



Assemblea e...altro!

Questo numero della Newsletter sarà divulgato dopo la pausa estiva, permettendoci di riprendere il nostro colloquio con i soci.

Nei mesi scorsi, l'evento istituzionale più saliente è stata l'Assemblea soci.

Il giorno 18 luglio, ci siamo visti a Milano, per l'appuntamento annuale dedicato all'Assemblea.

Come già l'anno scorso, la concomitanza con una Sessione di Studio ha fatto sì che i partecipanti fossero numerosi, nonostante la vicinanza alle sospirate ferie estive.

L'Assemblea è stata l'occasione "formale" per conoscere, dalla voce del Presidente, quali e quante siano state le attività svolte dalla precedente Assemblea e quante quelle in programma per i restanti mesi del 2007. Argomento importante è stata, inoltre, la relazione del vice-presidente Toffanin sulla situazione economica dell'Associazione che, a fronte di una attenta gestione, possiamo definire molto positiva.

Ai soci presenti è stato consegnato il primo volume delle Guide AIEA, la nuova collana nella quale saranno pubblicati i documenti conclusivi dei Gruppi di Ricerca

AIEA partecipa

Il Capitolo di Malta di ISACA organizza per il 12 ottobre 2007 il proprio convegno annuale, "IT Governance Conference: Governing IT", che sarà abbinato all'incontro dei Presidenti e Vicepresidenti dei Capitoli Europei e Africani avrà un carattere internazionale. Per AIEA, interverrà il Vicepresidente Orillo Narduzzo, che presenterà un caso pratico di utilizzo di COBIT a supporto dell'IT Governance.

Patrocinio

AIEA patrocina il Corso di Alta Formazione in Information Security Management e le 4 giornate della Sicurezza organizzate a Roma dalle riviste ICT Security Forum e Safety & Security Forum

Accordo MIP-Politecnico di Milano e CEFRIEL.

AIEA è lieta di comunicare che è stato rinnovato un importante accordo fatto con MIP-Politecnico di Milano e CEFRIEL.

L'accordo fa riferimento alla sesta edizione del Corso di Alta Formazione in Information Security Management.

Il corso, che si terrà sia a Milano sia a Roma, è nato dalla collaborazione di CEFRIEL e MIP-Politecnico di Milano.

Il corso si svolgerà da ottobre 2007 a giugno 2008. Sarà a "part-time", con lezioni venerdì e sabato, ogni 15 giorni.



La Direzione del Corso offre all'Associazione uno sconto del 10% sulla quota di partecipazione (5.800 + iva se personale o 7.000 + iva se aziendale) per tutti i soci che volessero iscriversi.

Per ulteriori informazioni: site: www.securman.it

La domanda di ammissione dovrà essere compilata direttamente sul sito www.securman.it allegando un dettagliato curriculum vitae professionale e di studi.

AIEA ringrazia CEFRIEL e MIP per la opportunità accordata!

Notizie dai Gruppi di Lavoro

Gruppo di lavoro "VAL-IT"

E' in fase di chiusura il Gruppo di Lavoro "Traduzione VAL-IT". Il documento originale è stato completamente tradotto e se ne sta facendo il controllo qualità. Appena terminate le verifiche, il documento sarà stampato e reso disponibile ai soci.

Gruppo di lavoro "SOX2"

E' in fase di chiusura il Gruppo di Lavoro "Traduzione Sarbanes Oxley 2". Il documento originale è stato completamente tradotto e se ne sta facendo il controllo qualità. Appena terminate le verifiche, il documento sarà stampato e reso disponibile ai soci.

Esame CISA e CISM di giugno 2007

Ricordiamo che, nel mese di agosto, i soci che hanno superato l'esame, sono stati avvertiti, direttamente da ISACA. L'elenco dei soci promossi che hanno autorizzato ISACA a rendere noto il risultato dell'esame è presente sul sito AIEA

Ricordiamo, inoltre, che nelle sessioni di studio saranno consegnati ai nuovi CISA/CISM (ed a quelli che lo sono dal 2003 ed ancora non lo hanno ritirato) i PIN inviati direttamente da ISACA.

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

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.

Percorsi formativi

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



Segnaliamo, inoltre che il 21 settembre a Roma ed il 28 settembre a Milano, inizieranno i corsi di preparazione all'esame CISA e CISM, previsto a Dicembre 2007.

Il corso ITIL Foundation, organizzato in collaborazione con HP, sarà tenuto:
a Milano, nei giorni dall'1 al 4 ottobre 2007
a Roma, nei giorni dal 12 al 15 novembre 2007

Il corso Lead Auditor, dopo il gradimento avuto a Milano, sarà ripetuto a Roma nella settimana dall'8 al 12 ottobre p.v.

Corsi in-house

Informiamo inoltre che, dopo le positive valutazioni dei corsi erogati, ad AIEA è stato richiesto di tenere dei corsi in house.

Opportunità per i soci

A seguito dell'accordo ASIS-ISACA-ISSA, i soci AIEA godranno di uno sconto sul corso di preparazione all'esame ISC2, organizzato da CLUSIT. Nessuno sconto è previsto, per l'iscrizione all'esame (Il contratto di Education Affiliate cita: "No discounts may be offered for the examination")

Il sito AIEA

Alla data del 31 luglio 2007, i visitatori hanno superato il numero di 73.700, con oltre 1200 pagine visitate, mediamente, al mese.

E' interessante notare che gennaio e settembre sono i mesi con più visitatori e che i giorni con il maggior numero di accessi sono, mediamente, il martedì ed il mercoledì.

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.

Un saluto ad un amico che ci ha lasciati

Il giorno 13 luglio 2007, improvvisamente, ci ha lasciati il nostro socio ed amico Angelo Nolli, (Cartasi-SI HOLDING SPA-ARCHITETTURE E SICUREZZA ICT).
Ai familiari giungano le nostre più sentite condoglianze.

Notizie da ISACA

Da Express-line del mese di luglio riportiamo quanto segue:



ISACA to Offer New Credential

At the upcoming International Conference, ISACA will formally announce its newest credential program specifically developed for professionals who have responsibilities for managing and/or governing the IT-related contribution to an enterprise to achieve its business objectives. The certification, supported by the IT Governance Institute® (ITGI™) and built on its intellectual property, will promote the advancement of IT professionals who wish to be recognized for their governance-related experienced and knowledge. The formal name of the certification is expected to be announced shortly, at which time an announcement will be available at www.isaca.org/news.

The initial IT governance professional certification exam is expected to be administered in December 2008. A grandfathering program will be announced shortly, through which highly experienced IT governance professionals may apply for certification without taking the exam. More information will be available soon on the ISACA and ITGI web sites, www.isaca.org and www.itgi.org.

Annual Revocation

The annual CISA and CISM revocation took place on 20 June 2007 for those who did not pay their annual fees and/or report their annual 2006 continuing professional education (CPE) hours. These individuals are no longer allowed to present themselves as certification holders or use the CISA or CISM title. CISAs and CISM's whose certification was revoked due to noncompliance with the CPE policy have 60 days to appeal their revocation by submitting a written request to ISACA International Headquarters.

Il numero di luglio di Global Communiqué informa che:

Lynn Lawton, of Watford, UK, è stata eletta "International President of ISACA"

A lei ed al suo staff gli auguri di tutto il Consiglio Direttivo di AIEA

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

[ANSSAIF](#)

[CLUSIT](#)

[GARANTE DELLA PRIVACY](#)



ESTRATTO NEWSLETTER ANSSAIF DEL 22 GIUGNO 2007

CIO Survey 2007: breve sintesi della presentazione del rapporto

Si è svolta martedì 12 giugno presso l'Auditorium Assolombarda di Milano, la presentazione del rapporto finale CIO Survey 2007 promossa da Microsoft, HP e AMD e realizzata da NetConsulting.

L'incontro è stato introdotto da **ARRIGO ANDREONI**, Presidente del Club per le Tecnologie dell'informazione (Club TI) di Milano e Chairman IT Governance di Telecom Italia, mentre la presentazione dei risultati della ricerca è stata fatta da **GIANCARLO CAPITANI**, Amministratore Delegato di NetConsulting.

La CIO Survey 2007 si è posta come obiettivo quello di analizzare i principali trend strategici e informativi che le Aziende leader del settore privato stanno mettendo in atto. Il motivo di fondo è quello di monitorare quanto e come le imprese italiane si stiano trasformando, quanto lo faranno in futuro e quanto lo faranno attraverso l'IT, o meglio attraverso un approccio di business technology.

- I temi approfonditi nel Survey sono :
- Gli obiettivi strategici delle aziende e dell'IT
- I progetti IT
- I progetti applicativi
- La spesa IT
- Le politiche di sourcing.

Da quanto emerge in sintesi dalla CIO Survey 2007, la condizione necessaria perchè strategie, progetti e obiettivi indicati dalle aziende si possano concretizzare è che si vincano tre sfide importanti :

- La prima è la sfida della produttività, sulla quale il gap dell'Italia rispetto ai maggiori Paesi si è aggravato negli anni, che richiede consapevolezza che gli effettivi guadagni di produttività si ottengono non soltanto riducendo costi ma utilizzando in modo più intensivo e strategico l'IT.
- La seconda è la sfida dell'innovazione che significa innovare di più non solo nei processi, ma anche nei prodotti.
- La terza, e più importante sfida, è quella di crescita dell'intero paese, crescita che deve recuperare i gap accumulati e che deve essere stabile e di qualità. Questa crescita non può che ripartire dalle imprese.

Con riferimento alle tematiche relative alla Sicurezza Informatica e alla Continuità Operativa dal Survey traspare quanto segue.

Uno dei primi obiettivi strategici dei CIO è la gestione dei rischi, ove all'interno del quale il problema della sicurezza è sempre più avvertito. Uno degli indicatori più importanti in proposito è rappresentato dalla crescita degli investimenti in software e servizi IT che le aziende stanno effettuando, investimenti che ammontano a fine 2006 a 541 mld euro con una crescita del 12,8% contro l'1,6% del mercato totale.

L'interesse nei confronti di tematiche relative alla gestione del rischio da parte dei CIO si basa su due fenomeni di tipo strutturale:



- Il primo è legato all'aumento del numero di utilizzatori interni di strumenti IT e della popolazione che accede a banche dati
- Il secondo è relativo al fatto che le minacce alla sicurezza provengano molto più dall'interno che non dall'esterno e che la quota di queste ultime cresca al crescere della dimensione delle aziende.

In questo scenario la *compliance* si inserisce come un driver aggiuntivo che tende a modificare il modo con cui l'azienda interpreta e risolve il problema della sicurezza. Questo spiega come mai proprio i settori nei quali la normativa è più estesa e stringente sono quelli nei quali la spesa media in sicurezza IT è più elevata.

Sempre relativamente alla sicurezza informatica, all'interno dello studio sono poi analizzate le peculiarità dei singoli settori industriali .

A seguire, dopo la presentazione dei risultati è stato effettuato un panel di alcuni CIO tra quelli intervistati per condurre la Survey che, insieme alle aziende sponsor, hanno partecipato ad una tavola rotonda commentando i risultati della ricerca.

L'incontro si è poi concluso con la premiazione di due iniziative IT ritenute meritevoli che sono state premiate da **ALESSANDRO MUSUMECI**, Presidente della Federazione Nazionale delle Associazioni Professionali di Information Management (FidaInform) e Direttore Sistemi Informativi del Comune di Milano.

Il sole 24 ORE e TRENITALIA sono stati pertanto premiati, il primo per "il progetto di business più innovativo, mentre Trenitalia ha conseguito il premio "La figura femminile che nell'IT ha contribuito al processo di rinnovamento dell'azienda in cui opera".

I premi sono andati al progetto innovativo di TRENITALIA che grazie alla tecnologia sarà in grado di offrire ai clienti disabili la prenotazione di speciali servizi e attrezzature di assistenza in fase di salita o discesa dal treno e assicurare l'informativa a tutto il personale interessato; è stata premiata la dott.ssa **Daniela Chiappini**.

Per la figura femminile che nell'IT ha contribuito al processo di rinnovamento dell'azienda in cui opera" è stata inoltre premiata la dott.ssa **Gisella Giongo** per il progetto CRM24, che comporta la realizzazione di un'avanzata architettura SOA per ottimizzare i processi di vendita, generare una visione unificata del cliente e di abilitare l'azienda a scelte di acquisizioni e variazioni organizzative.



ESTRATTO NEWSLETTER ANSSAIF DEL 28 GIUGNO 2007

Annulato l'incontro del 28 giugno presso INFORAV.

Per cause non dipendenti da noi, siamo stati costretti ad annullare l'incontro nel quale erano previsti tre temi: il furto di identità, la gestione dell'emergenza, il progetto AIEA - ANSSAIF sulle problematiche di certificazione del BCP.

E' stato deciso di aggiungere i tre sopradetti temi a quelli già previsti per il prossimo Convegno Annuale che si terrà, quest'anno, a Castel Gandolfo presso l'Hotel Villa degli Angeli, nei giorni 14, 15 e 16 Settembre.

Nei prossimi giorni verrà diffuso il programma completo che, come per gli anni passati, prevede anche delle manifestazioni che coinvolgono le gentili accompagnatrici / accompagnatori.

Le PMI esonerate dalle misure minime di Sicurezza

Alleghiamo il Comunicato Stampa del CLUSIT, emanato per prendere una decisa posizione nei riguardi di questa iniziativa parlamentare.

COMUNICAZIONE AI SOCI CLUSIT =====

Cari soci,

Il Clusit ha diramato nei giorni scorsi un Comunicato Stampa per prendere posizione sull'esonero per le PMI dalle misure minime di sicurezza. Il CS, che vi riporto integralmente in calce alla presente, è stato ripreso da buona parte delle testate di settore ma non ha interessato più di tanto i quotidiani a diffusione nazionale.

Invito tutti coloro che hanno rapporti personali in ambito politico o mediatico di voler trasmettere il contenuto del CS, per cercare di far capire il problema e di evitare che il provvedimento, che è stato votato a larghissima maggioranza alla Camera, passi anche in Senato.

Grazie per la collaborazione.

Paolo Giudice

Segretario Generale CLUSIT

Clusit: no all'esonero per le PMI dalle misure minime di sicurezza La protezione dei dati è una priorità irrinunciabile. Proposte per sostenere le Pmi italiane ad affrontare gli adempimenti di legge.

Milano, 18 giugno '07



Nella seduta 164 del 5/6/2007, la Camera dei Deputati ha votato, a larghissima maggioranza, un progetto di legge che prevede l'esonero per le imprese fino a 15 addetti dall'osservanza delle misure minime di sicurezza per il trattamento dei dati previsti negli art. 33-35 della legge 196/03.

Un provvedimento in forte controtendenza rispetto a quanto sta accadendo in tutto il resto del mondo. I governi nazionali e gli enti sovranazionali come OCSE e Commissione Europea richiamano continuamente ad un maggiore impegno nella protezione delle infrastrutture informatiche, sulle quali si basano le economie di tutti i paesi avanzati, in special modo le Piccole e Medie Imprese, oggi le più esposte ai rischi di intrusione e di attacco informatico.

Il CLUSIT, Associazione Italiana per la Sicurezza Informatica, è impegnato da anni nel nostro paese in un'azione di sensibilizzazione sul tema della sicurezza delle informazioni e dei sistemi e non può che esprimere il suo disappunto per questa iniziativa che rischia di compromettere una parte significativa dei risultati sinora raggiunti.

La legge 196/03 oggi e la 675/96 prima sono state un elemento molto importante per richiamare l'attenzione delle diverse realtà italiane sul tema della protezione dei dati. Nel progetto di legge vi è forse l'intento di "facilitare" e snellire le procedure e i costi delle tecnologie all'interno delle PMI. In realtà si corre il grosso rischio di favorire un modello di sviluppo anacronistico e non competitivo.

Dice Gigi Tagliapietra, Presidente del CLUSIT: "Esentare le Piccole e Medie Imprese dal rispetto di norme di sicurezza espone tutti a gravissimi rischi di attacco: sono infatti le PMI, che costituiscono la stragrande maggioranza delle aziende italiane, l'obiettivo principale delle nuove forme di criminalità in rete e la vulnerabilità di un elemento della rete è la vulnerabilità di tutti." Sappiamo che le PMI hanno difficoltà a proteggersi e temono gli adempimenti burocratici" prosegue Tagliapietra, "ma sarebbe come decidere di non vaccinare i bambini contro le malattie infettive per evitare loro la puntura dell'iniezione."

Aggiunge il Prof. Danilo Bruschi: "L'innovazione non può che passare attraverso le tecnologie dell'informazione e della comunicazione, e lo sfruttamento della piena potenzialità di queste tecnologie non può prescindere da una loro corretta protezione. Sbaglia chi pensa di poter fare innovazione senza sicurezza informatica".

Il CLUSIT chiede che il suddetto progetto di legge sia sospeso, e riconoscendo le possibili difficoltà che alcune Pmi possono incontrare in una corretta applicazione delle legge 196/03, propone che lo stesso sia sostituito con una serie di iniziative mirate a facilitare e supportare le PMI in questo compito.

Tali iniziative possono comprendere:

- il supporto all'istituzione di consorzi di aziende ed esperti del settore che operativamente supportino le aziende;

il sostegno economico delle spese sostenute dalle PMI per assolvere ai suddetti adempimenti. In questo modo quelle che sembrano a molti inutili elucubrazioni di qualche tecnocrate, diventerebbero un momento di crescita per l'intero sistema paese.



ESTRATTO NEWSLETTER ANSSAIF DEL 13 LUGLIO 2007

Insero del Sole 24 Ore sulla Sicurezza.

Come preannunciato dal CLUSIT, Lunedì 9 luglio è stato pubblicato un interessante e stimolante inserto sui temi correnti.

Erano presenti articoli di esponenti e professionisti del CLUSIT, nonché un articolo dell'ing. Anthony C. Wright, dal titolo: "Una materia per fronteggiare possibili scenari di rischio - L'importanza di poter acquisire una capacità strategica per poter rispondere ad incidenti e continuare l'attività ad un livello accettabile". L'inserto è consultabile o scaricabile dal sito ANSSAIF.

Riflessioni sulla Gestione dell'emergenza.

Grazie alle relazioni piene di esperienze e know-how di BiT Systems - Borsa Italiana, CST, International Crime Analysis Association, Value Team VP Tech, ed il contributo di esperti di tante Aziende, Gruppi Bancari ed Imprese Assicuratrici, è stato prodotto un documento che è stato inviato ad ABILab, come concordato. Ciò quale contributo ai fini della pubblicazione di linee guida sulla Gestione dell'Emergenza.

Il documento è reperibile sul sito istituzionale ANSSAIF.

L'ultimo attacco di phishing

Da oggi "gira" in rete la seguente email:

Gentile cliente ,

Nell'abito di un progetto di verifica dei data anagrafici forniti durante la sottoscrizione dei servizi di Banca di Roma e stata riscontrata una incongruenza relativa ai dati anagrafici in oggetto da Lei forniti all momento della sottoscrizione contrattuale. L'inserimento dei dati alterati puo costituire motivo di interruzione del servizio secondo gli art. 135 e 137/c da Lei accettati al momento della sottoscrizione, oltre a costituire reato penalmente perseguibile secondo il C.P.P ar.415 del 2001 relativo alla legge contro il riciclaggio e la trasparenza dei dati forniti in auto certificazione . Per ovviare al problema e necessaria la verifica e l'aggiornamento dei dati relativi all'anagrafica dell'Intestatario dei servizi bancari. Effettuare l'aggiornamento dei dati cliccando sul seguente collegamento sicuro: [Accedi a collegamento sicuro](#)

Cordiali Saluti

Se uno sprovveduto Cliente, che non si è affatto accorto degli errori di italiano presenti nel testo e che continua ad ignorare l'esistenza di questa tipologia di attacchi, dovesse accedere al sito indicato, qualora avesse installato un adeguato prodotto di antivirus e firewall - il cui costo non supera i 50? l'anno - riceverebbe il seguente messaggio:

Il Filtro siti Web ha impedito di aprire questa pagina Web, che potrebbe essere una frode.



Se si desidera comunque accedere alla pagina bloccata:

- Aprire la console principale di XXXXXXXXX (nome del pacchetto, omissso per evitare pubblicità; NdA).
- Fare clic su Controlli Internet e e-mail
- In Filtro siti Web, fare clic sul pulsante Impostazioni....
- Fare clic sulla scheda Siti Web approvati nella finestra visualizzata successivamente, quindi aggiungere l'indirizzo del sito Web (riportato di seguito) all'elenco.

Indirizzo: <http://www.kastleskorner.com/images/index.htm>

Il nostro Cliente dovrebbe a questo punto recedere dal comportamento a dir poco incosciente!

Il mercato è pertanto oramai in grado di fornire prodotti consolidati che avvisano il Consumatore di possibili frodi.

Cogliamo l'occasione per fare una considerazione.

Abbiamo osservato alcuni siti di banche che sono state colpite dal Phishing e quelli di altre che ancora non lo sono state.

A nostro parere, i messaggi ai Clienti sono ancora "poveri" e, a volte, non chiari (il linguaggio del Servizio Legale va molto spesso tradotto o spiegato in un italiano più semplice!).

Alcuni siti, ad esempio, affermano in home page: "attenzione alle email truffaldine". Che vuol dire? Come riconosco, io Consumatore, una email "truffaldina"? Ha un colore diverso? Quale?

In questi casi, ci domandiamo, il Responsabile della Comunicazione è stato interpellato?

Le banche, prima di ricordare al Consumatore che è un suo dovere dotare il computer delle opportune difese, quale un pacchetto software antivirus, personal firewall e capacità di individuare software "malevolo", con installazione automatica degli aggiornamenti non appena disponibili, deve avvertirlo che non deve mai accedere al sito istituzionale tramite collegamento diretto, ossia cliccando su un indirizzo Internet suggerito dalla email che gli è pervenuta, anche se appare essere della sua banca.

Se così facesse, equivarrebbe a commettere l'errore di quelli che, interpellati al telefono o al citofono da una persona che si qualifica per un funzionario della banca o del Gas, forniscono i dati riservati richiesti o sborsano denaro.

E' buona norma, in questi casi, chiamare la propria banca, al numero di telefono conosciuto o reperito dalle Pagine Gialle, e chiedere conferma della richiesta ricevuta. Quante frodi si eviterebbero in questo modo!



ESTRATTO NEWSLETTER ANSSAIF DEL 20 AGOSTO 2007

Incontri Mensili dei Soci.

Ricordiamo che i prossimi incontri si terranno:

- ROMA - 9 Ottobre ed il 13 Novembre - presso la BNL, Via di S. Anselmo (Piazza Albania), primo piano dalle ore 14,30 alle ore 17,30;
- MILANO - 16 Ottobre ed il 20 Novembre - presso PRAXI, Via Mario Pagano, n° 69/A, Auditorium dalle ore 14,30 alle ore 17,30.

Le relazioni verteranno sui temi che ci occupano (ORM e BCM; Verifiche dei BCP; Cyber attacks: esterni ed interni; la tutela del Consumatore; Crisis management) e daranno ampio spazio al dibattito fra i presenti.

Le locandine, contenenti il programma dettagliato, saranno distribuite con la prossima newsletter, non appena avuta conferma della partecipazione da parte dei relatori.

Phishing.

In quest'ultimo periodo vi è stato un incremento nel numero e tipologia di email di phishing. Le Aziende attaccate sono prevalentemente:

Banca di Roma / Capitalia; eBay; Banca Intesa; Banca Sella; Banco di Sicilia; Poste Italiane.

Abbiamo individuato almeno 5 varianti di "esche".

Adducendo ogni volta una differente scusa (l'esca, appunto), i criminali cercano di far abboccare un ipotetico incosciente (o ignorante) correntista ad accedere al sito indicato nella email e li fargli inserire i suoi codici segreti (e da quel momento non lo sono più!).

Le esche più frequenti:

- è richiesta la verifica dei dati del correntista per motivi di sicurezza;
- il conto è stato bloccato (segue la motivazione del blocco, quale ad esempio aver digitato troppe volte un codice errato, e quindi le indicazioni per ripristinarlo);
- accedere ad un conto più sicuro (.e.. vai! più sicuro di così!);
- si ha diritto ad un premio (sic!);
- è stata portata a termine una presunta richiesta di pagamento a terzi e quindi il conto corrente è stato addebitato dell'importo indicato (segue collasso dello sprovveduto correntista per



un ingiustificato addebito e, a questo punto, il suo "abbozzare" all'amo inserendo i dati personali!).

Sul sito abbiamo riportato alcuni di questi esempi.

I sistemi di antispam in commercio, in genere, si accorgono che qualcosa non va in questi messaggi e li segnala come SPAM, ma ciò non avviene sempre, data anche la difficoltà di interpretazione ed il rischio di errori, con conseguente lamentela da parte del Cliente.

Le banche, oltre a migliorare i sistemi di sicurezza, monitorizzano la rete e grazie all'intervento delle Autorità (in particolare della Polizia delle Comunicazioni e del GAT), vengono bloccati i siti criminali.

Trattasi però di una lotta senza fine: ad ogni "bastione" di difesa creato corrisponde un attacco nuovo !!!!

Non ultimo, i cyber criminali stanno mettendo in cantiere altre tecniche, più sofisticate (nel documento sopra citato abbiamo anche riportato un invito a leggere una presunta cartolina di auguri: questa tipologia di email tende a far scaricare sul computer del Cliente un software malevolo che successivamente agisce in modo assai pericoloso e subdolo).

Il Consumatore, il Correntista, il Cliente, deve capire due regole fondamentali:

- non dare mai le proprie credenziali (codice utente, password, numero del conto, ecc.) o dati strettamente personali a qualcuno che ce le chiede, per nessun motivo, qualsiasi sia il canale adottato (email, telefono, citofono, alla porta, ecc.); si deve sempre verificare la veridicità della richiesta telefonando o andando in banca, parlandone con un responsabile se del caso;
- il computer va dotato dei necessari software che ne garantiscano il funzionamento e la protezione, e li aggiorni frequentemente (quanti non hanno software di protezione perché accedono a siti. o non vogliono spendere 50 euro per un software?).

Alla luce di queste e di altre considerazioni che qui, per brevità non stiamo a descrivere, abbiamo predisposto - a distanza di due anni dal precedente - un nuovo volumetto in accordo con ADICONSUM da distribuire ai Consumatori, onde sensibilizzarli ricordando loro poche ma semplici regole.

Il volumetto verrà distribuito in Italia quest'autunno.

Nel frattempo abbiamo ritenuto opportuno monitorare i sistemi di difesa degli intermediari finanziari, in quanto non ci sembra che tutte le Aziende utilizzino appieno le tecnologie che il mercato offre: ciò crea una disparità che finisce con il confondere il Consumatore che, a fronte di messaggi rassicuranti della propria banca, legge sui giornali testimonianze di perdite economiche su Internet anche considerevoli.



ESTRATTO NEWSLETTER CLUSIT 31 agosto 2007

=====

1. CYBERCRIME

=====

Phishing.

In quest'ultimo periodo vi è stato un incremento nel numero e tipologia di email di phishing. Le Aziende attaccate sono prevalentemente: Banca di Roma / Capitalia; eBay; Banca Intesa; Banca Sella; Banco di Sicilia; Poste Italiane.

Abbiamo individuato almeno 5 varianti di "esche". Adducendo ogni volta una differente scusa (l'esca, appunto), i criminali cercano di far abboccare un ipotetico incosciente (o ignorante) correntista ad accedere al sito indicato nella email e li fargli inserire i suoi codici segreti (e da quel momento non lo sono più!).

Le esche più frequenti:

- è richiesta la verifica dei dati del correntista per motivi di sicurezza;
- il conto è stato bloccato (segue la motivazione del blocco, quale ad esempio aver digitato troppe volte un codice errato, e quindi le indicazioni per ripristinarlo);
- accedere ad un conto più sicuro (.e.. vai! più sicuro di così!);
- si ha diritto ad un premio (sic!);
- è stata portata a termine una presunta richiesta di pagamento a terzi e quindi il conto corrente è stato addebitato dell'importo indicato (segue collasso dello sprovveduto correntista per un ingiustificato addebito e, a questo punto, il suo "abboccare" all'amo inserendo i dati personali!).

Sul sito abbiamo riportato alcuni di questi esempi.

I sistemi di antispam in commercio, in genere, si accorgono che qualcosa non va in questi messaggi e li segnala come SPAM, ma ciò non avviene sempre, data anche la difficoltà di interpretazione ed il rischio di errori, con conseguente lamentela da parte del Cliente. Le banche, oltre a migliorare i sistemi di sicurezza, monitorizzano la rete e grazie all'intervento delle Autorità (in articolare della Polizia delle Comunicazioni e del GAT), vengono bloccati i siti criminali. Trattasi però di una lotta senza fine: ad ogni "bastione" di difesa creato corrisponde un attacco nuovo !!!

Non ultimo, i cyber criminali stanno mettendo in cantiere altre tecniche, più sofisticate (nel documento sopra citato abbiamo anche riportato un invito a leggere una presunta cartolina di auguri: questa tipologia di email tende a far scaricare sul computer del Cliente un software malevolo che successivamente agisce in modo assai pericoloso e subdolo).



Il Consumatore, il Correntista, il Cliente, deve capire due regole fondamentali:

- non dare mai le proprie credenziali (codice utente, password, numero del conto, ecc.) o dati strettamente personali a qualcuno che ce le chiede, per nessun motivo, qualsiasi sia il canale adottato (email, telefono, citofono, alla porta, ecc.); si deve sempre verificare la veridicità della richiesta telefonando o andando in banca, parlandone con un responsabile se del caso;
- il computer va dotato dei necessari software che ne garantiscano il funzionamento e la protezione, e li aggiorni frequentemente (quanti non hanno software di protezione perché accedono a siti o non vogliono spendere 50 euro per un software?).

Alla luce di queste e di altre considerazioni che qui, per brevità non stiamo a descrivere, abbiamo predisposto - a distanza di due anni dal precedente - un nuovo volumetto in accordo con ADICONSUM da distribuire ai Consumatori, onde sensibilizzarli ricordando loro poche ma semplici regole.

Il volumetto verrà distribuito in Italia quest'autunno.

Nel frattempo abbiamo ritenuto opportuno monitorare i sistemi di difesa degli intermediari finanziari, in quanto non ci sembra che tutte le Aziende utilizzino appieno le tecnologie che il mercato offre: ciò crea una disparità che finisce con il confondere il Consumatore che, a fronte di messaggi rassicuranti della propria banca, legge sui giornali testimonianze di perdite economiche su Internet anche considerevoli.

(Fonte: ANSSAIF www.anssaif.it)

=====

NOTIZIE E SEGNALAZIONI DAI SOCI

=====

ROMA CAPUT MEDIA! L'AUTUNNO ICT CHE PROIETTA LA CAPITALE NEL MONDO 26-27 Settembre 2007, Marriott Park Hotel - Roma VON Europe 2007, Broadband Business Forum 2007, Video on the Net Europe 2007, Videogov e Netcomm Roma E-commerce Forum: questi gli eventi internazionali e nazionali che si terranno in co-location a Roma il 26-27 Settembre 2007.

Nel corso della due giorni capitolina i leader del mondo ICT e multimediale presenteranno tutte le ultime novità:

- VMNO, Security & Privacy, Open Source e Mobile VoIP
- Municipal Wireless, WiMax, Reti Mesh
- Web e IP TV, DRM, Video Sharing e Web 2.0
- Videosorveglianza in ambito pubblico, in particolare Urban e Homeland Security



- Stato dell'arte sull'eCommerce italiano Clusit è tra i patrocinatori di VON Europe 2007 e Broadband Business Forum 2007 e contribuirà alla realizzazione di un workshop sulla sicurezza legata all'adozione delle comunicazioni IP based in azienda e agli apparati Wireless e mobili.

Chairman della conferenza sarà Raoul Chiesa, Membro del Comitato Direttivo e del Comitato Tecnico Scientifico del CLUSIT.

Per consultare il Programma della manifestazione, per la registrazione gratuita e per partecipare alle conferenze:

www.romacaputmedia.com

=====

MAGGIORE ESPERIENZA PER CERTIFICARSI CISSP

=====

Dal 1° ottobre 2007 entreranno in vigore nuovi termini relativi all'esperienza lavorativa ed all'endorsement.

- Esperienza professionale:

L'esperienza lavorativa richiesta per ottenere la certificazione CISSP® passerà da 4 a 5 anni e deve coprire almeno 2 dei 10 domini del CBK®. E' rilevante che dei 5 anni di esperienza un anno può essere sostituito da una laurea (almeno quadriennale) ed un secondo anno può essere sostituito da una certificazione di quelle elencate alla pagina <https://www.isc2.org/cgi-bin/content.cgi?page=1016>.

- Endorsement:

Chi avrà passato l'esame per certificarsi CISSP, CAP®, o SSCP® dovrà produrre l'endorsement sottoscritto da persona che abbia già ottenuto una certificazione (ISC)². Maggiori e più particolareggiate informazioni sono disponibili alla

pagina <https://www.isc2.org/cgi-bin/content.cgi?page=1227>.

Il calendario dei seminari ed esami CISSP in Italia vede il prossimo appuntamento a Roma:

Dal 22 al 26 ottobre il seminario; il 24 novembre l'esame.

Per chi passerà l'esame in questa sessione varranno i nuovi termini.

Le modalità di registrazione sono alla pagina

www.clusit.it/isc2/calendario_isc2.htm.

Ogni altra informazione può essere richiesta a isc2@clusit.it



=====

EVENTI SICUREZZA

=====

18 settembre 2007, Milano - Seminario Clusit VoIP (in)security

https://edu.clusit.it/scheda_seminario.php?id=11

25 settembre 2007, Milano

La sicurezza dallo A allo z. Le nuove soluzioni per IBM System z

<http://www-306.ibm.com/software/it/events/zsecurity/>

25-27 settembre 2007, Roma

The 8th International Common Criteria Conference

www.8iccc.com/index.php?option=com_content&task=view&id=35&Itemid=43

26-27 settembre 2007, Roma

ROMA CAPUT MEDIA

www.romacaputmedia.com/

2 ottobre 2007, Roma - Seminario Clusit La sicurezza fisica: parte

indispensabile della sicurezza delle informazioni

https://edu.clusit.it/scheda_seminario.php?id=16

3 ottobre 2007, Roma



Associazione Italiana
Information Systems Auditors



La sicurezza dallo A allo z. Le nuove soluzioni per IBM System z

<http://www-306.ibm.com/software/it/events/zsecurity/>

9 ottobre 2007, Firenze - Seminario Clusit VoIP (in)security

https://edu.clusit.it/scheda_seminario.php?id=13

16 ottobre 2007, Milano - Seminario Clusit La sicurezza fisica:

parte indispensabile della sicurezza delle informazioni

https://edu.clusit.it/scheda_seminario.php?id=17

22-26 ottobre 2007, Roma

Seminario CISSP

www.clusit.it/isc2/calendario_isc2.htm



- NUOVI INTERVENTI DEL GARANTE CONTRO LO SPAMMING
- COMUNI E ACCERTAMENTI FISCALI SOLO CON DATI SICURI
- MEDICI E ZTL :MAGGIORI GARANZIE PER I PAZIENTI

Nuovi interventi del Garante contro lo spamming

Vietato il trattamento dei dati ad un sito Internet e a due società che inviavano fax promozionali

Nuovi interventi del Garante contro l'invio di e-mail e fax pubblicitari indesiderati. L'Autorità ha vietato l'uso illecito di dati personali a fini di marketing a tre società che operavano senza consenso dei destinatari. Nel primo caso il Garante, in seguito alla segnalazione di un utente che lamentava la ricezione di e-mail pubblicitarie indesiderate, ha vietato il trattamento dei dati ad un sito Internet che promuoveva libri. Chiamata a dar conto del proprio operato l'azienda dichiarava di utilizzare una mailing list per l'invio mensile di un messaggio "memo" relativo ai libri presentati sul sito e, ritenendolo lecito, inviava ai nuovi utenti, reperiti in rete, un messaggio pubblicitario, insieme alla richiesta del consenso. Nel vietare il trattamento dei dati il Garante ha ribadito non si possono inviare e-mail per pubblicizzare un prodotto o un servizio senza aver prima ottenuto il consenso del destinatario, e che è necessario ottenerlo prima di effettuare qualunque uso dell'indirizzo di posta elettronica. Negli altri due casi, invece, i segnalanti lamentavano la ricezione di pubblicità indesiderata via fax da parte di aziende che promuovevano servizi. Di fronte all'Autorità, le società hanno dichiarato che i messaggi pubblicitari erano rivolti a soggetti economici presenti negli elenchi "categorici" (es. pagine gialle) e non a consumatori e, quindi, ritenevano di potersi avvalere di una disposizione di carattere generale del Codice della privacy che permette di prescindere dal consenso degli interessati, quando il trattamento riguarda informazioni relative allo svolgimento di attività economiche. Tuttavia, secondo quanto affermato dai segnalanti, i dati personali erano presenti solo su elenchi telefonici ordinari e utilizzabili quindi solo per comunicazioni interpersonali, non avendo fornito alcun consenso per il loro uso a fini di marketing. Né, dalla documentazione è risultato che sia stato richiesto un successivo consenso dei destinatari.

Comuni: accertamenti fiscali solo con dati sicuri

Innalzare il livello di sicurezza di Siatel, anche attraverso sistemi di autenticazione biometrica

La collaborazione tra Fisco ed enti locali per la lotta all'evasione fiscale deve garantire la sicurezza della trasmissione dei dati per via telematica. È la condizione posta dal Garante in un parere espresso su uno schema di provvedimento del Direttore dell'Agenzia delle entrate che riguarda le modalità di partecipazione dei comuni all'accertamento fiscale. Entro il 30 novembre 2007 l'amministrazione finanziaria dovrà implementare il livello di sicurezza di Siatel, il sistema per la trasmissione telematica delle informazioni, integrandolo con misure che irrobustiscano le procedure di autenticazione e che limitino nel tempo e nella localizzazione sulla rete la possibilità di accesso ai dati. Nel caso di accessi particolari o di utilizzo di determinati dati, ci si potrà avvalere anche su sistemi di *strong authentication*, basati su caratteristiche biometriche. I municipi, o le società e gli enti partecipati da loro incaricati, potranno comunicare all'amministrazione finanziaria dati anagrafici, codice fiscale e partita Iva delle persone fiscalmente domiciliate nel comune (o ritenute collegate al territorio comunale) nei confronti delle quali verranno rilevati e segnalati fatti, atti e negozi che evidenziano comportamenti evasivi ed elusivi (c.d. "segnalazioni qualificate"). Le comunicazioni, con l'esclusione di dati sensibili e giudiziari, potranno riguardare i seguenti ambiti di intervento: commercio e professioni, proprietà edilizie e patrimonio immobiliare, residenze fittizie all'estero, disponibilità di beni indicativi di capacità contributiva. A loro volta i comuni che ne faranno richiesta potranno ricevere dall'Agenzia delle entrate dati relativi ai bonifici bancari e postali per le ristrutturazioni edilizie, informazioni sulle utenze (energia elettrica, acqua e gas), sulle denunce di successioni, sui contratti di locazione di immobili

Medici e ztl: maggiori garanzie per i pazienti

Non si possono richiedere dati sui pazienti visitati nelle zone ztl per annullare le multe effettuate

I comuni non possono chiedere ai medici generalità o altre informazioni che identifichino le persone visitate a domicilio nelle aree ztl. Ai medici, inoltre, è vietato presentare documenti contenenti dati personali dei pazienti per la contestazione delle multe. Lo ha prescritto il Garante in seguito ad alcune segnalazioni di medici che avevano effettuato delle visite a pazienti domiciliati in zone ztl ed erano stati multati perché privi di permesso. Nelle segnalazioni si manifestava una doppia esigenza: consentire alla categoria l'esercizio della propria attività di urgenza senza essere sanzionata e, nel contempo, garantire il diritto del paziente residente in una ztl a non subire violazioni della privacy. In particolare i medici chiedevano di verificare se le procedure adottate dal comune per il rispetto delle norme di circolazione dei veicoli all'interno delle zone a traffico limitato - comunicazione dei dati anagrafici del paziente, luogo e ora della visita, del codice regionale o di una dichiarazione della stessa persona visitata - fossero compatibili con le norme sulla protezione della privacy. E se fosse inoltre corretta la prassi di alcuni uffici territoriali di governo di chiedere una analoga documentazione per l'accoglimento dei ricorsi presenti dai medici contro le multe. Nel definire le segnalazioni il Garante ha ritenuto sproporzionate e non indispensabili le richieste rivolte ai medici da parte dei comuni. L'accertamento delle violazioni per l'accesso alla ztl, può essere perseguito infatti, secondo l'Autorità, attraverso altre modalità, parimenti efficaci, ma rispettose del diritto alla protezione dei dati personali, quali, ad esempio, la comunicazione dell'indirizzo e del numero civico presso il quale è stato prestato intervento, la targa del veicolo del medico che ha effettuato la visita, il numero di iscrizione all'ordine professionale. L'Autorità ha stabilito, inoltre, che, in caso di ricorso, gli uffici territoriali di governo non possono sollecitare la produzione di documenti contenenti generalità o altre informazioni delle persone visitate in grado di rilevare le condizioni di salute. In questi casi è prevalente infatti, il diritto alla riservatezza dei pazienti.

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