ISACA Newsletter 1|2008

ISACA
Serving IT Governance Professionals
Switzerland Chapter

newsletter

After Hours Seminar • 26.2.2008

IT und Wirtschaftskrieg in der Schweiz – wird die mangelnde IT-Security das Problem in der Schweiz?

Mit der zunehmenden Abhängigkeit von Netzwerken und Informationstechnologien bieten sich nicht nur Chancen, sondern auch neue Gefahren. Informationen sind heutzutage Ausgangspunkt, Hauptmittel und Ziel verschiedenster IT-gestützter Angriffe. ➜ **Mehr auf Seite 4**

Inhalt

Kennen Sie die PCI DSS?

Es handelt sich um den «Payment Card Industry Data Security Standard» mit (noch) geringem Bekanntheitsgrad in der Schweiz.

➜ **Mehr auf Seite 2**

Connaissez-vous les PCI DSS?

Il s'agit du «Payment Card Industry Data Security Standard», vraisemblablement encore bien méconnu en Suisse.

➜ **Suite à la page 3**

ISACA-Kurse und -Veranstaltungen

Die aktuellsten Veranstaltungs- und Kursdaten auf ➜ **Seite 5**

Impressum

Herausgeber:
ISACA Switzerland Chapter
c/o ITACS Training AG
Stampfenbachstrasse 40
8006 Zürich
kurse@isaca.ch

Redaktion:
Michael Kuss
KPMG AG
Badenerstrasse 172
8026 Zürich
mkuss@gmx.net

Redaktionsschluss
Nr. 2|2008: 5. März 2008

Satz und Gestaltung:
ITACS Training AG
Felice Lutz
8006 Zürich

Editorial

«Der Laie staunt, der Fachmann glotzt, der Spezialist weint Tränen.» Mit diesem Zitat nach Wilhelm Busch, wurde der Medienrummel um den milliardenschweren Spekulationsskandal bei der Bank Société Générale wohl am treffendsten beschrieben.

Ein einzelner Börsenhändler wird beschuldigt, dem Kreditinstitut mit Spekulationsgeschäften einen Verlust von 4,9 Milliarden Euro eingebracht zu haben. Die genauen Hintergründe und Verantwortlichkeiten sind derzeit noch Gegenstand der Ermittlungen.

Schon vor 13 Jahren gelang es einem britischen Derivathändler, mittels Spekulationen den Zusammenbruch der ältesten britischen Investmentbank zu verursachen. Durch Scheingeschäfte und Manipulation an den IT-Systemen gelang es Nick Leeson, seine Verluste vor den Kontrollinstanzen der Barings Bank zu verbergen. Fast alle Banken der Welt passten damals ihre internen Kontrollsysteme an.

Aktuell wird gegen Jérôme Kerviel, dem beschuldigten Händler der Société Générale, wegen Vertrauensbruch, Manipulation von IT-Systemen und Fälschungen ermittelt. Dies wird vermutlich auch wieder zu weltweiten Anpassungen von Risikomanagement und internen Kontrollsystemen führen.

Auch der Berufstand der IT-Revisoren ist nun in der Pflicht einen Beitrag zur effektiven Ausgestaltung von Kontrollen und Risikomanagement zu leisten, schon um alleine den Leuten entgegenzutreten, die meinen, eine immer komplexer werdende Finanzwelt sei auch durch Kontrollsysteme und Risikomanagement nicht mehr zu beherrschen.

Michael Kuss

CISA Certified Information Systems Auditor
CISM Certified Information Security Manager
IT Governance Institute

Focus

Kennen Sie die PCI DSS?

Autor: Michel Huissoud

Bei PCI DSS handelt es sich um den «Payment Card Industry Data Security Standard», und ich weiss nicht, ob die Existenz dieser Normen in der Schweiz bekannt ist. Seit ich sie dank den News unseres Freundes Marc Barbezat (➜ www.b3b.ch) entdeckt habe, bin ich über die mangelnde Bekanntheit erstaunt. Sogar die Anwendungsverantwortlichen scheinen diese Normen zu ignorieren, welche durch die Haupt-Hersteller von Kreditkarten herausgegeben wurden und Anforderungen stellen, die alles andere als trivial sind.

Kleiner Test: Bietet Ihr Unternehmen oder Ihre Verwaltung ihren Kunden die Bezahlung per Kreditkarte an? Falls ja;

- besitzt sie für ihre Firewalls über eine schriftliche Begründung und Bezeichnung aller verfügbaren Protokolle mit der Ausnahme von http (hypertext transfer protocol, HTTP), SSL (secure sockets layer, SSL), SSH (secure shell, SSH) und von VPN (virtual private network)?

- Werden alle anwendbaren Firewall- und Router-Regeln vierteljährlich überprüft?

- Wird vorgesorgt, dass die internen IP-Adressen nicht aus dem öffentlichen Internet einsehbar sind? D.h werden interne Adressbereiche nach RFC 1918, Portadressübersetzung (port address translation, PAT) oder Netzwerkadressübersetzung (network address translation, NAT) eingesetzt?

- Sind Sie sicher, dass Ihr Unternehmen nach der Autorisation keine sensiblen Authentisierungsdaten speichert (selbst wenn verschlüsselt)? Es handelt sich hier um den Inhalt der magnetischen Spur, den Namen des Kontoinhabers, die primäre Kontonummer (primary account number, PAN), das Verfallsdatum, den Dienstcode und eine allfällige persönliche Identifikationsnummer (personal identification number, PIN)?

Hier handelt es sich nur um einige der zahlreichen Anforderungen, die in diesem 24-seitigen Dokument beschrieben sind. Es ist kostenlos in den Sprachen Deutsch, Französisch und Englisch auf der ➜ www.pcisecuritystandards.org verfügbar.

Es ist schwierig, sich über die zivilrechtlichen Verantwortlichkeiten zu äussern, ohne die vertraglichen Beziehung zwischen Ihrem Unternehmen und diesen Instituten genau zu kennen. Es steht jedoch ausser Zweifel, dass im Falle eines Schadens im Zusammenhang mit einem Datendiebstahl, die Frage, ob diese Normen respektiert wurden oder nicht, sich als grundlegend erweisen könnte.

Dieses Dokument kann auch denjenigen unter Ihnen helfen, die «best practices» suchen, um Security-Verantwortliche zu überzeugen. Sie finden dort beispielsweise Regeln wie:

- Begrenzen der Anzahl von Zugriffsversuchen, indem eine Benutzer-ID nach 6 Versuchen gesperrt wird.
- Festlegen der Sperrdauer auf 30 Minuten oder bis ein Administrator die Benutzer-ID wieder aktiviert.
- Wenn eine Session während 15 Minuten inaktiv ist, muss der Benutzer sein Passwort wieder eingeben, um das Terminal zu reaktivieren.

Ich wünsche eine gute Lektüre und nehmen Sie vielleicht an einem Workshop zur Umsetzung der PCI DSS teil!

Bestellung von Büchern bei der AFAI (zum Beispiel CobiT auf französisch)

Die Mitglieder des ISACA Switzerland Chapters können alle Publikationen der AFAI (➜ www.afai.fr) zum ISACA-Mitgliedertarif bestellen. Es genügt, die Mitgliedsnummer anzugeben, die sich auf Ihrer persönlichen Karte befindet.

Focus

Connaissez-vous les PCI DSS?

Autor: Michel Huissoud

Il s´agit des «Payment Card Industry Data Security Standard» et je ne suis pas sûr que l´existence de ces normes soit connue en Suisse. Depuis que je les ai découvertes grâce à la News de notre ami Marc Barbezat (➜ www.b3b.ch), je m´étonne de cette méconnaissance. Même les responsables d´applications semblent ignorer ces normes édictées par les principaux fournisseurs de cartes de crédit et qui posent des exigences loin d´être triviales.

Petit test: votre entreprise - ou votre administration offre-t-elle à ses clients la possibilité de payer par carte de crédit? Si oui,

- dispose-t-elle pour ses pare-feux d´une justification et de la consignation par écrit de tous les protocoles disponibles en dehors des protocoles http (hypertext transfer protocol, HTTP), SSL (secure sockets layer, SSL), SSH (secure shell, SSH) et de réseau privé virtuel (virtual private network, VPN)?

- un examen trimestriel des ensembles de règles applicables aux pare-feux et aux routeurs est-il effectué?

- a-t-elle mis en œuvre un déguisement d´adresse Internet, pour éviter que les adresses internes ne soient traduites et divulguées sur Internet. Utilisation de technologies mettant en œuvre l´espace adresse RFC 1918, telles qu'une traduction d´adresse de port (port address translation, PAT) ou une traduction d´adresse de réseau (network address translation, NAT)?

- êtes-vous sûr que votre entreprise ne stocke aucune donnée d´authentification sensible après autorisation (même si elles sont cryptées). Il s´agit notamment du contenu d´une quelconque piste de la bande magnétique, du nom du titulaire du compte, du numéro de compte primaire (primary account number, PAN), de la date d´expiration, du code de service et d´un éventuel numéro d´identification personnel (personal identification number, PIN)?

Il ne s´agit là que de quelques-unes des nombreuses exigences décrites dans ce document de 24 pages disponible gratuitement en français, allemand et anglais sur le site ➜ www.pcisecuritystandards.org.

Il est difficile de se prononcer sur les questions de responsabilité civile sans étudier les contrats qui lient votre entreprise à ces instituts. Il ne fait cependant aucun doute que si dommage devait être lié à un vol de données, la question du respect ou du non-respect de ces normes pourrait se révéler fondamentale.

Ce document peut également aider ceux d´entre vous qui cherchent des «bonnes pratiques» afin de convaincre des responsables sécurité. Vous y trouverez par exemple des règles comme celles-ci:

- limiter le nombre de tentatives d´accès en verrouillant l´identité d´utilisateur après au plus 6 tentatives;
- fixer la période de verrouillage à trente minutes, ou jusqu'à ce qu'un administrateur active l'identitéd'utilisateur;
- si une session est inactive depuis plus de 15 minutes, imposer à l´utilisateur de saisir à nouveau son mot de passe pour réactiver le terminal

Bonne lecture et rendez-vous peut-être à un atelier d´échange sur la mise en œuvre de ces PCI DSS!

After Hours Seminar • 26. Februar 2008

IT und Wirtschaftskrieg in der Schweiz – wird die mangelnde IT-Security das Problem in der Schweiz?

Referent: Marc Henauer, MELANI

Mit der zunehmenden Abhängigkeit von Netzwerken und Informationstechnologien bieten sich nicht nur Chancen, sondern auch neue Gefahren.

Informationen sind heutzutage Ausgangspunkt, Hauptmittel und Ziel verschiedenster IT-gestützter Angriffe.

Vor allem der Datendiebstahl, also die Spionage setzt sich ungebremst fort und wird von Akteuren privater oder staatlicher Natur betrieben.

- Was sind die Gefahren heute?
- Welche Akteure mischen im Geschäft mit und wie tun sie dies?
- Beispiele für Spionage und andere Angriffe auf Unternehmen (E-Banking etc...)
- Wohin zeigt der Trend?
- Und was bleibt zu tun?

➜ **Zur Anmeldung**

Agenda

25. März 2008
Internes Sicherheits-Kontrollsystem im Bankenumfeld
Referent: Kurt Niederberger, LKB

29. April 2008
IT-Revisionsplanung und -Durchführung - ein Praxisbericht
Referent: Christian Balmer, ZKB

27 Mai 2008
Thema noch offen

24. Juni 2008
Thema noch offen

29. Juli 2008
Keine Veranstaltung während den Sommerferien

26. August 2008
Thema noch offen

by Bitterli Consulting
itacs training

Details und andere Kurse siehe unsere Homepage: ➜ www.itacs.ch

Interessante Konditionen bei der Buchung von mehreren, beliebig kombinierbaren Kursen dieser Trainings-Woche

ITACS Training AG
Stampfenbachstr. 40
CH-8006 Zürich
Tel. +41 (0)44 444 11 01
kurse@itacs.ch

ITACS Training ist der offizielle Ausbildungspartner des ISACA Switzerland Chapter
www.isaca.ch

ISACA Serving IT Governance Professionals Switzerland Chapter

IT Security Training Week • 5.–9. Mai 2008
Bestehend aus 5 einzeln buchbaren Tageskursen

IT-Risikomanagement
Grundbegriffe, Risikoanalysen für IT-Systeme, IT-Projekte und IT-Anwendungen. Strategisches Risikomanagement, ORM, ...

ISO 27001/2 verstehen und anwenden
Die wichtigsten Elemente eines ISMS kennen und in 30 klaren Schritten implementieren oder verbessern

Erfolgreiche Awareness-Kampagnen
Systematische Planung/Durchführung von Aktivitäten und Kampagnen für anhaltende Awareness (mit zahlreichen Beispielen/Erkenntnissen aus der Praxis)

Sichere Anwendungsentwicklung
Projekt-, Entwicklungs- und eigentliche Applikationsrisiken; Vorgehen zur Gewährleistung sicherer Anwendungen, inkl. Organisation und Durchführung von Security Penetration Testing

Grundlagen der Kryptologie
Alle notwendigen Fachbegriffe und Erkenntnisse; besonders geeignet für IT-Prüfer, Sicherheitsspezialisten, Manager

ISACA-Kurse und -Veranstaltungen

Diese Übersicht enthält die aktuellsten Veranstaltungs- und Kursdaten. Details: ➜ **www.isaca.ch**

26.2.2008	➜ **After Hours Seminar** IT und Wirtschaftskrieg in der Schweiz – wird die mangelnde IT-Security das Problem in der Schweiz?
9.3. – 2.4.08 **Stockholm**	➜ **European Conference on Computer Audit, Control and Security**
31.3. – 2.4.08	➜ **Praxisgerechte Anwendung von ISO 27001 und ISO 27002** Ein Muss für Sicherheitsverantwortliche, Risikomanager und alle anderen, welche den Zwillingsstandard erfolgreich in ihrem Unternehmen umsetzen wollen
31.3. – 4.4.08	➜ **Avaloq-Einführung für IT-Revisoren** Grundlagen, Konzepte und Bedienung des Avaloq Banking Systems. Vertiefung in Parametrisierung u.a. von Security-, Workflow- und Rule Engine
31.3. – 4.4.08 **Edinburgh**	➜ **ISACA Training Week**
3. – 4.4.08	➜ **Effiziente Interview- und andere Kommunikationstechniken** Verbesserung des persönlichen Kommunikationsverhaltens von Revisoren/ Sicherheitsbeauftragten in kritischen Situationen
10.4. – 20.5.08	➜ **CISM-Prüfungsvorbereitungskurs 2008|1** Für Informationssicherheitsbeauftragte: die kompakte Variante zur gezielten Vorbereitung auf die internationale CISM-Prüfung
14.4. – 19.5.08	➜ **CISA-Prüfungsvorbereitungskurs 2008|1** Für IT-Prüfer/Sicherheitsspezialisten: die kompakte Variante zur gezielten Vorbereitung auf die internationale CISA-Prüfung
21.4. – 25.4.08	➜ **Hacking Defense Training Week** Wirksame Verteidigung von Hacking-Angriffen mit anspruchsvollen Fallstudien Eine Intensivwoche (nur) für Fortgeschrittene!
5. – 9.5.08	**IT Security Week; bestehend aus 5 einzeln buchbaren Kompaktkursen** • Montag 5. Mai 2008: ➜ **IT-Risikomanagement** • Dienstag, 6. Mai 2008: ➜ **ISO 27001/2 verstehen und anwenden** • Mittwoch, 7. Mai 2008: ➜ **Erfolgreiche Awareness-Kampagnen** • Donnerstag, 8. Mai 2008: ➜ **Sichere Anwendungsentwicklung** • Freitag, 9. Mai 2008: ➜ **Grundlagen der Kryptologie** Beachten Sie das attraktive Preismodell der IT Security Training Week ➜ **Kursübersicht**

Wo nichts anderes vermerkt, finden die Veranstaltungen/Kurse in den Schulungsräumlichkeiten von ITACS Training AG, Stampfenbachstrasse 40, 8006 Zürich, statt.