Indice

1. NUOVI SOCI

Hanno aderito al Clusit:

- ASSINTEL (Milano)
- ASTARO AG (Karlsruhe - DE)
- Quint Wellington Redwood Italia (Milano)

2. NOVITÀ IMPORTANTI IN TEMA DI DPS

Sulla Gazzetta Ufficiale n.147 del 25 giugno è stato pubblicato il Decreto Legge 25 giugno 2008 n.112 "Disposizioni urgenti per lo sviluppo economico, la semplificazione, la competitività, la stabilizzazione della finanza pubblica e la perequazione tributaria".

In particolare, l'Art. 29 "Trattamento dei dati personali" modifica sostanzialmente gli obblighi previsti dal d. lg. 30 giugno 2003, n.196, in quanto abroga di fatto il DPS (sostituendolo con l'autocertificazione) per tutte le aziende che non trattano dati sensibili o che trattano solo dati sensibili inerenti salute e malattia dei propri dipendenti, senza indicazione della diagnosi.

Riportiamo di seguito un estratto:

1. All'articolo 34 del decreto legislativo 30 giugno 2003, n. 196, dopo il comma 1 è aggiunto il seguente:

«1-bis. Per i soggetti che trattano soltanto dati personali non sensibili e l'unico dato sensibile è costituito dallo stato di salute o malattia dei propri dipendenti senza indicazione della relativa diagnosi, l'obbligo di cui alla lettera g) del comma 1 e di cui al punto 19 dell'Allegato B è sostituito dall'autocertificazione, resa dal titolare del trattamento ai sensi dell'articolo 47 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, di trattare soltanto dati personali non sensibili, che l'unico dato sensibile è costituito dallo stato di salute o malattia dei propri dipendenti senza indicazione della relativa diagnosi, e che il trattamento di tale ultimo dato è stato eseguito in osservanza delle misure di sicurezza richieste dal presente codice nonchè dall'Allegato B).».

Il Garante per la protezione dei dati personali ha introdotto delle semplificazioni per taluni adempimenti previsti dal d.lg. 30.06.2003, n.196. Le semplificazioni riguardano i trattamenti per finalità amminisrative e contabili, sia in ambito pubblico che privato, in particolare nei riguardi di piccole e medie imprese, liberi professionisti e artigiani.

Il provvedimento del Garante è disponibile su www.garanteprivacy.it/garante/doc.jsp?ID=1526724

3. CYBERCRIME

Nuova forma di Phishing

Oltre a far leva su vincite di televisori, accrediti sui conti, assegnazione per sorteggio di apparati tecnologici, comunicazione di reati e preavviso di sanzioni al codice della strada, si sta diffondendo in questi giorni una diversa forma di social engineering che utilizza la formula del "rimborso su ritardi dei treni" e sembra provenire da Trenitalia SpA.

La mail che viene inviata, a firma di un presunto responsabile rimborsi Trenitalia SpA, si presenta come segue:

Da: Trenitalia [mailto:trenitalia@rimborsi-online.com]
Inviato: mercoledì 4 giugno 2008 0.02
A: info@anssaif.it
Oggetto: Rimborso Trenitalia
Gentile Viaggiatore,
Ferrovie dello Stato è lieta di informarla che dal 1° Maggio 2008 è possibile richiedere il rimborso sui ritardi effettuati su tutte le tratte nazionali.
A seguito di ciò, la informiamo che da un nostro controllo contabile, le spetta un rimborso di Euro 780,00.
La invitiamo a visualizzare il modulo in allegato, e seguire le istruzioni per farci pervenire tale modulo.
N.B. Il rimborso avverrà mediante bonifico bancario entro e non oltre 5 giorni lavorativi dalla ricezione.

Qualora si verificassero problemi con il mdulo allegato, può visitare il nostro sito o scaricare nuovamente il modulo qui

---

Certi di averle fatto cosa gradita Porgiamo Distinti Saluti
Ennio Zibris
Responsabile Rimborsi
Trenitalia S.p.A.

Alla mail viene allegato un file "MODULOA344508.zip" (642 B) che, unzippato, risulta contenere due file entrambi di 1Kb NESSUNO DEI QUALI APRIBILE e precisamente:

- AcrobatReader.txt
- MODULOA344508.pdfx.txt

La pericolosità di tale tecnica di social engineering consiste proprio nella furbizia adottata: nell'impossibilità di aprire i moduli allegati (CHE NON CONTENGNO NULLA) il destinatario della mail viene invitato a visitare il sito www.rimborsi-online.com dal quale scaricare il modulo citato zippato.

Tuttavia il file ZIP che si scarica, contiene un EXE al cui interno si annida il virus

"Trojan-Downloader.Win32.Agent.lyg"

(Engine error code: 0x00010000; Engine version: 5.0.0.38; Pattern version: 080604.093211.828550; Pattern date: 2008.06.04 09:32:11) individuato dai più comuni antivirus, se installati.

Il sito civetta, per completezza di informazione, risulta essere stato registrato in California il 2 giugno 2008 a nome di un utente anonimo (WhoisGuard Protected (a3d100cd29d0483b960f33ed32667381.protect@whoisguard.com)che ha fornito come indirizzo "8939 S. Sepulveda Blvd. #110 - 732 Westchester, CA 90045"

(Tratto dalla Newsletter ANSSAIF - www.anssaif.it)

4. RACCOMANDAZIONE OECD SULLA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE

Con questa raccomandazione, l'OECD traccia delle linee guida sulle politiche nazionali e sul come migliorare la cooperazione internazionale per la protezione delle infrastrutture critiche, la cui perturbazione o distruzione avrebbero un impatto importante sulla sicurezza e il benessere dei cittadini, o sul funzionamento del governo o dell'economia. Queste linee guida si basano su best practices evidenziate in uno studio comparativo dell'OECD sulle policies in materia di critical information infrastructures (CII) di sette paesi

La raccomandazione: www.oecd.org/dataoecd/1/13/40825404.pdf

Lo studio comparativo: www.oecd.org/dataoecd/25/10/40761118.pdf

Fonte:
www.oecd.org/topic/0,3373,en_2649_37441_1_1_1_1_37441,00.html?rssChId=37441#40862210

5. PROPRIO QUANDO SI RICOMINCIA A PARLARE DI NUCLEARE

La gestione delle patch è un problema che deve sempre essere affrontato attentamente, specialmente se siamo in ambienti industriali (sistemi di controllo), soprattutto nelle Infrastrutture Critiche

-Software Update Caused Emergency Shutdown at Nuke Plant (June 5, 2008)

Flaws in a software update caused the Hatch nuclear power plant in Baxley, GA to shut down in early March of this year. The software update was made on just one computer on the plant's business network.

That computer monitors chemical and diagnostic data from one of the plant's primary control systems.

A spokesperson said the emergency system reacted as it was designed to and that the security and safety of the plant were never in danger.

Although technicians knew of the two-way communication between some computers on the corporate and control networks, the engineer who installed the update was not aware that reboot on the corporate side would force a reset on the control side.

Network connections between the affected servers have since been severed.

www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958_pf.html

[Editor's Note (Northcutt): Not terribly amazing, nor is this the first time: www.cdi.org/nuclear/kurchatov.cfm

http://findarticles.com/p/articles/mi_m1511/is_n5_v17/ai_18199114

www.nbcsandiego.com/news/15415516/detail.html]

(Autore: Enzo Maria Tieghi)

6. IN FINALE MA SENZA SOLDI

Riportiamo integralmente l'articolo di Gigi Tagliapietra, pubblicato su NOVA (Il Sole 24Ore) del 12 giugno.

Non tutti sanno che siamo campioni del mondo di security. Lo siamo stati negli anni scorsi con i team dell'Università di Milano e del Politecnico di Milano e il 7 dicembre scorso un team italiano ha nuovamente vinto la gara di "Capture The Flag" indetta dall'Università di Santa Barbara in California.

Ora la squadra del Laboratorio Sicurezza e Reti (Laser-CERT-IT) dell'Università degli Studi di Milano che ha partecipato alle qualificazioni per il Capture The Flag al DEFCON (una delle conferenze più importanti nel mondo della sicurezza informatica) è arrivata al terzo posto e si è aggiudicata l'accesso alla finale di Las Vegas dall'8 al 10 agosto prossimi.

La selezione è stata molto difficile perché i team in gara da ogni parte del mondo erano 371 e i posti per la finale solo 7 e più che una gara si tratta di una prova di pentathlon con cinque diverse prove da superare, alcune delle quali richiedono più di 10 ore di frenetica attività da parte dell'intero team.

A parte l'orgoglio di bandiera perché è importante il Capture The Flag? "E` un ottimo esercizio", dice Mattia Monga, animatore del team italiano e responsabile del CERT-IT, "per imparare a difendersi con competenza, serve toccare con mano quanto sappiano essere diabolici gli attaccanti e occorre un ampio spettro di competenze perché ci sono applicazioni da analizzare, prove di analisi investigativa, esami di codici binari alla ricerca di vulnerabilità, esercizi di *presa del controllo* di sistemi online e di macchine in rete, quiz e test di conoscenza: insomma c'è proprio di tutto."

Il *gioco*, proprio come a Rubabandiera, consiste nel catturare files nascosti nel sistema degli avversari e nel contempo difendere quelli celati nel proprio, ma soprattutto di mantenere attivi i servizi che il proprio sistema offre alla rete. Non basta quindi essere dei bravi *attaccanti*, bisogna essere altrettanto abili e attenti nella difesa dei propri sistemi dagli assalti altrui perché i punti ottenuti dalla *cattura di una bandiera avversaria* si moltiplicano in base alla capacità di garantire la continuità operativa dei propri servizi.

Non è un segnale di poco conto l'eccellenza italiana in questa attività perché la security non richiede solo competenza tecnologica ma anche intuito, capacità di *pensiero laterale*, improvvisazione, interdisciplinarietà e grande spirito di collaborazione.

Come in altri ambiti di ricerca anche la sicurezza informatica soffre di scarsi investimenti e di risorse limitate e il nostro team non fa eccezione: la partecipazione alla finale di Las Vegas è a rischio perché occorre trovare circa 20.000 euro per finanziare la spedizione.

"Serve un team di almeno dieci persone che si diano il cambio" dice ancora Monga "perché la prova dura ininterrottamente per due giorni e mezzo dato che l'obiettivo degli organizzatori è proprio quello di creare il più possibile una situazione realistica, in cui anche la disattenzione, la noia e la fatica hanno un ruolo non secondario."

Intanto grazie alle prime notizie circolate in rete dal blog di Nova100, la Microsoft Italia ha deciso di dare un sostanziale contributo perché la squadra possa gareggiare e l'auspicio è che altre aziende seguano il suo.

Lo scopo non è solo quello di partecipare e di vincere, ma anche di mantenere elevato il livello di conoscenze e di esperienze che si acquisiscono in occasioni di questo genere e soprattutto di sviluppare una inestimabile rete di relazioni personali tra esperti a livello mondiale che sono indispensabili per difendersi efficacemente in caso di attacco.

Lo hanno ribadito con forza i rappresentanti del CERT Estone quando hanno presentato al meeting organizzato dall'Unione Europea sulle sfide della sicurezza del futuro, le loro riflessioni dopo l'attacco informatico subito dal loro paese nella primavera scorsa: servono competenze che non si improvvisano perché gli attaccanti sono abili, scaltri, determinati, serve attenzione e grande lavoro perché quando ti attaccano più di 16.000 computer simultaneamente è come difendersi da un enorme branco di piranas. Una cosa è certa, gli attacchi ormai vengono attivati su scala mondiale e senza collaborazione internazionale non c'è possibilità di difesa.

7. RAPPORTO ASSINFORM 2008

Oggi, 30 giugno, è stato presentato a Roma il Rapporto Assinform 2008 sull'Informatica, le Telecomunicazioni e i Contenuti Multimediali.

Su www.assinform.it sono disponibili i dati del rapporto e il convegno di presentazione in videostream http://rapporto2008.dolmedia.tv

Il comunicato stampa, che riassume i dati del rapporto:
www.assinform.it/aree_sx/informazioni/comunicati/comunicato_rapporto_2008.htm

8. INFOSECURITY ROMA

È terminata la terza edizione di Infosecurity Roma (10-11 giugno) e i convegni Clusit hanno riscosso un gran successo. Al seminario Clusit del primo giorno hanno partecipato ben 144 persone (senza precedenti per un seminario di taglio tecnico).

Ai convegni del giorno dopo, spesso gli spettatori sono rimasti in piedi, per esaurimento dei posti.

Le presentazioni sono disponibili su www.clusit.it/archivio.htm#infosec08RM

9. SICUREZZA E UTENTI INTERNI

Un recente sondaggio che ha interessato oltre 7.000 professionisti di sicurezza in tutto il mondo, ha fatto emergere che le Aziende sono molto più preoccupate che in passato dei rischi rappresentati dalle minacce provenienti dall'interno e pongono sempre maggiore attenzione sulla formazione del personale e la protezione dei dati.

I punti più significativi della ricerca:

Il 51% del campione ha ammesso di considerare come minaccia principale la propria forza lavoro interna

Percentuale questa cresciuta rispetto ad un analogo sondaggio del 2006. Fenomeno che può trovare giustificazione con l'aumento del numero di dipendenti che operano da remoto: "Ciò ha accresciuto le possibilità di attacco da parte di un aggressore, sia esso un dipendente disonesto che uno in buona fede ma in possesso di dispositivi che non gli consentono un accesso protetto ai dati da remoto".

Il 48% degli intervistati è convinto che la sicurezza non la si implementa unicamente con strumenti tecnologici.

Tutti sono difatti convinti che il rispetto volontario delle policy aziendali di sicurezza è stato il fattore principale ad aver garantito fino ad oggi una sufficiente protezione dei dati. Per questo si è rilevata una maggiore propensione delle aziende ad investire in formazione del proprio personale.

E' stato rilevato inoltre un crescente interesse nel proteggere i dati di natura confidenziale.

Circa il 68% degli intervistati prevede un aumento della spesa nel 2008 per la protezione dei dati: il 66% considera più importante la sicurezza dei database, mentre il 58% reputa vitali i processi di rimozione e conservazione dei dati.

Il documento completo è disponibile su:
https://www.isc2.org/download/2008_Global_WF_Study.pdf

(Tratto dalla Newsletter ANSSAIF - www.anssaif.it)

10. GRUPPO CLUSIT SU LINKEDIN E FACEBOOK

Nel mese di febbraio avevamo costituito un Gruppo Clusit su www.linkedin.com, a cui hanno già aderito circa 150 soci (per aderire: www.linkedin.com/e/gis/54878/4636632385C5).

Purtroppo non abbiamo potuto rispondere positivamente ad altrettante richieste di adesione al Gruppo pervenute da parte di operatori del settore che non avevano i requisiti per farne parte, e cioè: essere soci individuali, essere dipendenti di aziende socie o aver partecipato alle attività del Clusit e/o a progetti specifici in cui è coinvolto il Clusit.

Ora abbiamo il piacere di segnalarvi che su www.facebook.com è stato creato il gruppo 'CLUSIT - Associazione Italiana per la Sicurezza Informatica':

www.facebook.com/group.php?gid=11171618175&ref=ts

A differenza di Linkedin, che è uno strumento di social networking orientato principalmente alle relazioni professionali, Facebook è piuttosto orientato alle relazioni personali e, come tale, può raggruppare anche gli amici e simpatizzanti del Clusit.

Gruppo CISSP Italia su LinkedIn

Ci viene segnalata la creazione di un gruppo LinkedIn per i Certificati CISSP Italiani, o che risiedono e lavorano in Italia.

Questo l'indirizzo per l'iscrizione, che é riservata ai possessori di una certificazione CISSP: www.linkedin.com/e/gis/119039/4DA7FC5869BF

12. ICASI - INDUSTRY CONSORTIUM FOR ADVANCEMENT OF SECURITY ON THE INTERNET

È stata annunciata la costituzione di ICASI, Industry Consortium for Advancement of Security on the Internet www.icasi.org.

ICASI intends to be a trusted forum for addressing international, multi-product security challenges. This trusted forum extends the ability of information technology vendors to proactively address complex security issues and better protect enterprises, governments, and citizens, and the critical IT infrastructures that support them. ICASI shares the results of its work with the IT industry through papers and other media.

Il comunicato stampa: www.icasi.org/articles/art_001.htm

12. OFFERTE DI LAVORO

Una importante azienda manifatturiera del settore metalmeccanico che opera in contesti internazionali, nell'ottica del potenziamento dell'area engineering, ricerca due figure professionali con competenze in sicurezza informatica.

In particolare si ricerca, per la sede di Roma:

1. Un **SYSTEM ENGINEER FOR SECURITY DESIGN ACCREDITATION** (RIF 2981)

La posizione, che dovrà operare in regime di nulla osta di sicurezza, avrà le seguenti responsabilità:

- Monitorare e assicurare che l'implementazione e la manutenzione della certificazione, in materia di sicurezza ed il processo di accreditamento, siano in linea con l'oggetto della valutazione.
- Rappresentare il punto di riferimento tecnico per il subappaltatore.
- Garantire la corretta applicazione delle procedure da parte del subappaltatore come pure la coerenza del Security Design.

Il candidato ideale è in grado di seguire il processo di accreditamento di un sistema complesso, per il quale ha maturato esperienza nel gestire i vari aspetti, in ottica di sicurezza, seguendo la conformità con le norme nazionali ed internazionali e secondo i progetti di "classified complex system".

Si richiede:

- Età: 35/40 anni;
- Titolo di studio: Laurea in Ingegneria o titolo equivalente;
- Esperienza: almeno 7-10 anni di esperienza nel ruolo (nell'ambito del sistema di navigazione satellitare e nell'ambito della sicurezza).
- Conoscenza delle lingue: Molto buona la conoscenza della Lingua Inglese.
- Soft Skill: capacità analitiche e di precisione, affidabilità, attitudini relazionali.

2. Un **SENIOR SYSTEM ENGINEER EXPERT IN SYSTEM SECURITY** (RIF 2982)

La posizione, che dovrà operare in regime di nulla osta di sicurezza, è leader del gruppo di riferimento ed è responsabile del coordinamento tecnico delle attività relative alla sicurezza dei sistemi complessi. Dovrà occuparsi delle seguenti attività:

- Analisi e valutazione della vulnerabilità e del rischio.
- Definizione di Piani di Sicurezza ed identificazione dei requisiti/funzionalità dei Sistemi di Sicurezza anche a livello di progettazione;
- Analisi degli impatti dovuti a variazioni nella progettazione del sistema di sicurezza in riferimento alla valutazione e ai costi;
- Attuare la messa in sicurezza dei dati nel settore delle tlc (Key management e crittografia del flusso dei dati);

- Analisi per l'identificazione di questioni relative all'AIV a livello di sistemi di progettazione complessa;
- Attuare le procedure e la normative in materia di sicurezza sia a livello nazionale che internazionale.

Dovrà inoltre:

- Supportare l'interfaccia con il cliente e con i subappaltatori;
- Garantire la coerenza, identificare i punti critici e proporre le opportune azioni risolutive.

Il candidato ideale ha maturato una significativa esperienza in ambito Navigation System e in Security Activity.

Si richiede:

- Titolo di studio: Laurea Ingegneria o titolo equivalente;
- Esperienza: almeno 5 anni di esperienza nel ruolo.
- Conoscenza delle lingue: Molto buona la conoscenza della Lingua Inglese.
- Soft Skill: Attitudine al coordinamento di un team, problem solving, autonomia decisionale, risolutezza.

Chi fosse interessato, può scrivere a info@clusit.it

13. 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

Il Master in Sicurezza Informatica dell'Università di Roma "La Sapienza", diretto dal prof. Luigi V. Mancini, Vi invita a partecipare ai seguenti seminari:

Mercoledì 2 luglio 2008 alle ore 18:00

On European Program from critical infrastructures protection

Relatore: Mike Thornton (Joint Research Center, European Commission)

Mercoledì 9 luglio 2008 alle ore 18:00

"A real world approach to ICT law and corporate policies"

Relatore: Andrea Monti (Avvocato, diritto delle telecomunicazioni e delle tecnologie dell'informazione.)

I seminari si tengono nell'Aula Alfa, Dipartimento di Informatica (piano terra), Via Salaria 113, Roma. L'ingresso è gratuito ed è consentito, tramite iscrizione, fino all'esaurimento dei posti disponibili.

Coloro che fossero interessati, sono invitati a confermare la propria adesione alla segreteria del Master: mastersicurezza@di.uniroma1.it

Business Continuity, perchè il Business non vada in frantumi

Vi segnaliamo un bell'articolo del socio Anthony Cecil Wright, pubblicato su Office Automation, che trovate su

www.clusit.it/docs/0804offaut.pdf

14. EVENTI SICUREZZA

2-7 agosto 2008, Las Vegas
Black Hat Briefings & Training USA
www.blackhat.com/html/bh-usa-08/bh-us-08-main.html

8-10 agosto 2008, Las Vegas
DEFCON 16
www.defcon.org

8-11 settembre 2008, Amsterdam
SANS Process Control & SCADA Security Summit 2008
www.sans.org/euscada08_summit

16 settembre 2008, Milano
Seminario Clusit
(in fase di definizione)

16-17 settembre 2008, Rotterdam
Govcert.NL Symposium
www.govcertsymposium.com

7 ottobre 2008, Roma
Seminario Clusit
(in fase di definizione)

7-8 ottobre 2008, Milano
Insurance IT Forum 2008 - Sconto di 200 € per i soci Clusit
www.iir-italy.it/upload/general/D3945D15.pdf

7-9 ottobre, Madrid
Information Security Solutions Europe (ISSE) 2008
www.isse.eu.com

20-24 ottobre 2008, Roma
Seminario CISSP
www.clusit.it/isc2/calendario_isc2.htm

27-29 ottobre 2008, London
RSA Conference Europe 2008
www.rsaconference.com/2008/Europe/Home.aspx

22 novembre 2008, Roma
Esame CISSP
www.clusit.it/isc2/calendario_isc2.htm

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