Liebe NIFIS-Mitglieder,
sehr geehrte Interessenten und Förderer,

in meiner Funktion als NIFIS-Vorstand in den letzten zwei Jahren und als Sicherheitsberater für mittelständische und international tätige Unternehmen in den letzten 17 Jahren bei KPMG in Deutschland, habe ich immer eine Leitthese meinen Kunden gegenüber propagiert: „Unternehmenssicherheit sollte immer aus der Geschäftsstrategie und Business-Prozessperspektive getrieben werden."

Aber in der Praxis habe ich nur selten Unternehmen gesehen, die diese Leitthese transparent und effektiv umgesetzt haben. Oft können wichtige Grundsatzfragen nicht ohne weiteres beantwortet werden: Wie viele Systeme sind im Unternehmen im Einsatz? Welche davon gelten als unternehmenskritisch? Wer ist eigentlich für die Sicherheit zuständig, und wie häufig treten Sicherheitsvorfälle auf? Selbst welche Personen genau auf unternehmenskritische Daten zugreifen können, wissen viele nicht auf Anhieb.

Das Ziel von NIFIS ist es, Unternehmen Hilfestellung bei solchen Themen zu geben. Konkret können sich Unternehmen an diversen herstellerunabhängigen Kompetenzzentren beteiligen und so einen effektiven Austausch mit Experten pflegen. Mehr dazu und weitere interessante Neuigkeiten erfahren Sie in der aktuellen Ausgabe von NIFIS advice.

Viel Spaß beim Lesen wünscht Ihnen

Brad Chapman

Vorstand der NIFIS

HIGHLIGHTS

NIFIS inside

Effektives Risikomanagement

Weltweite Wirtschaftsbeziehungen sind ohne das Internet nicht mehr denkbar – umso interessanter werden die Nervenbahnen der Wirtschaft leider auch für Hacker, Industriespione und Terroristen. Ziel zerstörerischer und hinterhältiger Angriffe sind nicht nur Regierungen oder Großunternehmen, sondern auch viele kleine und mittlere Betriebe.

„Wer sich als Führungskraft nicht für die Sicherheit digitaler Unternehmenswerte interessiert und engagiert, handelt grob fahrlässig", betont deshalb NIFIS-Vorstandsvorsitzender Peter Knapp. Er fordert einen offensiven Umgang mit den Risiken und gezieltes Management zum Schutz vor Angriffen aus dem Datennetz. Wichtig sei für Unternehmen und öffentliche Einrichtungen, endlich zu handeln. Statt Gerede und Scheinaktivität sollten sie in effektives Risikomanagement investieren. ❑

Kurze Umfrage zu BCM

NIFIS führt derzeit eine Blitzumfrage zum Thema Business Continuity Management (BCM) durch. Im Mittelpunkt stehen dabei die Fragen, ob es im Unternehmen/der Institution bereits BCM gibt, wann eine Einführung geplant ist, oder ob es gar nicht zum Einsatz kommen soll. Die Beantwortung dauert weniger als fünf Minuten. Über eine rege Teilnahme würden wir uns freuen! ❑

Computerwoche kostenlos

Dank der Kooperation von NIFIS mit der Computerwoche haben die Mitglieder die Chance, die führende deutschsprachige IT-Wochenzeitung zeitlich uneingeschränkt **kostenlos** zu beziehen!

COMPUTERWOCHE

Hierfür ist lediglich ein Fragebogen auszufüllen, der sieben Fragen zur Einordnung des Unternehmens und den geplanten Investitionen beinhaltet. Das Formular erhalten Sie unter newsletter@nifis.de. ❑

Kooperation: NIFIS und Hessen Agentur

Die HA Hessen Agentur GmbH unterstützt als Kooperationspartner die Arbeit von NIFIS. Sie wurde Anfang 2005 als 100-prozentige Landestochter gegründet und bündelt alle nichtmonetären Aktivitäten der hessischen Wirtschaftsförderung.

Ziel der Hessen Agentur ist es, das Vertrauen der Bürger, Investoren und Touristen in den Standort Hessen zu stärken und die Vorteile des Landes national wie international bekannt zu machen. Hierfür vernetzt sie Kompetenzträger in Gesellschaft, Wissenschaft, Politik und Wirtschaft.

Außerdem informiert sie als Kompetenzzentrum für neue Medien über den Einsatz neuer Informations- und Kommunikationstechnologien und liefert praxisorientierte Konzepte für strukturpolitische Entscheidungen und Entwicklungsvorhaben. Weitere Informationen finden Sie hier. ❑

Einladung zum AK International

Der AK International lädt herzlich zur Sitzung am 27. November nach Offenbach am Main ein. Viele Mitgliedsunternehmen sind nicht nur innerhalb Deutschlands, sondern länderübergreifend tätig und nutzen in verschiedenen Staaten ITK-Dienstleistungen.

Im Rahmen des Geschäftsbetriebs kommt es dabei häufiger zu identischen oder zumindest gleich gelagerten Problemfällen, sei es in technischer oder rechtlicher Hinsicht. Gemeinsam mit dem Deutschen Verband für Post, Informationstechnologie und Telekommunikation e.V. hat NIFIS deshalb einen Arbeitskreis International ins Leben gerufen, in dessen Rahmen sich Interessierte über die Erfahrungen sowohl im ITK-Bereich, als auch im Postbereich austauschen können. ►

Fokussierte Themen sind unter anderem der Datentransfer über Grenzen hinweg (Safe-Harbour-Prinzip), Telefonie über das „ungeschützte“ Internet, Leistungsmerkmale von TK-Anlagen, Aus- und Einfuhrbestimmungen sowie SPAM und SPIT.

Die Teilnahme ist **kostenfrei** möglich. Neue Interessenten sind willkommen und wenden sich bitte vorab an newsletter@nifis.de. ❑

Expertenforum BCM: Gründung und Folgetermin

Am 17. September hat sich unter dem Dach von NIFIS ein Expertenforum zum Thema Business Continuity Management (BCM) konstituiert. Bei dem Treffen in Frankfurt am Main wurden die Erwartungen der Teilnehmer ausgetauscht, um schließlich die Ziele des Expertenforums zu definieren.

BCM ist eine Managementmethode zur Erstellung und Implementierung von Prozessen und Konzepten für die Fortführung des Geschäftsbetriebs unter Krisenbedingungen. Mit ihr wird ein wesentlicher Grundstein für das Überleben von Unternehmen gelegt. Das Expertenforum bietet eine Plattform, um gemeinsam Prozesse und Lösungen für BCM zu erarbeiten und somit einen schnelleren Einstieg in diese Problematik zu gewährleisten. Oberstes Ziel für NIFIS ist, die Informations- und Internet-Sicherheit der Mitglieder zu erhöhen.

In verschiedenen Untergruppen werden nun zunächst grundlegende Themen erarbeitet, beispielsweise die thematische Ausrichtung des Forums geschärft und existierende rechtliche Vorschriften sowie Normen zusammengefasst. Beim nächsten Treffen am 12. Dezember sollen die ersten operativen Fragen im Rahmen BCM behandelt werden.

Interessenten wenden sich bitte an newsletter@nifis.de. ❑

NEUE MITGLIEDER

Schmitz & Teichmann Betriebsberatung GmbH

„Wir sind NIFIS beigetreten, um unseren Beitrag zur Stärkung der Sicherheit der Informationstechnik gerade bei kleinen und mittleren Unternehmen zu leisten. Sicherheit als wirtschaftlicher Umgang mit Risiken ist schon immer ein Teil unternehmerischen Handelns gewesen, und heute ist es dringlich, in diesem positiven Sinne auch die IT einzubeziehen. Unsere Kunden stärken daher ihr Unternehmen mit Sicherheitsbewusstsein und mit sicheren IT-Strukturen."

Thomas Teichmann, Geschäftsführer Schmitz & Teichmann Betriebsberatung GmbH

impuls IT Beratungsgesellschaft mbH

„Als hersteller- und produktneutrales Beratungsunternehmen unterstützen wir unsere Kunden speziell in der Effizienzsteigerung und Qualitätssicherung im IT-Betrieb. Die Sicherheit steht dabei, insbesondere im Umfeld des Identity Management und der ganzheitlichen Provisioning-Verfahren, im Vordergrund. NIFIS bildet dabei für uns eine Plattform des gegenseitigen Erfahrungsaustausches abseits der täglichen Projekte.“

Marc A. Dierichsweiler, Geschäftsführer Impuls IT Beratungsgesellschaft mbH

NIFIS ist prinzipiell für alle Unternehmen und Personen offen, die sich für das Thema Informations- und Internet-Sicherheit interessieren und versteht sich als Ansprechpartner bei Fragen oder Problemen der Mitglieder. Weitere Infos finden Sie hier.

NIFIS-Siegel für]init[

Die]init[AG hat erneut den umfassenden Sicherheitscheck bestanden und darf nun für weitere zwölf Monate das NIFIS-Siegel führen. Damit kann die Agentur für digitale Kommunikation ihren hohen Sicherheitsstandard gegenüber Kunden, Mitarbeitern und Geschäftspartnern belegen. Die Erteilung des speziell für die mittelständische Wirtschaft entwickelten Siegels erfolgt auf Basis einer umfangreichen Selbstanalyse, bei der 82 Fragen aus den Bereichen organisatorische, logische, technische sowie physikalische Sicherheit beantwortet und vom NIFIS-Siegelrat analysiert werden.

Für NIFIS-Mitglieder ist der Erwerb des Siegels ebenso wie die Rezertifizierung **kostenfrei** möglich. Für Nicht-Mitglieder kostet die Bewertung 150 Euro. Weitere Informationen erhalten Sie hier. ❑

GenericIAM weiter auf Kurs

Am 12. Oktober traf sich das NIFIS-Expertenforum Identity Management in Frankfurt am Main. Im Mittelpunkt standen Fragen, Probleme und konkrete Lösungen im Zusammenhang mit der ganzheitlichen Verwaltung digitaler Identitäten. Dabei wurde ausführlich der aktuelle Stand der verschiedenen Arbeitsgruppen „Organisation“, „Presentation“, „Modelling“ und „Validation“ vorgestellt und die nächsten Schritte diskutiert. In einem interessanten Vortrag erläuterte zudem Henning Guder von der Service for Business IT Ruhr GmbH, warum aus seiner Sicht Identity Management mehr als „nur" Compliance ist.

Ziel des Expertenforums ist es, unter dem Titel GenericIAM einen Baukasten typischer, in den Unternehmen immer wieder auftauchender, „generischer“ Prozesse ► für das Identity und Access Management zusammen zu stellen. Mit diesem Referenzmodell soll es künftig den Unternehmen möglich sein, IAM-Projekte mit deutlich reduziertem Aufwand zum Erfolg zu führen.

Das nächste Treffen ist für den 8. Februar 2008 in Frankfurt geplant. Die Teilnahme ist **kostenlos** möglich. Neue Interessenten sind willkommen und wenden sich bitte vorab an newsletter@nifis.de. ❑

Einladung zum Expertenforum Datenschutz

Am 28. November konstituiert sich in Offenbach unter dem Dach von NIFIS und DVPT ein Expertenforum, das sich mit dem Themenkomplex Datenschutz beschäftigen wird. Ziel ist es, gemeinsam Prozesse und Lösungen für den Datenschutz zu erarbeiten und Erfahrungen im Umgang mit datenschutzrechtlichen Problemen auszutauschen. NIFIS-Vorstand Dr. Thomas Lapp, zuständig für Rechtsfragen und einer der Initiatoren des Forums, wird die Leitung übernehmen.

Alle Interessierten sind herzlich eingeladen, sich **kostenfrei** und auf neutraler Ebene mit anderen Entscheidern aus der Wirtschaft zu diesen Themen auszutauschen. Die Anmeldung ist noch bis zum 21. November möglich. ❑

IMMER UP DO DATE

Um Sie effizient zu schützen, bietet NIFIS auf ihrer Website tagesaktuelle Warnhinweise zu Bedrohungen im Internet. Alle aufgeführten Meldungen sind CERT-geprüft (Computer Emergency Response Team) und haben ein hohes Schadens- und Risikopotenzial. Links zu weiterführenden Informationen unterstützen Sie beim schnellen Beseitigen der Sicherheitsbedrohung.

Veranstaltungstipps

6. IT-Sicherheitstag NRW

Leitlinien und Faktoren für ein erfolgreiches IT-Sicherheits-Management stehen im Fokus des 6. IT-Sicherheitstags Nordrhein-Westfalen am 21. November in Köln. Unter anderem wird Angelika Stiehl von Controlware Details zur IT-Sicherheit in Speicherumgebungen erläutern. Horst Brandenburg (Honda Motor Europe) betrachtet in seinem Vortrag die Sicherheit pragmatisch: von der Strategie zur Umsetzung.

Näheres zur Versicherbarkeit von IT-Risiken erklärt Klaus Eusterholz von der Gerling Allgemeine Versicherungs AG. Prof. Dr. Andreas Pinkwart, Innovationsminister des Landes NRW, wird zudem die Gewinner des „IT-Sicherheitspreises NRW 2007" bekannt geben. Eine Begleitausstellung sowie Workshops zur Vertiefung der Konferenzthemen runden das Informationsangebot des ganztägigen Fachkongresses ab.

Die Teilnahmegebühr beträgt 150 Euro zzgl. MwSt.. ❑

Sicheres Unternehmensnetzwerk

Viele Unternehmen planen eine stärkere Absicherung zentraler IT-Ressourcen, um künftig nur noch berechtigten Mitarbeitern und „sauberen“ Endgeräten den Zugriff auf ihr Netzwerk zu erlauben. Controlware stellt in einer Roadshow praxiserprobte Strategien vor, vergleicht aktuelle Lösungen der marktführenden Hersteller und beleuchtet die Aufwände und Herausforderungen im Betrieb. Die Teilnehmer erhalten Grundlagen zur effizienten Verbesserung ihrer IT-Umgebung und signifikanten Erhöhung der internen Sicherheit. Die Roadshow macht im November in sechs deutschen Städten halt, die Teilnahme ist **kostenfrei** möglich. ❑

Service

Expertenfrageecke

Wie funktioniert E-Mail-Verschlüsselung, und warum sollte ich diese einsetzen?

An dieser Stelle beantworten regelmäßig Experten Fragen, die NIFIS häufig erreichen. In dieser Ausgabe steht Mathias Gärtner NIFIS-Vorstand, selbstständiger und öffentlich bestellter Sachverständiger für IT, zur Verfügung. Sollten auch Sie eine Frage haben, senden Sie diese einfach an newsletter@nifis.de.


Mathias Gärtner, NIFIS-Vorstand

Elektronische Post ist heute ein nahezu unverzichtbarer Bestandteil der modernen Geschäftskommunikation. Täglich werden darüber Nachrichten unterschiedlichsten Inhalts ausgetauscht; vom einfachen „Hallo“ bis hin zum Vertragsentwurf oder Personaldaten. Kaum jemand macht sich Gedanken darüber, wie diese E-Mails transportiert werden, und wer sie alles mitlesen kann.

E-Mails sind Postkarten, nicht mehr oder weniger: Jeder kann sie (mit)lesen!

Ein Weg, das mögliche Mitlesen zu verhindern, ist das Verschlüsseln des Textes der E-Mail. Der einfachste Weg der Verschlüsselung ist das Nutzen eines Verschlüsselungsprogramms wie zum Beispiel PGP mit einem so genannten Pre-shared Key. Der Empfänger bekommt hierbei vor dem E-Mail-Austausch über einen anderen Weg den Schlüssel mitgeteilt, mit dem er die E-Mail entschlüsseln kann. Der Nachteil dieser Methode liegt darin, dass man ständig neue Schlüssel austauschen sollte, um eine kryptografische Analyse zu verhindern und dass das Austauschen des Schlüssels einen hohen logistischen Aufwand bedeutet.

Besser geeignet sind so genannte asymmetrische Verschlüsselungsverfahren. Hierbei existiert für jede Person ein Schlüsselpaar. Dieses besteht aus einem Public Key und einem Private Key. Der Public Key wird nun generell an jeden möglichen Absender verteilt oder sogar frei veröffentlicht. Der Private Key bleibt, wie der Name schon sagt, geheim; nur der Eigentümer sollte ihn kennen.

Wird nun an einen Empfänger eine E-Mail verschickt, wird sie mit dem Public Key verschlüsselt. Der Algorithmus ist so aufgebaut, dass ein mit dem Public Key verschlüsselter Text nur mit dem dazu gehörigen Private Key entschlüsselt werden kann. Muss der Schlüssel gewechselt werden, so reicht es, den neuen Public Key bekannt zu geben.

Heutige E-Mail-Programme, wie zum Beispiel Outlook oder Thunderbird, sind in der Lage solche Schlüssel bequem und automatisch zu verwalten. Nach dem Importieren eines vorher mit Hilfe anderer Systeme erstellten (oder gekauften) Schlüsselpaares muss nur noch spezifiziert werden, dass man verschlüsseln möchte.


Bild © Thommy Weiss / PIXELIO

Eine Einschränkung gibt es allerdings: Um eine verschlüsselte E-Mail zu einem Empfänger zu schicken, muss der Public Key dieses Empfängers bekannt sein. Hat er keinen Schlüssel verteilt, so muss weiterhin unverschlüsselt gesendet werden. ❑

Praxistipp

Sicherer Einsatz von Voice over IP

Thilo Rößler, Technical Consultant bei Claranet, erläutert, wie mittelständische Unternehmen VoIP implementieren sollten, um die Vorteile der IP-Telefonie bei gleichzeitig maximaler Sicherheit zu nutzen.


Thilo Rößler,
Technical Consultant

Für die Einführung von VoIP im Unternehmen werden oft günstige oder gar kostenfreie Telefongespräche als ausschlaggebendes Argument genannt. Doch entscheidender sind die hohe Verfügbarkeit und Sicherheit. So ist die Verschlüsselung von Sprachdaten bei klassischer Telefonie in der Regel unmöglich, mit etwas technischem Aufwand können Daten abgefangen und Gespräche mitgehört werden. Im VoIP-Bereich besteht die Möglichkeit, Telefonate zu verschlüsseln. Hierzu können die Protokolle SIPS/SRTP verwendet werden, die nicht nur unerwünschtes Mithören verhindern, sondern auch die aus dem Privatkundenumfeld bekannten und oft thematisierten Sicherheitslücken wie das „Kidnapping“ von Verbindungen oder die illegale Nutzung von VoIP-Accounts schließen.

Für Mittelständler, die ihre Außenstellen, Heimarbeitsplätze und mobilen Mitarbeiter einbinden wollen, empfiehlt sich der Einsatz eines virtuellen Firmennetzes (Virtual Private Network/VPN), denn hier werden die genannten Risiken durch den abgesicherten Informationsfluss bereits vorab unterbunden. Ebenfalls auf der sicheren Seite sind Unternehmen, die eine virtuelle TK-Anlage (Hosted PBX/IP Centrex) einsetzen. Die Teilnehmervermittlungsanlage steht dabei physikalisch im Rechenzentrum des Internet Service Providers und ist direkt mit dem IP-Netzwerk verbunden. Die Infrastrukturen in den Rechenzentren sind auf Hochverfügbarkeit und Sicherheit ausgelegt, entsprechend zuverlässig kann die ausgelagerte Telefonzentrale betrieben werden. Eine separate Telefonanlage vor Ort ist nicht mehr notwendig, Administration und Management erfolgen standortübergreifend via Web-Oberfläche.

Im Gegensatz zu VoIP-Angeboten für Privatkunden bietet der Markt für den geschäftlichen Einsatz umfangreiche VoIP-Lösungen mit Leistungsmerkmalen klassischer Telefonie wie beispielsweise Weiterleitung und Rufnummernportierung. Trotzdem ist VoIP (noch) nicht für alle Unternehmen die optimale Lösung, vor allem bei ISDN-gestützten Spezialanwendungen. Für alle anderen bietet VoIP aber erhebliche Einsparpotenziale, beispielsweise durch den Wegfall klassischer Anschlusskosten (S0/S2M).

Grundvoraussetzungen für die Nutzung der VoIP-Technologie sind:

- eine leistungsfähige Breitband-Internet-Anbindung (empfehlenswert ist eine SDSL-Leitung mit Flatrate-Tarif)
- ein lokales Datennetz mit Priorisierungsmechanismus (Quality of Service) für eine gewohnt hohe Sprachqualität

Wissenschaftler stehen NIFIS Rede und Antwort

Das 3. ReH..Mo-Symposium Ihrer Forschungsstelle behandelt Web 2.0 als „Geschäftsmodell für die öffentliche Hand“. Sollten Staat und Verwaltung angesichts der bekannten IT-Sicherheits-Risiken im „Mitmach-Web“ nicht zurückhaltender agieren?

Prof. Dr. Heckmann: Die Risiken des User Generated Content (Datenschutz, Urheberrecht, Ehrenschutz etc.) gelten natürlich für alle Web-2.0-Applikationen, unabhängig davon, ob sie von privater oder öffentlicher Seite angeboten werden. Die Maßstäbe der strengen Forenhaftung, die der Bundesgerichtshof in jüngster Zeit entwickelt hat, wären so etwa auf ein interaktives virtuelles Rathaus zu übertragen.

Dennoch sehe ich mehr Chancen als Risiken für den Staat, Web 2.0 auch als Motor der Verwaltungsmodernisierung einzusetzen. Zum einen fördert dies Transparenz und Partizipation, zum anderen kann der Bürger dort „abgeholt“ werden, wo er sich zurzeit überwiegend aufhält. Aus diesem Grund ist auch der Podcast der Bundeskanzlerin erfolgreich, gibt es ein explizites E-Government-Wiki, und setzen sowohl die Bundesregierung als auch Länder und Kommunen auf neue Interaktionsformen, die den Bürger nicht mehr als „Störenfried“, sondern als Ressource ansehen.


Prof. Dr. Dirk Heckmann ist Inhaber des Lehrstuhls für Öffentliches Recht, Sicherheits- und Internetrecht an der Universität Passau, wo er den bundesweit einzigartigen Studienschwerpunkt zum „IuK-Recht in der Verwaltung“ initiiert hat. Gemeinsam mit dem international renommierten Informatiker Hermann de Meer leitet er dort auch das interdisziplinäre Institut für IT-Sicherheit und Sicherheitsrecht.

NIFIS legt großen Wert auf Wissenstransfer und Erfahrungsaustausch zwischen Wirtschaft, Politik und Wissenschaft. Die Universitätsprofessoren Prof. Dr. Klaus Merle (Mainz), Prof. Dr. Maximilian Herberger (Saarbrücken) und Prof. Dr. Dirk Heckmann (Passau) beraten NIFIS in Fragen rund um die Informations- und Internet-Sicherheit. NIFIS holt an dieser Stelle von den Experten regelmäßig Lösungsvorschläge zu aktuellen Herausforderungen und Antworten auf brisante Fragen ein. ❑

Sicherheitsupdate

Provider fürchten steigende Durchschlagskraft von Cyberattacken

Mit Datendurchsatzraten von bis zu 24 Gigabit pro Sekunde erreichen bösartige Angriffe auf Netzwerke und Server neue Rekorde. Auch wenn die Abwehrmechanismen der meisten Provider die schlimmsten Angriffe bereits im Keim ersticken, kann nachhaltiger Schaden an der IT-Infrastruktur entstehen.

Das geht aus dem Worldwide Infrastructure Security Report von Arbor Networks hervor. Das Unternehmen befragte weltweit rund 70 Netzbetreiber zu ihren Erfahrungen mit Cyberattacken zwischen Juli 2006 und Juni 2007. Viele Provider fürchten demnach um ihre Backbone-Infrastruktur, weil viele der eingesetzten Server bislang nur Bandbreiten bis maximal zehn Gigabit pro Sekunde unterstützen. Immer mehr Attacken fänden aber mit weitaus höheren Durchsätzen statt. Bei Geschwindigkeiten von über 20 Gigabit pro Sekunde könnten die Backbones das aufkommende Datenvolumen kaum noch vollständig abwehren und nähmen vermehrt Schaden.

Die Netzbetreiber sehen den Grund in der zunehmenden Durchschlagskraft der Angriffe vor allem in den Botnetzen, die aus Tausenden von gekaperten Rechnern bestehen. Das allein reiche bereits aus, um ein mittleres Rechenzentrum in die Knie zu zwingen. Arbor Networks berichtet, dass viele Netzbetreiber mit einem Mehrangebot von Managed Security Services auf die Bedrohungslage reagieren. Damit sollen in erster Linie die Netzwerke von Unternehmenskunden besser geschützt werden. Um die Kosten im Rahmen zu halten, komme bei der Früherkennung von Bedrohungen verstärkt Open-Source-Software zum Einsatz.

Simon Hülsbömer, Redaktion COMPUTERWOCHE

Weitere interessante Sicherheits-Nachrichten des NIFIS-Kooperationspartners Computerwoche finden Sie hier. ❑

IMPRESSUM

Herausgeber
NIFIS e.V.
Weismüllerstraße 21
60314 Frankfurt
Tel.: 0 69 / 40 80 93 70
Fax: 0 69 / 40 14 71 59
E-Mail: newsletter@nifis.de
Internet: http://www.nifis.de
Peter Knapp (V.i.S.d.P.)

Redaktion
FRESH INFO +++
Nicole Chemnitz (CvD)
http://www.fresh-info.de