Nationale Initiative für Internet-Sicherheit

advice
Ausgabe 03/2006

Liebe Mitglieder, liebe Leserinnen und Leser,

seit einigen Jahren können IT-Servicedienstleister verstärkt feststellen, dass die Kundenanforderungen im Zusammenhang mit der Erfüllung von gesetzlichen Anforderungen stetig zunehmen. Die gesetzlichen beziehungsweise regulatorischen Anforderungen aus Kundensicht an ein Outsourcingverhältnis sind einerseits branchenspezifisch ausgerichtet (zum Beispiel MA Risk, KWG 25a II) und/oder davon abhängig, ob die Regelungen des Sarbanes Oxley Acts anzuwenden sind. Damit werden die Fähigkeiten der IT-Servicedienstleister zur Erfüllung gesetzlicher Anforderungen aus Kundensicht zunehmend eine wesentliche Grundlage für eine weiterhin erfolgreiche Positionierung im Markt sowie für stabile und ausbaubare Geschäftsbeziehungen.

Aus Sicht der IT-Servicedienstleister besteht somit die Anforderung, eine Kontrollwelt, besser noch ein Managementsystem zu implementieren, welches diesen An- und Herausforderungen gewachsen ist und gemeinsam mit zukünftig noch zu erwartenden Kundenanforderungen wachsen kann. Vor diesem Hintergrund bildet ISO 27001 in seiner Grundausstattung, aber auch seiner Flexibilität eine hervorragende Basis, um gegenwärtigen und zukünftigen Kundenbedürfnissen gerecht werden zu können. Mehr dazu und viele andere interessante Dinge erfahren Sie in der aktuellen Ausgabe von NIFIS advice.

Viel Spaß beim Lesen wünscht Ihnen

Brad Chapman, Vorstand der NIFIS

HIGHLIGHTS

Unternehmen riskieren BDSG-Verstöße

36 Prozent der IT-Entscheidungsträger in Deutschland sind nach eigener Einschätzung nicht umfassend mit dem Bundesdatenschutzgesetz (BDSG) vertraut, obwohl es bereits 1990 in Kraft trat. Das ergab eine Umfrage von Compuware und NIFIS unter mehr als 100 deutschen IT-Führungskräften.

Kein Wunder, dass sie deshalb teilweise gegen das BDSG verstoßen und dabei das Risiko von Bußgeldern oder anderen Maßnahmen eingehen. So benutzen etwa 64 Prozent der IT-Entscheidungsträger echte Kundendaten für Anwendungstests.

Damit riskieren sie, dass Kundendaten unbemerkt an Dritte gelangen, warnt Gerald Pfeiffer, Manager Solutions Delivery bei Compuware, und ergänzt: „Dies kann nicht nur ernsthafte Auswirkungen auf das Vertrauen der Kunden und auf den Ruf des Unternehmens haben, sondern auch das Geschäftsergebnis beeinträchtigen."

Die Variante, einfach keine Kundendaten zu nutzen, ist jedoch auch nicht so einfach. Das Schaffen umfassender Testdaten ist zeit- und kostenaufwändig. ►

Zu geringe Datenmengen beim Test einer Anwendung bedeuten wiederum, dass die Wahrscheinlichkeit von Fehlern im späteren Live-Einsatz sehr hoch ist.

„Die datenschutzrechtlich saubere Vorgehensweise ist gestuft. In der Testphase werden keine Echtdaten, sondern spezielle Testdaten verwendet. Erst wenn die Software qualitätsgesichert und getestet ist, sind Praxiserprobungen mit Echtdaten zulässig, wenn dabei die Vorgaben des BDSG beachtet werden", erläutert NIFIS-Vorstand Dr. Thomas Lapp.

Eine Möglichkeit zur Lösung des Problems ist die Anonymisierung der Daten. In einem automatisierten Prozess können Werte ausgetauscht werden, sodass die Felder intakt bleiben, aber kein Rückschluss auf einzelne Personen gezogen werden kann. Weitere Informationen finden Sie hier. ❑

Webweiser 5.0

Zum fünften Mal findet der „Webweiser für Entscheider – E-Business im Mittelstand“ statt. Der immer stärker werdende Wettbewerb im elektronischen Geschäftsverkehr verlangt nach fundiertem Know-how. Erfolgsentscheidend sind heutzutage sowohl eine sichere Basis, auf der ein Unternehmen agieren kann, als auch ►

das Wissen um den Aufbau und das Ausschöpfen von Wettbewerbsvorteilen. Im Kloster Schiffenberg bei Gießen referieren am 20. September namhafte Unternehmen neben regionalen Vertretern der IT-Branche in 18 Fachvorträgen zu diesen aktuellen Themen. NIFIS-Vorstand Dr. Thomas Lapp wird ab 15.45 Uhr in seinem Vortrag die Frage klären: Sicherheit der IT – Warum geht mich das an? Veranstalter der Fachtagung ist der NIFIS-Kooperationspartner BIEG Hessen. Das Teilnahmeentgelt beträgt 65 Euro. Weitere Informationen finden Sie hier. ❑

Eigene Mitarbeiter bedrohen IT-Sicherheit

Die größte Bedrohung für die IT-Sicherheit eines Unternehmens sind nicht Viren, Hacker oder Phishing-Attacken, sondern die eigenen Mitarbeiter. Die Experten von NIFIS gehen davon aus, dass mehr als die Hälfte der Sicherheitsvorfälle in den Betrieben auf das Konto der eigenen Angestellten geht.

Viele Unternehmen sind sich der zunehmenden Gefahr im eigenen Haus durchaus bewusst. „Es hapert aber noch an der Ergreifung adäquater Maßnahmen, um das davon ausgehende Schadenspotenzial einzudämmen", sagt NIFIS-Vorstandsvorsitzender Peter Knapp.

Die Initiative möchte deshalb zum einen die Mitarbeiter aktiv über aktuelle Bedrohungen aufklären. Zum anderen will sie die Führungsebene bei der Einführung von Konfliktmanagementsystemen, der angemessenen Ausgestaltung von Arbeitsverträgen und der Beschaffung schützender IT-Systeme unterstützen.

Wichtig ist im ersten Schritt zu unterscheiden, ob die Bedrohung durch eigene Mitarbeiter bewusste oder unbewusste Schädigungen sind. Auftretende Sicherheitslücken, weil die Mitarbeiter bestimmte Verhaltensregeln nicht kennen, können beispielsweise durch Information und Schulungen beseitigt werden. Schwieriger wird es bei Sicherheitsvorfällen, die auf Böswilligkeit oder Nachlässigkeit zurückzuführen sind. ►

Die Gründe dafür liegen meist in der mangelnden Motivation der Mitarbeiter oder schwelenden Konfliktherden zwischen einzelnen Personen oder Abteilungen. Empfehlenswert sind hier die Einführung eines Konfliktmanagementsystems und der Einsatz interner Mediatoren. Weitere Informationen finden Sie hier. ❑

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.

ISO/IEC 27001-Zertifikat als Wettbewerbsfaktor

Die zunehmende Internationalisierung der Unternehmen und ihrer Geschäftsbeziehungen macht es notwendig, dass diese sowohl intern als auch extern ein nachvollziehbares Maß an Informationssicherheit leben und dokumentieren. Ausschlaggebend ist hierbei die Planung, Organisation und Integration der Informationssicherheit in sämtliche Geschäftsprozesse eines Betriebes. Aus diesem Grund rät NIFIS, dass Unternehmen ein Information Security Management System (ISMS) schaffen, um dieses in einem nächsten Schritt zertifizieren zu lassen.

„Ein zertifiziertes ISMS wird in Zukunft ein Qualitätsmerkmal von Unternehmen sein und somit auch entscheidend zum geschäftlichen Erfolg in einem immer schwierigeren Marktumfeld beitragen", bestätigt Brad Chapman, Partner bei KPMG, einem der Gründungsmitglieder der NIFIS. Als Zertifizierungsschema zur Zertifizierung eines ISMS ist der British Standard (BS) 7799 beziehungsweise dessen Nachfolgenorm ISO/IEC 27001 international verbreitet und anerkannt. ►

Die auf der Basis des ISO/IEC-Standards durchgeführte Zertifizierung eines ISMS dokumentiert, dass das Unternehmen seine Informationssicherheit im Sinne eines Managementsystems betreibt und somit bewusst mit dem Thema Informationssicherheit umgeht.

So ein Zertifizierungsprojekt erfordert jedoch eine sorgfältige Vorbereitung. Hilfreich ist das NIFIS-Siegel – ein Selbstaudit, der an den ISO/IEC 27001-Standard angelehnt ist. Geeignet ist dies insbesondere für mittelständische Unternehmen, die sich bisher noch nicht mit dem Thema Zertifizierung von Internet- und Informations-Sicherheit auseinandergesetzt haben sowie diejenigen, die langfristig eine ISO/IEC 27001-Zertifizierung anstreben.

Ziel ist es, mit geringem Aufwand Lücken und Mängel in den eingesetzten Systemen und Prozessen aufzudecken, um anschließend geeignete Gegenmaßnahmen zu definieren und umzusetzen. Mitglieder von NIFIS können sich **kostenlos** um das Siegel bewerben, für Nichtmitglieder liegen die Kosten bei 150 Euro. ❑

NIFIS begrüßt neue Mitglieder

Im dritten Quartal konnte NIFIS wieder einige neue Mitglieder gewinnen, die an dieser Stelle herzlich willkommen geheißen werden: Astaro AG, Blumen Mächtlen GbR, OKI Systems GmbH, SiG Software Integration GmbH, ST-oneline und der Verband der Metall- und Elektrounternehmen Hessen e.V. genießen nun die Vorteile der NIFIS-Mitgliedschaft und können die Aktivitäten des Vereins aktiv mitgestalten.

NIFIS ist 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: VoIP sicher betreiben

Die 10. EUROFORUM-Jahrestagung zum Thema IT-Sicherheit findet vom 18. bis zum 21. September in Düsseldorf statt. Sie richtet sich vor allem an Geschäftsführer, IT-Sicherheitsverantwortliche, CISO sowie IT-Sicherheitsdienstleister. Die Veranstaltung bietet die Gelegenheit, sich umfassend über aktuelle Trends und neue technische Herausforderungen der IT-Sicherheit zu informieren.

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 gehört. ❑

NIFIS beim IT-Security-Forum

Vom 27. bis zum 30. November findet das IT-Security-Forum in Bad Homburg statt. Bereits zum 6. Mal treffen sich IT-Security-Verantwortliche zu Praxisvorträgen, Erfahrungsaustausch und Workshops. Vier Tage lang versorgen Spezialisten und Fachgrößen die Teilnehmer mit interessanten Analysen und Informationen, um auf aktuelle Bedrohungen wirksam reagieren zu können. ►

Besondere Schwerpunkte liegen in diesem Jahr in den fünf Fachforen zu den Themen Schnittstellensicherheit, Identity & Accesss Management, Awareness, Applikations-Sicherheit und Security Prozesse. Im Bereich Applikations-Sicherheit wird Vojislav Kosanovic vom NIFIS-Gründungsmitglied KPMG über die Sicherheit in Web-Applikationen referieren.

Im Mittelpunkt stehen dabei Client- und Server-Security, die Sicherheit von JavaWebStart (JWS) & .NET-Anwendungen sowie Angriffe auf Datenbanken mittels SQL-Injection. Alle Forumsteilnehmer des IT-Security-Forums erhalten freien Zutritt zum parallel stattfindenden Business Continuity Management Forum. ❑

Wir über uns

Mitgliederinterview IT Advisory Group

Als NIFIS-Gründungsmitglied gibt die IT Advisory Group Einblicke in Business Security Management.

Die IT Advisory Group Unternehmensberatung AG, kurz ITAG, wurde 2001 gegründet und ist eine 100-prozentige Tochter der Magirus AG. Ihre Schwerpunktaufgaben sind die Bereiche Systemsmanagement, SAP sowie Sicherheit, Prozessberatung und Biometrie. Der Hauptsitz befindet sich in Mainz, die offizielle Zentrale in Stuttgart. Die ITAG beschäftigt zurzeit 40 Berater. Die meisten Kunden sind Großunternehmen, die in den Bereichen Rechenzentrums- und Systemsmanagement betreut werden.

Die Redaktion von NIFIS advice sprach mit:

Vorstand Lars Büchel und Arslan Brömme, Berater Security & Biometrics.

Welche Leistungen erbringen Sie konkret im Bereich der IT-Sicherheit?

Brömme: Die IT Advisory Group bewegt sich vornehmlich im technischen Bereich der IT-Sicherheit, vor allem Schutz-, Sicherheits- und Bewertungsfragen von Rechenzentren. Zu den Leistungen zählen unter anderem die Auditierung und Evaluierung von bestehenden Sicherheitssystemen und konzeptionellen Entwürfen. Darüber hinaus werden auch neue Themengebiete in der IT-Sicherheit aktiv angegangen, wie beispielsweise RFID und Biometrie.

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

Büchel: Da gibt es eine ganze Reihe von Aspekten. Zum einen das Schaffen von Awareness, von Bewusstseinsbildung bei Unternehmen, denn viele haben die Tragweite des Themas IT-Sicherheit noch nicht vollkommen erfasst. Sie scannen E-Mails auf Viren und haben vielleicht auch eine Firewall. Aber das bedeutet nicht wirklich Sicherheit. Oftmals fehlen die Ideen und Konzepte hinsichtlich der Aufstellung einer richtigen, durchgehenden und greifenden Sicherheitspolitik. Und das ist das, was wir anbieten, und was wir über unsere Mitgliedschaft bei NIFIS in den Markt hineintragen möchten. Zum anderen geht es auch um Networking: Was machen andere Unternehmen, was können wir verbessern, lernen, wo mit anderen kooperieren?

NIFIS bündelt als Kompetenzzentrum das Fachwissen ausgesuchter Gründungsmitglieder. Für welchen Themenkomplex sind Sie dabei zuständig?

Büchel: Wir sind schwerpunktmäßig im Bereich Business Security Management tätig. Dabei betrachten wir die notwendigen Sicherheitsmechanismen in einem Unternehmen aus Sicht der Geschäftsführung, des Managements und der IT-Leitung. Die Evaluation ermittelt hierbei unter anderem den Geschäftswert der eingesetzten IT-Sicherheitstechnologien und -maßnahmen.

Warum ist Business Security Management wichtig?

Brömme: Das Sicherheitsmanagement ist insbesondere ein organisatorischer und nicht nur ein technischer Aspekt, um Sicherheitsmaßnahmen Erfolg versprechend in einem Unternehmen zu etablieren. Sicherheit sollte nicht nur auf dem Papier existieren, sondern unternehmensweit „gelebt“ werden. Dieses hat vor allem Einfluss auf die Unternehmenskultur. Die standardisierte Evaluation von IT-Sicherheitsmaßnahmen in Unternehmen ermöglicht zielgerichtet auch eine Vergleichbarkeit zur Einschätzung des Sicherheitsniveaus der nationalen IT-Sicherheitsinfrastruktur in Deutschland. ►

„Standardisierte Evaluation" – was ist das genau?

Büchel: Die IT Advisory Group hat zusammen mit dem Fraunhofer Institut für System- und Softwaretechnik das Joint Venture INNOVA Beratungsgesellschaft mBH gegründet. Gemeinsam haben wir ein softwarebasiertes Produkt namens ITEM entwickelt, wobei ITEM für IT Evaluation Management steht. Es trifft im Rahmen von Erhebung, Analyse und Bewertung eine Aussage dazu, wie gut und angemessen die vorhandene IT für die Herausforderungen der Gegenwart und der Zukunft ist. Das Produkt nimmt die standardisierte Bewertung vor, es basiert auf wissenschaftlicher Grundlagenforschung zur Bewertung von IT. Das Fraunhofer Institut hat die Methodik entwickelt und versucht, nicht nur technische oder ökonomische Aspekte anzuschauen, sondern die Komplettheit der IT unter dem Oberbegriff „Angemessenheit". Die IT Advisory Group hat das technische und zum Teil auch das ökonomische Know-how in die Entwicklung von ITEM eingebracht.

Wie sieht Ihre Unterstützung für NIFIS-Mitglieder konkret aus?

Brömme: Wir entwickeln gemeinsam mit unseren NIFIS-Partnern Prozesse zur Evaluierung und Zertifizierung der in einem Unternehmen eingesetzten IT-Sicherheitsmaßnahmen. Unternehmen können zunächst einmal das NIFIS-Siegel beantragen. Dabei führen sie einen Selbstaudit durch und bekommen eine erste Einschätzung der Sicherheitslage. Zur Abdeckung des weitergehenden Bedarfs plant NIFIS Lösungen zu entwickeln, die in den nächsten Monaten konkretisiert werden sollen.

Warum sollten weitere Unternehmen Mitglied bei NIFIS werden?

Büchel: Da kann man den alten Gewerkschaftsspruch anwenden: Einigkeit macht stark. Es geht bei der NIFIS in erster Linie um Bewusstseinsbildung in Bezug auf die IT-Sicherheit. Das funktioniert nur dann gut, wenn viele mitmachen. Das Gründungsmotto der NIFIS lautet: aus der Wirtschaft für die Wirtschaft. Wir sind ein Verein mit Mitgliedern, die sich selbst engagieren möchten, ihre eigene Sicherheit fördern und dafür sorgen, dass die Welt um sie herum sicherer wird.

Wie sehen Sie die weitere Entwicklung von NIFIS?

Büchel: Wir haben einen sehr guten Start hingelegt. Der Verein ist etwa ein Jahr alt und konnte kontinuierlich Mitglieder gewinnen. Wir sehen die künftige Entwicklung der NIFIS sehr positiv. Meine Vorstellung, die zum Teil schon verwirklich wurde, ist, dass NIFIS eine nationale Initiative darstellt, die wirkliches Gewicht hat, die gehört wird, der man zuhört, die aber auch Ideen und Erkenntnisse präsentiert und wichtige Impulse für den Wirtschaftsstandort Deutschland liefert.

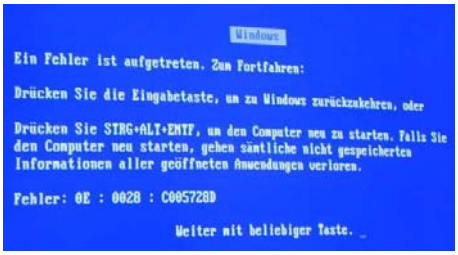
Wir danken für dieses Gespräch! ❑

Wir für Sie

Stopfen Sie Ihre Sicherheitslöcher!

Sicherheitslücken sind eine Bedrohung, mit der sich Unternehmen dringend auseinandersetzen müssen. Um rechtzeitig über Gefahren informiert zu sein, bietet NIFIS ihren Mitgliedern einen Warn- und Informationsdienst.

Eine Sicherheitslücke ist eine Schwachstelle in einer Software, durch die ein schädliches Programm oder ein Hacker in den Rechner eindringen kann. Sicherheitslücken in einem Betriebssystem wie Windows oder Linux oder in einem Anwendungsprogramm wie der Textverarbeitung entstehen nicht plötzlich, sondern durch Programmierfehler. Sie lassen sich auch bei sorgfältigster Programmierung nicht vermeiden. Man schätzt, dass pro 1.000 Zeilen Code im Mittel etwa zwei Fehler auftreten. Diese Sicherheitslücken werden irgendwann von Hackern oder Sicherheitsspezialisten entdeckt. Weil einmal entdeckte Sicherheitslöcher unter Garantie ausgenutzt werden, und zwar schneller als einem lieb sein kann, ist es wichtig, diese Sicherheitslücken schnellstmöglich zu stopfen. So stand zum Beispiel für die vom Blaster-Wurm weltweit ausgenutzte Sicherheitslücke schon rechtzeitig ein Patch (Flicken) vom Softwarehersteller zur Verfügung. Systeme, auf denen der Patch installiert war, waren von dem Angriff nicht betroffen.



Tagesaktuelle Information statt aufwändiger Suche

Um hier rechtzeitig über Sicherheitslücken informiert zu werden, bietet NIFIS im Rahmen der Mitgliedschaft einen Warn- und Informationsdienst (WID) an. Die Bereitstellung des Dienstes erfolgt in Kooperation mit der CERTCOM AG. Durch die Verteilung tagesaktueller Warnungen und Hinweise (Security Advisories) per E-Mail werden NIFIS-Mitglieder stets über aktuelle Bedrohungen (Sicherheitslücken) informiert. Eigene, aufwändige Recherchen sind daher nicht mehr erforderlich. Die in die deutsche Sprache übersetzten Security Advisories sind nach Risiko, Schadens- und Eintrittspotenzial klassifiziert, sodass ein Administrator auf den ersten Blick erkennt, welche Systeme betroffen sind und bei welchen Kombinationen von Betriebssystem und Anwendungssoftware die Schwachstelle auftritt. Ist keines der betroffenen Systeme in Betrieb, so ist das Advisory unerheblich und muss nicht weiter beachtet werden.

Bei Interesse am „WID" senden Sie einfach eine entsprechende E-Mail an newsletter@nifis.de. ❑

Praxistipp

Kontinuierliche Klimaüberwachung in Rechenzentren

Heiße Sommer, neue Technologien und der Anspruch, alle verfügbaren Kapazitäten in den Serverschränken maximal auszunutzen, sind eine extreme Belastung für die meisten Rechenzentren. Die hohe Leistungsfähigkeit der Geräte und die damit verbundene hohe Wärmeabgabe reizen die physikalischen Möglichkeiten konventioneller Klimatisierungsmethoden wie die Klimatisierung durch den Doppelboden oder eine einfachen Raumklimatisierung in vielen Fällen aus und können in den Rechenzentren für Hot-Spots sorgen. Der Grund dafür ist, dass es physikalisch gesehen extrem schwierig wird, eine beliebige Menge an kalter Luft durch die Racks zu leiten. In Rechenzentren mit einer hohen Packungsdichte müssen deshalb zusätzliche Maßnahmen eingeleitet werden, die vom Einbau einfacher Luftleitbleche bis hin zur Integration kostenintensiver Wasserkühlungen reichen können.

Peter Knapp
Vorstandsvorsitzender NIFIS

Wichtig für den ausfallsicheren Betrieb ist nicht nur der Einsatz leistungsfähiger Systeme, sondern auch die regelmäßige Wartung und Überwachung, denn sollte die Klimatisierungsinfrastruktur ausfallen oder nicht mehr ordnungsgemäß funktionieren, ist es, abhängig von der Packungsdichte, nur eine Frage von Minuten oder wenigen Stunden, bis sich die Server aufgrund von Überhitzung abschalten. Deshalb ist eine permanente Überwachung und Aufzeichnung von Luftfeuchtigkeit und Raumtemperatur in Rechenzentren wichtig, damit frühzeitig Entwicklungen erkannt werden können. Wenn ein Klimatisierungsgerät nicht ordnungsgemäß funktioniert, kann sich dies über mehrere Stunden abzeichnen, da die Raumtemperatur sukzessive ansteigt. Durch ein Monitoring – eine menschliche oder technische Überwachung – können solche Tendenzen frühzeitig erkannt, und rechtzeitig Ursachenforschung und Gegenmaßnahmen noch vor dem Erreichen einer Alarmschwelle eingeleitet werden.

Empfehlenswert ist jedoch die Überprüfung der Funktionsfähigkeit der gesamten Klimatisierungsinfrastruktur. Dazu bieten sich regelmäßige Technikkontrollen an, die von Mitarbeitern durchgeführt werden sollten, da die Wahrnehmung des menschlichen Auges über den Sensor hinaus Informationen liefert. Um allen Eventualitäten entgegenzuwirken, sollte zusätzlich noch ein Alarmierungssystem eingebunden werden, das bei einem bestimmten Schwellenwert reagiert. In der Praxis haben sich die Kombination aus menschlicher Intelligenz und Technik als zuverlässiges Konzept bewährt.

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

Sicherheitsupdate

Wirtschaftskriminalität nimmt zu

Mehr als 89.000 Fälle von Wirtschaftskriminalität hat das BKA im vergangenen Jahr in Deutschland verzeichnet. Das ist ein Anstieg um 9,9 Prozent gegenüber 2004. Wie das BKA in seiner jährlichen polizeilichen Kriminalstatistik weiter mitteilt, hat vor allem der Bereich Wirtschaftskriminalität mit dem „Tatmittel Internet“ deutlich zugelegt und zwar um 73,1 Prozent auf 4.643 Fälle. Das Segment wird allerdings erst seit 2004 überhaupt erfasst, noch nicht alle Bundesländer haben deshalb diese Daten vorgelegt. Der durch Wirtschaftskriminalität verursachte Schaden sank von 5,6 Milliarden Euro im Jahr 2004 auf 4,2 Milliarden Euro im Jahr 2005. ❑

Viren verursachen Milliardenschaden

In den USA wurde 2005 etwa ein Drittel der Internet- und Computer-Anwender zum Opfer eines Cyberspace-Angriffs. Das berichtet die US-amerikanische Verbraucherorganisation Consumer Reports. Insgesamt hätten die Anwender in den vergangenen zwei Jahren mehr als acht Milliarden US-Dollar Schaden hinnehmen müssen – 5,2 Milliarden US-Dollar allein durch Viren. Phishing verursachte Berechnungen der Organisation zufolge einen Schaden von 630 Millionen, Spyware von 2,6 Milliarden US-Dollar. Mehr als die Hälfte der telefonisch zu diesen Themen befragten 2.000 Haushalte fühlte sich massiv durch Spam belästigt. ❑

USA ist Spamland Nummer 1

23,2 Prozent der weltweiten Spam-E-Mails kamen im zweiten Quartal aus den USA. Das berichtet Sophos. In der Rangliste folgen China (20 Prozent), Südkorea (7,5 Prozent) und auf Platz vier Frankreich (5,2 Prozent). Deutschland liegt mit 2,5 Prozent auf Platz neun, wobei der Anteil im ersten Quartal noch drei Prozent betrug. Nach Kontinenten verteilt führt Asien laut Sophos mit 40,2 Prozent deutlich, Europa hole aber auf und habe mit 27,1 Prozent bereits Nordamerika überholt. Immer mehr Spam-E-Mails benutzen Grafiken statt Text und gelangen so an den Filtern vorbei: Im Januar lag ihre Zahl bei 18,2, im Juni bereits bei 35,9 Prozent. ❑

Viele Viren passieren Scanner

Gängige Virenscanner erkennen nur jedes fünfte Schadprogramm – 80 Prozent der Viren und Würmer passieren diese problemlos und landen auf den Rechnern. Das berichtet das Australian Computer Emergency Response Team (AusCERT). Zum einen verfügten die Entwickler von Malware über immer größeres Know-how. Andererseits kooperieren die Hersteller der Software zu wenig, sie sollten sich austauschen, um einen best möglichen Schutz der Anwender zu erreichen, empfiehlt das AusCERT. ❑

IT-Sicherheit branchenabhängig

Die einzelnen Branchen weisen sehr große Unterschiede bei der Sicherheit von Informationen und Computersystemen auf. Das ergab die alljährliche Deloitte Sicherheitsstudie. Die Finanzindustrie investiere schon seit vielen Jahren mit absoluter Priorität in IT-Sicherheit. In dieser Branche sei die Zahl krimineller Cyberattacken rapid gestiegen, viele Angriffe zielten direkt auf materiellen Gewinn ab.

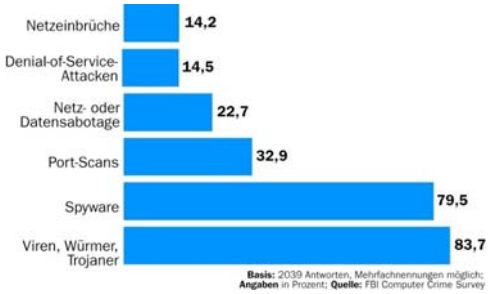
88 Prozent der Finanzdienstleister verfügen über unternehmensweite Business-Continuity-Programme – im Bereich der Technologie-, Medien- und Telekommunikationsunternehmen (TMT) waren es gerade einmal die Hälfte der Befragten. Mehr als die Hälfte der befragten TMT verzeichnete in den letzten zwölf Monaten konkrete Angriffe, rund ein Drittel davon resultierte in einem signifikanten finanziellen Schaden. Die TMT müssten dringend nachholen, indem sie vor allem eine umfassende Sicherheitsstrategie entwickeln und einführen.

Die Branche Life Sciences sei stark auf die Erfüllung von Compliance-Anforderungen konzentriert. Zwei Drittel der Befragten beschäftigen mittlerweile einen Chief Security Officer. Allerdings verfügen lediglich sieben Prozent über ein ausgereiftes, unternehmensweites Datenschutzprogramm. ❑

Spyware – die unterschätzte Gefahr

Nicht nur lästig und schwer zu beseitigen: Spionage-Tools, mit denen Unbefugte Firmeninterna ausspionieren können, sind eine Bedrohung, die Administratoren zunehmend zu schaffen macht.

Niemand lässt sich gern auf die Finger schauen. Doch das Interesse an dem, was andere auf ihrem Heim-PC oder Bürorechner tun, nimmt angesichts des lukrativen Geschäfts mit heimlich erforschten Informationen stetig zu. Eine Vielfalt an Spionagewerkzeugen, auch „Spyware" oder „Adware" genannt, ermöglicht es den häufig kriminellen Urhebern, ihre Neugier zu befriedigen und aus den ergatterten Daten Profit zu schlagen.



Grundsätzlich handelt es sich dabei um Programme, mit denen sich das Verhalten eines PC-Anwenders überwachen und auswerten lässt. Ihre Bandbreite reicht von einfachen Cookies über entsprechende Funktionen innerhalb werbefinanzierter Hilfsprogramme über das so genannte Browser-Hijacking bis hin zu komplexen Tools, die einzelne Aktivitäten protokollieren und sogar die Komplettüberwachung eines Rechners erlauben.

Obwohl Spyware in ihrer ersten harmlosen Erscheinungsform bereits vor rund zehn Jahren auftauchte, entdeckten Sicherheitsforscher erst 1999 ein Programm, das – via Gratis-Download auf den Rechner geschmuggelt – tatsächlich personenbezogene Informationen an seinen Urheber zurückschickte. In den vergangenen sechs Jahren haben sich die hinterlistigen Schnüffel-Tools rasant weiterentwickelt und stellen ► nach Einschätzung von Experten bald eine größere Bedrohung dar als klassische Viren und Würmer.

Mittlerweile hat das Spyware-Problem erschreckende Ausmaße angenommen. Der jüngsten „Computer Crime Survey" des FBI zufolge standen Attacken durch Spionagesoftware gleich nach dem Befall durch Viren ganz oben auf der Liste der im Jahr 2005 verzeichneten Sicherheitsvorfälle. Zusammen verursachten die beiden Bedrohungen finanzielle Verluste in Höhe von rund zwölf Millionen Dollar.

Auch der „State of Spyware Report" von Webroot für das erste Quartal 2006 deutet darauf hin, dass die Digitalspionage kein Strohfeuer, sondern ein längerfristiges Problem ist: Demnach hat die Quote der von Spyware infizierten, privat genutzten PCs mit 87 Prozent ihren Höchststand seit Anfang 2005 erreicht. Nahezu unverändert kritisch ist die Spyware-Lage offenbar in Unternehmen: Dem Security-Anbieter zufolge treiben auf infizierten Firmen-PCs nach wie vor durchschnittlich 21,5 komplexe Spionageprogramme wie Systemmonitore oder trojanische Pferde ihr Unwesen.

Mögliche Konsequenzen

Eine Webroot-Umfrage unter kleinen und mittelständischen Unternehmen ergab zudem, dass im ersten Quartal 2005 mehr als die Hälfte dieser Betriebe Opfer eines Spyware-Angriffs wurden. Zu den beklagten Folgen zählten nicht nur reduzierte Systemleistung (65 Prozent der Befragten) und geringere Mitarbeiterproduktivität (58 Prozent), sondern auch ein „Negativeinfluss" auf den Firmengewinn (35 Prozent) sowie Vertriebsverluste (20 Prozent).

Nach Einschätzung des Sicherheitsanbieters Aladdin, demzufolge sich das Spyware-Aufkommen 2005 im Vergleich zum Vorjahr sogar verdreifacht hat, spionieren bereits rund 15 Prozent aller Schnüffler-Varianten unternehmenskritische Daten wie Passwörter und Benutzernamen aus und sind somit als „ernsthafte Gefahr" einzustufen.

Meist werden die beiden Begriffe Spyware und Adware synonym ►

verwendet. Dabei lassen sich die beiden Programmgattungen nur bedingt vergleichen. So sind die häufig im Schlepptau von Peer-to-Peer-Programmen oder Banner-Werbung befindlichen Adware-Tools nicht per se als „bösartig" zu bezeichnen: Sie dienen primär dazu, das Surfverhalten der Anwender zu analysieren, um Werbeinhalte gezielt auf dessen Interessen zuzuschneiden, und weisen in der Regel auf die Weiterleitung der gewonnenen Daten hin. Auch erfolgt ihre Installation nicht heimlich, sondern meist über die via Nutzungsbedingungen der Software eingeholte Zustimmung des PC-Besitzers.

Böswillige blinde Passagiere

Von anderem Kaliber ist Spyware, die versucht, sich vom Nutzer unbemerkt auf dem Rechner einzunisten, und häufig auch ohne bestätigenden Mausklick des Anwenders auf die Festplatte gelangt. Sie nutzt dazu Sicherheitslücken im Betriebssystem und im Browser aus und verschleiert ihre Existenz raffiniert. Im schlimmsten Fall protokollieren die digitalen Schnüffel-Tools sämtliche Tastatureingaben – damit liegen auch alle Passwörter sowie Konto- oder Kreditkartendaten offen – und senden dieses Log an entfernte Rechner. Spyware bedroht demnach die Vertraulichkeit sensibler institutioneller wie persönlicher Informationen. Allerdings treten die digitalen Spione häufig nicht mehr im Alleingang, sondern zunehmend in Kombination mit Bedrohungen wie Spam, Viren oder Würmern auf.

Oft reicht es schon, einige Gratisprogramme herunterzuladen oder mit einem ungepatchten PC beziehungsweise laxen Sicherheitseinstellungen zu surfen, um sich ein ganzes Heer digitaler Spione einzufangen. Dabei gelangt Spyware im Normalfall nicht isoliert ins Firmennetz, sondern getarnt im Schlepptau anderer, scheinbar harmloser Datenpakete. Klassische Wirte sind Free- oder Shareware. Gängig ist auch der Transport via E-Mail – hier verbirgt sich die Spyware häufig hinter einer ausführbaren „Exe"-Datei – sowie über alle Arten von Files, die per Peer-to-Peer-Programmen ausgetauscht werden. ►

Mit immer ausgefeilteren Methoden versuchen die Spyware-Autoren, die Diagnose- und Removal-Tools der Antivirenhersteller auszutricksen.

Dabei geht es in erster Linie darum, die digitalen Spione vom Anwender unbemerkt zu installieren. Hierzu arbeiten Spam und Spyware häufig Hand in Hand: Der Nutzer bekommt eine harmlos anmutende Mail, die jedoch einen Trojaner mitbringt. Verschärfend wirkt sich das Zusammenspiel mit Würmern und Bots aus, da diese zur Massenverbreitung solcher Mails beitragen, aber auch die Kombination mit Viren, die am Zielort automatisch Spyware herunterladen, hat es in sich. Ein weiterer Infektionsherd sind Web-Seiten mit aktivem Spionagecode, der sich beim Aufrufen, ohne sichtbares Dialogfenster, heimlich auf den Rechner lädt („Drive-by-Download").

Zu den gefährlichsten Schnüfflerkategorien gehören Keylogger. Dabei handelt es sich um schwer auffindbare Überwachungswerkzeuge, die jede Tastatureingabe protokollieren sowie Screenshots anfertigen können und die Spionagedaten dann in unauffälligen Paketen verschicken. Beim Browser-Hijacking wiederum wird die Startseite des Browsers auf zwielichtige Portale umgelenkt, während ein verborgenes Skript die Einstellung der ehemaligen Startseite verhindert.

Vorbeugen und enttarnen

Ganz auszuschließen ist die Infektion mit Spyware nicht, doch lässt sich der Digitalspionage gezielt vorbeugen. Als erste Maßnahme sollten Unternehmen ihren Mitarbeitern klare Regeln im Hinblick auf Web-Nutzung, den Schutz persönlicher Zugangscodes sowie den Umgang mit elektronischer Post und externen Speichermedien an die Hand geben.

Häufig lässt sich der Befall durch Spyware aber nur mit technischen Mitteln verhindern oder aufdecken. Zu den unerlässlichen Schutzvorrichtungen zählt ein Web-Filter am Gateway, der den Zugriff auf als kritisch eingestufte Sites unterbindet und verdächtige URLs blockiert. Auf Gateway- und Desktop-Ebene eingerichtete Viren- und Spyware-Filter wiederum ► untersuchen den ein- und ausgehenden Datenverkehr sowie auf den Systemen befindliche Applikationen auf bekannte Viren- und Spyware-Signaturen.

Weitere Abwehrmaßnahmen sind ein Spam-Filter zum Abblocken von Junk-Mails sowie der Einsatz einer Firewall. Dank ihrer Reporting-Funktionen, die die Netzauslastung messen, kann diese ebenfalls Hinweise auf einen Befall durch Spyware liefern. In ganz hartnäckigen Fällen ist unter Umständen ein tieferer Griff in die Trickkiste beziehungsweise die Analyse von Logfiles und Netz-Traffic vonnöten. Hilfreiche Dienste können hier Netz-Sniffer wie das quelloffene „Ethereal" leisten, das den Datenverkehr protokolliert und so Schadcode lokalisieren kann. *(Katharina Friedmann)*

Weitere aktuelle Security-Informationen finden Sie hier. ❑

IMPRESSUM

Herausgeber
NIFIS e.V.
Weismüllerstraße 21
60314 Frankfurt
Tel.: 0 69 / 40 80 93 70
Fax: 0 69 / 40 14 71 59
E-Mail: newsletter@nifis.de
Internet: http://www.nifis.de
Peter Knapp (V.i.S.d.P.)

Redaktion
FRESH INFO +++
http://www.fresh-info.de