Indice

1. NUOVI SOCI

Recentemente hanno aderito al CLUSIT le seguenti organizzazioni:

- Dipartimento di Chimica Generale - Università di Pavia (Pavia),
- ENTER (Milano)
- European Space Agency ESRIN (Frascati - RM)
- F5 Networks (Milano),
- I.S.I.S. (Repubblica di San Marino)
- NOXS Italy (Cernusco sul Naviglio - MI).

2. LA POSTA ELETTRONICA

Riportiamo un articolo di Gigi Tagliapietra, apparso sul numero di questa settimana del Corriere delle Comunicazioni.

LA POSTA IN GIOCO

Garantire la funzionalità della posta elettronica è un tema cruciale per i singoli e per le imprese, è il primo passo per la business continuity. Ma non è solo questione di tecnologia

Quando si pensa alla posta elettronica si pensa spesso a un servizio di assoluta marginalità rispetto alle applicazioni strategiche d'azienda, un servizio generalmente gratuito, offerto in "omaggio" purché si acquistino altre cose.

Eppure la posta elettronica rappresenta oggi per le aziende un sistema di comunicazione assolutamente indispensabile alla vita stessa dell'impresa.

Anche con l'acqua abbiamo atteggiamenti contradditori: siamo un paese con grandi risorse idriche eppure siamo il secondo consumatore mondiale di acqua in bottiglia, con ben 5 miliardi di bottiglie all'anno, oltre 170 litri pro capite (Fonte- Annuario 2002/2003 delle acque minerali e di sorgente Italia).

Perchè paghiamo 500 volte di più (!!!) qualcosa che ci piove addirittura addosso? Perchè sappiamo che è un elemento indispensabile alla nostra vita e l'acqua per essere utile al nostro organismo deve essere filtrata da agenti patogeni e deve essere disponibile in qualsiasi momento:a casa, in viaggio, mentre facciamo sport o stiamo sdraiati al sole.

Come l'acqua anche la posta, perchè sia utile alla vita dell'impresa deve essere filtrata da contenuti dannosi, disponibile nei momenti critici, accessibile quando si è lontani.

I mail server sono oggi esposti ad attacchi continui e sono veicolo involontario di diffusione di virus e worm anche perchè ci si è dimenticati di quanto sia importante, da sempre il "presidio delle fonti", avere controllo diretto o da parte di nostri sicuri alleati delle nostre risorse primarie.

Lo scopo della sicurezza informatica è quello di garantire che i sistemi chiave dell'azienda siano protetti per consentire all'azienda stessa di sviluppare la propria missione: è questo il motivo per cui parliamo di business continuity come punto focale della sicurezza.

Quale sistema è più cruciale e più "indifeso" se non proprio la posta?

Il primo passo verso la business continuity è quindi quello di riesaminare i nostri sistemi di posta elettronica per garantire che sia sempre funzionante e filtrata con la certezza che non dovremo spendere 500 volte di più!

Privatezza ed autenticità

I recenti attentati di Londra hanno richiamato l'attenzione sulla rilevanza della posta elettronica anche come "arma" utilizzata dai gruppi terroristici e criminali per coordinare le loro iniziative. Come sempre accade sull'onda di eventi drammatici, si sono fatte proposte per limitare e controllare l'utilizzo indiscriminato di strumenti che proprio per la loro natura di libertà rappresentano una minaccia in un utilizzo malevolo.

Torna sui tavoli dei legislatori il tema della definizione degli ambiti in cui "violare" il segreto della corrispondenza, non solo elettronica, e il grande rischio è di prendere provvedimenti "spettacolo" ma del tutto inefficaci sul piano pratico.

Qualcuno ha in mente un nuovo Echelon per la posta? Uno strumento per analizzare "on the fly" tutti i miliardi di messaggi che circolano in rete? Troppo complesso? Allora si chiede di archiviare tutti i messaggi per poterli analizzare successivamente! Avete idea di cosa stiamo parlando in termini dimensionali? Cosa potremmo dimostrare in termini legali, che un determinato giorno Tizio ha scritto a Sempronio? Ma era davvero Tizio? o qualcuno da un certo indirizzo IP con un certo login? O qualcuno che ha manomesso tali informazioni?

L'autenticazione degli interlocutori è un elemento fondamentale da tenere in considerazione e se l'anonimato è stato un cavallo di battaglia a difesa delle libertà individuale oggi l'identificazione certa di mittenti e destinatari rappresenta un passaggio cruciale per contenere fenomeni come lo spam o il phishing.

Non dobbiamo dimenticare che esistono dietro a questi ragionamenti punti di vista molto diversi e "storie sociali" del tutto diverse, si pensi al fatto che l'anagrafe comunale o la carta d'identità, che per noi sono strumenti di convivenza civile, in alcuni settori del mondo anglosassone sono visti come minaccia alla libertà personale.

Tra i due estremi, tra Echelon e "puoi anche essere un cane e nessuno lo saprà", di certo occorre trovare soluzioni concrete e ragionevoli che siano effettivamente utili al contrasto della criminalità e siano nel contempo utili a ciascuno di noi per utilizzare la posta in modo tutelato. I principali attori (aziende di telecomunicazione, internet providers, esperti di sicurezza) non possono agire "di rimessa", non possono aspettare norme controverse per criticarle o sperare che tutto resti come è oggi.

Se la rete non sarà sicura, se dovesse venire meno la fiducia che gli utenti hanno nei sistemi telematici, sarebbe un danno enorme per tutti per cui credo sia doveroso iniziare un processo che porti tutti gli attori a farsi promotori di iniziative concrete ed efficaci per rispondere alla sfida della sicurezza.

Rispetto e valori non solo tecnologie.

L'uso, spesso smodato, delle e-mail ci ha fatto perdere di vista un terzo importantissimo aspetto: quello della autorevolezza del "mezzo" e la conservazione dei documenti nel tempo.

La scrittura di una lettera, rispetto alla comunicazione verbale, serviva non solo a rendere formale e attenta la comunicazione ma a consentire, nel tempo, la ricostruzione di un dialogo e delle sue ragioni, economiche o sentimentali che fossero. La "carta intestata" era un sinonimo di autenticità e la sua scomparsa nel mondo delle e-mail pone temi analoghi a quelli legati all'autenticazione degli individui.

Se in passato esisteva la "sacralità del timbro" e la consapevolezza che scrivere qualcosa sulla carta intestata aziendale implicava assunzione di responsabilità importanti, la struttura "da-a-cc-argomento-testo" ci allontana dall'idea che stiamo compiendo un atto formalmente rilevante e se è vero che "Il mezzo è il messaggio" come diceva McLuhan, il senso di ciò che diciamo è più nel mezzo che nel contenuto.

Oggi la posta elettronica crea una comunicazione diretta e velocissima ma rende assolutamente problematica per una organizzazione, la ricostruzione di processi e di impegni con rilevanti conseguenze economiche e giuridiche.

Come garantire la conservazione nel tempo dei messaggi, come garantire la facile ricostruzione delle sequenze di dialogo, come ritrovare ordini e conferme in questo mondo sempre più effimero? Come mantenere l'unitarietà quando la posta, anche d'impresa è

distribuita nelle caselle personali degli utenti e sparpagliata su centinaia di hard disk? Si possono trovare soluzioni tecnologiche ma non credo siano sufficienti: la risposta deve essere anche vista in termini di rivalutazione del valore che ciascuno di noi da alla comunicazione scritta. Se non diamo valore alle cose, difficilmente troveremo in noi le ragioni per difenderle o per proteggerle e nemmeno comprenderemo gli sforzi che altri vorranno fare per il nostro bene.

Dobbiamo aiutare gli utenti a comprendere che le nostre caselle di posta non sono solo "nostre", se siamo in azienda, anche se lo siamo solo virtualmente, dobbiamo vedere i messaggi che abbiamo nelle nostre caselle come la posta cartacea che una volta avevamo fisicamente sul tavolo: prima di gettarla nel cestino o di confonderla con altri documenti ci abbiamo sempre pensato su.

Anche i messaggi non sono solo "nostri": un messaggio che riceviamo è innanzitutto di chi ce lo ha mandato e non è corretto inoltrarlo ad altri senza il consenso dell'autore.

Lo fareste con una lettera scritta a mano, magari in cui qualcuno che si fida di voi vi apre il suo cuore? La posta è preziosa perchè tratta materiale prezioso: le nostre parole sono un pezzo di noi, noi nella nostra relazione con gli altri.

La posta elettronica è importante per noi come individui e nel contempo una risorsa aziendale strategica e vitale, il diritto alla confidenzialità e il rispetto sono regole sociali che non scompaiono con internet o con il wi-fi. Se pensiamo che la sicurezza sia solo bit e bytes ci perdiamo la sua vera natura che è principalmente etica.

La posta elettronica è davvero come l'acqua: non continuerà a uscire dai rubinetti se ciascuno di noi non la tratterà come un bene prezioso. Le inondazioni e gli tsunami sono lì ogni tanto a ricordarci anche la sua potenza devastante.

3. PESSIMA INIZIATIVA ANTI-PHISHING

Nella newsletter dello scorso giugno ci preoccupavamo per il fatto che negli USA alcuni Istituti Finanziari inviano ai propri clienti via email l'annuncio di nuovi servizi, con l'URL da cliccare per attivarli; generalmente questo tipo di messaggio dice anche che cliccando l'URL verranno chieste le username e password del servizio online che già si ha presso la banca, e che questo attiverà automaticamente il nuovo servizio, che poi sarà possibile personalizzare.

Fortunatamente, a giugno non ci risultavano pratiche di questo tipo nella comunicazione delle banche italiane ed europee.

Ebbene, due settimane or sono una importante banca italiana ha inviato ai propri clienti, utenti del servizio home banking, un'e-mail che costituisce il classico esempio di ciò che una banca NON DEVE fare !!

Riportiamo parte del testo della mail, dove abbiamo messo delle xxxxx al posto del nome della banca e di altri dati identificativi.

Gentile Cliente,

tra gli interventi volti a contrastare le varie forme di "furti di identità elettronica" condotti mediante attacchi diretti ai sistemi informativi degli utenti (es. key-logging, spyware ecc...) oppure attraverso forme di raggiro dell'utente (es. phishing) il nostro Istituto, a far data dal 12 settembre 2005, ha deciso di ridurre l'importo massimo per bonifico a xxxxx euro per le disposizioni impartite mediante xxxxx.

A tal proposito, La preghiamo di collegarsi al sito internet www.xxxx utilizzando i codici di accesso già in Suo possesso e di prendere visione della nuova versione del "Manuale Operativo" che riporta l'introduzione di detto limite nonché i consigli sulla sicurezza.

.....ecc.....ecc.....

Per qualsiasi chiarimento e per il necessario supporto operativo è a Sua completa disposizione il Call Center Clienti al numero verde xxxxx.

Cordiali saluti

BANCA xxxxx

Quando abbiamo telefonato al numero verde della banca, l'operatore ha confermato l'autenticità dell'e-mail.

In pratica la banca, pur sostenendo in tutta la propria comunicazione che non invierà MAI una mail nella quale si chiedono i codici di accesso, ha fatto proprio questo. Un cyber criminale avrebbe potuto benissimo copiare pari pari la mail autentica e farla circolare sul web, modificando semplicemente il link al sito (puntandolo ovviamente ad un sito fasullo, identico a quello della Banca xxxxx).

Il fatto è ancora più grave in quanto il sistema di xxxxx non prevede password dispositive e dunque quando si accede con i codici personali, si può direttamente operare e fare transazioni.

Sbagli di questo tipo rischiano di rendere inutili tutti gli sforzi compiuti dalle banche italiane, dagli operatori del settore, da Istituzioni, Polizia e Associazioni di consumatori per prevenire gli utenti sui pericoli del phishing.

4. CONVEGNI IN AMBITO SMAU

CLUSIT ha collaborato all'organizzazione di un convegno che si terrà nel pomeriggio di giovedì 20 ottobre, dal titolo:

"Sicurezza ICT: cosa sta succedendo nel nostro paese !?".

Anche nel nostro paese, è in continua crescita il numero di enti ed aziende che hanno colto l'importanza della Sicurezza Informatica come fattore abilitante per lo sviluppo del proprio business e che quindi sono oggi impegnate a migliorare in base ai criteri di confidenzialità, integrità e disponibilità i propri servizi.

Scopo di questo convegno è quello di fornire ai partecipanti una panoramica delle iniziative strategiche in corso di progettazione e/o realizzazione nei settori più importanti della nostra economia. A parlarne sono stati invitati coloro che in prima persona stanno partecipando al disegno o alla realizzazione di questi progetti nei comparti della Pubblica Amministrazione, nel mondo bancario, nel mondo delle Piccole e medie imprese e nel mondo dei fornitori di servizi telematici.

Il programma del convegno sarà quanto prima disponibile sul sito del CLUSIT e su quello di SMAU

Sempre in ambito **SMAU** - **Fiera di Milano, dal 19 al 23 ottobre**, si svolgeranno i seminari di **e-Academy** (www.webb.it/html/eacademy/index.php)

Molti di questi, della durata di 50 minuti ciascuno, tratteranno di sicurezza informatica e sono previsti anche 2 interventi del CLUSIT.

1. *Giovedì 20 ottobre, ore 10:00*

"**Formazione, aggiornamento e certificazioni in Sicurezza Informatica**"

Abstract: La sicurezza è pervasiva in ogni processo informatico e per gestirla sono necessarie vaste ed approfondite conoscenze tecniche. Per questo la formazione specifica, il continuo aggiornamento e le certificazioni rappresentano uno strumento indispensabile per la gestione della sicurezza e un investimento strategico per l'azienda. Nel corso del Seminario saranno illustrate le iniziative del CLUSIT con l'intento di aiutare le aziende e gli operatori del settore IT nella scelta di percorsi formativi e di certificazione, che consentano anche di ottenere un adeguato riconoscimento delle proprie competenze.

2. *Venerdì 21 ottobre, ore 13:00*

"**Sicurezza Informatica: strumento basilare per la Business Continuity**"

Abstract: L'investimento in Sicurezza Informatica e' la base necessaria per costruire una solida infrastruttura su cui poggia l'intera organizzazione aziendale. Un piano di Business Continuity non deve essere visto solo come "ancora di salvezza" in caso di incidente, ma come strumento strategico a supporto di ogni evenienza fortuita o meno. Nel corso del seminario saranno illustrati alcuni dei principi base della sicurezza informatica ed i comportamenti che chiunque, all'interno di un'azienda, deve adottare per non mettere in pericolo la continuità operativa e alle volte la sopravvivenza stessa dell'azienda.

5. INFOSECURITY ITALIA 2006 - COMITATO SCIENTIFICO

Il Comitato Scientifico di Infosecurity Italia 2006, che anche quest'anno sarà diretto dal Prof. Danilo Bruschi, vede un maggior coinvolgimento del mondo accademico e delle associazioni del settore.

Hanno già confermato la loro partecipazione:

- Antonello BUSETTO, Direttore Rapporti Istituzionali FEDERCOMIN (www.federcomin.it)
- Sergio CIPRI, Segretario Generale itSMF (www.itsmf.it)
- Luisa FRANCHINA, Direttore Generale ISCOM (www.iscom.gov.it)
- Alfonso FUGGETTA, Direttore Cefriel (www.cefriel.it)
- Luigi MANCINI, Dipartimento di Informatica dell'Università La Sapienza (www.uniroma1.it/dipinfo)
- Vincenzo MEROLA, Dipartimento Innovazione e Tecnologie, Presidenza del Consiglio
- Giulio OCCHINI, Presidente uscente e Direttore Generale AICA (www.aicanet.it)
- Silvano ONGETTA, Presidente AIEA (www.aiea.it)
- Stefano QUINTARELLI, Presidente AIIP (www.aiip.it)
- Federico RAJOLA, Direttore CETIF (www.cetif.it)
- Erminio SEVESO, Presidente AUSED (www.aused.org)
- Domenico VULPIANI, Direttore del Servizio Polizia Postale e delle Comunicazioni - Ministero degli Interni (www.poliziadistato.it/pds/informatica)
- Anthony Cecil WRIGHT, Presidente ANSSAIF (www.anssaif.it)

6. COSTITUITO IL CAPITOLO ITALIANO DI ISSA

È stata appena costituita **AIPSI**, l'Associazione Italiana Professionisti della Sicurezza Informatica, Capitolo italiano di **ISSA** (Information Systems Security Association)

I soci fondatori, anche membri del Consiglo Direttivo, sono:

Agrelli Massimo, DePaoli Claudio, Giudice Giorgio (Tesoriere), Mapelli Maurizio (Segretario), Misitano Marco (Comunication Officer), Molteni Elio (Presidente), Pasquinucci Andrea, Quintarelli Stefano, Telmon Claudio, Zanero Stefano.

ISSA, che conta più di 13.000 soci con oltre 100 Capitoli in tutto il mondo, è l'organizzazione non-profit che rappresenta il più grande network di professionisti del settore. AIPSI si presenta come "associazione di categoria" con un ruolo quindi complementare a quello del Clusit, che fin dall'inizio ha incoraggiato e sostenuto l'iniziativa, portata avanti in gran parte da alcuni dei suoi soci più attivi.

Altre informazioni sono su: www.issa.org.

Il sito del Capitolo è www.issa-italy.org, l'indirizzo e-mail: info@aipsi.org.

7. NOTIZIE DAI SOCI

Terzo convegno Net&SystemSecurity, all'Auditorium del CNR di Pisa

Quest'anno l'associazione informatica @System in collaborazione con l'istituto IIT del CNR, il Dipartimento di Informatica di Pisa, il Dipartimento di Ingegneria dell'informazione (Elettronica, Informatica, Telecomunicazioni) e con il patrocinio di CLUSIT, Comune di Pisa, Provincia di Pisa, ha realizzato il terzo convegno Net&SystemSecurity che si terrà presso l'Auditorium del CNR di Pisa.

L'intera sessione mattutina sarà dedicata al Mobile&Wireless Security (802.11i - WiMax, Location-Based Wireless Security, Mobile Security: Case study in PA) con la presenza anche

di una sessione di Hack-Live. Il pomeriggio sarà aperto dalla sessione che tratterà la nuova scommessa della SUN Microsystems, OpenSolaris, alla quale seguiranno quattro sessioni parallele che spaziano a 360° su tutto l'ambito della sicurezza informatica e riguarderanno i seguenti temi:

- J2ME Security
- Linux Server Security
- Kernel Linux Security
- ASP.NET Security

La partecipazione è gratuita ma si consiglia la registrazione.

Per maggiori informazioni: www.atsystem.org

l'**OCSI** (Organismo per la Certificazione della Sicurezza Informatica), ha reso noto le date in cui si terranno i corsi di formazione sui Common Criteria e sulla certificazione di sicurezza.

Il primo corso, dal titolo "La certificazione della sicurezza informatica: guida per l'applicazione dei Common Criteria", si terrà a Roma, presso la sede dell'OCSI, nei giorni 26-28 ottobre 2005. La seconda edizione è prevista per aprile 2006. Il corso è destinato a coloro che sono interessati a diventare valutatori o assistenti

nell'ambito dello Schema Nazionale. E' articolato in tre giornate, in cui sono fornite, oltre a indicazioni sulle procedure e strategie dello Schema nazionale di valutazione e certificazione della sicurezza, informazioni dettagliate sullo svolgimento delle attività di valutazione in base ai Common Criteria.

Il secondo corso, dal titolo "Nozioni di base sulla Certificazione della Sicurezza informatica", si terrà, sempre a Roma presso la sede dell'OCSI, il giorno 4 novembre 2005. La seconda edizione è prevista per aprile 2006. La giornata è destinata a tutti coloro che, pur non prevedendo un diretto coinvolgimento nelle attività di valutazione, necessitano di informazioni generali sull'utilità e sulle modalità di ottenimento della certificazione di sicurezza. Inoltre, vengono fornite nozioni sul concetto di certificazione di sicurezza e sulla strategia dello Schema nazionale.

Tutti i dettagli dell'iniziativa sono disponibili sul sito web dell'OCSI (www.ocsi.gov.it) e, in particolare, all'indirizzo web www.ocsi.gov.it/Default.aspx?tabid=184

8. SEMINARI CLUSIT DI SETTEMBRE

SEMINARIO CLUSIT

Elementi probatori negli illeciti: Raccolta e mantenimento degli elementi probatori negli illeciti informatici.

MILANO 04 ottobre 2005

ROMA 25 ottobre 2005

Sono disponibili ancora alcuni posti a Roma.

Il modulo per registrarsi: www.clusit.it/edu/reg_sem_form.pdf

Per i Soci Clusit la partecipazione è gratuita*

PROGRAMMA

Mattina

- attività illecita attraverso l'uso delle tecnologie informatiche
- problematiche giuridiche legate agli insider (dipendenti infedeli)
- aspetti sostanziali e processuali della prova
- la computer forensic ed il valore probatorio degli elementi raccolti

- il ruolo delle policy aziendali nella prevenzione degli illeciti
- il rapporto con la polizia giudiziaria durante l'attività d'indagine
- la responsabilità dell'azienda per il reato del dipendente (aspetti civili e penali)

Pomeriggio
- computer forensics: una nuova disciplina della polizia scientifica
- computer forensics: l'arte di avanzare con fantasia e una legislazione vacante
- computer forensics: sequestro, catena della custodia, presentazione delle prove
- regole di comportamento nell'assunzione della prova informatica
- le attività propedeutiche
- le regole da rispettare
- gli errori più comuni
- alcuni esempi pratici

Agenda:
08,50 registrazione e consegna del materiale didattico
09,10 inizio seminario
10,50 coffe break
11,10 ripresa seminario
12,50 termine della sessione del mattino
13,00-14,00 buffet
14,10 inizio sessione pomeridiana
15,50 coffe break
16,10 ripresa seminario
17,50 termine del seminario
Docenti: Bruno Fiammella, Andrea Ghirardini
Luogo:
- Milano allo StarHotel Splendido - Viale Andrea Doria, 4
- Roma al Centro di formazione Percorsi Srl - Viale Manzoni 22

*Condizioni e modalità di iscrizione per Soci e non soci su www.clusit.it/edu
Per ogni informazione chiedere a edu@clusit.it

9. EVENTI SICUREZZA (Tutti i dettagli sulle manifestazioni sono disponibili sul sito CLUSIT alla voce EVENTI)

4 ottobre 2005, Milano
Seminario CLUSIT "Elementi probatori negli illeciti

6 ottobre 2005, Milano
Seminario informativo su BS 7799: lo standard per la gestione della sicurezza delle informazioni

7 ottobre 2005, Udine
"Tutti i vantaggi della Rete...SENZA RISCHI 2005: l'Alra Affidabilità nella gestione del Dato"

13 ottobre 2005, Pisa
Terzo convegno Net&SystemSecurity, all'Auditorium del CNR

18 ottobre 2005, Roma
Seminario CLUSIT "Elementi probatori negli illeciti"

19-23 ottobre, Milano
SMAU 2005

8 novembre 2005, Milano
"ICT, dalla Sicurezza alla Gestione Continua del Business"

14-18 novembre, Milano
Seminario di preparazione all'esame CISSP

23-24 novembre 2005, Roma
"Firma Digitale, E-Mail Certificata e CNS"

CLUSIT - ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA*
Dipartimento di Informatica e Comunicazione - Università degli Studi di Milano
Via Comelico 39 - 20135 MILANO - cell. 347.2319285
* associazione senza fini di lucro, costituita il 4 luglio 2000