Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS - SETTEMBRE 2013

****

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- Novità legali: Articolo sullo stato del Regolamento UE sulla privacy

Da Stefano Tagliabue di Telecom Italia: "segnalo un articolo che descrive in modo chiaro lo stato di avanzamento dei lavori per l'emissione del Regolamento UE sulla privacy. Tra i possibili scenari prospettati, c'è anche l'emissione entro aprile 2014 di una "light version" del Regolamento, che tratti solo dei principi essenziali della privacy, lasciando spazio ad ulteriori interventi legislativi dopo le elezioni europee".

Il link:
- http://www.wsgr.com/publications/PDFSearch/burton-090213.pdf

****

02- Novità legali: Privacy e spamming

Il Garante ha emesso delle "Linee guida in materia di attività promozionale e contrasto allo spam":
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2542348

Non riportano nulla di nuovo rispetto a quanto già previsto dal Codice Privacy e da altri precedenti provvedimenti, credo con l'eccezione del social spam e del marketing "virale".

Per una sintesi del Provvedimento, segnalo l'articolo di CINDI:
- http://www.cindi.it/le-linee-guida-del-garante-privacy-contro-lo-spam

****

03- Novità legali: Decreto del fare (DL 69) convertito: wi-fi, fascicolo sanitario, fax

Il DL 69 del 2013 noto come "Decreto del fare" e con titolo "Disposizioni urgenti per il rilancio dell'economia", è stato convertito in Legge con modificazioni dalla L. 98 del 2013.

E' possibile leggere la versione consolidata ricercando il DL 69 del 2013 su www.normattiva.it.

L'articolo 10 sulla liberalizzazione delle wi-fi è stato modificato e ora si può veramente dire che le wi-fi sono libere: per gli esercizi per cui l'offerta di accesso non costituisce l'attività commerciale prevalente (bar, ristoranti, hotel, scuole e altro) non sono più necessarie registrazioni e le reti non devono più essere realizzate da imprese abilitate.

Attenzione però che le reti di telecomunicazioni devono comunque rispondere ai requisiti di sicurezza degli impianti stabiliti dalla Legge 46 del 1990.

Per quanto riguarda il fascicolo sanitario elettronico, il Garante aveva espresso delle perplessità sul testo originario dell'articolo 17. Ora questo articolo è stato completamente riscritto.

L'articolo 14 presenta inoltre un'interessante novità. Esso modifica l'articolo 47 del Codice dell'Amministrazione digitale che già indicava che "le comunicazioni di documenti tra le pubbliche amministrazioni avvengono di norma mediante l'utilizzo della posta elettronica". Ora è stato aggiunto che "E' in ogni caso esclusa la trasmissione di documenti a mezzo fax". Pare un primo passo verso l'eliminazione del fax e spero che i successivi passi siano fatti quanto prima.

****

04- Novità legali: Privacy e 231 (DL 93)

Max Cottafavi di Spike Reply mi ha segnalato questo articolo dal titolo "Privacy, responsabilità da 231":
- www.ilsole24ore.com/art/norme-e-tributi/2013-08-27/privacy-responsabilita-064214.shtml

In sintesi, l'articolo 9 del DL 93 del 2013 inserisce nel Dlgs 231 del 2001 i reati di trattamento illecito di dati personali, falsità nelle dichiarazioni e notificazioni al Garante, omissione di adozione delle misure minime di sicurezza, inosservanza di provvedimenti del Garante, svolgimento di indagini sulle opinioni dei lavoratori, controllo a distanza dei lavoratori con impianti audiovisivi.

Questi reati sono penali, ossia imputabili ad una persona fisica. Ora, anche le imprese nel loro complesso possono essere oggetto di sanzioni per quegli illeciti se sono commessi nel suo interesse o vantaggio e se non era previsto un "modello organizzativo" finalizzato a contrastarli.

Ad ogni modo, questo provvedimento è un DL. Sarà opportuno aspettare a quando sarà convertito in Legge entro il 14 novembre. Per intanto mi chiedo se si hanno notizie di sentenze in merito ai reati penali stabiliti dal Codice Privacy. Potrebbero essere un ottimo punto di partenza per capire meglio gli impatti di questo DL.

La Cassazione, come enunciato dall'articolo sopra riferito, ha emesso una relazione in merito al DL 93/2013, dedicando poche righe alla questione privacy. Andrebbero lette considerando che era agosto e la privacy non era il punto più importante del provvedimento (il DL riporta altre misure molto importanti come quelle sul femminicidio): per questo non cita l'articolo 169 (quello sulla mancata adozione delle misure minime) e fa un richiamo alle "società commerciali e associazioni private", quando il Dlgs 231 ha impatto per tutti gli enti.

****

05- Novità legali: DL 93: frode e sostituzione dell'identità digitale

Il DL 93 del 2013, già citato sopra, tratta anche di stalking, frode informatica e sostituzione dell'identità digitale. Il problema, per quest'ultimo punto, è che non vi è una definizione certa di "identità digitale". Per alcuni si tratta di un concetto molto esteso e comprende l'insieme di informazioni relative a un soggetto presenti on line, per altri si può ridurre alle credenziali di accesso ad un sistema informatico.

Di tutto questo tratta un interessante articolo su CINDI:
- http://www.cindi.it/la-frode-informatica-aggravata-dalla-sostituzione-dellidentita-digitale/

Ricordo però che il DL 93 è, appunto, un Decreto Legge. Pertanto, è opportuno attendere la sua conversione in Legge (con modifiche) per vedere quale sarà il testo finale.

****

06- Standardizzazione: SPICE (modelli di maturità) e ISO/IEC 27001

L'SC 7 del JTC 1 dell'ISO/IEC sta lavorando su una nuova edizione dello standard ISO/IC 15504 noto anche come SPICE. Per essere molto sintetici, lo SPICE è quello standard che tratta della capacità e della maturità dei processi e delle modalità per dimostrarle e valutarle. La nuova edizione prevede anche una riorganizzazione e rinumerazione degli standard da 33001 (in particolare, la ISO/IEC 33001 presenterà un'introduzione e la terminologia, la 33002 i requisiti per effettuare un assessement dei processi, eccetera).

Di particolare importanza sono i "process reference model (PRM)" e i "process assessment model (PAM)", documenti che descrivono i processi in modo da poterli analizzare e valutare secondo quanto previsto dallo standard.

Due delle norme della serie ISO/IEC 330xx, attualmente in bozza, hanno l'ambizione di presentare un esempio di PRM e un esempio di PAM per la gestione della sicurezza delle informazioni in relazione con la ISO/IEC 27001.

L'iniziativa raccoglierà certamente il favore di quanti vorrebbero introdurre i modelli di capacità anche nella sicurezza delle informazioni. Io devo confessare che l'iniziativa mi lascia perplesso soprattutto perché si è appena finito di scrivere la futura ISO/IEC 27001 dopo molte discussioni e immediatamente ne viene presentata una sorta di interpretazione che, potenzialmente, potrà introdurre delle confusioni (per fare un esempio banale, nei requisiti del risk assessment della ISO/IEC 27001 non si parlerà più di

"asset" per evitare di imporre un modello di risk assessment basato sugli asset; per motivi di ordinamento alfabetico, però, il processo di "asset management" è proprio il primo presentato nella bozza di PAM ridando, seppure involontariamente, un'impropria importanza agli asset stessi).

Da un altro punto di vista, l'iniziativa presenta elementi interessanti. Uno dei primi riguarda l'Annex A della ISO/IEC 27001 da sempre oggetto di critiche e discussioni. Infatti, mentre la ISO 9001 e la ISO 14001, per esempio, riportano i requisiti dei processi di gestione della qualità e dell'ambiente nel corpo del testo dello standard, la ISO/IEC 27001 riporta processi importantissimi come la gestione degli incidenti in un allegato, conferendogli così un diverso livello di interpretazione. Le proposte di PRM e PAM, per contro, evidenziano questi processi allo stesso livello degli altri e comportano un'altra visione dei requisiti.

Tutto questo richiederebbe una riflessione, anche sul futuro della ISO/IEC 27001, sicuramente interessante. Ritengo però, come ricordato inizialmente, sia necessario aspettare qualche tempo, quando la nuova versione della ISO/IEC 27001 sarà stata adottata e oggetto di ampia discussione.

****

07- Standardizzazione: Pubblicata la ISO/IEC TR 27019 per l'energy utility industry

Franco Ferrari del DNV Italia mi ha segnalato che il 15 luglio è stata pubblicata la ISO/IEC TR 27019 dal titolo " Information security managemen guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry".

Si tratta di una estensione della 27002 con controlli specifici per chi offre servizi di energia. Come specificato dalla 27019 stessa, essa è il recepimento della norma tedesca DIN SPEC 27009:2012-04.

****

08- ENISA Annual Incident Reports 2012

Dal gruppo LinkedIn "Italian Security Professional" ricevo la notizia dell pubblicazione, il 20 agosto, del "Annual Incident Reports 2012" dell'ENISA:
- https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012.

Per me, la parte più interessante riguarda l'analisi delle cause degli incidenti: il 76% degli incidenti sono causati da "errori dei sistemi"; in questa categoria, se ho capito correttamente anche le tabelle successive, sono inclusi anche gli errori software, il sovraccarico delle risorse, eccetera. Io sommerei questo 76% agli "errori umani" (5%), per avere questo risultato: il 81% degli incidenti è stato determinato da errori umani (si dovrebbe anche cercare di ragionare sul 13% degli incidenti determinati da "errori di terze parti", ma i dati non sono sufficienti).

Le conclusioni sono facili da tirare: quando si parla di sicurezza è necessario riflettere attentamente sulle persone, sulla loro formazione e competenza (di cui ho già parlato in precedenza), sugli strumenti loro messi a disposizione e sui processi che devono seguire.

****

09- Notizie: NSA vuole tagliare il 90% degli AdS

Dopo il caso Snowden, l'NSA ha deciso di tagliare il 90% dei propri amministratori di sistema (AdS). Gli attuali AdS, pare, sono in gran parte fornitori (Snowden incluso) e non interni.

A questo punto mi faccio delle domande, per le quali non ho risposte definitive:
- dei sistemi automatizzati sono realmente più sicuri rispetto a quelli manuali? Certamente sono più efficienti e probabilmente più efficaci, ma non è detto che siano anche più sicuri.
- è una buona iniziativa dire al 90% del proprio personale che sarà licenziato il prima possibile?
- il personale interno è veramente più affidabile di quello esterno?

Due articoli segnalati da SANS Newsbyte:
- http://www.nbcnews.com/technology/nsa-cut-system-administrators-90-percent-limit-data-access-6C10884390
- http://www.theregister.co.uk/2013/08/09/snowden_nsa_to_sack_90_per_cent_sysadmins_keith_alexander/

****

10- Notizie: TOR, Lavabit e Silent Circle

Questa estate l'FBI ha arrestato un tizio che diffondeva materiale pedopornografico attraverso la rete TOR:
- http://www.tomshw.it/cont/news/tor-non-e-piu-blindata-l-fbi-si-infiltra-e-arresta-un-pedofilo/48227/1.html

TOR, come è noto, è un sistema per la navigazione web e l'uso di servizi Internet in modo anonimo. Come riassunto dall'articolo sopra citato, può essere usato per scopi legittimi, ma anche per scopi illegittimi.

La cosa interessante, come mi hanno spiegato e come riporta l'articolo, è che l'FBI ha sfruttato un bug del browser non aggiornato. Insomma: il solito patch non fatto.

Altra notizia (dal Clusit Group di LinkedIn) riguarda i servizi di e-mail "sicura" Lavabit e Silent Circle:
- http://www.technologyreview.com/news/518056/why-e-mail-cant-be-completely-private/

Onestamente, non conosco per nulla questi servizi e mi sfugge quale livello di sicurezza garantiscono (forse riescono a mantenere anonimi anche i mittenti e destinatari). Essi sono stati chiusi su iniziativa dei loro stessi promotori per evitare di dover consentire l'accesso alle forze dell'ordine USA, in modo analogo a quanti hanno aderito al progtto PRISM.

Credo che il titolo dell'articolo dica tutto: l'e-mail non può essere completamente riservata. Detto in parole più popolari: l'unico modo di mantenere un segreto è non dirlo a nessuno (figuriamoci comunicarlo via e-mail!).

****

11- Attacchi e minacce: Automobili e sicurezza informatica

Oggi le automobili si basano sempre più su dispositivi informatici per il loro funzionamento. Ovviamente, alcuni hacker si sono dedicati alla ricerca di vulnerabilità e ne hanno trovate.

L'articolo in inglese (segnalato dal Gruppo LinkedIn del Clusit):
- http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/.

Una traduzione in italiano (segnalato dal Gruppo LinkedIn del Clusit):
- http://punto-informatico.it/3860499/PI/News/hacker-dell-automotive.aspx.

Ulteriori vulnerabilità sono state individuate nei meccanismi di sicurezza del sistema di avviamento e un giudice ha imposto una censura alla pubblicazione della ricerca che le descriveva (dalla newsletter SANS NewsByte):
- http://arstechnica.com/tech-policy/2013/07/high-court-bans-publication-of-car-hacking-paper/.

In tutti questi casi mi faccio due domande.
- voglio avere il diritto di conoscere i dettagli delle vulnerabilità (con la conseguenza che siano note anche a malintenzionati) oppure di non vederle pubblicate, ma corrette?
- queste ricerche di vulnerabilità sono classificabili come "ricerche scientifiche", così come i loro autori le classificano?

****

12- Attacchi e minacce: Violati i social network di Alpitour

Le pagine Facebook del gruppo Alpitour sono state prese in possesso da malintenzionati (probabilmente dopo un attacco di phishing) che hanno postato dei link a siti malevoli:
- http://www.pierotaglia.net/facebook-fai-da-te-alpitour-ahi-ahi-ahi-pagine-facebook-hackerate

A questo proposito, è necessario riflettere sulla gestione dei social media da parte delle imprese.

Una prima riflessione è di Piero Tagliapietra, autore anche del post precedente, che elenca le modalità di attacco e alcune contromisure (la consapevolezza sembra essere quasi l'unica):
- http://www.pierotaglia.net/social-media-ransomware-concept/

Una seconda riflessione è di Andrea Zapparoli Manzoni, che ha segnalato la notizia su Alpitour sul Gruppo Clusit di LinkedIn. Anche in questo caso, dopo una descrizione dello stato della sicurezza dei social media, sono elencate delle contromisure, le cui più importanti sono quelle organizzative e di consapevolezza:
- http://www.slideshare.net/idialoghi/i-dialoghi-social-business-security-social-media-week-2011

****

13- Misure di sicurezza: Firewall: configurarli con Drop o Reject?

Questo articolo sulla configurazione dei firewall è interessante:
- http://www.achab.it/blog/index.cfm/2013/9/drop-vs-reject-qual--la-differenza.htm

Mi rendo conto che si tratta di un articolo base, ma smonta il principio secondo cui un firewall debba essere configurato per non fornire risposte al mittente di un pacchetto quando questo è bloccato. In altre parole, l'articolo consiglia di impostare il firewall con regole di "Reject" (per fornire risposte) e non con regole di "Drop".

Mi ha fatto anche piacere leggere un articolo tecnico in italiano che non dice sempre le stesse cose.

_____

Cesare Gallotti
Ripa Ticinese 75
20143 Milano (Italia)
Tel: +39.02.58.10.04.21
Mobile: +39.349.669.77.23
Web: http://www.cesaregallotti.it
Blog: http://blog.cesaregallotti.it
Mail: cesaregallotti@cesaregallotti.it
PEC: cesaregallotti@mailcert.it