

Liebe NIFIS-Mitglieder,
sehr geehrte Interessenten und Förderer,



es freut mich, Ihnen mitteilen zu können, dass sich unser Verein fortlaufend positiv weiterentwickelt. Ein Beweis hierfür ist, dass sich NIFIS kontinuierlich mit aktuellen Themen befasst, die meines Erachtens nach einen hohen Wertbeitrag für alle Mitglieder und Interessenten liefern. Unter anderem konnte NIFIS die Gründung des neuen Kompetenzzentrums für „Identity Management“ im Dezember 2006 abschließen. Weiterhin hat NIFIS im April 2007 die Gründung neuer Kompetenzzentren für „Business Continuity Management“ (BCM) und Datenschutz beschlossen.

Diese Kompetenzzentren befassen sich mit Fragen, Problemen und konkreten Lösungen im Zusammenhang mit der ganzheitlich risikoorientierten Governance, dem Management und der Sicherheit von geschäftskritischen Daten in deutschen Unternehmen sowie dem Erfüllen von gesetzlichen Auflagen im Allgemeinen.

Die Mitwirkung in diesen Kompetenzzentren öffnet NIFIS-Mitgliedern den Zugang zu Experten, die über langjährige und praxiserprobte Erfahrung in den jeweiligen Fachgebieten sowie über vordefinierte Lösungsansätze verfügen. Aus meiner Sicht liegt genau hier der Mehrwert, den NIFIS liefert. Wenn ein Unternehmen durch solche Experten derartige Problemstellungen in Zusammenhang mit einem Auftragsverhältnis bearbeiten lässt, muss üblicherweise ein Vielfaches der NIFIS-Mitgliedsgebühr für Beratungshonorare und/oder Konferenzgebühren bezahlt werden.

Alle NIFIS-Mitglieder und -Interessenten sind herzlich eingeladen, sich in diesen Expertenforen zu engagieren! 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	
Erstes NIFIS-Forum voller Erfolg	Seite 2
Wir über uns	
Mitgliederinterview Interxion	Seite 4
Wir für Sie	
Internet-Experten aus der Wissenschaft unterstützen NIFIS	Seite 6
Sicherheitsupdate	
Europas IT-Profis fürchten Datenlecks mehr als Viren und Hacker	Seite 7

Neuer Name, bewährte Strategie

Auf der Mitgliederversammlung am 22. Mai in Frankfurt am Main hat NIFIS eine Erweiterung ihres Namens beschlossen: Aus der Nationalen Initiative für Internet-Sicherheit wird ab sofort die Nationale Initiative für Informations- und Internet-Sicherheit.

Das Kürzel NIFIS bleibt weiterhin bestehen. Ebenso wie der Fokus der neutralen und unabhängigen Organisation, konkrete Maßnahmen für den Anwender umzusetzen. Die sprachlich nur marginale Änderung der Firmierung hat inhaltlich durchaus eine besondere Bedeutung. ►

„Die Sicherheit geschäftskritischer Daten wird in deutschen Unternehmen nach wie vor zu sehr zu einem reinen IT-Thema degradiert. Es steckt jedoch wesentlich mehr dahinter, schließlich geht es nicht nur um technische Fragen, sondern in erster Linie auch um organisatorische und rechtliche Aspekte,“ bekräftigt der Vorstandsvorsitzende Peter Knapp.

Die Vertraulichkeit, Integrität und Verfügbarkeit jeder einzelnen Information ist im digitalen Zeitalter die Basis für das Überleben und nachhaltiges Wachstum des Geschäfts. Deshalb handele es sich mithin nicht um ein IT-, sondern um ein Business-Thema, das in der Führungsetage behandelt werden sollte. NIFIS wolle daher ►



ganz im Sinne ihrer beratenden und aufklärenden Tätigkeit schon im Namen ein Zeichen setzen. Die Strategie, die sich in den letzten beiden Jahren bewährt hat und die Initiative von vermeintlich vergleichbaren Organisationen abgrenzt, wird fortgesetzt. Dabei legt NIFIS viel Wert auf eine enge Verzahnung zwischen Wirtschaft und Wissenschaft. Kontinuität in der Fortführung der umfangreichen Aufklärungs- und Beratungstätigkeit ist auch deshalb zu erwarten, da im Vorstand mit Peter Knapp (Geschäftsführer Interxion), Dr. Thomas Lapp (Rechtsanwalt und Mediator) und Brad Chapman (Partner bei KPMG) künftig dieselben Personen agieren wie bisher.

Neu hinzugekommen ist Mathias Gärtner, dessen Tätigkeitsschwerpunkte als selbstständiger und öffentlich bestellter Sachverständiger für IT neben forensischen Arbeiten und allgemeinen Gutachten bei Planungs- und Beratungsaufgaben im Zusammenhang mit Computernetzwerken und IT-Sicherheit liegen.

Mehr zur Entwicklung und Strategie von NIFIS verraten Peter Knapp und Volker Ludwig im Interview in diesem Newsletter. 

Erstes NIFIS-Forum voller Erfolg

Das erste NIFIS-Forum für angewandte Informations-Sicherheit fand Ende Mai in Frankfurt am Main statt. Im Mittelpunkt standen konkrete und vor allem praktisch umsetzbare Maßnahmen für die IT- und Informations-Sicherheit in mittelständischen und größeren Unternehmen. Mehr als sechzig Fach- und Führungskräfte nutzten die Chance, sich in den Fachvorträgen der hochkarätigen Referenten umfassend zu informieren, welche Trends, Risiken und Kernaspekte die Sicherheit aktuell und künftig bestimmen.

Den ersten Vortrag hielt Dr. Thorsten Henkel, Bereichsleiter Sichere Prozesse und Infrastrukturen beim Fraunhofer-Institut für Sichere Informationstechnologie (SIT). 

Er erläuterte den Paradigmenwechsel in der IT und die sich daraus ergebenden – zum Teil sehr neuartigen – Probleme und Risiken im Bereich der Informations-Sicherheit. Zukünftige IT-Netze seien in noch höherem Maße mobil, dynamisch, vernetzt und serviceorientiert und böten dadurch zusätzliche Lücken, die geschlossen werden müssten.

„Die Betrachtungsweise muss sich ändern, denn Sicherheit ist kein rein technisches Thema, das sich nur auf einzelne Bereiche bezieht. Es muss vielmehr Nutzer und Prozesse in den Mittelpunkt stellen, um nur ein Beispiel für den notwendigen Paradigmenwechsel zu nennen“, betonte Dr. Henkel.



Dr. Karsten Weronek, Head of Corporate Information Management bei der Fraport AG, berichtete in seinem Vortrag über die Enterprise Architektur als Lösungsansatz für Informations-Sicherheit.

Die Teilnehmer konnten sich aufgrund der geschilderten Erfahrungen ein umfassendes Bild davon machen, wie die Fraport AG mit ihrer sehr komplexen und weit verzweigten IT-Infrastruktur, die Vertraulichkeit, Verfügbarkeit und Integrität ihrer Daten sicherstellt. Außerdem erläuterte Dr. Weronek, welche Herausforderungen es dabei zu meistern gilt und wie Sicherheitslücken über die Betrachtung der Gesamtarchitektur und von End-to-End-Ketten geschlossen werden.

Viel diskutiert wird in der Branche derzeit über die ganzheitliche Behandlung digitaler Identitäten, in Fachkreisen besser unter dem Namen Identity Management bekannt. Dr. Horst Walther, Leiter des Expertenforums Identity Management bei NIFIS, erläuterte 

ausführlich die verschiedenen Aspekte des Themas. „Die Komponenten und Einzelaufgaben des Identity Managements sind nicht neu. Neu ist der Wandel in der Betrachtungsweise, die sich von der Ansehung dieser Disziplin als isolierte technische Lösung entfernt und hinbewegt zu einem ganzheitlichen Ansatz. Identity Management folgt aus übergreifenden Anforderungen, benötigt eine einheitliche technische Architektur und sollte in jedem Unternehmen unter einer einheitlichen und zentralen Verantwortung stehen“, so Dr. Walther.

Im abschließenden Vortrag zeigte Wolfgang Geßling, Abteilungsleiter RZ-Produktion bei der sds business services GmbH, am Beispiel des eigenen Unternehmens auf, wie eine interne Zertifizierung des Rechenzentrums nach dem ISO Standard 27001 durchgeführt wurde. In einem sehr straff organisierten Projekt wurden die Unternehmensprozesse klassifiziert und ISO-konform gestaltet. Darüber hinaus mussten strikte Richtlinien etabliert werden, die beispielsweise die Nutzung von E-Mails, Internet oder WLAN am Arbeitsplatz regeln.



„Die Resonanz zeigt uns, dass wir mit unserem Konzept, den Anwender mit seinen praktischen Erfahrungen in den Mittelpunkt zu stellen und stets die Umsetzbarkeit von Maßnahmen in der Unternehmenspraxis im Blick zu haben, richtig liegen“, resümierte NIFIS-Vorstand Peter Knapp.

Die Präsentationen werden bei Interesse gerne zugeschickt, schreiben Sie hierfür einfach eine E-Mail an newsletter@nifis.de. 

Neue Foren freuen sich auf Mitarbeit

NIFIS möchte künftig noch mehr Raum für intensiven Austausch und tief greifende inhaltliche Arbeit bieten. Hierfür ist unter anderem zeitnah die Gründung eines Expertenforums für „Business Continuity Management“ (BCM) geplant. Die Leitung übernimmt Rolf von Rössing, KPMG Partner. Inhaltlich soll vor allem besprochen werden, welche Risiken es in Unternehmen gibt und wie diese bewertet und abgesichert werden, damit im Ernstfall eine Weiterarbeit möglich ist. Außerdem ruft NIFIS in Kürze noch ein weiteres Expertenforum ins Leben, das sich ausführlich mit dem Thema Datenschutz beschäftigt. Interessierte Unternehmen, die in den Foren mitarbeiten möchten, wenden sich bitte an newsletter@nifis.de. □

NEUE MITGLIEDER



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](#).

Bericht: 1st European Identity Conference

Vom 7. bis 10. Mai wurden in München bei der 1st European Identity Conference die Kernthemen des Identity & Access Managements (IAM) heiß diskutiert. Mehr als 100 internationale Experten referierten über Compliance & Identity Risk Management, Authentication Trends & SSO, Identity Federation & User-Centric Identity Management, Roles & Provisioning sowie SOA & Identity as a Service. ►

„Die Konferenz war vor allem aufgrund des dicht gepackten Programms und der hochkarätigen Redner ein überwältigender Erfolg. Davon sind alle überrascht worden. Die hervorragende Resonanz zeigt die Bedeutung des Themas als wichtige unternehmensorganisatorische Aufgabe“, erläutert Dr. Horst Walther vom Konferenz-



veranstalter Kuppinger, Cole und Partner und Leiter des NIFIS-Expertenforums Identity Management. Zwei Stunden erläuterte er in einem Pre Conference Meeting die Notwendigkeit von definierten Prozessen beim IAM.

Das Expertenzentrum erarbeitet derzeit unter dem Titel GenericIAM einen Baukasten typischer, in den Unternehmen immer wieder auftauchender, „generischer“ Prozesse für IAM. Mit diesem Referenzmodell soll es künftig den Unternehmen möglich sein, IAM-Projekte mit deutlich reduziertem Aufwand zum Erfolg zu führen.

Etwa 30 interessierte Teilnehmer nutzten den zweistündigen Vortrag, um sich ausführlich über das Thema zu informieren. Viele folgten der Einladung, die angeregten Diskussionen am NIFIS-Stand zu vertiefen oder gar aktiv die Arbeit des Forums inhaltlich zu unterstützen. Ende Juni trifft sich das NIFIS-Expertenforum in einer wichtigen dreitägigen Klausurtagung, um weitere Details des ersten Modells GenericIAM 2007 zu erarbeiten, das noch in diesem Jahr veröffentlicht werden soll. □

IFRS 7: Finanzrisiken managen

Mit der Veröffentlichung der IFRS 7 und der Verpflichtung, diese verbindlich ab dem 1. Januar 2007 anzuwenden, sind erhöhte Anforderungen, insbesondere ►

an die externe Risikoberichterstattung, verbunden. KPMG zeigt in einem Seminar, welche Neuerungen in der Offenlegung für Industrie- und Handelsunternehmen bestehen und zeigt anhand von Beispielen für Anhangauszüge Umsetzungsmöglichkeiten auf. Die Veranstaltung findet am 19. Juli in Frankfurt statt, die Teilnahmegebühr beträgt 150 Euro. □

Wireless & Mobile Security in Köln

Vom 17. bis zum 19. September findet in Kooperation mit NIFIS die Wireless & Mobile Security 2007 in Köln statt. Die Teilnehmer erfahren in interessanten Vorträgen, wie Gefahren beim Einsatz drahtloser Netze und mobiler Endgeräte vermieden werden können.



Marcel Knop von NIFIS wird am ersten Forumtag über „LAN-basierte WLAN-Untersuchungen/War-Driving Orten und Verhindern unerlaubter Funkverbindungen“ referieren. Am 19. September können die gehörten Vorträge in Intensivworkshops vertieft werden. □

Applikations-Performance messen

Geschäftskritische, webbasierte Anwendungen, die von Mitarbeitern, externen Kunden oder Geschäftspartnern genutzt werden, informieren selten unmittelbar darüber, wenn ein Anwender unzufrieden ist und einen Geschäftsprozess nicht ausführen kann.

Wenn sich Anrufe im Helpdesk häufen und eventuell auftretende Performance-Probleme via Eskalationsstufen „gelöst“ werden, könnten bereits Kunden vergrault und rentable Geschäfte entgangen sein. Compuware zeigt in halbtägigen kostenlosen Seminaren, wie Service Level Agreements eingerichtet und eingehalten sowie Performance-Probleme schnell erkannt werden können. ►

Die Workshops „Applikations-Performance aus Anwenderperspektive messen“ finden ab Juli in mehreren deutschen Städten statt. □

VO.IP Germany

Voice- und IP-Kommunikation steht am 30. und 31. Oktober im Mittelpunkt der VO.IP Germany in Frankfurt am Main. Deutschlands größte Kongressmesse für diesen Themenbereich bietet durch praktische Vorführungen und Vorträge namhafter Vertreter vornehmlich aus der Wirtschaft, aber auch ▶

aus Politik, Regulierung und Verbänden, einen umfassenden Überblick über den Entwicklungsstand, die Zusammenhänge und Auswirkungen des Zusammenwachsens von Sprache und Daten, Netzen und Systemen in Unternehmen. ▶



NIFIS-Vorstand Peter Knapp gibt in einem Vortrag Ausblick auf die Sicherheit im Jahr 2008.

Zudem nimmt er an der Podiumsdiskussion zum Thema „Zukunft der Kommunikation – (Wie) Sichern die Verbände die Wettbewerbsfähigkeit des Kommunikationssektors?“ teil.

Einen Höhepunkt bildet die Verleihung der VO.IP Germany Awards in den Kategorien Systeme, Dienste/ASP, Applikationen und Mobility zum Veranstaltungsabschluss. □

Wir über uns

Mitgliederinterview Interxion

Als Initiator von NIFIS gibt Interxion Einblick in die Entstehung, Kernkompetenzen und weiteren Pläne der Initiative.



Interxion ist Europas führender Anbieter von Carrier-neutralen Rechenzentren und Managed Services. Das Unternehmen unterstützt mehr als 1.000 Firmenkunden aus nahezu allen Wirtschaftszweigen mit einer umfangreichen Palette an Internetinfrastruktur-Dienstleistungen.

Interxion betreibt mit etwa 200 Mitarbeitern 22 Rechenzentren in elf Ländern und bietet Zugang zu 15 der wichtigsten europäischen Internetaustauschknoten sowie zu den Netzen von insgesamt 460 Netzbetreibern. In Deutschland betreibt Interxion fünf operative Rechenzentren an den Standorten Frankfurt und Düsseldorf.

Carrier-neutraler Rechenzentrumsbetreiber – was bedeutet das denn?

Knapp: Man kann unsere Funktion gut mit der eines Flughafens vergleichen. Flughäfen sind nichts anderes als Infrastrukturbetreiber, die dafür sorgen, dass Personen und Pakete transportiert beziehungsweise ausgetauscht werden können. Darüber hinaus werden noch Services angeboten wie Parkhäuser, Boutiquen und Restaurants und dafür bekommt der Flughafen Geld. Wir tun auch so etwas, aber für den IT-Bereich.

Wir sorgen dafür, dass Infrastruktur, Strom und Klimatisierung funktionieren, Internetanbindungen zur Verfügung stehen und die notwendige Sicherheit gewährleistet ist. All unsere Kunden betreiben eigenes IT-Equipment innerhalb unserer Häuser und tauschen untereinander Leistungen aus. Wir sind dabei nur die neutrale Plattform, wie ein Flughafen der das Umsteigen von einer Airline zu einer anderen ermöglicht.



Peter Knapp
Geschäftsführer

Interxion ist der Initiator von NIFIS. Was war der Auslöser für die Gründung?

Knapp: Die Gründe waren vielschichtig. Wir haben schon immer den aktiven Austausch innerhalb der einschlägigen Sicherheitskreise, der Wirtschaft und auch in die Behörden hinein gepflegt. Information ist im Sicherheitsumfeld extrem wichtig.

Sicherheit und Verfügbarkeit sind unser Geschäft. Wir können aber nur einen kleinen Teil der Wertschöpfungskette innerhalb der Internet- und Informationssicherheit darstellen. Interxion ist kompetent im Bereich physische Sicherheit in Rechenzentren, aber das Sicherheitsthema umfasst wesentlich mehr: Hardware, Software, Leitungen, Prozessthemen und organisatorische Themen, die Adressierung des Managements etc.. Weil wir die gesamte Wertschöpfungskette abbilden wollten, suchten wir uns gezielt Unternehmen, die sehr kompetent in ihrem Bereich sind und die Kette optimal ergänzen. Das waren dann unsere handverlesenen Gründungsmitglieder für diesen Verein. ▶

Ludwig: Der Startschuss für NIFIS fiel im Jahr 2004 als wir, verknüpft mit unserem fünfjährigen Firmenjubiläum, zu einer akademischen Feier zum Thema „Fünf Jahre sicheres Internet in Deutschland“ geladen hatten. Nachdem wir als Unternehmen jahrelang einen Beitrag zur Erhöhung der Sicherheit im Datenaustausch auf Providerebene geleistet haben, wollten wir diese Idee weitertragen und zwar zu den Nutzern der digitalen Netze.

Ein von Anfang an wichtiger Aspekt war, die Sicherheit nicht technisch zu betrachten, sondern als Managementaufgabe zu positionieren. In Anwesenheit von verschiedenen prominenten Vertretern aus Politik, Wirtschaft und Wissenschaft, darunter auch der hessische Ministerpräsident Roland Koch, haben wir im Rahmen der Feierlichkeiten die Gründung der NIFIS angekündigt und breite Unterstützung erhalten.

Ende Mai 2005 erfolgte dann die Gründungsversammlung von NIFIS. Was unterscheidet die Initiative von anderen Organisationen?

Knapp: Wir bilden eine neutrale Plattform, die völlig herstellerunabhängig und branchenübergreifend ist. Dabei richten wir uns ausdrücklich an die Nutzer der Informationstechnologie; wir sind kein IT-Verband! Die Mitglieder sollen sich in einer neutralen Umgebung austauschen können, Informationen erhalten, pragmatische Lösungen erarbeiten, die aus der Wirtschaft für die Wirtschaft bereitgestellt werden. Alle arbeiten ehrenamtlich mit, keiner bekommt auch nur einen Euro dafür. Wir sind nicht interessens- oder geldgesteuert. Da sind wir sehr strikt!

NIFIS hat sehr hochkarätig besetzte Beiräte. Wie kam es denn dazu?

Knapp: Unseren Exekutivbeirat haben wir gezielt mit kompetenten Bundestagspolitikern und parteiübergreifend besetzt. Wir brauchen ihn ausdrücklich nicht dazu, um Lobbyismus zu betreiben, sondern wir wollen uns mit ihm austauschen, ob unsere Ideen in die richtige Richtung gehen und Feedback und Anregungen einfließen lassen. Er fungiert als Schnittstelle.

Beim wissenschaftlichen Beirat geht es vom Ansatz her ebenfalls um eine Sparringspartnerfunktion. Wir unterhalten uns über die Methoden, die wir entwickeln möchten und können fachlich-methodische Unterstützung anfordern. Ansonsten pflegen wir einen sehr lockeren Austausch mit dem wissenschaftlichen Beirat, der auch ganz bewusst fachübergreifend besetzt ist mit Spezialisten aus den Bereichen Informatik, Juristerei und Wirtschaft.

Ludwig: Die Beiräte haben sich vor der Übernahme ihrer Aufgabe ausführlich über uns informiert, die Ziele genau geprüft und die Alleinstellungsmerkmale erkannt und verstanden. Die Entscheidung für NIFIS spricht auch für die Qualität unserer Arbeit und ist als ein Gütesiegel zu sehen.

NIFIS bündelt als Kompetenzzentrum das Fachwissen ausgesuchter Gründungsmitglieder. Interxion fokussiert die physische Sicherheit von Rechenzentren. Was machen Sie da genau, und wie unterstützen Sie die Mitglieder?

Knapp: Zum einen pflegen wir regelmäßig Arbeitskreise, in denen der Austausch unter den Mitgliedern gefördert wird. Zum anderen informieren wir über das Thema, beispielsweise auf Veranstaltungen, und präsentieren erarbeitete Lösungen. Von Anfang an hat Interxion auch eine konkrete Dienstleistung in NIFIS eingebracht: Die Mitglieder können innerhalb der Mitgliedschaft in begrenztem Umfang kostenlos Online-Datensicherung beziehen.

Ludwig: Außerdem haben wir einen großen Beitrag zur Entwicklung des NIFIS-Siegels geleistet. Dort haben wir den kompletten Bereich physische Sicherheit eingebracht und auch den Arbeitskreisleiter gestellt. Darüber hinaus unterstützen wir bei Anfragen, der Lösung konkreter Problemfälle und forcieren die Marketing- und Öffentlichkeitsarbeit der Initiative.

Wie schätzen Sie die bisherige Entwicklung von NIFIS ein?

Knapp: Wir haben zurzeit etwa 50 Mitglieder, branchenübergreifend, interessenübergreifend, kleine und große Unternehmen, darunter Fraport, OKI und DEKRA. Ursprünglich sind wir im Rhein-Main-Gebiet gestartet – jetzt haben wir Mitglieder deutschlandweit aus fast allen Bundesländern. Ich persönlich finde es deshalb ziemlich beachtlich, was wir innerhalb von verhältnismäßig kurzer Zeit auf die Beine gestellt haben.

Ludwig: Wir haben an zahlreichen Veranstaltungen teilgenommen, sind wahrnehmbar in der Öffentlichkeit, haben Kontakte in die Politik, die Behörden und auch zur Presse. Das wir in dieser kurzen Zeit als die einzige private, neutrale und nicht herstellergesteuerte Organisation in der Öffentlichkeit wahrgenommen werden, sehe ich als großen Erfolg. Wir haben gemessen an unseren Ressourcen wirklich schon eine Menge erreicht.

Aus welchen Gründen werden die Unternehmen Mitglied?

Knapp: Wir dachten ursprünglich, dass die Leistungen ausschlaggebend sind. Heute stellen wir aber fest, dass der Austausch das Zuggpferd ist, die Teilnahme an Arbeitskreisen, konkretes, themenorientiertes Arbeiten. Wir verfügen über hervorragende Spezialisten, beispielsweise in unserem Expertenforum Identity Management. Dort haben sich kompetente Leute zusammengeschlossen, und das zeigt, wie dieses Konzept funktioniert. ►



Volker Ludwig
Marketing Manager DACH

Welche konkreten Ziele geht NIFIS als Nächstes an?

Ludwig: Wir wollen wesentlich mehr inhaltliche Arbeit leisten, mehr Austausch unter den Mitgliedern betreiben, Stammtische organisieren, Mitgliedern eine Plattform zum Austausch geben und uns weniger auf die Entwicklung von Serviceleistungen konzentrieren.

Knapp: Wir planen die Installation von weiteren Expertenforen. Konkret wird ein Forum zu Business Continuity Management unter Leitung eines hochkarätigen KPMG-Experten gegründet. Da manifestiert sich auch wieder unsere Ausrichtung, organisatorische und Prozessthemen zu betrachten. Wir denken des Weiteren an ein Expertenforum zum Thema Datenschutz. Zudem fand bereits in Kooperation mit dem DVPT die konstituierende Sitzung von unserem Arbeitskreis International statt. Natürlich werden bestehende Arbeitskreise wie der zur Validierung fortgesetzt.

Das erste NIFIS Forum hat sehr erfolgreich stattgefunden. Wird es eine Fortsetzung geben?

Knapp: Definitiv ja! Es war ein Highlight, und wir sind mit dem Verlauf und der Resonanz sehr zufrieden. Es wird eine Herausforderung, die Qualität der Vorträge im nächsten Jahr auf dem gleichen Niveau zu halten. Die Vorträge waren ausschließlich inhaltlich orientiert und sensationell gut. Ich habe schon viele Veranstaltungen besucht, aber das war mit das beste, das ich bislang gesehen habe. Neutral und ohne Kosten für die Teilnehmer.

Wo sehen Sie NIFIS in drei Jahren?

Ludwig: Es gibt Themen, die überholen sich. Das Thema Sicherheit gehört nicht dazu, im Gegenteil: Es wird in Zukunft noch wichtiger werden. Somit werden wir über kontinuierliche Aufklärung, Pressearbeit, Veranstaltungen und all die anderen Aktivitäten immer mehr Unternehmen erreichen und auf diese Weise unsere Mitgliederbasis ausbauen. Das bietet uns wiederum die Möglichkeit, Themen intensiver zu betreuen und zusätzliche Themen zu adressieren.

Knapp: Wir haben Sicherheit von Anfang an nicht als Modeerscheinung gesehen, NIFIS ist langfristig und nachhaltig angelegt. Wir wollen einen Mehrwert liefern und zur Sicherheit beitragen, um Unternehmen bei den größer werdenden Herausforderungen zu unterstützen. Dabei werden wir den eingeschlagenen Weg konsequent weiter verfolgen.

Wir danken für dieses Gespräch! □

Wir für Sie

Internet-Experten aus der Wissenschaft unterstützen NIFIS

NIFIS erhält prominente Unterstützung aus dem Bereich der Wissenschaft. Die Universitätsprofessoren Prof. Dr. Klaus Merle (Mainz), Prof. Dr. Maximilian Herberger (Saarbrücken) und Prof. Dr. Dirk Heckmann (Passau) beraten NIFIS ab sofort in Fragen rund um die Internet-Sicherheit. „Der Beirat stellt sicher, dass die Lösungen von NIFIS stets auf den aktuellen wissenschaftlichen Erkenntnissen basieren und modernste Verfahren berücksichtigen“, sagt NIFIS-Vorstandsvorsitzender Peter Knapp. „Unternehmen werden von der weit reichenden Erfahrung der IT-Experten profitieren. Außerdem ist die stete Fortentwicklung geeigneter Schutzmaßnahmen gegen alle denkbaren Angriffe auf Firmendaten gewährleistet.“

Prof. Dr. Klaus Merle ist seit 1993 Leiter des Zentrums für Datenverarbeitung der Johannes-Gutenberg-Universität in Mainz. Er hat federführend am Aufbau eines eigenen Netzes der Hochschulen von Rheinland-Pfalz auf Basis eines Dark-Fiber-Rings mitgewirkt.

Auf seine Initiative geht auch die kabellose Vernetzung des Universitäts-Campus in Mainz zurück. Die Hauptarbeitsgebiete von Prof. Dr. Merle im Fachbereich Physik, Mathematik und Informatik sind Telekommunikation sowie Hardware und Software für verteilte Systeme.

Prof. Dr. Maximilian Herberger verfügt als Direktor des Instituts für Rechtsinformatik an der Universität des Saarlandes in Saarbrücken über das notwendige Know-how an den Schnittstellen zwischen Recht und Internet.

Arbeitsschwerpunkte sind E-Commerce, Rechtsdatenbanken, juristische Expertensysteme, EDV-Sicherheit, Internet-Recht, juristische Lernprogramme und E-Learning-Konzepte. Er leitet das Juristische Internet-Projekt Saarbrücken und führt zudem den Vorsitz über den Deutschen EDV-Gerichtstag e.V.

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 „luK-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. Ende 2003 wurde er zum nebenamtlichen Richter am Bayerischen Verfassungsgerichtshof gewählt. Er ist zudem Mitglied im Gründungssenat der Deutschen Hochschule der Polizei. □

Praxistipp

In NIFIS advice 01/2007 hat Brad Chapman an dieser Stelle auf die Notwendigkeit von Identity- und Access Management zum Schutz von Informationswerten hingewiesen und praktische Tipps zur Umsetzung gegeben. Mittlerweile hat sich herumgesprochen, dass ein fehlendes internes Kontrollsystem und das Unterlassen von Maßnahmen zum Schutz von Informationswerten zu einer persönlichen Haftung von Managern führen können. Weniger beachtet wird, welche weiteren Folgerungen aus derartigen Fehlern resultieren können. Wenn im Unternehmen keine Vorkehrungen zum Schutz von Informationswerten getroffen werden, ist dies eine Pflichtverletzung. Im Hinblick auf die ausdrückliche Regelung im Gesetz und die regelmäßige Berichterstattung in den Medien ist diese Pflichtverletzung als grob fahrlässig anzusehen.



Dr. Thomas Lapp
NIFIS-Vorstand

Die Einstufung einer Pflichtverletzung als grob fahrlässig hat Konsequenzen in verschiedenen Bereichen des Unternehmens. Viele Unternehmen sind gezwungen, sich gegenüber Kunden zu exakten Lieferterminen zu verpflichten. Die Kunden sind auch nicht mehr bereit, „Computerprobleme“ als Ausrede für Lieferverzögerungen zu akzeptieren. Die Kunden verlassen sich vielmehr auf fristgerechte Lieferung und verlangen bei Verzögerungen Schadensersatz. Klauseln zum Ausschluss der Haftung helfen dann nicht weiter. Rechtlich ist es in Allgemeinen Geschäftsbedingungen nicht zulässig, die Haftung für grob fahrlässige Pflichtverletzungen auszuschließen. Daher wird für Schäden aufgrund grob fahrlässiger Pflichtverletzungen in vollem Umfang gehaftet.

Auch Versicherungsverträge enthalten häufig Klauseln, wonach die Versicherungen nicht für grob fahrlässig verursachte Schäden eintreten. Es besteht dann kein Versicherungsschutz.

Normalerweise haften Arbeitnehmer nicht für die Schäden, die sie bei Ausübung ihrer Tätigkeit ihrem Arbeitgeber oder anderen zufügen. Die Rechtsprechung hat, insbesondere im Straßenverkehr und beim Einsatz teurer Maschinen, die Risiken überwiegend dem Arbeitgeber zugewiesen. Für Schäden, die durch leicht fahrlässige Pflichtverletzung verursacht sind, haften Arbeitnehmer gar nicht. Sind jedoch grob fahrlässige Pflichtverletzungen die Ursache, haften auch Arbeitnehmer für die dadurch verursachten Schäden. Wer also als Arbeitnehmer für die IT und/oder die IT-Sicherheit verantwortlich ist, muss auch Maßnahmen zum Schutz der Informationswerte ergreifen. Soweit ihm kein Budget zur Umsetzung zur Verfügung steht, muss er zumindest auf die Notwendigkeit von Maßnahmen hinweisen.

Gesetzlich verpflichtet sind Unternehmen allerdings nur, überhaupt Maßnahmen zum Schutz der Informationswerte zu ergreifen. Es müssen nicht die neuesten und nicht die teuersten Maßnahmen sein. Man sollte aber nach aktuell anerkannten Standards vorgehen, um den Vorwurf des grob fahrlässigen Fehlverhaltens zu vermeiden. □

Sicherheitsupdate

Europas IT-Profis fürchten Datenlecks mehr als Viren und Hacker

Datendiebstahl steht für europäische Unternehmen ganz oben auf der Gefahrenskala – weit vor Malware und externen Angreifern. Zu diesem Ergebnis kommt ein Bericht der Kaspersky-Tochter Infowatch.

Das Gros der europäischen IT-Profis misst internen Bedrohungen eine größere Bedeutung bei als der Gefahr, die etwa von Hackern, Viren oder Spam ausgeht. Das ergab die Untersuchung „Interne IT-Bedrohungen Europa 2006“ von Infowatch. Dazu hat der auf Data-Leakage-Prevention spezialisierte Lösungsanbieter CIOs sowie IT- und Sicherheitsspezialisten in 410 europäischen Firmen zum Thema „interne Sicherheit“ befragt.

Demnach erachten europäische Unternehmen den Datendiebstahl (78 Prozent) als primäre IT-Bedrohung. An zweiter Stelle auf der Gefahrenskala steht die Fahrlässigkeit der Angestellten (65 Prozent), gefolgt von Gefahren durch Viren (49 Prozent), Hacker (41 Prozent) und Spam (32 Prozent).

Am stärksten sehen die Befragten die interne Datensicherheit durch den Verlust vertraulicher Informationen (93 Prozent) sowie deren Verfälschung (85 Prozent) bedroht. ►

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.

Über tragbare Speichermedien (69 Prozent) wie USB-Sticks und Notebooks, E-Mail (65 Prozent) sowie das Internet beziehungsweise Web-Mail und Foren (58 Prozent) gelangen vertrauliche Daten den Studienteilnehmern zufolge am leichtesten nach außen. Als schlimmste Folge eines Datenverlusts für das eigene Unternehmen nannten die Befragten die Schädigung des Firmen-Images (63 Prozent) sowie die Abwanderung von Kunden (51 Prozent).

Dem Bericht zufolge konnten nur elf Prozent der Befragten mit Sicherheit ausschließen, dass es in ihrer Organisation im vergangenen Jahr zu einem unerwünschten Datenabfluss gekommen ist, während 37 Prozent keinerlei Angaben dazu machen konnten. 42 Prozent der Studienteilnehmer wiederum räumten eine bis fünf undichte Stellen, neun Prozent sogar sechs bis 25 solcher Schwachstellen ein.

In einem scheinen sich Europas IT-Profis weitgehend einig: Um Datenverluste durch Insider zu vermeiden, bedarf es zwar einer technischen Lösung, ohne flankierende organisatorische Maßnahmen und Schulungen verfehlt diese jedoch ihre Wirkung. Laut Infowatch setzen derzeit trotz des erhöhten Gefahrenbewusstseins nur 16 Prozent der Unternehmen ein Anti-Data-Leakage-System ein. Auf die Frage, was sie daran hindert, führten die IT-Verantwortlichen einen Mangel an Standards (42 Prozent), Budgetgrenzen (36 Prozent) sowie nicht genügend ausgebildete Spezialisten (29 Prozent) auf. Mehr als die Hälfte der Studienteilnehmer ist allerdings der Meinung, dass Organisationen innerhalb der EU per Gesetz dazu verpflichtet werden sollten, persönliche Daten vor Insidern zu schützen. Mehr zum Thema Sicherheit finden Sie im Security-Expertenrat der Computerwoche.

Katharina Friedmann, Redaktion COMPUTERWOCHE

Weitere aktuelle Security-Informationen 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 +++
<http://www.fresh-info.de>

Das Werk ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urhebergesetzes ist ohne Zustimmung von NIFIS strafbar. Dies gilt insbesondere für Vervielfältigungen, Verarbeitung, Mikroverfilmung und die Einspeicherung und Verarbeitung in elektronischen Systemen. Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Für die namentlich gekennzeichneten Beiträge trägt die Redaktion lediglich die presserechtliche Verantwortung. Produktbezeichnungen und Logos sind zu Gunsten der jeweiligen Hersteller als Warenzeichen und eingetragene Warenzeichen geschützt.