

FileMaker® 8

Sicherheitshandbuch



© 2004-2005 FileMaker, Inc. Alle Rechte vorbehalten.

FileMaker, Inc.

5201 Patrick Henry Drive

Santa Clara, California 95054, USA

FileMaker ist eine Marke von FileMaker, Inc., eingetragen in den USA und anderen Ländern, und ScriptMaker und das Dateiodner-Logo sind Marken von FileMaker, Inc.

Die FileMaker-Dokumentation ist urheberrechtlich geschützt. Sie dürfen diese Dokumentation ohne schriftliche Genehmigung von FileMaker weder vervielfältigen noch verteilen. Diese Dokumentation darf ausschließlich mit einer gültigen, lizenzierten Kopie der FileMaker-Software verwendet werden.

Alle in den Beispielen erwähnten Personen und Firmen sind rein fiktiv und jegliche Ähnlichkeit mit bestehenden Personen und Firmen ist rein zufällig.

Die Danksagungen und Urheberrechtshinweise finden Sie im entsprechenden Dokument, das mit der Software geliefert wurde.

Weitere Informationen finden Sie auf unserer Website:
www.filemaker.de.

Edition: 01

Inhalt

Kapitel 1

Datenbanksicherheit

Über dieses Handbuch	5
Sicherheitsziele	5
Potenzielle Gefahren für Ihre Daten	6
Sicherheitsplanung	7

Kapitel 2

Die Top 10 in puncto Sicherheit

1. Physische Sicherheit verbessern	9
2. Betriebssystemsicherheit verbessern	9
3. Netzwerksicherheit herstellen	10
4. Sicherheitsplan für Ihre Datenbanken entwickeln	11
5. Datenzugriff mithilfe von Konten und Berechtigungen einschränken	12
6. Datenbanken und andere wichtige Dateien sichern	13
Über FileMaker Pro-Dateiwiederherstellung	14
7. Antivirus-Software installieren, ausführen und aktualisieren	14
8. Sicherheitsmaßnahmen testen	15
9. Sicherheitsmaßnahmen bewerten, iterieren und optimieren	15
10. Zur Sicherheitsoptimierung auf FileMaker Pro 8 und FileMaker Server 8 aktualisieren	16
Sicherheitserweiterungen in FileMaker Pro	16
Sicherheitserweiterungen in FileMaker Server	16

Kapitel 3

Integration von Sicherheit in Ihre Lösungen

Einschränken des Zugriffs mithilfe von Konten und Berechtigungen	19
Tipps zum Beschränken des Dateizugriffs	20
Tipps zum Erstellen von wirksamen Passwörtern	21
Überlegungen beim Bereitstellen von Dateien mit FileMaker Server	21
Sicherheitsüberlegungen beim Web Publishing	22
Tipps und Überlegungen beim Design von Web Publishing-Datenbanken	22
Schutz Ihrer Datenbanken vor Angriffen aus dem Web	25
Web-Server-Sicherheit	26
Verwendung von Verschlüsselung oder VPNs zum Schutz von Daten	26
Secure Sockets Layer (SSL)-Sicherheit für Web Publishing	26
Über drahtlose Netzwerke	27
XML-Überlegungen	27
Überlegungen zu Apple Events und ActiveX	28

Kapitel 1

Datenbanksicherheit

FileMaker® Pro-Software ermöglicht Ihnen, Datenbanken zu erstellen, die einzeln, gemeinsam im Peer-to-Peer-Betrieb, gemeinsam über FileMaker Server, über ODBC oder JDBC oder gemeinsam innerhalb eines Intranets oder mit Internet-Benutzern verwendet werden können. Es ist von besonderer Bedeutung, dass Sie darüber nachdenken, welche Daten gemeinsam genutzt werden, welche Arten von Schwachstellen bestehen und wie Daten und Datenbankdateien zu schützen sind. In manchen Fällen sind Daten nicht besonders sensibel, geschäftsrelevant oder vertraulich oder die Software selbst wird nur von einer Einzelperson an einem sicheren Standort oder einer offenen, zuverlässigen Umgebung verwendet, in der Sicherheitsüberlegungen nicht von Belang sind. In den meisten Fällen jedoch sind Daten geschäftsrelevant oder vertraulich und Sie müssen geeignete Schritte unternehmen, um sie zu schützen. Sie sollten Sicherheitsmaßnahmen für alle Phasen der Entwicklung, des Testens und des Einsatzes planen und umsetzen.

Über dieses Handbuch

- Dieses Dokument behandelt Sicherheitsfragen für FileMaker 7 und 8. Sicherheitsbezogene Informationen zu früheren Versionen von FileMaker Pro erhalten Sie durch den Download von Dokumenten von www.filemaker.de.
- Um in Bezug auf FileMaker-Sicherheitsfragen auf dem aktuellsten Stand zu sein, besuchen Sie die FileMaker Security-Website unter www.filemaker.de/support/security. Dort können Sie sich auch für den FileMaker Security Newsletter anmelden.
- Schrittweise Erläuterungen zu FileMaker Pro-Funktionen zum Schutz von Datenbankdateien einschließlich der Definition von Konten und Zugriffsrechten finden Sie in der FileMaker Pro Hilfe.
- Der in der FileMaker Pro-Dokumentation verwendete Begriff *Web Publishing* bezieht sich auf Datenbanken, auf die Benutzer im Internet oder in einem Intranet mithilfe eines Webbrowsers zugreifen können.
- In diesem Handbuch bezieht sich „FileMaker Pro“ sowohl auf FileMaker Pro als auch auf FileMaker Pro Advanced. Ausgenommen ist die Beschreibung von Funktionen, die spezifisch für FileMaker Pro Advanced sind.

Wichtig Sie können PDF-Dateien der FileMaker 8-Dokumentation von www.filemaker.de/downloads herunterladen. Aktualisierungen dieses Dokuments erhalten Sie ebenfalls auf der Website.

Sicherheitsziele

Beim Schutz Ihrer FileMaker-Datenbanken sind drei allgemeine Themenkreise zu berücksichtigen:

- Datenschutz
- Integrität
- Verfügbarkeit

Datenschutz

Wenn Sie eine Datenbank entwickeln und einsetzen, sind Sie dafür verantwortlich sicherzustellen, dass unbefugte Personen keinen Zugriff auf die Daten haben.

Datenintegrität

Entwickeln Sie ein System, das ausreichend offen ist, um autorisierten Benutzern zu ermöglichen, Daten anzulegen und zu aktualisieren und gleichzeitig unbeabsichtigte Änderungen zu verhindern. Ferner müssen Sie den Zugriff durch unbefugte Personen ausschließen, die die Dateien manipulieren könnten. Leider gibt es Menschen, die versuchen könnten, auf Ihre Informationssysteme zuzugreifen und Unternehmenswerte zu stehlen.

Datenverfügbarkeit

Datenbanken sollten Benutzern nur zur Verfügung stehen, wenn sie benötigt werden. Dies ist ein grundlegender, aber häufig übersehener Gesichtspunkt. Datenbankdesigner und Netzwerkadministratoren müssen nicht nur an Hacker denken, sondern auch an Mitarbeiter, die über mehr als kritischen Zugriff verfügen. Machen Sie es sich zum Ziel Ihrer Entwicklungen, Zugriff sowohl auf Daten als auch auf bestimmte Funktionen nur denjenigen zu gewähren, die ihn wirklich benötigen. Aktivieren Sie keine Sharing-Optionen wie Web Publishing, wenn sie nicht benötigt werden.

Potenzielle Gefahren für Ihre Daten

Sie müssen Ihre Daten und Ihr Datenbankdesign vor unbeabsichtigten und beabsichtigten Änderungen schützen. Jemand könnte versuchen, Aspekte Ihres Designs zu kopieren, von anderen Benutzern eingegebene Daten einsehen, das System beschädigen (eventuell durch Nutzung einer anderen Benutzerkennung), falsche Daten eingeben, Ihre Berichte und Layouts zerstören, Berechnungen verfälschen oder Scripts unbrauchbar machen.

Zu den gängigsten Gefahren für Ihre Daten gehören:

- Unbeabsichtigte Gefahren durch bekannte Personen sowie Unfälle Autorisierte Benutzer können unbeabsichtigt Fehler machen, Daten sehen, die sie nicht sehen sollten, Datensätze löschen oder ändern, auf die sie keinen Zugriff haben sollten, und Dateien löschen oder beschädigen, so dass das System nicht mehr zur Verfügung steht.
- Beabsichtigte Gefahren durch bekannte Personen Berücksichtigen Sie Hacker, die davon profitieren, auf Daten zuzugreifen, die sie nicht sehen sollten, die Daten verfälschen könnten oder absichtlich versuchen, Ihre Daten zu korrumpieren.
- Ungebetene Eindringlinge oder Gefahren von anonymen Personen In der Regel sind dies Internetbasierte Gefahren durch Eindringlinge mit anonymem Zugang, die versuchen, Informationen zu stehlen, Schaden zu verursachen oder das Web-System außer Betrieb zu setzen.

Es ist wichtig zu beachten, dass kleine Unternehmen und größere Arbeitsgruppen den Gefahren gleichermaßen ausgesetzt sind, speziell im Internet. Mitarbeiter in kleinen Unternehmen und Heimbüros könnten davon ausgehen, dass sie sicher sind, weil sie nicht auffallen, aber das ist leider ein Irrtum. Hacker verwenden automatisierte Tools, um verwundbare Systeme zu entdecken und in sie einzudringen. Der Wert der Daten bestimmt in der Regel Zeit und Aufwand, den ein Hacker investieren wird, um ein System zu knacken. Oft besteht das Ziel des Angriffs lediglich darin, ein System zu finden, das verwendet werden kann, um die Spuren des Angriffs auf ein anderes System zu verschleiern.

Kleine Unternehmen bieten im Allgemeinen einen leichteren Zugang als größere Organisationen, weil ihnen oft eine gute Abschirmung (z. B. Firewalls, die von erfahrenen Netzwerkadministratoren unterhalten werden) fehlt und sie nicht über die grundlegenden Sicherheitsstandards für ihre Computersysteme (z. B. wenn nicht alle Computer die sichersten Betriebssysteme verwenden) verfügen.

Eindringlinge von außen versuchen regelmäßig, Zugriff auf Daten von Arbeitsgruppen oder kleinen Unternehmen zu bekommen. Gelegentlich besteht ihr Ziel darin, das System zu deaktivieren, häufiger jedoch versuchen sie, Zugang zu vertraulichen Informationen wie Kreditkartennummern oder Identifikationsdaten wie Kennwörter und Geburtsdaten zu erhalten. Eindringlinge befinden sich in der Regel weit von der Arbeitsgruppe entfernt und haben wahrscheinlich nur geringe Kenntnisse über das System. Sie verwenden automatisierte Scripts, um Systeme aufzuspüren, die bekannte Schwächen aufweisen. Nur ein bescheidenes Maß an Sicherheit reicht schon aus, damit sie sich ein anderes Ziel auszusuchen.

Sicherheitsplanung

Beginnen Sie, indem Sie sich mit den in FileMaker Pro integrierten Sicherheitsfunktionen vertraut machen: Konten und Berechtigungen. Planen Sie einen flexiblen, mehrschichtigen und iterativen Sicherheitsansatz.

- Ihr Sicherheitsplan sollte ausreichend flexibel sein, um die typischen Datenzugriffsanforderungen der einzelnen Benutzer zu berücksichtigen.
- Berücksichtigen Sie die Sicherheit in jeder Ebene des Zugangs, einschließlich Abschließen von Computern, Setzen von Konten und Berechtigungen in den Datenbanken, Einschränken des Zugriffs auf Verzeichnisse und anderer Schritte, um die Daten zu schützen.
- Bewerten Sie die Datensicherheit kontinuierlich, um sicherzustellen, dass Ihre Daten noch geeignet geschützt sind. Dies beinhaltet das Überprüfen, ob Benutzer die neuesten und sichersten Versionen der Software einsetzen, das Ändern von Passwörtern auf regelmäßiger Basis, das Auswerten von Protokolldateien, um Überraschungen zu vermeiden, und das rigorose Einhalten eines Sicherungsschemas. Konfigurieren und testen Sie die Sicherheitsoptionen, während Sie Ihren Dateien Struktur und Daten hinzufügen.

Die folgende Tabelle zeigt, wie ein Entwickler oder Netzwerkadministrator Variablen am Arbeitsplatz und damit verbundene Risiken bewerten könnte.

Arbeitsplatzvariablen	Wirkung auf Risikostufe
Unerfahrenes Personal bei der Dateneingabe, häufiger Mitarbeiterwechsel, neue Computerbenutzer	Hohes Risiko unbeabsichtigter Gefahren, hauptsächlich verursacht durch Dateneingabefehler und schlechte Sicherungstechniken
Unerfahrene Datenbankentwickler	<ul style="list-style-type: none"> • Hohes Risiko unbeabsichtigter Gefahren, verursacht durch Mitarbeiter, die über ungeeigneten Zugriff auf Dateien und Datenbankfunktionen verfügen • Mitarbeiter könnten unbeabsichtigte Gefahren darstellen, indem Sie Dateien weitergeben, ohne die entsprechenden Sicherheitsmaßnahmen zu ergreifen. • Daten werden ungeschützt offen gelegt, wenn FileMaker Pro-Konten und -Berechtigungen nicht geeignet konfiguriert sind, um die Dateien entsprechend zu schützen.
Unerfahrene Netzwerkadministratoren	<ul style="list-style-type: none"> • Hohes Risiko unbeabsichtigter Gefahren, hauptsächlich verursacht durch unzureichende Betriebssystemsicherheit und schlechte Sicherungstechniken • Eine geringe Netzwerksicherheit erhöht das Risiko absichtlicher Gefahren, speziell wenn Dateien über das Internet oder in einem Wireless-Netzwerk freigegeben werden. • Risiken bestehen auch, wenn auf Dateien über Datei-Server zugegriffen wird, anstatt das integrierte Netzwerk-Sharing von FileMaker Pro und FileMaker Server zu verwenden. Mitarbeiter können ungeeignete Kopien der Dateien erstellen und Datensatzsperrern und mögliche Datenbeschädigungen verursachen, wenn Dateien mit ungeeigneten Methoden freigegeben werden.
Unzureichende physische Sicherheit	Hohes Risiko beabsichtigter Gefahren aufgrund eines möglichen Computer-Diebstahls
Datenbanken speichern vertrauliche oder wertvolle Daten.	Erhöhtes Risiko beabsichtigter Gefahren des Datendiebstahls, speziell wenn Daten über das Internet freigegeben werden oder der Zugriff auf die Daten nicht angemessen überwacht und geschützt wird.

Kapitel 2

Die Top 10 in puncto Sicherheit

Vergewissern Sie sich, dass die Datenbankdateien, Host-Computer, Arbeitsplatzrechner und die Netzwerke, die auf sie zugreifen, sicher vor Diebstahl und Beschädigung sind. Dieses Kapitel beschäftigt sich mit zehn Sicherheitsmaßnahmen, die Sie umsetzen können, um Ihre Daten und Ihre Geräte zu schützen. Diese Top 10 sind:

- Physische Sicherheit verbessern
- Betriebssystemsicherheit verbessern
- Netzwerksicherheit herstellen
- Sicherheitsplan für Ihre Datenbanken entwickeln
- Datenzugriff mithilfe von Konten und Berechtigungen einschränken
- Datenbanken und andere wichtige Dateien sichern
- Antivirus-Software installieren, ausführen und aktualisieren
- Sicherheitsmaßnahmen testen
- Sicherheitsmaßnahmen bewerten, iterieren und optimieren
- Zur Sicherheitsoptimierung auf FileMaker Pro 8 und FileMaker Server 8 aktualisieren

Jede dieser Maßnahmen wird in diesem Kapitel detailliert beschrieben.

1. Physische Sicherheit verbessern

Bewerten Sie Ihre Computer, um sicherzustellen, dass sie physisch sicher sind.

- Der Host-Computer sollte ein eigener Rechner sein, der an einem Tisch oder unbeweglichen Gegenstand mit einem Schloss befestigt ist. Sichern Sie den Computer so, dass seine Festplatte nicht entfernt werden kann. Schränken Sie den Zugang zu dem Computer ein, indem Sie ihn in einem abgeschlossenen Raum aufstellen.
- Sichern Sie die Client-Workstations, die auf eine Datenbank zugreifen. Befestigen Sie die Computer mit Schlössern und schränken Sie den Zugang ein, indem Sie einen Bildschirmschoner verwenden, der ein Kennwort erfordert.
- Stellen Sie die physische Sicherheit von Sicherungskopien der auf Wechseldatenträgern wie Bändern und CDs gespeicherten Dateien sicher.

2. Betriebssystemsicherheit verbessern

Setzen Sie die Sicherheitsfunktionen Ihres Betriebssystems ein, um den Zugriff auf wichtige Daten einzuschränken. Der Netzwerkadministrator sollte nur den Personen Zugriff gewähren, die befugt sind, das System bzw. die FileMaker-Datenbanken zu verwalten und zu warten. Zusätzlich zu beachten:

- Benutzerkennungen und Kennwörter des Systems sollten protokolliert werden.
- Der Zugriff auf die Anwendung FileMaker Pro sowie Dateiverzeichnisse, Server und Webseiten sollte eingeschränkt werden.
- Die Einstellungen für Remote-Zugriffe wie File Sharing und FTP sollten überprüft werden.

- Der Zugriff für das Hinauf- und Herunterladen von Dateien sollte eingeschränkt werden.
- Stellen Sie sicher, dass alle Benutzer die neueste und sicherste Version der Betriebssystem-Software verwenden.
- Um Vorgänge zu rationalisieren, können Sie die externe Authentifizierung aktivieren, die Benutzerkonten verwendet, die in der Windows-Domänenauthentifizierung oder im Apple OpenDirectory konfiguriert wurden. Weitere Informationen finden Sie unter „Sicherheitserweiterungen in FileMaker Server“ auf Seite 16.
- Legen Sie FileMaker Pro-Dateien nicht auf Datei-Servern ab, um sie freizugeben. Verwenden Sie die integrierte Netzwerkfunktion von FileMaker Pro und FileMaker Server. So können die Dateien nicht unerlaubt kopiert und Datensatzsperrern oder potenzielle Dateibeschädigungen bei ungeeigneten Freigabemethoden ausgeschlossen werden.

3. Netzwerksicherheit herstellen

In einem Intranet oder dem Internet freigegebene Datenbanken verwenden das TCP/IP-Protokoll. Sie können das TCP/IP-Protokoll auch für die Freigabe von Datenbanken im Peer-to-Peer-Betrieb oder über FileMaker Server verwenden. Auch wenn sich TCP/IP gut für den Datentransport und den Zugriff auf Daten durch Clients eignet, galt bei seiner Entwicklung das Hauptaugenmerk nicht der Sicherheit. Ohne Vorsichtsmaßnahmen kann das Protokoll unbefugten Zugriff auf Ihren Host-Computer, die Server-Software, Datenbanken und eventuell andere Client-Rechner in Ihrem internen Netzwerk ermöglichen. TCP/IP bietet keinen umfassenden Datenschutz. Daher ist es wichtig, ungebetenen Besuchern den Weg durch Einrichtungen wie Firewalls und SSL-Datenverschlüsselung zu versperren. Informationen zu Produkten von Drittanbietern wie Verschlüsselungsprogrammen finden Sie unter „Verwendung von Verschlüsselung oder VPNs zum Schutz von Daten“ auf Seite 26.

- In den meisten Fällen wird eine Firewall verwendet, die ein Netzwerk in zwei unterschiedliche Bereiche aufteilt, einen öffentlichen Bereich („außerhalb der Firewall“) und einen privaten Bereich („innerhalb der Firewall“ bzw. „hinter der Firewall“). Benutzer, die sich außerhalb der Firewall befinden, haben nur auf die TCP/IP- oder Hardware-Adressen Zugriff, die Sie freigeben. Dies ermöglicht es Ihnen, sich auf die Sicherheit der nach außen freigegebenen Server zu konzentrieren, während die Computer hinter der Firewall weniger Sicherheitsvorkehrungen benötigen.
- Der Einsatz von Wireless-Netzwerkeinrichtungen wie Apple AirPort und anderen 802.11b-Netzwerkkarten und -Basisstationen kann zu Sicherheitsproblemen führen. Da diese Geräte die Netzwerkdaten auch über die Grenzen Ihres Firmengebäudes hinaus übertragen können, sollten die drahtlos übertragenen Netzwerksignale unbedingt verschlüsselt werden. Verwenden Sie stets die maximal verfügbare Stufe der Signalverschlüsselung. Weitere Informationen finden Sie unter „Über drahtlose Netzwerke“ auf Seite 27.

* Sie können für manche Funktionen einen eingeschränkten Zugriff festlegen (z. B. für das Löschen von Datensätzen), indem Sie datensatzweise Berechtigungen verwenden. Weitere Informationen zu datensatzweisen Berechtigungen finden Sie in der FileMaker Pro Hilfe.

5. Datenzugriff mithilfe von Konten und Berechtigungen einschränken

Verwenden Sie Konten und Berechtigungen als grundlegende Sicherheitsmethode innerhalb von FileMaker Pro-Dateien. Mit Konten und Berechtigungen können Sie die Anzeige und Aktionen von Benutzern in einer Datenbankdatei einschränken. Sie können Folgendes einschränken:

- Dateizugriff: Benutzer müssen einen Kontonamen und ein Passwort eingeben, um eine Datei zu öffnen.
- Datenzugriff: Setzen Sie bestimmte Datensätze oder Felder aus einzelnen Tabellen auf „Nur Lesen“ oder blenden Sie sie komplett aus.
- Layoutzugriff: Benutzer werden daran gehindert, Layouts im Layoutmodus anzuzeigen bzw. zu ändern.
- Zugriff auf Wertelisten und Scripts: Benutzer werden daran gehindert, auf Wertelisten und Scripts zuzugreifen und sie zu ändern sowie Scripts auszuführen.
- Datenausgabe: Benutzer werden daran gehindert, Daten auszudrucken oder zu exportieren.
- Menüzugriff: Stellen Sie nur eine eingeschränkte Auswahl von Menübefehlen zur Verfügung.

Wenn Dateien mit Konten eingeschränkt sind, müssen Benutzer den Kontonamen und das Passwort kennen, bevor sie eine Datenbank öffnen oder eine Verbindung zu ihr aufbauen können. Der eingegebene Kontoname und das Passwort bestimmen, welche Berechtigungen ihre Aktionsmöglichkeiten in einer Datei beschränken. Weitere Informationen über Konten und Berechtigungen finden Sie in „Einschränken des Zugriffs mithilfe von Konten und Berechtigungen“ auf Seite 19.

Tipps

- Ihre Sicherheit ist nur so gut wie die Benutzerkonten und Passwörter, die Sie definieren. Weitere Informationen finden Sie unter „Tipps zum Erstellen von wirksamen Passwörtern“ auf Seite 21.
- Geben Sie niemandem Ihren Kontonamen und Ihr Passwort auf der Administratorebene bekannt. Dies schützt Ihre Dateien für den Fall, dass Ihre physische Sicherheit oder Ihre Betriebssystem- oder Netzwerksicherheit umgangen wurde.
- FileMaker Server kann so konfiguriert werden, dass Datenbanken eine externe Serverauthentifizierung auf der Basis von Gruppennamen ausführen anstelle von Konten/Passwörtern, die in der Datenbank gespeichert sind. Weisen Sie für ein höheres Maß an Sicherheit externen Server-Kontentypen keine vollen Zugriffsrechte zu. Weitere Informationen finden Sie unter „Sicherheitserweiterungen in FileMaker Server“ auf Seite 16.

Wichtig Eine neue FileMaker Pro-Datei ist ursprünglich nicht geschützt. Beim Öffnen von Dateien werden Benutzer automatisch mit dem Admin-Konto angemeldet, dem die Berechtigungen für vollen Zugriff zugewiesen sind. Damit keine weiteren Personen eine Datenbank mit vollem Zugriff öffnen können, benennen Sie das Admin-Konto um und weisen ihm ein Passwort zu. Bevor Sie die Datei gemeinsam mit Kollegen benutzen, planen Sie die Sicherheit der Datei und weisen Sie jedem Benutzer die erforderliche Zugriffsebene zu.

6. Datenbanken und andere wichtige Dateien sichern

Entwickeln Sie Pläne zur Wiederherstellung von Daten einschließlich alternativer Sites und Systeme, um geschäftsrelevante Informationsdienste zu betreiben. Eine aktuelle Sicherungskopie kann Situationen retten, in denen ein Benutzer die Administratorkontoinformation für eine Datei verliert oder Daten durch einen Benutzerfehler (oder manchmal auch mangelhaftes Datenbankdesign) gelöscht oder fehlerhaft geändert wurden.

Beachten Sie folgende Punkte:

- Stellen Sie Datenbanken mit FileMaker Server bereit und sorgen Sie für automatisierte Sicherungen nach einem regelmäßigen Zeitplan.

Verwenden Sie keine Sicherungssoftware anderer Anbieter für FileMaker Pro-Datenbanken. Erstellen Sie zunächst mit FileMaker Server eine Sicherungskopie Ihrer Datenbank und führen Sie dann die Software eines anderen Anbieters für diese Kopie aus. Sicherungssoftware kann geöffnete, bereitgestellte Datenbanken beschädigen.

Erstellen Sie beispielsweise lokale Sicherungskopien von Dateien wochentags um 6:00, 9:00, 12:00, 15:00, 18:00 und 23:30 Uhr. Führen Sie um Mitternacht eine inkrementelle Sicherung des gesamten Systems auf das Unternehmenssicherungssystem durch. Führen Sie schließlich Freitag um Mitternacht eine vollständige Systemsicherung durch. Kopieren Sie die Sicherungsbänder und bewahren Sie sie an einem anderen Ort auf. Wenn dann der Server aus einem beliebigen Grund ausfällt (außer bei einem katastrophalen Ausfall mehrerer Laufwerke), kann die neueste Sicherungskopie der Datendateien verwendet werden, d. h., es sind maximal Daten von drei Stunden verloren gegangen. Bei einem katastrophalen Laufwerksausfall kann das Band des vorherigen Abends verwendet und der Verlust damit auf einen Tag minimiert werden. Natürlich können diese Verfahren auf Ihre spezielle Situation und Datenanforderungen zugeschnitten werden.

- Stellen Sie sicher, dass Sicherungskopien nicht beschädigt oder unzugänglich sind. Prüfen Sie ihre ordnungsgemäße Funktionsweise, *bevor* Sie sie brauchen. Kontrollieren Sie Ihr Festplattenlaufwerk und Ihre Sicherungsdateien regelmäßig mithilfe von Diagnosewerkzeugen.
- Stellen Sie sicher, dass Sie ein vollständiges Dateiset aus Ihren Sicherungskopien wiederherstellen können.
- Exportieren Sie die Daten regelmäßig als Sicherheit bei Dateibeschädigung.
- Schützen Sie auch die Sicherungsmedien. Bewahren Sie Sicherungskopien an einem separaten und feuersicheren Ort auf.
- Berufen Sie Sicherungsadministratoren, die Dateien abrufen können, falls der Netzwerkadministrator nicht greifbar ist.
- Sehen Sie eine redundante Stromversorgung vor. Bei einer Unterbrechung der Stromzufuhr sollte eine unterbrechungsfreie Stromversorgung (USV) mindestens 15 Minuten lang aktiv sein, damit Sie alle Dateien sicher schließen können. Wenn die Stromzufuhr nicht rechtzeitig wiederhergestellt werden kann, sollten Sie den Einsatz eines Generators für die Stromversorgung der Server in Erwägung ziehen. Berücksichtigen Sie auch Stromquellen für Router und Firewalls. Ist die Kommunikation problematisch, wenn Ihr Internet-Zugang 48 Stunden oder länger unterbrochen ist?
- Überlegen Sie, wie Sie Ihre Dienstleistungen weiterhin zur Verfügung stellen können, wenn ein Eindringling Ihren Datenbankserver beschädigt und dieser Server nicht in seinen vorherigen Zustand gebracht werden kann.

- Beurteilen Sie weitere mögliche Situationen und entwickeln Sie einen Plan, um auf jeden einzelnen Fall zu reagieren.

Zusätzlich sollten Netzwerkadministratoren das Risiko für Datensysteme und geschäftsrelevante Funktionen bewerten. Bedenken Sie zum Beispiel:

- Diebstahl von Daten oder geistigem Eigentum.
- Störung, Diebstahl oder Beschädigung der Netzwerkinfrastruktur wie Server, Netzwerke, Datenspeicher oder Sicherungsspeicher. Schaden kann durch geknackte Passwörter oder andere Arten der Sabotage und Zerstörung entstehen. Die meisten Vorfälle haben ihren Ursprung innerhalb des Unternehmens.
- Störung oder Beschädigung der Unternehmensinfrastruktur durch Feuer, Umweltgefahren oder biologische Bedrohungen, Überschwemmungen usw.
- Störung oder Beschädigung der öffentlichen Infrastruktur einschließlich Stromversorgung, Telekommunikation (Sprache und Daten), Transportnetz (Straßen, Busse, Züge) durch Umwelt- oder Wetterbedingungen wie Tornados oder Überschwemmungen.

Wichtig Verwenden Sie bei einem Serverausfall, z. B. einem unerwarteten Stromausfall, Festplattenfehler oder Softwarefehler, die Sicherungsdateien. Jeder Systemfehler, der die korrekte Beendigung von FileMaker Server verhindert, kann zu beschädigten Dateien führen, wenn Cache-Daten nicht auf Platte geschrieben und die Dateien nicht korrekt geschlossen wurden. Selbst wenn die Dateien wieder geöffnet werden, sollten Sie eine Konsistenzprüfung oder Wiederherstellung durchführen, da die Datei eine nicht offensichtliche Beschädigung enthalten könnte. Eine Dateiwiederherstellung kann nicht garantieren, dass Probleme behoben wurden.

Über FileMaker Pro-Dateiwiederherstellung

Verwenden Sie die Wiederherstellungsfunktion, wenn eine Datenbankdatei nicht korrekt geschlossen wurde und die Daten seit der letzten Sicherung wiederhergestellt werden müssen. Die Wiederherstellung legt eine neue Datei mit einem anderen Namen als dem der Originaldatei an, da sie die Datei nicht ersetzen soll. Bei diesem aggressiven Verfahren können Layouts, Scripts usw. entfernt werden, um ein Maximum der verloren gegangenen Daten herzustellen. Die Daten sollten aus der wiederhergestellten Datei exportiert und in eine saubere Sicherungskopie der originalen Datenbankdatei importiert werden.

Da eine Wiederherstellung längere Zeit beanspruchen kann, erstellen Sie lokale Sicherungen in einem Intervall, das berücksichtigt, wie viele Daten verloren gehen können.

7. Antivirus-Software installieren, ausführen und aktualisieren

Da die meisten Computer über einen Internet-Zugang verfügen, sind sie durch Viren gefährdet, die durch E-Mail-Anhänge übertragen werden. Stellen Sie sicher, dass alle Mitarbeiter regelmäßig Software zur Virenprüfung ausführen und die typischen Warnsignale für Viren kennen. Mitarbeiter sollten alle Dateien überprüfen, bevor sie sie auf ihren Computer kopieren oder herunterladen. Außerdem sollten sie niemals unverlangte Anhänge öffnen, selbst wenn diese von einer ihnen bekannten Person stammen.

Hinweis Führen Sie Virenschutzprogramme nicht an geöffneten, bereitgestellten Datenbanken aus. Schließen Sie die Datenbanken, bevor Sie das Virenschutzprogramm ausführen.

8. Sicherheitsmaßnahmen testen

Es ist wichtig, alle Szenarien zu testen, um zu gewährleisten, dass Benutzerkonten wie erwartet mit allen Sharing-Technologien funktionieren.

Beispiel:

- Öffnen Sie die Datei in verschiedenen Benutzerkonten und testen Sie die definierten Berechtigungen. Stellen Sie sicher, dass die Beschränkungen wie geplant funktionieren, und nehmen Sie etwaige erforderliche Korrekturen an den Berechtigungen vor.
- Testen Sie Navigation und Scripts mit allen Benutzerkonten. Da Konten über verschiedene Berechtigungen verfügen können, bedenken Sie, dass der Zugriff auf einige Funktionen, wie Layouts, Tabellen und Scripts, eventuell nicht für alle Benutzer möglich ist.
- Wenn Benutzer auf Ihre Datenbanken auf ganz verschiedene Weise zugreifen, z. B. im Web mit Instant Web Publishing, XML oder JDBC, testen Sie auch Konten mit diesen Technologien.
- Wenn Sie Dateien im Web veröffentlichen, öffnen Sie Scripts und aktivieren Sie Web-Kompatibilität anzeigen, um sicherzustellen, dass alle Schritte unterstützt werden. Wenn Ihre Scripts nicht Web-kompatible Schritte enthalten, legt der Scriptschritt „AnwenderAbbruchZulassen setzen“ fest, wie nachfolgende Schritte gehandhabt werden. Weitere Informationen finden Sie im Handbuch *FileMaker Instant Web Publishing*, das sich im Ordner „Elektronische Dokumentation“ (im Ordner „Deutsch Extras“) befindet.
- Testen Sie, ob unerwartete Ergebnisse geliefert werden. Öffnen Sie z. B. Dateien mit verschiedenen Benutzerkonten und versuchen Sie, Aktionen auszuführen, zu denen Benutzer nicht berechtigt sind. Entziehen Sie den Zugriff auf Berechtigungen, wann immer möglich.
- Bitten Sie andere Entwickler, in unangemessener Weise auf Ihre Daten zuzugreifen.
- Führen Sie regelmäßig Tests durch, nicht nur während der Entwicklung, sondern auch während des Einsatzes.

9. Sicherheitsmaßnahmen bewerten, iterieren und optimieren

Es ist wichtig, einen iterativen Sicherheitsansatz zu verwenden. Wenn zum Beispiel neue Benutzer auf die Datenbank zugreifen, sollten Sie die geeignete Zugriffsebene auf die Daten und die Datenbankstruktur abhängig von den Aufgaben oder Rollen der neuen Benutzer in einem Unternehmen erneut beurteilen.

Stellen Sie sich selbst die folgenden Fragen, bevor Sie eine FileMaker Pro-Datenbank entwickeln, und dann immer wieder, wenn sich die Dateien ändern:

- Was ist wichtig?
- Warum ist es wichtig?
- Wie wichtig ist es?
- Wie schädlich wäre Verlust oder Bekanntgabe?
- Was ist die minimale Sicherheitsebene, um Verlust oder Bekanntgabe zu vermeiden?
- Mit welchen Werkzeugen lässt sich diese Sicherheit erzielen?

Um die Sicherheit zu beurteilen, aktivieren Sie Protokolldateien in FileMaker Pro und FileMaker Server und überprüfen Sie die Aktionen der Benutzer. Sie können auch Aktionen verfolgen, indem Sie Scripts und Berechnungen verwenden, die den Kontonamen, das Passwort und die IP-Adresse des Benutzers erfassen.

10. Zur Sicherheitsoptimierung auf FileMaker Pro 8 und FileMaker Server 8 aktualisieren

Sicherheit wurde in FileMaker Pro 7 und FileMaker Server 7 neu gestaltet. Wenn Sie von einer Version vor 7.0 upgraden, verwenden Sie das neue Sicherheitsmodell, das eine zuverlässigere und rationellere Vorgehensweise bei der Zuweisung von Konten und Berechtigungen bietet.

Sicherheitserweiterungen in FileMaker Pro

- Das Sicherheitsmodell ist intuitiver und ähnlich bedienbar wie andere Werkzeuge. Sie können Benutzerkonten und Passwörter anlegen und Berechtigungen für mehrere Benutzer und Tabellen gemeinsam nutzen.
- Da FileMaker Pro mehrere Tabellen in einer Datei unterstützt, können Sie eine Datenbank, die aus einer einzelnen Datei und mehreren Tabellen besteht, mit einem Set von Konten und Berechtigungen schützen.
- Mithilfe der Funktion „Hole(Kontoname)“ können Sie den aktuellen Benutzer in Funktionen und Scripts bestimmen. Dies eröffnet zahlreiche Möglichkeiten, zum Beispiel das Erstellen von Scripts, die nur von bestimmten Kontonamen ausgeführt werden können.
- Sie können verlangen, dass Benutzer beim nächsten Öffnen der Datenbank ein neues Passwort angeben, und Einstellungen aktivieren, nach denen Benutzer ihre Passwörter nach der angegebenen Anzahl an Tagen ändern müssen.
- Sie können eine Mindestlänge für Passwörter festlegen.
- In FileMaker-Netzwerken verwenden Kontonamen und Passwörter einen nicht umkehrbaren Verschlüsselungsalgorithmus, der eine Dechiffrierung durch Werkzeuge zum Knacken von Passwörtern verhindert. Benutzerkontonamen und -passwörter werden auf dem Hostcomputer verifiziert. Damit werden Eindringversuche auf dem Client-Computer oder Versuche zum Knacken von Passwörtern mit den ausführbaren oder temporären Dateien verhindert. Sie müssen Ihren Kontonamen und Ihr Passwort an einem sicheren Ort aufbewahren. Wenn Sie den Kontonamen und das Passwort verlieren, müssen Sie die Dateien neu erstellen.

Sicherheitserweiterungen in FileMaker Server

Wenn Sie Datenbanken mit FileMaker Server bereitstellen, können Sie eine Reihe von Funktionen nutzen, um Ihre Daten sowohl für FileMaker Pro als auch für Web-basierte Clients besser zu schützen. Informationen zu bestimmten Funktionen finden Sie im *FileMaker Server Advanced Web Publishing Installationshandbuch* oder im *FileMaker Server Administratorhandbuch*.

- Um die Benutzerkontoinformationen und die Daten mit FileMaker-Netzwerken zu verschlüsseln, aktivieren Sie Sichere Verbindungen zu FileMaker Server.

- Wenn Sie Dateien für Web-basierte Clients bereitstellen, aktivieren Sie SSL-Verschlüsselung in einer Webserver-Anwendung, um Daten zu verschlüsseln, die vom Host an Gast-Computer im Web übertragen werden. Weitere Informationen finden Sie unter „Secure Sockets Layer (SSL)-Sicherheit für Web Publishing“ auf Seite 26.
 - Sie können für die Web Publishing Engine bestimmte erweiterte Zugriffsrechte aktivieren und deaktivieren, z. B. Instant Web Publishing, XML und XSLT. Wenn Sie z. B. wissen, dass alle Dateien auf einem Server gemeinsam mit Instant Web Publishing genutzt werden, können Sie alle anderen Arten von Web-Publishing deaktivieren. Selbst wenn eine Datei erweiterte Zugriffsrechte umfasst, die den Zugriff auf XML-Daten erlauben, ist der Zugriff auf XML-Daten nicht verfügbar, während die Datei mit dieser Web Publishing Engine bereitgestellt wird. Weitere Informationen finden Sie im Handbuch *FileMaker Server Advanced Web Publishing Installation*.
 - Wenn Ihr Unternehmen zentral verwaltete Authentifizierung für Benutzer und Gruppen verwendet, z. B. Apple OpenDirectory oder eine Windows-Domäne, können Sie Konten einrichten, die Benutzer auf der Basis Ihres Authentifizierungsservers authentifizieren. Damit können Sie den Zugriff auf Datenbanken mit Ihrem bestehenden Authentifizierungsserver steuern, ohne eine unabhängige Liste mit Konten in jeder FileMaker Pro-Datenbankdatei zu führen. Weitere Informationen zum Authentifizieren von Konten mit externen Servern finden Sie in der FileMaker Server Hilfe.
- Wichtig** Wenn eine Datenbankdatei ein oder mehrere Externe-Server-Konten enthält, verwenden Sie unbedingt Sicherheitseinstellungen des Betriebssystems, um direkten Zugriff auf die Datei zu beschränken. Andernfalls kann eventuell ein unbefugter Benutzer die Datei auf ein anderes System verschieben, das Ihre Authentifizierungsserver-Umgebung repliziert, und Zugriff auf die Datei erlangen. Gruppennamen für Konten, die mit der Funktion für externe Server authentifiziert werden, werden als Zeichenfolgen gespeichert. Wenn der Gruppename auf einem anderen System reproduziert wird, kann auf die kopierte Datei mit den Berechtigungen zugegriffen werden, die den Mitgliedern dieser Gruppe zugewiesen wurden. Dies kann zu unzulässiger Bekanntgabe von Daten führen.
- Aktivieren Sie Protokolldateien und Dateisicherungsfunktionen für eine wirksame und bequeme Datenbankpflege.

Kapitel 3

Integration von Sicherheit in Ihre Lösungen

Entwickler und Netzwerkadministratoren müssen die Verantwortung übernehmen für die Verwaltung von Sicherheit in Design und Einsatz ihrer Datenbankdateien sowie für die routinemäßige Verwaltung von Sicherheit.

Einschränken des Zugriffs mithilfe von Konten und Berechtigungen

Sie schützen Ihre Dateien in erster Linie durch das Definieren von Konten und Zugriffsrechten in FileMaker Pro. Es ist ratsam, den Zugriff auf jede Datei mit einem Admin-Passwort zu beschränken, das nur Sie kennen. Damit schützen Sie Dateien, wenn andere Sicherheitsmaßnahmen umgangen wurden.

Wichtig Informationen über die Konvertierung von Sicherheitseinstellungen aus Datenbanken einer älteren Version als 7.0 in die neuere FileMaker Pro-Version finden Sie unter *Konvertieren von FileMaker-Datenbanken aus früheren Versionen*. Umfassende Informationen und schrittweise Anleitungen zur Verwendung von Kontonamen, Passwörtern und Berechtigungen finden Sie in der FileMaker Hilfe.

Konten authentifizieren Benutzer, die versuchen, eine geschützte Datei zu öffnen.

- Jedes Konto gibt einen Kontonamen und (optimalerweise) ein Passwort an.
- Jede Datenbankdatei enthält zwei vordefinierte Konten: Admin und Gast. Dem Admin-Konto, das zur größeren Sicherheit umbenannt werden sollte, werden die Berechtigungen für vollen Zugriff zugewiesen. Das Gast-Konto, das sich nicht umbenennen lässt, gestattet Benutzern, eine Datei ohne Angabe eines Kontonamens und Passworts zu öffnen. Standardmäßig wird dem Gast-Konto der Nur-Lese-Zugriff zugewiesen, aber Sie können in „Konten und Zugriffsrechte“ andere Berechtigungen festlegen.
- Legen Sie zur maximalen Sicherheit für jeden Benutzer ein eindeutiges Konto an.

Berechtigungen geben eine Zugriffsebene für eine Datenbankdatei an. Jede Datenbankdatei enthält drei vordefinierte Berechtigungen: Voller Zugriff, Nur Dateneingabe, Nur Lesezugriff.

- Jedem Konto wird eine Berechtigung zugewiesen, die die Zugriffsebene für Personen festlegt, die eine Datei mit diesem Konto öffnen.
- Für die Beschränkung des Datenbankzugriffs können Sie Berechtigungen festlegen, z. B. welche Layouts und Menüs verfügbar sind und ob das Drucken erlaubt ist. Berechtigungen können auch den Zugriff auf Datensätze oder Felder bestimmter Tabellen in einer Datei beschränken.

Erweiterte Zugriffsrechte bestimmen die Optionen der gemeinsamen Datennutzung, die durch eine Berechtigung gestattet werden. Sie können Zugriffsrechte für den gemeinsamen Zugriff auf Dateien mit einem FileMaker-Netzwerk, über Instant Web Publishing, Custom Web Publishing mit XML oder XSLT, von ODBC- oder JDBC-Clients und FileMaker Mobile aktivieren. Alle erweiterten Zugriffsrechte sind standardmäßig deaktiviert.

Wichtig Definieren Sie für maximale Sicherheit Konten, die Benutzernamen und Passwörter für alle Dateien verlangen. Nutzen Sie die Sicherheitsfunktionen und fordern Sie Benutzer auf, nach einer bestimmten Zeit ihre Passwörter zu ändern und eine Mindestlänge für Passwörter zu verwenden.

Tipps zum Beschränken des Dateizugriffs

- Vermeiden Sie automatische Anmeldung, indem Sie einen Kontonamen und ein Passwort im Dialogfeld „Dateioptionen“ angeben.
- Die Verwendung desselben Passworts in jeder Datei ist oft zweckmäßig, wenn Benutzer mit mehreren Lösungsdateien in einer Sitzung arbeiten müssen. Dies ist nicht mehr möglich, wenn Benutzer ihr eigenes Passwort ändern (es sei denn, sie ändern es entsprechend in allen Dateien). Wenn Sie Konten anlegen, müssen Sie sie in allen Lösungsdateien erstellen. Sie können bequem mehrere Tabellen in einer Datei definieren. Erwägen Sie die Bereitstellung von Dateien mit FileMaker Server und den Einsatz eines externen Authentifizierungsservers wie Windows Domain oder Apple OpenDirectory. Weitere Informationen finden Sie unter „Sicherheitserweiterungen in FileMaker Server“.
- Wenn Konten von mehreren Personen benutzt werden, ändern Sie das Passwort regelmäßig. Ändern Sie auch den Kontonamen und das Passwort, wenn Personen die Gruppe verlassen.
- Erstellen Sie eine Startdatei, die nur über Scripts mit kritischen Dateien interagiert. Die Startdatei speichert keine Daten, sondern verschiebt sie mithilfe von Scripts in kritischere Dateien. Lassen Sie Benutzer die Dateien mit dem Standard-Kontonamen und Passwort öffnen, die den Zugriff auf vertrauliche Daten und riskante Funktionen, z. B. das Löschen von Daten, beschränken. Die Scripts können Aktionen ausführen, auf die Sie Benutzern keinen Zugriff gewähren möchten (etwa das Löschen von Datensätzen), indem Sie Script mit vollen Zugriffsrechten ausführen aktivieren.
- Sie können Datensatz-Zugriffsrechte für die Anzeige, die Bearbeitung und das Löschen der Datensätze innerhalb jeder Tabelle festlegen. Beschränken Sie den Zugriff von Benutzern auf bestimmte Datensätze nach einer Vielzahl von Optionen, z. B. ihrer Abteilung, ihrer Position, ihren Aufgaben usw. Weitere Informationen zu Datensatz-Zugriffsrechten finden Sie in der FileMaker Pro Hilfe.

Wichtig Die Beschränkung des Zugriffs auf bestimmte Datensätze führt ein komplizierteres Datenzugriffsmodell ein. Testen Sie Ihre Lösung gründlich, indem Sie sich mit verschiedenen Benutzerkonten anmelden und alle Layouts, Berichte und Scripts überprüfen. Dokumentieren Sie unbedingt die jeweiligen Bedingungen, damit Benutzer wissen, wie sie vorgehen können.

- Verwenden Sie keine Layouts für die Sicherheit. Die einzige Methode zum Schutz von Dateien, z. B. von CGI-Anfragen oder anderen Quellen, ist die Einschränkung des Kontozugriffs auf Feld- oder Tabellenbasis. Weitere Informationen erhalten Sie im FileMaker Pro-Hilfethema über das Zusammenspiel zwischen Layout-Zugriffsrechten und Datensatz-Zugriffsrechten.

- Wenn Sie Datenbanken aus FileMaker Pro-Versionen vor Version 7.0 konvertieren, überprüfen Sie alle Dateiverweise in Ihrer Lösung und löschen Sie die, die Sie nicht benötigen. Im Dialogfeld „Dateiverweise“ werden Informationen wie Speicherort und IP-Adressen angezeigt, die Informationen offen legen könnten, die Sie nicht verbreiten möchten. Prüfen Sie die Konvertierungsprotokolldatei auf den Status und Probleme, die möglicherweise bei der Konvertierung aufgetreten sind. Weitere Informationen finden Sie unter *Konvertieren von FileMaker-Datenbanken aus früheren Versionen*.
- Mit FileMaker Pro Advanced können Sie die Berechtigungen für vollen Zugriff sowie alle Konten mit den Berechtigungen für vollen Zugriff permanent entfernen (einschließlich des Admin-Kontos). Diese Aktion kann nicht widerrufen werden. Sie sollten sie nur ausführen, wenn Sie absolut sicher sind, dass nie wieder jemand vollen Zugriff auf die Datei benötigt. Weitere Informationen finden Sie im *FileMaker Pro Advanced Entwicklerhandbuch*.

Tipps zum Erstellen von wirksamen Passwörtern

- Sichere Passwörter sind länger als acht Zeichen und enthalten gemischte Groß- und Kleinbuchstaben sowie mindestens eine Zahl. Kombinieren Sie etwa zwei Wörter ohne jeglichen Bezug zueinander und ersetzen Sie Buchstaben durch Zahlen, z. B. b00tze!t (Null anstelle von „o“ und ein Ausrufezeichen anstelle von „i“).
- Wenn die Dateien im Web veröffentlicht werden, sollten Kontonamen und Passwörter nur druckbare ASCII-Zeichen verwenden, z. B. a-z, A-Z und 0-9. Benutzen Sie für sicherere Kontonamen und Passwörter auch Interpunktion wie „!“ und „%“, aber keine Doppelpunkte. Wenn Sie Datenbanken mit FileMaker Server Advanced bereitstellen, aktivieren Sie SSL-Verschlüsselung.
- Weniger sicher sind Passwörter mit leicht zu erratenden Zeichenfolgen wie Namen (besonders die von Familienangehörigen und Haustieren), Geburts- und Hochzeitstagen sowie die Wörter *Passwort, Standard, Master, Admin, Gast, Client* und ähnliche Standardbegriffe.
- Ändern Sie Passwörter häufig, etwa alle 30 oder 90 Tage.
- Verwenden Sie Passwörter nur einmal.
- Wenn möglich, weisen Sie jedem Benutzer ein eindeutiges Passwort zu. Wenn Sie Benutzerkonten gemeinsam benutzen müssen, ändern Sie das Passwort unbedingt regelmäßig.
- Sammeln Sie Passwörter nicht zentral in einer Datei oder Liste, es sei denn, diese Datei oder Liste ist gut gesichert.
- Teilen Sie keine Benutzerkonten mit anderen Benutzern. Benutzer sollten nur Kontonamen und Passwörter von Dateiadministratoren erhalten.

Überlegungen beim Bereitstellen von Dateien mit FileMaker Server

Beachten Sie bei der Bereitstellung von Datenbanken mit FileMaker Server folgende Punkte:

- Wenn Sie Remote-Zugriff aktivieren, verlangen Sie unbedingt ein Passwort. Weitere Informationen finden Sie in der FileMaker Server Hilfe.
- Speichern Sie FileMaker Pro-Dateien auf einem lokalen Server (nicht in Netzwerkverzeichnissen). Einer der wichtigsten Leistungsfaktoren ist das schnelle Lesen und Schreiben von Daten auf Platte.

- Deaktivieren Sie File Sharing oder stellen Sie sicher, dass Benutzer nicht direkt auf Dateien zugreifen können, die von FileMaker Server bereitgestellt werden. Wenn sich eine FileMaker Pro-Datei von einem Dateiserver kopieren lässt, ist sie durch „Offline“-Angriffe gefährdet. Beispielsweise werden Gruppennamen für Konten, die mit der Funktion für externe Server authentifiziert werden, als Zeichenfolgen gespeichert. Wenn der Gruppenname auf einem anderen System reproduziert wird, kann auf die kopierte Datei mit den Berechtigungen zugegriffen werden, die den Mitgliedern dieser Gruppe zugewiesen wurden. Dies kann zu unzulässiger Bekanntgabe von Daten führen. Weitere Informationen finden Sie unter „Sicherheitserweiterungen in FileMaker Server“ auf Seite 16.
- Das Unterdrücken eines Dateinamens im Dialogfeld „Remote öffnen“ oder der Instant Web Publishing-Datenbank-Homepage ist kein Ersatz für die Verwendung von Konten und Zugriffsrechten zum Schutz einer Datei.
- Befehle der FileMaker Server-Befehlszeilenschnittstelle (CLI) können Kontonamen und Passwörter enthalten. Stellen Sie sicher, dass nicht autorisierte Benutzer Passwörter nicht anzeigen können, die als Teil von CLI-Befehlen angezeigt werden. Setzen Sie zur Einschränkung der Zugriffsrechte auf Scriptdateien und Stapeldateien, die CLI-Befehle mit Passwörtern enthalten, die Funktionen Ihres Betriebssystems für Dateieigentümer und Berechtigungen ein.

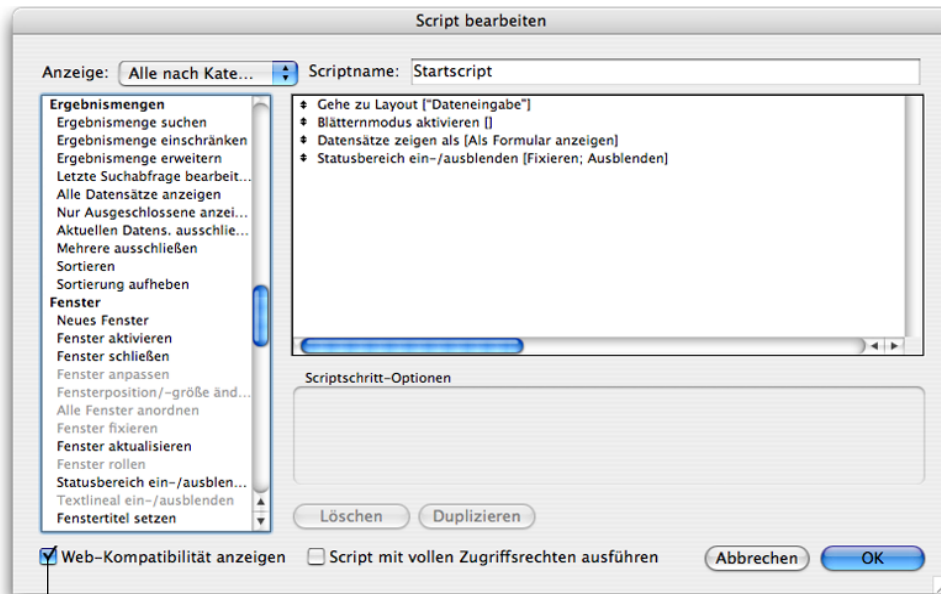
Sicherheitsüberlegungen beim Web Publishing

Mit der FileMaker Pro-Software können Sie Datenbanken in Ihrem Intranet oder im Internet veröffentlichen, so dass Benutzer die Datenbanken mithilfe eines Web-Browsers durchblättern, durchsuchen und aktualisieren können. Dies stellt ein größeres Risiko dar als die gemeinsame Dateibenutzung mit anderen FileMaker Pro-Clients.

Tipps und Überlegungen beim Design von Web Publishing-Datenbanken

1. Definieren Sie Konten und Berechtigungen.
 - Schützen Sie alle Dateien mit Benutzernamen und Passwörtern. Sie können das Gastkonto verwenden, das sich mit einem Standard-Benutzernamen und -Passwort anmeldet, falls es nicht zweckmäßig ist, eindeutige Konten für Clients zu benutzen. Dadurch steht Ihre Datei jedoch jedem zur Verfügung, der die IP-Adresse oder den Domänennamen des Computers kennt, der die Datenbank bereitstellt.
 - Weisen Sie Zugriffsrechte zum Ändern von Daten und Datenbankstruktur nur zu, wenn es nötig ist.
 - Aktivieren Sie nur die erforderlichen erweiterten Zugriffsrechte für Web Publishing. Wenn Sie z. B. nur Custom Web Publishing mit XSLT verwenden, aktivieren Sie die entsprechenden erweiterten Zugriffsrechte in den jeweiligen Berechtigungen und lassen die übrigen erweiterten Zugriffsrechte für Web Publishing deaktiviert.
2. Wenn Sie Lösungen aus Versionen vor Version 7.0 konvertieren, beachten Sie, dass die Web-Sicherheitsdatenbanken nicht mehr unterstützt werden. Sie müssen die Konten, Passwörter und zugehörigen Berechtigungen auf Ihre konvertierten Datenbankdateien in FileMaker Pro übertragen. Informationen hierzu finden Sie unter *Konvertieren von FileMaker-Datenbanken aus früheren Versionen*.

3. Zur höheren Sicherheit können FileMaker Pro-Clients keine Datenbanken mit Remote-Zugriff mehr im Web veröffentlichen. Sie können Dateien nur vom Host-Computer aus im Web veröffentlichen.
4. In Instant Web Publishing sind Sie nicht mehr auf vordefinierte Layouts zur Datenanzeige eingeschränkt. Alle Layouts stehen Web-Benutzern abhängig von ihren Konten zur Verfügung. Sie können Layouts für alle Konten mit Berechtigungen einschränken, aber Sie sollten sich hinsichtlich der Sicherheit nicht auf Layouts verlassen. Verwalten Sie den Zugriff auf Daten mit Tabellen, Datensätzen, Feldern, Scripts und Wertelisten, um die größte Sicherheit zu erzielen.
5. Wenn Instant Web Publishing-Clients in Instant Web Publishing nicht auf Abmelden klicken oder ein Script ausführen, das den Schritt „Programm beenden“ enthält, ist die Verbindung zu der Datenbank immer noch aktiv. Die Daten stehen eventuell anderen Web-Benutzern zur Verfügung oder Benutzer werden daran gehindert, auf die Datei zuzugreifen. Außerdem sollten Web-Benutzer den Browser verlassen, um die Kontoinformation aus der Cache-Datei des Webbrowsers zu löschen. Weitere Informationen finden Sie im Handbuch *FileMaker Instant Web Publishing*, das sich im Ordner „Elektronische Dokumentation“ (im Ordner „Deutsch Extras“) befindet.
6. Wählen Sie im Dialogfeld „Sharing“ die Option Nicht auf Instant Web Publishing-Homepage anzeigen, um einen Dateinamen aus der integrierten Instant Web Publishing-Datenbank-Homepage auszublenden. Dies empfiehlt sich, wenn Ihre Lösung aus mehreren Dateien besteht und Sie nicht möchten, dass alle Dateinamen angezeigt werden. Diese Funktion sollte nicht das Definieren von Konten und Zugriffsrechten in Dateien ersetzen.
7. Betrachten Sie die Ergebnisse von Scripts.
 - Wenn ein Script einen Schritt zum Löschen von Datensätzen enthält und ein Web-Benutzer die Datei mit einem Konto öffnet, das das Löschen von Datensätzen nicht zulässt, wird dieser Scriptschritt nicht ausgeführt. Das Script könnte jedoch weiter ausgeführt werden, so dass unerwartete Ergebnisse auftreten können. Aktivieren Sie eventuell Script mit vollen Zugriffsrechten ausführen, damit Scripts Datensätze löschen oder andere eingeschränkte Aktionen ausführen können, auf die Benutzer gewöhnlich nicht mit ihren Konten und Zugriffsrechten zugreifen dürfen. Sie können Benutzer daran hindern, ein bestimmtes Script auszuführen, indem Sie ihre Berechtigungen ändern und Scripts angeben, die für bestimmte Benutzer auf Kein Zugriff eingestellt sind.
 - Im Web veröffentlichte Datenbanken sollten Scripts enthalten, die keinerlei schädliche Wirkung haben, wenn sie von beliebigen Web-Benutzern ausgeführt werden. Um nicht unterstützte Scriptschritte anzuzeigen, öffnen Sie das Script und wählen Sie im Dialogfeld „Script bearbeiten“ die Option Web-Kompatibilität anzeigen. Grau dargestellte Scripts werden nicht im Web unterstützt.
 - Wenn Schritte in Ihren Scripts nicht unterstützt werden (z. B. Schritte, die nicht Web-kompatibel sind, wie „E-Mail senden“, oder zu deren Ausführung Benutzer nicht berechtigt sind), legen Sie mit dem Scriptschritt AnwenderAbbruchZulassen fest, wie nachfolgende Schritte gehandhabt werden. Weitere Informationen finden Sie im Handbuch *FileMaker Instant Web Publishing*, das sich im Ordner „Elektronische Dokumentation“ (im Ordner „Deutsch Extras“) befindet.



Wählen Sie **Web-Kompatibilität anzeigen**, um die Script-Schritte grau darzustellen, die nicht Web-kompatibel sind.

8. Speichern Sie keine Datenbankdateien oder vertrauliche Daten im FileMaker Pro Web-Ordner (oder einem seiner Unterordner).
9. Aktivieren Sie Protokolldateien, um die IP-Adresse von Benutzern aufzuzeichnen, die auf Ihre im Web veröffentlichten Dateien zugreifen (sowie Datum und Uhrzeit der Anfragen und andere Optionen).
10. Mit FileMaker Pro können Sie den Zugriff auf Benutzer mit einer IP-Adresse beschränken, die Sie vorab angeben. Beim Bereitstellen von Dateien mit FileMaker Server Advanced können Sie in der Web-Server-Anwendung Einschränkungen für Client-IP-Adressen festlegen.
11. Wenn Sie im Web veröffentlichte Datenbanken mit FileMaker Server Advanced bereitstellen, können Sie zusätzliche Sicherheitsmaßnahmen wie SSL-Verschlüsselung verwenden, die eventuell in Ihrer Web-Server-Anwendung zur Verfügung stehen. Weitere Informationen erhalten Sie unter „Secure Sockets Layer (SSL)-Sicherheit für Web Publishing“ auf Seite 26. Sie können auch Web-Publishing-Technologien deaktivieren, die Sie nicht nutzen. Weitere Informationen finden Sie im Handbuch *FileMaker Server Advanced Web Publishing Installation*.
12. Wenn Sie im Web veröffentlichte Datenbanken mit FileMaker Server Advanced bereitstellen, verwendet die Web Publishing Engine zur Kommunikation mit FileMaker Server Advanced und Ihrem Web-Server bestimmte Ports und Protokolle. Sie müssen eventuell Ports öffnen oder Protokolle auf Ihren Host-Computern und Firewalls zulassen. Weitere Informationen finden Sie im Handbuch *FileMaker Server Advanced Web Publishing Installation*.
13. Wenn Sie Datenbanken mit FileMaker Server Advanced bereitstellen und Custom Web Publishing mit XML verwenden, können Sie Ihre Sicherheit von einem Webbrowser testen, um etwaige offen gelegte Elemente zu ermitteln:

- Um die Namen der Datenbanken anzusehen, die im Web mit XML veröffentlicht sind, geben Sie diese Adresse in das Adressfeld des Browsers ein:

`http://<ip:port>/fmi/xml/fmresultset.xml?-dbnames`

- Um Datenbanken zu sehen, die im Web mit XSLT veröffentlicht wurden, geben Sie diese Adresse ein:

`http://<ip:port>/fmi/xsl/stylesheet_name.xsl?-grammar=fmresultset&-dbnames`

- Um die Felder für einen Datensatz in Ihrer Datenbank zu sehen, geben Sie diese Adresse in das Adressfeld des Browsers ein:

`http://<ip:port>/fmi/xml/fmresultset.xml?-db=dbname&-lay=layoutname&-findany`

- Um die Namen der Scripts in einer Datenbank anzuzeigen, geben Sie diese Adresse in das Adressfeld des Browsers ein:

`http://<ip:port>/fmi/xml/fmresultset.xml?-db=dbname&-scriptnames`

- Um die Namen der Layouts in einer Datenbank anzuzeigen, geben Sie diese Adresse in das Adressfeld des Browsers ein:

`http://<ip:port>/fmi/xml/fmresultset.xml?-db=dbname&-layoutnames`

Informationen über Anfragenbefehle und Parameter finden Sie im Handbuch *FileMaker Server Advanced Custom Web Publishing*.

Schutz Ihrer Datenbanken vor Angriffen aus dem Web

Beginnen Sie, indem Sie die Sicherheitsmaßnahmen in diesem Dokument lesen. Ihr Host-Computer ist sowohl Ihre Verbindung zur Außenwelt als auch, falls ungeschützt, die Verbindung der Außenwelt zu Ihrem internen Netzwerk. Prüfen Sie das Folgende:

- Für im Web freigegebene Lösungen, insbesondere im Internet, eignen sich Konfigurationen mit zwei (oder mehr) Computern, die die Datenbank von den Web-Publishing-Komponenten, Firewalls, SSL und anderen Internet-Standardtechnologien trennen. Dies schützt den Zugriff auf ihre Dateien sowie die Kommunikation zwischen dem Webbrowser der Web-Benutzer und dem Server.
- Überprüfen Sie die Einstellungen für Remote-Zugriffe, wie z. B. File Sharing und FTP, und stellen Sie sicher, dass der direkte Zugriff auf den Host-Computer zum Hoch- und Herunterladen von Dateien eingeschränkt wird, so dass kein unberechtigter Zugriff auf Ihre Dateien erfolgen kann.
- Wenn Sie eine FileMaker Pro-Datenbank mit TCP/IP bereitstellen, gestatten Sie möglicherweise ungebetenen Besuchern Zugriff auf Ihren Host-Computer und das interne Netzwerk. Eine Firewall ist unerlässlich, um Ihr Netzwerk abzutrennen und Dateien „hinter der Firewall“ zu schützen, damit Benutzer außerhalb der Firewall auf keine TCP/IP-Adressen zugreifen können, die Sie nicht freigegeben haben.

Web-Server-Sicherheit

Die Web-Server-Anwendung hat die entscheidende Aufgabe, Datenanfragen zu verarbeiten und zu beantworten, wenn Sie Datenbanken, Bilder und anderen Inhalt im Web veröffentlichen. Wenn ein Benutzer eine Internetadresse in das Adressfeld des Browsers eingibt, fordert er die Web-Server-Software der entsprechenden Adresse auf, Daten oder ein Bild zu suchen und auf den Computer des Benutzers herunterzuladen, wo diese dann im Browser angezeigt werden. Der Web-Server verfügt über eigene Sicherheitsmechanismen zum Schutz der Integrität dieses Prozesses.

Wenn Sie Datenbanken mit FileMaker Server Advanced freigeben, verwenden Sie eine Web-Server-Anwendung eines anderen Anbieters wie z. B. Microsoft Internet Information Server (IIS) oder Apache HTTP Server, um Dateien im Web zu veröffentlichen. Sie können die zusätzlichen Sicherheitsfunktionen wie SSL-Verschlüsselung nutzen, um Daten sicherer vom Host an die Web-Clients zu übertragen.

Verwendung von Verschlüsselung oder VPNs zum Schutz von Daten

Erwägen Sie die Verwendung von Verschlüsselung und VPNs (Virtual Private Networks) zum Schutz Ihrer Daten in einem TCP/IP-Netzwerk. Bei der Verschlüsselung werden Daten (verständlicher Text) so manipuliert, dass das Ergebnis (verschlüsselter Text) nur für bestimmte Anwendungen verständlich ist.

Sie können Daten auf eine der folgenden Arten schützen:

- Richten Sie ein sicheres VPN ein, um Ihren Netzwerkverkehr teilweise (oder vollständig) bei der Übertragung in einem WAN (Wide Area Network) zu verschlüsseln.
- Stellen Sie Datenbanken mit FileMaker Server Advanced bereit und konfigurieren Sie SSL-Verschlüsselung in der Web-Server-Anwendung.
- Kombinieren Sie die obigen Methoden.

Secure Sockets Layer (SSL)-Sicherheit für Web Publishing

Das SSL-Protokoll ist ein Standard für die verschlüsselte und authentifizierte Kommunikation zwischen Web-Servern und Clients (Webbrowsern). SSL-Verschlüsselung ist nur für Datenbanken verfügbar, die mit FileMaker Server Advanced bereitgestellt wurden, und wird in der Web-Server-Anwendung aktiviert, z. B. Microsoft Internet Information Server (IIS) oder Apache HTTP Server von der Apache Group.

Bei der SSL-Verschlüsselung werden Informationen, die zwischen Servern und Clients übertragen werden, mithilfe von mathematischen Formeln in unverständliche Informationen umgewandelt. Der englische Fachausdruck für diese Chiffrier-Algorithmen ist *Ciphers*. Diese Algorithmen nutzt der Empfänger, um mithilfe von Schlüsseln, den so genannten *Chiffrierschlüsseln*, die Informationen wieder in verständliche Daten umzuwandeln.

Informationen über das Aktivieren und Konfigurieren von SSL erhalten Sie in der Dokumentation zu Ihrem Web-Server.

Über drahtlose Netzwerke

Eine weitere Sicherheitsschwäche stellen drahtlose Netzwerkgeräte des 802.11x-Standards dar, die so genannten „Wi-Fi“-Verbindungen:

- eine Station (oder das Gerät mit dem Funkzugriff nach 802.11x-Standard) wie z. B. ein Laptop
- ein Zugangspunkt (Wireless Hub oder Bridge), von dem aus auf das Netzwerk zugegriffen wird
- das LAN (Local Area Network) selbst
- ein Authentifizierungsserver, ein separates Gerät, das Clients überprüft, wenn sie eine Netzwerkverbindung versuchen

Ein Netzwerk bleibt bei Funkzugriff offen für das Abfangen von Datenpaketen durch ein beliebiges Funkgerät im Bereich eines Senders. Dies ermöglicht Eindringlingen die Verbindung zu Unternehmensnetzwerken durch Wireless-Protokolle. Diese unberechtigten Zugriffe können mithilfe von High-Gain-Antennen weit außerhalb des üblichen Arbeitsbereichs erfolgen.

Wenn beispielsweise FileMaker Server Advanced Dateien bereitstellt, könnte ein Eindringling auf Daten zugreifen, falls die Dateien nicht über genügend Kontosicherheit verfügen. Ein Eindringling, der weiß, wie ein WAN den Zugriff steuert, könnte Zugriff zum Netzwerk erhalten, eine gültige Computeradresse stehlen und deren zugewiesene IP-Adresse benutzen. Eine typische Vorgehensweise ist es, abzuwarten, bis der gültige Computer über das Netzwerk stoppt, dann dessen Position im Netzwerk zu übernehmen und Zugriff auf alle Geräte im Netzwerk oder das weitere Internet zu erlangen.

Wichtig Schützen Sie bei der Beurteilung der physischen Sicherheit Ihres Netzwerks Ihre Funknetzsignale durch Passwort und Verschlüsselung. Verwenden Sie stets die maximal verfügbare Stufe der Signalverschlüsselung.

XML-Überlegungen

XML- und XSLT-Stylesheets gelten als Industriestandard für den Zugriff auf Daten sowie ihre Verteilung und Präsentation. Mit der Custom Web Publishing-Funktion in FileMaker Server Advanced lassen sich mithilfe von XSLT-Stylesheets XML-Daten filtern und umwandeln. Damit können Metadaten in XML-Dateien, die an Web-Benutzer gesendet werden, entfernt oder geändert werden (z. B. um Feldnamen auszublenden) oder statische Query-String-Parameter (wie Werte von Datenbank- und Layoutnamen) definiert werden, damit sie nicht von Web-Benutzern gesehen oder geändert werden können. Weitere Informationen finden Sie im Handbuch *FileMaker Server Advanced Custom Web Publishing*.

Hinweis Als XML formatierte Daten sind grundsätzlich Text. Das bedeutet, dass sie potenziell abgefangen und gelesen werden, sofern sie nicht durch geeignete Methoden verschlüsselt werden. Wenn Sie Daten mit TCP/IP übertragen und Datenbanken mit FileMaker Server Advanced bereitstellen, sollten Sie in der Web-Server-Anwendung SSL-Verschlüsselung verwenden. Damit blockieren Sie „Packet-Sniffer“-Programme, die den Netzwerkverkehr überwachen und eventuell in der Lage sind, FileMaker Pro-Daten zu extrahieren.

Wichtig Aktivieren Sie erweiterte Zugriffsrechte nur dann, wenn es unbedingt erforderlich ist.

Überlegungen zu Apple Events und ActiveX

FileMaker Pro kann Befehle von Apple Events in Mac OS bzw. von ActiveX in Windows verarbeiten. Dies kann zu unerwarteten Ergebnissen führen, wenn z. B. die Zeit für ein externes Script überschritten wird und es den nächsten Befehl nicht verarbeitet.

Testen Sie bei der Einführung von Technologie anderer Hersteller stets alle Scripts und Benutzerszenarien gründlich.