****
IT SERVICE MANAGEMENT NEWS - SETTEMBRE 2012
****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità. E' possibile dare il proprio contributo e diffonderla a chiunque.

E' disponibile il blog http://blog.cesaregallotti.it

E' possibile iscriversi o disiscriversi
- scrivendo a cesaregallotti@cesaregallotti.it
- seguendo le istruzioni riportate nella pagina http://www.cesaregallotti.it/Newsletter.html

Sulla stessa pagina è possibile consultare l'informativa sul trattamento dei dati personali.

****
Indice

****
01- Assicurazioni e sicurezza informatica

L'ENISA, il 28 giugno, ha pubblicato lo studio "Incentives and barriers of the cyber insurance market in Europe". E' possibile scaricarlo dalla pagina ufficiale (io ne ho avuto notizia dalla newsletter del Clusit):
- https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe

Lo studio è molto interessante e provo di seguito a riassumerne i punti salienti.

I rischi di sicurezza informatica rispondono alle caratteristiche dei modelli di assicurazione e, pertanto, potrebbero essere oggetto di polizze.

Nonostante ciò, il mercato delle assicurazioni per la ciber-sicurezza in Europa non è maturo. I motivi individuati sono i seguenti:
- non ci sono sufficienti dati attuariali (ma questo non ha impedito di avviare il mercato delle assicurazioni sull'inquinamento delle piattaforme petrolifere, sul danno ai satelliti, sulle controversie di lavoro);
- perdite potenziali incerte: i danni maggiori sono spesso dovuti al valore di beni intangibili (le informazioni), per i quali non sono disponibili metodi di valutazione
- difficoltà a comprendere quali rischi assicurare (attacchi criminali, attacchi terroristici, rotture di

apparecchiature, perdita di dati), a loro volta non sempre facili da distinguere in caso di incidente
- le innovazioni tecnologiche non permettono di fare previsioni basate su casi precedenti
- difficoltà a definire quale possa essere il limite superiore delle perdite da assicurare; a questo aspetto sono collegate le caratteristiche di "interdipendenza della sicurezza" (il livello di rischio non dipende solo dalle carattersitiche dell'assicurato, ma anche di altri quali partner, fornitori vari, eccetera) e di "rischi correlati" (un singolo evento può danneggiare più assicurati o essere talmente distruttivo da richiedere un risarcimento non conveniente per l'assicuratore)
- mancanza di meccanismi di ri-assicurazione, ossia della possibilità per l'assicuratore di assicurarsi a sua volta nel caso in cui riceva numerose richieste di risarcimento nello stesso momento (fatto che può capitare in occasione di certi attacchi o eventi naturali come sopra accennato)
- ridotta visibilità sull'efficacia delle misure di sicurezza (lo studio tratta anche delle certificazioni ISO/IEC 27001 e Common Criteria; io aggiungerei qualche considerazione sulla difficoltà di valutazione di un meccanismo di sicurezza);
- la percezione che i prodotti assicurativi ora disponibili sono sufficienti per i potenziali assicurati (tranne poi scoprire che non è così al momento della richiesta di risarcimento)
- il possibile "azzardo morale", per cui l'assicurato non realizza un buon livello di prevenzione perché si sente già coperto dall'assicurazione
- collegato a questa, la possibilità che l'assicurato, a fronte di un incidente, investa in campagne di comunicazione per ridurre il danno consequenziale o secondario (di immagine), non occupandosi delle cause per cui si è verificato l'incidente e lasciando quindi aperte delle vulnerabilità
- la possibile "selezione avversa", ossia il fatto che la disponibilità di informazioni per calcolare il premio è assimetrica: l'assicurato non fornisce tutti i dati a sua disposizione all'assicuratore (io aggiungo che forse neanche li ha)

Si aggiunge che il Lloyds ha dichiarato che il mercato delle ciber-assicurazioni è in crescita (ma chissà quanto questa dichiarazione ha fini pubblicitari) e potrebbe avere una spinta dal futuro Regolamento UE sulla privacy che richiede di notificare ogni violazione alle autorità preposte.

Concludo scivolando sul personale: sul rapporto ho trovato che "la sicurezza quantitativa (uno dei pezzi fondamentali per le assicurazioni) è supportata da metodi di validità non chiara, secondo alcuni studi recenti" e cita un articolo del 2009. Io lo dico almeno dal 2002 che non è possibile quantificare la sicurezza: non è difficile arrivarci, basta aver fatto almeno un'analisi dei rischi. Purtroppo, anche recentemente, ho avuto modo di incontrare qualcuno che sostiene la fattibilità delle analisi quantitative.

****

02- Legale: Garante privacy (Regole per le scuole; comunicazione delle violazioni)

Regole per le scuole

Il Garante Privacy ha pubblicato un opuscolo con le regole applicabili alle scuole.

La maggior parte sembrano regole di buon senso.

Ringrazio Daniela Quetti della DFA per la segnalazione:
- la pagina del Garante: http://www.garanteprivacy.it/garante/doc.jsp?ID=1922676

Comunicazione delle violazioni di dati personali

Riporto pari pari la segnalazione che ha fatto Daniela Quetti della DFA.

Segnalo che l'Autorità Garante per la Protezione dei dati personali ha aperto la consultazione pubblica per le Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali:
- http://www.garanteprivacy.it/garante/doc.jsp?ID=1915485

Seppur ad oggi è previsto l'obbligo di comunicazione delle violazioni per soli fornitori di servizi telefonici e di accesso a Internet, penso sia importante una lettura dato che la riforma della legislazione comunitaria prevederà probabilmente tale obbligo per tutti i titolari e certamente queste linee rappresentano l'orientamento verso cui si sta andando.

Spero che dopo la consultazione, ci saranno dei riferimenti più precisi rispetto alle variabili da considerare per decidere se una violazione è meritevole o meno di comunicazione (soprattutto considerando le sanzioni per omessa o ritardata comunicazione).

****

03- Legale: Modifiche alla normativa sul Segreto di Stato

Dal blog Over Security apprendo che è stata approvata la Legge 133 del 2012 che modifica la Legge 124 del 2007, quella sul Segreto di Stato (il titolo è "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto").

Le modifiche non mi sembrano rilevanti per le finalità delle imprese private.

E' possibile leggere il testo su www.normattiva.it.

E' anche possibile leggere il comunicato dell'AdnKronos:
- http://www.adnkronos.com/IGN/News/Politica/Servizi-segreti-Senato-approva-la-riforma-e-legge_313560499627.html

****

04- Legale: Conservazione delle registrazioni

Finalmente, causa anche mia pigrizia, ho trovato i punti normativi per cui la documentazione contabile debba essere conservata per almeno 10 anni: si tratta dell'articolo 2220 del Codice Civile che recita:
<< Le scritture devono essere conservate per dieci anni dalla data dell'ultima registrazione.
- Per lo stesso periodo devono conservarsi le fatture, le lettere e i telegrammi ricevuti e le copie delle fatture, delle lettere e dei telegrammi spediti.
- Le scritture e documenti di cui al presente articolo possono essere conservati sotto forma di registrazioni su supporti di immagini, sempre che le registrazioni corrispondano ai documenti e possano in ogni momento essere rese leggibili con mezzi messi a disposizione dal soggetto che utilizza detti supporti.>>

Questo è quanto ho trovato su http://www.studiocataldi.it/codicionline.asp.

Ho trovato questo riferimento in un dossier de Il Mondo (segnalatomi da Franco Ferrari del DNV), che riporta una comunicazione commerciale dell'azienda Faber System dal titolo "meglio conservare le e-mail". Io penso che l'articolo in questione (anche richiamato dall'articolo 22 della Legge 600 del 1973) faccia riferimento alle sole scritture contabili e non bisognerebbe esagerare. Penso anche che i documenti aziendali non dovrebbero essere conservati nelle caselle di posta, ma in altri archivi.

POST SCRIPTUM

Aggiorno questo articolo su una segnalazione che mi è arrivata che riporto di seguito.

Il Codice Civile riporta anche i seguenti articoli:
- art. 2946 "prescrizione ordinaria": salvi i casi in cui la legge dispone diversamente, i diritti si estinguono per prescrizione con il decorso di dieci anni;
- art. 2945 "Effetti e durata dell'interruzione": per effetto dell'interruzione s'inizia un nuovo periodo di prescrizione.

L'art 2945 è particolarmente insidioso; infatti sottointende che se si interrompe la conservazione (per esempio si estrae un documento per fornirlo ad un cliente) si riparte con il periodo di 10 anni.

Inoltre per le banche vale ciò che indica il Testo Unico Bancario (d. lgs n.385 del 1 settembre 1993) all'art. 119 "Comunicazioni periodiche alla clientela" che il cliente ha «diritto di ottenere, a proprie spese, entro un congruo termine e comunque non oltre novanta giorni, copia della documentazione inerente a singole operazioni poste in essere negli ultimi dieci anni.»

****

05- Legale: TAR di Puglia - se il documento non è firmato digitalmente

Se ho capito correttamente la notizia (riportata dalla newsletter DFA): l'Azienda Sanitaria Locale Barletta Andria Trani emette un bando di gara a cui è necessario rispondere attraverso una specifica procedura telematica alla quale si può accedere solo con user-id e PIN personali; il vincitore si vede successivamente escluso perché l'offerta non era firmata digitalmente. Ovviamente, l'accesso attraverso user-id e password personali può essere considerato come forma di firma elettronica, ma non equivalente alla sottoscrizione, richiesta dalla normativa vigente sulle gare.

La sentenza: http://www.giustizia-amministrativa.it/DocumentiGA/Bari/Sezione%201/2011/201100350/Provvedimenti/201201019_01.XML

Il commento: http://www.filodiritto.com/index.php?azione=visualizza&iddoc=2798

****

06- Legale: ACTA - Bocciato dalla UE

Dalla newsletter di DFA trovo la notizia sulla bocciatura da parte del Parlamento UE dell'accordo ACTA per l'anti-pirateria. Da quanto avevo letto in merito, sembra che abbiamo evitato una legge repressiva.
- http://www.bbc.co.uk/news/technology-18704192
- http://www.wired.com/threatlevel/2012/07/eu-kills-acta

Sono a favore del riconoscimento dei diritti economici di quanti creano e producono opere d'arte. Ma la normativa proposta sembrava decisamente repressiva. Inoltre, è anche opportuno chiarire quanto sia difficile, oggi, trovare e-book, film e telefilm se non si ha l'hardware specifico di Amazon, Barnes & Nobles o Apple. Per le altre piattaforme, l'offerta è notevolmente meno vasta e più dispersa; per avere un livello di offerta simile ad Amazon (che richiede di usare solo le sue piattaforme) o ad Apple (idem), bisogna rivolgersi a eMule o al circuito Torrent. E allora: che le società produttrici di intrattenimento si diano come priorità la creazione di un mercato più facile da fruire prima di prendersela con i pirati.

****

07- Legale: modifiche al Codice dell'Amministrazione Digitale

Il Decreto Semplificazioni (DL 5 del 2012, poi convertito e modificato dalla Legge 35 del 2012, ha anche modificato il Codice dell'Amministrazione Digitale.

Le modifiche hanno impatto maggiormente sui rapporti con la Pubblica Amministrazione:
- la messa a disposizione di una piattaforma di interoperabilità tra Pubblica Amministrazione e prestatori di servizi di pagamento
- l'obbligo di permettere i pagamenti alla Pubblica Amministrazione anche via bonifico
- ulteriori obblighi alla Pubblica Amministrazione ad usare gli strumenti informatici, inclusa la PEC, per le comunicazioni anche con i cittadini
- è stato chiarito meglio che la Pubblica Amministrazione è invitata ad acquisire software freeware e non solo open source
- l'obbligo per i piccoli Comuni a concentrare con altri enti i servizi IT a scopo risparmio

Maggiori dettagli sul numero 02 del 2012 di IGED:
www.omat360.it/iged-ultimo

****

08- Standardizzazione: Novità ISO/IEC 20000 (ISO/IEC 20000-3:2012 e ISO/IEC 20000-1 in italiano)

ISO/IEC 20000-1 in italiano

Questo mese, la UNI ha pubblicato la traduzione in italiano della ISO/IEC 20000-1:2011. Visto che la traduzione è di quest'anno, la norma prende il codice UNI CEI ISO/IEC 20000-1:2012 e titolo "Tecnologie informatiche - Gestione del servizio - Parte 1: Requisiti per un sistema di gestione del servizio".

Non c'è nulla da dire oltre a quanto ho già scritto in occasione dell'uscita della versione in inglese: http://blog.cesaregallotti.it/2010/12/20000-1isoiecfdis.html

Sulla traduzione italiana, dico solo che avrei usato più spesso il plurale laddove in inglese è stato usato il singolare e in italiano è stato mantenuto. In altre parole, avrei iniziato dal titolo utilizzando "Tecnologie informatiche - Gestione dei servizi - Parte 1: Requisiti per un sistema di gestione dei servizi". Mi suona buffo e inappropriato parlare di "Gestione del problema", "Gestione dell'incidente" e così via. Così come si sembra buffo e inappropriato parlare di "sicurezza dell'informazione". Ho interrogato qualche anglofono che mi ha dato ragione (dicendo che il plurale è "assumed" in queste costruzioni sintattiche).

Detto ciò, potete acquistare la norma in italiano presso l'UNI Store: http://store.uni.com/

Pubblicata la ISO/IEC 20000-3:2012

Dall'ITSM (ITIL) Professionals Group Members di LinkedIn ho avuto notizia, poi confermata dal sito ISO, che il 14 agosto è stata pubblicata la nuova versione della ISO/IEC 20000-3 "Guidance on scope definition and applicability of ISO/IEC 20000-1".

Come noto, la ISO/IEC 20000-1 può essere applicata a tutti i fornitori di servizi IT, ma non tutti possono conformarsi a tutti i suoi requisiti. Questo perché è necessario avere il pieno governo di tutti i processi descritti dalla norma e quando si utilizzano fornitori esterni non sempre è possibile.

La norma descrive quindi i criteri da utilizzare per comprendere se un'organizzazione (o parte di essa) può essere conforme a tutta la ISO/IEC 20000-1.

La norma non si limita però a questo e fornisce anche utili requisiti per condurre delle verifiche ad un sistema di gestione dei servizi IT.

Rispetto alla precedente versione del 2009, questa è stata completamente riscritta, presenta più esempi e prende in carico le esperienze accumulate in questi anni.

****

09- Tribunali e Dropbox

Mi hanno segnalato che la consegna agli avvocati delle copie dei fascicoli della Procura del Tribunale di Pisa avviene attraverso Dropbox dopo opportuna richiesta dell'avvocato stesso.

Trovate conferma al link http://www.procura.pisa.it/rilascio_digitale.aspx e poi leggendo il "Modulo di adesione al servizio di rilascio copie atti in formato digitale".

La cosa, inizialmente, mi ha lasciato perplesso. Però poi ho pensato queste cose:
- l'uso di DropBox coinvolge solo un fornitore esterno contro i due della mail (uno per mittente e uno per destinatario, senza contare i partner intermedi utilizzati per la trasmissione)
- DropBox obbliga ad avere una connessione cifrata verso il server, cosa che non sempre succede con l'email
- il Tribunale potrebbe comunque gestire le connessioni verso i propri sistemi informatici, ma non è detto che i propri sistemisti siano più affidabili di quelli di DropBox (a meno che non si soffra della sindrome di Fort Apache)
- se il Tribunale gestisse delle connessioni verso sistemi interni, difficilmente potrebbe gestire le credenziali in modo più efficiente e efficace di quanto non faccia DropBox

- DropBox soddisfa i criteri di privacy previsti dalla nostra normativa (aderisce a Safe Harbour, come mi ha segnalato Valerio Vertua, Legal & Privacy Director di CSA)

Alla fine, ho concluso che DropBox è un'ottima soluzione per la consegna di documenti tra aziende diverse, anche riservati. Potrei anche non avere considerato qualche cosa e per questo attendo contributi dai miei lettori.

Una sola cosa mi ha lasciato perplesso: se il Tribunale sta usando DropBox in modalità gratuita, cosa succederà quando avrà superato i 2 GB di capacità (i fascicoli, se poi hanno fotografie, mi immagino possano essere anche pesanti)? Viste le complesse procedure seguite dalla Pubblica Amministrazione per i pagamenti, non oso immaginarlo.

****

10- Oracle non corregge una vulnerabilità

Oracle ha deciso di non correggere una vulnerabilità al TNS listener presente nelle versioni 10g e 11g del proprio database. Gli utenti sono quindi invitati ad adottare il workaround descritto in un Security Alert.

Oracle ha detto chiaramente che la correzione costerebbe troppo:
- http://www.h-online.com/security/news/item/No-patch-for-critical-Oracle-database-vulnerability-1649106.html

Ecco le lezioni che si traggono da questa notizia:
- in ambito ITIL e ISO/IEC 20000: un ottimo esempio per spiegare le definizioni di workaround, problema, known error e soluzione di un problema
- in ambito sicurezza: un ottimo esempio del fatto che non è possibile accontentarsi dei patch e dei fix pubblicati dai produttori, ma è anche necessario leggere i bollettini, le newsletter e i security alert per vedere se ci sono dei workaround da adottare.

Ringrazio Vito Losacco che mi ha inoltrato la newsletter Minded Security Early Warning del Minded Security Research Lab su cui era riportata questa notizia.

****

11- 10 steps to cyber security: la guida del UK GCHQ

Dalla newsletter del SANS, si ha la notizia che il UK Government Communications Headquarters ha attivato il programma "Cyber security guidance for business". Nella pagina dedicata si trovano alcune guide certamente interessanti. Nulla di nuovo, ma il promotore è degno di nota:
- http://www.bis.gov.uk/policies/business-sectors/cyber-security/downloads

****

12- Guida alla sicurezza informatica personale

Dal blog Over Security ho avuto la notizia della pubblicazione di "Il giornalista Hacker. Piccola guida per un uso sicuro e consapevole della tecnologia" di Giovanni Ziccardi.

Un pdf di 36 pagine con riportati, tra gli altri, gli strumeni utili per cifrare i propri dati, navigare in modo anonimo su Internet, cancellare in modo sicuro i file.

Il link:
- blog.marsilioeditori.it/files/2012/04/Il_giornalista_hacker.pdf

****

13- Qualche tool per analizzare la sicurezza

Io seguo da diversi mesi e con interesse il blog Over Security. E' dedicato maggiormente alla tecnologia rispetto al mio, ma è spesso interessante.

Il blog segnala anche diversi strumenti per la verifica tecnologica della sicurezza. Io ho raccolto alcune segnalazioni e, pur senza averle mai testate, mi sento di elencarle:
- W3af (Web Application Attack and Audit Framework) è un web scanner dedicato alla sicurezza delle applicazioni Web; il sito ufficiale è http://sourceforge.net/projects/w3af/; sono convinto che gli sviluppatori di applicazioni web dovrebbero imparare ad usarlo oppure utilizzare altri prodotti simili (cosa che spesso non succede)
- Nessus è il più famoso strumento di analisi della rete e ora è disponibile la verisione 5; il sito è www.nessus.org
- Nmap, il famoso software di port scanning, è ora alla versione 6; il sito web è http://nmap.org/6/
- WPA tester: un simpatico strumento Android da utilizzare nel caso in cui abbiate perso la chiave della vostra wi-fi (ehm ehm ehm); mi piacerebbe averlo per pc (solo perché ogni volta che perdo la chiave della mia wi-fi non ho voglia di fare copia incolla dal cellulare al pc); il sito è https://carlomandroid.wordpress.com/download-wpa-tester/

****

14- Attack Surface Analyzer 1.0 della Microsoft

La Microsoft ha rilasciato il tool Attack Surface Analyzer. Questo è uno strumento gratuito che analizza le applicazioni e segnala se introducono vulnerabilità nei sistemi Windows.

Lodevole iniziativa che, come anche indicato dalla newsletter SANS NewsBites, ha due facce: da una parte mette a disposizione uno strumento che si spera sia adottato, dall'altra parte potrebbe avallare l'idea che la sicurezza possa essere verificata alla fine dello sviluppo (e non anche prima e durante).

Il link:
- https://blogs.msdn.com/b/sdl/archive/2012/08/02/attack-surface-analyzer-1-0-released.aspx