Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – APRILE 2014

****

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 dis-iscriversi
- 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- Prossimi appuntamenti

Il 5 giugno organizzo, come membro del Consiglio direttivo di DFA (www.perfezionisti.it), alla Statale di Milano, il DFA Open Day 2014 su questi due argomenti:
- OSINT e Investigazioni Digitali
- Security e Incident Response aziendale

Maggiori informazioni saranno date il mese prossimo. Per intento: segnatevi la data!

****

02- Standardizzazione: UNI CEI ISO/IEC 27001:2014

E' stata pubblicata la traduzione italiana della ISO/IEC 27001:2013.

Ahimè... non ce l'abbiamo fatta a pubblicarla con data 2013!

La trovate su http://store.uni.com.

****

03- Standardizzazione: Quaderno su PCI-DSS

Segnalo la pubblicazione del Quaderno Clusit "PCI-DSS: Payment Card Industry. Data Security Standard" di Fabio Guasconi.

Il quaderno è aggiornato alla versione del PCI-DSS 3.0.

Ottimo per chi vuole cominciare a conoscere questo standard:
- http://clusit.it/download/index.htm

****

04- Novità legali: Dlgs 21/2014 - Contratti a distanza e Codice del consumo

Da Altalex segnalo le modifiche al Codice del consumo per quanto riguarda i contratti a distanza introdotti dal Dlgs 21/2014 di recepimento della Direttiva Europea 2011/83/UE:
-
http://www.altalex.com/index.php?idu=264948&cmd5=021c46ab76df2fd7050bbc8c56ed7fe1&idnot=66790

In sintesi e copiando quanto riportato da Altalex, e ricordando che l'informativa precontrattuale comprende tutte le clausole da prevedere anche negli acquisti Internet, le maggiori novità sono:
- obbligo di informativa precontrattuale più gravoso rispetto al precedente e di forma scritta;
- diritto di ripensamento: il consumatore può recedere dall'acquisto entro 14 giorni ma se l'informativa è incompleta ha 12 mesi;
- restituzione del prodotto: il consumatore ha la possibilità di restituire il prodotto, anche se deteriorato.

L'articolo di Filodiritto è più esaustivo:
- http://www.filodiritto.com/contratti-tra-consumatori-e-professionisti-litalia-recepisce-la-direttiva-europea-e-modifica-il-codice-del-consumo/

****

05- Novità legali: Regolamento Agcom diritto d'autore online

Dal 31 marzo è entrato in vigore il Regolamento Agcom per la tutela del Diritto d'autore online.
- http://www.marchiebrevettiweb.it/29-diritto-di-autore/2397-entra-in-vigore-oggi-il-regolamento-per-la-tutela-del-diritto-d-autore-online.html

Esso prevede che i soggetti titolari o licenziatari di un diritto d'autore possano segnalare all'Autorità le violazioni avvenute via Internet. Per questo è a disposizione il sito:
- https://www.ddaonline.it

Notizia dal gruppo infotechlegale.it di LinkedIn.

****

06- Novità legali: Direttiva UE Network and Information Security (NIS)

Massimo Cottafavi di Security Reply mi ha segnalato questo articolo sulla Direttiva Europea "Network and Information Security (NIS)":
- http://www.networkworld.com/news/2014/031314-new-eu-cybersecurity-law-avoids-279681.html

Massimo mi fornisce già un commento che copio e incollo: "Interessante l'estensione dell'obbligo di data brech alle infrastrutture critiche anche se ancora oggi questo termine viene utilizzato in modo improprio e con un focus "parziale" rispetto a quelle che nella realtà potrebbero essere considerate infrastrutture critiche. Da vedere poi i tempi di recepimento della Direttiva a livello nazionale…".

Infatti, si intendono come strutture critiche solo quelle previste dal Dlgs 61 del 2011 (energia e trasporti); gli operatori di telecomunicazione non sono ritenuti infrastrutture critiche (nel 2014!).

****

07- Novità legali: Regole tecniche protocollo e conservazione digitale

Sono state pubblicate le nuove regole tecniche in materia di protocollo per la Pubblica Amministrazione e di conservazione sostitutiva.

Sono due provvedimenti importanti, soprattutto il secondo, applicabile anche ai privati, perché stabilisce come deve essere fatto un sistema di conservazione dei documenti informatici che assicuri l'identificazione certa del soggetto che ha formato il documento e l'integrità del documento.

Le regole si trovano sulla pagina ufficiale dell'Agid:
- http://www.agid.gov.it/notizie/protocollo-conservazione-digitale-gazzetta-le-nuove-regole-tecniche

Segnalo anche un articolo in merito su iged.it (e mi lamento con chi si è inventato il formato di lettura):
- http://issuu.com/stefanoforesti/docs/iged114_light/7?e=1523602/7213043

****

08- Novità legali: Stato Regolamento europeo privacy

Da Filodiritto segnalo questo articolo sul Regolamento in materia di protezione dei dati personali:
- www.filodiritto.com/parlamento-europeo-approvato-in-prima-lettura-il-nuovo-regolamento-in-materia-di-protezione-dei-dati-personali

In sintesi, c'eravamo quasi, ma il Parlamento è in scadenza e passerà la pratica al futuro (elezioni in Italia il 25 maggio). Ricordo che l'UK sta spingendo per posticipare il più possibile l'approvazione di questo provvedimento.

****

09- Delle definizioni di rischio

Stefano Ramacciotti mi ha segnalato le diverse definizioni di rischio nelle norme ISO e nella legislazione italiana:
- ISO Guide 73 (e anche ISO/IEC 27000): effetto dell'incertezza degli eventi. Le note poi dicono che il rischio è spesso caratterizzato da una combinazione di eventi potenziali e le loro conseguenze.
- il Dlgs 81: probabilità di raggiungimento del livello potenziale di danno nelle condizioni di impiego o di esposizione ad un determinato fattore o agente oppure alla loro combinazione;
- Direttiva Seveso III: probabilità che un determinato evento si verifichi in un dato periodo o in circostanze specifiche.

Ecco quindi il mio (nostro) punto di vista.

La ISO Guide 73 usa la definizione di rischio legata agli "effetti", ossia agli impatti. Essa è originata dalla formula "rischio = probabilità x conseguenza". Esemplificando, essa deriva dall'uso del rischio così: se mi rubano 10 penne all'anno di 1 Euro ciascuna, allora ho una perdita annua di 10 Euro all'anno; quindi il rischio relativo al furto di penne è pari a 10 euro all'anno.

La Direttiva Seveso III usa il termine rischio come sinonimo di minaccia. Così come è scritta è una sciocchezza. Che senso ha valutare la probabilità di una minaccia senza considerarne gli impatti? Si potrebbero avere minacce estremamente probabili (pioggia e neve, per esempio) i cui impatti sono risibili; i terremoti a Milano ci sono eccome, ma non hanno impatti perché la pianura li attenua.

Però la prima definizione della Treccani (www.treccani.it) è proprio "Eventualità di subire un danno" e quindi riguarda solo la minaccia. Ahinoi.

La definizione del Dlgs 81 è un poco più e pare voglia dire "probabilità che si verifichino degli eventi per cui si hanno dei danni consistenti" e già qui gli impatti si collegano ai danni. Mentre le norme ISO chiedono di stabilire l'accettabilità del rischio (e quindi, potenzialmente, dei danni complessivi annui, il Dlgs 81 chiede di stabilire il danno accettabile e poi di valutare le minacce (i rischi, in quel caso) che li potrebbero provocare.

****

10- Minacce e attacchi: Heartbleed (vulnerabilità in OpenSSL)

La minaccia oggi più discussa è chiamata Heartbleed.

In sostanza, se si usano delle versioni vulnerabili di OpenSSL si rischia un'intrusione da parte di malintenzionati:
- http://heartbleed.com/

Sarà interessante vedere quanti faranno gli aggiornamenti necessari e quanti no.

****

11- Minacce e attacchi: Rapporto Clusit 2014 e atti Security Summit

E' stato pubblicato il Rapporto Clusit 2014 sulla sicurezza informatica in Italia. Confermo che è molto interessante:
- http://clusit.it/rapportoclusit/

Sono stati anche pubblicati gli atti del Security Summit:
- https://www.securitysummit.it/milano-2014/atti/

Confesso che non ho trovato cose molto interessanti in questi atti. Ma credo sia un problema del formato "presentazione". Se però qualcuno vuole segnalare qualcosa che mi sono perso, lo faccia!

****

12- Minacce e attacchi: Full disclosure mailing list

Questa non la conoscevo, ma sembra fondamentale: una mailing list dove sono riportate le vulnerabilità dei sistemi informatici:
- http://insecure.org/news/fulldisclosure/

Notizia tratta dal SANS NewsBites.

****

13- Minacce e attacchi: Attacco a Target e uso scorretto dei controlli di sicurezza

Dal SANS NewsBites segnalo un articolo in merito all'attacco alla Target, un fornitore di servizi collegati alle carte di credito:
- http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data#p1

L'attacco alla Target è avvenuto a fine 2013 e la notizia è stata pubblicata da molte parti. Non mi dilungo, ma ricordo solo che dei malintenzionati sono riusciti a rubare 40 milioni di numeri di carte di credito.

La cosa interessante, a mio parere, è soprattutto questa: Target aveva superato l'audit PCI per gestire i dati delle carte di credito e aveva installato il prodotto FireEye (da affiancare ad un prodotto Symantec) per rilevare malware sui propri sistemi. Il prodotto FireEye era costato 1,6 milioni di dollari e ha funzionato: quando i malintenzionati avevano installato il malware sui server della Target per poi recuperare i numeri di carte di credito, FireEye ha lanciato allarmi al SOC e... nessuno ne ha fatto nulla.

Qui si sono sommate due pratiche nefaste:
- certificarsi per avere il pezzo di carta e avviare progetti solo per dare prove agli auditor (tra l'altro, allo stesso costo del miglioramento reale, perché 1,6 milioni di dollari non sono uno scherzo);
- acquistare e, forse, installare prodotti (a costo elevato) e non pensare ai processi.

Temo che, come sempre, nessuno imparerà la lezione.

****

14- Applicazione della sicurezza: Normative e procedure

Come già scritto in precedenza, ho tenuto un intervento sulle tecniche di auditing per il Corso di perfezionamento in privacy e data protection
- http://blog.cesaregallotti.it/2014/03/presentazione-audit.html

In quell'occasione spiegai che gli audit interni vanno condotti intervistando il personale e verificando le loro attività facendo riferimento alle procedure interne. Qualcuno mi ha chiesto: "ah... non sulla norma? non sul Codice Privacy e i Provvedimenti del Garante?".

La risposta è... nì.

Infatti, è mia opinione che il personale non possa essere chiamato a seguire un testo di Legge così com'è. Sia per carenza di competenze (alcuni articoli sono di difficile interpretazione anche a chi segue la materia da anni), sia perché ogni organizzazione è diversa dall'altra e l'attuazione dei requisiti normativi varia di volta in volta. Per esempio, chi deve fare il riesame delle utenze con accesso ai dati personali (gli amministratori di sistema o i responsabili dei diversi uffici)? come deve essere attuato operativamente il meccanismo di "custodia delle password"? che livello di controllo va esercitato sui fornitori? eccetera.

Quindi: il requisito normativo deve essere riportato in procedure (o istruzioni o regolamenti) a cui il personale deve attenersi.

Quindi l'audit dovrebbe essere diviso in due parti: la prima, a tavolino, per verificare se i requisiti normativi sono stati incorporati correttamente nelle procedure; la seconda, sul campo, per verificare se le procedure sono seguite dalle persone.

****

15- Applicazione della sicurezza: SCADA e Ufficio acquisti

Sul gruppo LinkedIn Italian Security Professional è stata lanciata una discussione sugli SCADA, ossia sui sistemi industriali, prendendo lo spunto dalla presentazione di Alessio L.R. Pennasilico e Cristiano Cafferata al Security Summit di Milano 2014 dal titolo " Quando il frigorifero inizia ad inviare Phishing, forse andrebbe rivalutata la strategia di security":
- https://www.securitysummit.it/milano-2014/atti/atti-20-marzo/

Ci tengo a copiare e incollare un ottimo intervento che condivido al 100% (sarà che in questo periodo sono coinvolto in un paio di attività in ambienti manifatturieri):
<<
1) Bisogna lavorare sul procurement. Gli apparati e i sistemi devono rispondere a requisiti di sicurezza. Corretto prendersela con produttori poco attenti e sensibili, ma ancor peggio c'è chi questi apparati li compra. Anni fa l'ignoranza era una buona scusa, ora non più

2) Se non si possono fare modifiche, il cliente dovrebbe valutare il costo/beneficio di passare a soluzioni più sicure, se non subito, al prossimo upgrade tecnologico. Informerei il vendor e il venditore, anche se questo potrebbe portare a poco.

Il settore dovrebbe lavorare su standard specifici, in modo da "certificare" i prodotti compliant e aiutare gli operatori nella scelta. C'è ancora MOLTA strada da fare.
>>

E una risposta a questo commento è anch'essa molto interessante (parafraso un poco):
<<
E' vero: il procurement va citato, ma se non ha delle linee guida in materia di sicurezza, beh, il "fallo" è dietro l'angolo.
>>

****

16- Applicazione della sicurezza: Password sempre necessarie?

Da una discussione sul gruppo LinkedIn "Italian Security Professional", trovo questo interessantissimo intervento di Luca Savoldi che permette di riflettere sulla necessità o meno delle password. La conclusione, mia, è ovvia: sono sempre necessarie, ma ci possono essere alcune limitate e controllate eccezioni.

<<
Dimostrazione che anche l'IT e la sicurezza IT, se non pensata per l'ambiente industriale, può essere pericolosa. La regola fondamentale e imprescindibile in ambienti SCADA è che la Security (IT) deve supportare la Safety e quindi i sistemi di Safety.

In una sala controllo di un importante raffineria si conclude l'audit di importante ente inglese che si occupa di dare la valutazione agli impianti industriali. Viene assegnato un bollone rosso perché le postazioni della sala controllo non rispettano le policy di sicurezza per le password degli account di dominio (nominale, 7 o 11 caratteri, maiuscola, numero, carattere speciale, logoff automatico).

Con quale criterio si può pensare di assegnare una simile policy ad una postazione la cui priorità è l'accessibilità in caso di emergenza?

La sala controllo ha un controllo accessi con badge nominale e riconoscimento visivo. Solo 10 persone possono entrare. L'interno è ovviamente videosorvegliato. Per cui chi è dentro ad operare è un operatore riconosciuto.

Pensate se per caso succede un'emergenza e bisogna premere il comando di apertura o chiusura di una valvola per impedire un esplosione. Bisogna intervenire in tempi rapidissimi. E se nel momento di panico l'operatore non riesce a digitare la sua password? o se sviene e deve intervenire il collega sulla sua postazione?
<<