Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – NOVEMBRE 2016
****

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- Standard: Stato delle norme della famiglia ISO/IEC 27000

Il 27 ottobre si è concluso ad Abu Dhabi il 53o meeting dell'ISO/IEC JTC 1 SC 27, il cui WG 1 si occupa delle norme della serie ISO/IEC 27000. Io ho partecipato in qualità di delegato italiano (in tutto la delegazione italiana era composta da 4 persone). I delegati erano in tutto 110 da 29 Paesi.

La buona notizia è che abbiamo finito i lavori sulla ISO/IEC 27003, ossia la guida all'interpretazione della ISO/IEC 27001:2013. Alcuni sperano sarà pubblicata entro fine 2016, io penso che lo sarà per inizio 2017. Questa norma è importante perché ci ha permesso di consolidare alcune decisioni prese per la ISO/IEC 27001. Certamente questa norma risulta pubblicata in ritardo, ben 3 anni dopo la ISO/IEC 27001, però era necessaria.

Sono partiti i lavori per la nuova ISO/IEC 27002, con una prima fase che consiste nell'elaborazione di una "design specification" (utile per evitare successivi ritardi). Nella migliore delle ipotesi uscirà tra 4 anni. Gli

esperti hanno deciso di modificare la norma esistente per includere gli aggiornamenti tecnici necessari e per migliorare il testo già esistente (chiunque l'abbia letto con attenzione ha notato ripetizioni, eccessivi approfondimenti in qualche punto, eccessiva sintesi in altri).

Sono ripartiti, dalla fase di design specification, i lavori per la ISO/IEC 27005 sulla valutazione del rischio. Negli ultimi 4 anni gli esperti non hanno trovato un accordo per la modifica di questa norma e quindi si ripartirà da capo, con una nuova impostazione. Come ho già scritto in passato, molti sono d'accordo sulla direzione da prendere (ossia superare la metodologia asset-minacce-vulnerabilità basata sui "censimenti"), ma non hanno trovato il modo per affrontarla. La mia opinione è che in troppi vogliono promuovere la propria idea senza riuscire ad arrivare ad una sintesi di tutte.

Il problema dietro la ISO/IEC 27005 è che la ISO/IEC 27001 promuove l'uso di metodologie meno dettagliate, mentre la ISO/IEC 27005 (che dovrebbe essere una guida all'attuzione della ISO/IEC 27001) promuove invece l'approccio opposto. Anzi, proprio per questo motivo alcuni partecipanti hanno rilevati dei "difetti" nella attuale ISO/IEC 27005 che la mette in conflitto con la ISO/IEC 27001. Francamente, non so cosa pensare e cercherò di capire come questa questione sarà risolta.

Sono partiti o continuati i lavori per altre norme, tra cui la revisione delle ISO/IEC 27007, 27008, 27014, 27017 e 27019, la nuova ISO/IEC 27021, la pubblicazione di linee guida sulla "cyber resilience" (sarà quindi un business continuity per l'IT) e la "cyber insurance" (questa è in uno stadio successivo alla design specification ed è stata avviata la pratica per un "new item proposal"). La ISO/IEC 27015 sarà eliminata.

Infine, si vuole inaugurare una serie ISO/IEC 27100 sulla cyber security. Io continuo a vedere indecisione su cosa voglia dire "cyber security" (in realtà, nessuno vuole dirlo; si parla in pratica solo di IoT e tutti i lavori che ho visto sinora, incluso quello del NIST, parlano di sicurezza IT aziendale). Vedremo.

****

02- NIST: Sicurezza per le piccole imprese

Fabio Teoldi mi ha segnalato la nuova edizione della pubblicazione del NIST "NISTIR 7621 - Small Business Information Security: The Fundamentals". Si trova in questa pagina:
- http://csrc.nist.gov/publications/PubsNISTIRs.html

Mi piace e non solo perché il titolo non riporta "cyber", ma "information".

Potremo discutere lungamente dei controlli inclusi ed esclusi, ma mi sembra un'iniziativa importante, oltre che ben fatta.

****

03- OWASP Application Security Verification Standard

È disponibile la versione 3.0.1 della OWASP Application Security Verification Standard (ASVS): https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project.

Mi sembra una interessante check list per 3 livelli diversi di criticità delle applicazioni. La check list può essere vista "al contrario" ed essere usata non solo per le verifiche, ma anche per gestire i progetti.

Questa mi è stata segnalata da Daniel Halber di HID Global e lo ringrazio.

****

04- Attacchi: Riscaldamento in Finlandia bloccato

Questa notizia l'ho letta sul SANS NewsBites: degli appartamenti in Finlandia sono rimasti senza acqua calda per una settimana perché il sistema di riscaldamendo è stato oggetto di attacco DDOS: http://www.theregister.co.uk/2016/11/09/finns_chilling_as_ddos_knocks_out_building_control_system/.

La cosa può far sorridere (Brian Honan, sul SANS NewsBites, commenta: "This brings a whole new definition to a cyber cold war").

Però ci sono lezioni da imparare:
- il sistema, fosse stato progettato correttamente, non doveva bloccarsi in assenza di attacco da Internet (classico caso per cui una funzionalità migliorativa diventa più importante delle funzionalità di base);
- chi ha progettato il sistema non aveva previsto un firewall di controllo accessi da Internet.

****

05- Attacchi: DDoS con l'IoT

Venerdì 21 ottobre, Internet ha avuto dei problemi. In particolare, molti servizi popolari (inclusi Twitter e Netflix) sono risultati inaccessibili.

Il tutto è successo perché Dyn, un DNS centrale di Internet, è stato oggetto di un attacco DDoS. Fin qui nulla di nuovo, se non l'ulteriore consapevolezza di quanto sia fragile l'infrastruttura informatica su cui oggi basiamo la nostra vita. La novità è che il DDoS è stato scatenato usando i "dispositivi di casa", ossia gli oggetti che compongono l'IoT e che troppi considerano come inoffensivi, le volte che sono consapevoli della loro esistenza.

Due articoli (in italiano e in inglese) che riassumono gli eventi:
- http://www.ilpost.it/2016/10/24/attacco-informatico-venerdi-21-ottobre-mirai-dyn/;
- https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/.

Un ulteriore articolo: http://www.darkreading.com/vulnerabilities---threats/root-and-the-new-age-of-iot-based-ddos-attacks-/d/d-id/1327281.

Commento finale: i dispositivi IoT sono quasi tutti sviluppati e mantenuti senza alcuna considerazione per la sicurezza. Dubito saranno mai disponibili delle patches per tutti i dispositivi vulnerabili al malware Mirai, quello usato per infettare i dispositivi e poi lanciare l'attacco a Dyn.

****

06- Privacy: Videoriprese ai lavoratori che commettono reato

Il caso in breve: dei dipendenti timbravano l'entrata e uscita dal lavoro in orari diversi da quelli reali. Il datore di lavoro ha quindi verificato con delle telecamere e la Cassazione ha approvato il metodo:
- http://www.filodiritto.com/news/2016/videoriprese-cassazione-penale-consentito-al-datore-di-lavoro-riprendere-i-lavoratori-che-commettono-reato.html.

Ecco la ragione: "le garanzie procedurali regolate dall'articolo 4 dello Statuto dei Lavoratori non si applicano qualora il controllo di videoriprese sia effettuato al fine di accertare la commissione di reati: nel caso specifico, il delitto di truffa".

Purtroppo l'articolo non dice se e come era fornita informativa sulle videoriprese.

****

07- Privacy: PIA e valutazione del rischio

Sulla newsletter di ottobre 2016 del European data protection supervisor (EDPS) si trova un articolo dal titolo "ISRM and DPIAs: what they are and how they differ". L'articolo si trova a pagina 4 del pdf: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Newsletters/Newsletter_49_EN.pdf.

Secondo l'EDPS, la valutazione del rischio relativo alla sicurezza delle informazioni (ISRM), riguarda solo i rischi di sicurezza, mentre il privacy impact assessment (PIA) è più ampio e include anche i casi in cui potrebbero essere violati i diritti degli interessati.

Il ragionamento, però, non mi convince: quando il Regolamento richiama i rischi, essi riguardano principalmente i trattamenti e i diritti degli interessati. Quindi: quando si parla di rischi in ambito privacy, io non vedo differenza tra ISRM e PIA.

Per i più attenti: il "risk assessment" è una parte del "risk management" e, a rigore, non ha senso paragonare un meccanismo gestionale (ISRM) con uno di valutazione (PIA), ma credo che sia stato fatto un errore terminologico e con ISRM intendano ISRA (information security risk assessment).

L'ISRM è richiesto dal Regolamento Europeo 45/2001, applicabile a istituzioni e organismi comunitari (mentre il recente GDPR, ossia il Regolamento 169/2016, riguarda tutte le entità).

L'EDPS ha anche pubblicato a marzo (quindi i riferimenti normativi non sono corretti, visto che il GDPR è stato pubblicato a maggio) una linea guida gli ISRM. Essa è in realtà un riassunto della ISO/IEC 27005: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/16-03-21_Guidance_ISRM_EN.pdf.

Grazie a Pierfrancesco Maistrello per alcuni consigli e precisazioni su questo post.

****

08- Legale: Normativa e-commerce

Segnalo questi 4 articoli proposti da Altalex sul commercio elettronico e in particolare sul D. Lgs. 70 del 2003. Mi sembra una buona occasione per ripassare.

1- E-commerce B2C: vendere online tra rispetto della normativa e attenzione al cliente:
- http://www.altalex.com/documents/news/2016/04/06/e-commerce-b2cvendere-online-tra-rispetto-della-normativa-e-attenzione-per-il-cliente;
2- Se il consumatore cambia idea: il diritto di recesso nell'e-commerce di prodotti:
- www.altalex.com/documents/news/2016/07/06/e-commerce-e-diritto-di-recesso;
3- Le controversie online: le ADR del commercio elettronico:
- www.altalex.com/documents/news/2016/06/30/controversie-online-adr-commercio-elettronico;
4- Vendita online dei beni alimentari: requisiti, adempimenti e peculiarità:
- www.altalex.com/documents/news/2016/10/21/vendita-online-dei-beni-alimentari.

****

09- Dati e sanità

Pasquale Tarallo mi ha segnalato questa sua presentazione relativa ai dati in ambiente sanitario:
- http://www.slideshare.net/tarallop/healthcare-data-management-67790102.

Mi racconta, tra l'altro, che è rimasto molto colpito dalla scarsa attenzione alla privacy nelle strutture sanitarie. E ha ragione (ci sono passato anche io di recente, anche se per cose decisamente modeste).

****

10- IT Audit & Cloud

Segnalo la pubblicazione "IT Audit & Cloud" di AIEA:
- http://www.aiea.it/attivita/gruppi-di-ricerca/it-audit-cloud.

Presenta una bella carrellata dei rischi da considerare quando si usano servizi cloud, delle condizioni contrattuali da prevedere e di altre misure pertinenti. Non tratta dettagli tecnici ed è molto breve. Una lettura interessante, insomma.

****

11- CISPE: codice per i fornitori cloud

Enrico Toso di DB Consorzio, che ringrazio, mi ha segnalato questa iniziativa: un codice di condotta per i fornitori di servizi cloud, promosso da Cispe, una coalizione di cloud provider.

L'articolo di partenza:
- http://www.adnkronos.com/soldi/economia/2016/10/02/sicurezza-trasparenza-nel-cloud-nasce-primo-codice-condotta-europeo_yIuOK4YMWtlIkIRgWd2a0L.html.

Il sito del CISPE da cui scaricare il documento: https://cispe.net/.

I miei commenti (posto che il documento mi sembra ben fatto):
- attualmente è disponibile un documento in bozza e questo è un peccato;
- chissà se tra le molte iniziative sul cloud (incluse quelle promosse da CSA, ma non solo), questa avrà una buona rilevanza.