



XXI Convegno annuale: siamo pronti!

Sì, siamo proprio pronti ad accogliervi al nostro XXI Convegno annuale, a Livorno.

Nella prestigiosa Accademia Navale, nei giorni 24 e 25 maggio potremo ascoltare gli interventi di qualificati professionisti sui temi di IT Assurance, IT Governance, Analisi Rischi ed Information Security.

La sera del 24 maggio è dedicata alla cena sociale, che sarà tenuta in un ristorante tipico livornese.

Tutto il Consiglio Direttivo (ma in particolar modo il nostro Presidente che ha fatto la cabina di regia) ha partecipato all'organizzazione.

Sul nostro sito www.aiea.it potrete trovare notizie aggiornate sulla logistica e sugli sconti riservati alle aziende.

La documentazione degli interventi sarà distribuita direttamente al Convegno, su CD.

Certi di aver, anche questa volta, risposto alle richieste ed alle indicazioni dei soci, vi aspettiamo numerosi!

AIEA organizza un “Workshop COBIT”

Martedì 5 giugno 2007, a Milano presso la sede AIEA (Via Valla 16), è previsto un Workshop su COBIT.

Sono quasi 200 i professionisti che hanno frequentato i corsi AIEA di COBIT Base e Avanzato.

A loro e a quanti desiderano confrontarsi con chi sta utilizzando con successo questo modello proponiamo questa opportunità di approfondimento. Sul sito è disponibile la locandina del Workshop

http://www.aiea.it/pdf/corsi/2007/AIEA%20Workshop%20COBIT%202007%20MI%20_2_.pdf

Gruppo di lavoro “Traduzione booklet Sarbanes Oxley”

Dopo aver ottenuta l'autorizzazione da ISACA, è in corso la traduzione della seconda edizione del volume:

IT control objectives for Sarbanes-Oxley

The role in the design and implementation of internal control over financial reporting

Del gruppo di lavoro, coordinato da Daniela Bolli (Poste Italiane), fanno parte:

Pierangelo Ballotta

Fabio Di Sanza

Luigi Giambarini

Guido Leone

Ezio Miozzo

Luciano Orifiammi

Francesco Passi

Silvia Tagliaferro

Sergio Tagni

Roberto Tarussio

Simone Tomirotti

Marco Verneti

Le prossime attività di AIEA

Ricordiamo ai soci che sul sito www.aiea.it è disponibile il calendario aggiornato di tutti gli eventi e dei corsi programmati nei prossimi mesi.

Esame CISA e CISM di giugno 2007

Stanno terminando i corsi di preparazione dell'esame CISA/CISM.

Ricordiamo, che la **data dell'esame è il 9 giugno 2007**.

Per la **sessione invernale**, del prossimo dicembre 2007, le date da ricordare sono:

Inizio iscrizioni: 15 agosto

Data ultima per l'iscrizione: 26 settembre

Esame 8 dicembre 2007

Percorsi formativi

Il corso **Lead Auditor ISO 27001**, si terrà a Milano nel periodo dal 25 al 29 Giugno 2007, presso la Sede AIEA - Valla 16

Il programma e la scheda di iscrizione sono disponibili sul sito

Segnaliamo che a Roma, il Corso COBIT 4.0 è in programma nelle seguenti date:

Corso COBIT 4.0 BASE: 23- 24 ottobre 2007

Corso COBIT 4.0 AVANZATO: 20- 21 novembre 2007

Riceviamo da ISACA

Di seguito, il testo di una mail ricevuta da ISACA:

From: Dept: Certification

To: silvano.ongetta@tiscali.it

Sent: Thursday, May 03, 2007 11:38 PM

Subject: Chapter representatives at exam site

Dear ISACA CISA/CISM Coordinators and Chapter Presidents,

ISACA has experienced another successful registration period for the 9 June 2007 exam, with almost 16,000 CISA and over 2,000 CISM candidates registered. These numbers reflect the tremendous support you provide in marketing the exam and preparing candidates for the upcoming exam.....

.....seguono istruzioni operative sulla logistica dell'esame.....

.....

Kind Regards,

Certification Department

ISACA: Serving IT Governance Professionals

3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois USA 60008

Avviso ai soci

Per la stesura della Newsletter e per la predisposizione del notiziario InfoAIEA, stiamo cercando soci disposti a collaborare. L'idea è di mettere in piedi un "Comitato di redazione" che collabori alla messa a punto dei nostri due documenti. Chi fosse interessato è pregato rivolgersi in segreteria.

Bibliografia

E' on line il nuovo numero di InterLex (<http://www.interlex.it>)

Vi informiamo che sul sito www.cnipa.it sono disponibili molti documenti di interesse per i nostri soci. Ricordiamo, inoltre, che il CNIPA organizza incontri o seminari aperti anche ai soci AIEA.

Seguono estratti di newsletter di altre associazioni

[AIPSI](#)

[ANSSAIF](#)

[CLUSIT](#)

[GARANTE DELLA PRIVACY](#)

Disponibile in PDF all'indirizzo

http://www.aipsi.org/newsletter/Aipsi_NewsLetter-10-2007_4.pdf

In Primo Piano ##

- ISSA European Security Conference 2007

Il 6 giugno a Roma presso l'Hotel Sheraton di Via del Pattinaggio, all'interno dello spazio "Infosecurity Storage Expo", si svolgerà la seconda edizione della "ISSA European Security Conference".

Memori del successo dello scorso anno, abbiamo chiesto ad ISSA International (ed ottenuto) di poter organizzare la conferenza in Italia per il secondo anno consecutivo. Questo è per AIPSI una nota di merito che ci fa ovviamente molto piacere.

L'agenda verrà pubblicata sul sito AISPI (ma non solo) non appena avremo

tutti i dettagli insieme alle modalità di iscrizione gratuita come per lo scorso anno.

Un anticipo doveroso: il Keynote della mattina sarà tenuto da Howard A. Schmidt, presidente ISSA International, nonché Security Advisor di Bush nel 2002. Già questo mi sembra un buon motivo per non mancare, ma altri interessanti interventi ci terranno "sicuramente" attenti nel corso dell'intera giornata!

Eventi con la partecipazione di AIPSI ##

- Corso SANS a Roma, 21-26 Maggio, Roma
"Hacker Techniques, Exploits & Incident Handling", Security 504

SANS Institute, in collaborazione con AIPSI ed HP, e' lieto di Annunciare che terrà uno dei piu popolari corsi a Roma dal 21 al 26 maggio. Tutti i dettagli si trovano al sito <http://www.sans.org/roma07>. Il training

sarà tenuto in italiano con materiale didattico in inglese da Arrigo Triulzi, trainer SANS. E' la prima volta che SANS tiene il famoso corso SEC504: Hacker Techniques, Exploits & Incident Handling in Italiano. L'evento sarà a Roma presso gli uffici HP di Via Achille Campanile 86. La classe ha posti limitati e si raccomanda quindi di non aspettare l'ultimo minuto per l'iscrizione.

Ai soci AIPSI e' riservato uno sconto del 10% sul prezzo di listino,

contattare info@aipsi.org per le modalita' di sconto o per altre informazioni.

ISSA News

- Nuovo Sito ISSA

il sito internazionale di ISSA (www.issa.org) è stato riorganizzato e rinnovato.

Ti invitiamo a prendere visione delle principali novità:

CHAPTER DIRECTORY

Lista dei Chapter in tutto il mondo (basata su Google Maps)

<http://www.issa.org/Chapters/Chapter-Directory.html>

JOURNAL ARCHIVES

disponibile per i Soci l'intero archivio degli ISSA Journal, su pdf

<https://www.issa.org/Members/Journal.html>

STREAMLINED RENEWAL

Su questa sezione del sito è possibile rinnovare l'iscrizione on-line

<https://www.issa.org/Join/Renew-Online.html>

UPDATE YOUR PROFILE

Per aggiornare il Vostro profilo

<https://www.issa.org/Members/Your-Profile.html>

- IT360° Conference & Expo 2007, April 30 – May 2, 2007
Metro Toronto Convention Centre – Toronto, ON, Canada

- ISSA Webcast

I Webcast di ISSA sono disponibili su

<http://www.issa.org/current-webcast.html> a partire dalla data indicata.

- ISSA Journal

Are you interested in contributing an article to the ISSA Journal?

Please contact editor@issa.org, and review the Editorial Guidelines

<http://www.issa.org/PDF/TheISSAJournalGuidelines.pdf> - PDF, 48kb)

Varie

- The Open Web Application Security Project (OWASP), Milano, 15 - 17 Maggio

The Open Web Application Security Project (OWASP) ha il piacere di annunciare che la sesta Application Security Conference si terrà in Italia a Milano dal 15 al 17 Maggio prossimi.

Quest'anno la Conferenza includerà:

- Un Training day (15 Maggio): 3 corsi di una giornata ciascuno sul tema dell'application security.
- La Conferenza principale (16-17 Maggio) prevede un keynote giornaliero, presentazioni sul tema della sicurezza applicativa, paper su temi avanzati, la presentazione dei nuovi progetti OWASP e due panel per incoraggiare la discussione tra i partecipanti.

L'obiettivo della Conferenza è quello di presentare e discutere i temi Più innovativi nel campo della Web Application Security: gli speaker fanno Parte dell'insieme dei maggiori esperti world wide nel panorama della sicurezza delle applicazioni.

Le Conferenze OWASP AppSec sono dedicate alle problematiche e alle Soluzioni di sicurezza applicativa nel mondo reale. E' un'occasione per conoscere molti aspetti dell'application security, incluse le persone, i processi e le prospettive tecnologiche.

Estratto ANSSAIF Newsletter del 3/5/2007

Incontri a Roma e Milano su: "La Gestione dell'emergenza ed il BCP".

Martedì 8 maggio alle ore 15,00 presso la sala stampa al primo piano di Via S. Anselmo, in **Roma** presso la **BNL** (complesso di Piazza Albania), si terrà un incontro sul tema in oggetto.

In particolare, professionisti esperti consentiranno la presentazione di **esperienze pratiche in tema di simulazione dei piani e di gestione dell'emergenza.**

In questo ambito, verranno anche illustrate delle applicazioni sia di **simulazione che di gestione del BCP assistite da computer.**

La formula innovativa di queste sessioni pomeridiane consiste nell'ampio spazio assegnato alle domande ai relatori ed al dibattito fra i presenti.

La stessa edizione si terrà **martedì 15 maggio a Milano** nella Sala Emiciclo, al secondo piano presso la **BNL in Piazza San Fedele 2** (Duomo).

Si prega di prenotarsi mandando una email all'indirizzo: info@anssaif.it

Tutti gli incontri programmati sulle problematiche relative alla Gestione dell'emergenza rientrano in un'iniziativa congiunta ABILab - ANSSAIF finalizzata alla realizzazione di linee guida per le banche. E' pertanto importante la partecipazione di tutte le banche.

Ricordiamo che altri incontri sono previsti secondo il seguente calendario:

Roma:

12 giugno, nel quale oltre a trattare il tema della Gestione dell'emergenza, si parlerà dell'impatto di SEPA sulle banche, e di manutenzione del BCP.

10 luglio

9 ottobre

13 novembre

a **Milano:**

19 giugno, nel quale oltre a trattare il tema della Gestione dell'emergenza, si parlerà dell'impatto di SEPA sulle banche, di manutenzione del BCP e verrà illustrato **il piano di emergenza** da attivare in caso di pandemia, aviaria o di altra natura, **messo a punto da alcune banche svizzere**.

(ottobre e novembre: non sono ancora state stabilite le date).

Il token sta morendo?

Durante il convegno ANSSAIF tenutosi a Vallombrosa lo scorso settembre 2006 ho presentato gli attuali limiti, rischi e i metodi di attacco che possono minare la fiducia del consumatore nel sistema di autenticazione a due fattori (two-factor authentication).

A luglio 2006 l'americana CityBank è stata vittima di un attacco di quello che definisco come il nuovo phishing (per maggiori informazioni potete leggere qui:

http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html .

Se quello di CityBank poteva essere una novità nel panorama delle frodi via Internet, con le ultime notizie provenienti dall'Olanda dobbiamo oramai accettare il fatto che il panorama dei metodi sta cambiando. I clienti della ABM-Amro hanno subito un attacco in aprile 2007 e alcuni conti correnti derubati dei loro soldi (la notizia è riportata qui: <http://www.out-law.com/page-7967>).

Gli attacchi non hanno presentato novità di esecuzione diverse da quelle descritte al convegno: l'utente è attirato su un sito web che opera come proxy del cliente verso la banca. Un perfetto attacco Man-in-the-middle da manuale. Questo dimostra come è oramai poco costoso scrivere codice che possa fare da "corriere" per le credenziali del cliente, aprendo la strada a tutti gli altri gruppi criminali. Il fattore di interesse è che il concetto del "Man-in-the-middle" non è verticale alla tecnologia delle autenticazioni/autorizzazioni a 2 fattori, ma può essere applicato indiscriminatamente a qualunque tipo di trasmissione non istituita in forma esclusiva tra le parti. Prepariamoci quindi a veder sempre di più attacchi in "real-time".

Certamente se i Clienti non cadessero nei trabocchetti delle email "invitanti", evitando quindi di accedere a siti ove i criminali possono inviare ed attivare sul computer della vittima i trojan responsabili dei "dirottamenti" ai siti fasulli, non sarebbero accaduti i casi citati dalla stampa. Ma il Cliente è sempre "padrone", dice il noto adagio, ed allora le aziende di servizio devono affrontare nuovi rischi, nuovi investimenti, se vogliono che il Cliente sia protetto.

Queste le brutte notizie, passiamo ora alle buone.

Abbiamo un immenso vantaggio competitivo sui gruppi criminali: conosciamo i nostri clienti. So che molti di voi, come il sottoscritto, alla menzione del "Behavioral Profiling" si trovano a disagio, ma è anche una delle armi più interessanti contro questi attacchi.

Behavioral Profiling è oggi utilizzato negli aeroporti, soprattutto americani, con risultati molto alterni, così come dai grandi gruppi di carte di credito. Cosa potrebbe fare una banca che non ha mai applicato questa metodologia? Si può cominciare, ad esempio, con operazioni a basso costo, come il controllo della provenienza delle connessioni. Alcune ditte offrono database costantemente aggiornati sulla posizione geografica degli IP. Un investimento di pochi euro, tra database ed implementazione dei controlli, permette di avere il polso della situazione sulla provenienza dei nostri clienti. Se proprio vogliamo essere più sofisticati potremmo legare insieme le posizioni

geografiche dei nostri clienti con le operazioni da loro fatte. Questi accorgimenti, con il tempo, ci danno il prezioso vantaggio di poter creare un cruscotto di pre-allarme. Ma i nostri clienti non si contano nelle unità, ma nelle decine di migliaia, a volte nei milioni.

Ecco come il Behavioral Profiling può diventare veramente interessante: osservare un numero rilevante di connessioni originanti dallo stesso IP sito presso uno stato estero, che guarda caso risulta in una lista nera, diventa un ottimo indicatore di un attacco verso i nostri clienti in atto.

Un altro uso degli indicatori geografici è quello relativo alle distanze: è possibile per un cliente collegarsi dall'Italia e, 2 ore dopo, collegarsi dalla Korea? Un certo sospetto diventa legittimo. Interessante l'articolo di Mr. Richard Baker, Chief Identity Architect della BT (potete leggerlo qui: <http://www.out-law.com/page-7927>) dove ci informa come sta cominciando a profilare i propri clienti proprio in base alle loro abitudini, aggiungendo così un ulteriore tassello nella maglia della sicurezza contro le frodi telefoniche.

Ma cosa succederà quando tutti faranno Behavioral Profiling? Tra 2 o 3 anni circa cominceremo a vedere collegamenti provenienti dall'interno della nostra nazione, magari sfruttando siti precedentemente hackerati. E allora a cosa sarebbe servito tutto questo sforzo? A guadagnare quei 2 anni che ci servono per implementare una soluzione a lungo termine: estendere le nostre maglie di difesa alla clientela.

Come ho già avuto modo di proporre, perché non estendere il concetto del perimetro di sicurezza anche al cliente? E' oramai indubbio che la soluzione perfetta è parte di un futuro lontano, una firma digitale è ben poca cosa senza un adeguato sistema sicuro. Dobbiamo quindi sempre più *investire sul fattore umano*, formare i nostri clienti e lavorare insieme ai produttori di browsers, sistemi operativi e gli enti di certificazione (IETF fra tutti) per fornire un adeguato "kit del piccolo meccanico" che non sia invasivo ma al tempo stesso altamente efficace. Un modo per "abbracciare" i nostri clienti, assicurandoli del fatto che li riconosciamo mantenendoli protetti.

E il "Man-in-the-middle"? Lo ritroveremo di nuovo: cercheranno di inserire programmi nei computer degli utenti allo scopo di manipolare gli stati di memoria, ma converrete anche voi che tra scrivere un programmino in PHP e/o ASP e scrivere un codice Assembler per la manipolazione della memoria esiste una differenza d'investimento elevata, oltre a dover accedere ad un know-how che ad oggi non è particolarmente diffuso. Ed ecco che abbiamo guadagnato altri 3 anni di difesa. Complessivamente questi investimenti porteranno l'aspettativa di vita delle protezioni a 5/6 anni. E fra 6 anni avremo sistemi che potranno degnamente lavorare a stati di memoria stagni per così implementare le vere firme digitali.

Estratto Newsletter Clusit del 30 aprile 2007

=====

2. GERMAN EU COUNCIL PRESIDENCY - INTERNATIONAL CONFERENCE "IT SECURITY 2007"

=====

Il ministero dell'interno Tedesco, nell'ambito del semestre di presidenza della UE organizza il 4 e 5 giugno una conferenza sulla sicurezza informatica.

Interverranno tra gli altri:

Wolfgang Schäuble, Federal Minister of the Interior

Viviane Reding, EU Commissioner for the Information Society and Media -tbc

Willi Berchtold, President of the Federal Association for Information Technology, Telecommunications and New Media e.V. (BITKOM e.V.) - tbc
Andrea Pirotti, Executive Director of the European Network and Information Security Agency (ENISA).

Il Clusit sarà presente col suo presidente, Gigi Tagliapietra, che è stato invitato a presentare in seduta plenaria i risultati di un gruppo di lavoro dell'ENISA che si è occupato di iniziative di awareness a favore dei cittadini.

Il secondo giorno, in particolare, si affronterà anche il tema di un "CERT per icittadini", per il quale alcuni paesi presenteranno delle iniziative che le proprie istituzioni nazionali stanno già realizzando. Il Clusit sta proprio lavorando, in collaborazione con le istituzioni nazionali, ad un progetto che prevede, tra l'altro, un servizio di assistenza online dedicato ai cittadini e il presidente Tagliapietra non mancherà di portare il suo contributo alla discussione.

=====
3. INFOSECURITY ROMA: UN'APERTURA DI GRANDE PRESTIGIO
=====

Il giorno 5 giugno, per la manifestazione di apertura di Infosecurity Roma (5-6 giugno), siamo riusciti a coinvolgere le istituzioni ai più alti livelli.

Dopo il benvenuto e l'apertura dei lavori da parte del Ministro delle Comunicazioni, Paolo Gentiloni (*), si terrà una tavola Rotonda con i rappresentanti delle Istituzioni, con la partecipazione eccezionale del Segretario Generale dell'ITU (*), dal titolo:
"Sicurezza delle informazioni e dei sistemi come servizio per il cittadino e le imprese"

Moderatore: Luca De Biase, Capo Redattore Nova24 (Sole24Ore)

Partecipanti alla Tavola Rotonda:

- Hamadoun Touré, Segretario Generale ITU
- Luigi Nicolais, Ministro per le Riforme e l'Innovazione nella Pubblica Amministrazione
- Luigi Vimercati, Sottosegretario di Stato - Ministero delle Comunicazioni
- Francesco Pizzetti, Presidente dell'Autorità Garante per la protezione dei dati
- Danilo Bruschi, Presidente Onorario Clusit

(*) In attesa di conferma

=====
4. CYBERCRIME
=====

Riportiamo integralmente un interessante articolo apparso sull'ultima newsletter ANSSAIF (www.anssaif.it).

Durante il convegno ANSSAIF tenutosi a Vallombrosa lo scorso settembre 2006 ho presentato gli attuali limiti, rischi e i metodi di attacco che

possono minare la fiducia del consumatore nel sistema di autenticazione a due fattori (two-factor authentication).

A luglio 2006 l'americana CityBank è stata vittima di un attacco di quello che definisco come il nuovo phishing: per maggiori informazioni potete leggere

http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html

Se quello di CityBank poteva essere una novità nel panorama delle frodi via Internet, con le ultime notizie provenienti dall'Olanda dobbiamo oramai accettare il fatto che il panorama dei metodi sta cambiando. I clienti della ABM-Amro hanno subito un attacco in aprile 2007 e alcuni conti correnti derubati dei loro soldi (la notizia è riportata qui: www.out-law.com/page-7967).

Gli attacchi non hanno presentato novità di esecuzione diverse da quelle descritte al convegno: l'utente è attirato su un sito web che opera come proxy del cliente verso la banca. Un perfetto attacco Man-in-the-middle da manuale. Questo dimostra come è oramai poco costoso scrivere codice che possa fare da "corriere" per le credenziali del cliente, aprendo la strada a tutti gli altri gruppi criminali. Il fattore di interesse è che il concetto del "Man-in-the-middle" non è verticale alla tecnologia delle autenticazioni/autorizzazioni a 2 fattori, ma può essere applicato indiscriminatamente a qualunque tipo di trasmissione non istituita in forma esclusiva tra le parti. Prepariamoci quindi a veder sempre di più attacchi in "real-time".

Certamente se i Clienti non cadessero nei trabocchetti delle email "invitanti", evitando quindi di accedere a siti ove i criminali possono inviare ed attivare sul computer della vittima i trojan responsabili dei "dirottamenti" ai siti fasulli, non sarebbero accaduti i casi citati dalla stampa. Ma il Cliente è sempre "padrone", dice il noto adagio, ed allora le aziende di servizio devono affrontare nuovi rischi, nuovi investimenti, se vogliono che il Cliente sia protetto.

Queste le brutte notizie, passiamo ora alle buone.

Abbiamo un immenso vantaggio competitivo sui gruppi criminali: conosciamo i nostri clienti. So che molti di voi, come il sottoscritto, alla menzione del "Behavioral Profiling" si trovano a disagio, ma è anche una delle armi più interessanti contro questi attacchi. Behavioral Profiling è oggi utilizzato negli aeroporti, soprattutto americani, con risultati molto alterni, così come dai grandi gruppi di carte di credito. Cosa

potrebbe fare una banca che non ha mai applicato questa metodologia? Si può cominciare, ad esempio, con operazioni a basso costo, come il controllo della provenienza delle connessioni. Alcune ditte offrono database costantemente aggiornati sulla posizione geografica degli IP. Un investimento di pochi euro, tra database ed implementazione dei controlli, permette di avere il polso della situazione sulla provenienza dei nostri clienti. Se proprio vogliamo essere più sofisticati potremmo legare insieme le posizioni geografiche dei nostri clienti con le operazioni da loro fatte. Questi accorgimenti, con il tempo, ci danno il prezioso vantaggio di poter creare un cruscotto di pre-allarme. Ma i nostri clienti non si contano nelle unità, ma nelle decine di migliaia, a volte nei milioni.

Ecco come il Behavioral Profiling può diventare veramente interessante: osservare un numero rilevante di connessioni originanti dallo stesso IP sito presso uno stato estero, che guarda caso risulta in una lista nera, diventa un ottimo indicatore di un attacco verso i nostri clienti in atto.

Un altro uso degli indicatori geografici è quello relativo alle distanze: è possibile per un cliente collegarsi dall'Italia e, 2 ore dopo, collegarsi dalla Korea? Un certo sospetto diventa legittimo. Interessante l'articolo di Mr. Richard Baker, Chief Identity Architect della BT (potete leggerlo qui: www.out-law.com/page-7927) dove ci informa come sta cominciando a profilare i propri clienti proprio in base alle loro abitudini, aggiungendo così un ulteriore tassello nella maglia della sicurezza contro le frodi telefoniche.

Ma cosa succederà quando tutti faranno Behavioral Profiling? Tra 2 o 3 anni circa cominceremo a vedere collegamenti provenienti dall'interno della nostra nazione, magari sfruttando siti precedentemente hackerati. E allora a cosa sarebbe servito tutto questo sforzo? A guadagnare quei 2 anni che ci servono per implementare una soluzione a lungo termine: estendere le nostre maglie di difesa alla clientela.

Come ho già avuto modo di proporre, perché non estendere il concetto del perimetro di sicurezza anche al cliente? E' oramai indubbio che la soluzione perfetta è parte di un futuro lontano, una firma digitale è ben poca cosa senza un adeguato sistema sicuro. Dobbiamo quindi sempre più investire sul fattore umano, formare i nostri clienti e lavorare insieme ai produttori di browsers, sistemi operativi e gli enti di certificazione (IETF fra tutti) per fornire un adeguato "kit del piccolo meccanico" che non sia invasivo ma al tempo stesso altamente efficace. Un modo per "abbracciare" i nostri clienti, assicurandoli del fatto che li riconosciamo mantenendoli protetti.

E il "Man-in-the-middle"? Lo ritroveremo di nuovo: cercheranno di inserire programmi nei computer degli utenti allo scopo di manipolare gli stati di memoria, ma converrete anche voi che tra scrivere un programmino in PHP e/o ASP e scrivere un codice Assembler per la manipolazione della memoria esiste una differenza d'investimento elevata, oltre a dover accedere ad un know-how che ad oggi non è particolarmente diffuso. Ed ecco che abbiamo guadagnato altri 3 anni di difesa.

Complessivamente questi investimenti porteranno l'aspettativa di vita delle protezioni a 5/6 anni. E fra 6 anni avremo sistemi che potranno degnamente lavorare a stati di memoria stagni per così implementare le vere firme digitali.

Forse.

I.P.ANSSAIF

=====

5. INCHIESTA SUPSI

=====

Il Dipartimento Tecnologie Innovative della SUPSI (Scuola Universitaria Professionale della Svizzera Italiana) ha promosso un'inchiesta sulla sicurezza informatica nelle piccole e medie aziende della Svizzera italiana per poter capire quanto si sta facendo per la protezione dei dati aziendali e dei sistemi informativi. Sia nel caso di una piccola

realtà con pochi computer, così come nella grande organizzazione con una complessa rete aziendali, i risultati raccolti permettono di fare un confronto tra situazioni analoghe, non solo sulle soluzioni tecniche ma anche sui processi e le regole di comportamento.

E possibile consultare i risultati su

www.dti.supsi.ch/Content/main/pdf/X_isi_Documento.pdf

Su <http://isi.dti.supsi.ch/> è anche disponibile uno strumento di analisi dinamica dei dati.

7. NOTIZIE E SEGNALAZIONI DAI SOCI

(La deadline per l'invio di eventuali segnalazioni dei soci per la pubblicazione sulla newsletter è il 25 di ogni mese)

Nei giorni 29 e 30 maggio 2007 si terrà un seminario dal titolo "La dinamica dei contratti ICT. Dal body rental all'outsourcing", corso a due voci tenuto da Luigi Vannutelli e Daniela Rocca. Per maggiori informazioni ed iscrizioni: www.iter.it/seminari_01.htm. Per i soci Clusit è previsto uno sconto del 15%.

Il 6 Giugno 2007, in collaborazione con Infosecurity, si terrà a ROMA, presso l'hotel Sheraton Via del Pattinaggio 100, l'edizione 2007 della "ISSA European Security Conference".

Si segnalano, fra gli interventi, i due "keynote" (mattino e pomeriggio) rispettivamente di:

- Howard Schmidt, Presidente di ISSA International, nonché "Former White House Cyber Security Advisor" del presidente americano Bush nel 2002-2003.
- Antonio Amendola, Senior Adviser to the Secretary General of AGCOM, the Italian Communications Authority.

L'agenda della conferenza è disponibile su

www.aipsi.org/eventi/download/agenda_issa_rome_2007.pdf

La partecipazione è libera previa registrazione su

www.aipsi.org/eventi/evento_0bcf4d2e3d4cc27a44e6138916063b5bc5ace414/form

La Fondazione Ugo Bordoni e l'OCSI stanno organizzando l'ottava edizione della /International Common Criteria Conference/ (ICCC) che si terrà dal 25 al 27 settembre a Roma. La conferenza ha l'obiettivo di riunire organismi di certificazione, laboratori di valutazione, esperti e responsabili della sicurezza IT, utilizzatori di sistemi IT critici e sviluppatori di prodotti commerciali che hanno interesse nella progettazione, nell'implementazione, nella valutazione e certificazione della sicurezza IT.

Per ulteriori informazioni sulla conferenza, incluse quelle relative ad una eventuale partecipazione in qualità di Sponsor o di Speaker in una delle sessioni, si invita a consultare il sito www.8iccc.com.

8. EVENTI SICUREZZA

9 maggio 2007, Firenze - Seminario CLUSIT

"L'utilizzo delle strumentazioni informatiche e telematiche aziendali.

Poteri di controllo e repressione degli abusi da parte del datore di lavoro"

https://edu.clusit.it/scheda_seminario.php?id=7

La partecipazione e' gratuita per il soci Clusit, che possono registrarsi online su <https://edu.clusit.it>

Istruzioni per la registrazione su www.clusit.it/registrazioni2007.htm

15-17 maggio 2007, Milano - 6th OWASP AppSec Conference

www.owasp.org/index.php/6th_OWASP_AppSec_Conference_-_Italy_2007

18 maggio 2007, Cernobbio (CO) - "Realizzare un Data Centre sicuro, performante, scalabile e di facile gestione, i trend tecnologici e i requisiti da considerare per realizzare e disporre di una struttura Ced integrata e pronta alle nuove esigenze del sistema informativo aziendale"

21-23 maggio 2007, Roma - Corso OCSI sulla "Certificazione della sicurezza informatica: guida per l'applicazione dei Common Criteria"

www.ocsi.gov.it/LinkClick.aspx?link=195&mid=195

23-25 maggio 2007, Parigi - EUROSEC 2007 - 18ème Forum européen sur la sécurité des systèmes d'information

www.devoteam.fr/eurosec/2007/home.php?lang=fr

5-6 giugno 2007, Roma - INFOSECURITY Roma

www.infosecurity.it/IT/roadshow/programma.aspx

6 giugno 2007, Roma - Seminario CLUSIT

"Il Social Engineering e la sua applicazione nel penetration testing professionale"

https://edu.clusit.it/scheda_seminario.php?id=8

14 giugno 2007, Milano - Seminario CLUSIT

"Computer forensic: aggiornamenti"

https://edu.clusit.it/scheda_seminario.php?id=9

20 giugno 2007, Roma - Seminario CLUSIT

"Computer forensic: aggiornamenti"

https://edu.clusit.it/scheda_seminario.php?id=10

26 giugno 2007, Segrate (MI) - "La Security nei sistemi di controllo ed automazione, nelle reti ed infrastrutture"

www.anipla.it/FILE_ANIPLA/FILE_MENU/File_Archivio/PROG/2007/gds_26-06-07.pdf



- MAGGIORI GARANZIE A TUTELA DEGLI INVALIDI CIVILI
- UNA POLITICA EUROPEA PER I SISTEMI RFID

Maggiori garanzie a tutela degli invalidi civili

Le aziende sanitarie locali non devono più indicare la diagnosi sui certificati di invalidità

Le aziende sanitarie locali non dovranno più indicare la diagnosi su certificati che attestano il riconoscimento dell'invalidità civile per l'iscrizione alle liste del collocamento obbligatorie o per la richiesta di esenzione dalle tasse scolastiche o universitarie.

Dovranno, inoltre, adottare gli accorgimenti necessari, quali distanze di cortesia, spazi per colloqui riservati, consegna e trasferimento della documentazione in busta chiusa, ed impartire precise istruzioni al personale sanitario, per garantire un elevato livello di tutela della riservatezza delle persone. Lo ha stabilito, con un provvedimento di cui è stato relatore Giuseppe Chiaravallotti, l'Autorità Garante al termine dell'esame di alcune segnalazioni di invalidi civili che lamentavano la violazione delle disposizioni in materia di protezione dei dati personali e chiedevano maggiori garanzie per la loro dignità: in particolare, che fossero omissi da talune certificazioni i riferimenti personali alle patologie invalidanti, specie nei casi in cui fosse stato riscontrato lo stato di sieropositività o l'infezione da Hiv. Richieste legittime secondo l'Autorità. Se può risultare infatti lecito riportare le patologie nei verbali delle commissioni mediche che accertano tipo e grado di invalidità, perché oltre ad essere prescritto dalla normativa è indispensabile in caso di revisione o di ricorso, non è giustificato indicare gli stessi dati nelle certificazioni per l'iscrizione al collocamento o per avere l'esenzione dalle tasse scolastiche. Innanzitutto perché l'indicazione di tali dati non risulta indispensabile e poi perché vi sono normative che prevedono tutele rafforzate per specifiche patologie: ad esempio, le garanzie previste dalla legge 135 del 1990 per i malati di Aids limitano la comunicazione dei risultati di accertamenti per l'infezione da Hiv alla sola persona che si è sottoposta agli esami. Inoltre, tra i requisiti essenziali per avere diritto ad esenzioni o per l'iscrizione a categorie protette, quali l'appartenenza ad una famiglia in disagiate condizioni economiche, l'aver subito una riduzione della capacità lavorativa ecc.,

non risulta mai la patologia sofferta. Ai fini del collocamento, infine, è prevista solo una valutazione delle funzionalità della persona disabile per individuarne le capacità lavorative.

L'Autorità prosegue così nell'azione di tutela dei dati personali in ambito sanitario, che oltre ai numerosi interventi specifici, ha già visto l'adozione di un provvedimento a carattere generale, nel novembre 2005, relativo alle grandi strutture sanitarie pubbliche e private.

Una politica europea per i sistemi Rfid

Sicurezza e privacy fra gli obiettivi primari della Commissione europea

Una politica europea per i sistemi Rfid, la nuova tecnologia che consente l'identificazione attraverso l'uso di radiofrequenze: questo l'obiettivo perseguito dalla Commissione europea attraverso la Comunicazione recentemente diffusa all'esito di una consultazione pubblica conclusasi nel 2006. Una politica a tutto campo, che coniughi l'esigenza di sfruttare le potenzialità di questa tecnologia con l'attenzione alla tutela della privacy ed ai possibili rischi per la salute e l'ambiente. Non è certamente un caso che una parte consistente della Comunicazione della Commissione europea sui sistemi a radiofrequenza in Europa (http://ec.europa.eu/information_society/policy/rfid/doc/rfid_en.pdf) sia dedicata all'analisi delle tematiche connesse alla tutela della vita privata ed ai rischi percepiti rispetto all'Rfid. La consultazione pubblica lanciata nel 2006 dalla Commissione ha segnalato chiaramente che al primo posto fra le preoccupazioni dei cittadini c'è proprio la tutela della privacy. In questo contesto, tutela della privacy non significa soltanto proteggere l'integrità del dato personale in sé, ma soprattutto evitare possibili abusi legati all'interconnessione fra i sistemi basati sulla tecnologia Rfid ed altri sistemi per la gestione delle informazioni (bancarie, commerciali, o di altro genere). La Comunicazione della Commissione riconosce senza ambiguità l'esigenza di dare risposta a queste

preoccupazioni, anche attraverso il coinvolgimento delle autorità di protezione dati che sono chiamate a fornire indicazioni specifiche sulle modalità per garantire che le applicazioni della tecnologia siano rispettose della privacy. La formula-chiave, in questo ambito, è “privacy by design”, ossia fare in modo che la tutela della privacy sia inscritta nella struttura operativa dei sistemi Rfid fin dal momento della loro progettazione. Significativo il fatto che una percentuale elevata delle risposte alla consultazione pubblica (70%) indichi nelle soluzioni tecnologiche la via più opportuna, mentre ben il 66% ritiene che la normativa in materia di protezione dati debba essere aggiornata con riguardo alla tecnologia Rfid.

Il Gruppo articolo 29 sta lavorando da tempo su queste tematiche: oltre al documento di lavoro con cui, nel 2005 (v. Newsletter 31 gennaio 2005), è stata ribadita la validità di alcuni principi fondamentali fissati dalla direttiva sulla protezione dei dati anche nel contesto delle tecnologie Rfid (e tali principi sono stati ripresi puntualmente nella Comunicazione della Commissione, che ha sottolineato l'esigenza di un'adeguata sensibilizzazione a tutti i livelli oltre alla necessità di effettuare un vero e proprio *privacy impact assessment* prima di procedere con l'implementazione di specifici sistemi Rfid), è al lavoro una task force che sta esaminando l'applicazione del concetto di dato personale al contesto Rfid.

Da queste iniziative potranno scaturire indicazioni importanti, anche in vista della redazione di una Raccomandazione che la Commissione intende sviluppare entro la fine del 2007 su tutti gli aspetti dell'utilizzazione delle tecnologie Rfid, con particolare riguardo alla tutela della privacy. I Garanti europei sono chiamati anche a collaborare al Gruppo di lavoro (Rfid *Stakeholder Group*) che la Commissione costituirà prossimamente per elaborare la strategia europea concernente l'Rfid, in previsione di un'ulteriore analisi a tutto campo (ma con particolare riguardo alla privacy ed alla fiducia degli utenti nei sistemi Rfid) che sarà condotta entro la fine del 2008.

NEWSLETTER

del Garante per la protezione dei dati personali
(Reg. al Trib. di Roma n.258 del 7/6/99).
Direttore responsabile: Baldo Meo.

Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n.121 - 00186 Roma.
Tel: 06/69677751 - Fax: 06/69677755. Newsletter è consultabile sul sito Internet www.garanteprivacy.it



- BANCHE: ACCESSO AI DATI E DIPENDENTI INFEDELI
- TELECAMERE IN PISCINA
- BANCHE E COMUNICAZIONI DI DATI PERSONALI A TERZI

Banche: accesso ai dati e dipendenti infedeli

Il Garante richiama un istituto di credito a maggiori controlli contro accessi non autorizzati alla Centrale rischi della Banca d'Italia

E' vietato l'accesso ai dati personali dei clienti conservati nella Centrale rischi della Banca d'Italia se non giustificato da legittime esigenze. Il principio è stato ribadito dal Garante che ha dichiarato illecito il comportamento di un dirigente di banca che, per scopi personali, aveva fatto controllare la posizione debitoria del cognato. L'Autorità, con un provvedimento di cui è stato relatore Mauro Paissan, ha prescritto all'istituto di credito di adottare misure di sicurezza mirate a contenere i rischi di accesso non autorizzato e di effettuare controlli più tempestivi ed efficaci sulla correlazione tra l'accesso ai sistemi di informazione creditizia e l'esigenza di trattare una pratica che giustifichi, nel rispetto della legge, le interrogazioni alla banca dati.

La decisione del Garante è stata presa a seguito di una segnalazione presentata da un ex cliente di una banca con la quale aveva cessato qualsiasi rapporto contrattuale dal 2001. Il cliente, messo a conoscenza che dopo tale data erano stati effettuati da parte dell'istituto di credito accessi alla Centrale rischi della Banca d'Italia relativi alla sua persona e al proprio coniuge, aveva chiesto spiegazioni. L'ente creditizio non aveva fornito idoneo riscontro alla richiesta del cliente, il quale si è quindi rivolto al Garante per vedere tutelati i suoi diritti.

In seguito agli accertamenti disposti dall'Autorità, la banca ha dovuto invece dichiarare che le richieste alla Centrale rischi della Banca d'Italia erano state effettuate indebitamente per ragioni di natura personale da parte di un dirigente dell'istituto di credito, cognato del cliente, che aveva incaricato alcuni collaboratori, pur apparentemente estranei alle finalità private da lui perseguite e non consapevoli dell'illiceità della richiesta, di effettuare le interrogazioni alla Centrale rischi.

Il Garante ha pertanto dichiarato illecito il trattamento dei dati effettuato a danno del cliente. Inoltre, diversamente da quanto dichiarato all'Autorità, la banca non aveva fornito al cliente, a fronte dei chiarimenti da lui richiesti, le vere ragioni dell'accesso illecito e ha pertanto violato il suo diritto ad essere preventivamente informato di ogni trattamento dati che possa interessarlo.

L'Autorità ha infine disposto la trasmissione degli atti alla magistratura per le valutazioni di competenza riguardo agli illeciti penali eventualmente configurabili.

Telecamere in piscina

Vietato riprendere le persone negli spogliatoi

E' vietato utilizzare sistemi di videosorveglianza che riprendano persone negli spogliatoi. Lo ha ribadito il Garante, con un provvedimento di cui è stato relatore Giuseppe Chiaravalloti, adottato a seguito di una segnalazione da parte dei Carabinieri relativa ad alcune telecamere installate in una piscina che riprendevano indebitamente clienti e ospiti. I Carabinieri erano intervenuti dopo la denuncia di un furto avvenuto all'interno degli spogliatoi ed avevano acquisito la videocassetta delle riprese effettuate dal sistema di videosorveglianza. Il sistema si avvaleva di due coppie di telecamere installate negli spogliatoi maschili e femminili della piscina, entrambe visibili. Dalle riprese emergeva che le telecamere, oltre a controllare la zona adibita a guardaroba, riprendevano direttamente le persone anche mentre si cambiavano. Nei pressi dei locali, alcuni cartelli riportavano soltanto una scarna informativa sull'uso di un sistema di videosorveglianza.

L'Autorità ha stabilito che il trattamento dei dati personali violava la riservatezza e la dignità delle persone in quanto, pur essendo lecito l'utilizzo della videosorveglianza per tutelarsi da eventuali danni o furti, non erano stati adottati accorgimenti tecnici volti ad evitare riprese di persone negli spogliatoi. Il Garante ha quindi disposto il divieto di installare telecamere con queste modalità e ha bloccato il

trattamento dei dati già raccolti ed eventualmente conservati. Ha poi prescritto alla società il rispetto delle regole in materia di videosorveglianza, disposte dal Garante con il provvedimento generale del 29 aprile 2004 qualora avesse comunque necessità di dotarsi di sistemi di videosorveglianza a tutela del patrimonio. La società avrà in particolare l'obbligo di adottare tutte le misure e gli accorgimenti necessari ad evitare la ripresa delle persone nei locali adibiti a spogliatoi e di assicurare una adeguata e dettagliata informativa ai clienti sulla presenza di telecamere.

Banche e comunicazioni di dati personali a terzi

Senza il consenso del cliente la banca non può inviare documentazione a persone estranee

Senza il consenso del cliente la banca non può inviare documentazione o estratti conto a persone estranee. Il principio è stato ribadito dall'Autorità Garante, in un provvedimento di cui è stato relatore Giuseppe Fortunato, che ha richiamato una banca al rispetto delle norme che disciplinano la comunicazione di dati personali a terzi. Queste regole prevedono che i dati vengano comunicati solo dopo aver acquisito il consenso della clientela, una volta che questa sia stata adeguatamente informata, oppure, senza consenso, nelle sole ipotesi stabilite dal Codice della privacy: ad esempio, per adempiere ad un obbligo previsto dalla legge o per dare esecuzione ad un contratto.

Il comportamento illecito è stato rilevato dal Garante a seguito del reclamo di un correntista che lamentava la comunicazione al fax dello studio del figlio di informazioni sulla sua situazione bancaria. In particolare la banca non è stata in grado di provare che la comunicazione fosse avvenuta con il consenso del cliente o che rientrasse comunque in una delle ipotesi previste dal Codice. A riprova di ciò, solo in un tempo successivo alla contestata comunicazione è intervenuta una espressa autorizzazione del padre che consentiva al figlio di visionare e fotocopiare documenti depositati presso la banca.

Già in precedenti occasioni il Garante ha affermato che la banca deve verificare che le comunicazioni di dati personali avvengano senza violare obblighi derivanti dalla legge o da un rapporto contrattuale così come stabilito anche dalle regole di comportamento contenute nel codice di autodisciplina elaborato dall'Abi, le quali prevedono che le banche debbano mantenere la riservatezza sulle informazioni acquisite dalla clientela o di cui comunque vengono a conoscenza per la loro funzione. Nel caso esaminato dal Garante non risulta, invece, che la banca abbia svolto la predetta verifica né abbia rispettato il codice di autodisciplina, comunicando senza autorizzazione

dati ad un estraneo in violazione del principio di liceità e correttezza sancito dal Codice della privacy.



AIEA

Sede: Via Valla, 16
20141 MILANO
Tel 02 - 84742365
Fax 02 – 700507644
E-mail: aiea@aiea.it