Liebe NIFIS-Mitglieder,

sehr geehrte Interessenten und Förderer,

verbunden mit den besten Wünschen für 2008 begrüße ich Sie zur ersten Ausgabe von NIFIS advice in diesem Jahr.

Unsere Initiative zählt mittlerweile rund 50 Firmenmitglieder sowie eine Reihe an Förderern, Unterstützern und Kooperationspartnern aus dem gesamten Bundesgebiet, die durch ihre aktive Mitarbeit in den vergangenen Jahren dazu beigetragen haben, NIFIS als Kompetenzzentrum für Informations- und Internet-Sicherheit zu positionieren und zu etablieren.

Als Ziel für das Jahr 2008 haben wir uns vorgenommen, die tiefgründige inhaltliche Arbeit in den Expertenforen weiter fortzusetzen und durch weit reichende Kooperationsprojekte mit Partnern und Medien zu begleiten. Parallel soll die Mitgliederbasis verbreitert werden, um die Aktivitäten der Initiative auch weiterhin erfolgreich gestalten und langfristig aufrechterhalten zu können.

Sollten Sie noch kein Mitglied der NIFIS sein, dann sind Sie herzlich eingeladen, sich an unseren vielfältigen Aktivitäten zu beteiligen und sich unserer Initiative in Form einer Mitgliedschaft anzuschließen.

Ich freue mich auf ein spannendes und ereignisreiches Jahr 2008 und wünsche Ihnen viel Spaß beim Lesen!

Peter Knapp

Vorstandsvorsitzender der NIFIS

HIGHLIGHTS

NIFIS inside

NIFIS kooperiert mit EC-M

NIFIS und das EC-M Beratungszentrum Elektronischer Geschäftsverkehr Mittelhessen sind eine Kooperation eingegangen. Das EC-M arbeitet seit 1998 erfolgreich daran, die Entwicklung des elektronischen Geschäftsverkehrs von Unternehmen in Mittelhessen zu fördern.

Dabei unterstützt das EC-M als ein Knoten des Netzwerks Elektronischer Geschäftsverkehr gezielt kleine und mittelständische Unternehmen in der Region bei der Einführung moderner Informations- und Kommunikationstechnologien. Die persönlichen Beratungen, Seminare, Workshops und Vorträge werden neutral und in der Regel **kostenlos** durchgeführt. ❑

Datenschutzauditgesetz im Fokus

Am 13. Februar laden NIFIS und DVPT herzlich zur zweiten Sitzung des Arbeitskreises Datenschutz ein. Diese findet ab 10 Uhr in Offenbach statt. Im Mittelpunkt des Treffens stehen das Datenschutzauditgesetz sowie das Thema Awareness. Die Teilnehmer wollen diskutieren, wie das Bewusstsein für Anforderungen des Datenschutzes gestärkt werden kann. Nach der ausführlichen Erörterung ist das Abfassen einer gemeinsamen Stellungnahme geplant. Zu der **kostenlosen** Veranstaltung können Sie sich hier anmelden. ❑

AK International diskutiert VoIP

Zum vierten Mal trifft sich der Arbeitskreis International, den NIFIS ebenfalls in Zusammenarbeit mit dem DVPT durchführt. Bei der Veranstaltung am 13. Februar ab 14 Uhr in Offenbach gibt es einen Überblick über die bereits besprochenen Themen. Ausführlich diskutiert wird diesmal der Einsatz von VoIP im In- und Ausland und das in technischer, organisatorischer und rechtlicher Hinsicht. Die Anmeldung zu dem **kostenlosen** Treffen ist online möglich. ❑

NIFIS-MITGLIEDERVERSAMMLUNG

Am Nachmittag des 16. April 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 werden den Mitgliedsunternehmen separat zugestellt.

Expertenforum IM lädt zu neuem Treffen

Am 8. Februar trifft sich das NIFIS-Expertenforum Identity Management (IM) in Frankfurt am Main. Besprochen wird dabei unter anderem eine veränderte Struktur in der Zusammenarbeit. „Der persönliche Austausch ist sehr wichtig, ich würde aber gerne stärker virtuell gemeinsam Inhalte erarbeiten, in unserer Diskussionsgruppe und im Blog. Dadurch können wir auch besser interessierte internationale Teilnehmer, beispielsweise aus Indien oder Israel, effektiver einbinden“, erklärt Dr. Horst Walther, der den Vorsitz des IM-Expertenforums innehat.

Das Expertenforum ist seinem Ziel, ein Referenzmodell mit typischen generischen Prozessen für das Identity- und Access Management zu erarbeiten, bereits einen großen Schritt näher gekommen. In einem Papier haben die Teilnehmer den NIFIS-Ansatz zur Entwicklung von generischen Identity- und Access-Management-Prozessen auf Basis einer Variante eines Zustandsübergangsmodells (so genannte gefärbte Petri-Netze) veröffentlicht.

Um eine feste Basis zu haben, gingen die Experten dabei von den fundamentalen Objekten in Unternehmen aus, die mit IM zu tun haben, wie die Identität, die Organisation, die Rolle usw.. Dann wurden die Beziehungen zwischen diesen Objekten ermittelt bis schließlich ein vollständiger Satz an generischen Objekten im Unternehmen bestand.

Aus deren Aktionen wurden dann Elementaraktivitäten abgeleitet und daraus die Prozesse (Top-Down) zusammengesetzt. An einem Beispiel, dem Prozess „approve request” (Antrag genehmigen), präsentierten die Experten dann ein vollständiges Modell in Form eines gefärbten Petri-Netzes. Zur besseren Verständlichkeit wurde dies zusätzlich in Form einer Ereignisprozesskette dokumentiert. ►

Unternehmen können durch dieses Papier leichter ihre Prozesse identifizieren sowie beschreiben und IAM-Projekte mit deutlich reduziertem Aufwand zum Erfolg führen. Sie können damit Verhaltensmuster erkennen und auch die Vollständigkeit von Prozessen überprüfen.

Als nächste Schritte möchte das Expertenforum IM weitere Prozesse wie „approve request” in dieser geeigneten Weise ableiten und darstellen. Ziel ist es, einen Satz von etwa 20 Prozessen zu erarbeiten, die immer wieder auftreten und die interessierte Unternehmen nur noch in ihre spezifischen Bezeichnungen (zum Beispiel Namen und Stellen) umwandeln müssen.

Neue Teilnehmer am Expertenforum IM sind jederzeit herzlich willkommen. Wenden Sie sich hierzu einfach an newsletter@nifis.de. ❑

NIFIS begrüßt neue Mitglieder

NIFIS ist prinzipiell für alle Unternehmen und Personen offen, die sich für die Themen Informations- und Internet-Sicherheit interessieren und versteht sich als Ansprechpartner bei Fragen oder Problemen der Mitglieder. Weitere Informationen finden Sie hier.

„Als unabhängiges Beratungshaus mit den Schwerpunkten Identity- und Access-Management sowie serviceorientierte Architektur machen wir oft die Erfahrung, dass IT-Sicherheit als wenig geschäftsrelevant angesehen und aus Kostengründen vernachlässigt wird. Im Vordergrund unserer Arbeit steht daher, Sicherheit weitgehend zu industrialisieren, zu standardisieren und in die Geschäftsprozesse zu integrieren. Als eines der ersten Mitglieder der Generic IAM bietet uns NIFIS eine gute Plattform für den Erfahrungsaustausch und die Arbeit an der Standardisierung von Prozessen.“

Jens Petersen, Geschäftsführer FirstAttribute GmbH

„Die sichere Ver- und Bearbeitung von Informationen und Daten ist heutzutage für nahezu alle Unternehmen und Behörden, aber insbesondere für mittelständische Betriebe, von existenzieller Bedeutung. Der BVMW, der sich als die „Stimme des Mittelstandes“ versteht, wird durch seine Mitgliedschaft in der NIFIS befähigt, den Unternehmen im Kampf gegen diese wachsenden Gefahren, technische, organisatorische und rechtliche Hilfestellung zu leisten, um seiner Informationspflicht noch besser gerecht zu werden.“

Gerhard Kaspar-Holthaus, Geschäftsführer Metropolregion Wiesbaden / Frankfurt am Main BVMW Bundesverband mittelständische Wirtschaft Unternehmerverband Deutschlands e.V.

„Die tekit Consult Bonn berät und zertifiziert Unternehmen in der Telekommunikation und IT. Innerhalb des Kompetenzzentrums der NIFIS möchte die tekit ihr Know-how einbringen und gleichzeitig im Expertenkreis sicherstellen, dass ihre Anforderungskataloge zum Beispiel für die Zertifizierung von Rechenzentren praxisgerecht gestaltet sind. Neben der Sicherheit von Prozessen und Produkten hat die Energieeffizienz im Rechenzentrumsbetrieb und IT-Einsatz besondere Aufmerksamkeit.“

Guido Hermanowski, Leiter Vertrieb tekit Consult Bonn GmbH (TÜV Saarland Gruppe)

Telepunkt wird rezertifiziert

Telepunkt darf für weitere zwölf Monate das NIFIS-Siegel führen. 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. ►

Damit kann Telepunkt nun einen hohen Sicherheitsstandard gegenüber Kunden, Mitarbeitern und Geschäftspartnern belegen und sich einen Wettbewerbsvorteil sichern. Für NIFIS-Mitglieder ist der Erwerb des Siegels ebenso wie die Rezertifizierung **kostenfrei** möglich. Für Nicht-Mitglieder kostet das Selbst-Audit 150 Euro; weitere Informationen erhalten Sie hier. ❑

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.

Veranstaltungstipps

München: 2nd European Identity Management Conference

Vom 22. bis zum 25. April veranstaltet das NIFIS-Mitglied Kuppinger Cole & Partner in München die zweite European Identity Management Conference. Erwartet werden mehr als 100 Referenten aus aller Welt, die über die neuesten Entwicklungen und Trends berichten sowie interessante Best Practices vorstellen, darunter Dave Kearns von Network World, André Durand von Ping Identity, Kim Cameron von Microsoft, Prof. Dr. Ottmar Beckmann von Volkswagen und Prof. Dr. Reinhard Posch, CIO der österreichischen Regierung.

Das erfolgreiche Konzept der ersten Konferenz wurde beibehalten: zahlreiche hochkarätige Sprecher in dichter Abfolge und genügend Möglichkeiten für Networking und Austausch mit den Kollegen. ►

Die klassischen IM-Themen wurden in diesem Jahr allerdings um E-Government und E-Health erweitert. Am 22. April finden zunächst die Pre-Konferenzworkshops und die Keynotes statt, am 23. beginnt das Konferenzprogramm mit den einzelnen Tracks. Wer bis zum 30. Januar bucht, zahlt 1.782 statt 1.980 Euro für die Teilnahme. ❑

Security World auf der CeBIT

Die CeBIT 2008 rückt immer näher und auch in diesem Jahr wird es wieder eine Security World geben: In über 100 Vorträgen berichten namhafte Experten renommierter Branchengrößen über relevante Sicherheitsaspekte der IT. Ambitionierten Anwendern, Profis und Entscheidern werden laut Veranstalter praxisnahe Einblicke und vertrauenswürdige Lösungen präsentiert. Die Slots finden statt vom 4. bis zum 9. März in Halle 6, Stand G16 / G24. ❑

Service

Experten im Interview

„Allein Virenscanner und Spam-Filter zu haben, reicht nicht.“

Spam als neuzeitliches Phänomen des Internets verursacht erhebliche wirtschaftliche Schäden: So entstehen nicht nur unnötige Kosten durch die zusätzliche Datenmenge, sondern auch für dessen Bearbeitung und Beseitigung. Doch inwiefern gehen damit auch Sicherheitsrisiken einher, und worauf müssen sich Unternehmen in Bezug auf Spam gefasst machen? NIFIS advice sprach mit Dr. Klaus-Peter Kossakowski. Sein Unternehmen PRESECURE berät in allen Bereichen rund um Rechner- und Netzwerksicherheit. Außerdem ist er Geschäftsführer des DFN-CERT. Dieses bietet schnelle und effektive Hilfe bei der Reaktion auf Sicherheitsvorfälle sowie Unterstützung bei der Durchführung vorbeugender Sicherheitsmaßnahmen.

Spam – da denkt man sofort an unerwünschte Werbe-E-Mails. Doch was genau zählt alles unter den Begriff?

Kossakowski: Spam ist zunächst einmal alles unerwünschte, was auflläuft. Außerdem kommt es noch auf das Kommunikationsmittel an, und da ist E-Mail nur eines. Überall wo sie einen Eingabekanal haben, kann etwas hereinkommen, dass sie nicht wünschen. Das kann die Telefonnummer sein, die Wohnadresse, die Mobilfunknummer oder auch die Faxnummer. Auch im Internet, in Foren oder bei Diensten wie ICQ findet sich Spam.

Was sind aus Ihrer Sicht die schlimmsten Auswirkungen von Spam?

Kossakowski: Die schlimmste Auswirkung zielt auf uns als Gesellschaft ab. Einerseits wird das Vertrauen in die Kommunikation beeinträchtigt. Alles was dieses Vertrauen unterminiert, schädigt die Anstrengungen der Leute, die etwas Gutes und Richtiges tun. Andererseits ist Spam ein Eintrittstor für viele Angriffe, gegen die die Nutzer einfach wehrlos sind. ►

Und der größte Schaden aus Sicht eines Unternehmens?

Kossakowski: Als Empfänger muss ich dafür bezahlen, dass mich jemand schädigt. Zum Beispiel indem ich den Traffic bezahle, Filterlösungen anschaffe oder einen Arbeitszeitausfall meiner Mitarbeiter erleide. Ich muss komplexe Strukturen aufbauen, um den E-Mail-Ansturm zu bewältigen, nur um am Ende festzustellen, dass der größte Teil unerwünscht ist. Außerdem können Konflikte zwischen Arbeitgeber und Arbeitnehmer entstehen: Wenn die private Kommunikation nicht ausdrücklich unterbunden ist, dürfen eingehende Mails nicht so einfach gescannt und herausgefiltert werden. Da müssen komplizierte rechtliche Vereinbarungen getroffen werden, und die Diskussion ist oft für beide Seiten demotivierend.

Wie groß ist die Gefahr, dass Malware auf diesem Wege verschickt wird beziehungsweise dass schadhafter Code eingebettet wird?

Kossakowski: Eine Spam-Welle mit ernsthafter Produktwerbung, die durch eingebetteten Schadcode gleichzeitig infizierte, gab es meines Erachtens noch nicht. Dies würde ja die Interessen des Werbenden verletzen. Allerdings gab es schon Beispiele, in denen Werbung oder verteilte Programme durch Fehler beim Versender vorher infiziert werden konnten. Immer öfter müssen wir allerdings damit rechnen, dass eine anscheinend ernsthafte Produktwerbung nur vorgetäuscht wird, um zum Klicken auf eine Website zu animieren. Auf der Website passiert dem Benutzer dann das Schlimmere, zum Beispiel eine Infektion durch einen Trojaner, der damit eine Hintertür in das Unternehmensnetzwerk öffnet.

Was können Unternehmen tun, um das Spam-Aufkommen bei sich zu verringern?

Kossakowski: Es gibt kleine Schritte. E-Mail-Adressen möglichst nicht in falsche Hände geraten zu lassen, ist ein guter Weg. Zum Beispiel sollten E-Mail-Adressen nicht als Klartext in Webseiten eingebunden werden, oder man kann Mitarbeiter auffordern, ihre E-Mail-Adressen nicht für den Eintrag in öffentlich zugängliche Internet-Seiten zu verwenden. Es gibt auch Ansätze, dass in bestimmten Abständen die E-Mail-Adressen verändert werden, oder dass Leute ihre bisherigen Adressen aufgeben, wenn diese mit zu viel Spam belastet werden. Das ist natürlich eine Hürde für die Kommunikationspartner.


Dr. Klaus-Peter Kossakowski, Geschäftsführer PRESECURE

Interessanter ist daher die Variante, unterschiedliche E-Mail-Adressen für unterschiedliche Zwecke zu verwenden. Wenn Mitarbeiter beispielsweise notwendigerweise in Internet-Foren teilnehmen, wo die E-Mail-Adressen als Teil des Profils hinterlegt werden, dann sollten sie eine andere Adresse verwenden als jene für die Kommunikation mit ihren Geschäftspartnern. Das ermöglicht auch eine Priorisierung der Arbeitslast, da sie im „Geschäftspartnerpostfach“ nur wichtige Sachen und hoffentlich wenig Spam erhalten.

Wie kann ich als Chef meine Mitarbeiter unterstützen?

Kossakowski: Es ist ganz wichtig auszuformulieren, was an privater Nutzung wie und warum erlaubt ist. Erster Schritt dabei ist, den Status zu ermitteln, ob private Kommunikation bislang explizit oder implizit erlaubt war. Danach sollten sich alle Parteien an einen Tisch setzen und eine gemeinsame Lösung erarbeiten, denn es betrifft die Interessen beider Seiten. Es geht nicht darum, dass man die private Internet-Kommunikation komplett unterbinden möchte, aber diese darf die betrieblichen Belange nicht stören und vor allem nicht notwendige Sicherheitsmaßnahmen gänzlich unterbinden.

Bei den Mitarbeitern muss daher das Bewusstsein für die Problematik geschärft werden. Dazu gehören Tipps, wie sie effizient mit Spam-E-Mails umgehen. Zum Beispiel sollten E-Mails, die als Spam erkennbar sind, direkt und ohne weitere Ansicht gelöscht werden. Bei E-Mails im HTML-Format sind oft Grafiken enthalten, die beim Öffnen von einem Internet-Server nachgeladen werden. Über diese Zugriffe kann der Spam-Versender nachvollziehen, dass die E-Mail-Adresse wirklich funktioniert und die E-Mail geöffnet wurde. Damit steigt der Wert der E-Mail-Adresse natürlich enorm an, und damit zwangsläufig auch die Menge an Spam, die an diese Adresse zukünftig verteilt wird.

Worauf muss ich als Unternehmer noch achten?

Kossakowski: Spam ist kein neues Problem. Doch die Lösungen im Unternehmen passen sich nicht so schnell an die Herausforderungen an. Allein Virenscanner und Spam-Filter zu haben, reicht nicht, die müssen auch aktualisiert und angepasst werden.

Was ist, wenn meine Unternehmensadressen für einen Spam-Angriff missbraucht wurden?

Kossakowski: Die Spammer versuchen die E-Mail beim Empfänger möglichst authentisch herüberkommen zu lassen, damit sie von den Filtern durchgelassen und auch aufgemacht wird. Daher versucht man eine glaubwürdige Adresse zu nehmen, also nicht xyz aus Nigeria, sondern Klaus-Peter Kossakowski von Presecure. Wenn E-Mail-Adressen aus Ihrem Unternehmen als augenscheinlicher Absender eingetragen wurden, merken Sie das meist aufgrund der Rückläufer von Adressen, die Sie gar nicht kennen. Bei einer globalen Spam-Welle und einem schlecht gepflegten Datenbestand, kann durch die Rückläufer der Mail-Verkehr Ihres Unternehmens bereits zum Erliegen kommen und der Server zum Absturz gebracht werden. ►

Es kommt aber noch schlimmer. Vom Spam belästigte Empfänger könnten einer Firma, die so genannte Blacklists pflegt und als Dienstleistung vermarktet, melden, dass sie binnen einer Stunde 1.000 unerwünschte Mails Ihres Unternehmens erhalten hat. Das führt dazu, dass Ihr Unternehmen als Spam-Verursacher auf die schwarze Liste eingetragen wird. Alle Server, die diese schwarzen Listen nutzen, um E-Mails zu blockieren, blockieren in Zukunft nicht nur die Spams mit den gefälschten Angaben Ihres Unternehmens, sondern Ihre gesamte Geschäftskommunikation. Es ist sehr schwierig von dieser Liste wieder herunterzukommen, teilweise muss hierfür sogar eine Schutzgebühr bezahlt werden!

Was kann ich denn als Unternehmen tun, wenn mein Name/die Adresse für so etwas missbraucht wurde?

Kossakowski: Quasi nichts, denn Sie finden in der Regel die Verursacher nicht. Ein Weg, den Geschäftspartnern die Vertrauenswürdigkeit Ihrer E-Mails zu demonstrieren, ist die Verwendung von digitalen Signaturen. Beispielsweise sind alle E-Mails vom DFN-CERT digital unterschrieben, sodass der Empfänger weiß, wo die E-Mail herkommt und dass diese auch auf dem Übertragungsweg nicht manipuliert wurde.

Unternehmen können die dazu verwendeten eindeutigen Zertifikate auch Mailservern zuordnen, sodass die Endanwender von der Problematik befreit sind und trotzdem ein vertrauenswürdiger Kanal zwischen Kommunikationspartnern auf Unternehmensebene geschlossen wurde. Arbeiten also etwa fünf Unternehmen im Partnerverbund, müssen die Administratoren einmalig fünf Server darauf einrichten, dass sie jeweils die vier anderen als vertrauenswürdig anerkennen. Alle ein bis zwei Jahre werden die Zertifikate ausgetauscht, und die Sache ist erledigt. Die tausenden Mitarbeiter dahinter werden gar nicht involviert, und die zertifizierten E-Mails können einfach durchgelassen werden.

Wir danken für dieses Gespräch! ❑

Expertenfrageecke

Welche Konsequenzen drohen einem Geschäftsführer bei Datendiebstahl?

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

Immer öfter liest man von Datendiebstahl. In der Regel geht es dabei nicht um „Diebstahl“. Mal werden bei einem Unternehmen die Daten der Kreditkarten von Kunden ausspioniert, ein anderes Mal werden CDs/DVDs oder gleich ganze Notebooks verloren oder gestohlen. In erster Linie ist dabei problematisch, dass sensible personenbezogene Daten in die Hände Unbefugter gelangen. Seltener gehen die Daten tatsächlich verloren und müssen aufwändig rekonstruiert werden.

RA Dr. Thomas Lapp, NIFIS-Vorstand

Unternehmen oder Behörden, denen sensible Daten anvertraut wurden, erleiden einen massiven Vertrauensverlust, wenn sie eingestehen müssen, dass sie diese Daten nicht vor fremdem Zugriff geschützt haben.

Daneben haben sie aber auch rechtliche Konsequenzen zu fürchten. Bei personenbezogenen Daten schreiben die Datenschutzgesetze vor, dass diese vor dem Zugriff Unbefugter zu schützen sind. Wenn dann Unbefugte mit den Kreditkartendaten einkaufen und dadurch ein Schaden entsteht, muss dieser ersetzt werden. Oft ist es für die Kunden aber schwer nachzuweisen, wie ihre Daten in die Hände der Täter gelangt sind. Schließlich ist der Schaden schwer zu beziffern, wenn die Buchung der Kreditkarte erstattet wird.

Gravierender sind hier die (meist wenig beachteten) Vertraulichkeitsvereinbarungen, die sich in vielen Verträgen zwischen Unternehmen finden. Diese sind meist mit happigen Vertragsstrafen unterlegt. Noch massiver sind die Folgen, wenn die Verletzung von Privatgeheimnissen mit Strafe bedroht ist, wie dies beispielsweise bei Rechtsanwälten, Ärzten, Kranken-, Unfall- oder Lebensversicherungen (nicht aber bei Banken!) der Fall ist.

Alle Fälle zeigen, dass die Daten gegen fremden Zugriff besser geschützt werden müssen. Daher sollte man überlegen, die Datenträger zu verschlüsseln, damit die Daten auch bei Verlust der Datenträger vor fremdem Zugriff sicher sind. ❑

Sicherheitsupdate

Rekord bei Datendiebstahl im Jahr 2007

Noch nie wurden weltweit so viele personenbezogene Daten entwendet wie 2007. Gegenüber dem Vorjahr verdreifachte sich die Zahl der Datendiebstähle. Experten rechnen für das laufende Jahr mit einer weiteren deutlichen Zunahme.

Eine Expertengruppe für Sicherheit im Internet, attrition.org, schätzt, dass bis zum 21. Dezember mehr als 162 Millionen Daten entwendet wurden. Das sind mehr als drei Mal so viel wie 2006, als eine Zahl von 49 Millionen erhoben wurde. Ursache der Steigerung sei vor allem die Explosion der von Unternehmen erstellten persönlichen Daten, sagte Brian Martin von attrition.org. Er erwarte daher eine weitere Zunahme von entwendeten Daten.

Allein 94 Millionen Daten entfallen allerdings auf einen einzigen Fall, den Kreditkartendiebstahl bei dem Unternehmen TJX Cos., das mehrere Discount-Ketten betreibt. Weitere große Fälle waren der Verlust von zwei CDs mit den persönlichen Daten von 25 Millionen Personen in Großbritannien und ein Hackerangriff auf die Datenbank eines Online-Brokers in den USA.

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