Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS –APRILE 2019

****

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

IT Service Management News di Cesare Gallotti è rilasciata sotto licenza Creative Commons Attribution 4.0 International License (creativecommons.org/licenses/by/4.0/deed.en_GB).
Bisogna attribuire il lavoro a Cesare Gallotti con link a http://www.cesaregallotti.it/Newsletter.html.

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

La newsletter è inviata via MailUp, offerta da Team Quality S.r.l.

Per iscriversi, cancellarsi e leggere l'informativa privacy:
http://www.cesaregallotti.it/Newsletter.html.

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

****

Indice

****

01- 15 aprile 1999-2019: 20 di consulenza in sicurezza delle informazioni

Il 15 aprile 1999 iniziai a lavorare come consulente di sicurezza delle informazioni.

Più che altro, entrai negli uffici di Securteam di Milano e mi diedero da studiare ITSEC e la metodologia aziendale Defender (dopo pranzo ebbi anche un abbiocco!).

Erano altri tempi: la BS 7799 (oggi ISO/IEC 27001) era roba per pochi, il DPR 318 non era ancora stato pubblicato, la prima certificazione italiana in materia di sicurezza delle informazioni non era stata neanche pensata e si pensava che "sicurezza delle informazioni" fosse un'espressione più significativa di "sicurezza informatica" (e non si parlava proprio di "cyber-security"). Per contro c'era già chi parlava di "visione olistica della sicurezza" e "sicurezza a 360 gradi".

Fui assunto da Securteam grazie all'apprezzamento che ebbi da Giulio Carducci dopo il colloquio fissato grazie all'invio del mio CV "a pioggia" (in cui dicevo che non sapevo quasi nulla di sicurezza delle informazioni, ma avevo fatto la tesi su crittorafia e crittanalisi). E poi negli uffici di Securteam trovai Maurizio (il responsabile dell'ufficio di Milano), Andrea, Laura, Donatella e Nino. Li anonimizzo perché è da tanto che non li sento, anche se sento che un filo di amicizia "silenziosa" ci leghi ancora tutti.

A loro va tutto il mio affetto e la mia stima e i miei ringraziamenti. Mi insegnarono a lavorare nel rispetto dei clienti, a studiare come un pazzo per svolgere al meglio il mio lavoro, a confrontarmi con i colleghi e a divertirmi a fare consulenza. Mi insegnarono anche che quella era la mia strada: loro lo avevano capito, mentre io nutrivo ancora dubbi.

****

02- Stato delle norme ISO/IEC 27xxx - Aprile 2019

La prima settimana di aprile 2019 a Tel Aviv (Israele) si è concluso l'incontro semestrale del ISO/IEC JTC 1 SC 27, ossia del comitato che si occupa della redazione delle norme della serie ISO/IEC 27000.

Al WG 1 (quello che si occupa della ISO/IEC 27001 e delle norme ad essa collegati) i registrati erano 143; al WG 5 (quello che si occupa di norme relative alla privacy) i registrati erano 139. La delegazione italiana era composta da ben 4 persone distribuite tra i WG 1, 4 e 5 (ringrazio quindi Fabio Guasconi, Alessandro Cosenza e *dato anonimizzato* per avermi aiutato anche con questa mia relazione).

Durante questo meeting, molte norme erano o in stato troppo avanzato o in stato troppo arretrato e quindi le discussioni erano relative o ai dettagli editoriali o all'impostazione del documento. In generale, quindi, poco interessanti.

Come sempre, segnalo le cose a mio parere più interessanti. Infatti i temi sono stati molto numerosi.

Per quanto riguarda le norme legate alla ISO/IEC 27001:
- la ISO/IEC 27001 per il momento non si tocca, ma nel prossimo futuro sarà aggiornata per essere pubblicata intorno al 2021 per includere la nuova lista dei controlli, per recepire le nuove richieste editoriali per tutti gli standard (p.e. la richiesta di avere termini e definizioni all'interno dello stesso documento, mentre oggi sono nella ISO/IEC 27000) e per discutere dell'utilità della Dichiarazione di applicabilità;
- per la ISO/IEC 27002, la discussione ha riguardato soprattutto quali controlli includere, quali eliminare e quali unire; si spera di affrontare discussioni più tecniche dal prossimo meeting;

- la ISO/IEC 27005 è ritornata al via e quindi la discussione ha riguardato l'impostazione; su questa norma, segnalo che il BSI ha pubblicato un suo aggiornamento; per quanto sono riuscito a leggere sembra interessante;
- per la ISO/IEC 27006, si sono affrontate alcune correzioni per la sua futura versione; purtroppo non ho seguito i lavori precedenti e, quindi, non ho contribuito come avrei voluto;
- per la ISO/IEC 27013, si è discusso della necessità di avviare il lavoro, visto che il gruppo che si occupa della ISO/IEC 20000 sta già pubblicando una norma simile (ISO/IEC 20000-7, che include anche riferimenti alla ISO 9001.

Il WG 1 si occupa anche di norme che richiamano più direttamente la cyber-security. In particolare, la ISO/IEC 27102 (sulle cyber-insurance) sarà promossa in "bozza finale" e quindi sarà pubblicata, dopo un ulteriore giro di controllo editoriale, a cavallo del 2019-2020.

Il WG 4 ha discusso di argomenti su cui pubblicare standard (al momento i lavori sono però molto indietro):
- IoT e domotica (in particolare la ISO/IEC 27030, linea guida su rischi, principi e controlli per la sicurezza e la privacy di IoT; attualmente al terzo working draft); per tutti i lavori IoT c'è una forte sinergia con l'SC 41;
- modello per i sistemi industriali.

Per quanto riguarda le norme legate alla privacy, segnalo che si sono conclusi i lavori sulla ISO/IEC 27552 (la norma per certificare i "sistemi di gestione per la privacy") e sarà pubblicata, probabilmente, entro giugno. Però manca una norma di supporto alla certificazione. Un'idea sarebbe quella di estendere la ISO/IEC 27006 (che a sua volta è un'estensione della ISO/IEC 17021 per la ISO/IEC 27001); per discutere compiutamente dell'argomento, si è avviata una richiesta di contributi che si concluderà tra 6 mesi (su questo penso che per il momento si potrebbe usare la ISO/IEC 17021; inoltre segnalo che al momento non è previsto l'uso della ISO/IEC 17065, come richiesto dal GDPR e pertanto bisognerà valutare la questione (in questi mesi cercherò di capire meglio come funziona la certificazione dei prodotti)).

Altri lavori di interesse per quanto riguarda la privacy:
- proseguiti i lavori sulla ISO/IEC 29184 sull'informativa e il consenso online;
- proseguiti i lavori anche su ISO/IEC 27045 dal titolo "Big data security and privacy – Processes" (per definire modelli di riferimento, valutazione e maturità del processo per il dominio della sicurezza e della privacy dei big data); altre norme legate ai big data sono le ISO/IEC 20546 e 20547.

Infine, importantissimo e sempre relativamente alla privacy, è con orgoglio che segnalo che un membro della delegazione italiana (quello anonimo!) è editor della norma ISO/IEC 27555, sulla cancellazione dei dati personali.

Il prossimo meeting sarà a ottobre a Parigi.

****

03- Sulla sicurezza e sulla selezione del personale

Segnalo questo mio articolo dal titolo "Sicurezza e selezione del personale":
- https://www.ictsecuritymagazine.com/articoli/sicurezza-e-selezione-del-personale/.

Si tratta di un argomento che mi dà molto da pensare, dai punti di vista etico e tecnico (i limiti imposti dal GDPR, la relazione tra comportamenti passati e quelli futuri). Sicuramente alcuni non concorderanno con alcune mie posizioni; nel caso, sono aperto a ricevere controdeduzioni.

Parte delle riflessioni sono scaturite da questo articolo di Altalex dal titolo "Rapporto di lavoro: incidenza dei comportamenti extralavorativi riprovevoli, anche anteriori":
- https://www.altalex.com/documents/news/2019/03/18/rapporto-di-lavoro-incidenza-dei-comportamenti-extralavorativi-riprovevoli-anche-anteriori.

****

04- Approvato il EU Cybersecurity Act

Alessandro Cosenza di BTicino mi ha segnalato che il 9 aprile, il Consiglio UE ha approvato definitivamente il Cyber security Act. La pagina ufficiale del Consiglio con l'atto:
- https://www.consilium.europa.eu/it/press/press-releases/2019/04/09/legislative-acts-adopted-by-the-general-affairs-council/

Dalla pagina è possibile scaricare il testo definitivo e accedere al comunicato stampa (di dicembre, ma evidentemente ancora valido):
- https://www.consilium.europa.eu/it/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/.

Nei prossimi giorni sarà pubblicato in Gazzetta Europea. Ricordo che si tratta di un Regolamento e pertanto non deve essere recepito dai singoli Stati membri.

Ora credo che il punto più importante da guardare per il futuro riguarderà gli schemi di certificazione che saranno promossi, senza sottovalutare le attività di miglioramento della sicurezza promosse da ENISA.
****

05- Convenzione tra Garante privacy e Accredia (nulla di nuovo)

Il 20 marzo 2019, Garante privacy e Accredia hanno firmato un accordo di collaborazione:
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9099558.

Se leggo correttamente, non avvia alcun schema di certificazione come previsto dal GDPR. Mette solo le basi affinché questo possa accadere in futuro. Infatti non sono stati ancora approvati schemi di certificazione a livello nazionale e dinanzi al Comitato Europeo per la Protezione dei Dati.

****

06- Sulle valutazioni del rischio oggettive (e quantitative)

In questi pochi mesi sto assistendo ad un ritorno dell'idea delle valutazioni del rischio quantitative e su quelle oggettive.

Pierfrancesco Maistrello mi ha ricordato, tra le altre cose, che c'è un Provvedimento del Garante sul data breach:
- https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9076378.

In un paragrafo, c'è scritto: "VISTI i considerando nn. 75 e 76 del Regolamento che suggeriscono che, di norma, nella valutazione dei rischi si dovrebbero prendere in considerazione tanto la probabilità quanto la gravità dei rischi per i diritti e le libertà degli interessati e che tali rischi dovrebbe essere determinati in base a una valutazione oggettiva".

Io e Pierfrancesco siamo d'accordo nel dire che si possono anche seguire approcci qualitativi (con valori semplici come "alto", "medio" e "basso"), ma i valori assegnati vanno giustificati, dimostrando così l'oggettività della valutazione. Sempre Pierfrancesco mi ricorda che un'ulteriore attività di supporto all'oggettività è la conduzione di un vulnerability assessment.

Delle valutazioni del rischio quantitative ho già scritto in passato e ripeto in sintesi i punti: i dati a disposizione sono troppo pochi e inaffidabili e valutazioni quantitative (se pure fossero possibili) richiederebbero un eccessivo dispendio di energie senza apprezzabili miglioramenti.

PS: recentemente ho visto valutazioni del rischio sulla salute dei lavoratori e sono spesso di tipo qualitativo (anche perché non si assegna un valore economico alla vita delle persone).

****

07- Microsoft Threat Modeling Tool

Tempo fa, Glauco Rampogna (professionista della sicurezza delle informazioni e della privacy, nonché Idraulico della privacy) mi ha segnalato che lui usa, per lo sviluppo del software sicuro, il Microsoft Threat Modeling Tool:
- https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool.

Si tratta di un modello basato su quello STRIDE ed è orientato all'analisi delle applicazioni IT.

Questo materiale di MS serve anche a ragionare sugli approcci di valutazione del rischio. Anche se questo MTM è dedicato allo sviluppo di software, i suoi principi possono essere facilmente estesi ai sistemi di gestione per la sicurezza delle informazioni e al GDPR. Da notare che qui non è prevista l'assegnazione di valori per calcolare un livello di rischio (io penso sia necessario assegnare valori qualitativi; purtroppo stanno riemergendo auditor che ripropongono la folle idea di approcci quantitativi senza che però ne siano disponibili e consigliati pubblicamente, a differenza di approcci qualitativi o, come questo, che non sono né l'uno né l'altro).

****

\08- CIS Controls v 7.1

Franco Vincenzo Ferrari del DNV GL mi ha segnalato la pubblicazione della versione 7.1 dei CIS Controls.

Avevo già parlato della versione 7 e non mi ripeto:
- http://blog.cesaregallotti.it/2018/03/i-controlli-di-sicurezza-del-cis.html.

La pagina da dove scaricare il materiale:
- https://www.cisecurity.org/controls/.

****

09- Sistemi di sorveglianza e sicurezza

Un mio articolo per ICT Security Magazine dal titolo "Sistemi di sorveglianza e sicurezza":
- https://www.ictsecuritymagazine.com/articoli/sistemi-di-sorveglianza-e-sicurezza/.

****

10- Rapporto Clusit 2019 e Atti del Security Summit 2019 di Milano

Segnalo la pubblicazione degli atti (ossia delle presentazioni) del Security Summit 2019 organizzato dal Clusit e che si è tenuto a Milano il 12, 13 e 14 marzo:
- https://securitysummit.it/event/Milano-2019/atti.

Personalmente ho assistito a poche presentazioni. Leggendo le slide, ecco quelle che mi hanno interessato di più:
- "E se fosse un attacco mirato proprio contro la tua organizzazione sapresti gestirlo", a cura di Alessio Pennasilico e Giorgio Di Grazia (presentazione principalmente didattica, e poi promotrice di uno specifico servizio);
- "Da molti giorni a pochi minuti, come fermare rapidamente gli attacchi di phishing in corso con Cofense", a cura di Angelo Salice e Claudia Pollio (simile alla precedente);
- "La tua rete, gli applicativi e i database sono performanti e protetti come vuoi, Il tuo traffico di rete è davvero il tuo, Il monitoraggio di rete ti fornisce una piena visibilità e una sicura analisi comportamentale" (promozione del prodotto Flowmon; mi è piaciuto l'approccio della presentazione, ossia la presentazione di casi reali; questo è un approccio opposto alle presentazioni precedenti, più didattiche);
- "Cloud a volo d'uccello", a cura di Daniele Catteddu (le slide le ho trovate insipide, mentre l'intervento, a cui ho assistito, mi è piaciuto molto; peccato non ne rimanga niente se non nella mia memoria);
- "Siamo sicuri della blockchain", a cura di Andrea Reghelin (in realtà, parla degli smart contract, argomento molto recente; questa presentazione facilita un primo approccio all'argomento).

Notoriamente, in occasione del Security summit a Milano è pubblicato il Rapporto Clusit 2019 sulla sicurezza ICT in Italia:
- https://clusit.it/rapporto-clusit/.

Il Rapporto è in realtà una doppia pubblicazione. La prima è il rapporto vero e proprio con dati e analisi sugli eventi del 2018 e sulle previsioni per il 2019. Parere personale: la quantità di dati è enorme ma, alla fine, non aiutano a migliorare la sicurezza informatica (qualcuno potrebbe supporre che i "non esperti" potrebbero interessarsi a questi numeri e quindi avviare dei processi di miglioramento, ma la mia esperienza mi dice di no).

La seconda parte del rapporto è una raccolta di articoli, alcuni decisamente interessanti.

****

11- Il caso delle password in chiaro di Facebook

A fine marzo è emersa la notizia che Facebook conservava le password dei propri utenti in chiaro. Per questo segnalo questo articolo di Wired:
- https://www.wired.com/story/facebook-passwords-plaintext-change-yours/.

La notizia ufficiale di Facebook:
- https://newsroom.fb.com/news/2019/03/keeping-passwords-secure/.

Un commento, a mio parere molto interessante, su Twitter, che io intitolerei "Facebook is more secure than 99.9% of other websites":
- https://twitter.com/ErrataRob/status/1109557359360131072.

Non sono un fan di Facebook e, come molti sanno, il problema di Facebook è come usano i dati dei loro utenti.

Qui si è fatto grande clamore per una notizia fornita da Facebook stessa (che ha commissionato un'analisi tecnica dei propri sistemi, che ha evidenziato un errore tecnico del sistema di logging degli accessi) e non un bug scoperto da un "ricercatore indipendente" o evidenziato da una violazione dei dati.

****

12- Il caso della Boeing e del software

Credo sia nota a tutti la brutta notizia del Boeing dell'Ethiopian Airlines precipitato il 10 marzo 2019.

L'incidente, gravissimo, è stato originato da un bug del software. Incredibilmente i comandi del software non potevano essere contrastati da un'azione umana, contrariamente a quanto raccomandato per tutti gli impianti con impatto sulla sicurezza delle persone. Inoltre sembra che la correzione al bug fosse già disponibile, ma solo a pagamento.

Penso che ogni commento sia superfluo.

Un articolo sul fatto che i fix fossero a pagamento dal titolo "Doomed Boeing Jets Lacked 2 Safety Features That Company Sold Only as Extras":
- https://www.nytimes.com/2019/03/21/business/boeing-safety-features-charge.html.

Un'analisi sull'errore del software dal titolo "Storie di aerei caduti e del loro software":
- https://www.zeusnews.it/n.php?c=27193.