Indice

1. NUOVI SOCI

Hanno aderito al Clusit:

- AIP Associazione Informatici Profesionisti (Perugia)
- IISFA Italian Chapter (Roma)

2. CALL FOR PAPER

Nuove idee per la sicurezza ICT

Nell'ambito del Security-Summit 2009, che si terrà a Milano dal 24 al 26 marzo, viene organizzata un'iniziativa che consenta a singoli utenti e/o organizzazioni non commerciali quali: Università, gruppi di interesse, gruppi di ricerca, di presentare nell'ambito della sicurezza informatica idee, progetti o prototipi non ancora sfruttati commercialmente.

Tutti coloro che sono interessati a cogliere questa opportunità sono invitati ad inviare a info@clusit.it un breve riassunto (3/4 pagine) del proprio progetto, che dovrà rientrare in una qualunque delle aree della sicurezza informatica con particolare riferimento a :

- Computer Forensic
- Analisi dei rischi
- Biometria
- Strumenti per la protezione dei sistemi in rete
- Nuove forme di intrusione informatica
- Programmi per la prevenzione degli attacchi
- Intrusion Detection System innovativi
- Applicazioni secure di: e-commerce, e-health, e-government, telelavoro
- Penetration testing
- Sistemi operativi sicuri

- Multimedia e Sicurezza
- Tecniche per la protezione dei contenuti in rete
- Tecniche per la protezione/violazione della Privacy
- Honeynet
- Correlazione degli eventi
- Standard di sicurezza
- Competitive Intelligence

Tutti i progetti presentati disporranno di uno spazio Poster ad essi dedicato, nel "Lab point" del Security Summit. I progetti saranno vagliati da un'apposita commissione, composta da aziende ed esperti del Clusit, che selezionerà i 5 migliori lavori, che saranno poi presentati nel corso di una Tavola Rotonda a cui sarà data ampia visibilità.

IL TERMINE ULTIMO PER L'INVIO DELLE PROPOSTE È FISSATO PER IL GIORNO 30 GENNAIO 2009. LE DECISIONI IN MERITO AI LAVORI SARANNO COMUNICATE AGLI AUTORI ENTRO IL GIORNO 10 MARZO 2009.

3. È POSSIBILE SOSTITUIRE IN ALCUNI CASI IL DPS CON UNA AUTOCERTIFICAZIONE

L'articolo 29 del decreto legge 25 giugno 2008 n. 112, convertito, con modificazioni, in legge 6 agosto 2008, n. 133 (Disposizioni urgenti per lo sviluppo economico, la semplificazione, la competitività, la stabilizzazione della finanza pubblica e la perequazione Tributaria) ha integrato l'articolo 34 del Codice in materia dei dati personali (d.lgs 196/2003) prevedendo alcune semplificazioni che riguardano il Documento Programmatico sulla Sicurezza (DPS) ed in generale l'applicazione delle misure minime di sicurezza per particolari tipologie di trattamento.

Prima della modifica, dal combinato disposto dell'art. 34 comma 1 lettera g) e del numero 19 dell'Allegato B del Codice emergeva che chiunque, senza eccezioni, trattasse dati sensibili o giudiziari mediante strumenti informatici era soggetto all'obbligo di redarre ed aggiornare il DPS.

Il d.l. 112/2008 ha invece aggiunto all'art. 34 del codice un nuovo articolo 1 bis in base al quale per "i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale" la redazione del DPS è sostituita dall'obbligo di autocertificazione del titolare del trattamento (es azienda titolare del rapporto di lavoro) di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte.

Da notarsi, che la semplificazione riguarda solo quei titolari che "trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale". L'applicazione della semplificazione, quindi, è subordinata alla verifica del rispetto dei limiti normativamente fissati.

Lo stesso articolo 1 bis prevede anche che in relazione ai trattamenti di cui sopra nonché a trattamenti comunque effettuati per correnti finalità amministrative e contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani, il Garante, sentito il Ministro per la semplificazione normativa, dovrà individuare con proprio provvedimento, da aggiornare periodicamente, modalità semplificate di applicazione del disciplinare tecnico di cui all'Allegato B) in ordine all'adozione delle misure minime di sicurezza. In attesa di conoscere il contenuto dell'atteso provvedimento del Garante (che già è intervenuto in data 19 giugno 2008 con un diverso provvedimento relativo alle "Semplificazioni di taluni adempimenti in ambito pubblico e privato rispetto a trattamenti per finalità amministrative e contabili") la modifica normativa introdotta è un evidente segnale della presa di coscienza del legislatore della necessità di semplificare gli adempimenti in materia di privacy in alcuni casi troppo gravosi per organizzazioni di piccole dimensioni.

Autore: Gabriele Faggioli

4. LE PEREGRINAZIONI DI GIGI

Il nostro Presidente è sempre più sollecitato a partecipare a gruppi di lavoro e tavoli di discussione a livello istituzionale ed il buon Gigi non si risparmia, con l'obiettivo di sensibilizzare sempre più il Governo ed il Parlamento alle tematiche che ci stanno a cuore.

Ha appena fatto un intervento, molto apprezzato, al Simposio del Govcert olandese a Rotterdham www.govcert.nl/symposium/programme.html.

Il 16 ottobre interverrà a Milano ad un evento sul tema della sicurezza della rete su invito del MIX (vedi http://blog.gigitaly.it/2008/09/vado-al-convegn.html)

La settimana successiva parlerà di sicurezza informatica al convegno dell'Internet Governance Forum in Sardegna, su invito del Ministro Brunetta (vedi http://blog.gigitaly.it/2008/09/un-invito-impor.html).

5. SCADA (Supervisory Control And Data Acquisition)

SANS Process Control & SCADA Security Summit.

È appena terminato l'appuntamento ad Amsterdam per la prima edizione europea del SANS SCADA Security Summit www.sans.org/euscada08_summit/event.php. Oltre 100 partecipanti, provenienti soprattutto dal Nord Europa (Scandinavia, Germania, UK, ecc.) ed alcuni esperti dagli USA. Il tema era quello di identificare le corrette strategie per la protezione di reti e sistemi di controllo (e SCADA) utilizzati nell'industria e nelle infrastrutture critiche.

Viene considerato definitivamente accantonato il tempo della "security by oscurity" : ormai le tecnologie utilizzate dai Sistemi SCADA sono le stesse in uso nell'IT.

Con un distinguo importante: il rischio è nettamente differente. Non sono (solo) i dati da proteggere ma anche e soprattutto l'integrità delle persone, degli impianti (le infrastrutture critiche, appunto), dell'ambiente, ecc.

Ecco quindi un nuovo significato per la sigla SCADA: Securing, Cooperation, Awareness, Disclosure, Assurance.

Con la speranza di ridurre il gap oggi esistente tra la security IT e la security dei Process Control System. Oggi stimato ancora di 10-15 anni e che si vuole portare a zero entro 5 anni!

Molti e qualificati gli interventi, illuminanti le proposte, intriganti le architetture e le strategie illustrate dagli specialisti: e l'auspicio di avere altrettanto interesse in un prossimo evento in Italia.

Autore: Enzo M. Tieghi

Se hai un problema informatico sullo SCADA, chiama l'FBI.

Su "Automation World" compare la seguente segnalazione: "Se sul tuo impianto si verifica un incidente informatico, la FBI lo vuole sapere"

www.automationworld.com/index.php?option=com_content&task=view&id=4557&Itemid=67

Nell'ambito del Security Summit 2009 www.securitysummit.it organizzeremo un convegno che tratterà di **Reti e sistemi di controllo in ambito industriale**.

È previsto anche un seminario Clusit, di taglio tecnico, su SCADA Security dal punto di vista procedurale, normativo e di best practices.

6. NEW HASH FUNCTIONS

New hash functions: ancora quattro mesi per presentare le proposte.

Come ricorderete, nel 2004/2005 ci furono rumors e poi conferme che in una universita' cinese era stato portato con successo un attacco alla caratteristica "collision-free", dell'algoritmo SHA-1.

Anche se la dimostrazione non metteva immediatamente in dubbio le applicazioni pratiche dell'algoritmo, come ad es. quella della firma digitale, a fine ottobre 2005 durante un convegno dedicato alla valutazione degli algoritmi di hash approvati dal NIST, quest'ultimo raccomandò di abbandonare lo SHA-1 in favore della famiglia SHA-2 (da 224bit a 512bit). Contemporaneamente iniziò ad organizzare una nuova "Competition", nello stile di quella organizzata per l'AES, allo scopo di sviluppare una nuova famiglia di algoritmi di hash.

La timeline, partita a giugno 2006 durante il Second Cryptographic Hash Workshop, ha tutto il 2008 come tempo disponibile per sottoporre proposte per il nuovo standard.

Distratti e ritardatari: rimangono solo quattro mesi; affrettatevi!

Tutte le informazioni sul progetto del nuovo algoritmo di hash, presso il sito del Computer Security Resource Center del NIST: http://csrc.nist.gov/groups/ST/hash/index.html

Un articolo che cerca di fare il punto, su Crypto Corner in IEEE Security & Privacy May/June 2008.

Autore: Sandro Fontana

7. PROBLEMI DI SICUREZZA IN ALCUNI FIREWALL CISCO

Anche un firewall, in ultima analisi, è un software, e può avere dei bug, in uno qualsiasi (o più) dei suoi sottosistemi.

La situazione meno desiderabile è quando questi bug vanno ad affliggere proprio i sottosistemi di sicurezza, perché ovviamente rendono l'oggetto assai poco utile, finché il problema software non sia stato debitamente corretto. Per fare un esempio, sarebbe un po' come avere una porta blindata la cui serratura abbia un sottile guasto: si apre — anche — con una chiave che si può avere in regalo in ferramenta.

Ovviamente, anche quando la patch è disponibile, il processo non è banalissimo, perché installare un qualsiasi aggiornamento su un sistema in produzione - a maggior ragione su un gateway, che è per definizione un collo di bottiglia - è problematico; anche nel migliore dei casi richiederà un'attenta pianificazione e, di conseguenza, un certo ritardo. L'esito complessivo è che questi firewall, e tutti i sistemi da essi protetti, rimangono vulnerabili per un periodo più o meno lungo. Facciamo ogni sforzo perché sia il più breve possibile.

Questa volta è successo a Cisco, che ha ovviamente messo a disposizione sul proprio sito una nota esplicativa con tutte le informazioni ed il materiale necessario.

Raccomandiamo quindi a tutti i soci di esaminare la cosa senza alcun indugio.

Autore: Mauro Cicognini

8. 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", in collaborazione con IBM, propone una giornata per discutere le ultime innovazioni per migliorare la qualità dei servizi IT da un punto di vista strategico, gestionale ed economico.

All'interno di questa giornata, si terrà la Cerimonia di consegna dei diplomi del Master di II livello in "Gestione della sicurezza informatica per l'impresa e la Pubblica Amministrazione, edizione speciale finanziata dalla Regione Lazio.

Nel pomeriggio si svolgerà il Terzo Workshop Italiano di Privacy and Security (PRISE 2008).

Informazioni e programma della giornata su http://mastersicurezza.uniroma1.it, sezione *Eventi*.

8. EVENTI SICUREZZA

4 ottobre 2008, Lanciano - CH
ICT Security Day 2008
www.ictsecurityday.it

7 ottobre 2008, Milano
Oracle Security Symposium - Gli strumenti di Sicurezza per l'Information Security Governance e il GRC
www.oracle.com/global/it/events/symposium/index.html

7 ottobre 2008, Roma
Seminario Clusit - La Sicurezza fisica: implementazioni concrete
https://edu.clusit.it/scheda_seminario.php?id=27

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

8 ottobre 2008, Roma
"Pensare Globale... Agire Locale"
www.horus.it/8ottobre.htm

8-9 ottobre 2008, Roma
Forum Expo ICT Security
www.nstecna.com/eventi/ict2008/index.php

15-18 ottobre 2008, Monte Carlo
Les Assises 08
www.lesassisesdelasecurite.com

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

27 ottobre 2008, Milano

Seminario Clusit - Gestione degli Eventi: dai log agli allarmi per la sicurezza e la compliance

https://edu.clusit.it/scheda_seminario.php?id=29

27-29 ottobre 2008, London

RSA Conference Europe 2008

www.rsaconference.com/2008/Europe/Home.aspx

29-30 ottobre 2008, Milano

Workshop ISA Server Jumpstart

www.isaserver.it/training

5 novembre 2008, Pula - CA

Seconda Giornata della Sicurezza Informatica in Sardegna

http://prag.diee.unica.it/giornatasicurezza

11 novembre 2008, Roma

Seminario Clusit - Gestione degli Eventi: dai log agli allarmi per la sicurezza e la compliance

https://edu.clusit.it/scheda_seminario.php?id=28

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