerdatei an die Zieldatei weiter.

Neben den ScriptMaker Scriptschritten zur Kontoverwaltung gibt es noch den neuen ScriptMaker Schritt „*Erneut anmelden*“, der für die Sicherheitsverwaltung außerordentlich nützlich ist. Über diesen Schritt kann sich der *Superuser* mit einem anderen Konto erneut anmelden, ohne die Datei schließen zu müssen.

Aber wie können *Superuser* oder Administratoren ohne Zugriff auf eine Datei mit [Voller Zugriff] die Sicherheitsverwaltung ausüben? Entwickler können Benutzern vorübergehend erlauben, durch ein Script Aktionen ausführen zu lassen, für die sie selbst keine Berechtigung haben. Jedes Script besitzt die Option „**Script mit vollen Zugriffsrechten ausführen**“, die der Entwickler für jedes Script einzeln einstellen kann. Die Kontoverwaltung wird dadurch möglich, dass eine individuelle, nachgeordnete Berechtigung für das Konto des *Superusers* auf die Scripts zur Kontoverwaltung beschränkt wird, diese aber mit vollen Zugriffsrechten ablaufen. Abb. 17 zeigt den Schalter „Script mit vollen Zugriffsrechten ausführen“ im Dialogfeld *Script bearbeiten*.

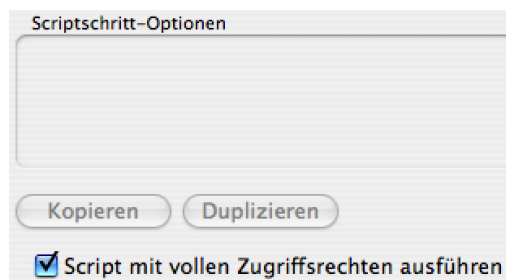


Abb. 17. Optionen für Script-Zugriff mit vollen Zugriffsrechten.

Ist die Option markiert, wird das Script ausgeführt<sup>18</sup>, als wäre der Benutzer mit einem Konto angemeldet, für das die Berechtigung [Voller Zugriff] aktiviert ist. Es ist wichtig zu beachten, dass dies nur für das *Script* gilt, nicht für den Benutzer. Zusammen mit der Möglichkeit, den Script-Zugriff für jede einzelne Berechtigung zu konfigurieren, kann der Entwickler sehr präzise festlegen, wer welche Aktionen ausführen darf. Mit derselben Funktion kann ein Entwickler auch einem *Superuser*, der über ein Konto mit einer bestimmten nachgeordneten Berechtigung angemeldet ist, den Zugriff auf die Funktionen *Datenbank definieren* und *Dateiverweise definieren* gestatten. Es ist klar, dass diese Berechtigung nur selten und mit Bedacht gewährt werden sollte.



## Verschlüsselter Netzwerkverkehr

In früheren Versionen des Produkts konnte Software zur Paketaufspürung genutzt werden, um über Netzwerke gesendete kodierte FileMaker Pro Passwörter zu entdecken, speziell wenn die vorherige Version von FileMaker Server sie auf kodierte Weise zur Verifikation an einen Gast schickte, bevor sie Zugriff auf die Datei gestattete.

In FileMaker Pro 8 erfolgt die Authentifizierung aber auf Server- und nicht auf Client-Ebene. Da Passwörter nicht in den Dateien gespeichert werden<sup>19</sup>, ist es viel schwieriger, sie abzufangen. Dazu kann, wie bereits im Abschnitt über FileMaker Server erwähnt, der Netzwerkverkehr jetzt in verschlüsselten Paketen übertragen werden. FileMaker Pro 8 und FileMaker Server 8 verwenden Sicherheitsalgorithmen, die weithin getestet wurden und als Industriestandards akzeptiert sind.

Die neuen FileMaker Pro und FileMaker Server Versionen verwenden die Industriestandard-Verschlüsselung TripleDES mit zusätzlichem HMACSHA-1 zur Integritätsprüfung<sup>20</sup>. TripleDES ist ein symmetrischer Algorithmus, der einen älteren Bruder namens DES (Data Encryption Standard) nutzt. DES wiederum ist ein Blockchiffre, der auf einen jeweils 64 Bit großen Datenblock einen Schlüssel mit 56 Bit anwendet. TripleDES ist eine große Verbesserung von DES, da das DES-Chiffre dreimal mit drei verschiedenen Schlüsseln angewendet wird, was einen 168-Bit-Schlüssel ergibt. Eine Darstellung der Funktionsweise von symmetrischer und asymmetrischer Verschlüsselung, öffentlicher Schlüssel usw. würde den Rahmen dieses technischen Briefings sprengen; die Bibliographie nennt jedoch einige Referenzen für Entwickler.

## Auslesen von Passwörtern

Die Verwendung so genannter „Passwort-Knacker“ war seit jeher ein Dorn im Auge von FileMaker Pro Entwicklern, die ihr geistiges Eigentum schützen und in ihren Lösungen Datenintegrität und Datenvertraulichkeit sicherstellen wollten. Diese ruchlosen kleinen Programme extrahierten einfach die Passwörter aus der Datei und stellten sie im Klartext dar. Außerdem waren, wie bereits angemerkt, schwach kodierte Kennwörter, die in TCP-Paketen über das Netzwerk gesendet wurden, anfällig dafür, abgefangen und entschlüsselt zu werden.

FileMaker Pro 8 speichert in der Datei nicht das Passwort, sondern das *Hash* des Passworts. Ein *Hash* ist das einmalige, unumkehrbare Resultat der Anwendung einer mathematischen Regel auf eine Datenfolge. Auch wenn das Hash<sup>21</sup> ausgelesen wird, ist es rechnerisch nicht möglich, den Vorgang umzukehren, um die gesuchten Daten zu erhalten: das *Passwort*. Legt der Benutzer einen Berechtigungsnachweis zur Authentifizierung vor, *hasht* FileMaker Pro den Nachweis und vergleicht das Ergebnis mit dem in der Datei. Besteht eine Übereinstimmung, wird der Benutzer als gültig authentifiziert. Daher ist es außerordentlich schwierig, Passwörter zu „knacken“.

## Andere beseitigte Probleme

FileMaker Pro 8 verwendet ein Unicode-Textformat. Temporäre Dateien, die an Clients gesendet werden, treffen in einem komprimierten Unicode-Format ein, was das Lesen mit einem Texteditor sehr schwierig macht. Zusätzlich zur Komprimierung sind die Dateien auch stark verschlüsselt.

Wir haben bereits im Abschnitt zur *Feinabstufung* angesprochen, dass FileMaker Pro 8 das Probleme beseitigt, vor denen vor allem Entwickler kommerzieller Lösungen, in früheren Version standen: zum einen ihr geistiges



Eigentum zu schützen, zum anderen Endbenutzern die Möglichkeit zu geben, eine Lösung in angemessenem Rahmen anpassen zu können. Dass Entwickler jetzt bestimmten Benutzerklassen das Anlegen neuer Objekte wie Layouts, Scripte und Wertelisten, nicht aber das Ändern bestehender Objekte dieser Art gestatten können, bietet ihnen ganz neue Flexibilität beim Design ihrer Lösungen. Dies wiederum hat beträchtliche Auswirkungen auf ihre Geschäftsmodelle, wie wir im letzten Abschnitt dieses technischen Briefings sehen werden.

### Probleme bei der Konvertierung früherer Versionen

Viele Entwickler und IS/IT/DBA-Manager werden bestehende Lösungen von FileMaker Pro 6 oder sogar älteren Versionen konvertieren, um die zahlreichen neuen Funktionen von FileMaker Pro 8, FileMaker Server 8 und FileMaker Server 8 Advanced zu nutzen. Je nach Aufbau des Sicherheitsschemas in den früheren Versionen wird eine Anzahl älterer Techniken aufgegeben, vor der Konvertierung umgebaut oder nach der Konvertierung korrigiert werden müssen, wenn die Sicherheitsfunktionen die gleichen Resultate wie zuvor erzielen sollen. Die Konvertierung ist ein komplexes Thema, das allein im Bereich der Sicherheit zahllose Feinheiten birgt. Entwickler finden in der Dokumentation auf der FileMaker Website umfangreiche und ausführliche Informationen zu diesen Themen.

Schlecht strukturierte Sicherheitspläne in FileMaker Pro 6 Dateien können bei der Konvertierung eine besondere Problemquelle darstellen. Fehlende Eindeutigkeit bei Gruppen, Nichtbeachtung von Groß-/Kleinschreibung bei Passwörtern und Gruppen und das Zuweisen von Passwörtern zu mehr als einer Gruppe – speziell Gruppen mit unterschiedlichen Zugriffsrechten – können in konvertierten Dateien zu unerwarteten Ergebnissen führen.

FileMaker Pro 6 Gruppen werden zu FileMaker Pro 8 Berechtigungen konvertiert. Die Konvertierung versucht, alte Berechtigungen für Gruppen und dazugehörige Passwörter möglichst genau zu duplizieren. Trotzdem sollten Entwickler konvertierte Berechtigungen überprüfen und dabei beachten, dass für einige Funktionen, z. B. die Dateifreigabe, jetzt erweiterte Zugriffsrechte aktiviert sein müssen. Hat ein Entwickler in FileMaker Pro 6 eine Gruppe speziell für das „Hauptkennwort“ angelegt, z. B. eine Gruppe namens „Nur\_Entwickler“, werden die Passwörter dieser Gruppe zu Konten, die der FileMaker Pro 8 Standardberechtigung [Voller Zugriff] zugewiesen werden. Außerdem wird FileMaker Pro 8, im Rahmen von Aufräumarbeiten und Redundanzbeseitigung, Gruppen mit identischen Berechtigungen zu einer *einzelnen, vereinheitlichten* untergeordneten Berechtigung konsolidieren, normalerweise mit mehreren Kontonamen und Passwörtern. Bei der Konvertierung zu FileMaker Pro 8 werden die alten FileMaker Pro 6 Passwörter **sowohl** als Name als auch als Passwort des Kontos verwendet. Da Kontonamen bei der Anmeldung im Klartext eingegeben werden, ließe sich so auch das Passwort ermitteln. Daher sollte sofort nach der Konvertierung der Kontoname so geändert werden, dass er sich vom Passwort unterscheidet.

Dieser Vorgang verursacht Probleme bei konditionalen Tests, die auf den alten Filemaker Pro 6 Gruppennamen angewiesen sind, der mit der Funktion STATUS(AKTUELLGRUPPEN) ausgelesen wurde. STATUS (AKTUELLGRUPPEN) wurde durch HOLE (DATEI BERECHTIGUNGEN) ersetzt; dies ist eine der neuen Hole-Funktionen, die die alten Status-Funktionen ersetzen. Dieser Test hat in FileMaker Pro 8 **ein anderes Ergebnis** als in FileMaker Pro 6, wenn sich der Berechtigungsname vom früheren Gruppennamen unterscheidet. Dies geschieht bei der Berechtigung [Voller Zugriff] nach der Konvertierung einer Gruppe, die speziell für Hauptkennwörter existierte. Es geschieht auch, wenn FileMaker Pro 6 Gruppen und Passwörter mit *identischen* Berechtigungen, aber *verschiedenen* Passwörtern konsolidiert wurden.



Betrachten Sie z. B. die Syntax des folgenden ScriptMaker Scriptschritts, der das „Hauptkennwort“ abfragt: **[Wenn (MusterAnzahl, Status(AktuellGruppen), „Nur\_Entwickler“))]**

Diese Formel hat in FileMaker Pro 6 das Ergebnis „Wahr“. In FileMaker Pro 8 funktioniert sie aber nicht mehr, da sie jetzt [MusterAnzahl (Hole(Datei Berechtigungen) ; „Nur-Entwickler“)] lautet, die Berechtigung aber [Voller Zugriff] heißt. Eine ähnliche Situation ergibt sich, wenn Passwörter mit identischen Berechtigungen einzeln zu unterschiedlichen, identischen Gruppen zugewiesen wurden. Hier könnte ein Test z. B. lauten: **[Wenn (MusterAnzahl, Status(AktuellGruppen), „VertriebMitarbeiter“))]**

Dieser Test hat in FileMaker Pro 6 das Ergebnis „Wahr“, funktioniert in FileMaker Pro 8 jedoch nicht, da die Gruppe „VertriebMitarbeiter“ mit Gruppen wie „MarketingMitarbeiter“ und „GeschäftsführungMitarbeiter“ zu einer einzelnen Berechtigung zusammengefasst wurde, die z. B. „MarketingMitarbeiter“ heißen könnte.

Entwickler müssen konvertierte Dateien überprüfen, um solche Abweichungen zu erkennen und für Abhilfe zu sorgen. Die folgende Tabelle listet einige, aber längst nicht alle Stellen auf, an denen solche Tests vorkommen.

Konditionale Scriptsteuerung [Wenn...]	Formeln für Formelfelder
Tests für Zugriff auf Datensatzebene	Automatisch eingegebene, berechnete Werte
Feldüberprüfung durch Berechnung	Konditionale Wertelisten
ScriptMaker Scriptschritte „Feldwert setzen“ und „Berechneten Wert einfügen“	AppleScript oder VB Skripte, die ganz oder teilweise aus Formelfeldern generiert werden
Scriptschritt „Ersetze alle Feldwerte“	Scriptschritt „Eigenes Dialogfeld anzeigen“

Entwickler müssen in vielen Fällen vor der Konvertierung ihre Lösungen auf potenzielle Sicherheitsprobleme überprüfen. Hierzu empfiehlt sich der „Datenbankbericht“ in FileMaker Pro 6 Developer oder die Werkzeuge „MetaDataMagic“ und „PasswordAdministrator“ von New Millennium Communications, Inc.<sup>22</sup> Achten Sie in allen Lösungsdateien auf Groß-/Kleinschreibung bei Passwörtern. Die Passwörter *Hans Müller*, *Hans müller* und *HaNs müller* sind in FileMaker Pro 6 identisch, nicht aber in FileMaker Pro 8.<sup>23</sup> Mit MetaDataMagic lassen sich Stellen aufspüren, an denen STATUS(AKTUELLEGRUPPEN) verwendet wurde, und vor oder nach der Konvertierung korrigieren.

### Auswirkungen auf Geschäftsmodelle und Abläufe bei Entwicklern und IS/IT/DBA-Managern

Die neuen Sicherheitsfunktionen von FileMaker Pro 8 und FileMaker Server 8 werden tiefgreifende Auswirkungen auf die Arbeitsweise von kommerziellen Lösungsentwicklern, selbständigen Entwicklern und IS/IT/DBA-Managern haben, ebenso wie auf die Geschäftsmodelle, welche die beratende Tätigkeit vieler Entwickler bestimmen.

Entwickler kommerzieller Lösungen mussten seit Jahren um den Schutz ihres geistigen Eigentums fürchten. Um dem Endbenutzer größtmögliche Flexibilität zu bieten, waren diese Entwickler in vielen Fällen gezwungen, ihre Lösungen in Formaten weiterzugeben, die entweder ungeschützt waren oder vollen Zugriff erlaubten. Die Alternativen bestanden in der zeitaufwändigen Aktualisierung von Kundendateien, dem Neuimport von Daten, der Verwaltung von Passwörtern und Gruppen sowie zahlreichen ähnlichen Zugriffsproblemen.



In FileMaker Pro 8 ist der Großteil dieses Zusatzaufwandes nicht mehr nötig. Entwickler können Endbenutzern, meist Administratoren oder *Superusern*, die Möglichkeit einräumen, Konten zu verwalten und eine Reihe von Objekten zu erstellen, wie Scripts, Layouts und Wertelisten, *ohne* dabei bestehende Objekte dieser Art zu beeinflussen oder Zugriff darauf zu erhalten. Ebenso müssen kommerzielle Entwickler nicht mehr befürchten, dass die Hauptkennwörter ihrer Lösungsdateien „geknackt“ werden und somit eine unautorisierte Nutzung ihrer Arbeit möglich ist. Falls ein kommerzieller Entwickler seine Lösung in die bestehende Lösung eines Kunden integrieren will, hat er darüber hinaus jetzt auch die Möglichkeit, in seine Lösung Einsprungstellen für Aufrufe aus der bestehenden Lösung einzubauen und diese mit erweiterten Zugriffsrechten zu schützen, was völlig neue Möglichkeiten für Produktgestaltung und -entwicklung eröffnet.

Selbständige Entwickler arbeiten in einem anderen Umfeld; sie erstellen individuelle Lösungen für spezifische Anforderungen und Abläufe eines Kunden. Das neue Sicherheitsmodell unterstützt auch dieses Geschäftsmodell. Selbständige Entwickler müssen jetzt nicht mehr die Verantwortung für die Verwaltung eines Mitarbeiterstamms tragen, der möglicherweise stark fluktuiert oder in dem sich Rollen häufig ändern. Auch hier hat der Entwickler die Möglichkeit, *Superusern* die Möglichkeit zum Erstellen, Deaktivieren, Aktivieren, Löschen und Zurücksetzen von Konten zu geben, und kann sich somit während der Dauer des Projekts darauf konzentrieren, die Funktionen des Systems zu perfektionieren und die Elemente der Datenbank exakt an die spezifischen Anforderungen und geschäftlichen Abläufe des jeweiligen Kunden anzupassen.

IS/IT/DBA-Mitarbeiter können jetzt bestehende Ressourcen nutzen, um die Sicherheit einer breiten Palette von FileMaker basierten Ressourcen zu realisieren, sei es im LAN oder WAN, beim Zugriff über einen Browser oder bei Software anderer Hersteller, die ODBC oder JDBC-Verbindungen nutzt. Die Authentifizierung für diese Ressourcen per Einmalanmeldung erleichtert es der IT-Abteilung, ihrer Verantwortung für die Sicherheit des Unternehmens nachzukommen, und vereinfacht das Hinzufügen oder Entfernen von Benutzern. Die Einführung verschlüsselter Datenübertragung zwischen FileMaker Server auf der einen und den FileMaker Pro Clients, einschließlich Web Publishing Engine, auf der anderen Seite ist für IT-Abteilungen eine große Hilfe, um die Sicherheitsrichtlinien ihres Unternehmens umzusetzen.

## Fazit

Die neuen Sicherheitsfunktionen von FileMaker Pro 8, FileMaker Server 8 und FileMaker Server 8 Advanced bieten einen neuen und dramatisch verbesserten Ansatz für den Schutz des geistigen Eigentums, die Vertraulichkeit von Daten und die Unverletzlichkeit von Daten. Durch sehr fein abgestufte Berechtigungen für den Zugriff auf FileMaker Pro Objekte, die Nutzung von als Industriestandard etablierten Mechanismen zur Kontoauthentifizierung und den Einsatz von Verschlüsselungsmechanismen für den Datenschutz bietet das neue Sicherheitsmodell Entwicklern und IS/IT/DBA-Managern viel mehr Sicherheit und Gewissheit als in der Vergangenheit. Diese Funktionen sind in neu angelegten FileMaker Pro Dateien von Anfang an vorhanden, und sie sind ebenfalls sofort verfügbar, wenn FileMaker Pro 8 eine Datei von einer früheren Version konvertiert.

Entwickler und IS/IT/DBA-Manager müssen und sollen das Thema Sicherheit ernst nehmen. Mit dem neuen Sicherheitsmodell erhalten sie alle erforderlichen Werkzeuge, damit sie ihrer Verantwortung gerecht werden können.



## Über den Autor

STEVEN H. BLACKWELL ist Partner-Mitglied der FileMaker Solutions Alliance und Präsident und CEO von Management Counseling Services [<http://www.FMP-Power.com>]. Er ist zweimaliger Gewinner des FileMaker Excellence Award und hat sich auf die Entwicklung individueller FileMaker Pro Lösungen, die Beratung bei FileMaker Pro Sicherheitsfragen und den Einsatz von FileMaker Server spezialisiert.

©2005 FileMaker, Inc. Alle Rechte vorbehalten. FileMaker ist eine Marke von FileMaker, Inc., eingetragen in den USA und anderen Ländern, und das Dateiordner-Logo und ScriptMaker sind Warenzeichen von FileMaker, Inc. Alle anderen Warenzeichen gehören ihren jeweiligen Besitzern. Sämtliche in den Beispielen aufgeführten Unternehmen, Organisationen, Produkte, Domain-Namen, E-Mail-Adressen, Logos, Personen, Orte und Ereignisse sind frei erfunden. Jede Ähnlichkeit mit lebenden Personen oder existierenden Firmen wäre rein zufällig. Technische Daten und Verfügbarkeit von Produkten können sich jederzeit ohne vorherige Ankündigung ändern. (Doc v3)

DIESES DOKUMENT WIRD IN DER VORLIEGENDEN FORM OHNE IRGENDNEINE GEWÄHRLEISTUNG ZUR VERFÜGUNG GESTELLT. FILEMAKER SCHLIESST JEDLICHE AUSDRÜCKLICH ODER STILLSCHWEIGEND VEREINBARETE GEWÄHRLEISTUNG AUS, EINSCHLIESSLICH INSBESONDERE DER IMPLIZITEN GEWÄHRLEISTUNG DER VERKÄUFLICHKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER GEWÄHRLEISTUNG BETREFFEND VERBORGENER MÄNGEL. IN KEINEM FALL KANN FILEMAKER ODER EINER SEINER LIEFERANTEN FÜR SCHÄDEN JEDWEDER ART HAFTBAR GEMACHT WERDEN, EINSCHLIESSLICH UNMITTELBARER SCHÄDEN, MITTELBARER SCHÄDEN, BEILÄUFIGER SCHÄDEN ODER FOLGESCHÄDEN, ENTGANGENER GESCHÄFTSGEWINNE, BUSSGELDER ODER BESONDERER SCHÄDEN, AUCH WENN FILEMAKER ODER SEINE LIEFERANTEN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDEN. EINIGE LÄNDER ERLAUBEN DEN AUSSCHLUSS ODER DIE BESCHRÄNKUNG DER HAFTBARKEIT NICHT. FILEMAKER KANN DIESES DOKUMENT JEDERZEIT OHNE VORHERIGE ANKÜNDIGUNG ÄNDERN. DIESES DOKUMENT IST MÖGLICHERWEISE VERALTET, UND FILEMAKER ÜBERNIMMT KEINE VERPFLICHTUNG ZUR AKTUALISIERUNG DER HIERIN ENTHALTENEN INFORMATIONEN.

### (Endnoten)

<sup>1</sup> Bruce Schneier, Gründer von Counterpane Labs, der führenden Firma für digitale Sicherheit, hat diese Probleme mit großer Überzeugungskraft und Beredsamkeit in seinem Buch *Secrets & Lies* erklärt (s. Bibliographie).

<sup>2</sup> Im FileMaker Tech Info Letter Nr. 108462 und in dem auf der FileMaker Website verfügbaren White Paper *Web Security* werden diese Themen detailliert behandelt.

<sup>3</sup> Eine Domain-Gruppe aus Active Directory oder Open Directory, nicht eine der alten FileMaker Pro 6 Gruppen.

<sup>4</sup> Bestimmte Sonderzeichen aus dem hohen ASCII-Bereich können Probleme verursachen, falls sie in FileMaker Pro 8 für den Zugriff von Web-basierten Konten benutzt werden. Einzelheiten hierzu finden Sie im PDF-Dokument *Web Publishing Guide* auf der FileMaker, Inc. Website.

<sup>5</sup> Wählen Sie im Menü *Ablage* bzw. *Datei* den Befehl „Dateioptionen...“ und deaktivieren Sie im Register „Öffnen/Schließen“ die automatische Anmeldung.



<sup>6</sup> Wie von entweder Active Directory oder Open Directory festgelegt.

<sup>7</sup> Ein Konto, dessen Berechtigung vollen und uneingeschränkten Zugriff auf alle Bereiche der Datei erlaubt. Das entspricht ungefähr dem Konzept des „Hauptpassworts“ in FileMaker Pro 6. Dieser Begriff ist jedoch veraltet und trifft in FileMaker Pro 8 nicht mehr zu.

<sup>8</sup> Zu diesem Zweck existieren zahlreiche Ressourcen; einige davon sind in der Bibliographie dieses technischen Briefings aufgeführt.

<sup>9</sup> Kontoname und Passwort des Kontos könnten mit dem Namen der Berechtigung identisch sein, z. B. *Marketing* oder *Vertrieb*. Achten Sie darauf, diese Testkonten am Ende des Entwicklungsprozesses zu löschen. Jeder Berechtigung können dann neue, „echte“ Konten zugewiesen werden.

<sup>10</sup> Weitere Informationen zum rollenbasierten Zugriff finden Sie im *FileMaker Advisor* Magazin, Januar 2004.

<sup>11</sup> Diese Funktion gibt den Namen des Kontos zurück, das auf die Datei zugreift. Bei externer Authentifizierung gibt es ebenfalls den Namen des Kontos zurück und **nicht** den Gruppennamen. Beachten Sie hierzu aber auch die Besprechung der Authentifizierungsreihenfolge.

<sup>12</sup> Konvertierte Datenbanken, in denen in früheren Versionen automatisch entweder der Name der Benutzers bei der Erstellung oder der letzten Änderung eingetragen wurde, sollten bei den Felddefinition in den Optionen für die automatische Eingabe auf den Kontonamen umgestellt werden. Allerdings muss die konvertierte Datei dann so angepasst werden, dass entweder der Kontoname dem Benutzernamen entspricht oder umgekehrt, vor allem wenn Tests für den Zugriff auf Datensatzebene auf diese Daten zurückgreifen.

<sup>13</sup> Das eigentliche Sicherheitsproblem ist dabei, dass der Entwickler mit der Erlaubnis zum Anlegen auch die Erlaubnis zur *Veränderung* der vom Entwickler erstellten Objekte derselben Klasse erteilt.

<sup>14</sup> Weitere Informationen zu den Protokollfunktionen finden Sie im technischen Briefing von FileMaker Inc. zu FileMaker Server 8, verfasst von Wim Decorte.

<sup>15</sup> Auch hier sind die unternehmensweiten Domain-Gruppen von Active Directory oder Open Directory gemeint, **nicht** die alten Gruppen von FileMaker Pro 6.

<sup>16</sup> Beispielsweise durch Installation von WPE und IIS/Apache auf demselben Computer, durch Einsatz eines VPN zwischen ihnen, falls sie (wahrscheinlich) auf verschiedenen Computern laufen, oder durch ein geschlossenes Netzwerk zwischen den Computern, auf denen FileMaker Server 8, WPE und Apache/IIS laufen. Die Multihoming-Fähigkeiten von FileMaker Server 8 erweitern die Möglichkeiten für solche Konfigurationen. Lesen Sie hierzu die technischen Briefings zu FileMaker Server und FileMaker Web Publishing. Für einige vorläufige beste Praktiken scheint es nötig zu sein, dass WPE und IIS/Apache auf demselben Computer laufen und Firewalls zur Gewährleistung der Datenvertraulichkeit eingesetzt werden. Übrigens sind Dual-Prozessor-Computer besonders gut für solche Konfigurationen geeignet.



<sup>17</sup> Weitere Einzelheiten finden Sie im technischen Briefing von FileMaker, Inc. zu FileMaker 8 Web Publishing, verfasst von Cris Ippolite.

<sup>18</sup> Für jedes aufgerufene Teilsript muss ebenfalls diese Option aktiviert sein, wenn es in der Lage sein soll, eine Aktion auszuführen, für die Berechtigungen mit [Voller Zugriff] erforderlich sind.

<sup>19</sup> Dies bedeutet auch, dass sie in der Benutzeroberfläche nicht sichtbar sind. Sie werden bei der Eingabe nicht angezeigt, und sie bleiben unsichtbar.

<sup>20</sup> <http://java.sun.com/j2se/1.4.2/docs/guide/security/jce/JCERefGuide.htm> enthält eine gute zusammenfassende Beschreibung des Hashed Message Authentication Code (HMAC).

<sup>21</sup> [http://searchDatabase.techtarget.com/sDefinition/0,,sid13\\_gci212230,00.html](http://searchDatabase.techtarget.com/sDefinition/0,,sid13_gci212230,00.html) enthält weitere Informationen zu Hashes.

<sup>22</sup> <http://www.newmillennium.com>

<sup>23</sup> Und denken Sie daran, dass Benutzer auf die korrekte Eingabe von Groß-/Kleinschreibung trainiert werden müssen, um alten Gewohnheiten entgegenzuwirken.

## Bibliografie

### Bücher

Alberts, Christopher J. und Dorofee, Audrey J. *Managing Security Risks. The OCTAVE™ Approach* (Addison-Wesley, New York, NY, 2002)

Barrett, Diane, Hausman, Kirk, und Weiss, Martin. *Security+* (Que, Indianapolis, IN, 2003)

Schneier, Bruce. *Secrets & Lies. Digital Security in a Networked World* (John Wiley & Sons, New York, NY, 2000)

Singh, Simon. *The Code Book* (Anchor Books, New York, 1999)

Strebe, Matthew. *Network Security Jumpstart* (Sybex, San Francisco, 2002)

### Artikel

“Internet Security” *Time*, 2.7.2001

Andress, Mandy und Edward, Mark T. „Beware Wireless Security Woes“ *E Business Advisor*, März 2002

Chang, Stephanie und Janowski, Davis D. „The lay of the wireless LAN“ *PC Magazine*, 21.5.2002

Hawkins, Dana. „Hide and they can't seek“ *US News & World Report*, 19.5.2003

Kerstetter, Jim und Weintraub, Arlene. „Cyber Alert. Portrait of an Ex-Hacker“ *Business Week*, 9.6.2003

Kerstetter, Jim. „You're Only As Good As Your Password“ *Business Week*, 2.9.2002

Marelia, Darren. „AD network Interactions“ *Windows & .Net magazine*, 1.3.2003

Vacca, John R. „Save Money With a Secure Remote-Access VPN“ *Business Security Advisor*, Juli/August 2002

