



# InDesign

*professionell . praxisnah . produktiv*

## *service*

### News

Wissenswertes für die professionelle InDesign-Praxis

### Tipps & Tricks

Tücken des »Umfließens« bzw. des Textverdrängens  
GREP-Stile und GREP-Suche mit Bedingungen nutzen

### Plug-ins & Skripte

Die »Blatner Tools«: ein Füllhorn an zusätzlichen Funktionen und Arbeitshilfen

### Praxis-Spezial

Interview mit David Blatner: Die Arbeit mit InDesign optimieren

# Wissenswertes für die professionelle InDesign-Praxis

## InDesign-Usergroup-Anwendung für Ihr iPhone

Seit Kurzem gibt es nun auch ein »iPhone Web App«, das Ihnen eine Übersicht über etliche InDesign-Usergroups bietet.

Über die Webbrowser-Funktion Ihres iPhone können Sie sich von deren Websites z. B. den letzten InDesign-Tipp oder die nächsten Termine abholen.

Leider ist das »InDesign User Group App« noch nicht im App-Store erhältlich.

Um es zu bekommen, starten Sie Safari auf Ihrem iPhone und gehen zu <http://indesignusergroup.com/iphone/meetings>, wo Sie durch die Installation geführt werden.



## Sicherheitslücke im Adobe Reader und in Adobe Acrobat – Adobe stellte Mitte Januar Abhilfe bereit

Adobe hat die kürzlich gemeldeten und teilweise bereits aktiv ausgenutzten acht Lücken im Adobe Reader und Adobe Acrobat bestätigt und Mitte Januar im Rahmen des dreimonatigen Patch-Zyklus ein Update herausgegeben.

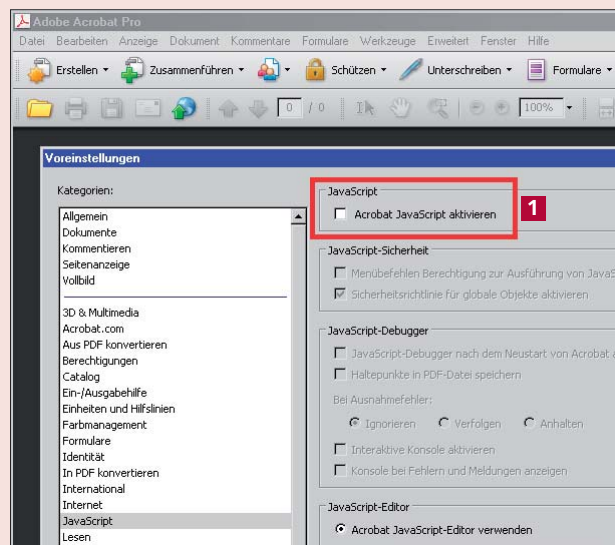
Betroffen sind laut Hersteller Adobe Reader 9.2 und frühere Versionen für Windows, Macintosh, Unix sowie Acrobat 9.2 und vorhergehende Versionen für Windows und Macintosh. Ursache des Sicherheitsproblems ist offenbar ein Fehler in der Adobe-JavaScript-Funktion DocMedia.newPlayer.

Die Lücken ermöglichen das Einschleusen und Ausführen von Code auf verwundbaren Systemen. Dazu genügt es, ein präpariertes PDF-Dokument zu öffnen.

Bislang verteilen die Virenautoren solche Dokumente nur gezielt per Mail. Die Firma F-Secure ([www.f-secure.de](http://www.f-secure.de)) hat in ihrem Blog Beispiele solcher Mails veröffentlicht.

Eine Möglichkeit, um nicht Opfer eines Angriffs zu werden, ist unter anderem das Abschalten von JavaScript im Reader oder Acrobat.

Hierzu öffnen Sie BEARBEITEN → VOREINSTELLUNGEN → JAVASCRIPT und deaktivieren die Option ACROBAT JAVASCRIPT AKTIVIEREN **1**.



An dieser Stelle verhindern Sie das Ausführen von JavaScript-Code komplett, was aus Sicherheitsaspekten heraus ohnehin kein Fehler ist. In JavaScript-Code können sich u. a. »Trojaner« verbergen.

Auf der sicheren Seite sind Sie, wenn Sie Ihren Adobe Reader bzw. Acrobat mit dem von Adobe kostenlos angebotenen Patch auf den neuesten Stand bringen.

Sie erhalten das Patch auf <http://get.adobe.com/de/reader/>