NR. 109 Dezember 2014 / Januar 2015
ISSN 1439-8362
6,90 EUR

Federwelt

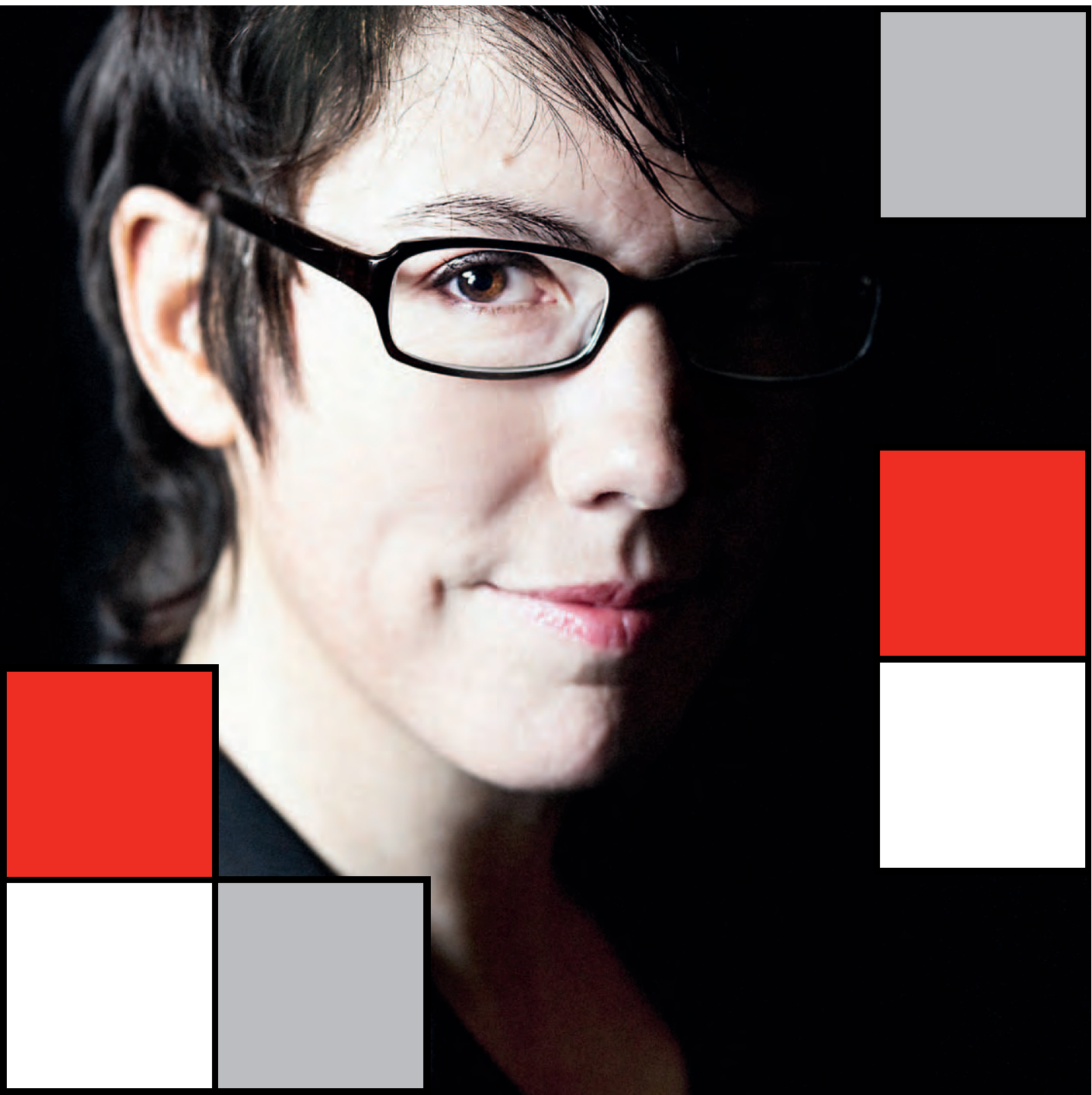
ZEITSCHRIFT FÜR AUTORINNEN UND AUTOREN

Nina George über internationalen Erfolg

So recherchieren Sie richtig! (Teil 1)

Was tun gegen Mobbing?

Textküche: Kurzkrimis und Kurzthriller



Martina Troyer. Foto: Teresa Rothwangl

So schützen Sie sich vor Hackern

Laura Rose im Gespräch mit Martina Troyer

Leider taugt der Beruf als AutorIn nicht als Schutzschild gegen Viren, Trojaner und andere Bösewichter, manche sind raffinierter als ein wirklich guter Plot und für normale User nicht zu erkennen. Wie kann man sich davor schützen, woran merkt man, wann man in Gefahr ist und wie bannt man diese Gefahr? Laura Rose hat nachgehakt.

Frau Troyer, was passiert bei einem Hackerangriff? Sucht ein Hacker sich persönlich ein Opfer aus?

Nein. Meistens ist ein ganzes System sein Ziel. Aber theoretisch könnte ein Leser, dem das Buch eines Autors nicht gefallen hat, auch konkret die Präsenz dieses Autors im Internet torpedieren.

In der Regel ist es das Ziel von Hackerangriffen, „Schadcode" einzuschleusen. Damit werden potenzielle Seitenbesucher einem erhöhten Risiko ausgesetzt, sich Viren, Trojaner oder andere, manchmal sehr gefährliche Gauner einzufangen. Eine Homepage, ein Blog wird somit zum Infektionsrisiko. Man selbst kann andere „anstecken". Das schadet der eigenen Reputation und kann sogar Geschäftsbeziehungen gefährden; zumindest ist es äußerst ärgerlich, und man sollte es nicht auf die leichte Schulter nehmen. Ein solcher „Befall" zieht nicht nur Kosten nach sich, um den Schadcode entfernen zu lassen. Er kann auch dazu führen, dass *Google* den Blog oder die Homepage als potenziell gefährlich einstuft und dies schon bei der Suche anzeigt. Keine gute Empfehlung für AutorInnen, oder? Natürlich lässt sich das alles korrigieren, aber der Aufwand und der „Schreck" für einen Betreiber und die Seiten- oder Blogbesucher sowie die Kosten der Beseitigung können schon recht hoch sein.

Also lieber zum Profi mit der Erstellung eines Internetauftritts oder Blogs?

Ja, oder sich selbst intensiv mit dem Thema beschäftigen. Da immer mehr Menschen ihre Websites im Alleingang basteln, was ja recht einfach ist, haben es die Hacker zunehmend leicht. „Normale" Anwender wissen meistens nicht so gut Bescheid, wo sie welches Häkchen setzen müssen im System, damit ihr Internetauftritt sicherer wird.

Bis vor einigen Jahren wurden Webseiten meist statisch angelegt, mit HTML programmiert. Jedoch waren diese schwierig zu pflegen. Man musste sich schon mit HTML auskennen, um Bearbeitungen vorzunehmen. Der Vorteil war, dass sich in diesem Bereich fast ausschließlich Profis tummelten. Heute kann jeder sich problemlos und ohne tiefergehende Computerkenntnisse beispielsweise *WordPress* herunterladen und an einem Nachmittag einen hübschen Auftritt als AutorIn basteln. Und damit wird es gefährlich, denn im Gegensatz zu den statischen HTML-Seiten sind diese dynamischen Inhaltsverwaltungssysteme (in der Fachsprache: Content-Management-Systeme, kurz: CMS) oft geradezu eine Einladung für Hacker. Dazu komme ich gleich noch.

Ich dachte, WordPress ist nur für Blogs?

Ja, eigentlich wurde *WordPress* als Blogsystem aufgesetzt. Blog ist ja die Abkürzung aus Web und Log, steht also für Web-Tagebuch. Tagebuch deshalb, weil man damit mit Datum versehene Einzelbeiträge erzeugen kann.

Dann wurde *WordPress* immer beliebter, immer weiter optimiert und ist nun zu dem beliebtesten Content-Management-System geworden. Einfach,

weil die Verwaltung und Erstellung von Inhalten so simpel und zugleich komfortabel in der Anwendung ist. So nutzten immer mehr Unternehmen das System auch für ihre ganz normalen Webauftritte – also die Gesamtheit von Einzelseiten. Heute gibt es da kaum mehr die Unterscheidung, ob Blog oder Website. Inhaltlich natürlich schon, aber das System ist dasselbe.

Erklären Sie bitte, was es mit einem Content-Management-System auf sich hat.
Die Ausgabe von Seiten erfolgt hier immer dynamisch. Also das, was man im Browser sieht, wird aus der Datenbank erst frisch zusammengefügt und als eine Webseite dargestellt.

Insofern betrifft das Problem der Absicherung alle mit *WordPress* aufgesetzten Webauftritte.

Und wenn man einfach einen anderen CMS- oder Blog-Anbieter wählt, zum Beispiel TYPO 3, Joomla *oder* Drupal?
Das ist keine Lösung. Die Lösung liegt darin, ein funktionierendes Sicherheitssystem zu installieren. Das Bundesamt für Sicherheit in der Informationstechnik, kurz BSI, hat in einer Studie 2013 die Sicherheit von Content-Management-Systemen der gängigsten Anbieter untersucht und kam zu dem Schluss, dass die grundsätzliche Sicherheit bei allen Systemen ähnlich zufriedenstellend sei, die Gefahren aber meist von Erweiterungen ausgehen. Im Fazit rät das BSI, nach der Installation relevante Sicherheitsoptionen anzupassen. Das macht deutlich: Heute kommt man um ein vernünftiges Sicherheitssystem nicht mehr herum.

In unserem letzten Gespräch rieten Sie AutorInnen ja dazu, einen Blog zu führen als hervorragendes Tool zur Selbstvermarktung mit Webstrategie. Nun geben Sie den Ratschlag, nicht nur die Strategie, sondern auch die Sicherheit im Auge zu behalten. Fangen wir mal von vorne an: Was sollte man beachten, wenn man eine Homepage oder einen Blog ins Netz stellt?
Es fängt beim ansprechenden, responsiven Design an. Heute besucht man Internetseiten als LeserIn nicht mehr nur über den Computer, sondern auch über Tablet-PCs, Notebooks und Smartphones. Ein solches Design, das sich automatisch an diese unterschiedlichen Darstellungsformen anpasst, ist zwingend zu empfehlen, wenn man seine LeserInnen nicht schon nach dem ersten Klick wieder verlieren will.

Das war's schon?
Fast! Kontinuierliche Aktivitäten im Blog, Vernetzung mit anderen, Bekanntmachung der Inhalte über soziale Netzwerke, Aufbau von Leserbindung durch authentische Kommunikation und interessante Inhalte sowie eine regelmäßige Pflege und Wartung des Systems gehören auch dazu. Und bei einem Blog vor allem natürlich Freude beim Schreiben für seine LeserInnen. Ein Autor, der einen Blog installiert, nur damit er auch einen hat, sollte lieber die Finger davon lassen. Ein Blog braucht viel Aufmerksamkeit seitens seines Betreibers – das ist die Voraussetzung, um Aufmerksamkeit bei den Usern zu wecken.

Sie empfehlen dringend, Internetauftritte mit CMS und Blogs warten zu lassen. Reicht es nicht, das einmal wirklich professionell aufzubauen oder aufbauen zu lassen? Das klingt ja wie beim Auto, das regelmäßig zur Inspektion muss ...
Ja, so ist es. Sie kaufen doch auch kein Auto, setzen sich rein, fahren los und erwarten, dass es die nächsten zehn Jahre ohne Macken läuft.

Beim Auto ist es für uns selbstverständlich, regelmäßig den Ölstand zu prüfen, die Zündkerzen zu wechseln oder den Keilriemen auszutauschen. Auch ein Blog sollte diese Aufmerksamkeit bekommen. *WordPress* zum Beispiel gibt regelmäßig Sicherheits-Updates heraus. Diese Updates sind mal mehr und mal weniger umfangreich. Die Entwickler merzen vorhandene Bugs, also kleinere Fehler, aus und schließen Sicherheitslücken, die durch Angreifer ausgenutzt wurden. Solche Updates sollte man als Blogger – und eben auch, wenn man „nur" seine Homepage über ein CMS laufen lässt – unbedingt mitnehmen. Stellen Sie sich vor, der Hersteller Ihres Autos macht eine Rückrufaktion. Würden Sie diese einfach ignorieren nach dem Motto: „Ach, das brauch ich eh nicht ...?" Vermutlich eher nicht.

Um Hackerangriffen vorzubeugen, sollte man also öfter mal zum Blog-TÜV gehen?
Auch wenn das zunächst seltsam klingt, aber regelmäßige Wartung und Service rund um die Aktualisierung der Software und der verwendeten Plug-ins (zu Deutsch: Erweiterungsmodule) sind meiner Erfahrung nach nicht nur Pflicht, damit der Blog oder Webauftritt funktioniert, sondern helfen auch dabei, sich vor Hackerangriffen aus dem Netz zu schützen. Schließlich will man ja – wie beim Auto-TÜV – sicher sein, dass der eigene Blog verkehrstüchtig ist und keine Gefährdung für andere VerkehrsteilnehmerInnen darstellt.

Noch ein Autobeispiel: Würden Sie Ihr Auto in einer Tiefgarage unabgeschlossen lassen? Oder den Schlüssel leicht sichtbar auf die Motorhaube legen?

Genauso verhält es sich allerdings häufig bei Bloggern oder Usern, die ihre Homepage mit viel

Freude und Kreativität selbst gebastelt haben. Die Oberfläche sieht wirklich toll aus, da hat sich jemand Mühe gegeben – starker Auftritt. Doch leider wurden grundlegende Sicherheitsmaßnahmen wie das Löschen und Ersetzen des Admin-Zugangs mit der ID=1 ignoriert oder zu unsichere Passwörter benutzt und damit Hackern regelrecht eine Einladung ausgesprochen: „Hier sind alle Türen offen! Kommt rein! Ihr braucht nicht mal Einbruchswerkzeug, nur die Türklinke runterdrücken!“

Woran merkt man denn, dass etwas passiert ist? Und wie kann man sich davor schützen?

Im besten Fall haben Sie bereits grundlegende Vorkehrungen getroffen: Zum Beispiel das Verstecken des Benutzernamens und der aktuell verwendeten *WordPress*-Version, die Hackern ansonsten zeigt, aus welchem „Modelljahr“ Ihr Auftritt ist und welche Schwachstellen offensichtlich sind. Auch das Aufzeichnen von Einbruchsversuchen mithilfe von Plug-ins wie *Limit Login Attempts* ist hilfreich und das zeitweise Blockieren bestimmter IP-Adressen, die immer wieder versuchen, Ihr Territorium zu übernehmen.

Wie die aktuellen Beispiele massenhaft gekaperter E-Mailadressen und Passwörter schon zeigten, sollten sichere Passwörter, möglichst lang und als Mix aus Buchstaben, Zahlen und Sonderzeichen, zur Grundausstattung gehören. Und regelmäßig geändert werden.

Indem Sie also grundlegende Einstellungen vornehmen, machen Sie es Angreifern aus dem Netz schwerer, Ihren Blog/Ihre Homepage zu kapern oder zu infizieren. Es lässt sich zwar nicht alles verhindern, denn die kriminelle Energie und auch das Wissen der Hacker werden leider immer größer. Aber man kann doch einiges unternehmen: also die Tür abschließen oder verstecken, sodass ein Eintritt für Bösewichter aus der Internet-Unterwelt schwieriger wird.

Wenn ich das so höre, frage ich mich ernsthaft, ob es wirklich klug ist, selbst einen Internetauftritt zu basteln beziehungsweise ob man nicht auf ein Content-Management-System verzichten sollte? Lieber altmodisch mit HTML und dafür sicher?

Gegenfrage: Sollten wir lieber alle wieder aufs Pferd umsteigen, anstatt das Auto zu benutzen? Es ist umständlicher mit HTML – und auch einfache Seiten können, wenn sie selten aktualisiert werden und zu wenig abgesichert sind, gehackt werden.

Fazit: Daran kommen Sie heute einfach nicht mehr vorbei und die Vorteile beim Einsatz eines Content-Management-Systems überwiegen: schnelles Publizieren, komfortable Bedienung dank Editoren, die mit anderen Schreibprogrammen vergleichbar sind, Vorteile durch einfache Möglichkeiten zur „Verschlagwortung“, automatischer Austausch von Benachrichtigungssignalen, wenn in einem anderen *WordPress*-Blog auf den eigenen Beitrag verlinkt wurde und, und, und ... Ganz zu schweigen von einem Plus an Suchmaschinenfreundlichkeit.

Wenn ich das so höre, glaube ich, dass ich jetzt doch lieber auch zum Profi gehe. Denn um das zu leisten, da muss eine herkömmliche Anwenderin doch sehr viel Wissen haben?

Ich plädiere ebenfalls für den Profi, ich selbst beschäftige übrigens auch eine „Web-Admine“, wenn es ans Eingemachte geht. Ich bin nun mal hauptberuflich Webstrategin.

Beim Wartungs- und Update-Service wird Ihnen der Profi einen Backup-Plan machen und die Updates der *WordPress*-Software und der Plug-ins über den FTP-Server vornehmen (etwa das Backup der Datenbank und des Dateisystems, das Herunterladen des neuen Versionspakets, gegebenenfalls das Löschen oder Deaktivieren veralteter Plug-ins oder bestimmter Dateien, das Erneuern von Sicherheitsschlüsseln, Hochladen der neuen Dateien, das Aktualisieren der Datenbank und der Plug-ins). Dann wird geprüft, ob nach dem Update noch alles funktioniert wie es soll.

Manche Plug-ins sind sinnvoll und nützlich, werden von den Entwicklern aber leider nicht regelmäßig gepflegt und aktualisiert und könnten somit inkompatibel mit der jeweils aktuellen Systemsoftware sein. Dann schlägt Ihnen der Profi geeignete

Ersatz-Plug-ins vor. Auch kann es vorkommen, dass Plug-in-Updates mit anderen verwendeten Plug-ins nicht mehr kompatibel sind und Sie plötzlich nur noch einen weißen Bildschirm sehen oder die Seite in Teilen nicht oder nur noch falsch angezeigt wird.

Zur Vereinfachung zurück zum Auto-Beispiel: Wenn man beim Zündkerzen-Wechsel eine Zündkerze verbaut, die nicht zum Motor passt, kann es sein, dass der Motor auf einmal nicht mehr anspringt oder sogar ganz kaputtgeht. Der Mechaniker, der sich auskennt, schlägt Ihnen also im besten Fall immer genau die richtige Zündkerze vor – so wie der Wartungsprofi Ihnen eben auch die Arbeit abnimmt, das mühsam selbst herauszufinden.

Also lautet Ihr Fazit schlichtweg: Vorbeugen?
Genau. Es ist wie so oft im Leben – hinterher ist man immer schlauer! Erst wenn mal eingebrochen wurde, fühlt man sich im eigenen Haus nicht mehr sicher und denkt über geeignete Sicherheitsmaßnahmen nach. Wenn es dazu aber gar nicht erst kommt, weil man Vorkehrungen getroffen hat, lebt es sich leichter und unbekümmerter.

Daneben hängt vieles natürlich vom eigenen Sicherheitsbedürfnis ab. Ein Wartungspaket ist aus meiner Sicht eine gute Möglichkeit, sich als AutorIn nur um das Wesentliche kümmern zu müssen, und das ist ja auch schon einiges: regelmäßiges Veröffentlichen von neuen Inhalten, Kommunikation mit den eigenen Fans, LeserInnen, Buch-BloggerInnen und Verlagen, Social-Media-Maßnahmen und sonstige Selbstvermarktungs-Aktivitäten. Denn schließlich geht es darum, mit dem eigenen Internetauftritt Spaß und Erfolg zu haben.

Letztlich sollten Sie es so sehen: Ihr Internetauftritt ist Ihr virtueller Zweitwohnsitz. Und wer hat schon gern Einbrecher und Bazillen in den eigenen vier Wänden! Da muss man eben Türen schließen und manchmal lüften, abstauben, nass wischen und saugen. Und das alles kann man im Sitzen tun.

Klingt gut: Hier ein Klick, da ein Klick – und Meister Proper nickt zufrieden. – Wir bedanken uns herzlich für dieses abermals sehr interessante Gespräch, liebe Frau Troyer.

> www.netzgewandt.de
> https://twitter.com/netzgewandt
> http://about.me/martinatroyer

Reich werden

mit Goetz Buchholz

Diesmal: 7.500 Euro für die etwas Älteren

Man wird ja mal fragen dürfen: Sind Sie schon 50 oder älter? Leben Sie hauptberuflich vom Schreiben? Und haben neben der Rentenversicherung über die KSK auch noch eine private Altersvorsorge?

Dreimal Ja? Dann können Sie von der VG Wort viel Geld bekommen: bis zu 7.500 Euro.

Klingt zu schön, um wahr zu sein? Dann also der Reihe nach: Nach ihrer Satzung führt die Verwertungsgesellschaft Wort die Hälfte ihrer Einnahmen aus der Bibliothekstantieme (und noch einige Gelder mehr) an ihr Autorenversorgungswerk ab. Dessen Aufgabe ist es, freie Autorinnen und Autoren bei der Altersvorsorge finanziell zu unterstützen. Das macht es seit 2010 so, dass es diesen Leuten die Hälfte des Geldes, das sie im Laufe der Jahre in eine private Renten-, eine Lebensversicherung oder einen Sparvertrag zur Altersvorsorge eingezahlt haben, nachträglich überweist. Also einfach schenkt.

Ja, im Ernst: Das ist zwar nicht immer ganz die Hälfte, weil der Auszahlungsbetrag derzeit auf 7.500 Euro gedeckelt ist – aber das ist ja auch deutlich mehr als gar nichts. Beantragen kann man dieses Geld frühestens in dem Jahr, in dem man 50 Jahre alt geworden ist, und spätestens bis zum 31.12. des Jahres, in dem man das gesetzliche Rentenalter erreicht hat. Dann freilich eilt es, denn danach geht nichts mehr!

Natürlich gibt es noch ein paar Bedingungen, damit man Anspruch auf diese Unterstützung hat: Man muss erstens: wahrnehmungsberechtigt bei der VG Wort sein, zweitens: über die Künstlersozialkasse rentenversichert sein, drittens: laut Steuerbescheid(en) in den letzten fünf Jahren jeweils mindestens 3.900 Euro und mindestens die Hälfte seines gesamten Einkommens mit freiberuflicher Autorentätigkeit verdient haben, und viertens: Geld in eine private Altersvorsorge eingezahlt haben, zu der man keine anderen Zuschüsse bekommen hat.

Wer sich da nicht sicher ist, den bittet die VG Wort, den Antrag trotzdem erst einmal zu stellen, denn *„in begründeten Ausnahmen"* geht es auch ohne diese Bedingungen. Das Formular steht auf http://tom.vgwort.de unter „Papierformulare/Merkblätter".

Also, wer schon über 50 ist: Warum noch warten? Und wer gerade Rentnerin geworden ist: Jetzt auf keinen Fall mehr warten! Im Jahr danach gibt's nichts mehr.

Mehr auf www.mediafon-ratgeber.de – Goetz Buchholz