Nationale Initiative für Internet-Sicherheit

advice
Ausgabe 04/2006

Liebe NIFIS-Mitglieder,
sehr geehrte Interessenten und Förderer,

ein ereignisreiches Jahr neigt sich dem Ende zu und NIFIS kann, als 18 Monate junger Verein, stolz auf das Geleistete zurückblicken. Ich möchte die Gelegenheit nutzen, um mich im Namen der NIFIS bei all den Personen und Unternehmen zu bedanken, die durch ihr Engagement das Vereinsgeschehen aktiv mitgestaltet und einen Beitrag zur Entwicklung des Vereins geleistet haben.

Auch für das kommende Jahr haben wir uns wieder einiges vorgenommen, um weitere Mehrwerte für unsere Mitglieder und neue Anreize für interessierte Unternehmen zu schaffen. Neben dem Forcieren der Kompetenzthemen möchten wir einen Stammtisch etablieren, durch den die vereinsinterne Kommunikation und die Wahrnehmung in der Öffentlichkeit verbessert werden sollen. Weitere Informationen dazu finden Sie in dieser Ausgabe von NIFIS advice – haben Sie viel Spaß beim Lesen!

Ich wünsche Ihnen, Ihren Familien, Mitarbeitern und Kollegen ein besinnliches und erholsames Weihnachtsfest und einen guten Start ins neue Jahr.

Mit freundlichen Grüßen

Peter Knapp

Vorstandsvorsitzender

HIGHLIGHTS

Kompetenzzentrum für „Identity Management“

NIFIS hat ein Kompetenzzentrum zu „Identity Management“ gegründet. Es befasst sich mit Fragen, Problemen und konkreten Lösungen im Zusammenhang mit der ganzheitlichen Verwaltung digitaler Identitäten. Den Vorsitz des neuen Expertenforums hat Dr. Horst Walther, Partner bei Kuppinger, Cole und Partner, übernommen.

Zu dem immer mehr an Bedeutung gewinnenden Thema hat der ausgewiesene Experte auf diesem Gebiet vor rund einem Jahr die Arbeitsgruppe „GenericIAM“ initiiert. Die Arbeitsgruppe, an der sich rund 20 Firmen beteiligen, darunter auch verschiedene DAX-Unternehmen, hat sich NIFIS angeschlossen und agiert ab sofort als Teil der Initiative.

Am 1. Dezember hat die bisherige Arbeitsgruppe GenericIAM unter NIFIS „konstituiert“ und knüpft ab sofort nahtlos an die seit rund einem Jahr geleistete inhaltliche Arbeit an. „Wir freuen uns, mit NIFIS die passende Organisation für Identity Management gefunden zu haben und unser Engagement einzig und alleine der inhaltlichen Arbeit widmen zu können“, begrüßt Dr. Horst Walther ► den Zusammenschluss. „Speziell vor dem Hintergrund der zunehmenden Digitalisierung ist Identity Management für unsere Mitglieder und die Wirtschaft von größter Bedeutung“, kommentiert Peter Knapp, Vorsitzender von NIFIS e.V., die Zusammenarbeit. ❑

NIFIS will Bundesregierung unterstützen

NIFIS bietet der Bundesregierung ihre aktive Unterstützung bei dem Vorhaben an, die Informationssicherheit in der Bundesrepublik Deutschland zu erhöhen. In ihrer Stellungnahme zum Aktionsprogramm „Informationsgesellschaft Deutschland 2010“ (iD2010) begrüßt der Sicherheitsverband der deutschen Wirtschaft ausdrücklich, dass die Bundesrepublik Deutschland den Bedrohungen für die Informationssicherheit künftig durch „Prävention, Reaktion und Nachhaltigkeit wirkungsvoll begegnen“ möchte, um dadurch „eine sichere Informationsgesellschaft“ zu schaffen. Insbesondere der vorgesehene Abbau der Bürokratie und die Etablierung prägnanter Regelungen seien in diesem Zusammenhang sinnvoll. „Allerdings ist das bloße Lippenbekenntnis allein nicht ausreichend“, betont NIFIS-Vorstand Peter Knapp. ►

„Jetzt kommt es darauf an, die sehr allgemein gehaltenen Feststellungen von iD2010 in konkrete Handlungen zur Erhöhung der Sicherheit umzusetzen. Dabei spielt die Einbindung der Wirtschaft eine maßgebliche Rolle.“ Hersteller von Sicherheitslösungen, Organisationen wie NIFIS und die Politik müssten an einem Strang ziehen, um Sicherheitskonzepte auf effiziente Weise zum Leben erwecken zu können.

Zahlreiche Projekte habe NIFIS bereits zu bekannten Problemen auf den Weg gebracht, bei denen sich die Politik immer noch im Planungsstatus befinde. Die angestrebte schnellere Reaktionsfähigkeit in IT-Krisen hat NIFIS beispielsweise durch die Bereitstellung von Hilfestellungen, sowohl in Form von Handlungsempfehlungen, Gesprächskreisen als auch Dienstleistungen, bereits mit konkreten Maßnahmen verwirklicht. ❑

NIFIS-Siegel der Bundesregierung voraus

Die Bundesregierung hat sich in ihrem Aktionsprogramm iD2010 auch zur Sicherung der Informationsinfrastrukturen der Bundesverwaltung beziehungsweise zur Beschreibung notwendiger Maßnahmen zur Sicherung der IT-Infrastrukturen in den Unternehmen geäußert. NIFIS hat bereits speziell für die mittelständische Wirtschaft das NIFIS-Siegel entwickelt.

Es stellt die erste Stufe im Prozess zur Vorbereitung einer Zertifizierung gemäß ISO 27001 dar und soll die Vertraulichkeit, Verfügbarkeit und Integrität von geschäftskritischen Daten in digitalen Unternehmensnetzwerken fördern. Im Selbstaudit beantworten die Antragsteller 82 Fragen aus den Bereichen organisatorische, logische, technische sowie physikalische Sicherheit. Diese Angaben werden vom NIFIS-Siegelrat analysiert und Mängel in den eingesetzten Sicherheitssystemen und Prozessen aufgezeigt. ►

Anschließend werden geeignete notwendige Maßnahmen zur Beseitigung der Mängel empfohlen, nach deren Umsetzung die Unternehmen das Sicherheitssiegel führen dürfen. Aktuell wurde das NIFIS-Siegel der Blumen Maechtlen GbR verliehen.

Mitglieder von NIFIS können sich **kostenlos** um das Siegel bewerben, für Nichtmitglieder liegen die Kosten bei 150 Euro.

Schreiben Sie bei Interesse eine E-Mail an newsletter@nifis.de. Weitere Informationen erhalten Sie hier. ❑

IT-Governance wichtig für alle

NIFIS rät Firmen dringend zur Einführung von IT-Governance. Während der Begriff Corporate Governance den rechtlichen und faktischen Ordnungsrahmen für die Leitung eines Unternehmens bezeichnet, übernimmt die IT-Governance die Leitfunktion für die Informationstechnologie.

Das Rahmenwerk für die Informationstechnologie gehört zwar primär zur Aufgabe der IT-Leitung, die Auswirkungen im Problemfall reichen jedoch in der Haftung bis auf die Vorstands- und Geschäftsführungsebene, warnt NIFIS-Vorstand und Rechtsanwalt Dr. Thomas Lapp. Für die Unternehmensführung stellt der Deutsche Corporate Governance Kodex den Bezugsrahmen dar. Er umfasst alle wesentlichen gesetzlichen Vorschriften zur Leitung und Überwachung deutscher börsennotierter Gesellschaften einschließlich deren Tochtergesellschaften nach nationalen und internationalen Standards.

Das Thema betrifft jedoch nicht nur die Vorstände von Großkonzernen, sondern auch den Mittelstand. „In einer Zeit, in der die Informationstechnologie in praktisch allen Unternehmen eine betriebswichtige Rolle spielt, fällt dem Ordnungsrahmen für die IT eine Schlüsselfunktion zu. Daher ist den Unternehmen unabhängig von der Firmengröße dringend zu raten, ein Regelwerk für IT-Governance aufzustellen, durchzusetzen und zu kontrollieren“, sagt Dr. Lapp. ►

NIFIS bietet als „Selbsthilfeorganisation der Wirtschaft“ unter anderem den Verantwortlichen für IT-Sicherheit ein Forum, um im gegenseitigen Erfahrungsaustausch Rahmenwerke für IT-Governance zu erarbeiten.

Weitere Informationen gibt es hier. ❑

NIFIS-Stammtisch geplant

Ab dem ersten Quartal 2007 organisiert NIFIS regelmäßig Stammtische, um den Austausch unter den Mitgliedern zu fördern. Der erste Treffpunkt wird Frankfurt am Main sein. Über zahlreiche Ideen und aktive Mitarbeit würden sich die Organisatoren freuen.

Interessenten wenden sich bitte an newsletter@nifis.de. ❑

NIFIS begrüßt neue Mitglieder

Im vierten Quartal konnte NIFIS wieder einige neue Mitglieder gewinnen, die an dieser Stelle herzlich willkommen geheißen werden:

- doubleSlash Net-Business GmbH,
- F.-J. Lang IT Security Consulting GmbH,
- Giegerich + Partner GmbH,
- iC Compass GmbH & Co. KG,
- ISM Institut für System-Management GmbH sowie
- Kuppinger, Cole und Partner

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 gibt es hier. ❑

Wir über uns

Mitgliederinterview COMPUWARE

Als NIFIS-Gründungsmitglied gibt Compuware Einblick in die Sicherheit von Software-Anwendungen.

Compuware ist ein Softwarehersteller und -dienstleister, primär im Bereich systemnaher Softwarewerkzeuge. Das Unternehmen wurde 1973 gegründet und hat derzeit weltweit circa 8.000 Mitarbeiter. Der Hauptsitz ist in Detroit (USA), die Firma ist in 33 Ländern weltweit vertreten. Kunden sind große und mittlere Unternehmen.

Die Redaktion von NIFIS advice sprach mit

Mareike Jacobshagen, MBA
Manager Marketing, EMEA Central Region

Was sind denn systemnahe Softwarewerkzeuge?

Compuware stellt Softwarewerkzeuge her und bietet damit verbundene Dienstleistungen an. Die Werkzeuge dienen beispielsweise zur Identifizierung von Fehlern und dem Fehlermanagement. Sie überprüfen Programmcodes auf Sicherheitslücken und melden, wenn sie eine potenzielle Angriffsfläche gefunden haben. Anschließend unterbreiten sie Vorschläge, was getan werden kann, um diese zu beseitigen. Unsere Expertise liegt darin, alle Abläufe innerhalb der IT-Organisation mittels verschiedener Lösungen effizienter und somit auch kostensparender und zielgerichteter zu gestalten. Dazu gehört auch, mittels Software und Services den IT-Wertbeitrag zum Unternehmenserfolg transparent zu machen.

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

Wir unterstützen NIFIS, weil wir für einige Themen im Bereich Security mehr Bewusstsein schaffen möchten, vor allem für Applikationssicherheit und Testdatenschutz.

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

Wir sind für die Sicherheit von Software-Anwendungen zuständig. Aktuellen Untersuchungen zufolge zielen circa 70 Prozent der so genannten Hacker-Angriffe auf Sicherheitslücken in Software-Anwendungen ab. Das können sowohl Standard-Softwareanwendungen als auch auf das Unternehmen zugeschnittene Anwendungen sein. In diesem Bereich möchten wir uns gerne engagieren und dafür sorgen, dass das Bewusstsein der Öffentlichkeit steigt, dass man Software von vornherein, also möglichst schon im Entwicklungsprozess, so gestalten muss, dass sie möglichst wenig Angriffsfläche bietet.

Netzwerke, mobile Geräte und eigene Mitarbeiter – das sind Unsicherheitsfaktoren, von denen wir häufiger hören. Inwiefern ist denn die Software in einem durchschnittlichen mittelständischen Unternehmen gefährdet?

Zunächst einmal ist Software in jedem Unternehmen im Einsatz. Ohne Software keine IT. Die eben erwähnten Hacker-Angriffe bergen also auch für mittelständische Unternehmen eine Gefahr. Aber wir müssen gar nicht von trickreichen Hackern ausgehen. Im Bereich Datenschutz muss zum Beispiel dafür gesorgt werden, dass nicht autorisierte Mitarbeiter keinen Zugriff auf bestimmte Datenbanken oder Software haben. Zugriffskontrollen und Authentifizierung sind hier wichtige Felder und eben auch der Testdatenschutz. Wenn beispielsweise eine Bank Anwendungen hat, die Kundendaten verarbeiten, dann werden diese in der Regel lediglich von autorisierten Mitarbeitern genutzt. Aber in dem Moment, wenn man die Software vielleicht warten oder ändern muss, gehen auf einmal fachfremde Leute mit dieser Software um und auch mit den damit zusammenhängenden Daten. Da muss genau geschaut werden, wie man die Daten schützt. Wenn man sich überlegt, dass Kundendaten von Dritten eingesehen oder gar zweckentfremdet werden, kann das extrem geschäftsschädigend wirken.

Was können Unternehmen konkret tun, um Software-Anwendungen sicherer zu machen?

Bei der Erstellung und Implementierung von neuer Software gibt es geeignete Prozesse, Methoden und Werkzeuge, um sie von Anfang an so sicher wie möglich zu machen. Man kennt ja die Security-Patches, die oft im Nachhinein von den Herstellern ausgeliefert werden. Das ist gut und wichtig. Aber noch besser wäre es, von vornherein dafür zu sorgen, dass diese Sicherheitslücken gar nicht erst entstehen. Da kann man im Vorfeld schon Einiges tun.

Gibt es einen leicht umsetzbaren Tipp, was ich als Unternehmen direkt und schnell selbst tun kann?

Sie könnten zum Beispiel Ihren Software-Lieferanten fragen, was er während des Entwicklungsprozesses getan hat, um eine unter Sicherheitsaspekten ►

möglichst unangreifbare Anwendung herzustellen. Das ist ein erster Schritt, der nichts kostet. Wenn Sie Software für Ihr Unternehmen maßgeschneidert entwickeln lassen, sollten Sie auf jeden Fall nach Methoden und Verfahren fragen, die vom Lieferanten bezüglich der Sicherheit zum Einsatz kommen.

Wie unterstützen Sie NIFIS-Mitglieder bei der Sicherheit von Software-Anwendungen?

Zum einen, indem wir uns mit Informationen und Aufklärungsarbeit im Rahmen des Gesamtkonzeptes von NIFIS um unsere Themen kümmern und in den Bereichen möglichst viel Transparenz schaffen wollen. Zum anderen arbeiten wir natürlich aktiv bei den verschiedenen Arbeitsgruppen mit, die helfen sollen, diese Security-Themen niedrigschwellig anzugehen, zum Beispiel das NIFIS-Siegel. Darüber hinaus arbeiten wir auch im Arbeitskreis Validierung mit, der eine Methode entwerfen wird, mit der Unternehmen ihre Sicherheit überprüfen können.

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

IT ist in unserem Internet-Zeitalter mittlerweile für alle erschwinglich und zugänglich geworden. Das ist einerseits toll – andererseits bietet das für Firmen auch eine große Angriffsfläche. Die Anzahl der IT-Experten ist groß geworden, und nicht alle haben gute Absichten. NIFIS klärt über die Risiken auf und gibt dann sehr pragmatische Hilfestellungen, wie man dem begegnen kann. Das ist für mich der Grund, warum die Unternehmen Mitglied werden sollten.

Wie sehen Sie die weitere Entwicklung von NIFIS?

Ich denke, dass NIFIS zunehmend eine breitere Basis finden und weitere Mitglieder gewinnen wird und aufgrund dessen eine größere Wahrnehmung in der Fachöffentlichkeit, aber auch in Wirtschaftskreisen, haben wird. Wir wollen mit NIFIS nicht nur IT-Verantwortliche ansprechen, sondern auch Geschäftsführer von mittelständischen Unternehmen mit dem Thema Sicherheit auf eine Art und Weise vertraut machen, dass sie nicht vorher Informatik studieren müssen.

Welche Themen möchten Sie im nächsten Jahr (bei NIFIS) forcieren?

Wir glauben, dass Softwaresicherheit noch länger ein wichtiges Thema bleiben wird. Je mehr auch von Herstellern und Kunden die Wiederverwendbarkeit von Software-Komponenten gefordert und gefördert wird, umso wichtiger wird das Thema. Die einzelnen Komponenten müssen von Anfang an so programmiert sein, dass sie möglichst wenig Angriffsfläche für Missbrauch bieten.

Wir danken für dieses Gespräch! ❑

Wir für Sie

Bringen Sie Ihre Daten in Sicherheit!

Immer mehr Daten in Unternehmen werden digital vorgehalten. Gleichzeitig nehmen die möglichen Gefahren wie Viren, Trojaner und Hackerangriffe zu. NIFIS stellt deshalb ihren Mitgliedern einen Online-Datensicherungsdienst zur Verfügung, mit dem automatisch die für den Geschäftsbetrieb kritischen und wichtigen Daten in einem Hochsicherheitsrechenzentrum abgelegt werden können.

Um den Online-Datensicherungsdienst zu nutzen, müssen nur einmalig die zu sichernden Daten definiert und das Sicherungsintervall festgelegt werden. Das System kann so konfiguriert werden, dass Daten nach bestimmten Kriterien automatisch zusätzlich revisionssicher archiviert werden. Zudem können die für den Geschäftsbetrieb nicht mehr kritischen Daten, die aber beispielsweise aufgrund gesetzlicher Bestimmungen vorgehalten werden müssen, vom Backupverzeichnis in ein Archiv verschoben werden.

Dank einer „agentenlosen Technologie“ muss lediglich auf einem PC oder Server im LAN die Managementsoftware installiert werden, die zur Systemkonfigurationen notwendig ist und die Datensicherung koordiniert. Für den Datensicherungsprozess bedeutet dies, dass die zu sichernden Daten im LAN virtuell gesammelt, inkrementiert, verschlüsselt (bis zu 256 nach AES), komprimiert und dann direkt in den in einem Hochsicherheitsrechenzentrum befindlichen Datentresor übertragen werden. Sollte es zu einem Datenverlust im Unternehmen kommen, sodass zuvor gesicherte Daten benötigt werden, können diese auf Knopfdruck in Echtzeit wiederhergestellt werden.

Gerade kleine und mittelständische Unternehmen profitieren vom Einsatz dieses Datensicherungssystems, da man nicht in eine eigene Backup-Infrastruktur investieren muss, und der Service skalierbar ist. Ebenso richtet sich der Dienst an Unternehmen, die Niederlassungen oder mobile Nutzer einbinden müssen. Mit der bereitgestellten Lösung können Daten (unter Microsoft, Novell, Linux, AS400, Mac und anderen Betriebssystemen) sowie verschiedene Datenbanksysteme, darunter Oracle, SQL, Exchange und Notes, während des laufenden Betriebs gesichert werden.

Mitglieder können die Online-Datensicherung im Rahmen der Mitgliedschaft kostenfrei in Anspruch nehmen. Je zu sicherndem GB Datenvolumen werden lediglich 1.400 NIFIS-Punkte berechnet. Bei Interesse senden Sie einfach eine entsprechende E-Mail an newsletter@nifis.de. ❑

Praxistipp

IT-Sicherheit in Vertragsverhandlungen

In Vertragsverhandlungen hört man immer wieder die Aussage „ein guter Vertrag wird nach Unterzeichnung in die Schublade gelegt und erst wieder hervorgeholt, wenn es zu Streitigkeiten zwischen den Vertragsparteien kommt". Dies spiegelt die allgemeine Geringschätzung der Bedeutung vertraglicher Regelungen wider. Viele Verhandlungspartner sind auf die so genannten „kommerziellen Bedingungen", nämlich Preis, Zahlungsziel und Teilzahlungen/Vorschüsse fixiert. Andere Teile der vertraglichen Vereinbarungen werden dagegen kaum beachtet.

Dr. Thomas Lapp, Rechtsanwalt und Vorstand der NIFIS

Dabei erstaunt, dass insbesondere auch die für den ausführlich ausgehandelten Preis zu erbringenden Gegenleistungen nur unzureichend beschrieben werden. Häufig wird auf die Dokumentation des Herstellers verwiesen, um beispielsweise den Leistungsumfang von Standardsoftware zu beschreiben. Auch bei individuellen Entwicklungen oder Anpassungen finden sich nur dünne Hinweise auf den vereinbarten Leistungsumfang.

Da kann es nicht verwundern, dass IT-Sicherheit entweder gar nicht oder nur indirekt über die „anerkannten Regeln der Technik" erwähnt wird. Wer bei der Definition seiner Anforderungen die IT-Sicherheit nicht erwähnt, darf nicht überrascht sein, wenn die Software letztlich keine ausreichenden Sicherheitsmechanismen enthält.

Besser ist es, die eigenen Anforderungen an die Sicherheit der IT zu definieren. Dabei ist die Bedrohungslage des Unternehmens ein wichtiger Faktor. Daneben sind die Anforderungen aus der Anlage zu § 9 BDSG zu berücksichtigen (Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und Trennungsprinzip).

Auch der Fragenkatalog zum NIFIS-Siegel gibt wertvolle Hinweise auf Sicherheitsanforderungen. Zudem sollten allgemeine Grundregeln definiert werden, welche ebenfalls Auswirkungen auf die Sicherheit haben. Die oft beklagten Sicherheitsprobleme, die die eigenen Mitarbeiter verursachen, sind in den wenigsten Fällen auf Vorsatz oder Desinteresse der Mitarbeiter zurückzuführen. Durch einfach und intuitiv bedienbare, fehlertolerante Software könnten viele Probleme vermieden werden.

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

Sicherheitsupdate

IT-Sicherheit auch von innen

Viele Unternehmen konzentrieren sich beim Thema IT-Sicherheit darauf, welche Gefahren möglicherweise von außen drohen. Sie gehen aktiv gegen Spam, Viren und Hacker vor. Doch was aus dem Unternehmen heraus geht, überprüfen wenige.

Eine Studie von Aberdeen zeigte, dass 72 Prozent der Befragten das externe Abrufen vertraulicher Geschäftsinformationen für eine mittlere bis große Bedrohung halten. Trotzdem verschlüsseln lediglich 25 Prozent ihre verschickten Daten. ►

Bei fast drei Viertel der Unternehmen ist mittlerweile Instant Messaging eine beliebte Möglichkeit, Daten schnell mit Kunden und Geschäftspartnern auszutauschen. Aber nur sieben Prozent der Befragten sehen Instant Messaging als geschäftskritisch. Aberdeen empfiehlt, klare Sicherheitsregeln festzulegen und alle Mitarbeiter diesbezüglich zu schulen. ❑

Hohe Verluste durch IT-Ausfall

Die Studie „The Global State of Information Security 2006" von PricewaterhouseCoopers (PwC) zeigt: Deutsche Unternehmen liegen mit ► durchschnittlich 78 IT-Ausfällen und -Problemen an dritter Stelle nach Schweden und Frankreich. Die Hälfte der IT-Probleme verursachten Hacker, 34 Prozent die eigenen und 13 Prozent ehemalige Mitarbeiter. Mit 58 Prozent zählten böswillige Codes wie Computerviren, Würmer und Pufferüberläufe wie im Vorjahr zu den häufigsten Waffen der Hacker gegen deutsche Unternehmen. Dadurch verlangsamten sich vor allem Netzwerke oder fielen ganz aus. Bei einem Drittel der Vorfälle wurden Daten beschädigt oder gingen verloren. Der Ausfall der IT verursachte in 26 Prozent der Unternehmen Verluste von bis zu 500.000 US-Dollar. ❑

Spam nimmt weiter zu

Im Oktober waren rund drei Viertel aller verschickten E-Mails Spam und somit 8,5 Prozent mehr als noch im September. Das ermittelte MessageLabs und führt dies vor allem auf zwei Schädlinge zurück: Die Trojaner SpamThru und Warezov laden immer neue Trojaner-Varianten und Spam-Vorlagen aus dem Netz und verschicken diese, sodass Scanner sie nur schwer identifizieren können. Die Zahl der verschickten Viren-Mails und Phishing-Mails blieb hingegen laut MessageLabs im Oktober nahezu konstant. Sie sank um 0,12 beziehungsweise 0,06 Prozentpunkte. ❑

Mobile Geräte sind hohes Risiko

Jeder verlorene Datensatz, beispielsweise eine Kundenadresse, bedeutet für Unternehmen eine Umsatzeinbuße von rund 100 US-Dollar. Das ermittelte das Ponemon-Institut in der Studie „2006 Cost of Data Breach". Verantwortlich für den Datenverlust waren in 70 Prozent der Fälle Probleme innerhalb des Netzwerks.

Mobile Geräte wie Laptops, PDAs und USB-Sticks stellten das größte Risiko dar, geschäftskritische Informationen zu verlieren. Rund 45 Prozent aller Vorfälle wurden durch diese Geräte verursacht. Das Ponemon-Institut rät festzulegen, wer auf das Netzwerk mit welchen Geräteklassen zugreifen kann. Zudem sollten Daten auf mobilen Geräten automatisch verschlüsselt werden. Lediglich zehn Prozent der Vorfälle wurden übrigens durch externe Hacker-Angriffe verursacht. ❑

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.

SANS: Die größten Internet-Bedrohungen 2006

Der drastische Anstieg von Zero-Day-Attacken zählt zu den großen Gefahren in diesem Jahr, heißt es in der jüngsten Top-20-Liste der Sicherheitslecks.

Zu den bedenklichsten Entwicklungen im laufenden Jahr zählt der Report die Häufung von Zero-Day-Attacken. Dabei handelt es sich um Angriffe, die unmittelbar nach dem Bekanntwerden einer Sicherheitslücke gestartet werden, noch bevor ein Patch zur Verfügung steht. Primäres Ziel dieser Attacken ist laut SANS nach wie vor Microsofts Internet Explorer (IE), immer häufiger geraten aber auch andere Produkte der Gates-Company ins Visier der Angreifer.

Auffallend ist nach Beobachtungen der Spezialisten die Anfälligkeit von Office-Produkten wie Powerpoint und Excel – die Zahl der Schwachstellen in Microsofts Bürosuite soll sich im Vergleich zum Vorjahr verdreifacht haben. So wurden 2006 allein in Office-Produkten 45 schwerwiegende bis kritische Sicherheitslöcher entdeckt – darunter neun Zero-Day-Lücken, die mangels Patch aktiv ausgenutzt wurden. Von den rund 20, meist von China aus lancierten Zero-Day-Angriffen in diesem Jahr waren laut SANS-Bericht allerdings auch Apples Safari-Browser und Wireless-Treiber betroffen.

Ebenfalls rapide steigt dem jüngsten Gefahrenindex zufolge die Zahl an SQL-Injection- und Cross-Site-Scripting-Lücken in Web-Anwendungen, deren Ausnutzung den direkten Zugriff etwa auf Datenbanken ermöglicht. Darüber hinaus gerät offenbar auch Voice over IP (VoIP) verstärkt ins Fadenkreuz der Hacker. Schützenhilfe leisten Angreifern hier Lecks unter anderem in Ciscos „Unified Call Manager" und der quelloffenen TK-Software „Asterisk".

Als weiteren Jahrestrend hebt der Bericht das zunehmende „Spear Phishing" hervor. Dabei handelt es sich um zielgerichtete Attacken auf einzelne Firmen oder Institutionen, denen mit vorgetäuschten Anliegen Finanzdaten, Geschäftsgeheimnisse oder geistiges Eigentum gestohlen wird. Darüber hinaus widmet sich der Report in der Kategorie „Security Policy and Personnel" der Bedeutung von Richtlinien und User-Verhalten für die Sicherheit. Zwei Problemfaktoren in diesem Kontext stellen den Experten zufolge exzessive Nutzerrechte sowie unautorisierte Geräte im Firmennetz dar. *(Katharina Friedmann, Redaktion COMPUTERWOCHE)*

Die ausführliche Liste der „SANS Top-20 Internet Security Attack Targets 2006" findet sich hier.

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