Liebe NIFIS-Mitglieder,

sehr geehrte Interessenten und Förderer,

im Jahr 2008 hat sich NIFIS sehr erfolgreich weiterentwickelt. Besonders positiv wirkt sich aus, dass die Geschäftsführung seit der Mitgliederversammlung durch die Europäische EDV-Akademie des Rechts (EEAR) wahrgenommen wird und dadurch in professionellen Händen liegt. Außerdem haben wir uns entschlossen, ein Vorstandsressort Öffentlichkeitsarbeit zu schaffen, welches von mir übernommen wurde. Damit werden Pressearbeit, Internetauftritt und NIFIS advice gebündelt, um die Kommunikation und die Wahrnehmung in der Öffentlichkeit zu optimieren. Anfang 2009 wird dann unsere neue Webseite online gehen, die auf einer veränderten technischen Basis beruht und stärker unsere Themenschwerpunkte widerspiegelt.

Auch in der inhaltlichen Arbeit hat sich bei NIFIS einiges getan. So wurde zum Jahresende der Arbeitskreis Validierung unter Leitung von Ingrid Dubois ins Leben gerufen. Einen kleinen Überblick über den Status in unseren Expertenforen und Arbeitskreisen erhalten Sie in dieser Ausgabe von NIFIS advice.

Im kommenden Jahr starten wir wieder direkt durch, um unseren Mitglieder Informationen und die Möglichkeit zum Austausch und Networking zu bieten: Im Januar führen die Arbeitskreise BCM und Datenschutz ihre nächsten Veranstaltungen durch. Der Arbeitskreis Identity Management zeichnet für eine gemeinsam mit secure-it.nrw geplante Veranstaltung am 29. Januar in Essen verantwortlich.

Ich möchte die Gelegenheit nutzen, 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 unserer Initiative geleistet haben. Ihnen, liebe Leserinnen und Leser, wünsche ich eine angenehme und gewinnbringende Lektüre, schöne und besinnliche Feiertage sowie ein gesundes und erfolgreiches Jahr 2009. Ich würde mich freuen, Sie bei einer der NIFIS-Veranstaltungen im nächsten Jahr persönlich zu treffen. Lassen Sie uns auch 2009 gemeinsam erfolgreich an der Weiterentwicklung der NIFIS arbeiten.

Dr. Thomas Lapp
NIFIS-Vorstand

HIGHLIGHTS

NIFIS inside

NIFIS fordert mehr Managerverantwortung

NIFIS ruft Unternehmen und Organisationen zum Umdenken auf. Informations-Sicherheit beginne im Top-Management heißt es aus den Reihen der Datenschutz-Experten. „Umgangssprachlich würde man auch sagen der Fisch stinkt vom Kopf her“, so NIFIS-Vorstand Dr. Thomas Lapp. Für Ausländer gebe es Einbürgerungstests, aber für Manager keine Wissenstests in punkto Informations-Sicherheit.

Die meisten überließen die Verantwortung im Unternehmen anderen Personen, zumeist den IT-Beauftragten. Das mache sie jedoch nicht von Verantwortung frei, und solch ein Verhalten müsse schnellstens geändert werden, fordert Lapp. So habe selbst die Telekom erkannt, dass ein Datenschutz-Vorstand dringend gebraucht werde.

Die NIFIS als Selbsthilfeorganisation der Wirtschaft zeigt jedoch nicht nur Schwachstellen auf. ► Sie unterstützt dabei, diese zu beseitigen. Dazu entwickelt beispielsweise der Arbeitskreis Datenschutz ein E-Learning-Tool und Workshops. Mehr dazu erfahren Sie im Statusbericht. ❑

NEUE MITGLIEDER

Omada

„Omada ist ein führender Microsoft Solution Provider für den Bereich Identity Management und ‚Microsoft Partner of the Year 2008’ in der Sparte ‚Security Solutions, Identity and Secure Access’. Mit dem Omada Identity Manager (OIM) bieten wir eine äußerst flexible benutzerzentrierte und geschäftsprozessorientierte Identity-Management-Lösung. NIFIS ist für Omada ein wichtiges Forum zur Erarbeitung von Standards und Best Practices im Bereich Identity Management; wir freuen uns auf eine aktive Mitarbeit!“

Martin Kuhlmann
Lead Solution Consultant
Omada

Zweimal NIFIS-Siegel verliehen

Die Internet POP Hannover GmbH erhält das NIFIS-Siegel und kann damit ihren hohen Sicherheitsstandard gegenüber Presse, Kunden und Geschäftspartnern belegen. „Das NIFIS-Siegel war für uns eine unkomplizierte und schnelle Art, den aktuellen Status unserer Bemühungen in unserem neuen Datacenter in Hannover realistisch darzustellen“, erläutert Markus Villwock von der Internet PoP Hannover GmbH.

Mit dem NIFIS-Selbstauditverfahren machen Unternehmen einen umfassenden Sicherheitscheck. Er ist ohne großen Aufwand und kostengünstig realisierbar. Sie erhalten einen Katalog mit 82 Fragen aus den Bereichen organisatorische, logische, technische sowie physikalische Sicherheit. Ein Experten-Gremium wertet die Antworten aus und zeigt vorhandene Sicherheitslücken auf. „Wir haben im Rahmen des Audits noch einiges über uns gelernt“, betont Villwock.

Bei einer positiven Bewertung durch das Experten-Gremium kann das Unternehmen für ein Jahr das NIFIS-Siegel führen. Danach ist eine Rezertifizierung erforderlich. Gerade erfolgreich abgeschlossen hat diese die]init[AG für Digitale Kommunikation.

Für NIFIS-Mitglieder ist der Erwerb des speziell für die mittelständische Wirtschaft entwickelten Siegels ebenso wie die Rezertifizierung **kostenfrei** möglich. Für Nicht-Mitglieder kostet das Audit 150 Euro. Weitere Informationen erhalten Sie hier. ❑

SAVE THE DATE

NIFIS-Mitgliederversammlung

26. März 2009

von 10.00 bis 11.30 Uhr

NIFIS-Vortrag bei VO.IP Germany

Welche neuen Möglichkeiten sich für Unternehmen aus dem Zusammenwachsen von Informationstechnologie und Telekommunikation ergeben – davon konnten sich die Besucher auf der VO.IP Germany am 28. und 29. Oktober in Frankfurt am Main überzeugen.

Die Kongressmesse für Voice- und IP-Kommunikation bot dank praktischer Vorführungen und Vorträgen namhafter Vertreter vornehmlich aus der Wirtschaft, aber auch von Politik, Regulierung und Verbänden, einen umfassenden Überblick über den Entwicklungsstand, die Zusammenhänge und Auswirkungen.

NIFIS-Vorstand Dr. Thomas Lapp berichtete im Themenblock „Zukunft“ über rechtliche Aspekte bei den Next Generation Networks. Er erläuterte zunächst Probleme und rechtliche Anforderungen bei der Netzneutralität. Anschließend beantwortete er in seinem Vortrag Rechtsfragen zu WLAN, insbesondere zum Thema Haftung.

Die Präsentation lassen wir Ihnen auf Wunsch gerne zukommen. Wenden Sie sich hierfür bitte an newsletter@nifis.de. ❑

Veranstaltungstipps

2. NIFIS – Forum für angewandte Informations-Sicherheit

Am 26. März 2009 veranstaltet NIFIS zum zweiten Mal sein Forum für angewandte Informations-Sicherheit. Getreu des Mottos „ Aus der Wirtschaft für die Wirtschaft“ können NIFIS-Mitglieder und -Interessierte das Forum nutzen, um sich über aktuelle Entwicklungen im Bereich der Informations- und Internet-Sicherheit zu informieren und untereinander auszutauschen.

Call for Papers

NIFIS-Mitglieder haben zudem die Möglichkeit, sich aktiv an der inhaltlichen Gestaltung des ► Forums zu beteiligen. Im „Call for Papers“ bittet NIFIS: Senden Sie bis zum 15. Januar 2009 Ihre Beiträge zu den zentralen Themen wie Datenschutz, Sichere Netze, Mobile Sicherheit, BCM, Sichere Rechenzentren & Green IT oder Zertifizierung & Validierung. Erläutern Sie beispielsweise Praxisbeispiele für den Umgang mit IT-Sicherheit in Ihrem Unternehmen oder bei Ihren Kunden, geben Sie Tipps und zeigen auch, auf welche Probleme Sie gestoßen sind.

Die Einsender der interessantesten Beiträge können diese dann auf dem Forum präsentieren. Gerne können Sie uns zunächst auch erst einmal Kurzexposees zukommen lassen. Rückfragen und Einsendungen richten Sie bitte an newsletter@nifis.de. ❑

Praxisforum Identity-Management

NIFIS und die Landesinitiative „secure-it.nrw“ laden gemeinsam am 29. Januar 2009 ab 14 Uhr zum Praxisforum Identity-Management (IM) nach Essen ein. Die Einführung einer IM-Lösung kann aufgrund der verschiedenen Teildisziplinen wie Zugangskontrolle, Berechtigungs- und Passwort-Management einige Schwierigkeiten bereiten. Das Praxisforum IM gibt einen kompakten Überblick und vor allem praktische Tipps.

NIFIS-Vorstand Dr. Thomas Lapp erläutert die rechtlichen Rahmenbedingungen. Paul Frießem vom Fraunhofer-Institut für Sichere Informationstechnologie SIT informiert über Lösungsansätze, Technologien und Standards. Jürgen Skirde von der RAG Aktiengesellschaft berichtet über die Einführung einer IM-Lösung in seinem Unternehmen. Abgerundet wird das Praxisforum durch den Vortrag von Dr. Horst Walther, Leiter des NIFIS-Arbeitskreises IM. Er präsentiert eine Checkliste für die erfolgreiche IM-Umsetzung.

Die Teilnahme ist **kostenfrei**, anmelden können Sie sich unter newsletter@nifis.de. ❑

Statusbericht aus den Arbeitskreisen

AK Identity Management: Rückblick auf ein bewegtes Jahr

Der NIFIS-Arbeitskreis Identity Management (IM) legte auch in diesem Jahr wieder den Schwerpunkt auf die Entwicklung generischer Prozesse für das Identity- und Access Management, kurz GenericIAM. Nach einem sehr praktischen Bottom-up-Ansatz und einem eher an die akademische Welt gerichteten Top-down-Ansatz beschritten die Teilnehmer jetzt einen dritten Weg der Modellierung, der einen Mittelweg darstellt.

Für die mittlerweile 28 Mitglieder des AKs ist gerade die praktische (Wieder-) Verwendbarkeit dieser allgemeinen IAM-Prozesse von entscheidender Bedeutung. Daher muss der Balanceakt gelingen, einerseits Prozesse zu liefern, die frei von Besonderheiten der spezifischen technischen Implementierung sind. Andererseits müssen sie unmittelbar von Technikern und Organisatoren verstanden werden können. Ferner müssen sie ausreichend organisatorisches Fachwissen in sich tragen, um den Aufwand einer Implementierung wirksam reduzieren zu können.

Die Arbeitsgruppe unter der Führung der Firma ImpulsIT hat sich daher dazu entschieden, von den betroffenen Objekten und den beteiligten Akteuren auszugehen. Daraus ergeben sich zwanglos bereits vollständig die elementaren Pflegeprozesse. In mehreren Arbeitsmeetings erfolgte eine Auswahl der häufigsten nicht-trivialen IAM-Prozesse. Sie befindet sich noch in der Abstimmung und bildet eine gute Basis für einen Erfolg im Jahr 2009.

Die Leitung des AK IM hat Dr. Horst Walther inne. Er ist Partner bei Kuppinger Cole + Partner und beschäftigt sich im Rahmen seiner Beratungstätigkeit schwerpunktmäßig mit der Beratung zu strategischen Identity-Management-Ansätzen sowie deren Umsetzung und Audit. ❑

AK Business Continuity Management: Normen und Standards im Fokus

Bei der Risiko- und Sicherheitsbewertung von Unternehmen spielt das Thema Business Continuity Management (BCM) eine wichtige Rolle. Die Methode zur Erstellung und Implementierung von Prozessen und Konzepten für die Fortführung des Geschäftsbetriebs unter Krisenbedingungen oder gar im Katastrophenfall bildet einen wesentlichen Grundstein für das Überleben von Unternehmen. Der NIFIS-Arbeitskreis BCM legte in diesem Jahr eine Zusammenfassung aller aktuellen Entwicklungen im Bereich Normen und Standards vor, welche über newsletter@nifis.de angefordert werden kann.

Künftig möchte sich der AK verstärkt fokussieren auf den Themenkomplex der Norm BS 25777 Information and Communication Technology Continuity sowie das Kapitel IT Services Continuity Management (ITSCM) von ITIL (ISO 20000). Zum einen wird somit der Schwerpunkt auf die informationstechnische Seite gelegt, was zu dem generellen Schwerpunkt von NIFIS passt. Zum anderen erfolgt diese Festlegung auch in Abgrenzung zum Business Continuity Institute (BCI), welches sich tendenziell mehr mit dem betriebswirtschaftlichen Bereich beschäftigt.

Den AK leitet Rolf von Rössing, der bei der KPMG das Thema BCM verantwortet. Er lädt herzlich ein, den Arbeitskreis BCM aktiv zu unterstützen. Die nächste Sitzung findet am 14. Januar 2009 von 14 bis 17 Uhr in Frankfurt am Main statt. ❑

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.

AK SiR: Informationsplattform mit Erfahrungsaustausch

Bei seinem Treffen am 9. Dezember in Frankfurt informierte der NIFIS-Arbeitskreis Sicherheit in Rechenzentren (SiR) ausführlich über das Schwerpunktthema „Strom“. Peter Heinemann, AK-Leiter und Security Manager der Interxion Deutschland GmbH, gab zunächst eine Einführung. Anschließend gewährte Alfred Heid, Netzplaner bei der HSE Technik GmbH & Co. KG, einen Einblick, welche Anforderungen aus dem Rechenzentrumsbereich an Netzbetreiber gestellt werden. Es wurden auch alternative Versorgungskonzepte angesprochen, die für reichlich Diskussionsstoff sorgten.

Thomas Federrath, Geschäftsführer der proRZ Rechenzentrumsbau GmbH, erläuterte danach ganzheitliche Aspekte eines ausfallsicheren Rechenzentrums. Sehr hilfreich war der abschließende Vortrag von Michael Schumacher, Senior Systems Engineer APC by Schneider Electric. Er stellte sehr detailliert USV-Versorgungskonzepte für den sicheren IT-Betrieb vor. Insgesamt nutzten die rund 20 Teilnehmer des AKs die Chance, viele Fragen zu stellen und das Thema Strom in allen Facetten zu beleuchten. ►

Für 2009 hat sich der AK SiR zum Ziel gesetzt, den NIFIS-Mitgliedern und Interessenten eine attraktive Informationsplattform zu bieten. Experten werden über die wesentlichen Themenschwerpunkte rund um die Sicherheit in Rechenzentren berichten. Gleichzeitig steht bei dem AK die Interaktivität im Fokus: Es gibt ausreichend Zeit für Fragen und den Austausch von Erfahrungen.

Beim nächsten Treffen des AKs dreht sich alles um das Thema „Klimatisierung im Rechenzentrum“. Es wird voraussichtlich im April stattfinden. Der Termin und die Agenda werden natürlich rechtzeitig bekannt gegeben. ❑

AK Validierung: Vom NIFIS-Siegel zum -Zertifikat

Am 3. Dezember trafen sich interessierte Spezialisten aus dem Bereich Informations-Sicherheit zur Auftaktveranstaltung des Arbeitskreises Validierung der NIFIS e.V.. Ingrid Dubois, Geschäftsführerin der dubois it-consulting gmbh und Leiterin des AKs, begrüßte die Mitglieder und weitere interessierte Unternehmensvertreter in den Räumen der Interxion in Frankfurt am Main.

Das Treffen diente zunächst dem Informationsaustausch zu aktuellen Bedrohungen, Sicherheitsvorfällen, Richtlinien und Standards. Bemängelt wurde von den Teilnehmern vor allem die fehlende Sensibilisierung der mittelständischen Unternehmen rund um den Datenschutz, die Datensicherheit und Informations-Sicherheit. Dies wurde gleichzeitig aber auch als Chance für die Öffentlichkeitsarbeit des Vereins gesehen.

Im Rahmen der angeregten und konstruktiven Diskussion wurde die große Lücke zwischen dem NIFIS-Siegel als Einstiegsmaßnahme und der Zertifizierung ISO/IEC 27001 herausgearbeitet. Genau hier sehen die Teilnehmer die Chance, ein NIFIS-Zertifikat zu positionieren: Mittelständische Unternehmen könnten damit ihre Prozesse dokumentieren und so einen weiteren Schritt in Richtung Informations-Sicherheit gehen.

Die große Herausforderung besteht darin, die vorhandenen Richtlinien so zu konsolidieren, dass ein sinnvoller „Next Step" auf dem möglichen Weg zu einer Zertifizierung nach ISO/IEC 27001 entstehen kann. NIFIS könnte hier eine zusätzliche Aufgabe als Zertifizierungsstelle übernehmen und so ihre Position am Markt ausbauen.

Die nächsten Sitzungen des AKs sind für den 4. Februar 2009 und den 13. Mai 2009 jeweils von 10 bis 15 Uhr bei NIFIS in Frankfurt geplant und für interessierte Mitglieder und Gäste offen.

Bei Interesse an den AKs wenden Sie sich bitte an newsletter@nifis.de. ❑

Service

Expertenfrageecke

Was verbirgt sich hinter dem Netzwerkzugangsschutz IEEE802.1x?

An dieser Stelle beantworten regelmäßig Experten Fragen, die NIFIS häufig erreichen, in dieser Ausgabe NIFIS-Vorstand Mathias Gärtner. Sollten auch Sie eine Frage an unsere Experten haben, senden Sie diese einfach an newsletter@nifis.de.

Mathias Gärtner, NIFIS-Vorstand

Heutzutage ist eine Vernetzung der Rechner untereinander für den reibungslosen Betrieb nicht mehr wegzudenken. Immer mehr Ressourcen, wie zentrale Fileserver sind nur noch über ein funktionierendes Netzwerk erreichbar. Das bedeutet aber, dass jeder Rechner, der Zugriff auf das Netzwerk hat, auch auf diese Daten zugreifen kann. Zwar gibt es immer einen Zugriffsschutz an den Ressourcen selbst, doch dieser ist meist schwach oder gar nicht ausgebildet und gepflegt.

Damit wird es immer wichtiger, von vorneherein den Zugang zum Netzwerk zu kontrollieren, denn natürlich sollen ausschließlich autorisierte Rechner beziehungsweise Benutzer Zugriff auf das interne Netz und damit die dort vorhandenen Ressourcen erhalten. Um diese Zugangskontrolle herstellerunabhängig und einheitlich zu gewährleisten, entwickelte eine Arbeitsgruppe der IEEE die dazu notwendige Methodik: Die Norm IEEE802.1x sieht vor, dass an jedem Gerät ein so genannter Supplicant-Prozess läuft, der vor dem ersten Netzwerkzugriff den Benutzernamen und das Passwort abfragt und an den Authenticator, meist einen Switch, weiterreicht. Dieser prüft die Zugangsberechtigung gegen eine Datenbank und erlaubt oder verbietet den Zugang. ►

Eine weitere Variante ist die Nutzung der Hardwareadresse eines Rechners als Usernamen und Passwort. Damit umgeht man die zusätzliche Eingabe der Daten durch den Benutzer und authentifiziert nur das Gerät. Die Variante hat aber den Nachteil, dass eben nicht der Anwender authentifiziert ist und somit keine Kontrolle darüber besteht, WER wirklich zugreift.

Nahezu alle Netzwerk- und die meisten Betriebssystemhersteller liefern inzwischen entsprechende Software und Hardware, sodass eine Implementierung weitgehend problemlos realisierbar ist. Aber nicht immer ist diese Methode ratsam oder funktioniert einwandfrei. So kann es bei Einsatz von Hubs oder „dummen“ Switches zu einer Authentifizierungslücke kommen, da hier nur der erste Teilnehmer authentifiziert wird, alle weiteren jedoch automatisch den Zugang erhalten. Ebenfalls sind Themen wie „WakeOnLan“ oder Geräte, die von sich aus nicht mit dem Netzwerk kommunizieren, wie zum Beispiel Drucker oder Messgeräte, nicht immer vollständig gelöst und bedürfen der genaueren Planung.

Zusammengefasst aber sollte auf einen Zugangsschutz beim Netzwerk nicht mehr verzichtet werden, da dies die erste Bastion einer umfassenden Informations-Sicherheit darstellt. ❑

Wissenschaftler stehen NIFIS Rede und Antwort

NIFIS legt großen Wert auf Wissenstransfer und Erfahrungsaustausch zwischen Wirtschaft, Politik und Wissenschaft. Die Universitätsprofessoren Prof. Dr. Dirk Heckmann (Passau), Prof. Dr. Maximilian Herberger (Saarbrücken) und Prof. Dr. Klaus Merle (Mainz) beraten NIFIS in Fragen rund um die Internet- und Informations-Sicherheit. NIFIS holt an dieser Stelle von den Experten regelmäßig Lösungsvorschläge zu aktuellen Herausforderungen und Antworten auf brisante Fragen ein.

Prof. Dr. Maximilian Herberger ist Inhaber des Lehrstuhls für Bürgerliches Recht, Rechtstheorie und Rechtsinformatik an der Universität des Saarlandes. Als Vorsitzender des Deutschen EDV-Gerichtstages, geschäftsführender Direktor des Instituts für Rechtsinformatik und Herausgeber der Internet-Rechtsinformatik-Zeitschrift JurPC beschäftigt er sich seit vielen Jahren praxisnah unter anderem auch mit den Themen Datenbanken, EDV-Sicherheit und Internet-Recht. Er ist Mitglied im Wissenschaftsbeirat von NIFIS.

In letzter Zeit wird verschiedentlich betont, man solle der Rolle des „admin-c“ mehr Aufmerksamkeit schenken. Wird da etwas unnötig dramatisiert, oder halten Sie diesen Appell für berechtigt?

Prof. Dr. Maximilian Herberger: Da wird bestimmt nichts überdramatisiert, der Appell ist vollständig berechtigt. Ich habe Fälle erlebt, in denen der admin-c nicht wusste, dass er zum admin-c bestellt worden war. Desgleichen habe ich Fälle erlebt, in denen die verantwortliche Unternehmensführung nicht wusste, wer als admin-c für die Website des Unternehmens Verantwortung trug. Da kann unternehmensorganisatorisch etwas nicht in Ordnung sein.

Die Frage ist deswegen so bedeutsam, weil der admin-c über eine echte Vollmacht verfügt. Die DENIC-Antragsformulare stellen dies zweifelsfrei klar:

„Der administrative Ansprechpartner (admin-c) ist die vom Domaininhaber benannte natürliche Person, die als sein Bevollmächtigter berechtigt und gegenüber DENIC auch verpflichtet ist, sämtliche die Domain betreffenden Angelegenheiten verbindlich zu entscheiden.“

Da die Domain ein werthaltiges Wirtschaftsgut ist, muss sichergestellt sein, dass nur zum admin-c bestellt werden kann, wer auch nach den sonstigen unternehmensinternen Regeln mit einer solchen umfassenden Vollmacht ausgestattet werden dürfte. Zugleich muss dafür Sorge getragen werden, dass der admin-c sich der Folgen seiner verantwortungsvollen Position bewusst ist und dass mögliche Haftungsrisiken mit ihm abgeklärt worden sind. Es versteht sich auch von selbst, dass – anders als verschiedentlich zu beobachten – der admin-c in aller Regel dem eigenen Unternehmen angehören sollte. Die im Rahmen gängiger IT-Outsourcing-Maßnahmen anzutreffende Praxis, einen admin-c beim IT-Dienstleister zu bestellen, ist keinesfalls empfehlenswert.

Schließlich gilt es noch zu beachten, dass der admin-c unter bestimmten Umständen in Hinsicht auf die Domain betreffende Fragen verklagt werden kann. Die Einzelheiten sind kompliziert (vgl. Markus Junker). Es ist auf jeden Fall angezeigt, diesbezüglich anwaltlichen Rat einzuholen.

Summa summarum: Es gehört zur juristischen Unternehmenskultur, der Rolle des admin-c gebührende Aufmerksamkeit zu widmen, vielleicht mehr Aufmerksamkeit als bisher. ❑

Praxistipp

Vorsicht beim Online-Banking – Kontrolle hilft

NIFIS-Mitglied Thomas Teichmann, Geschäftsführer und Berater für IT-Sicherheit der Schmitz & Teichmann Betriebsberatung GmbH, gibt in dieser Ausgabe Tipps zum sicheren Umgang mit Online-Banking.

Thomas Teichmann, Geschäftsführer Schmitz & Teichmann

Jeder, der im Internet unterwegs ist und besonders die, die es geschäftlich nutzen, sollten große Vorsicht walten lassen. So einfach und schnell viele Dinge, die uns hilfreich erscheinen oder sogar sind, auf diesem Wege erledigt werden können, so schnell und gar unerkannt kann ein elektronischer Langfinger sich auch Informationen über uns verschaffen. Auch über unser Bankkonto. Im Praxistipp habe ich deshalb einige sehr einfache Maßnahmen zum Schutz von Konten zusammengestellt, die per Internet abgerufen werden oder für die Sie per Internet oder Online-Banking Aufträge erteilen:

1. Verhalten Sie sich vorsichtig – wie sonst auch.

Drücken Sie jedem auf der Straße gleich Ihre Scheckkarte oder Ihr Portemonnaie in die Hand? Natürlich nicht. Also seien Sie auch im Internet vorsichtig, wem Sie Ihre persönlichen Daten und Kontoinformationen geben. Schauen Sie genau, ob Sie sich wirklich auf Ihrer echten Bank-Website einloggen, bereits ein vergessener Buchstabe oder Trennpunkt kann zu einer betrügerischen Seite führen. Löschen Sie unerwartete Mails von unbekannten Absendern, ohne sie zu lesen. Banken fordern niemals per E-Mail dazu auf, vertrauliche Daten wie PIN, TAN oder Kontonummer mitzuteilen.

2. Kontrollieren Sie regelmäßig in kurzen Abständen den Kontostand und die Buchungen.

Privat bedeutet das vielleicht alle zwei Tage. Wenn Sie täglich Ihren Rechner zum Surfen nutzen, schauen Sie auch täglich nach Ihrem Konto. Bei geschäftlicher Nutzung in einem Betrieb mit mehreren Personen sollte anhand eines schriftlichen Plans oder einer elektronischen Aufgabenliste geregelt werden, dass alle Konten einmal täglich geprüft werden. Die Prüfung sollte jeden Arbeitstag durchgeführt werden und nicht von einer Person abhängen. Urlaub, Dienstreisen oder Krankheit sind kein Grund, dies auszulassen. Programme für Online-Banking können durch vorbereitete Abfragen hilfreich sein. In größeren Betrieben wird dies sicherlich schon der Fall sein, auch wird dort immer ein Vier-Augen-Prinzip etabliert sein, um die Sicherheit zu erhöhen.

3. Versuchen Sie sofort zu klären, wenn Ihnen eine Buchung komisch vorkommt.

Das ist sehr wahrscheinlich dann der Fall, wenn Geld fehlt und Sie nicht wissen wieso. Überlegen Sie, ob Sie oder eine andere Person mit Berechtigung und Vollmacht oder Scheckkarte ganz rechtmäßig Geld überwiesen oder abgehoben hat. Wenn das nicht der Fall ist, sprechen Sie Ihre Bank an. Ohne weiteres Zögern. Die Größe des Betrags ist nicht so wichtig. Vielleicht kann Ihr Bankberater den Vorgang klären – oder anders helfen beziehungsweise das Konto umgehend sperren.

4. Setzen Sie Verschlüsselung ein.

Senden Sie Ihre sensiblen Daten nur über verschlüsselte Verbindungen. Banken setzen häufig das Verfahren SSL ein. Ob es verwendet wird, erkennen Sie an der Internetadresse „https …". ❑

IMPRESSUM

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

Redaktion
FRESH INFO +++
Nicole Chemnitz (CvD)
http://www.fresh-info.de