Liebe NIFIS-Mitglieder,

sehr geehrte Interessenten und Förderer,

in seiner Entscheidung zur Onlinedurchsuchung hat das Bundesverfassungsgericht das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geschaffen. Das Gericht begründete seine Entscheidung unter anderem damit, dass „der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert". Damit hat das Bundesverfassungsgericht die Gefährdung informationstechnischer Systeme ausdrücklich anerkannt und ihren Schutz im Grundgesetz verankert.

Grundrechte dienen zunächst dem Schutz des Bürgers vor staatlichen Eingriffen. Der Staat ist jedoch auch verpflichtet, den Bürgern die Ausübung ihrer Grundrechte zu ermöglichen. Beispielsweise muss eine rechtmäßige, friedliche Demonstration vor gewalttätigen Gegendemonstranten geschützt werden. In ähnlicher Weise könnte man den Schutz des Staates zur Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vor (kriminellen und sonstigen) Bedrohungen einfordern. Die Auswirkungen auf das Recht der IT-Sicherheit behandelt in dieser Ausgabe Professor Dr. Dirk Heckmann aus unserem wissenschaftlichen Beirat.

In dieser aktuellen Ausgabe von NIFIS advice stellen wir Ihnen außerdem unsere aktuellen Aktivitäten zur Informations- und Internet-Sicherheit vor und laden Sie zur Mitgliederversammlung sowie zum Expertenforum Datenschutzrecht ein. Ich würde mich freuen, Sie dort zu treffen.

Viel Spaß beim Lesen wünscht Ihnen

Thomas Lapp

Stellvertretender Vorstandsvorsitzender der NIFIS

HIGHLIGHTS

NIFIS inside

Fachbeitrag Risikomanagement

Erst die Subprime-Krise, dann der riesige Spekulationsverlust bei der französischen Großbank Société Générale. Da ist die Frage eines kleinen Unternehmers erlaubt: Ist Risikomanagement nicht selbst das Risiko, und soll ich dafür gar noch Geld ausgeben?

Thomas Teichmann, Berater für IT-Sicherheit und Organisation sowie Mitglied im NIFIS-Expertenforum Business Continuity Management, erläutert in einem Fachbeitrag, warum Risikomanagement richtig und wichtig ist. Außerdem berichtet er, wie man dabei vorgehen sollte, und welche Lehren aus dem Schaden der anderen gezogen werden können.

Dabei betont Teichmann: „Risikomanagement muss als unternehmerische Tätigkeit verstanden werden. Nur wenn es als Prozess eingeführt und gelebt wird, bringt es die Schutzwirkung, die von ihm erwartet wird." Den kompletten Fachbeitrag können Sie hier nachlesen. ❑

eco und NIFIS arbeiten zusammen

NIFIS kooperiert bereits seit einiger Zeit mit eco – dem Verband der deutschen Internetwirtschaft e.V.. eco versteht sich als Interessensvertreter und Förderer aller Unternehmen, die mit oder im Internet wirtschaftliche Wertschöpfung betreiben.

Die Kernkompetenz und Hauptarbeitsgebiete des Verbands konzentrieren sich auf die Themen Infrastruktur und Technologien, Inhalte (Content), Anwendungen, Recht und Politik. ❑

Bundesdatenschutzauditgesetz im Fokus

NIFIS kritisiert in einer Stellungnahme den Entwurf des Bundesdatenschutzauditgesetzes und rät der Bundesregierung zu Nachbesserungen. Der stellvertretende Vorstandsvorsitzende der NIFIS, Dr. Thomas Lapp, hält es für falsch, dass „im vorliegenden Referentenentwurf die Begutachtung der Sicherheit informationstechnischer Systeme und Komponenten vom Datenschutzaudit ausdrücklich ausgenommen wird". ►

Das Audit könne nur dann in angemessener und vollständiger Form durchgeführt werden, wenn auch die informationstechnischen Systeme und Komponenten einbezogen würden. Auch mangele es der Gesetzesvorlage an klar abgegrenzten und verwendeten Begriffen, und das vorgesehene Verfahren zur Bestellung von Sachverständigen sei ungeeignet. ❑

Expertenforum Datenschutz lädt zur dritten Sitzung ein

Am 13. Februar 2008 tagte das Expertenforum Datenschutz von NIFIS und DVPT und beriet erneut über den Referentenentwurf für ein Bundesdatenschutzauditgesetz. Die Experten bekräftigten ihre Meinung, dass eine derartige gesetzliche Regelung sehr begrüßenswert sei und zur Etablierung eines ausreichenden Niveaus des Datenschutzes in Deutschland erheblich beitragen könne.

Die gemeinsam erarbeitete Stellungnahme kritisiert einzelne Regelungen und enthält eine Reihe von konkreten Verbesserungsvorschlägen, die sich an den Gesetzgeber richten.

Das Expertenforum hat darüber hinaus die nächsten Themen festgelegt. Unter dem Oberbegriff „Awareness“ sollen in der nächsten Sitzung zwei konkrete Projekte in Angriff genommen werden. Zunächst will NIFIS eine E-Learning-Plattform einrichten, die es Entscheidungsträgern in Unternehmen ermöglicht, schnell und anschaulich die wesentlichen Fragen und Probleme des Datenschutzrechts kennen zu lernen.

Diese Plattform soll den Mitgliedern **kostenlos** und externen Unternehmen gegen Entgelt zur Verfügung gestellt werden. ►

Eine Arbeitsgruppe wird zur nächsten Sitzung konkrete Vorschläge für diese Plattform erarbeiten. Ein zweites Projekt ist die Entwicklung eines Workshops, mit dem in ein bis zwei Stunden der konkrete Bedarf eines Unternehmens im Hinblick auf die Anforderungen des Datenschutzes ermittelt werden kann. Auch hierzu hat sich eine Arbeitsgruppe gebildet, die zur nächsten Sitzung konkrete Vorschläge für den Ablauf und die Struktur eines derartigen Workshops vorlegen wird. Auch diese Workshops werden den Mitgliedern **kostenlos** und externen Unternehmen gegen geringes Entgelt angeboten.

Der Arbeitskreis lädt weitere Interessierte herzlich zur Mitarbeit ein. Die nächste Sitzung des Arbeitskreises findet am 16. April 2008 um 12.30 Uhr in Frankfurt statt. Die Teilnahme lässt sich daher sehr gut mit der Teilnahme an der anschließenden Mitgliederversammlung verbinden. Eine **kostenlose** Anmeldung ist über die NIFIS-Website möglich. ❑

Institut für Systemmanagement rezertifiziert

Das Institut für Systemmanagement darf für ein weiteres Jahr das NIFIS-Siegel führen und dadurch gegenüber Kunden, Mitarbeitern, Geschäftspartnern und zum Beispiel auch externen Prüfern seinen hohen Sicherheitsstandard dokumentieren.

Die Erteilung des speziell für die mittelständische Wirtschaft entwickelten Siegels erfolgte auf Basis einer umfangreichen Selbstanalyse. Das Unternehmen beantwortete 82 Fragen aus den Bereichen organisatorische, logische, technische sowie physikalische Sicherheit, die anschließend vom NIFIS-Siegelrat analysiert wurden.

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

NIFIS-MITGLIEDER-VERSAMMLUNG

Am 16. April um 15.00 Uhr findet die Mitgliederversammlung von NIFIS e.V. in Frankfurt am Main statt. Die Veranstaltung richtet sich ausschließlich an Vereinsmitglieder, die offizielle Einladung und die Tagesordnung wurden den Mitgliedsunternehmen bereits zugestellt.

Veranstaltungstipps

Datenschutz im Visier

Das Wissen eines Unternehmens über Produkte und Kunden ist wertvoller Bestandteil des Firmenvermögens. Diese Daten gilt es zu schützen. Doch wie kann man verhindern, dass wertvolle Informationen – sei es durch Zufall, Nachlässigkeit oder Absicht – in unbefugte Hände geraten? Und wie sehen die gesetzlichen Grundlagen aus?

Antworten auf diese Fragen gibt es auf der Veranstaltung des NIFIS-Mitglieds Compuware am 24. April in Stuttgart. Compuware präsentiert dabei praxiserprobte Lösungen für den Schutz von Informationen und berichtet über entsprechende Erfahrungen aus Kundenprojekten. Ernst & Young stellt die Anforderungen der IT-Revision dar und erläutert die häufigsten Schwachstellen.

Die Applied Security GmbH berichtet über Schutzmöglichkeiten gegen unautorisierten Zugriff und den Verlust vertraulicher Daten und präsentiert sieben praktische Regeln, die jeder beherzigen sollte, dem seine Daten lieb und teuer sind. Die Teilnahme an der Veranstaltung ist **kostenlos**, die Anmeldung hier möglich. ❑

Expertenforum IM präsentiert Ergebnisse

Beim 9. Treffen des NIFIS-Expertenforums Identity Management (IM) in Frankfurt stellten die Arbeitsgruppen ihren Fortschritt dar. Insbesondere die Herangehensweise an die Modellierung der ►

generischen Prozesse des Identity und Access Managements wurde noch einmal ausführlich diskutiert. Bei den Ansätzen bottom-up und top-down haben sich jeweils Vor- und Nachteile herauskristallisiert. Das Expertenforum wird deshalb beide Ansätze verfolgen. Dadurch soll die Qualität der Modelle gesteigert werden.

Erste Ergebnisse werden bei der 2nd European Identity Conference präsentiert, die am 22. April in München beginnt. In diesem Rahmen findet dann auch das 10. Treffen des NIFIS-Expertenforums IM statt.

Interessenten sind herzlich willkommen und wenden sich vorab bitte an newsletter@nifis.de; die Teilnahme am Expertenforum ist **kostenlos**. ❑

NIFIS bei 2. European Identity Conference

Über Trends im Umfeld des Identity und Access Managements (IAM) informiert die 2nd European Identity Conference vom 22. bis 25. April 2008 in München. Bei der Veranstaltung berichten über 100 Referenten aus aller Welt über die neuesten Entwicklungen sowie interessante Best Practices. NIFIS wird als Aussteller vor Ort sein.

Am 22. April finden die Pre-Konferenzworkshops und die Keynotes statt. In diesem Rahmen trifft sich auch das NIFIS-Expertenforum Identity Management von 9 bis 13 Uhr, zu dem alle Interessierten herzlich eingeladen sind. Am 23. April beginnt dann die Konferenz mit den einzelnen Tracks. ❑

NEUE MITGLIEDER

„Die THORANET Unternehmensberatung für Netzwerk- und Systemmanagement GmbH berät ihre Kunden in den Schwerpunktbereichen Identity Management, ITIL und Betriebsführung. Die Unterstützung von flexiblen Geschäftsprozessen in unterschiedlichen Systemen ist nur mit erprobten und standardisierten Verfahren zu bewältigen. Die Mitgliedschaft in der NIFIS ermöglicht es THORANET, diese Verfahren weiter zu entwickeln und dem eigenen Anspruch an permanente Verbesserung zum Wohle ihrer Kunden durch die Mitarbeit und den Erfahrungsaustausch gerecht zu werden."

Oliver Knicker
Leiter Vertrieb Thoranet

Service

Praxistipp

Vorsicht bei Tape-Backup

Peter Heinemann ist Security Manager bei Interxion. In seinem Praxistipp erläutert er, was beim Backup mit Tape-Lösungen beachtet werden sollte.

Obwohl festplatten-basierende Technologien den alt bekannten Tape-Lösungen technisch wie wirtschaftlich betrachtet überlegen sind, finden in vielen Unternehmen nach wie vor Tape-Lösungen Einsatz, das heißt Produktivdaten werden auf Magnetbändern gesichert. Eine gängige Variante, die sich in der Praxis etabliert hat, sieht vor, dass fünf so genannte Tagessicherungen durchgeführt werden, die am Ende der Woche durch ein Wochenbackup ersetzt werden.

Nach vier Wochen werden die einzelnen Wochenbackups in einem Monatsbackup und nach drei Monaten die Monatsbackups in einem Quartalsbackup zusammengefasst usw.. Generell müssen Backups verschlüsselt und am Ende des Sicherungsprozesses auf Wiederherstellbarkeit geprüft werden. Die Überprüfung wird gerne aufgrund von Zeitmangel oder falscher Prioritätensetzung vernachlässigt. Der ganze Aufwand nutzt aber nichts, wenn eine unzureichende Integrität den Datenwiederherstellungsversuch scheitern lässt und gegebenenfalls den Fortbestand des Unternehmens gefährdet.

Die Lagerung der Tapes sollte in einem dem Rechenzentrum ähnlichen Umfeld erfolgen. Optimale klimatische Bedingungen und der Schutz vor direkter Sonneneinstrahlung und magnetischen Feldern sind essenziell, um eine maximale Haltbarkeit und somit auch Wiederverwendbarkeit der Tapes zu gewährleisten. Der Raum, in dem die Datenbänder gelagert werden, muss denselben Sicherheitsvorkehrungen unterliegen wie das Produktivrechenzentrum, wobei die Lagerung der Tapes unbedingt räumlich getrennt erfolgen muss, da sonst zum Beispiel ein Brand Produktivdaten und Backup auf einen Schlag vernichten kann.

Sobald Daten nicht mehr für den laufenden Geschäftsbetrieb benötigt werden, erfolgt die Archivierung. Prinzipiell können frei gewordene Bänder wieder überspielt werden, wobei man regelmäßig die Qualität der Bänder überprüfen muss und sich nicht blind auf die Herstellerangaben verlassen sollte. ❑

Wissenschaftler stehen NIFIS Rede und Antwort

Das BVerfG hat in seinem Urteil zur „Online-Durchsuchung“ ein Grundrecht auf Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme begründet. Wie wirkt sich dieses auf das Recht der IT-Sicherheit aus?

Prof. Dr. Dirk Heckmann: Die Auswirkungen dieser Entscheidung gehen weit über die Reglementierung der Online-Durchsuchung hinaus. Das genannte neue Grundrecht ist ja nicht nur Abwehrrecht des Bürgers gegen staatliche Online-Zugriffe, sondern als Teil der so genannten objektiven Wertordnung auch eine Art Orientierungsmarke für die Gewährleistung von IT-Sicherheit bei der staatlichen, unternehmerischen und privaten IT-Nutzung.

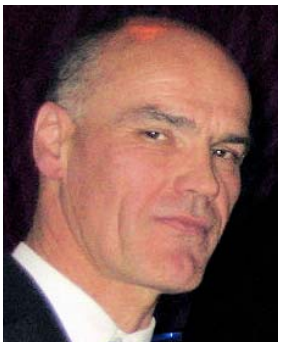
Das BVerfG hat zu Recht herausgestellt, dass die allgegenwärtige IT-Nutzung permanenten Gefährdungen ausgesetzt ist und dass dieser hohen Verletzlichkeit der IT-Infrastrukturen durch Schutzmaßnahmen zu begegnen ist. Dabei genügt der zweifellos wichtige Beitrag der IT-Sicherheitsbranche wohl nicht. Neben den Anstrengungen jedes einzelnen Nutzers ist auch der Staat gefordert, den wirksamen Gebrauch dieses Grundrechts zu gewährleisten. Wie er seiner Schutzpflicht genügt, bleibt abzuwarten. Möglicherweise sind auch die Sorgfaltsmaßstäbe und Haftungsregeln im IT-Sicherheitsrecht zu überdenken. ❑

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.

Expertenfrageecke

Identity Management – Wessen Aufgabe ist das eigentlich?

An dieser Stelle beantworten regelmäßig Experten Fragen, die NIFIS häufig erreichen. In dieser Ausgabe steht Dr. Horst Walther, Partner bei Kuppinger Cole + Partner und Leiter des NIFIS-Expertenforums für Identity Management Rede und Antwort. Sollten auch Sie eine Frage an unsere Experten haben, senden Sie diese einfach an newsletter@nifis.de.



Dr. Horst Walther,
Kuppinger Cole + Partner

Bei vielen Aufgaben im Unternehmen ist die Zuständigkeit intuitiv klar, etwa bei der Buchhaltung, der Revision oder dem Controlling. Beim Identity Management ist dies allerdings nicht so eindeutig. IM ist eine fachliche Aufgabe und Teil der Unternehmensorganisation. Wer sollte also im Unternehmen für Identity Management zuständig sein?

Human Resources

Identity Management behandelt den Umgang mit digitalen Identitäten, also dem digitalen Abbild von Individuen. Human Resources (HR) hat eine natürliche Affinität zu Personen, sie könnte sich der Aufgabe annehmen – will es aber meistens nicht. Denn so, wie sich die HR-Funktion als „Personalverwaltung“ sieht, ist sie relativ businessfern und die Reaktionszeit zu langsam.

Business

Im Fachbereich wiederum decken sich Verantwortung und Aufgaben. Allerdings fehlt methodisches und technisches Wissen. Hinzu kommt, das Identity Management eine unternehmensübergreifende Aufgabe ist. Der einzelne Fachbereich hingegen ist eben nur ein Bereich unter mehreren.

Informationssicherheit

Da die Erhöhung der Informationssicherheit häufig der Auslöser für die Einführung von damit zusammenhängender Technik und den zugehörigen Verfahren ist, wird hier häufig auch die Verantwortung dafür festgemacht. Zwar sind das Wissen um die Risiken und auch der entsprechende Sachverstand vorhanden, jedoch hat die ISS weder ein Organisationsmandat noch eine Ergebnisverantwortung.

IT

Da die IT die Maßnahmen des Identity Management umsetzen kann und muss und Sicherheitslücken hier offenbar werden – auch wenn sie originär aus anderen Bereichen stammen – nimmt sich die IT oft schon in Eigeninitiative der Aufgabe an. Das technische Umsetzungswissen dafür ist oft schon vorhanden. Was aber fehlt, ist das übergreifende Mandat für die Unternehmensgestaltung. Organisation ist eben nicht Technik.

Neue Funktion

Wenn die Organisationsaufgabe im Unternehmen nicht wirksam verankert ist, dann empfehlen wir, eine neue, interdisziplinär arbeitende Funktion zu schaffen. Sie muss für Identitäten, Rollen und Prozesse zuständig sein. Sie braucht organisatorisches und technisches Wissen – und ein Gestaltungsmandat für das Unternehmen. ❑

Sicherheitsupdate

Internet-Konzerne wissen mehr über Nutzer als je zuvor

Ein Marktforschungsinstitut hat erstmals konkrete Zahlen bezüglich der Datensammlung von Surfern durch Internet-Konzerne veröffentlicht.

Internet-Unternehmen wissen heute mehr über die Nutzer Bescheid als jemals zuvor. Dies belegt eine aktuelle Untersuchung des US-Marktforschungsinstitutes comScore, die das Potenzial von 15 großen Online-Konzernen zum Sammeln von User-Daten untersucht hat. Zu diesem Zweck wurden alle so genannten „data transmission events" – also jene Zeitpunkte, wo Nutzer-Daten an die Server der Unternehmen übermittelt werden – erfasst. Ergebnis der Analyse: Die großen Internet-Konzerne Yahoo, Google, Microsoft, AOL und MySpace verzeichneten alleine im Dezember 2007 mindestens 336 Milliarden derartiger Datentransfers. Die bereits seit einiger Zeit laut gewordenen Bedenken von Datenschützern in Bezug auf die Praktiken des Informationssammelns im Internet werden somit erstmals in Form von konkreten Zahlen greifbar.

„Jeder Nutzer hinterlässt durch die vergebene technische Kennung eine deutliche Spur im Internet", erklärt Marit Hansen, stellvertretende Landesbeauftragte für Datenschutz in Schleswig-Holstein, im Gespräch mit pressetext. Insbesondere die konkrete IP-Adresse eines Computers und die oft auf den Rechnern der Nutzer gespeicherten Cookies würden das Verfolgen des Wegs durch das Internet leicht ermöglichen. „Eine örtliche Zuordnung ist beispielsweise über die jeweilige IP-Adresse eines Nutzers ohne weiteres möglich", schildert Hansen. Neben den normalen Suchanfragen würden sehr viele Informationen zunehmend auch über die Mitgliedschaft in sozialen Netzwerken oder über das Verfassen eines Weblogs gesammelt. „Besonders die jüngere Nutzergeneration muss hier über die speziellen Risiken und Gefahren aufgeklärt werden", betont Hansen.

„Problematisch ist in diesem Zusammenhang vor allem, dass Nutzer gar nicht über derartige Praktiken des Datensammelns Bescheid wissen", kritisiert Hansen. Internet-Unternehmen würden in der Regel ihre Kunden nicht ausreichend darüber informieren. „Wenn ein Nutzer weiß, dass seine Daten für Werbezwecke aufgezeichnet werden und dem zustimmt, ist das in Ordnung", stellt Hansen fest. Eine persönliche Zustimmung sei in diesem Zusammenhang ausdrücklich von Nöten. „Die Einwilligung muss aber auch jederzeit zurückgezogen werden können", ergänzt Hansen. Zudem müsse dem Nutzer das Recht auf Einsicht und Korrektur der so erhobenen Daten eingeräumt werden. „Innerhalb der EU dürfen personenbezogene Daten nur unter bestimmten Voraussetzungen gesammelt werden", so Hansen. Entscheidend sei hier vor allem eine gesetzlich festgelegte Zweckbindung. „Nutzerdaten können so nicht generell, sondern immer nur auf einen bestimmten Zweck bezogen gesammelt werden", stellt Hansen klar.

Durch das Verfolgen und Analysieren des Internet-Traffics versuchen die Unternehmen Rückschlüsse auf die Interessen und persönlichen Vorlieben der User zu ziehen. Verwendet werden die so angehäuften Informationen vor allem, um die Inhalte – speziell die Werbebotschaften – im Internet besser auf die jeweiligen Wünsche der Kunden zuschneiden zu können. Laut dem comScore-Bericht hat das größte Datensammel-Potenzial derzeit Yahoo, auf dessen Seiten rund 110 Milliarden User-Datentransfers registriert worden sind. Rang zwei belegt die Community MySpace vor dem US-amerikanischen Onlinedienst AOL und dem Suchmaschinenbetreiber Google.

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