Liebe NIFIS-Mitglieder,
sehr geehrte Interessenten und Förderer,

seit Mai bin ich als Vorstand für NIFIS tätig. Erstmals habe ich die Ehre, das Vorwort für NIFIS advice zu schreiben und kann direkt von Neuerungen des Mediums berichten. Unser regelmäßiges Magazin für Mitglieder und Interessenten erfreut sich großer Beliebtheit. Dennoch sind wir bestrebt, es ständig zu verbessern. So erscheint NIFIS advice ab sofort zweimonatlich und wartet mit neuen interessanten Kategorien auf.

Durch meine Tätigkeit als öffentlich bestellter und vereidigter Sachverständiger für IT treffe ich häufig auf Fälle, in denen der Schaden bereits entstanden ist. Vieles hätte sich durch geeignete Maßnahmen im Vorfeld vermeiden lassen. Allerdings sind die zu beachtenden Themen, Techniken und gesetzlichen Auflagen sehr komplex. In NIFIS advice erhalten Sie umfangreiche Informationen und hilfreiche Tipps, die getreu unseres Mottos „aus der Wirtschaft für die Wirtschaft“ kommen, um die Sicherheit Ihres Unternehmens zu erhöhen.

Jedes Mitglied hat Lösungen für den einen oder anderen Bereich bereits implementiert und gibt in unseren Expertenforen seine Erfahrung im direkten Austausch weiter. Ab sofort greifen wir auch stärker in NIFIS advice auf dieses Wissen zurück: Ausführliche Berichte der Treffen und Interviews mit Experten bereichern das Medium. Intensive Kooperationen mit der Wissenschaft und Vereinigungen wie dem EDV-Gerichtstag helfen, Hintergründe zu beleuchten.

Auch Sie sind herzlich eingeladen, sich aktiv an NIFIS advice zu beteiligen: Schicken Sie uns Ihre Fragen, geben Sie anderen Unternehmen Praxistipps. Wenden Sie sich einfach an newsletter@nifis.de. Ich wünsche Ihnen nützliche Anregungen beim Lesen dieser Ausgabe.

Ihr Mathias Gärtner

NIFIS-Vorstand

HIGHLIGHTS

NIFIS inside

Claranet und Interxion erhalten erneut NIFIS-Siegel

Seite 2

Veranstaltungstipps

Expertenforum BCM

Seite 3

Service

Risiken der Nutzung von Internet und E-Mail am Arbeitsplatz

Seite 4

Spitzenpolitiker stehen NIFIS Rede und Antwort

Seite 6

Sicherheitsupdate

Hacker nehmen Führungskräfte und deren Angehörige ins Visier

Seite 6

NIFIS Inside

Mangelnde Dokumentation

76,5 Prozent der deutschen Unternehmen sind der Meinung, alle nötigen Maßnahmen zum Schutz personenbezogener Daten nach dem Bundesdatenschutzgesetz (BDSG) getroffen zu haben. Lediglich 56 Prozent dokumentieren hingegen detailliert die Zugriffe und Bewegungen innerhalb von Anwendungen und Datenbanken, zum Beispiel wer personenbezogene Daten eingibt, verändert oder gar gelöscht hat.

Datenmanipulation und -missbrauch können somit nicht in ausreichender Form nachverfolgt werden. Dies ergab eine Umfrage von Compuware in Zusammenarbeit mit NIFIS. „Durch die mangelnde Dokumentation riskieren die Unternehmen ihren guten Ruf sowie enorme finanzielle Schäden“, sagt Bernd Schmiedel, Senior PreSales Consultant von Compuware.

Eine Lösung zur Dokumentation und Rückverfolgung von Sicherheitsverletzungen sei dringend erforderlich, um die Betroffenen schneller zu identifizieren, die Ursachen leichter zu beheben und die Auswirkungen zu minimieren. Positiv zu vermerken ist, dass fast alle Unternehmen (96,5 Prozent) Firewalls einsetzen, 61,7 Prozent der Befragten führen spezifische Sicherheitstests ihrer Anwendungen durch. ❑

Angebot für Mitglieder

NIFIS erweitert die Kooperation mit der Computerwoche, um den Mitgliedern ein attraktives Angebot unterbreiten zu können: Wer unter Angabe seiner Mitgliedsnummer einen Fragebogen ausfüllt, bekommt die Computerwoche zeitlich uneingeschränkt kostenlos.

COMPUTERWOCHE

Das Formular mit sieben Fragen zur Einordnung des Unternehmens und den geplanten Investitionen kann unter newsletter@nifis.de angefordert werden.. ❑

Präventiver Schutz selten

Mehr als die Hälfte der von NIFIS für den Deutschen Sicherheitsreport befragten Branchenexperten hat im vergangenen beziehungsweise laufenden Jahr von Vorfällen im Hinblick auf die IT- oder Informations-Sicherheit im eigenen oder in einem anderen Unternehmen gehört.

Die deutschen Unternehmen seien bezüglich des Themas mittlerweile sensibilisiert, erklärt NIFIS-Vorstandsvorsitzender Peter Knapp. Allerdings müsse nun der zweite Schritt folgen: Die schnelle Umsetzung wichtiger Maßnahmen, um Sicherheitsvorfälle bereits im Vorfeld zu verhindern.

Dazu gehöre, die Anforderungen in Bezug auf die IT-Sicherheit explizit zu formulieren und in einem Katalog mit klaren Soll-/Ist-Listen zu überprüfen. Außerdem mangele es oft an klaren Verhaltensregeln, an denen sich die Mitarbeiter orientieren können. ❑

Exekutivbeirat bekommt Verstärkung

Silke Stokar von Neuforn, MdB

NIFIS gewinnt mit Silke Stokar von Neuforn (MdB BÜNDNIS 90/DIE GRÜNEN) eine weitere Expertin zum Thema Datenschutz.

In ihrem Amt als innenpolitische Sprecherin der Bundestagsfraktion BÜNDNIS 90/DIE GRÜNEN befasst sich Frau Stokar von Neuforn unter anderem mit der Reform des Bundesdatenschutzgesetzes (BDSG) sowie der Weiterentwicklung des Informationsfreiheitsgesetzes (IFG). NIFIS möchte künftig verstärkt das Thema Datenschutz behandeln. ►

Die Bundestagsabgeordnete selbst weiß sehr genau um den dringenden Handlungsbedarf bei der Sicherheit im Datenverkehr: „Wir brauchen in Deutschland Initiativen wie NIFIS, um Erfahrung und Top Skills auszutauschen und beim Thema Sicherheit immer einen Schritt voraus zu sein. So können wir helfen, die Wirtschaftskraft von Unternehmen, Staat und Haushalten zu schützen.“ ❑

Claranet und Interxion erhalten erneut NIFIS-Siegel

Mit dem NIFIS-Siegel können Unternehmen ihren hohen Sicherheitsstandard gegenüber Kunden, Partnern, externen Prüfern und Mitarbeitern belegen. Es dient der positiven Abgrenzung von Wettbewerbern und schafft einen Vertrauensvorsprung. Dies wird unter anderem durch die zeitliche Beschränkung des Siegels erreicht: Es darf jeweils nur für zwölf Monate geführt werden, bevor eine aktuelle Überprüfung den Sicherheitsstandard bestätigt.

Die beiden ersten Unternehmen, die nun erfolgreich die Rezertifizierung bestanden haben, sind Claranet und Interxion. 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 das Audit 150 Euro.

Weitere Informationen zum NIFIS-Siegel erhalten Sie hier. ❑

NIFIS kooperiert mit Deutschem EDV-Gerichtstag

NIFIS arbeitet eng mit dem EDV-Gerichtstag zusammen. Dieser sieht es als seine Aufgabe an, wichtige Entwicklungen verantwortlich zu begleiten und an der Entwicklung von Standards mitzuwirken. Der EDV-Gerichtstag will weiter dazu beitragen, die EDV-Instrumente für die juristische Arbeit auf das jeweils beste Niveau zu bringen. Dabei kommt dem Erfahrungsaustausch innerhalb und außerhalb der Arbeitskreise eine besondere Bedeutung zu. ❑

NEUE MITGLIEDER

PLUS PR

„Wir haben uns für die Mitgliedschaft bei NIFIS entschieden, weil das Thema Informations- und Internet-Sicherheit immer bedeutender wird. Wir legen besonderen Wert auf den Schutz von Informationen, die wir von unseren Kunden erhalten. Wir sind ja sehr häufig schon in den ersten Ideenfindungsphasen involviert. Auch kleine und mittlere Unternehmen sind über (fehlende) IT-Sicherheit angreifbar, daher wollen wir aus dem Informationsaustausch mit anderen Unternehmen lernen und unsere Performance verbessern.“

Petra Hermann,
Geschäftsführerin Plus PR

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.

Veranstaltungstipps

Expertenforum BCM

Am 17. September konstituiert sich unter dem Dach von NIFIS ein Expertenforum, das sich mit dem Themenkomplex Business Continuity Management (BCM) beschäftigt. Interessierte sind herzlich eingeladen, sich an der Gründung in Frankfurt am Main zu beteiligen, die Teilnahme ist nach vorheriger Anmeldung **kostenlos**.

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.

NIFIS möchte mit diesem Expertenforum eine Plattform schaffen, um gemeinsam Prozesse und Lösungen für BCM zu erarbeiten und somit einen schnelleren Einstieg in diese Problematik zu gewährleisten. Leiter des Forums ist Rolf von Rössing, der bei der KPMG Deutsche Treuhand AG das Thema BCM verantwortet und zudem im BCI-Vorstand der Chairman des Audit Committee ist. ❑

AK International

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. (DVPT) hat NIFIS deshalb einen Arbeitskreis International ins Leben gerufen, in dessen Rahmen sich Interessierte über die Erfahrungen im ITK- und Postbereich austauschen können. Erarbeitete Lösungsvorschläge werden anschließend allen Mitgliedern zur Verfügung gestellt. ►

In der ersten Sitzung im Juni 2007 wurden zunächst wichtige Themenfelder bestimmt, darunter Daten-Transfer über Grenzen hinweg (Safe-Harbour-Prinzip), Telefonie über das „ungeschützte“ Internet, Leistungsmerkmale von TK-Anlagen, Aus- und Einfuhrbestimmungen sowie SPAM und SPIT.

Um diese Themen zu vertiefen sowie neue Problemfelder zu diskutieren, lädt der AK International herzlich zur zweiten Sitzung am 19. September nach Offenbach am Main ein. Die Teilnahme ist nach Anmeldung **kostenlos** möglich, neue Interessenten sind herzlich willkommen. ❑

NIFIS unterstützt Webweiser 6.0

Bereits zum sechsten Mal lädt der Webweiser, die größte E-Business-Veranstaltung in Hessen, zu Expertengesprächen, Diskussionen und Workshops ein. Schloss Höchst ist am 12. September Schauplatz für die Themengebiete Online-Marketing, Recht und Sicherheit im E-Business sowie die Steuerung und Verbesserung von Geschäftsprozessen.

Die NIFIS-Vorstände Mathias Gärtner und Dr. Thomas Lapp halten jeweils einen Vortrag. Die Teilnahmegebühr beträgt 100 Euro pro Person und beinhaltet ein kulturelles und kulinarisches Rahmenprogramm. Veranstalter ist der NIFIS-Kooperationspartner BIEG Hessen. ❑

Wireless & Mobile Security 2007

Unterstützt von NIFIS findet vom 17. bis zum 19. September in Köln die Wireless & Mobile Security 2007 statt. 20 Experten diskutieren über die größten Gefahren im Umgang mit tragbaren Endgeräten und stellen ihre Strategien zur Absicherung der Geräte, sensibler Daten sowie drahtloser Netze vor. Zwei ganztägige Workshops, in denen technische Details vertieft werden, ergänzen das Forum. ❑

Günstiger an VO.IP teilnehmen

Am 30. und 31. Oktober findet in Frankfurt am Main die VO.IP Germany – Deutschlands wichtigste Kongressmesse für Voice- und IP-Kommunikation – statt. Die VO.IP Germany steht in diesem Jahr unter dem Motto „Konvergenz ist Chefsache" und hat sich zum Ziel gesetzt, einen umfassenden Überblick über den Entwicklungsstand, die Zusammenhänge und Auswirkungen in den Unternehmen zu geben. Durch die Programmbeteiligung von NIFIS erhalten die Mitgliedsunternehmen **25 Prozent Rabatt** auf den Eintrittspreis.

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

Kostenlose ITIL-Roadshow

Durch sechs deutsche Städte tourt im September die IT-Management-Roadshow von Controlware. Im Mittelpunkt der Veranstaltungsreihe steht „ITIL von der Theorie zur Praxis“. Gemeinsam mit verschiedenen IT-Service Management-Anbietern werden aktuelle Informationen zu ganzheitlichen ITIL-Lösungen präsentiert, um dabei zu helfen, Kosten zu senken und die Servicequalität zu erhöhen. Die Teilnahme ist **kostenlos**. ❑

NRW-Forschungstag IT-Sicherheit 2007

„Von der Forschung in den Markt: Wirtschaft und Wissenschaft im Dialog“ heißt es auch in diesem Jahr wieder beim „NRW-Forschungstag IT-Sicherheit 2007". Am 11. Oktober werden in Bochum Best-Practice-Beispiele und Erfolgsfaktoren für die Entwicklung innovativer IT-Sicherheitslösungen und marktnaher Forschungsprojekte vorgestellt. Die Teilnahme ist **kostenfrei**. ❑

Service

Expertenfrageecke

Risiken der Nutzung von Internet und E-Mail am Arbeitsplatz

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

In den Medien wird derzeit heftig darüber diskutiert, dass fast alle Mitarbeiter eines Unternehmens mit Internet-Zugang auch während der Arbeitszeit privat surfen und mailen. Was sind die Gefahren, die damit einhergehen, und wie sollte ein Geschäftsführer das Thema behandeln?


Dr. Thomas Lapp, NIFIS-Vorstand

Dr. Lapp: Vor allem besteht die Gefahr, dass Schadsoftware (Viren, Würmer, trojanische Pferde oder Spyware) durch die Mitarbeiter eingeschleust wird. Spyware soll sich inzwischen zur zweitgrößten Bedrohung im IT-Bereich entwickelt haben. Schadsoftware kann durch das Herunterladen von Daten, aber auch durch den Besuch von Webseiten oder die Nutzung von privaten, webbasierenden E-Mail-Diensten in das Netzwerk gelangen und erheblichen Schaden anrichten.

Unternehmen sind verpflichtet, IT-Risikomanagement zu betreiben. Werden keine ausreichenden Maßnahmen getroffen, kann dies zu einer persönlichen Haftung der Geschäftsführer oder Vorstände führen. Möglich sind technische Maßnahmen, wie eingeschränkte Rechte, um die Installation von Schadsoftware zu verhindern. Daneben sollten klare Regeln für die Nutzung von Internet und E-Mail sowie der Einsatz von geeigneter Filtersoftware zur Abwehr schädlicher Inhalte vertraglich vereinbart werden. Zudem sollten der Download und die Installation von Software sowie die Nutzung gefährlicher Dienste untersagt werden. Die Einhaltung derartiger Regeln muss regelmäßig kontrolliert werden, um zu verhindern, dass die Regeln wegen offensichtlicher Duldung von Verstößen ihre Wirkung verlieren. Ohnehin empfiehlt es sich, die Mitarbeiter regelmäßig an die Anforderungen der IT-Sicherheit zu erinnern. ❑

Experten im Interview

„Mit IAM versuchen wir, Struktur in das Chaos zu bringen.“

Dr. Angelika Steinacker ist seit über 20 Jahren auf dem Gebiet IT-Security tätig und bei der CSC Deutschland Solutions GmbH – einem der weltweit größten IT-Dienstleister – für das Thema Identity und Access Management (IAM) im deutschsprachigen Raum verantwortlich. Im Interview erklärt sie, was IAM ist, und warum sich Unternehmen damit auseinandersetzen sollten.

Prägnant auf den Punkt gebracht: Was genau ist IAM?

Steinacker: Das „I“ in IAM beschäftigt sich mit der Verwaltung aller Benutzer- und Berechtigungsinformationen in einem Unternehmen, das A mit dem Ausführen der Zugriffswünsche. Wenn Sie auf eine bestimmte Anwendung auf Ihrem Rechner zugreifen und Ihre Benutzerkennung sowie ein Passwort eingeben, dann steht das „A“ für diese Eingabe, und alles was diesbezüglich – hoffentlich für Sie im Verborgenen – abläuft.

Welche Identitäten werden beim Identity Management erfasst?

Steinacker: Das ist in jedem Unternehmen unterschiedlich. Es fallen die Informationen darunter, die dem Benutzer zugeordnet sind, zum Beispiel der Name und seine Funktion – all das, was benötigt wird, um zu entscheiden, worauf er zugreifen, was er anschauen, und womit er arbeiten darf. Wer in der Buchhaltung arbeitet, darf auf andere Programme und Daten innerhalb der Anwendungen zugreifen als jemand, der im Bestellwesen arbeitet. Aber auch gewisse Systeme wie Rechner oder Server können eine Identität haben, die erfasst werden muss. Hinzu kommen beispielsweise Informationen von Partnerunternehmen, sodass etwa Lieferanten auf bestimmte Daten zugreifen dürfen.

Es war aber doch schon immer klar: Ein Mitarbeiter muss auf die für ihn wichtigen Informationen zugreifen können, und wenn er das Unternehmen verlässt, muss dieser Zugriff verhindert werden. Warum ist das Thema IAM plötzlich ein so großes und wichtiges?

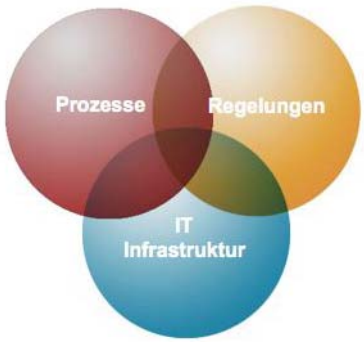
Steinacker: Die Idee ist nicht neu. Es gab schon immer Berechtigungskonzepte für einzelne Anwendungen oder Systeme. Aber erst in den letzten Jahren wurden die Anwendungen immer stärker miteinander vernetzt, auch über Unternehmensgrenzen hinweg. Die benötigten Informationen über einen Mitarbeiter, um ihm Zugriff auf bestimmte Anwendungen zu gewähren, wurden dadurch im Laufe der Zeit an vielen Stellen mehrfach und redundant gehalten. Außerdem wurden sie oft nicht gleichartig gepflegt. Mit IAM und dem, was dahinter steckt, versuchen wir nun, Struktur in dieses Chaos zu bringen. Neu daran ist das Ziel, über das gesamte Unternehmen hinweg einheitliche Strukturen zu schaffen, damit die Benutzer- und Berechtigungsverwaltung weniger aufwändig wird. ►

Was sind die größten Herausforderungen bei der praktischen Umsetzung?

Steinacker: Die größte Schwierigkeit ist, dass alle Beteiligten miteinander reden müssen. Früher hat der IT-Administrator die Daten verwaltet und – je nachdem wie gut die Prozesse organisiert waren – die Berechtigungen mehr oder weniger auf Zuruf vergeben. Die Berechtigungsstrukturen sind aber mittlerweile sehr komplex. Ein IT-Administrator ist gar nicht mehr in der Lage zu entscheiden, wer welche Berechtigungen für welche Aufgaben benötigt. Dies kann nur jemand sein, der das von der geschäftlichen beziehungsweise der fachlichen Seite her sieht. Involviert sind also die Endbenutzer, die Vorgesetzten, die IT-Abteilung, bei bestimmten Teilprozessen wie der Überprüfung von Zugriffsberechtigungen eventuell auch die Revision, das interne Audit. Wichtig ist auch, die HR-Abteilung einzubinden, weil diese viele der Informationen liefern kann und dadurch eine so genannte „goldene Quelle“ darstellt. All diese Beteiligten haben völlig unterschiedliche Sichten auf dieses Thema, und das größte Problem besteht darin, dass man Missverständnisse ausräumen und unterschiedliche Wünsche zwischen diesen Beteiligten unter einen Hut bringen muss.

Welche Unternehmen sollten sich mit IAM beschäftigen?

Steinacker: Meiner Meinung nach sollte sich jedes Unternehmen kritisch mit IAM auseinandersetzen. Wenn es dadurch seine Prozesse effizienter gestaltet und damit unnötige Arbeiten einspart, kann es schnell Effekte, insbesondere Gewinnsteigerungen, erzielen. Zudem gibt es Unternehmen, die unter gewisse Auflagen fallen, wie zum Beispiel SOX. Für die ist ein effizient und straff geführtes IAM unerlässlich, um bestimmte Nachweispflichten zu erfüllen. Die Berechtigungsverwaltung ist ein wichtiger Aspekt, um die Werte des Unternehmens zu schützen. Kein Unternehmen will, dass vertrauliche Informationen in die falschen Hände geraten. IAM zieht sich durch alle Branchen und hängt auch nicht allein von der Größe des Unternehmens ab, sondern von der Anzahl der Nutzer und der Anwendungen sowie den Berechtigungsstrukturen.



Kernkomponenten IAM

Das Gebiet ist sehr umfangreich. Wo fange ich am besten an?

Steinacker: Das kommt darauf an, was Sie bislang schon getan haben. Die meisten Unternehmen machen IAM bereits, denn jeder verfügt über eine Benutzer- und Rechteverwaltung. Die wenigsten gestalten diese jedoch über das ganze Unternehmen hinweg einheitlich. Wir empfehlen erst einmal eine kurze Bestandsaufnahme zu machen: Welche Prozesse können am ehesten optimiert werden, und in welcher Reihenfolge sollte vorgegangen werden? Hierbei kann die Unterstützung externer Experten hilfreich sein.

Wie viel Zeit nimmt das in Anspruch?

Steinacker: Die Bestandsaufnahme dauert meist nur wenige Wochen, bis erste greifbare Ergebnisse erzielt und Pläne für das weitere Vorgehen erstellt sind. IAM ist aber ein lebendiges Programm, das im Laufe der Zeit immer wieder angepasst werden muss. Umorganisationen, neue IT-Systeme und geschäftliche Anforderungen verändern die Berechtigungsstrukturen. Nachdem viele Unternehmen in den letzten Jahren im Wesentlichen Ad-hoc-Aktionen gestartet haben, sind mittlerweile immer mehr Unternehmen bereit, langfristig zu denken, da die kurzfristigen Aktionen auf Dauer mehr kosten.

Ist das Ergebnis von IAM dann „ein weiteres dickes Buch, das keiner liest“?

Steinacker: Nein, das soll sich natürlich nicht in einem dicken Buch widerspiegeln, sondern in den gelebten Prozessen. Der Endbenutzer möchte sich nur einmal anmelden und dann alle seine Anwendungen zur Verfügung haben. Die Revision will auf Knopfdruck von allen Mitarbeitern wissen, welche Berechtigungen sie zu welcher Zeit in welchem System haben. Der Geschäftsführer möchte die Häufigkeit der Passwortresets beim Helpdesk gerne um 30 Prozent senken, um Geld zu sparen. Wenn die Unternehmen wenige Anwendungen und überschaubare Größenordnungen haben, reicht eine kleine Datenbank, mit der sie die Informationen verwalten. Bei komplexeren Berechtigungsstrukturen lohnt es sich, für diese Verwaltung ein Tool einzusetzen. Die Erfahrung zeigt, dass die meisten Unternehmen sich kleine IAM-Komponenten selbst basteln, da für sie die Standarddatenbanken nicht mehr ausreichen. Spätestens dann ist es sinnvoll, sich auf dem Markt umzuschauen, was es dazu standardmäßig gibt. IAM heißt aber nicht, ein Tool zu kaufen und einzusetzen, sondern IAM besteht aus Prozessen, Regelungen und einer unterstützenden IT-Infrastruktur. Diese drei Komponenten müssen gut aufeinander abgestimmt sein, sonst nützt das beste Tool nichts.

Sie sind sehr engagiert im NIFIS-Expertenforum Identity Management. Warum?

Steinacker: Um sich gegenseitig zu unterstützen, die Erfahrungen, die man bei den einzelnen Projekten gemacht hat, auszutauschen, und so leichter effiziente Prozesse in Unternehmen und für Kunden zu erstellen. Die Mitglieder dieses Expertenforums haben im Laufe ihrer Arbeit festgestellt, dass es Ähnlichkeiten in diesen Prozessen gibt. Um dies für andere nutzbar zu machen, entwickeln wir gemeinsam ein Modell, das standardisierte IAM-Prozesse enthält.

Wir danken für dieses Gespräch! ❑

Spitzenpolitiker stehen NIFIS Rede und Antwort

„Welche Maßnahmen plant Ihre Partei zur Förderung der IT-Sicherheit in den Unternehmen?“

Dr. Martina Krogmann (CDU)

„Die wichtigsten Aufgaben der Politik sind Information und Beratung. Gerade in KMUs fehlt es oftmals an Problembewusstsein oder entsprechend ausgebildeten Fachkräften.

Von kostenlosen Handbüchern und Leitfäden bis hin zu Workshops und Pilotanwendungen reicht das Spektrum der Unterstützungsmaßnahmen – BSI, BMWi und BMI leisten hier vorbildliche Arbeit.

Diese Angebote können aber immer nur Hilfestellungen sein, denn letztendlich liegt das Thema IT-Sicherheit im Verantwortungsbereich der Unternehmen.“

Hans-Joachim Otto (FDP)

„Politischer Handlungsbedarf zur Herstellung oder Sicherung zuverlässiger und sicherer IT-Infrastrukturen beziehungsweise -anwendungen besteht in vielerlei Hinsicht: Ich denke da beispielsweise an einige Fehler, die bei der Reform des Computerstrafrechts gemacht wurden und an die weitere Verbesserung des Schutzes des geistigen Eigentums. Aber auch mittelbar müssen allgemeinere Defizite angegangen werden – wie beispielsweise die von der Großen Koalition vernachlässigten Rahmenbedingungen für einen starken Wettbewerb im TK-Infrastrukturmarkt.“

Silke Stokar von Neuforn (BÜNDNIS 90/DIE GRÜNEN)

„IT-Sicherheit und Datenschutz gehören zusammen. Nur, wer den Überblick über die eigenen Daten hat, kann ein IT-Sicherheits-Management aufbauen. Wir fordern ein modernes Bundesdatenschutzgesetz mit einem Online-Anwender-Handbuch.

Öffentliche Stellen und Unternehmen sollen verpflichtet werden, über Datenschutzpannen öffentlich zu informieren. Sichere Produkte und Dienstleistungen müssen durch ein gesetzlich geregeltes Zertifikat für Verbraucherinnen und Verbraucher klar erkennbar sein.“

NIFIS legt großen Wert auf Wissenstransfer und Erfahrungsaustausch zwischen Wirtschaft, Politik und Wissenschaft. Im Exekutivbeirat von NIFIS arbeiten die für das Thema Internet zuständigen Spitzenpolitiker parteiübergreifend zusammen, um die Sicherheit der deutschen Wirtschaft im Cyberspace zu erhöhen: Dr. Martina Krogmann (MdB CDU), Hans-Joachim Otto (MdB FDP), Jörg Tauss (MdB SPD) sowie Silke Stokar von Neuforn (MdB BÜNDNIS 90/DIE GRÜNEN). NIFIS möchte an dieser Stelle von den Experten unabhängig voneinander regelmäßig Lösungsvorschläge zu aktuellen Herausforderungen einholen. ❑

Sicherheitsupdate

Hacker nehmen Führungskräfte und deren Angehörige ins Visier

Das obere Management von Unternehmen gerät zunehmend ins Fadenkreuz von Cyberkriminellen. Der Security-Dienstleister MessageLabs verzeichnet eine drastische Zunahme an Angriffen, die auf einzelne Führungskräfte gerichtet sind.

Hacker haben offenbar die Führungsriege in Unternehmen als Angriffsziel für sich entdeckt. Nach dem „Intelligence Report" für Juni 2007 des auf E-Mail-Filtering spezialisierten Service-Anbieters MessageLabs richten sich immer mehr E-Mail-Attacken gezielt an einzelne Top-Manager in Unternehmen.

Allein am 26. Juni will der Messaging-Dienstleister mehr als 500 solcher Nachrichten abgefangen haben. Betroffen waren dem Report zufolge Manager auf der ganzen Welt. Nach einer Analyse der anvisierten Empfänger waren rund 30 Prozent der geblockten Mails an Personen mit dem Titel „Chief Investment Officers" und zehn Prozent davon an CEOs gerichtet, während knapp sieben Prozent der Nachrichten an CIOs beziehungsweise sechs Prozent an CFOs (Chief Financial Officers) adressiert gewesen sein sollen. Die restlichen 50 Prozent richteten sich laut Bericht an Forschungs- und Entwicklungsleiter sowie Geschäftsführer und Unternehmensvorstände.

Nach Angaben von Mark Sunner, Chief Security Analyst bei MessageLabs, wurden im Mai 2007 täglich im Schnitt zehn solcher an Personen im gehobenen Management adressierten Mails abgefangen. Im Vorjahr sei es lediglich eine Nachricht pro Tag gewesen. ►

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.

Gemessen an den 200 Millionen Mails, die MessageLabs täglich scanne, sei das Aufkommen zwar eher gering, räumt der Experte ein. Beunruhigend sei vielmehr die Beschaffenheit dieser Messages, die nach Angaben des Dienstleisters persönliche Details wie Namen und genaue Stellenbezeichnungen der Zielpersonen sowie ein Microsoft-Word-Dokument mit ausführbarem Code im Anhang enthielten. Wer es öffnet, aktiviert einen Trojaner, der den Opferrechner in Beschlag nimmt.

Um Zugriff auf vertrauliche Korrespondenz und geistiges Eigentum zu erlangen, hat es laut MessageLabs aber auch Nachrichten gegeben, deren anvisierte Empfänger mit der eigentlichen Zielperson des Angriffs in Beziehung standen – etwa Ehepartner oder andere Familienangehörige. Der aktuelle Trend deute darauf hin, dass Kriminelle im Hinblick auf ihre Opfer mittlerweile Recherche betreiben und sich möglicherweise auf Social-Networking-Sites wie Linked-In, MySpace oder Face Book gezielt Daten herauspickten, erläutert Sunner. „Wer wirklich etwas über den Hintergrund einer Person erfahren will, findet auf diesem Weg eine Menge."

Die Herkunft der jeweiligen Mails zu ermitteln, ist laut Sunner aufgrund der stets gefälschten Absendernamen schwierig. Die IP-Adressen, von denen sie verschickt worden seien, deuteten jedoch auf weltweit verstreute Computer hin.

Katharina Friedmann, 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 +++
http://www.fresh-info.de