ISACA Newsletter August 2010

newsletter

ISACA
Trust in, and value from, information systems
Switzerland Chapter

After Hours Seminar • Zürich

Dienstag, 31. August. 2010 • 16:40 – 17:40 Uhr

Datenbanken aus der Perspektive des Auditors
Referent: Thomas Baumann ➜ Mehr auf Seite 5

Rendez vous afterwork • Lausanne

Mercredi 15 Septembre 2010 • 14h00 – 17h15

Le vol de données disséqué
Atelier ISACA + IIA (ASAI) + CLUSIS

➜ Plus d'informations sur la page 4

Focus

USB (non UBS)-Sorpresa

➜ Maggiori informazioni a pagina 2

Inside

Large Chapters Meeting
Das grosse Treffen der europäischen ISACA Chapter in Paris ➜ Mehr auf Seite 4

ISACA-Kurse und -Veranstaltungen

Die aktuellsten Veranstaltungs- und Kursdaten ➜ Seite 6

➜ Security Training Week 2010 in English

Impressum

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

Redaktionsschluss:
9. September 2010

Redaktion:
Peter R. Bitterli
Stampfenbachstrasse 40
8006 Zürich
prb@bitterli-consulting.ch

Satz und Gestaltung:
ITACS Training AG
Felice Lutz
8006 Zürich

Editorial

Während 17 Jahren hat Michel Huissoud im Vorstand der ISACA als Vizepräsident sehr aktiv dazu beigetragen, dass zahlreiche Veranstaltungen über die Bühne gegangen und neue Arbeitsgruppen ins Leben gerufen worden sind. Mit seinem Rücktritt habe ich dessen Amt mit der Wahl an der Vereinsversammlung 2010 übernehmen dürfen. Einerseits tue ich dies als offizielle Vertreterin meiner Arbeitgeberin, der Eidg. Finanzkontrolle, und andererseits soll ich auch weiterhin das Bindeglied zwischen den alemannischen und französischen Sprachgebieten sein.

Auch wenn im Moment meine Tätigkeiten nicht mehr sehr prägend und sichtbar sind wie diejenigen meines Vorgängers, so wirke ich doch seit einigen Monaten im Hintergrund nach dem Motto „überall dort, wo es gerade brennt«. So tragen einige Protokolle meine Handschrift, weil kurzfristig die vorgesehenen Protokollführer ausgefallen waren. Der Romandie bzw. deren neuen Vertreterin im Vorstand stehe ich mit ermunternden Ratschlägen in einem schwierigen Umfeld bei, treffe Abklärungen in Zürich und leiste wo notwendig Übersetzungsdienste. Daneben unterstütze ich die Präsidentin so gut dies von Bern aus möglich ist. Sollte sie aus irgendwelchen Gründen ausfallen, so wäre es meine Aufgabe, sie kurzfristig und vorübergehend zu ersetzen.

Festgestellt habe ich in den letzten Monaten, dass auch der Vorstand ISACA vor grossen Herausforderungen steht: Ersatz zu finden für austretende Vorstandsmitglieder gestaltet sich genau so schwierig wie Interessengruppen aktiv zu halten oder den Newsletter mit interessanten Informationen bzw. Fachartikeln zu füllen. Die teilweise niedrigen Teilnehmerzahlen, sowohl an den offiziellen ISACA-Kursen wie auch an Veranstaltungen mit Partnerorganisationen, scheinen im direkten Zusammenhang mit der Finanzkrise zu stehen.

Welchen Nutzen haben Sie als Mitglied von ISACA Chapter Switzerland? Ich habe in den letzten Monaten gesehen, dass viele interessante und qualitativ hoch stehende Angebote unter dem Banner ISACA zur Verfügung stehen. Dahinter stehen Menschen mit grossem persönlichem Engagement und vielen unbezahlten Stunden. Vielleicht nehmen Sie sich einige Minuten Zeit, sich etwas genauer über die aktuellen Angebote zu informieren unter http://www.isaca.ch/.

Cornelia Simmen

CISA Certified Information Systems Auditor
CISM Certified Information Security Manager
CGEIT Certified in the Governance of Enterprise IT

Focus

USB (non UBS)-Sorpresa

Autore: Massimo Magnini

Negli ultimi tempi ho cominciato a credere che l'abbreviazione USB significhi Ultime Sorprese Bizzarre piuttosto che Universal Serial Bus!.

Effettivamente come la maggior parte delle organizzazioni, anche noi abbiamo scelto di proteggere con la crittografia non solamente i nostri Laptop (con il software Endpoint Encryption)[1] ma anche questi piccoli ma capaci e pratici contenitori di informazioni per potere scambiare e trasportare dati.

In italiano questi USB sono spesso e volentieri, ed aggiungo simpaticamente, definiti come «chiavette» (diminutivo di chiave cioè key). Ebbene la nostra organizzazione ha scelto tempo fa di proteggere queste chiavette mediante il software S450 emtec USB Disk Pro[2].

Per alcuni mesi non abbiamo registrato nessun problema di funzionamento ma recentemente abbiamo dovuto constatare che sebbene la chiavetta fosse protetta con una parola chiave, dopo l'inserimento nel laptop, era possibile accedere ai dati in modo trasparente, come se la protezione non esistesse! Nessun avvenimento «strano», quale ad esempio un'interruzione brusca di corrente od altro, poteva essere all'origine di questa situazione chiaramente inaccettabile.

Per capire questo fenomeno abbiamo fatto delle ricerche in internet ed abbiamo trovato dei documenti interessanti tra i quali uno dal titolo «Kryptografisch sicher? SySS knackt USB-Stick»[3].

Quest'azienda tedesca SySS ha infatti scoperto un grave difetto architetturale nella protezione crittografica di alcuni dischi «flash» USB - le nostre popolari «chiavette» nei formati tra 1 e 8 GB.

I produttori coinvolti sono aziende di primaria importanza, e normalmente note per l'affidabilità e la performance dei loro prodotti: SanDisk, Kingston e Verbatim. I prodotti in questione, inoltre, risultano certificati FIPS 140-2 (ma evidentemente l'audit di certificazione non ha rivelato il problema).

Fonte del difetto è il fatto che per accedere ai dati cifrati sulla chiavetta si usa un'applicazione, la quale richiede all'utente un'autenticazione. Tuttavia, una volta riconosciuto l'utente, l'applicazione invia alla chiavetta un segnale di sblocco sempre identico. Di conseguenza, modificando l'eseguibile di questa applicazione in modo che salti il passaggio di autenticazione si ottiene accesso a tutti i dati memorizzati sulla chiavetta in modo immediato e senza alcuna restrizione.

Il difetto dunque non è legato alla crittografia utilizzata sulla chiavetta (che è dichiarata essere AES-256), bensì:

1) all'utilizzo di un programma basato sul PC per autenticare l'utente e

2) alla scelta di usare di fatto una chiave crittografica fissa.

Vogliate dunque prendere nota di questo ed altri documenti sull'argomento ed agire di conseguenza!.

Dobbiamo anche in questo caso renderci conto dei possibili rischi insiti nell'utilizzo delle chiavette e soprattutto essere sensibili al fatto che, come spesso capita, un piccolo errore può avere delle gravi ed importanti conseguenze.

Per finire e per cambiare argomento non dimenticate di leggere gli articoli sul tema del disastro della piattaforma BP nel golfo del Messico; sembra molto probabile che si tratti di un «cyber incident»!.

➜ **Continuazione**

1 http://www.mcafee.com/de/enterprise/products/data_protection/data_encryption/index.html
2 http://www.emtec-international.com/de/produit.php?categorie=STMOB&gamme=CLES%20USB&ss_gamme=S450
3 http://www.syss.de

Focus

Continuazione «USB (non UBS)-Sorpresa»

Una breve citazione di quest'articolo: «*In his testimony Friday July 23, 2010, Michael Williams, the chief electronics technician aboard the Transocean-owned Deepwater Horizon, said that the rig's safety alarm had been habitually switched to a bypass mode to avoid waking up the crew with middle-of-the-night warnings. Williams also said that five weeks before the April 20 explosion, he had been called to check a computer system that monitored and controlled drilling. The machine had been locking up for months, Williams said, producing what he and others on the crew called a «blue screen of death.» «It would just turn blue. You'd have no data coming through, «Williams said today, according to the New York Times' story. With the computer frozen, the driller would not have access to crucial data about what was going on in the well*».

Dobbiamo tutti ben riflettere su questi temi legati alla sicurezza in generale ed aiutare i nostri colleghi meno versati per le informazioni tecniche a comprendere i rischi, ancora meglio imparare a prevenirli!.

Mi scuso con i lettori ma ritengo che ogni tanto sia una buona esperienza quella di sforzarsi di capire un tema espresso in una delle lingue officiali svizzere.

Vi auguro buona lettura.

Massimo Magnini
Swiss Federal Audit Office,
Comptence Center IT Audit

Inside

Large Chapters Meeting

Am 28. Juni 2010 trafen sich VertreterInnen von grossen Europäischen ISACA Chapter in Paris. Aufgrund der ähnlichen Problemstellungen dieser Chapter, sei es in der Kommunikation mit dem ISACA Headquarter in Amerika oder innerhalb des eigenen Chapters, entstand der Bedarf, sich gegenseitig auszutauschen, zu unterstützen und Synergien auszuschöpfen. Die Chapter, die vertreten waren mit ihren momentanen Mitgliederzahlen (Juni 2010) sind: Frankreich als Gastgeberin (666), Deutschland (1794), London (2336), Belgien (720) und die Schweiz (1032).

An diesem eintägigen Treffen wurden folgende Themen diskutiert: Umgang mit Übersetzungen und deren Verteilung/Verkauf, verschiedene Ausbildungsstrategien in den Ländern (z.B. Zusammenarbeit mit Universitäten), Möglichkeiten gemeinsamer Tagungen (nicht als Konkurrenz zu EuroCACS zu verstehen), Schaffung von länderübergreifenden Ausbildungs-Zertifikaten und Austausch von Ausbildungsprogrammen. Das Französische Chapter gab zudem eine Präsentation über seine Erfahrungen und derzeitige Situation, die zu weiteren Ideen und Anregungen führte und spezifische Fragen aufwarf. Die zehn am Meeting teilnehmenden Personen diskutierten lange und angeregt, sodass die Zeit im Fluge verstrich. Im Tagesablauf war natürlich Platz für ein feines "déjeuner" eingeplant - worauf sich die inzwischen hungrig geworden Leute freuten. Trotz des späten Mittagessens bot das Restaurant glücklicherweise noch die ganze Speisekarte zur Auswahl an. Der einzige Vegetarier unter den Teilnehmern musste sich allerdings mit einem "petit déjeuner" zufrieden geben - das französische Angebot in diesem Bereich schien noch ausbaufähig zu sein.

Am Nachmittag wurde u.A. die Aufgabenliste zusammengestellt - es gibt einige Folgeaktivitäten für die Chapter, d.h. für einzelne Vorstandsmitglieder. Das Treffen wurde von den Teilnehmern als sehr positiv und konstruktiv bewertet. Für den Herbst ist deshalb in Frankfurt ein nächstes Meeting geplant. Dort sollen die in der Zwischenzeit angegangenen Arbeiten weiterbesprochen und konkretisiert werden. Sicher werden wiederum Ideen und daraus folgende Aufgaben dazukommen.....

Wir werden Sie über weitere Entwicklungen auf dem Laufenden halten und nehmen gerne Anregungen entgegen.

Daniela Gschwend
Präsidentin ISACA Switzerland Chapter

Rendez vous afterwork ISACA Suisse Romande

Le vol de données disséqué

Tout savoir sur le vol de données - 15 sept 2010 - Atelier ISACA + IIA (ASAI) + CLUSIS

Pourquoi vole-t-on de l'information? Quel est le profil du voleur de données? Comment peut-on réduire le risque de vol? Quelles sont les moyens juridiques à votre disposition pour vous protéger? ... telles sont les principales questions auxquelles l'ISACA, le CLUSIS et l'ASAI vous proposent de répondre lors de leur atelier annuel commun:

Mercredi 15 Septembre 2010 • 14h00 à 17h15 • Hôtel Alpha Palmier (Lausanne, 2 min de la gare)
La participation à l'événement est gratuite (compte comme crédit de formation pour vos certifications) mais l'inscription est obligatoire. Non-membre : CHF 150.

➜ **Online-Régistration**

IT Governance Institute

Retrouvez dès maintenant les membres «ISACA Suisse romande» sur LinkedIn

After Hours Seminar

Datenbanken aus der Perspektive des Auditors

Zürich • Dienstag, 31. August 2010 • 16:40 – 17:40 Uhr

Die Präsentation beleuchtet das Monitoring von internen Kontrollen im Datenbankumfeld und behandelt dabei Themen wie Wiederherstellbarkeit, Zugriffsschutz, Sicherung der Datenintegrität und der Effizienz von Datenbanken. Zahlreiche Praxisbeispiele aus dem DB2 z/OS Umfeld dienen dem Auditor als Praxishilfe und helfen dem Datenbankadministrator als Vorbereitung für den nächsten Audit.

Bringt Euren Datenbankadministrator auch mit an die Präsentation!

Das Referat beinhaltet folgenden Schwerpunkte:

- Risiken und Schwachstellen in Datenbanksystemen
- Risk Management: Die Rollen von IT Audit vs. Datenbankadministration
- Continuous Assessment von Risiko-Indikatoren
- Continuous Monitoring von internen Kontrollen
- Praxisbeispiele, konkrete Kontrollen und deren Prüfprozeduren (zum Mitnehmen und selber Anwenden)

Referent: Thomas Baumann

➜ Zur Anmeldung

ISACA-Kurse und -Veranstaltungen

30.8.10	➜ **IKS in IT revisionssicher implementieren** • **Wird definitiv durchgeführt** • ➜ **Anmeldung noch möglich** Effiziente Vorbereitung auf (angekündigte) Revisionen und Schutz vor übertriebenen Forderungen
6.–10.9.10	➜ **Avaloq-Einführung** • **Wird definitiv durchgeführt** • ➜ **Anmeldung noch möglich** Für interne und externe Revisoren und Sicherheitsbeauftragte
14.–15.9.10	➜ **BACEE/ISACA Operational Risk Conference** • ISACA erhalten 30% Rabatt
15.9.10	**Rendez vous afterwork ISACA Suisse Romande • Lausanne** ➜ **Online-Régistration**
6.10.10	➜ **Clevere IT-Risikoanalysen für Sicherheitsprofis und Wirtschafts-/IT-Prüfer** Effiziente Durchführung von IT-Risikoanalysen in allen Schichten der "Cremeschnitte"
7.–8.10.10	➜ **Szenario-basiertes IT-Risikomanagement** Hochkonzentriertes Fachwissen und Praxistipps für wirksame Risikomanagement-Prozesse mit Hilfe von IT-Risikoszenarien
11.–12.10.10	➜ **Wirksame Projekt- und Portfoliocontrolling** (IT-) Projekte effizient und wirksam überwachen und steuern
11.–15.10.10 **Geneva**	➜ **Introduction to Avaloq for (IT) Auditors and (IT) Security Representatives** Handling of the Avaloq banking system with an emphasis on parameterization of security, workflow and rule engine
18.–19.10.10	➜ **Konfliktmanagement und konfliktfähige Kommunikation** Konfliktträchtige Situationen erfolgreich meistern
25.10.10	➜ **Einführung in Enterprise Risk Management** Sicherheit durch proaktive Handhabung der Risiken
Geneva	**Security Training Week 2010 (All Courses in English !) • In Geneva**
25.10.10 26.10.10 27.10.10 28.–29.10.10	➜ **Introduction to Information Security** ➜ **Understanding and Securing the Wireless Network** ➜ **Using ISO 27002 to Audit Mobile Technology** ➜ **Auditing Windows Active Directory – a Walkthrough Case Study** All these courses can be booked in combination with one or more of our other courses of the Training Week
1.–3.11.10	➜ **Avaloq – Reporterstellung für Revisoren & Sicherheitsbeauftragte** Effiziente Erstellung von verlässlichen Reports aus dem Avaloq Banking System
3.11.–23.11.10	➜ **CISA-Prüfungsvorbereitungskurs 2010|2** Kompakter Prüfungsvorbereitungskurs für erfahrene Kursteilnehmer
Diverse Daten	**Meeting der IG SAP zum Thema "Compliant Change Management - Trennung von Build und Run"** Die Interessensgemeinschaft SAP (IG SAP) der ISACA Schweiz ist ein Informations-Austausch Forum für Informatikrevisoren und Sicherheitsbeauftragte… ➜ **Details und Anmeldung**
	Security Training Week 2010 (All Courses in English !) • In Zurich
1.–2.11.10 3.11.10 411.10 5.11.10	➜ **Auditing Windows Active Directory – a Walkthrough Case Study** ➜ **Introduction to Information Security** ➜ **Understanding and Securing the Wireless Network** ➜ **Using ISO 27002 to Audit Mobile Technology** All these courses can be booked in combination with one or more of our other courses of the Training Week

Weitere Kurs- und Veranstaltungsanbieter

➜ **Glenfis**	➜ **RISK IT Overview Kurs** Risk IT - das Risiko Management Framework von ISACA	**6.9.2010** bei Glenfis AG, Zürich
➜ **Glenfis**	➜ **CobiT Foundation Kurs mit optionaler Zertifizierung** CobiT® 4.1 - IT Governance Foundation Kurs	**20.–22.10.10** bei Glenfis AG, Zürich
➜ **Datenschutzforum**	➜ **Fachwissen für Datenschutzverantwortliche** Kompetenz von Praktikern für Praktiker • ISACA-Mitglieder erhalten Rabatt	**7.–8.10.2010** Hotel Rigi Kulm
➜ **ISSS**	➜ **Innovative Alternativen zum Passwort** Ist das Passwort aus dem Computeralltag nicht mehr wegzudenken?	**26.10.2010** Hotel Novotel, Zürich
➜ **MIS Training**	➜ **4th Annual Chief Security Officer (CSO) Summit 2010** ISACA-Mitglieder erhalten Rabatt	**1.–3.12.2010** Hotel Radisson, Wien