

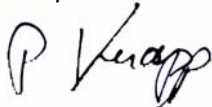
Liebe Mitglieder, liebe Leserinnen und Leser,

ich freue mich, Ihnen heute unseren Newsletter „NIFIS advice“ vorstellen zu dürfen. Er wird Sie quartalsweise über die Aktivitäten der Nationalen Initiative für Internet-Sicherheit auf dem Laufenden halten. Wir möchten Sie regelmäßig informieren und aufzeigen, wie Sie maximal von der NIFIS-Mitgliedschaft profitieren und die gebotene aktive sowie passive Hilfe nutzen können.

Neben Veranstaltungshinweisen und Praxistipps werden wir Ihnen das Kompetenzzentrum NIFIS näher bringen. In jeder Ausgabe von NIFIS advice wird ein Gründungsmitglied vorgestellt, das Expertenwissen zu einem bestimmten Thema hat und Ihnen als neutraler Ansprechpartner zur Verfügung steht. Außerdem möchten wir Ihnen die einzelnen NIFIS-Dienstleistungen vorstellen, die Mitglieder kostenlos und zum Schutz ihres Unternehmens einsetzen können.

In dieser Ausgabe stellen wir Ihnen das neue NIFIS-Siegel vor, und ich möchte Sie an dieser Stelle bitten, Ihre Chance zu nutzen und das Selbstaudit in Ihrem Unternehmen durchzuführen.

Viel Spaß beim Lesen wünscht Ihnen



Peter Knapp, Vorstandsvorsitzender



HIGHLIGHTS

NIFIS Inside

Veranstaltungstipps:

NIFIS auf der EICAR Konferenz und beim WebhostingDay

Seite 2

Wir über uns:

NIFIS-Gründungsmitglied Controlware gibt Einblick in Beweggründe, Ziele – und VoIP

Seite 3

Wir für Sie:

Versicherung von Hardware und Daten

Seite 4

Praxistipp:

Manager persönlich für IT-Sicherheit haftbar

Seite 5

Sicherheitsupdate

Seite 5

NIFIS-Siegel: Erster Schritt in sichere Zukunft

Viele Unternehmen sind sich der Gefahren aus dem Internet nicht bewusst und riskieren dadurch ihren geschäftlichen Erfolg. Um die Vertraulichkeit, Verfügbarkeit und Integrität von geschäftskritischen Daten in digitalen Unternehmensnetzwerken zu fördern und sicherzustellen, hat NIFIS ein Sicherheitssiegel für die mittelständische Wirtschaft entwickelt.

Kostengünstige Selbstanalyse erhöht nachhaltig Sicherheit

Um das im Rahmen der CeBIT vorgestellte Siegel zu erhalten, muss das Unternehmen in einem Selbstaudit 82 Fragen beantworten. Diese befassen sich inhaltlich mit allen relevanten Themen aus den Bereichen organisatorische, logische, technische sowie physikalische Sicherheit. Nach der Auswertung durch ein Experten-Gremium, dem NIFIS-Siegelrat, erhält jeder Bewerber basierend auf den Ergebnissen eine Analyse. Diese dokumentiert seinen Sicherheitsstatus und zeigt innerbetriebliche Lücken und Mängel in den eingesetzten Sicherheitssystemen und Prozessen auf. Anschließend werden geeignete notwendige Maßnahmen zur Beseitigung der Mängel empfohlen, um die Sicherheit im Unternehmen nachhaltig zu erhöhen.

NIFIS-Siegel verschafft Vorteile

Bei einer positiven Bewertung erhält das Unternehmen zudem eine Urkunde und darf zwölf Monate lang das NIFIS-Siegel führen. Damit dokumen-



tiert es nicht nur seinen Sicherheitsstandard gegenüber Mitarbeitern, Kunden und Geschäftspartnern. Das NIFIS-Siegel

kann sogar die Kreditwürdigkeit des Unternehmens gemäß den Basel II-Kriterien verbessern und das Haftungsrisiko für Vorstände und Geschäftsführer reduzieren.

Zudem schafft das NIFIS-Siegel einen Wettbewerbsvorteil. Es ist die erste Stufe im Prozess zur Vorbereitung einer Zertifizierung gemäß des anerkannten Standards ISO/IEC 27001. Als zweite Stufe wird NIFIS eine Vor-Ort-Validierung anbieten, die in den nächsten Monaten konkretisiert wird.

Das NIFIS-Selbstauditverfahren ist **ohne großen Aufwand** und kostengünstig durchführbar: Für NIFIS-Mitglieder ist es **kostenfrei**, Nicht-Mitglieder zahlen 150 Euro.

Prüfen und optimieren Sie jetzt Ihren Schutz vor Gefahren aus dem Internet! Schreiben Sie bei Interesse eine E-Mail an newsletter@nifis.de. Weitere Informationen erhalten Sie [hier](#). □

NIFIS begrüßt neue Mitglieder

NIFIS freut sich im ersten Quartal über zahlreiche neue Mitglieder, darunter die Unternehmen Camdata, ProRZ und Heitzig Consulting. Der Verein heißt sie herzlich willkommen und bietet ihnen die Möglichkeit, seine Aktivitäten aktiv mitzugestalten.

NIFIS ist prinzipiell für alle Unternehmen und Personen offen, die sich für das Thema Internet-Sicherheit interessieren und versteht sich als Ansprechpartner bei Fragen oder Problemen der Mitglieder. Besonders kleine und mittelständische Unternehmen profitieren von den Angeboten der NIFIS, da vielfältige Informationen und hilfreiche Dienstleistungen im Rahmen der Mitgliedschaft bereitgestellt werden. Weitere Informationen finden Sie [hier](#). □

NIFIS präsentiert sich auf der EICAR Konferenz

Am 1. und 2. Mai findet in Hamburg die Jahreskonferenz der European Expert Group for IT-Security (EICAR) statt. Thema ist diesmal „Security in the mobile and networked World“. Das europäische Event bietet in Präsentationen neue Erkenntnisse internationaler Forscher und Ergebnisse aus den EICAR-Task-Forces zu Sicherheitsthemen wie Content Security und RFID.

Um einen besseren Wissenstransfer zwischen Forschung und Anwendung im Bereich Sicherheit zu leisten, öffnet EICAR mit einem Management-Track die Veranstaltung zum ersten Mal auch IT-Anwendern.

Weitere Informationen zur Veranstaltung finden Sie im [Einladungsflyer](#) und unter <http://www.eicar.org>. NIFIS-Mitglieder erhalten **25 Prozent Rabatt** auf den Eintrittspreis.

Schreiben Sie einfach eine E-Mail an newsletter@nifis.de. □

NIFIS aktiv auf dem WebhostingDay

Am 28. März veranstaltet intergenia den WebhostingDay 2006 im Event-Center des Phantasialands in Brühl bei Köln. Der WebhostingDay 2006 ist das größte Branchentreffen der Webhosting-Industrie in Europa und bietet ein ideales Umfeld zum Networking. Insgesamt rechnet intergenia mit rund 350 Gästen.

Im so genannten main.FORUM, dem Hauptauditorium, berichten Entscheider aus der internationalen Webhosting-Branche von ihren Erfahrungen und Visionen.

Von 10.45 bis 11.30 Uhr referiert hier Peter Knapp, Vorstandsvorsitzender NIFIS e. V., über „Internet-Sicherheit im Hosting-Umfeld: technische, rechtliche und organisatorische Herausforderungen“.

Im „work.SHOP“ stellen Partner des WebhostingDay interessante Lösungen und Produkte vor, und in der Begleitmesse „hosting.FAIR“ können Interessierte direkt in Kontakt mit interessanten Firmen und Ausstellern zum Thema Webhosting treten.

Das ausführliche Programm finden Sie im [Einladungsflyer](#) und unter <http://www.webhostingday.de>. Für NIFIS-Mitglieder ist die Teilnahme **kostenlos**, Nicht-Mitglieder zahlen 279 Euro.

Bitte senden Sie bei Interesse eine E-Mail an newsletter@nifis.de. □

Mitgliederversammlung NIFIS

Am 17. Mai findet in Frankfurt am Main die Mitgliederversammlung von NIFIS e.V. statt. Die Veranstaltung richtet sich ausschließlich an Vereinsmitglieder, die offizielle Einladung und die Tagesordnung werden den Mitgliedsunternehmen separat zugestellt. □

Konstituierende Sitzung des Exekutivbeirates

Der Exekutivbeirat von NIFIS traf sich am 26. Januar im Paul-Löbe-Haus in Berlin zur konstituierenden Sitzung. In dem Gremium sind die für das Thema Internet zuständigen Spitzenpolitiker aus SPD, CDU und FDP vertreten. Sie möchten hier parteiübergreifend zusammenarbeiten, um die Sicherheit der deutschen Wirtschaft im Cyberspace zu erhöhen.



Beiräte mit Ernennungsurkunden v.l.n.r. Otto (MdB), Knapp, Tauss (MdB), Lapp

Dem Exekutivbeirat von NIFIS gehören an:

Dr. Martina Krogmann ist Mitglied der CDU-Medienkommission und seit November 2005 Parlamentarische Geschäftsführerin in der CDU/CSU-Bundestagsfraktion. Bereits in der 14. und 15. Wahlperiode war sie Internetbeauftragte ihrer Fraktion.

Jörg Tauss ist seit 1999 Sprecher für Bildung, Forschung und Medien der SPD-Bundestagsfraktion, seit Oktober 2002 auch medienpolitischer Sprecher der SPD-Fraktion im Bundestag. Er gilt als langjähriger Internet-Verfechter und hatte als einer der ersten Abgeordneten des Deutschen Bundestages eine eigene Homepage.

Hans-Joachim Otto ist seit sieben Jahren medien- und kulturpolitischer Sprecher der FDP-Bundestagsfraktion und somit zuständig für Internet und Medien. Mitte November 2005 wurde er zum Vorsitzenden des 20-köpfigen Bundestagsausschusses für Kultur und Medien benannt. □

Wir über uns

Mitgliederinterview Controlware

Als NIFIS-Gründungsmitglied gibt Controlware Einblick in Beweggründe, Ziele – und VoIP.



Controlware bietet als international agierender Systemintegrator und IT-Dienstleister seit der Gründung im Jahr 1980 komplette Serviceleistungen rund um das Netzwerk an. Die Unternehmenszentrale befindet sich in Dietzenbach bei Frankfurt am Main. Neben zehn Standorten in Deutschland ist Controlware in Asien, Europa und Nordamerika vertreten. National kümmern sich 350 Mitarbeiter um die Belange der Kunden, darunter Banken, die Großindustrie sowie mittelständische Unternehmen.

Die Redaktion von NIFIS advice sprach mit



Dietrich Böke
Technischer Direktor



Manfred Rothkugel
Manager Competence Center Security

Sie sind Gründungsmitglied von NIFIS. Warum unterstützen Sie die Initiative?

Rothkugel: Informationssicherheit ist eines der Kernthemen von Controlware, mit dem wir uns bereits seit mehr als zehn Jahren schwerpunktmäßig befassen. Dabei stellen wir immer wieder fest, dass es in dem Bereich viele strukturierte und generische Ansätze gibt, die für Großunternehmen hervorragend funktionieren. Aber der typische Mittelständler ist damit oftmals überfordert und scheut die vermeintliche Komplexität des Themas. Genau dort möchte NIFIS unterstützen, damit Unternehmen mit begrenztem Aufwand das notwendige Maß an Sicherheit implementieren können. Als konkretes Ergebnis verweise ich gerne auf das neu vorgestellte NIFIS-Siegel als praxisorientierte Hilfestellung für dokumentierte Sicherheit im Unternehmen. Ein weiteres Tool entsteht beispielsweise gerade für den Themenschwerpunkt VoIP in unserem Haus mit dem Ziel, dem Mittelstand einen Leitfaden an die Hand zu geben. Dieser soll leicht verständlich und pragmatisch aufzeigen, was im VoIP-Umfeld in punkto Sicherheit beachtet werden muss.

NIFIS bündelt als Kompetenzzentrum das Fachwissen von Expertenunternehmen. Für welchen Themenkomplex sind Sie dabei zuständig?

Böke: Für das gesamtheitliche Thema Sicherheit und im Besonderen für den Bereich „Sichere Sprachinfrastruktur mit Voice over IP (VoIP)“. Wir haben uns diesen Kernbereich für unser Engagement ausgesucht, weil wir zum einen als Systemintegrator seit über 20 Jahren Netze aufbauen und über umfangreiche Kenntnisse zum Aufbau von Kommunikationsstrukturen verfügen. Zum anderen haben wir Kompetenz im Sicherheitsumfeld, die sich gut damit verknüpfen lässt. Wir stehen allen Mitgliedern und Interessierten gerne für Fragen in dem Bereich zur Verfügung.

Warum entscheiden sich immer mehr Unternehmen dafür, VoIP einzuführen?

Rothkugel: Mit VoIP kann die kommunikative Distanz zum Kunden und Partner verkürzt werden. Eine weitere Motivation liegt in der Schaffung von Mehrwertlösungen durch die Zentralisierung von Diensten und die Verknüpfung von herkömmlicher TK-Technik mit EDV-Prozessen. Dabei können nicht nur neue Dienste etabliert, sondern dank geringerer Komplexität vor allem auch Betriebs- und Kommunikationskosten gesenkt werden. Zudem werden derzeit immer mehr Nebenstellenanlagen abgelöst: Da hierbei sowieso Investitionen getätigt werden müssen, fällt die Entscheidung leicht, die bisher nur für Daten genutzte Leitung für Sprache mitzunutzen.

Gibt es Nachteile, sodass Sie manchen Unternehmen von VoIP abraten?

Böke: Rein aus technischen oder Qualitätsgründen gibt es keine Schlechterstellung durch VoIP. Die Lösungen haben mittlerweile die entsprechende Marktreife. Je nachdem von welchem Hersteller welche Applikationen eingesetzt werden, ist die Technologie auch für alle Unternehmensgrößen geeignet. Klassische TK-Anlagen bieten jedoch teilweise bis zu 400 Möglichkeiten zur Programmierung der Telefone. Diese sind noch nicht alle bei VoIP etabliert oder funktionieren nicht so wie in der klassischen TK-Anlage. Wenn Unternehmen viele dieser individuellen Programmierungen einsetzen, macht der Umstieg manchmal keinen Sinn.

Was empfehlen Sie Unternehmen, die VoIP einführen möchten?

Rothkugel: Wichtig ist erst einmal zu klären, welche Ziele aufgrund der Einführung erreicht werden sollen und ob sich diese wirklich erfüllen lassen. Welche Anforderungen hat das Unternehmen und wie können diese mit VoIP umgesetzt werden? Dann sollte geprüft werden, ob ein bestehendes Netz beispielsweise dafür bereit ist, die Quality of Service zu gewährleisten, denn Sprachdaten sind empfänglich gegen bestimmte Arten von Störungen. Das sind natürlich alles nur erste Schritte. Wichtig ist eine kompetente Beratung im Vorfeld, bei der auch Sicherheitsaspekte mitbetrachtet werden müssen. ►

Wie unterstützt controlware die Unternehmen konkret dabei?

Böke: Wir beraten bei der Entscheidungsfindung, erstellen einen Kriterienkatalog oder eine Machbarkeitsstudie, um herauszufinden, ob die Einführung von VoIP für dieses Unternehmen sinnvoll ist. Fällt die Entscheidung positiv aus, können wir konkrete Lösungen planen, installieren und auch betreiben. Selbstverständlich besteht auch die Möglichkeit, dass wir die Verantwortlichen im Unternehmen anleiten, die Lösung selbst sicher zu implementieren.

Warum sollten weitere Unternehmen Mitglied bei NIFIS werden?

Rothkugel: Die Mitgliedsunternehmen profitieren schon jetzt von zahlreichen Services, wie dem NIFIS-Siegel, dem Warn- und Informationsdienst oder der Online-Datensicherung. Sie erhalten somit einen echten Mehrwert. Außerdem wird NIFIS zunehmend in der Öffentlichkeit wahrgenommen, was beispielsweise die Mitarbeit bei der Umsetzung von NPSI (Nationaler Plan zum Schutz der Informationsinfrastrukturen) beim Bundesministerium des Innern zeigt. Vielen mittelständischen Unternehmen ist oft auch gar nicht bewusst, dass sie beispielsweise von dem Thema „Kritische Infrastrukturen“ betroffen sind. Deshalb tut es ihnen gut, sich entsprechend zu organisieren, um sich frühzeitig positionieren zu können.

Was wünschen Sie sich für die Zukunft von NIFIS?

Böke: NIFIS an sich und der klare Fokus auf Internet-Sicherheit sind mehr als interessant. Daher gehe ich davon aus, dass NIFIS sich sehr positiv weiterentwickelt und sich der Einfluss noch stärker bemerkbar macht. Meine Vision ist, dass NIFIS zukünftig als einer der entscheidenden Verbände im Bereich Sicherheit genannt wird. In der Konsequenz hoffe ich, dass es uns so gemeinsam gelingt, nicht nur die Sensibilisierung für das Thema Informations-Sicherheit in der Wirtschaft zu verbessern, sondern vor allem das konkrete Sicherheitsniveau in den Unternehmen zu erhöhen.

Wir danken für dieses Gespräch! □

Wir für Sie

Versicherung für Hardware und Daten

Elektronikversicherungen erfreuen sich immer größerer Beliebtheit. Doch hat ein Mitarbeiter aus Versehen ein Notebook vom Tisch fallen lassen oder wichtige Dokumente unwiederbringlich beschädigt, folgt oft das böse Erwachen: Diese Schäden werden nicht von dieser Versicherung abgedeckt. NIFIS bietet deshalb ihren Mitgliedern eine Versicherung, die auch für Hardwareschäden, die durch menschliches Versagen entstanden sind, sowie für die Datenwiederherstellung aufkommt.

Versicherungen zum Schutz der Informationstechnologie werden in Deutschland weit verbreitet angeboten und treffen auf eine entsprechende Akzeptanz im Markt. Diese als Elektronikversicherung bekannten Abschlüsse decken aber in der Regel nur solche Schäden ab, die zum Beispiel durch Überspannung, Brand oder Diebstahl verursacht werden. Im Schadensfall wird dann die beschädigte oder zerstörte Hardware ersetzt. Die größten Fehlerquellen, das menschliche Versagen oder eine Fehlbedienung, können aber nicht versichert werden.

Die Elektronikversicherungen lassen aber einen weiteren Aspekt vollkommen außer Acht: Viel wichtiger als die leicht austauschbare Hardware sind in den meisten Fällen die Datenbestände, die auf den Geräten gelagert werden und nicht ohne weiteres wiederhergestellt werden können. Dabei sind gerade die Daten entscheidend für den Fortbestand des Unternehmens. Sind Produktionsdaten, Kundendaten und Bestellungen unwiederbringlich gelöscht oder nur mit großem Zeit- und Kostenaufwand wiederherstellbar, bedeutet das für viele die Insolvenz.

NIFIS bietet Lösung

Deshalb hat NIFIS gemeinsam mit einem führenden Versicherungsunternehmen eine Daten- und Hardwareversicherung entwickelt, die genau diese beiden Schwachstellen abdeckt. Damit bietet NIFIS ihren Mitgliedern die Möglichkeit, eine weitergehende Versicherung abzuschließen, die in dieser Form sonst nicht auf dem Versicherungsmarkt erhältlich ist. Die NIFIS Daten- und Hardwareversicherung kommt auch bei menschlichem Versagen oder Fehlbedienung für die entstandenen Schäden auf und deckt ebenfalls die Kosten, die im Falle eines Datenverlusts für die Wiederherstellung der Daten entstehen. Sollten die Daten gänzlich verloren sein, würden sogar die Kosten für eine manuelle Datenerfassung abgedeckt. Die Daten und Hardwareversicherung kann im Rahmen der Mitgliedschaft für 1.400 NIFIS-Punkte genutzt werden. Die Versicherung deckt Schäden für Hardware in Höhe von 12.500 Euro und für Daten in Höhe von 10.000 Euro je Schadensfall. Selbstverständlich können größere Summen abgedeckt werden, dies bedarf einer gesonderten Vereinbarung.

Sie interessieren sich für die Daten- und Hardwareversicherung? Senden Sie uns einfach eine E-Mail an newsletter@nifis.de, und wir schicken Ihnen weiterführende Informationen. □



Ein Geschenk für Mitglieder:
Das NIFIS-Versicherungspaket

Praxistipp

Manager persönlich für IT-Sicherheit haftbar

Die Gewährleistung von Sicherheit in der Informationstechnologie ist gerade auch aus rechtlicher Sicht geboten. Das Management eines Unternehmens ist gesetzlich verpflichtet, den Schutz der Interessen der Gesellschaft zu gewährleisten. (§§ 43 GmbHG, 93 AktG). Wird gegen diese Verpflichtungen schuldhaft verstoßen, sind die Manager persönlich haftbar und müssen damit rechnen, auch mit ihrem privaten Vermögen für entstandene Schäden einzustehen. Dies gilt selbst dann, wenn der einzelne Manager für die IT gar nicht zuständig ist, da generell alle Vorstandsmitglieder beziehungsweise Geschäftsführer für die Gesamtaufgaben der Geschäftsleitung zuständig sind.



Dr. Thomas Lapp, Rechtsanwalt und Vorstand der NIFIS

Die Abhängigkeit der modernen Unternehmen von einer funktionierenden IT wird immer größer. Manche Unternehmen können einen Ausfall der IT nur Stunden, einen Teilausfall unwesentlich länger überleben. Die Folgen eines Ausfalls oder einer Funktionseinschränkung betreffen jedoch nicht nur interne Prozesse, sondern auch Kundenbeziehungen. Im günstigen Fall sind sie unangenehm und bedeuten „nur“ eine Verärgerung des Kunden – im ungünstigen Fall lösen sie jedoch eine Kettenreaktion aus, wenn Kunden ihrerseits daraufhin Liefertermine und fest vereinbarte Servicelevel nicht einhalten können, die vielleicht mit harten Vertragsstrafen verknüpft sind. Anders als in den Anfangstagen des Computereinsatzes in Unternehmen zählt heute die Aussage „Computerfehler“ nicht mehr als Ausrede, um Vertragsstrafen zu entgehen.

Für Unternehmen sind daher ein effizientes Risikomanagement und Vertragsmanagement notwendig: Bestehende Risiken müssen erkannt, nach Eintrittswahrscheinlichkeit und Tragweite kategorisiert und geeignete Maßnahmen vorgesehen werden, um den Eintritt dieses Risikos zu vermeiden und bei Realisierung den Schaden zu begrenzen. Im Rahmen des Vertragsmanagements muss der Überblick behalten werden, welche bestimmten Servicelevel, Verfügbarkeiten, Lieferzeiten oder Ähnliches dem Kunden versprochen wurden und welche Auswirkungen die zuvor genannten Risiken auf diese Versprechen haben können.

Gerade im Rahmen von Outsourcingprojekten wird mit den Anbietern in der Regel über Verfügbarkeiten und Servicelevel gesprochen. Oft wird dabei eine Abwägung zwischen den Kosten und dem Nutzen vorgenommen. Notwendig ist es aber auch, stets die Anforderungen aufgrund der eigenen Verträge mit den Kunden im Auge zu behalten. Vor allem wenn zentrale Prozesse des Unternehmens in fremde Kontrolle gegeben werden, sind Risikoanalyse und Abgleich der eigenen Pflichten mit den eingekauften Services notwendig.

Bei Rückfragen wenden Sie sich bitte an newsletter@nifis.de. □

Sicherheitsupdate

Fokus: Sicherheit von innen

Mitarbeiter oder Outsourcingpartner rücken immer mehr ins Blickfeld der CIOs, wenn es um Gefahren der IT-Sicherheit geht. „Sicherheit von innen“ gewinnt an Bedeutung, wobei begrenzte IT-Ressourcen und die Komplexität der Software als die größten Herausforderungen bei der Umsetzung eingeschätzt werden, so eine aktuelle Aberdeen-Studie. Um so genannte „Daten-Lecks“ zu vermeiden, achten 67 Prozent der Befragten auf sichere Passwortwahl. 66 Prozent führen Listen, wer Zugang zu welchen Daten hat. Wichtig sei, dass Unternehmen Mitarbeiter schulen und Vorgaben bei der Implementierung von Sicherheitslösungen machen. □

Mangelnde Netzwerk-Sicherheit

Die Mobilität ihrer Mitarbeiter stellt Unternehmen vor neue Sicherheitsprobleme. Bei einer Umfrage von Dynamic Research gaben zwei Drittel der 500 teilnehmenden Unternehmen in Deutschland, Großbritannien und Frankreich an, Sicherheitsprobleme mit ihren Netzwerken zu haben. Nur 40 Prozent können zentral prüfen, ob angemeldete Rechner den Sicherheitsrichtlinien entsprechen. 30 Prozent finden gelegentlich auch nicht autorisierte mobile Geräte und Notebooks in ihrem Netzwerk. Mehr als die Hälfte der deutschen Unternehmen verlassen sich bei der Prüfung ihres Sicherheitsstatus' ausschließlich auf Anti-Viren-Lösungen. □

Wandel der Cyber-Kriminalität

Die bevorzugten Opfer von Internet-Kriminalität sind statt Privatleuten immer häufiger Unternehmen, Behörden und Organisationen. Zu diesem Ergebnis kommt der nun von IBM präsentierte Global Business Security Index Report 2005. Kluge und organisierte Profitjäger, aber auch Unternehmens-Insider werden mit ihren Attacken immer zielgenauer und richten dabei auch größeren Schaden an. Als weitere Gefahren nennt der Report unter anderem Mobbing mit Online-Mitteln (zum Beispiel durch gefälschte E-Mails) und den leisen Datendiebstahl mit mobilen Geräten, bei dem Daten heimlich kopiert und zweckentfremdet werden. □

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.

Zukunft gehört Gateway-Security

Die Bedrohung durch Spam wird einer Studie des Marktforschers Berlecon zufolge weiter zunehmen. Nicht nur, dass die lästigen Nachrichten in Europa mittlerweile 70 Prozent des E-Mail-Verkehrs ausmachen sollen – sie sind auch immer häufiger mit Viren und Spyware verseucht oder sollen Phishing-Zwecken dienen. Als Lösung sieht Berlecon den Bereich Gateway-Security, bei dem der Schutz vor Spam, Viren und Hackern in einem integrierten Produkt vereint wird. Anbieter entsprechender Lösungen haben laut Studie ähnlich gute Marktchancen wie solche, die auf E-Mail-Life-Cycle-Management setzen, das auch Funktionalitäten zur Archivierung und Verfügbarkeit, Klassifikation und Suche einbezieht. Derzeit sei der Markt noch sehr dynamisch. □

E-Mail-Speicherung mangelhaft

Etwa die Hälfte der europäischen IT-Manager verfügt über keine Richtlinien, welche E-Mails gespeichert werden müssen. Das ergab eine Studie des britischen Unternehmens Dynamic Markets Limited. Außerdem gaben nur vier Prozent der 1.700 befragten IT-Chefs an, tagsüber regelmäßig Backup-Kopien von E-Mails zu machen, bei den meisten erfolgt die Sicherung lediglich nachts. Die Notwendigkeit der Speicherung sei mittlerweile vielen Unternehmen bewusst – bei der Umsetzung gebe es jedoch große Mängel. □

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>

Das Werk ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urhebergesetzes ist ohne Zustimmung von NIFIS strafbar. Dies gilt insbesondere für Vervielfältigungen, Verarbeitung, Mikroverfilmung und die Einspeicherung und Verarbeitung in elektronischen Systemen. Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Für die namentlich gekennzeichneten Beiträge trägt die Redaktion lediglich die presserechtliche Verantwortung. Produktbezeichnungen und Logos sind zu Gunsten der jeweiligen Hersteller als Warenzeichen und eingetragene Warenzeichen geschützt.