

## THEMA AM SAMSTAG: UNTERNEHMEN UND DIE IT-WELT

## Mit freier Software lässt sich sparen

Auch in kleinen und mittleren Unternehmen kann der Einsatz so genannter freier und Open-Source-Software interessant sein. Mit diesem Thema startet am Dienstag eine Informationsreihe der Wirtschaftsförderer von Stadt und Landkreis. Professor Wilhelm Meier von der Fachhochschule Zweibrücken ist einer der Referenten. Mit ihm sprach vorab Andrea Daum.

**Herr Meier, Sie versuchen, das Thema Freie und OpenSource-Software kleinen und mittleren Unternehmen (KMU) schmackhaft zu machen. Was ist Freie und OpenSource-Software genau?**

Wenn wir von Freier und OpenSource-Software (FOSS) sprechen, denken die meisten Leute, dass sie sich in einem rechtsfreien Raum bewegen. Das stimmt aber nicht. Eigentlich ist genau das Gegenteil der Fall. Freie Software ist gekennzeichnet durch vier Grundprinzipien. Sie ist zweck-, kopier-, veränder- und vier-ten wiederverteilbar.

**Und das bedeutet?**

Zweckfrei bedeutet: Ich darf mir die Software im Internet oder irgendwo besorgen und kann sie für jeden beliebigen Zweck einsetzen. Der Hersteller beziehungsweise das Projekt schreibt mir nicht vor, für welchen Zweck ich sie einsetzen darf beziehungsweise für welchen nicht. Wenn ich beispielsweise freie Software nutze, die für eine Modellbahnkonzipiert wurde, dann kann mir der Hersteller nicht vorschreiben, dass ich sie im Extremfall nicht für ein richtiges Bahnsystem einsetzen darf. Das Risiko trage ich natürlich vollständig selbst. Freie Software muss kopierfrei sein, das heißt, ich darf sie kopieren, weitergeben, das bedeutet auch verkaufen. Veränderbar ist ein Kunstwort von mir. Es bedeutet, dass ich den Zugang zum Quelltext des Programms habe, dass ich Veränderungen am Programm vornehmen kann, es beispielsweise auf die Bedürfnisse des Unternehmens anpassen kann. Da spielt dann auch die Musik, die es interessant macht für KMU. Schließlich noch die Wiederverteilerfreiheit. Das bedeutet, dass ich das möglicherweise veränderte Programm wieder verteilen kann und darf, aber nicht muss. Wenn ich es verteile, dann immer unter den genannten Grundprinzipien.

**Wo wird solche Software (FOSS) denn schon eingesetzt?**

Vielen Leuten ist gar nicht bewusst, dass sie schon mit FOSS arbeiten. Beispielsweise surft fast jeder im Internet. Der Rechner steht zu Hause und greift auf Server zu, auf denen zu weit über 50 Prozent FOSS läuft. Verschlüsselungssoftware, die die Banken für Internet-Homebanking nutzen, arbeitet wohl fast ausschließlich mit FOSS. Das heißt: Jeder, der dazu in der Lage ist, kann sich das Programm anschauen und dann entscheiden, ob er ihm vertraut oder nicht. Bei proprietärer CloseSource-

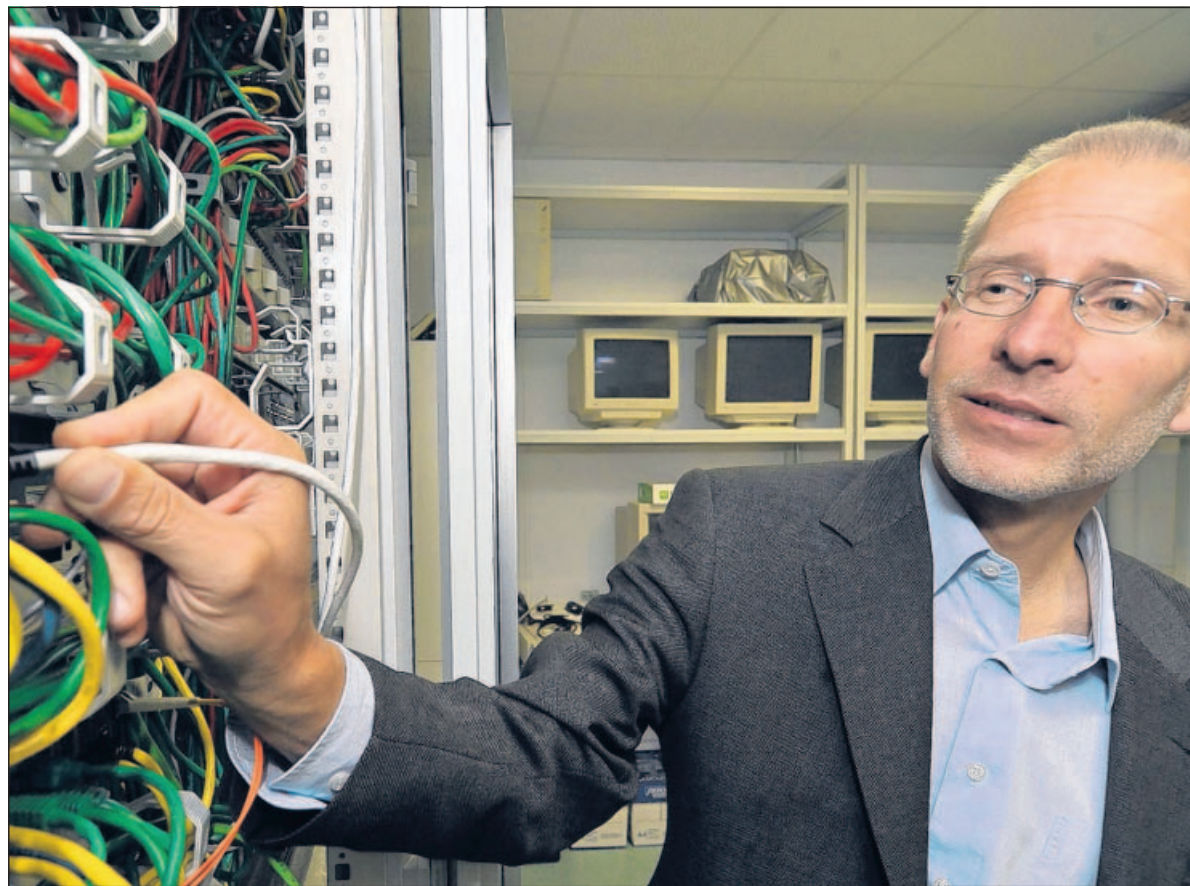
**ZUR PERSON**

Wilhelm Meier stammt aus dem nordrhein-westfälischen Lage. Nach dem Studium der Elektrotechnik an der Leibniz-Universität in Hannover promovierte er an der Universität der Bundeswehr in Hamburg. Von 1996 bis 2000 arbeitete er bei der Deutschen Bahn AG, übernahm dort den Bereich Unix. 2000 erhielt er den Ruf als Professor an die Fachhochschule in Zweibrücken. Er lehrt im Fachbereich Informatik und Mikrosystemtechnik. Das Projekt KMUX Freie/OpenSource-Software für kleine und mittlere Unternehmen ist ein Schwerpunkt seiner Arbeit. Meier ist verheiratet, hat zwei Kinder. „Wir sind die Linux-Familie“, sagt er über sich und seine Familie, denn auch privat nutzt Familie Meier freie und Open-source-Software. Wenn er Zeit hat, geht Meier gerne wandern und macht Musik. (add)

Software (CSS) geht das nicht, da müssen Sie dem Hersteller einfach glauben, dass es sicher ist. Kritiker sagen, wenn ein Programm offen ist und – überspitzt ausgedrückt – jeder beliebige Informatikstudent darauf zugreifen kann, dann ist es unsicher. Dieses Argument lässt sich leicht entkräften. Denn tausende Programmierer können sich das Programm anschauen und stellen ganz schnell fest: Da stimmt etwas nicht. Bei CSS ist das nicht möglich. Fest steht, dass FOSS nicht unsicherer ist als lizenzierte Software.

**Wo liegt für Unternehmen der Vorteil im Einsatz von FOSS?**

Ohne Dienstleistung, ohne eine Beratungsleistung lässt sich Software heute fast gar nicht mehr sinnvoll einsetzen. Wenn freie Software eingesetzt wird, spare ich mir die Lizenzgebühr. Dieses gesparte Geld kann ich für die Dienstleistung ausgeben, die mir das Programm im Unternehmen einführt oder auf meine Bedürfnisse zuschneidet. Ich kann das Geld also intelligenter ausgeben. Ohne Dienstleistung geht es auch bei proprietärer Software nicht. Bei FOSS



Wilhelm Meier lehrt an der Fachhochschule Zweibrücken im Fachbereich Informatik und Mikrosystemtechnik. Freie und offene Software für Unternehmen ist einer seiner Arbeitsschwerpunkte. FOTO: SEEBALD

habe ich aber den weiteren Vorteil, dass ich mir den Dienstleister frei aussuchen kann. Große Software-Unternehmen haben oft fest vergebene Vertriebsbereiche, das heißt: ich bin an einen bestimmten Dienstleister gebunden.

**Wenn Unternehmen Geld sparen können, sollte man eigentlich meinen, Sie seien dem Thema gegenüber aufgeschlossen...**

Man muss da unterscheiden. In bestehenden Firmen hat Microsoft oft fast ein Monopol für das Betriebssystem. Dann gibt es die so genannte Branchensoftware. Zum Beispiel eine Software, die Lederzuschnitte optimiert. Diese sehr spezielle Software wird meist von kleinen Softwareunternehmen hergestellt, die oft gar nicht die Möglichkeit sehen, dass sie ihre Branchenlösung unabhängig von einer bestimmten Plattform, also beispielsweise Microsoft programmieren könnten. Der Neugründer kann hingegen von Anfang an sagen: Ich will auf FOSS setzen. Zumindest bei Dingen wie E-Mail, Telefondienst, Internet, Bildbearbeitung und vielem mehr. Alles, was

branchenspezifisch ist, lässt sich mit FOSS leicht realisieren. Das liegt schon in der Natur der Sache, denn diese Dinge interessieren weltweit, interessieren also auch viele Programmierer. Bei Branchenlösungen ist es anders. Die Menge der metallverarbeitenden Betriebe, die Aluminiumteile links herum gebogen herstellen, ist natürlich begrenzt. Dann ist es schwierig, auf der ganzen Welt genügend Entwickler zu finden. Dabei vergessen die kommerziellen Hersteller aber im Grunde, sich ein Stückchen von dem OpenSource-Markt abzuschneiden. Es geht nicht darum, dass ihr Programm FOSS ist. Es geht für sie darum, dass sie ihre Produkte so schreiben, dass diese in Kombination mit FOSS laufen, zum Beispiel zusammen mit Programmen wie OpenOffice oder Linux.

**Wie sehen Sie denn die Zukunft von FOSS, wie wird sich der Markt entwickeln?**

Erwender werden vermehrt Plattformneutralität fordern. Die Fokussierung auf Windows wird schwinden, auch weil der Punkt gesehen wird, dass Lizenzierungsgebühren

gespart werden können. Wichtig ist, dass den FOSS Bedingungen zugrunde liegen, die mittlerweile justizabel sind, das gibt Rechtssicherheit.

**Aktuell und kurzfristig dürften wohl eher noch Schnittstellen zwischen freier und proprietärer Software, die beispielsweise Microsoft-basiert ist, zu lösen sein oder?**

Ja, aber da gibt es ja entsprechende Beratungsdienstleistungen. Beispielsweise auch an der Fachhochschule. Wenn ein Unternehmen kommt und sagt, ich möchte das, habe aber eine spezielle Branchensoftware, dann könnte man beispielsweise im Rahmen einer Bachelorarbeit nach einer Schnittstellenlösung suchen. In 80 Prozent der Fälle funktioniert das auch ohne unlösbare technische Schwierigkeiten.

**Was sind denn die Vorteile von FOSS für die Unternehmen, abgesehen von gesparten Lizenzgebühren?**

Ich kann sie optimal auf meine Arbeitsabläufe abstimmen. Sagen wir mal mit einer proprietären Software und einer freien, vergleichbaren Software ließen sich 75 Prozent der Be-

**INFO-REIHE**

Loht sich freie Software für ein Unternehmen? Wann sind Firmen-Daten sicher oder was bedeutet elektronische Archivierung? – Mit solchen und weiteren Fragen beschäftigt sich eine neue Info-Reihe zu Informations- und Kommunikationstechnologie in kleinen und mittleren Unternehmen (KMU). Veranstalter sind die Wirtschaftsförderungsgesellschaft Südwestpfalz des Landkreises und das Amt für Wirtschaftsförderung Pirmasens in Zusammenarbeit mit Fachleuten der Fachhochschule Kaiserslautern und der Wirtschaft.

Die fünf Veranstaltungen beginnen jeweils um 18 Uhr und finden in der Fachhochschule Pirmasens statt (Raum Stockholm im Gebäude A, 1. OG, Zimmer A 114):

- Dienstag, 22. September: Freie und Open Source Software – Chancen und Risiken für KMU
- Dienstag, 6. Oktober: IT-Sicherheit – Was muss, was kann? Einfach sicher!
- Dienstag, 27. Oktober: Elektronische Archivierung – Suchst du noch oder findest du schon?
- Dienstag, 17. November: Qualifizierte elektronische Signatur – Wie geht das? Wer braucht es? Wie nutzt man sie in KMU?
- Donnerstag, 10. Dezember: VoIP (interne) Telefonie über Netzwerk – Was steckt dahinter und welchen Nutzen können KMU daraus ziehen?

Die Teilnahme ist kostenlos; es gibt noch freie Plätze. Anmeldungen unter Telefon 06331/809-139 oder 06331/1426206. (tre)

triebsvorgänge optimal abbilden. Dann kann das dem Unternehmen eventuell reichen. Wenn ich aber in den fehlenden 25 Prozent meine Chance zum Wettbewerbsvorteil sehe, dann kann ich nur die FOSS genau auf meine Anforderungen abstimmen, da ich hier Quelltexte ändern kann. Bei CSS geht das nicht. Ob ich diese Veränderungen, dieses neue Produkt dann wieder weiter verteile oder nicht, das ist meine Sache, das ist meine Freiheit. Letzteres kann durchaus Sinn machen, weil Unternehmen dann beispielsweise Entwicklungskosten teilen können.

**Worauf muss geachtet werden beim Einsatz von FOSS?**

Auf Zukunftsfähigkeit. Denn es bringt nichts, einen großen Strauß an Programmen zu haben, deren Projekte gefährdet sind. Augenmaß ist gefragt, denn sonst kostet mich auch FOSS unterm Strich viel Geld. Hier empfiehlt sich eine unabhängige Beratung. Ich würde keinem Unternehmen, das nicht aus der IT-Branche kommt, raten, sich selbst FOSS-Software zusammenzustellen, sondern sich beraten zu lassen.

## Das größte Risiko sitzt vorm PC

Wie wichtig die Sicherheit im Umgang mit Firmendaten ist, scheint Mitarbeitern und Chefs oft nicht bewusst zu sein. Sonst würden Experten nicht immer wieder auf ähnliche Fehler stoßen, wie Georg Schütz, ein weiterer Referent der IT-Reihe, feststellt. Dabei können Fehler teuer zu stehen kommen.

VON GEORG SCHÜTZ

Bonn 14. September 2009: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bewertet die IT-Sicherheitslage in Deutschland für das zweite Quartal 2009 mit „erhöhtes Risiko“. Besorgniserregend sind für die Experten nicht nur gezielte Angriffe, wie zum Beispiel auf die US-Flugkontrolle, oder der Diebstahl von Datenträgern der britischen Luftwaffe. Insbesondere die Verbreitung von „Würmern“ wie „Conficker“ oder „Koobface“ und die Entdeckung eines ganzen Netzes, ein so genanntes Bot-Netz (von roBOTer-Netz), mit der schier unvorstellbaren Zahl von 1.900.000 gekaperten Rechnern unter fremder Kontrolle sind sehr bedenklich. Von diesem Netz waren auch Regierungsstellen und Unternehmen betroffen. Jüngstes Opfer der Auswirkungen eines solchen Bot-Netzes waren die Mailkunden bei T-Online Anfang September, als über mehrere Tage Mails nur sehr verspätet oder gar nicht ankamen, weil die Bot-Rechner T-Online mit Spam-Mails überschwemmt.

Beim Lesen derartiger Berichte drängt sich der Verdacht auf, dass hier Kriminelle mit großem technischem Aufwand am Werke sind. Der Blick in die Praxis in Unternehmen und bei privaten IT-Benutzern zeigt aber, dass „das größte Risiko vor dem Computer sitzt und nicht darin steckt“, wie es ein IT-Sicherheitsexperte des Heise-Verlags während eines Forums auf der Computer-Messe

CeBIT einmal formulierte.

In der Tat kommen die meisten IT-Sicherheitsprobleme in Unternehmen nicht von außen, sondern von innen. Dabei wäre den meisten Risiken mit sehr einfachen Methoden und ein bisschen Disziplin beizukommen. Die größten Fehler beim Umgang mit IT in Unternehmen sind:

- keine aktuellen Systeme; Sicherheitsupdates werden nicht gemacht,
  - keine wirksame Kontrolle der Aktivitäten im Internet,
  - jeder darf fast alles aus dem Internet herunterladen,
  - keine aktuellen Virens Scanner, Spam-Blocker und Schutzsoftware,
  - keine eingeschränkten Benutzerrechte, jeder darf Software installieren,
  - keine Zugangskontrolle, Passwörter sind öffentlich,
  - jeder darf USB-Geräte und CD/DVD-Brenner benutzen,
  - keine aktuelle Datensicherung.
- Der oben erwähnte Koobface-Wurm animiert die Benutzer so genannter sozialer Netze wie Facebook oder mySpace dazu, Schadsoftware herunterzuladen. Im Unternehmen stellen sich spontan die Fragen: „Was macht der Mitarbeiter bei Facebook?“ und „Wieso darf er diese Software laden?“ Beides lässt sich wirkungsvoll zum Beispiel mit Web-Inhalts-Filtern vermeiden.

Wenn die Software schon heruntergeladen wurde oder als Anhang mit einer Mail kam, wieso wird sie

dann nicht auf Viren- oder Schadsoftware geprüft? – Meistens deswegen, weil entweder gar kein Virens Scanner läuft oder keine aktuelle Version vorhanden ist, die sich täglich aktualisiert. Tipp: Wer auch den Kostenvorteil freier und OpenSource Software nutzen will, der greife zu ClamWin Free Antivirus.

Und wenn die Software ungeprüft auf der Festplatte liegt: Wieso darf der Mitarbeiter sie installieren? Einfache Antwort: Weil der PC falsch konfiguriert ist und jeder alles darf. Das BSI fordert hingegen das „Need-to-know-Prinzip“, was heißt: Jeder sollte nur das sehen und tun dürfen, was er für die tägliche Arbeit benötigt. Das lässt sich auch in kleinen Unternehmen und zu Hause einfach über Benutzerrechte und Benutzerrollen steuern.

Wirksame Rechte- und Rollenkonzepte verlangen aber auch Disziplin bei Passwörtern und Zugangsschutz. Die beste Rollenverteilung nutzt nichts, wenn der Versammlungsleiter das Passwort der Personalabteilung oder der Konstruktionsmitarbeiter kennt oder überhaupt keine Passwörter vergeben wurden. Wenn dann noch allen Benutzern der Zugang zu USB-Steckplätzen und CD-Brennern offen steht, dann muss man sich nicht mehr über Datendiebstahl wundern. Gerade in Zeiten der Krise sind Betriebsgeheimnisse, Kundenadressen, Lieferantendaten oder Personalangaben eine gefragte Handelsware oder vielleicht sogar die Eintrittskarte in ein konkurrieren-

des Unternehmen. Die Gegenmaßnahmen sind einfach und wirkungsvoll: USB lässt sich abschalten, CD-Brenner sind in wenigen Sekunden ausgebaut, denn in den wenigsten Arbeitsplätzen sind sie auch notwendig. Hier noch ein Tipp zur Vertiefung des Themas: Einen Workshop zu diesem Thema wird es am 28. Oktober beim Bundesverband mittelständischer Unternehmen in Pirmasens geben. Experten zeigen, wie man Datendiebstahl erkennt und verhindert und gelöschte Daten wieder herstellt.

Ein eigentlich einfaches Thema sind aktuelle Datensicherungen. Unternehmer sind dazu verpflichtet, den Zugriff auf alle Daten sicher zu gestalten. Dazu gehört natürlich auch, dass Daten nicht einfach verloren gehen dürfen. Beim Ausfall von Systemen benötigt man eine brandaktuelle Sicherung. So weit die Theorie. In der Praxis sind Sicherungen oft Wochen und Monate alt und es hat noch keiner geprüft, ob die Sicherungsmedien überhaupt Daten enthalten. Eine Erfolgsmeldung des Sicherungsprogramms bedeutet aber noch lange nicht, dass man mit der Sicherung etwas anfangen kann...

**DER AUTOR**

Der Diplom-Wirtschaftsingenieur Georg Schütz ist seit 2003 in Pirmasens als Unternehmensberater selbstständig. Zuvor war er fünf Jahre bei dem Software-Unternehmen SAP sowie fünf Jahre als Organisationsleiter für IT-Wirtschaft bei Globus tätig.

