Liebe NIFIS-Mitglieder,

sehr geehrte Interessenten und Förderer,

durch die Diskussionen über die geplante Online-Durchsuchung und den so genannten Bundestrojaner sowie insbesondere die Entscheidung des Bundesverfassungsgerichts ist der Schutz personenbezogener Daten wieder stärker ins Blickfeld geraten. Spitzelskandale bei Unternehmen wie Lidl oder Deutsche Telekom haben dazu ebenfalls beigetragen. Bündnis90/Die Grünen wollen fünf der 19 Grundrechtartikel der Verfassung um das Recht auf informationelle Selbstbestimmung erweitern und haben dazu einen entsprechenden Gesetzentwurf vorbereitet.

Handlungsbedarf für den Gesetzgeber ist, über eine eventuelle Grundgesetzänderung hinaus, reichlich vorhanden. Regelungen zum Datenschutz für Arbeitnehmer werden genauso schmerzlich vermisst, wie datenschutzrechtliche Regelungen für Rechtsanwälte und andere Freiberufler und ein gesetzlicher Rahmen für Datenschutz-Audits.

Wollen wir die Aufbruchstimmung verstärken und nicht im Keim ersticken, müssen wir jedoch bald einen Begriff finden, der mehr Identifizierungspotenzial bietet, als „Datenschutz" oder „Datenschutzrecht". Sicher hat das Bundesverfassungsgericht in seiner Entscheidung bewusst auf diese Begriffe verzichtet. Richtig sexy ist allerdings auch der vom BVerfG verwendete Begriff Schutz von „Integrität und Vertraulichkeit informationstechnischer Systeme“ nicht. Dennoch sollten wir die Kraft von Begriffen nicht vernachlässigen und Energie in die Suche nach einer neuen und identitätsstiftenden Bezeichnung investieren. Unserem Anliegen, personenbezogene Daten vor Missbrauch zu schützen, würde dies gut tun.

Diese Ausgabe von NIFIS advice hat einen Schwerpunkt im Datenschutzrecht. Ich wünsche Ihnen viel Spaß bei der Lektüre der Beiträge.

Dr. Thomas Lapp
NIFIS-Vorstand

HIGHLIGHTS

NIFIS inside

Expertenforum BCM startet durch

Das Expertenforum BCM beschäftigt sich mit der betrieblichen Kontinuität im weitesten Sinne, geht jedoch insbesondere auf die Belange der NIFIS ein. In den vergangenen Sitzungen wurden unterschiedliche Themen behandelt, die in konkreten Arbeitsaufträgen ihren Niederschlag gefunden haben. Diese reichen von der eigentlichen BCM-Methodik bis zur bestehenden Vorschriftenlage in den deutschsprachigen Ländern. Die Ansprache neuer potenzieller Mitglieder erfolgt nunmehr auch über eine Gruppe in XING (NIFIS Business Continuity Management Arbeitskreis), die mittlerweile auf über 50 Mitglieder gewachsen ist. Dieses Instrument wird für den Gedankenaustausch und die Terminplanung verwendet.

Zwischenzeitlich wurde insbesondere die Zusammenarbeit mit der deutschen Organisation des internationalen Business Continuity Institute (BCI) in bestem Einvernehmen geregelt. Aufgrund der speziellen Ausrichtung der NIFIS ► sind in der Kooperation mit dem BCI erhebliche Synergien gegeben, die sich beide Organisationen zunutze machen wollen. Beispielsweise ist geplant, gemeinsame Veranstaltungen des Expertenforums und des BCI-Regionalforums Mitte durchzuführen.

Aufgrund besonderer Entwicklungen und Veränderung in der Sponsorenstruktur war es unvermeidlich, die Aktivitäten der Gruppe zu überdenken; dies führte im ersten Halbjahr 2008 zu einer schöpferischen Pause. Mittlerweile hat der Vorstand der NIFIS hierzu klare und positive Beschlüsse getroffen, die unmittelbar zu einer Wiederaufnahme der Aktivitäten geführt haben. Im Sinne dieses Neuaufbruchs ist der nächste Sitzungstermin unmittelbar nach Ende der hessischen Sommerferien geplant; entsprechende Terminvorschläge sind in der XING-Gruppe einsehbar.

Das Expertenforum wünscht sich ausdrücklich weitere Mitglieder, um eine möglichst weit gefasste Erfahrung aus vielen Branchen und Perspektiven sicherzustellen.
Bei Interesse können Sie sich gerne auch an newsletter@nifis.de wenden. ❑

NIFIS sponsert IM-Diplomarbeit

Die GenericIAM Gruppe bietet die Chance für eine Diplomarbeit, die von NIFIS gesponsert wird, zum Thema: „Prozessanalyse im Bereich der Enterprise Identity Management Systeme – Analyse, Ableitung und Entwicklung einer Prozesslandkarte“. Die Diplomarbeit soll im Umfeld des EIdM für Unternehmen die Erfassung und Qualifizierung spezieller Lösungsmodelle im Bereich der Prozesse, Objekte, sowie deren Attribute und Relationen als Aufgabe haben.

Dabei sollen anhand von in der Praxis durchgeführten Fallstudien Gemeinsamkeiten ermittelt werden, die später zur Ableitung von generischen Prozessen und Modellen im Bereich des EIdM dienen sollen. Die Arbeit selbst gliedert sich dabei in diverse Module.

Weitere Details zu der Ausschreibung gibt es hier; bei Fragen oder Interesse wenden Sie sich bitte an newsletter@nifis.de. ❑

Expertenforum IM lädt ein

Das 11. Treffen des NIFIS-Expertenforums Identity Management (IM) findet am 26. September von 10 bis 17 Uhr in Frankfurt statt. Dabei gibt es wieder ausführliche Berichte aus den einzelnen Arbeitsgruppen Organisation (Horst Walther), Modelling (Marc Dierichsweiler), Validation (Angelika Steinacker) und Presentation (Peter Weierich).

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 zeigt Wirkung

Die Claranet GmbH hat erneut die Zertifizierung mit dem NIFIS-Siegel beantragt. Bereits vor einem Jahr hatte das Unternehmen erfolgreich den umfassenden Sicherheitscheck mit dem Selbstauditverfahren absolviert. „Bei der Beantwortung des Fragenkatalogs wurden uns Aspekte bewusst, die wir daraufhin verbessert haben“, erklärt Uli Schunk, Marketing Executive bei Claranet. „In punkto ‚Sicherheit im Rechenzentrum’ wurde beispielsweise nach einem relevanten System für Notfallkühlung gefragt, über das wir bislang nicht verfügten. Inzwischen haben wir eine redundante Auslegung der Systeme in unserem Rechenzentrum eingeführt.“

Das neue Kühlsystem im Claranet Rechenzentrum arbeitet nach dem Prinzip der n+1-Konstellation und gewährleistet ein permanent optimales Klima. Bei Ausfall eines der andauernd aktiven Klimamodule greift diese Technik automatisch auf ein zusätzliches Modul zurück, womit der notwendige Kühlkreislauf weiterhin aufrecht gehalten wird. Der Themenpunkt ‚Benutzerrichtlinien’ im Fragebogen führte zu Verbesserungen innerhalb der Informations-Kommunikation bei Claranet. Seit einem Jahr führt Claranet nun ein Wiki als interne Wissensdatenbank, in der schriftliche Richtlinien zum Umgang und zur Bedienung der Systeme fixiert werden.

„Diese Verbesserungen führen wir unter anderem auf das NIFIS-Siegel zurück“, betont Schunk. Insgesamt enthält der Katalog des Selbstauditverfahrens 82 Fragen aus den Bereichen organisatorische, logische, technische sowie physikalische Sicherheit. ►

Aber nicht nur intern hatte das Siegel für Claranet Auswirkungen. Das Unternehmen dokumentiert damit extern seinen hohen Sicherheitsstandard gegenüber Presse, Kunden und Geschäftspartnern, zum Beispiel auf der Website und in Marketingunterlagen.

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 zum NIFIS-Siegel 150 Euro.

Weitere Informationen erhalten Sie hier. ❑

NEUE MITGLIEDER

„Die Henkel AG & Co. KGaA ist mit ihren drei Unternehmensbereichen ‚Wasch- und Reinigungsmittel', ‚Kosmetik und Körperpflege' sowie ‚Klebstoff Technologie' in weltweit 125 Ländern vertreten und damit eines der am stärksten international ausgerichteten Unternehmen in Deutschland. Die Henkel IT betreibt seit dem Jahr 1992 eine zentrale Provisioninglösung.

Bis 2005 war eine Eigenentwicklung im Einsatz, seit 2005 nutzen wir eine zweite Produktlösung mit Metadirectory und Userprovisioning. Von der NIFIS-Mitgliedschaft erwartet Henkel im Bereich des IAM einen Wissens- und Informations-Austausch mit anderen Unternehmen, um die eingesetzte Lösung möglichst auf einem aktuellen Stand der Technik zu halten. Aus diesem Grund ist Henkel auch an einer aktiven Teilnahme sehr interessiert.“

Roland Stahl
Henkel AG & Co. KGaA
FI/RSC D User Management

Veranstaltungstipps

3. Mobile & Wireless Security Forum

Am 16. und 17. September findet das 3. Mobile & Wireless Security Forum mit NIFIS-Unterstützung in Köln statt, das wieder über aktuelle Themen und Trends beim Einsatz mobiler Endgeräte und drahtloser Netze informiert. In zwölf Fach- und Expertenvorträgen erfahren die Teilnehmer, wie sie ihre Endgeräte absichern und Smartphones sowie PDAs sicher in ihre Unternehmens-IT integrieren.

Zudem berichten Experten darüber, wie sie WLANs sicher aufbauen und betreiben, und was sie bei einer Sicherheitsprüfung per White Hacking beachten müssen. ►

Ebenfalls thematisiert werden unter anderem Risikomanagement bei mobilen Endgeräten und User Education.

Ein besonderes Highlight ist das Live War Driving durch Köln, bei dem SySS-Geschäftsführer Sebastian Schreiber ungesicherte WLANs und offene Access Points in der Stadt aufspürt.

Zudem befasst sich ein ganztägiger Workshop am 18. September eingehend mit sicherer mobiler Kommunikation und mit Managed Wireless Enterprise Security. ❑

IT-Management Roadshow 2008

Controlware tourt im September mit der Veranstaltungsreihe „ITIL von der Theorie zur Praxis“ durch sechs deutsche Städte. Im Mittelpunkt stehen dabei nicht die schon häufig erklärten Inhalte von ITIL V3, sondern konkrete Praxiserfahrungen. Namhafte IT-Service-Management-Anbieter berichten über ihre Erkenntnisse bei der Implementierung von ITIL-Prozessen und geben Tipps, um die Aufwendungen für den Kunden überschaubar zu machen.

Die Veranstaltung richtet sich an alle, die durch ITIL-Prozesse Kosten senken und die Servicequalität erhöhen möchten. Die Teilnahme ist **kostenfrei**. ❑

Service

Expertenfrageecke

Wie schütze ich meine Daten auf einem Laptop?

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

Laptops, sowie alle anderen mobilen Geräte, stellen eine große Herausforderung für die Datensicherheit dar, denn sie verlassen sehr häufig den geschützten Bereich des eigenen Büros. Studien zeigen, dass eine erhebliche Anzahl von Datenträgern und Laptops in Taxis vergessen werden. Alleine bei den Behörden wurden im letzten Jahr in Deutschland 400 Laptops als verloren oder verschwunden gemeldet. Wie viele bei Firmen verloren gegangen sind, ist statistisch gar nicht erfasst.

Wichtig ist, dass hier nicht nur die mobilen Geräte, sondern vor allem auch die darauf gespeicherten, teilweise sehr sensitiven Daten in fremde Hände gelangt sind. Damit Unbefugte bei direktem Zugriff auf das Gerät die Daten nicht lesen können, müssen diese besonders geschützt werden. Dies kann am besten durch Verschlüsselung erreicht werden. Dabei gibt es zwei verschiedene Varianten: Zum einen kann die Datei selbst verschlüsselt werden, zum anderen die gesamte Festplatte beziehungsweise Partition.

Mathias Gärtner, NIFIS-Vorstand

Die erste Methode der Einzelverschlüsselung klingt zunächst sinnvoll, denn hier braucht nur das verschlüsselt werden, was wirklich wichtig ist. Allerdings muss man hier immer eine Auswahl treffen, was wichtig ist und was nicht. Dieser Entscheidungsprozess überfordert oftmals. Auch werden hierbei die Eigenheiten der verwendeten Betriebssysteme, zumeist Windows, vernachlässigt. So erzeugt das MS-Office Paket sehr viele Datenspuren außerhalb der Verschlüsselung, wenn eine Datei geöffnet wurde. Ein halbwegs erfahrener Forensiker ist somit in der Lage, den Inhalt einer verschlüsselten Datei zu lesen, weil eben Spuren davon nicht verschlüsselt, zum Beispiel als temporäre Datei, vorliegen. Zudem muss bei der Einzelverschlüsselung jede Datei bei Verwendung durch Eingabe des Passwortes wieder einzeln entschlüsselt werden.

In der zweiten Variante wird hingegen alles verschlüsselt, auch die unwichtigen Daten und temporären Dateien. Damit entfällt auch das Problem der Auswahl. Ich empfehle daher generell, die gesamte Festplatte mit geeigneten Werkzeugen zu verschlüsseln. Das hat noch einen weiteren Vorteil: Der Benutzer muss lediglich einmalig beim Starten des Systems ein Entschlüsselungspasswort eingeben und kann dann ungestört arbeiten. ❑

Praxistipp

Maßnahmen zum IT-Grundschutz

NIFIS-Mitglied Thomas Teichmann von der Schmitz & Teichmann Betriebsberatung GmbH erläutert aufgrund eines aktuellen Vorfalls Details zum IT-Grundschutz und verrät konkrete Maßnahmen.

In einem Bericht des ARD-Fernsehmagazins „Report“ wurden offene Zugänge zu Daten bei den Meldeämtern verschiedener Städte und Gemeinden festgestellt. Der vermeintlich Schuldige für den schwerwiegenden Fall der Verletzung des Datenschutzes war schnell gefunden: der Softwarelieferant. Doch die Verantwortung für die Einhaltung des Datenschutzes liegt beim Betreiber eines Informations-Systems, nicht beim Lieferanten. Wenn eine Behörde oder ein Unternehmen eine Datenbank mit personenbezogenen Daten einrichtet, müssen die Verantwortlichen auf die Einhaltung von Datenschutzbestimmungen achten und bestehen. Wer unsicher ist, sollte sich informieren, einen Berater hinzuziehen oder bei NIFIS nachfragen.

Thomas Teichmann, Geschäftsführer Schmitz & Teichmann

In diesem spektakulären Fall lag für das installierte System ein Kurzgutachten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein vor, das dem System eine datenschutzrechtlich einwandfreie Funktionsweise attestiert. Das ist gut, aber es bezieht sich auf das Grundsystem und Konzept, nicht auf die einzelne Installation in einem Meldeamt. Was die Datenschutzprüfer nicht zu prüfen hatten, und nicht ahnen konnten, ist, dass die Installateure das System wohl regelmäßig mit einem Standardbenutzer und Standardstartkennwort installierten, und die Kommunen es dabei beließen, und in vielen Kommunen weder Datenschutz noch IT-Grundschutz geprüft wurden. Startkennworte, die bei Lieferung und Installation eines Systems eingesetzt werden, sind generell unsicher. Zu viele Leute, vom Entwickler bis zu Pilotanwendern, kennen diese Zugangsdaten. Es gibt spezialisierte Websites für Standardkennworte. Daher wird ein erfahrener Softwareinstallateur nicht nur empfehlen, diese Zugangsdaten direkt nach der Installation zu ändern, er wird darauf bestehen.

Aber es gibt noch weitere grundsätzliche Maßnahmen, um Datenschutz und IT-Sicherheit zu verbessern. Beispielsweise sollte noch vor der ersten Installation ein Konzept für die Verwaltung der Benutzerrechte, Benutzernamen und Kennworte erstellt werden, etwa als Teil des Pflichtenhefts. Mit der ersten Übernahme „echter" Daten sollte in demselben Zug nur noch mit Benutzernamen und Kennworten nach dem Rechtekonzept gearbeitet werden.

Die ausführliche Übersicht der empfohlenen Maßnahmen zum IT-Grundschutz gibt es hier. ❑

Spitzenpolitiker stehen Rede und Antwort

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 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 und Meinungen zu aktuellen Herausforderungen einholen.

Zur Aufnahme der informationellen Selbstbestimmung in das Grundgesetz

Die Fraktion Bündnis 90/Die Grünen hat sich zur Aufgabe gemacht, den Schutz der Grundrechte, im Hinblick auf den durch die neuen Entwicklungen der heutigen Informations-Gesellschaft überkommenen Grundrechtskatalog, sicherzustellen. Dies blieb bisher dem Bundesverfassungsgericht vorbehalten wie im Volkszählungsurteil oder zuletzt beim Urteil zur Online-Durchsuchung. Aber nicht nur das Recht auf informationelle Selbstbestimmung, auch die Informations-Freiheit, der absolute Schutz des Kernbereichs privater Lebensgestaltung sowie der Schutz von technischen Informations-Systemen sollen in das Grundgesetz integriert werden.

„Es ist an der Zeit, dass der (Verfassungs)Gesetzgeber die informationelle Selbstbestimmung endlich in das Grundgesetz aufnimmt. Deshalb hat meine Fraktion als erste einen Gesetzentwurf dazu vorgelegt (BT-Drs. 16/9607). Damit wird dieses elementare Grundrecht allgemein verständlicher und der tatsächlichen Bedeutung des Datenschutzes in der heutigen IT-Gesellschaft besser gerecht.

Der Kern des Grundrechts auf informationelle Selbstbestimmung ist durch die jahrzehntelange Rechtsprechung des Bundesverfassungsgerichts hinreichend klar umschrieben. Sie ist gleichsam die Füllung des Datenschutzartikels, den wir vorschlagen. Dazu gehören unter anderem der Grundsatz der Datensparsamkeit und die Zweckbindung.“

SILKE STOKAR VON NEUFORN (Bündnis 90/Die Grünen)

Zum Entwurf des Bundesdatenschutzauditgesetzes

Ausgangspunkt des Gesetzgebungsvorhabens zu einem Bundesdatenschutzauditgesetz ist § 9 a BDSG, der die gesetzliche Regelung eines Audits ermöglicht. Ziel ist es, einen adäquaten wirtschaftlichen Mehrwert bei der Einhaltung des Datenschutzrechtes für die Unternehmen zu schaffen. Es soll von den Unternehmen öffentlichkeits- und werbewirksam eingesetzt werden können.

„Datenschutz als Grundrechtsschutz ist eine unverzichtbare Funktionsbedingung für jegliches demokratisches Gemeinwesen. Gewährleistet ist ein solcher Grundrechtsschutz nur dann, wenn die Erhebung, Speicherung und Nutzung von personenbezogenen Daten grundsätzlich der freien Selbstbestimmung unterliegen. Angesichts der technologischen Entwicklungen mit ständig wachsenden Datenbeständen und einer zunehmenden Vernetzung ist dies wichtiger denn je. Der zunehmenden Konvergenz der Technik muss eine Konvergenz des Datenschutzrechtes folgen, ohne dabei das bestehende Schutzniveau abzusenken.

Ein Bundesdatenschutzauditgesetz ist ein erster wesentlicher Baustein hin zu einer Fortentwicklung des Datenschutzes von einem reinen Instrument der Eingriffsverwaltung hin zu einem auf die globalisierte Marktwirtschaft abgestimmten modernen Steuerungsinstrument des präventiven Datenschutzes. Ein qualitätsgesichertes Datenschutzaudit bildet ein Instrument zur Implementierung einer Win-win-Situation, und stellt zugleich einen Kernaspekt eines neuen Datenschutzverständnisses dar.“

JÖRG TAUSS (SPD)

NIFIS begrüßt das Gesetzesvorhaben grundsätzlich, beleuchtet jedoch in einer Stellungnahme einzelne Punkte im Entwurf kritisch.

Sicherheitsupdate

Datenmissbrauch wird zu spät entdeckt

Meist bemerken Unternehmen erst Monate nach einem Datenverlust, dass ihre Informationen kompromittiert wurden. Das Gros der Verstöße ist dabei nicht etwa Insidern, sondern externen Quellen wie Geschäftspartnern zuzuschreiben. Das ergab eine Langzeituntersuchung von Verizon Business.

In drei Viertel aller Fälle von Datenmissbrauch kommt es bereits innerhalb von Tagen zur Kompromittierung der Daten, 63 Prozent der Vorfälle werden allerdings erst Monate später entdeckt. Das ergab der „2008 Data Breach Investigation Report" von Verizon Business, der auf rund 500 forensischen Untersuchungen anhand von 230 Millionen Datensätzen im Zeitraum zwischen 2004 und 2007 basiert. Bis die Datenlecks dann gestopft waren, dauerte es der Analyse zufolge in fast jedem zweiten Fall Wochen – nur bei 37 Prozent wurden die undichten Stellen bereits innerhalb von Stunden oder Tagen behoben. Hinzu kommt, dass 75 Prozent aller Datenverluste nicht von den betroffenen Organisationen selbst, sondern von Dritten aufgedeckt wurden.

Dabei ging die überwiegende Mehrheit der Verstöße nicht etwa von Insidern wie Mitarbeitern oder IT-Administratoren (18 Prozent), sondern von externen Quellen aus (73 Prozent). Erstaunliche 39 Prozent dieser Fälle sind dem Report zufolge Geschäftspartnern zuzuschreiben – die Zahl dieser Verstöße soll im Untersuchungszeitraum von vier Jahren um das Fünffache gestiegen sein.

Dabei werden die meisten Datenverluste offenbar durch eine Kombination von Faktoren und weniger durch einzelne Hacker-Angriffe ausgelöst. So waren 62 Prozent der Fälle auf schwere interne Fehler zurückzuführen, die direkt oder indirekt zu dem Datenverlust beitrugen, während es sich bei 59 Prozent um Hacking oder versuchte Systemeinbrüche handelte. 39 Prozent der Hacker-Attacken waren auf die Anwendungsebene gerichtet, nur 23 Prozent zielten auf das Betriebssystem. Laut Studie nutzten 18 Prozent dieser Angriffe eine bereits bekannte Schwachstelle aus, wobei für 90 Prozent dieser Sicherheitslücken schon gut sechs Monate vor dem Verstoß Patches zur Verfügung standen.

Unter dem Strich, so die Verizon-Experten, hätten sich neun von zehn Fälle von Datenmissbrauch in Unternehmen und Behörden durch angemessene Sicherheitsvorkehrungen verhindern lassen. ►

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.

Von Datenmissbrauch besonders gebeutelt werden offenbar der Einzelhandel sowie die Getränke- und Lebensmittelindustrie: Diese Branchen waren laut Studie von gut der Hälfte der analysierten Fälle betroffen. Auf den traditionell gut geschützten Finanzdienstleistungssektor entfielen indes nur vier Prozent der Vorkommnisse. Bei den Angriffen aus Asien – speziell China und Vietnam – wurden laut Bericht häufig Lücken in Applikationen ausgenutzt, während Website-Defacements vorwiegend auf Attacken aus dem Nahen Osten zurückzuführen waren. IP-Adressen aus Osteuropa und Russland wiederum standen oft hinter der Kompromittierung von Point-of-Sale-Systemen. (kf)

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