Nationale Initiative für Internet-Sicherheit

advice
Ausgabe 02/2006

Liebe Mitglieder, liebe Leserinnen und Leser,

eine aktuelle Studie verdeutlicht erneut die Meinung vieler IT-Verantwortlicher: Die größte Bedrohung der IT-Sicherheit sind nicht Hacker, Viren oder Phishing-Attacken, sondern die eigenen Mitarbeiter. Leider wird in der Studie nicht gefragt, welche Konsequenzen daraus gezogen werden.

Die Bedrohung durch die Mitarbeiter hat mehrere unterschiedliche Ursachen: Unwissenheit, Böswilligkeit, Nachlässigkeit und mangelnde Fehlertoleranz der Systeme. Gegen Unwissenheit helfen am besten die Information und Schulung der Mitarbeiter. Hierfür müssen die Unternehmen den Mitarbeitern die Zeit geben, sich ausreichend zu informieren und die Informationen aktuell sowie in ansprechender und verständlicher Form bereitstellen. Nachlässigkeit oder gar böser Wille sind oft Folge mangelnder Motivation oder schwelender Konflikte. Hier können Konfliktmanagementsysteme im Unternehmen helfen, solche Probleme und Konflikte frühzeitig zu erkennen und zu lösen. Interne Konflikte wirken sich nicht nur als IT-Risiken aus, sondern lähmen auch die Kreativität und Produktivität im Unternehmen. Ausreichende Nutzerfreundlichkeit und Fehlertoleranz werden bei IT-Investitionen zu wenig als Anforderungen herausgestellt. Diese Aspekte sollten stets im jeweiligen Vertrag als wesentliche Pflicht des Lieferanten verankert sein.

NIFIS hilft ihren Mitgliedern dabei, die Mitarbeiter über aktuelle Bedrohungen zu informieren und schützt sie aktiv. Außerdem können sie bei uns die Unterstützung bei der Einführung von Konfliktmanagementsystemen, der Vertragsgestaltung und IT-Beschaffung anfordern. Mehr zu unseren Services wie dem Security Advisory Dienst, dem NIFIS-Siegel und dem kombinierten Spam- und Antiviren-Filter erfahren Sie in dieser Ausgabe von NIFIS advice. Natürlich gibt es auch wieder einige Veranstaltungstipps und News rund um den Markt der IT-Sicherheit.

Viel Spaß beim Lesen wünscht Ihnen

Dr. Thomas Lapp, Vorstand der NIFIS

HIGHLIGHTS

NIFIS Inside

NIFIS empfiehlt elektronische Signatur

Seite 3

Wir über uns

Vorstellung CERTCOM: Interview mit Peter Bovekamp

Seite 4

Wir für Sie

Kombinierter Spam- und Antiviren-Filter schützt vor hohem finanziellen Schaden

Seite 5

Praxistipp

Neue Marktchancen dank Informationssicherheit

Seite 6

Sicherheitsupdate

Seite 6

NIFIS-Siegel erfolgreich gestartet

Mehrere Unternehmen können mittlerweile mit dem NIFIS-Siegel ihren Sicherheitsstandard gegenüber Mitarbeitern, Kunden und Geschäftspartnern nachweisen. Im Selbstaudit haben sie 82 Fragen aus den Bereichen organisatorische, logische, technische sowie physikalische Sicherheit beantwortet.

Der NIFIS-Siegelrat hat diese Antworten analysiert und innerbetriebliche Lücken sowie Mängel in den eingesetzten Sicherheitssystemen und Prozessen aufgezeigt. Anschließend wurden geeignete notwendige Maßnahmen zur Beseitigung der Mängel empfohlen, nach deren Umsetzung die Unternehmen das Sicherheitssiegel führen durften.

Das NIFIS-Siegel haben bislang erhalten: Claranet GmbH, KPMG Deutsche Treuhand-Gesellschaft Aktiengesellschaft, Interxion Deutschland GmbH, IT Advisory Group AG, telepunktmarketing und]init[AG.

Das NIFIS-Siegel wurde speziell für die mittelständische Wirtschaft entwickelt und ist die erste Stufe im Prozess zur Vorbereitung einer Zertifizierung gemäß ISO 27001. Für NIFIS-Mitglieder ist der Erwerb des Siegels **kostenfrei** möglich, 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 bietet KMU Datentresor

NIFIS hat einen bundesweiten Online-Datensicherungsdienst für kleine und mittelständische Unternehmen gestartet. Mit dem Service, der im NIFIS-Mitgliedsbeitrag (ab 25 Euro monatlich) **enthalten** ist, können Firmen ihre kritischen und wichtigen Daten über das Internet in einem Hochsicherheitsdatenzentrum einlagern. ►

Dieser „Datentresor" hat das erste deutsche Sicherheits- und Qualitätszertifikat des eco – Verband der deutschen Internetwirtschaft erhalten. Demnach ist das Datenzentrum als sichere Infrastruktur auf höchstem Niveau beispielsweise gegen technische Störfälle, Naturkatastrophen und Cybercrime wie Datenklau geschützt. Die Übertragung und Ablage aller Datenbestände erfolgt in verschlüsselter Form, sodass selbst ein Eindringling, der die Daten aufspürt, diese nicht lesen geschweige denn verwenden kann.

„NIFIS hat für die mittelständische Wirtschaft bis hin zum Selbstständigen und Freiberufler eine kostengünstige Möglichkeit geschaffen, Daten in einem der sichersten Rechenzentren Deutschlands abzulegen", erklärt NIFIS-Vorstandsvorsitzender Peter Knapp. Kommt es in den Unternehmen zum Computercrash beziehungsweise Datenverlust, lassen sich die abgelegten Daten via Internet schnell und einfach zurückholen. ❑

Spam kostet jährlich vier Milliarden Euro

NIFIS warnt vor der unterschätzten und stark zunehmenden Gefahr für die deutsche Wirtschaft durch unerwünschte und virenverseuchte E-Mails. „Das Problem besteht heute nicht mehr so sehr darin, dass Unternehmen keine Schutzmaßnahmen ergreifen. Es werden aber Lösungen eingesetzt, die nicht spezifisch auf die Anforderungen der Betriebe abgestimmt sind und deshalb große Lücken aufweisen", berichtet NIFIS-Vorstandsvorsitzender Peter Knapp.

Auf diese Weise entstehe ein Sicherheitsgefühl, das trügerisch sei. Die Experten von NIFIS gehen davon aus, dass allein in Deutschland der jährliche finanzielle Schaden durch unerwünschte E-Mails mittlerweile die Grenze von vier Milliarden Euro überschritten hat. Hauptursache für den Schaden sei das Absinken der Produktivität der Mitarbeiter, die Spam aus ihren E-Mail-Postfächern entfernen müssen. ❑

Mittelstand muss IT-Sicherheit ganzheitlich betrachten

Viele mittelständische Unternehmen unterziehen das Thema IT-Sicherheit keiner ganzheitlichen Betrachtung und gehen dadurch erhebliche Sicherheitsrisiken ein. Zwar werden einzelne Aspekte wie etwa der Virenschutz ernst genommen – andere Gebiete wie beispielsweise die Zugriffsrechte der eigenen Mitarbeiter dafür oftmals sträflich vernachlässigt.

NIFIS rät daher allen mittelständischen Firmen, die betriebliche Informationssicherheit auf allen Stufen von der Konzeption über einen Audit bis hin zur Realisierung und dem Betrieb der Sicherheitslösungen genauestens zu überprüfen. Mit dem ganzheitlichen Ansatz kann sich die Wirtschaft auch wirksam auf die neuen Basel II-Regelungen vorbereiten, die zum 1. Januar des nächsten Jahres in Kraft treten werden. Weitere Informationen finden Sie hier. ❑

NIFIS empfiehlt elektronische Signatur

Obwohl die notwendige Technik und Infrastruktur schon seit längerer Zeit zur Verfügung stehen, setzen viele Unternehmen immer noch keine qualifizierten elektronischen Signaturen ein. Aufgrund dieser Fahrlässigkeit können E-Mails gefälscht werden und Hacker mühelos die Inhalte mitlesen. Dabei schreibt beispielsweise Paragraf 9 des Bundesdatenschutzgesetzes vor, dass Unternehmen beim Umgang mit personenbezogenen Daten die Grundanforderungen hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität erfüllen müssen.

„Die qualifizierte elektronische Signatur ermöglicht die Sicherstellung von Authentizität und Integrität der Kommunikation auf elektronischem Wege, ohne dass es hierfür eines erheblichen finanziellen oder organisatorischen Aufwandes bedarf", erläutert Dr. Thomas Lapp, Rechtsanwalt und NIFIS-Vorstand. ►

Dabei ergeben sich sogar Einsparpotenziale, wenn etwa dank der Verwendung der Signatur auf elektronische Rechnungen umgestellt werden kann. ❑

Online-Datensicherung: wirtschaftlich, technisch und rechtlich?

Das NIFIS-Gründungsmitglied Interxion bietet Unternehmen die Möglichkeit, sich **unverbindlich und kostenlos** über Online-Datensicherung zu informieren. In interessanten Vorträgen wird dabei aufgezeigt, wie Unternehmen nicht nur wirtschaftlich und technisch davon profitieren. Rechtlich gesehen verpflichtet der Gesetzgeber das Management von Unternehmen, persönlich für ein Sicherheitssystem zu sorgen, damit existenzbedrohende Gefahren frühzeitig erkannt werden können.

Dies bezieht sich speziell auch auf Datensicherung, denn sollten die kritischen und wichtigen Datenbestände eines Unternehmens nicht verfügbar sein, kann schnell eine existenzbedrohende Krise entstehen. In diesem Fall können Geschäftsführer, Vorstände und IT-Verantwortliche auch mit ihrem Privatvermögen für den Schaden verantwortlich gemacht werden. Weitere Details erfahren Interessierte am 5. September ab 9 Uhr in Frankfurt am Main beziehungsweise am 7. September in Düsseldorf. ❑

Sicherheitskongress vormerken

Am 24. und 25. Januar 2007 plant NIFIS einen Sicherheitskongress. Dieser wird in Frankfurt am Main stattfinden. Sollten Sie Interesse daran haben, an einem Stand Ihre Produkte oder Dienstleistungen vorzustellen, wenden Sie sich bitte an newsletter@nifis.de. Weitere Informationen erhalten Sie in Kürze unter http://www.nifis.de und selbstverständlich in der nächsten Ausgabe von NIFIS advice. ❑

Workshop zu Datenschutz und -sicherheit in Produktions- und Testumgebungen

Es ist eine Zwickmühle: Einerseits benötigen Unternehmen realitätsnahe, konsistente Testdatenbestände, um schneller stabile Applikationen zu erzielen und ihre Softwarequalität zu steigern. Andererseits verbietet das Gesetz seit dem 23. Mai 2001 (BDSG), Kopien von Produktivdaten zu Testzwecken zu verwenden.

Ein **kostenloser** halbtägiger Intensiv-Workshop soll klären, welchen Ausweg es aus dieser Zwickmühle gibt und welche Datenschutz-Strategien heutzutage effizient und wirklich sicher sind.

Experten erläutern, wie Unternehmen Testdaten bereitstellen, die den realen Bedingungen entsprechen, aber keine personensensiblen Echtdaten enthalten, und wie sie das Testmanagement auf diese Weise komfortabler und effizienter gestalten können.

Veranstalter und NIFIS-Gründungsmitglied Compuware lädt alle Interessierten hierzu herzlich am 4. Juli ab 9.30 Uhr ins Copthorne Hotel nach Hannover beziehungsweise am 6. Juli ebenfalls ab 9.30 Uhr ins Le Meridien nach München ein. ❑

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.

Roadshow: Das Beste aus IT & TK 2006

„Trends, Prognosen, harte Fakten – Das Beste aus IT & TK 2006" präsentiert NIFIS-Gründungsmitglied Controlware auf einer Roadshow. Sowohl für das Management als auch für Techniker finden sich passende Vorträge. Themen sind unter anderem IP-Telefonie, Content Security, Server Based Computing, Storage Networking und ITIL. Die Teilnahme ist **kostenlos**, die Teilnehmerzahl begrenzt. Die Roadshow macht halt: am 29. Juni in Dietzenbach, am 4. Juli in Stuttgart und am 6. Juli in München. Agenda und Online-Anmeldung gibt es hier. ❑

NIFIS auf 10. EUROFORUM-Jahrestagung

IT-Sicherheit steht im Mittelpunkt der 10. EUROFORUM-Jahrestagung vom 18. bis zum 21. September in Düsseldorf. Hochkarätige Referenten informieren umfassend über aktuelle Trends und neue technische Herausforderungen der IT-Sicherheit. Dabei bietet die Veranstaltung die Gelegenheit, Erfahrungen und Wissen auszutauschen sowie aktuelle Maßnahmen und Produkte zur Herstellung der IT-Sicherheit zu diskutieren. Am 20. September wird NIFIS mit einem Fachvortrag zum Thema VoIP präsent sein: Dipl.-Ing. Stefan Schönleber, Leiter Competence Center IP-Kommunikations-Applikationen beim NIFIS-Gründungsmitglied Controlware, berichtet ab 15.45 Uhr, wie VoIP sicher betrieben werden kann und was zu einem erfolgreichen IP-Telefonie-Projekt überhaupt gehört. Die 10. EUROFORUM-Jahrestagung zum Thema IT-Sicherheit richtet sich vor allem an Geschäftsführer, CISO, IT-Sicherheitsverantwortliche sowie IT-Sicherheits-Dienstleister. ❑

NIFIS begrüßt neue Mitglieder

Im zweiten Quartal konnte NIFIS wieder einige neue Mitglieder gewinnen, die an dieser Stelle herzlich willkommen geheißen werden: Netsign, CIT Jena und die EKF Evangelische Krankenhaus Fördergesellschaft mbH genießen nun die Vorteile der NIFIS-Mitgliedschaft und können die Aktivitäten des Vereins aktiv mitgestalten.

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. ❑

Wir über uns

Mitgliederinterview CERTCOM

Als NIFIS-Gründungsmitglied gibt CERTCOM Einblick in Beweggründe, Ziele – und CERTs.

CERTCOM

Die CERTCOM AG ist der führende Hersteller von Produkten und Dienstleistungen für den Bereich Active Business IT-Security. Sie betreibt das erste kommerzielle CERT, das offen ist für jedes Unternehmen, das durch herstellerunabhängige CERT-Dienste seine Sicherheit verstärken möchte. Der Hauptsitz des Unternehmens ist in Mönchengladbach.

Die Redaktion von NIFIS advice sprach mit

Peter Bovekamp,
Vorstand

Was sind eigentlich CERTs?

CERT steht für Computer Emergency Response Team (CERT). Das erste Team dieser Art ist 1988 in den USA entstanden als der Morrison-Wurm das damalige Internet zu circa 80 Prozent lahm gelegt hat. Die amerikanischen Bundesbehörden haben sich gedacht, wir brauchen ein Koordinationszentrum, um den nun sicher häufiger auftretenden Gefahren entgegenzuwirken. So entstand das erste CERT. Nach dem Vorbild gibt es mittlerweile weltweit 170 organisierte Teams, die aber meist Unternehmen oder Behörden zugeordnet sind. In Deutschland hat zum Beispiel das Bundesamt für Sicherheit in der Informationstechnik ein eigenes CERT, aber auch Siemens und die Commerzbank. Kleine und mittelständische Unternehmen haben jedoch nicht die Ressourcen für ein eigenes CERT. Sie sind von dem Informationsfluss abgeschnitten und können oft notwendige Maßnahmen nur verspätet ansetzen – zu einem Zeitpunkt also, an dem bereits Schäden eingetreten sind. Die Idee der CERTCOM ist nun, unternehmensübergreifend tätig zu werden, um kostengünstig CERT-Dienstleistungen zur Verfügung zu stellen.

Wie sehen diese Dienstleistungen aus?

Das wichtigste ist sicherlich unser Warn- und Informationsdienst, den auch die Mitglieder von NIFIS nutzen können. Sie erhalten per E-Mail Informationen, wenn eine Schwachstelle entdeckt wurde und wie sie beseitigt werden kann. Da wir Mitglied im Deutschen CERT-Verbund sind, findet ein reger Wissensaustausch mit anderen CERTs statt. So sind wir immer auf dem neuesten Stand und können unsere Kunden frühzeitig warnen. Durchschnittlich gibt es fünf bis 16 Sicherheitswarnungen pro Tag. Bei Bedarf kann der Kunde auch einen Filter einrichten, um nur über die Schwachstellen informiert zu werden, die die eigenen Systeme betreffen.

NIFIS bündelt als Kompetenzzentrum das Fachwissen ausgesuchter Gründungsmitglieder. Für welchen Themenkomplex ist die CERTCOM dabei zuständig?

Für den Aufbau einer flächendeckenden CERT-Infrastruktur. Zurzeit bedienen wir unsere Kunden nur aus der Ferne: Sie rufen bei uns an und sagen: Mein Netzwerk wird angegriffen, könnt ihr mir helfen? Wir geben dann per Telefon oder E-Mail Anweisungen, was zu tun ist. Unsere Zielgruppe ist damit aber teilweise überfordert. Deshalb ist es unser Ziel, zusammen mit NIFIS eine flächendeckende CERT-Infrastruktur aufzubauen. Künftig soll es vor Ort Notfallteams geben, die von uns geschult und zertifiziert werden. Wenn der Kunde einen Notfall hat, können sie vor Ort eingreifen. Das erste Team wurde bereits eingerichtet, die weitere Entwicklung hängt aber auch von der Akzeptanz bei den Unternehmen ab. Oftmals ist deren Sensibilität in Bezug auf IT-Sicherheit immer noch sehr gering.

Wie kann ein Unternehmen seine IT-Sicherheit verbessern?

Erst einmal sollte es das Thema ernst nehmen. Zudem sollte jedes Unternehmen einen Sicherheitsleitfaden erstellen, der natürlich auch gelebt werden muss: Wie der aussieht ist sehr unterschiedlich, da die Unternehmen über heterogene Strukturen verfügen. Klar, brauchen alle eine Firewall und einen Virenscanner. Aber das Thema ist viel komplexer. Deshalb haben wir das NIFIS-Siegel eingeführt, das Mitglieder kostenlos beantragen können. Unternehmen können so schnell feststellen, wo Schwachstellen bestehen. Das Siegel ist aber nur die erste Stufe im Prozess zur Vorbereitung einer Zertifizierung gemäß des anerkannten Standards ISO 27001. Als zweite Stufe planen wir eine Vor-Ort-Validierung, für die wir in den nächsten Monaten die Richtlinien festlegen. ►

Warum plant NIFIS die Einführung einer Vor-Ort-Validierung?

In Deutschland wird es künftig so sein, dass viele Auftraggeber ihre Zulieferer dazu verpflichten, sich nach dieser ISO-Norm zertifizieren zu lassen. Es gibt derzeit aber lediglich vier akkreditierte Zertifzierungsunternehmen, die jetzt schon stark ausgelastet sind, vor allem mit Großkunden, die eine Zertifizierung benötigen. Geplant ist deshalb, dass NIFIS-Auditoren in die kleinen Unternehmen gehen und helfen, die Zertifizierung vorzubereiten. Diese ist dann nicht mehr so zeitaufwändig und kostenintensiv, da die Unternehmen unter unseren Vorgaben eine ganze Menge selbst tun können.

CERTCOM ist Gründungsmitglied von NIFIS. Warum unterstützen Sie die Initiative?

Wir engagieren uns bei NIFIS, weil wir die Sensibilität für IT-Sicherheit in Deutschland erhöhen möchten. Außerdem wollen wir die Wirtschaft informieren, dass es NIFIS e.V. als neutrale Anlaufstelle gibt, bei der jeder aktiv mitarbeiten kann, um IT-Sicherheit zu praktizieren. Wichtig sind hierbei auch die Arbeitskreise, in denen sich die Mitglieder austauschen können. Zum dritten möchten wir unser Fachthema in die Initiative einbringen und das Kompetenzzentrum mit dem Aufbau der flächendeckenden CERT-Infrastruktur unterstützen. Diese anspruchsvolle Aufgabe lässt sich nur in der Gemeinschaft bewältigen.

Was wünschen Sie sich für die Zukunft von NIFIS?

Ich wünsche mir, dass viele Mitglieder kommen, damit man gemeinsam das Thema Informationssicherheit in der deutschen Wirtschaft bearbeiten kann. Je mehr Mitglieder kommen, umso größer wird die Akzeptanz von NIFIS. Aber NIFIS findet schon heute Beachtung, was beispielsweise die zahlreichen Gespräche mit Politik und Presse belegen. Aber ich wünsche mir, dass noch mehre Menschen sensibilisiert werden können.

Warum sollten Ihrer Ansicht nach weitere Unternehmen Mitglied bei NIFIS werden?

Unser Verein ist branchenneutral, „aus der Wirtschaft für die Wirtschaft“ haben wir uns auf die Fahnen geschrieben. Noch mehr Menschen aus der Wirtschaft sollten für die Wirtschaft aktiv mitarbeiten. Unsere Mitglieder haben direkten Zugriff auf das Kompetenzzentrum und können zudem diverse Dienste in Anspruch nehmen, wie die Daten- und Hardwareversicherung, unseren Security Advisory Dienst oder die Online-Datensicherung. Dadurch rechnet sich die Mitgliedsgebühr.

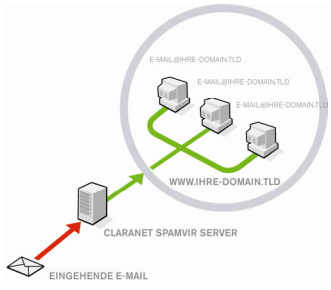
Wir danken für dieses Gespräch! ❑

Wir für Sie

Kombinierter Spam- und Antiviren-Filter schützt vor hohem finanziellen Schaden

Seit dem Jahr 2000 ist die Rate der Spam- und Viren-E-Mails von etwa fünf auf bis zu 60 Prozent rapide angestiegen. In manchen Unternehmen fallen heute bis zu 80 Prozent der eingehenden E-Mails in die Kategorie „unerwünschte Nachrichten“. Um Arbeitszeit- und IT-Ressourcen nachhaltig zu schonen, empfiehlt NIFIS „spamVir protect“: Die effiziente und leistungsfähige Kombi-Lösung aus Spam-Filter und Virenscanner schützt die gesamte Domain eines Unternehmens vor unerwünschten E-Mails und kann im Rahmen der NIFIS-Mitgliedschaft kostenfrei genutzt werden.

Führende Sicherheitsexperten gehen davon aus, dass in Deutschland der jährliche finanzielle Schaden durch unerwünschte E-Mails die magische Grenze von vier Milliarden Euro bereits überschritten hat. Hauptursache ist das Absinken der Produktivität der Mitarbeiter durch unerwünschte E-Mails. Selbst bei einer minimalistischen Annahme von täglich sechs Minuten Spam-Bearbeitung pro Mitarbeiter fallen hochgerechnet bis zu 20 Stunden im Monat in einem Unternehmen mit zehn Beschäftigten an. Mit „spamVir protect“ werden die Ressourcen Arbeitszeit und IT nachhaltig geschont. Die Lösung ist ideal für alle Unternehmen, bei denen E-Mails zum alltäglichen Geschäftsverkehr zählen.



Schutz der gesamten Domain

Der kombinierte Spam-Filter und Virenscanner ist im Vergleich zu gängigen Filterprodukten nicht auf einzelne E-Mail-Boxen oder PCs beschränkt, sondern bietet Schutz für die gesamte Domain. Der intelligente Spam-Erkennungs-Algorithmus mit aktivem Spam-Rating und Realtime Virus-Scanning sorgt dafür, dass alle eingehenden E-Mails vor der Auslieferung an die unternehmenseigenen Mailserver auf Spam analysiert, klassifiziert und nach Viren überprüft werden. Spam-E-Mails lassen sich direkt auf dem Server löschen, in einer Spam-Box isolieren oder mit einer eindeutigen Spam-Kennzeichnung zur weiteren Bearbeitung zustellen. Implizites Mail-Relaying garantiert darüber hinaus die verlustfreie Zustellung erwünschter E-Mails. Eine „spamVir protect“-Demo-Tour auf der Claranet-Website zeigt, wie man als Spam-Administrator ausgesprochen effizient über ein leicht bedienbares Webinterface individuelle Black- und Whitelists pflegen, die Spam-Box bedienen und Mailhost-Blacklists aktivieren kann.

Sie interessieren sich für „spamVir protect“? Senden Sie uns einfach eine E-Mail an newsletter@nifis.de, und wir schicken Ihnen weiterführende Informationen. ❑

Praxistipp

Neue Marktchancen dank Informationssicherheit

Der Schutz von und der Umgang mit Informationen werden für viele Unternehmen in Zeiten von steigenden regulatorischen Anforderungen und zunehmender Globalisierung immer häufiger zum kritischen Erfolgsfaktor. Technische Maßnahmen zum Schutz von Informationen sind in vielen Unternehmen gut bis sehr gut implementiert und werden auch beherrscht. Leider ergeben sich, bedingt durch organisatorische Schwächen, immer wieder Lücken in der Informationssicherheit, die zu Kompromittierungen von für Unternehmen wertvollen Informationen führen können.

Ein wirksamer Schutz von Software, Hardware, Diensten, Personal und immateriellen Werten setzt eine Kombination fokussierter und abgestimmter, technischer und organisatorischer Maßnahmen voraus. Globale Akzeptanz erlangten dabei die internationalen Standards ISO/IEC 27001:2005 und ISO/IEC 17799:2005. Diese beiden ISO-Standards zum Thema Information Security Management geben wertvolle Anleitungen zur Einführung, zum Betrieb und zur Verbesserung eines Information Security Management Frameworks (ISMS). Ziel ist dabei, Informationssicherheit im Rahmen eines Systems und nicht, wie häufig praktiziert, lediglich als eine lose Ansammlung von Sicherheitsmaßnahmen zu behandeln. Dies hilft Unternehmen, den Herausforderungen aufgrund von Globalisierung, Prozessstandardisierung und regulatorischen Anforderungen gerecht zu werden. Zusätzlich werden die internen Prozesse auf eine einheitliche Basis gestellt und die Risiken aus dem Umgang mit Informationen reduziert.

Brad Chapman,
NIFIS-Vorstand

Durch eine Zertifizierung des Informationssicherheits-Managementsystems nach ISO/IEC 27001 wird ein bewusster und verantwortungsvoller Umgang mit eigenen und vom Kunden überlassenen Informationen dokumentiert. Gleichzeitig wird die Reputation des Unternehmens am Markt erhöht.

NIFIS-Gründungsmitglied KPMG ist beim United Kingdom Accreditation Service (UKAS) als ISO/IEC 27001-Zertifizierer akkreditiert und hat seitdem weltweit zahlreiche Zertifizierungen bei Unternehmen aller Größenklassen durchgeführt oder die Implementierung von ISO/IEC 27001 beratend begleitet.

Analog zu dem formellen Zertifizierungsansatz gemäß ISO/IEC 27001 hat NIFIS ein Selbstaudit entwickelt, das sich an diesen internationalen Standards orientiert und allen Unternehmen die Möglichkeit bietet, die Wirksamkeit der getroffenen Sicherheitsvorkehrungen und Prozesse zu überprüfen. Das NIFIS-Selbstaudit ermöglicht es Unternehmen, den derzeitigen Zustand der Informationssicherheit zu erkennen, Verbesserungspotenziale aufzudecken und entsprechende Maßnahmen abzuleiten.

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

Sicherheitsupdate

Mehr Taten über das Internet

Im Jahr 2005 gab es in Deutschland weniger Verbrechen als noch im Vorjahr. Allerdings nimmt die Anzahl der Taten zu, die mithilfe des Internets begangen werden. Das geht aus der Kriminalstatistik 2005 hervor, die Bundesinnenminister Wolfgang Schäuble und der Vorsitzende der Innenministerkonferenz, Günther Beckstein, gemeinsam vorgestellt haben. Demnach stieg die Zahl der verzeichneten Fälle von Internet- und Computer-Kriminalität im Vergleich zum Vorjahr überproportional um 11,9 Prozent auf 15.875 Fälle. ❑

Die 20 größten IT-Sicherheitslücken

Die IT-Sicherheitsexperten vom SANS Institute haben ihre Liste der gravierendsten Internet-Gefahren aktualisiert. Unter anderen registrieren sie eine Zunahme der Bedrohungen für Mac OS X. Die Zahl der Probleme, die durch Softwarefehler auf Anwenderseite in Windows-Services hervorgerufen werden, ist hingegen rückläufig. Das Institut warnt darüber hinaus vor den so genannten Zero-Day-Angriffen auf den Internet Explorer sowie der steigenden Anzahl von Sicherheitslücken in den alternativen Browsern Firefox und Mozilla. ❑

Hacker greifen gezielter an

Unternehmensnetzwerke sind zunehmend gezielten Angriffen ausgesetzt, warnt die Zeitung Computer-Partner. Nach ihren Erkenntnissen gehen Angriffe häufig von Konkurrenzunternehmen aus und dienen nicht nur der Spionage, sondern auch zur Erpressung und Sabotage. Dabei werden Programme verwendet, die speziell für dieses eine Angriffsziel entwickelt wurden. Häufig werde beispielsweise mittels DoS-Attacke der Server lahm gelegt. Schwachstelle seien zudem vor allem ungeschützte WLAN-Verbindungen. ❑

Mittelstand investiert in IT-Sicherheit

Der deutsche Mittelstand plant höhere Investitionen in die IT-Sicherheit. Das geht aus einer aktuellen Untersuchung der Marktforscher von IDC hervor. Auf einer Skala von 1 bis 5 war den meisten Befragten die Vermeidung von Datenverlusten am wichtigsten (1,3), noch vor der Aufrechterhaltung des Geschäftsbetriebs (1,5) und der Vermeidung finanzieller Schäden (1,6).

Fast alle Befragten setzen zwar zahlreiche Sicherheitskomponenten ein, geben aber auch zu, dass noch Verbesserungsbedarf besteht: Zwei Drittel halten das eigene Sicherheitsniveau für „durchschnittlich“, 26 Prozent für „gut“, während sechs Prozent noch großen Handlungsbedarf sehen. 98 Prozent der Befragten hatten schon mit Viren zu kämpfen, 84 Prozent wurden mit Spam und 74 Prozent mit Trojanern konfrontiert.

Die Marktforscher haben im Rahmen ihrer Studie die Verantwortlichen für IT-Sicherheit in rund 200 Unternehmen mit weniger als 500 Mitarbeitern, aber mindestens 50 PC-Arbeitsplätzen befragt. ❑

Kleine Unternehmen achten auf Sicherheit

Kleine Unternehmen nehmen die Gefahren für die IT-Sicherheit zunehmend ernst und sind auch bereit, in den Schutz davor zu investieren. Das ergab eine Studie von TechConsult im Auftrag von Microsoft, für die 200 Unternehmen mit zwei bis 49 Mitarbeitern befragt wurden.

Rund 18 Prozent der kleinen Firmen werden demnach ihre Ausgaben für die IT-Sicherheit im Jahr 2006 erhöhen, 80 Prozent der Befragten wollen ihr Budget zumindest auf dem Vorjahresniveau belassen. Mehr als die Hälfte der Unternehmen hält IT-Sicherheit für „sehr wichtig", für weitere 34 Prozent ist sie „wichtig".

Während die Finanzdienstleister nach Branchen gesehen besonders vorbildlich agieren, gibt es bei den kleinen Industriebetrieben und Handelsbetrieben den größten Nachholbedarf: 32 beziehungsweise 17 Prozent gaben hier an, dass sie die IT-Sicherheit für „weniger wichtig“ halten. Dabei erleben zehn Prozent der kleinen Industriebetriebe und sechs Prozent der kleinen Handelsunternehmen drei bis fünf Rechnerausfälle pro Jahr. ❑

Instant Messaging birgt Sicherheitsrisiko

Viele Unternehmen wollen ihren Mitarbeitern die Kommunikation via Instant Messaging (IM) ermöglichen, weil diese ihrer Einschätzung nach für die Angestellten genauso wichtig ist wie die Kommunikation über E-Mail. Dabei vernachlässigen sie allerdings die damit einhergehenden Sicherheitsrisiken.

Wie das Beratungsunternehmen Butler Group ermittelte, nutzt die Mehrheit der Firmen eine oder mehrere IM-Lösungen. Die Technologien werden meist formlos eingeführt und kaum in bestehende Sicherheitskonzepte integriert. Über IM können jedoch Viren, Würmer, Trojaner und Spyware in die Unternehmens-IT eingeschleust werden. Deshalb müssten die Services hinsichtlich der Einhaltung rechtlicher Anforderungen, der allgemeinen Archivierung sowie privaten Nutzung geregelt werden. ❑

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