Liebe NIFIS-Mitglieder,

sehr geehrte Interessenten und Förderer,

ich freue mich, Ihnen die neueste Ausgabe von NIFIS advice präsentieren zu dürfen.

Auch in dieser Ausgabe finden Sie wieder viele interessante Themen. Schwerpunkte liegen diesmal auf den Bereichen Business Continuity Management (BCM) und Identity Management (IM). Ein Interview mit unserem Mitglied Thomas Teichmann über das Thema BCM sowie der Bericht über unser Expertenforum IM und die IM-Konferenz sollen Ihnen helfen, wichtige Informationen aus diesen Bereichen für Ihre tägliche Arbeit zu erhalten.

Aus dem wissenschaftlichen Beirat beantwortet Prof. Dr. Maximilian Herberger eine Frage aus seinem aktuellen Tätigkeitsumfeld an der Universität des Saarlandes. Wie gewohnt finden Sie in der Rubrik Expertenfrageecke Antworten auf häufig gestellte Fragen und Problemstellungen rund um die Informations- und Internet-Sicherheit, diesmal geht es um den Datenschutz bei mobilen Geräten.

Besonders möchten wir auch auf unsere Kooperationen hinweisen, mit denen NIFIS erheblich an Reichweite gewinnt und das Thema Sicherheit weiter vorangebracht wird.

Ich wünsche Ihnen in diesem Sinne nützliche Anregungen beim Lesen von NIFIS advice.

Mathias Gärtner

Vorstandsmitglied der NIFIS

HIGHLIGHTS

NIFIS inside

NIFIS zieht Bilanz

Am 16. April hatte NIFIS zur jährlichen Mitgliederversammlung nach Frankfurt am Main eingeladen. Der Vorstandsvorsitzende Peter Knapp begrüßte die Anwesenden und präsentierte die Aktivitäten und Ergebnisse des vergangenen Jahres. NIFIS werde nach wie vor von Wirtschaft, Politik und Wissenschaft als kompetenter Ansprechpartner für Fragen auf dem Gebiet der Informations- und Internet-Sicherheit wahrgenommen.

Die Schwerpunkte der NIFIS-Aktivitäten lagen in den Bereichen Veranstaltungen, Öffentlichkeitsarbeit und Mitgliederakquisition. Höhepunkt der Events stellte das 1. NIFIS-Forum für angewandte Informations-Sicherheit mit zahlreichen Teilnehmern und hochkarätigen Referenten dar. Aber auch im Rahmen anderer Veranstaltungen war NIFIS präsent, zum Beispiel bei der ersten European Identity Conference, dem COMPUTERWOCHE Data-Center-up-to-date, der CeBIT und der VO.IP Germany. ►

Neben den quartalsweisen Sitzungen der NIFIS-Expertenforen Identity Management und „Sicherheit in Rechenzentren“ erfolgte die Konstituierung der zwei Expertenforen Business Continuity Management und Datenschutz. Peter Knapp forderte die Mitglieder zu verstärkter Mitarbeit und Nutzung der verschiedenen Plattformen auf.

Neues Management

In diesem Zusammenhang teilte er mit, dass das Management des Vereins in Zukunft von den Mitarbeitern der Europäischen EDV-Akademie des Rechts gGmbH (EEAR) übernommen wird. Die gemeinnützige GmbH wird den Vorstand sowohl bei administrativen Aufgaben als auch bei der Akquise neuer Mitglieder unterstützen. Die EEAR mit Sitz in Merzig ist an der Schnittstelle zwischen IT und Recht aktiv und hat in vielen bundesweiten Projekten Kompetenzen und Netzwerke gewonnen, die sie in ihren neuen Aufgabenbereich für NIFIS einbringen wird.

Die gewohnten Kontaktdaten (Telefon 0 69 / 40 80 93 70, E-Mail newsletter@nifis.de) bleiben bestehen. ❑

Expertenforum Validierung und Zertifizierung

Am 1. Juli trifft sich ab 15 Uhr unter dem Dach von NIFIS e.V. in Frankfurt am Main ein neues Expertenforum, das sich mit dem Themenkomplex Validierung und Zertifizierung von IT-Sicherheit beschäftigen wird. Die Leitung übernimmt Dimitrios Mourousiadis, Geschäftsführer der BiSS technologies. NIFIS bietet Unternehmen bereits auf Basis eines Selbstaudits eine pragmatische Möglichkeit, das eigene Sicherheitsnivau zu überprüfen und mit dem anerkannten NIFIS-Siegel zu dokumentieren.

Aufbauend hierzu soll in Anlehnung an den internationalen Standard ISO 27001 die Möglichkeit geboten werden, die IT-Sicherheit modular zu erweitern und zertifizieren zu lassen. Diese Module und die Details der Zertifikatsvergabe möchte das Expertenforum erarbeiten. Sie sind herzlich eingeladen, sich an diesem Expertenforum zu beteiligen und sich **kostenlos** und auf neutraler Ebene mit anderen Interessierten aus der Wirtschaft auszutauschen.

Bei Interesse wenden Sie sich bitte an newsletter@nifis.de. ❑

NIFIS-Siegel dokumentiert Sicherheit

Mit dem NIFIS-Selbstauditverfahren machen Unternehmen einen umfassenden Sicherheitscheck. Er ist ohne großen Aufwand und kostengünstig realisierbar. Sie erhalten einen Katalog mit 82 Fragen aus den Bereichen organisatorische, logische, technische sowie physikalische Sicherheit. Ein Experten-Gremium, der so genannte NIFIS-Siegelrat, wertet die Antworten aus und zeigt vorhandene Sicherheitslücken auf. Bei einer positiven Bewertung kann das Unternehmen für ein Jahr das NIFIS-Siegel führen und dadurch gegenüber Kunden, Mitarbeitern, Geschäftspartnern und zum Beispiel auch externen Prüfern seinen hohen Sicherheitsstandard dokumentieren. Für NIFIS-Mitglieder ist der Erwerb des speziell für die mittelständische Wirtschaft entwickelten Siegels ebenso wie die Rezertifizierung **kostenfrei** möglich. Für Nicht-Mitglieder kostet das Audit 150 Euro.

Weitere Informationen erhalten Sie hier. ❑

NEUE MITGLIEDER

„Als IT-Security-Dienstleister ist die BiSS technologies spezialisiert auf Beratungs- und Prüfungsleistungen in den Bereichen Compliance, IT-Security und Business Continuity. Bei NIFIS sind wir insbesondere an der aktiven Mitarbeit am Expertenforum Validierung und Zertifizierung interessiert. Hier möchten wir gemeinsam mit den anderen Teilnehmern Wege aufzeigen, IT-Sicherheit schnell und kostengünstig zu implementieren und aufrecht zu erhalten."

Dimitrios Mourousiadis, Geschäftsführer BiSS technologies

NIFIS und BIEG Hessen kooperieren

NIFIS arbeitet mit dem BIEG Hessen – Beratungs- und Informationszentrum Elektronischer Geschäftsverkehr zusammen. Um im Wettbewerb dauerhaft zu bestehen, muss heute auch der Mittelstand die Chancen der elektronischen Märkte nutzen. Hilfestellung bietet hier das BIEG Hessen.

Es berät kleine und mittlere Unternehmen kostenlos und unterstützt unter anderem bei der Planung und Implementierung unternehmensgerechter Strategien zur Nutzung des elektronischen Geschäftsverkehrs. Das BIEG Hessen ist eine Einrichtung der Industrie- und Handelskammern Frankfurt am Main, Fulda, Hanau-Gelnhausen-Schlüchtern und Offenbach am Main und wird vom Bundesministerium für Wirtschaft und Technologie gefördert. ❑

Basisprozessmodelle für Identity Management

Das NIFIS-Expertenforum Identity Management (IM) hat unter der Creative-Commons-Lizenz einen Arbeitsbericht veröffentlicht. Darin stellen die Autoren ein Basisprozessmodell auf der Grundlage so genannter Petrinetze vor. Hierbei werden nicht nur die grundsätzlichen Vorgehensweisen, Objektbeziehungen und Rollen erläutert, sondern diese gleich auf typische Prozesse übertragen. Am Beispiel eines Antrags- und Genehmigungsprozesses für SAP-Rollen wird sauber modelliert, welche Aktoren (Personen) für welche Objekte zuständig sind (Ownership) und wie welche Aktionen ausgelöst werden.

Das Expertenforum will eine möglichst umfassende Bibliothek von Standardprozessen erarbeiten, die die organisatorischen Vorarbeiten von IM-Projekten deutlich vereinfachen und beschleunigen sollen. Die Modellierung erfolgt Top-Down und wird dann durch die Petrinetze erweitert. ❑

Veranstaltungstipps

NIFIS bei 2. European Identity Conference

Zum wichtigsten Event im Bereich Identity Management (IM) in Europa trafen sich Branchenkenner und -interessierte vom 22. bis zum 25. April in München. Mehr als 100 Referenten aus aller Welt berichteten bei der 2nd European Identity Conference über die neuesten Entwicklungen sowie interessante Best Practices. Mit dabei waren führende Experten wie Dave Kearns von Network World, André Durand von Ping Identity und Kim Cameron von Microsoft.

Am Stand von NIFIS fand sich ein interessiertes internationales Publikum ein, zahlreiche angeregte Gespräche konnten geführt und neue Kontakte geknüpft werden. Im Rahmen der Pre-Konferenzworkshops traf sich vor Ort auch das NIFIS-Expertenforum IM. ►

Dabei stellten die einzelnen Arbeitsgruppen ihren Fortschritt dar. Dr. Horst Walther von Kuppinger Cole + Partner und Leiter des IM-Expertenforums hielt im Rahmen der Konferenz zudem zwei Vorträge zum Stand des Rollenmanagements und zum Thema Compliance. ►

Das nächste Treffen des NIFIS-Expertenforums IM findet am 27. Juni in München statt. Interessenten sind herzlich willkommen und wenden sich vorab bitte an newsletter@nifis.de. Die Teilnahme ist **kostenlos**. ❑

Roadshow Security 2.0

NIFIS-Mitglied Controlware berichtet in einem Security-2.0- Workshop ausführlich über aktuelle Trends bei IT-Sicherheitslösungen. Dabei wird gezeigt, wie Firewall-Regelwerke und das IP-Adress-Management effizienter gestaltet werden können. ►

Zudem erfahren die Teilnehmer, wie sie der Gefahr von Datendiebstahl im Unternehmen mithilfe von Data Leak Prevention sinnvoll entgegenwirken können. Natürlich gibt es auch ausreichend Gelegenheit, sich mit Experten auszutauschen und individuelle Anforderungen zu diskutieren.

Die Roadshow Security 2.0 macht am 5. Juni in Hannover und am 11. Juni in München halt, die Teilnahme an der Veranstaltung ist **kostenfrei**. ❑

Service

Expertenfrageecke

Datenschutz bei mobilen Geräten

An dieser Stelle beantworten regelmäßig Experten Fragen, die NIFIS häufig erreichen, in dieser Ausgabe Rechtsanwalt und NIFIS-Vorstand Dr. Thomas Lapp. Sollten auch Sie eine Frage an unsere Experten haben, senden Sie diese einfach an newsletter@nifis.de.

Immer mehr Mitarbeiter haben sensible Firmendaten auf mobilen Geräten. Was sollte deshalb beim Datenschutz- und Datensicherheitskonzept beachtet werden?

Dr. Thomas Lapp, NIFIS-Vorstand

Notebooks, Handys, Smartphones und andere Kleinstcomputer werden gern auf kleine und große Reisen und zu allen möglichen Terminen mitgenommen. Sie bieten unterwegs hohen Arbeitskomfort, da sie mobile Alleskönner sind: Sie tauschen Daten mit normalen Bürosystemen, Kontakte, Termine, Aufgaben, Notizen werden auf die Mobilgeräte exportiert beziehungsweise mit diesen synchronisiert. Darüber hinaus können damit auch E-Mails empfangen und alle Arten von Dateien mobil gelesen und bearbeitet werden.

Diese praktischen Informationen enthalten jedoch vielfach personenbezogene Daten, die nach den Datenschutzgesetzen zu schützen sind. Dies gilt auch für Kontakte, soweit der Ansprechpartner mit Name, E-Mail und Durchwahl und nicht nur das Unternehmen selbst gespeichert ist. Auch Termine, Aufgaben und alle anderen Dateien enthalten häufig personenbezogene Daten. Darüber hinaus sind in vielen auf mobilen Geräten gespeicherten Dateien geheimhaltungsbedürftige Informationen enthalten. Dabei kann es sich um Betriebsgeheimnisse des eigenen Unternehmens handeln. Handelt es sich um Geheimnisse von Vertragspartnern, so ist in den Verträgen meist eine Geheimhaltungsvereinbarung getroffen, die massive Vertragsstrafen sowie die Verpflichtung zum Ersatz von entstehenden Schäden vorsieht. Gehen die Geräte verloren, können erhebliche finanzielle Folgen, bis zur Existenzgefährdung des Unternehmens, eintreten.

Soweit es keine systematische Bearbeitung dieses Risikos im Unternehmen gibt, wird man der Unternehmensführung vorwerfen können, ihre Verpflichtung zur Schaffung eines internen Kontrollsystems vernachlässigt zu haben. Dies kann bei Eintritt eines Schadens die persönliche Haftung der Unternehmensführung zur Folge haben.

In jedem Unternehmen ist es erforderlich, die von den Mitarbeitern eingesetzten mobilen Geräte zu erfassen und jeweils festzuhalten, ob und wie ein Schutz von Daten gegen unbefugte Kenntnisnahme, Nutzung oder Veränderung möglich ist. Sodann muss für das Unternehmen festgelegt werden, welche mobilen Geräte eingesetzt werden dürfen, und es ist für jedes Gerät zu bestimmen, welche Daten darauf übertragen beziehungsweise mit diesen synchronisiert werden dürfen. Hierbei ist eine Abwägung zwischen dem Schutzbedürfnis im Hinblick auf die Daten einerseits, den Anforderungen an die mobile Nutzung und die Möglichkeit zum Schutz der Daten auf dem Mobilgerät andererseits zu treffen. Bei der Heterogenität der Geräte wird dies dazu führen, dass einige der mobilen Geräte von der Nutzung in Unternehmen ausgeschlossen werden, während andere auf die Verarbeitung weniger sensibler Daten zu begrenzen sind. ❑

Wissenschaftler stehen NIFIS Rede und Antwort

Obwohl Sicherheit bei Internet-Projekten stets als oberste Priorität anerkannt wird, kommt es doch immer wieder zu Sicherheitsproblemen. Wo sehen Sie Ursachen dafür, und was kann man zur Verbesserung der Lage tun?

Prof. Dr. Maximilian Herberger: Sicherheit ist nicht nur eine Frage der Technik, sondern wesentlich auch eine Frage der Mentalität derjenigen, die mit Technik umgehen. Deswegen ist es wichtig, eine Sicherheitskultur zu schaffen, die durch adäquates Problembewusstsein und sicherheitsorientiertes Denken gekennzeichnet ist. Schon im Vorfeld der beruflichen Tätigkeit sind hier Schulen und Universitäten gefragt.

Zugleich ist es wichtig zu erkennen, dass es sich angesichts des schnellen Technikwandels mit immer neuen Risikopotenzialen bei der Sicherheitserziehung nicht um eine punktuelle Aufgabe handelt. Vielmehr gilt es, dauerhafte Begleitstrukturen zu entwickeln, die das Sicherheitsbewusstsein stets auf aktuellem Niveau halten.

Da sich Sicherheitsrisiken häufig im Zusammenspiel mehrerer Systeme ergeben, (man denke etwa an den Kunden-PC beim Electronic Banking im Dialog mit dem IT-System der Bank über das Internet), setzt adäquates Sicherheitsmanagement eine Kooperation über Systemgrenzen hinweg voraus, eine Denkweise also, der oft sektorale Kapselungen entgegenstehen. ❑

Prof. Dr. Maximilian Herberger ist Inhaber des Lehrstuhls für Bürgerliches Recht, Rechtstheorie und Rechtsinformatik an der Universität des Saarlandes. Als Vorsitzender des Deutschen EDV-Gerichtstages, geschäftsführender Direktor des Instituts für Rechtsinformatik und Herausgeber der Internet-Rechtsinformatik-Zeitschrift JurPC beschäftigt er sich seit vielen Jahren praxisnah unter anderem auch mit den Themen Datenbanken, EDV-Sicherheit und Internet-Recht. Er ist Mitglied im Wissenschaftsbeirat von NIFIS.

„BCM muss man heutzutage haben, das ist Existenzsicherung!“

Thomas Teichmann ist Geschäftsführer der Schmitz & Teichmann Betriebsberatung GmbH mit vielfältiger Erfahrung im gesamten IT-Umfeld. Schon frühzeitig interessierte er sich nicht nur für die IT-Technik, sondern vor allem für alles Organisatorische und Persönliche, was mit IT verbunden ist. In diesem Zusammenhang engagiert er sich mit Enthusiasmus im Bereich Business Continuity Management (BCM). In NIFIS advice beantwortet er die wichtigsten Fragen zu dem Thema.

Wie definieren Sie BCM, und warum benötigen wir den „neumodischen“ Begriff?

Die Idee hinter dem Business Continuity Management ist nicht neu: Im betriebswirtschaftlichen Bereich ist es schon immer Aufgabe der Geschäftsführung, den Geschäftsbetrieb aufrecht zu erhalten. BCM greift aber konkret diese Aufgabe heraus und umfasst alle Konzepte, Planungen und Maßnahmen. Im Rahmen der Reorganisationen in den vergangenen 20 Jahren ist in den Unternehmen unter Aspekten der Wirtschaftlichkeit die Betriebssicherheit zum Teil vernachlässigt worden, sodass der Gesetzgeber 1998 mit dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, kurz KonTraG, darauf reagierte. Es besagt explizit, dass der Geschäftsführer persönlich dafür verantwortlich ist, dass der Geschäftsbetrieb weitergeht und nicht nur ständig Kosten gespart werden. BCM nimmt die Aufforderung auf. Die Wahrnehmung in den Unternehmen wird durch den eigenen Namen verstärkt.

Wenn BCM alles umfasst, was die Geschäftstätigkeit eines Unternehmens gefährden könnte, vom Feuer bis zum Hackerangriff, wie bekommt man System in den Informationswust?

BCM kann man in drei Bereiche untergliedern: die IT, das Facility Management, also alles was an das Gebäude gebunden ist, und das Personal. Es darf sich aber nicht wie Blei auf alles im Unternehmen legen und Prozesse lähmen. BCM muss als handhabbarer und auch wirtschaftlich kontrollierbarer Prozess installiert werden. Dafür gibt es die Definition des BCM-Prozesses.

Wird Ihrer Erfahrung nach einer der drei BCM-Bereiche besonders gerne vernachlässigt?

Bei den großen Unternehmen sind alle drei Bereiche meist gut geregelt, in kleineren Unternehmen mangelt es oft an allen dreien. Allein der Punkt Vertretungsregelungen ist für viele schon eine enorme Herausforderung. Sie sind für einzelne Tipps dankbar, nehmen sich aber ungern des gesamten BCMs an. Die Initiierung kommt meist von außen, wenn beispielsweise die Bank bei Vorlage eines BCM-Berichts günstigere Kreditkonditionen bietet. Auch Wirtschaftsprüfer fragen danach, und im Bereich der IT ist es schon lange Gegenstand der IT-Revision. Wenn nach dem IT-Grundschutz unter 27001 der ISO-Norm geprüft wird, muss der IT-Verantwortliche beantworten, was zur Vermeidung vorhersehbarer Risiken unternommen wurde. Die Initiierung von der Geschäftsführung kommt eher, wenn ein Schadensfall eingetreten ist, der durch eine BCM-Maßnahme im Vorfeld kostengünstiger gelöst oder vermieden hätte können. ►

Wenn ein Unternehmen BCM angehen will, wie geht es am besten vor?

Die Geschäftsführung sollte sich im regelmäßigen Turnus die geschäftskritischen Prozesse anschauen. Sie sollte sämtliche möglichen Gefährdungen ermitteln und auflisten: Was darf nicht schief gehen, weil sonst die Weiterführung des Geschäftsbetriebs gefährdet ist? Welche Funktion oder Person darf nicht ausfallen? Wer hat Schlüssel für welche Gebäude, Räume, den Tresor? Was passiert, wenn derjenige nicht da ist? Das allein bringt schon sehr viel Erkenntnis. Für die einzelnen Bereiche sollte die Geschäftsführung dann die Abteilungsleiter oder Verantwortlichen hinzuziehen und direkt befragen, wo sie geschäftskritische oder existenzbedrohende Gefährdungen sehen. Wichtig ist, für eine offene Atmosphäre zu sorgen. Mitarbeiter sind vorsichtig beim Benennen von Fehlern, wenn der Chef nachfragt, denn diese könnten vielleicht auf sie zurückfallen.

Was folgt nach dieser Gefährdungsliste?

Thomas Teichmann,
Geschäftsführer
Schmitz & Teichmann

Nachdem die Liste erstellt ist, muss man Maßnahmen ermitteln, um die Gefährdung auszuschließen. Vor der tatsächlichen Umsetzung sollten diese aber zunächst wirtschaftlich bewertet und gewichtet werden. Das ist die Business-Impact-Analyse. Wenn die Maßnahmen teurer sind als der Schaden, der eintreten könnte, dann sollte man das momentan bei der Auflistung belassen. Vielleicht entdeckt man bei der nächsten Analyse eine andere, günstigere Maßnahme oder geht einen Zwischenschritt. Wichtig ist der Überblick, was getan werden muss, und dann die Einleitung von konkreten Schritten zur Verbesserung und Beseitigung der als gravierend eingeschätzten Risiken.

Was sollte ein Unternehmer tun, um ein Minimum an BCM zu bekommen?

Es gibt ein paar ganz einfache Grundregeln, die in jedem Unternehmen greifen – egal, wie groß es ist, auch wenn die zunächst trivial klingen. Man muss festlegen: Wer stellt überhaupt fest, dass der Notfall eingetreten ist, für den man sich wappnen will. Bei einem Feuer ist das einfach, aber wer weiß beispielsweise bei einem längeren Stromausfall, was in welcher Reihenfolge zu tun ist?

Dann sollte es unbedingt eine aktuelle Liste mit Telefonnummern für den Notfall geben, die an mindestens zwei räumlich getrennten Stellen bereit gehalten wird und gut sichtbar sowie lesbar ist.

Das Verhalten im Notfall muss gelegentlich geübt werden. Brandschutzübungen kennt man. Aber viele Unternehmen unterschätzen beispielsweise, dass bei extremen Sommertemperaturen die Klimaanlagen überfordert sein könnten. Es kann helfen, wenn in der Mittagshitze bestimmte Geräte ausgeschaltet werden. Doch welche sind für ein paar Stunden verzichtbar, und in welcher Reihenfolge werden sie am besten abgeschaltet? Damit das im Ernstfall richtig läuft, sollte die Vorgehensweise praktisch geübt werden. Das ist auch wichtig, um Panik zu vermeiden.

Wie kann BCM so in die Organisation aufgenommen werden, dass es die notwendige Durchsetzungskraft erhält?

Das ist einer der Schwerpunkte, an denen wir derzeit im NIFIS-Expertenforum BCM arbeiten. BCM muss ständig beobachtet werden, weil sich Geschäftsprozesse ändern. Dadurch entstehen andere Risiken, einige fallen auch weg. Ein Unternehmen mittlerer Größe kann sich keinen BCM-Verantwortlichen als Vollzeitstelle leisten. Man muss einen Mitarbeiter finden, der das Thema in seiner Fragestellung ernst nimmt und bereit ist, sich dieser Aufgabe zusätzlich anzunehmen. Es muss jemand sein, der Verantwortung trägt, der auch von der Hierarchieposition her schon den notwendigen Respekt bekommt. Das birgt ein Dilemma, wenn jemand für operative Geschäftsprozesse verantwortlich ist, und er als BCM-Beauftragter Maßnahmen vorschlagen sollte, die diese Prozesse verlangsamen oder aufwändiger gestalten. Da steht er sich womöglich selbst im Wege.

Ist ein externer BCM-Beauftragter die bessere Lösung?

Prinzipiell würde ich sagen: Wenn die Ressourcen im Hause vorhanden sind, sollte auf jeden Fall ein Interner benannt werden. Er bekommt eher Dinge mit, die gut oder schlecht laufen. Kann er sich zeitlich nicht ausreichend darum kümmern, macht es Sinn, dass regelmäßig ein externer Berater überprüft, ob die BCM-Prozesse so stimmen und eingehalten werden. Dieser ist es gewohnt, die richtigen Fragen zu stellen, gibt Anregungen, sieht das Unternehmen aus einer anderen Sicht. Und – er ist kein Vorgesetzter.

Was sind weitere Schwerpunkte des NIFIS-Expertenforums?

NIFIS beschäftigt sich mit dem Thema Informations- und Internet-Sicherheit. Deshalb ist das NIFIS-Expertenforum BCM auch sehr IT-lastig. Wir schauen aber auch: Was können wir von anderen Instituten in unterschiedlichen Bereichen lernen und wie können wir das für IT-Fragen übernehmen. Wir erarbeiten in sachlicher Atmosphäre brauchbare Anleitungen für den täglichen Bedarf kleiner und mittlerer Unternehmen, damit sie das Thema selbst in die Hand nehmen können. ►

IMMER UP TO 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.

Was erhoffen Sie sich für die Zukunft von BCM?

Beim BCM ist es wie mit anderen Sicherheitsmaßnahmen auch: Es rechnet sich nicht direkt. In eine Krankenversicherung zahlt man jeden Monat einen Beitrag ein und ist sogar froh, wenn man gesund bleibt und diese nicht zum Einsatz kommt. Und es gibt den gesellschaftlichen Druck: Krankenversicherung muss sein. Wenn ein Unternehmer zum anderen sagt: „Hast Du schon BCM eingeführt?“ und der andere antwortet: „Das muss man doch heutzutage haben, das ist doch Existenzsicherung“, dann haben wir gewonnen! ❑

Sicherheitsupdate

Europäer entdecken Identity Management

Nach einer aktuellen Studie von KPMG hat sich das Thema Identity and Access Management (IAM) in der europäischen Unternehmenslandschaft vom theoretischen Konzept zur realen Geschäftspraxis entwickelt.

Nach einer ausgedehnten Hype-Phase ist das Thema IAM bei den europäischen Unternehmen nun offenbar branchen- und länderübergreifend angekommen. Zu diesem Schluss kommt KPMG in seiner „2008 European Identity & Access Management Survey". Um herauszufinden, wie es in der Firmenlandschaft um die nachweisliche und effektive Verwaltung von Identitäten und deren Berechtigungen, sprich: das User-, Access- und Authentisierungs-Management sowie Provisioning und Audit bestellt ist, hat das Wirtschaftsprüfungs- und Beratungsunternehmen CEOs, CIOs, Security-Verantwortliche und interne Prüfer von 235 Firmen in 21 europäischen Ländern zum Stand der Dinge in ihren Organisationen befragt.

Sämtliche Studienteilnehmer haben demnach in den vergangenen drei Jahren ein oder mehrere IAM-Projekte in Angriff genommen. Zwei Dritteln der Unternehmen steht dafür mittlerweile ein dediziertes Budget zur Verfügung. Die Nase vorn haben hier die als „Early Adopters" eingestuften Finanzdienstleister, die im Schnitt über um 20 Prozent höhere IAM-Etats verfügen als in anderen Branchen agierende Firmen. Mit den geringsten diesbezüglichen Mitteln bescheiden sich Organisationen im Infrastrukturbereich, im Regierungsumfeld sowie im Gesundheitswesen, die laut Studie als „IAM-Nachzügler" gerade erst die Fühler ausstrecken.

Der Untersuchung zufolge konzentriert sich das Gros der aktuellen IAM-Projekte auf das Management und die Kontrolle des Zugriffs auf interne Systeme und Informationen, während das Federated Identity Management, also die firmenübergreifende Verknüpfung von IAM-Umgebungen, noch wenig verbreitet ist.

Haupttreiber für IAM-Projekte

Unternehmen gehen IAM-Vorhaben in erster Linie an, weil sie hoffen, Compliance-Vorgaben besser einhalten und ihre Risiken minimieren zu können. Außerdem versprechen sie sich optimierte Anläufe und dadurch einen höheren Business Value.

Was die Risikoeindämmung mittels IAM betrifft, erwarten die Firmen vor allem eine genauere Kontrolle darüber, wer Zugriff auf welche Informationen hat. User-Management-Reporting sowie -Kontrollen wiederum sollen es erleichtern, Compliance-Vorgaben zu erfüllen. Darüber hinaus erhoffen die Unternehmen Verbesserungen bei bestimmten Vorgängen – insbesondere, wenn Mitarbeiter ihre Funktion wechseln oder die Organisation verlassen. Kostensenkungen gehören nicht zu den primären Motiven für IAM-Initiativen, allerdings wird erwartet, dass der darüber zu erzielende Abbau des administrativen Overheads zu niedrigeren Gesamtkosten führt. weiterlesen

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