Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – MARZO 2015

****

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- 2 luglio: DFA Open Day
02- Novità legali: SPID - Identità digitale
03- Standardizzazione: UNI 10459:2015 - Professionista della Security
04- Standardizzazione: ISO/IEC TR 90006 - Commento
05- Standardizzazione: ISO/IEC 29147 - Vulnerability disclosure
06- Standardizzazione: ISO/IEC 20000-9 e servizi cloud
07- Indagini sui rischi e sugli attacchi
08- Indagine sulle funzioni interne di audit e la cybersecurity
09- Cyber che?
10- Inganno e autoinganno
11- Misure di sicurezza: Internet of Things
12- Misure di sicurezza: NISTIR 8023 per i "Replication devices"
13- Misure di sicurezza: Threat exchange
14- Attacco ai siti olandesi
15- Chief Humor Officer (CHO)

****

01- 2 luglio: DFA Open Day

Questo è un annuncio preliminare: il 2 luglio 2015, presso la Statale di Milano, si terrà il DFA Open Day.

Per saperne di più su DFA: http://www.perfezionisti.it/.

Anche quest'anno gli interventi rigaurderanno applicazioni di tecniche forensi, progetti internazionali correlati, novità giuridiche e legali.

Quindi: segnatevi la data! E se qualcuno conosce qualche potenziale sponsor, me lo faccia sapere (l'impegno per lo sponsor sarebbe molto ridotto).

Per gli ansiosi: non terrò alcun intervento; mi occuperò solo dell'organizzazione, di presentare i diversi relatori e di mantenere un po' d'ordine nelle domande.

****

02- Novità legali: SPID - Identità digitale

A dicembre avevo parlato del Regolamento UE eIDAS:
- http://blog.cesaregallotti.it/2014/12/regolamento-ue-910-del-2014-e-cad_11.html

Agostino Oliveri di Sicurdata mi ha segnalato che il Regolamento introduce anche un sistema per la gestione dell'identità digitale. In Italiano questo meccanismo vede una prima regolamentazione nel DPCM 24 ottobre 2014 ed è denominato "Sistema Pubblico per la gestione dell'Identità Digitale - Spid" (meglio non commentare certi acronimi).

Agostino mi ha anche inviato un articolo:
- http://www.agendadigitale.eu/identita-digitale/1304_il-regolamento-eidas-vara-il-marchio-di-fiducia-europeo.htm

Qui si parla dello Spid alla fine e si dice che "lo Spid è un sistema aperto attraverso il quale soggetti pubblici e privati, previo accreditamento da parte dell'Agenzia per l'Italia Digitale, potranno offrire servizi di identificazione elettronica a cittadini e imprese"; "in questo modo consentirà ai cittadini di avvalersi della propria identità digitale per accedere ai servizi on line messi a disposizione dalle singole Pubbliche Amministrazioni o anche dai privati che aderiranno a tale sistema".

Per saperne ancora di più, segnalo la pagina di AgID:
- http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/spid

Si osservi che i regolamenti attuativi, ad oggi, sono ancora in bozza.

****

03- Standardizzazione: UNI 10459:2015 - Professionista della Security

Enzo Ascione di Intesa Sanpaolo Group Services mi ha segnalato la pubblicazione della norma UNI 10459:2015 dal titolo "Attvità professionali non regolamentate: Professionista della Security - Requisiti di conoscenza, abilità e competenza". La norma tratta di sicurezza sia fisica sia delle informazioni (anche se l'accento è sicuramente sulla prima).

Enzo mi ha anche segnalato un articolo in merito:
http://www.snewsonline.com/notizie/attualita/l_evoluzione_del_ruolo_del_security_manager_funzioni_e_profili_del_professionista_della_security_aziendale_nuova_norma_uni_10459_2015-2939.

Franco Vincenzo Ferrari di DNV GL mi ha segnalato che, sempre in merito agli organismi di vigilanza, è stata recentemente firmata una convenzione tra Accredia e il Dipartimento della Pubblica Sicurezza. Accredia quindi potrà accreditare gli organismi di certificazione affinché certifichino gli istituti di vigilanza in base alle normative UNI 11068:2005 e UNI CEI EN 50518:2014 relative alle centrali operative e di telesorveglianza, UNI 10891:2000 per gli istituti di vigilanza privata e UNI 10459:2015 riguardante i professionisti della security:
- http://www.accredia.it/news_detail.jsp?ID_NEWS=1819&areaNews=95&GTemplate=default.jsp.

Personalmente sono un po' perplesso, visto che si tratta di tantissime competenze per cui un esperto che discetti di sicurezza fisica, informatica e investigazioni, alla fine risulta essere un tuttologo senza reali competenze. Ma non vorrei essere inutilmente pessimista (il titolo di una norma UNI che usa il termine "security" e non "sicurezza" mi ha messo di malumore fin dall'inizio).

****

04- Standardizzazione: ISO/IEC TR 90006 - Commento

Tony Coletta, che rappresenta l'Italia al ISO/IEC JTC 1 SC 7, mi ha risposto in merito al mio post sulla ISO/IEC 90006 (e lo ringrazio molto):
- http://blog.cesaregallotti.it/2015/02/isoiec-tr-90006.html

Tony mi scrive: "C'è almeno una cosa che considero interessante nella 90006 e a cui ho contribuito: trovare nella 20000 l'equivalente dei controlli della progettazione e sviluppo della 9001 (riesame, verifica e validazione). In qualche misura si trovano, ma la 20000 li chiama "test" e "verifiche" e li sparge nei punti più strani. Forse nella nuova edizione della 20000 si utilizzerà una terminologia più appropriata".

Mi associo alla speranza di Tony: che ci sia standardizzazione negli standard e che la lunga e onorata storia della ISO 9001 (malgrado non tutte le certificazioni siano ineccepibili) non sia ignorata, per presunzione, da chi scrive altri standard.

Tony mi segnala anche di vedere la differenza di definizione del termine "document". Infatti, nella ISO/IEC 20000 è stata aggiunta una nota alla definizione dei documenti ("specificano intenti da conseguire") per renderla più omogena a quella delle registrazioni ("riportano i risultati ottenuti o forniscono evidenza delle attività svolte").

****

05- Standardizzazione: ISO/IEC 29147 - Vulnerability disclosure

Franco Ferrari mi ha segnalato la pubblicazione (a febbraio 2014) della ISO/IEC 29147 dal titolo "Vulnerability disclosure". Già Stefano Ramacciotti me l'aveva segnalata a suo tempo.

La norma presenta un processo, e le relative considerazioni, che i produttori di sistemi informatici dovrebbero seguire per ricevere e verificare le segnalazioni sulle vulnerabilità dei propri prodotti e per risolverle.

****

06- Standardizzazione: ISO/IEC 20000-9 e servizi cloud

Franco Ferrari di DNV GL mi ha segnalato la pubblicazione della ISO/IEC TR 20000-9 dal titolo "Guidance on the application of ISO/IEC 20000-1 to cloud services".

La prima impressione (ma anche la seconda, per cui ho chiesto aiuto a Tony Coletta, nostro rappresentante italiano al ISO/IEC JTC1 SC 7, che ringrazio) è che sia una norma inutile.

Non l'ho letta, ma speravo potesse essere una lettura della ISO/IEC 20000-1 che potesse essere utile a chi non la conosce bene, ma non è così.

Ovviamente si tratta della solita norma sul cloud, spinta dalla moda ma da poche idee originali. Spiace vedere tante energie sprecate in standard inutili.

****

07- Indagini sui rischi e sugli attacchi

Inizio anno, tempo di rapporti sulla sicurezza dei più vari tipi.

Il primo, di Protiviti, ha titolo "Executive Perspectives on Top Risks for 2015" e riguarda i rischi (non solo di sicurezza delle informazioni) percepiti da 280 membri di Board e Top Management:
- http://www.protiviti.com/toprisks

In sintesi i rischi ritenuti più importanti sono quelli correlati ai cambiamenti normativi, all'economia generale, agli attacchi informatici, alla disponibilità del personale, alla mancanza di procedure relative alla gestione delle crisi, alle difficoltà di comprendere le aspettative dei clienti. Il decimo rischio forse li riassume tutti: "le attività attuali non riescono ad avere le prestazioni attese in merito a qualità, rapidità, costi e innovazione ". Il mio commento sintetico e, purtroppo, basato su quello che vedo: ne discutono, ma poi non promuovono né seguono attentamente azioni per trattare questi rischi; il motivo, credo, è che i manager sono giudicati nel breve termine su fatturato e utile; "sostenibilità nel medio e lungo termine" non è normalmente un parametro di giudizio.

Questa preoccupazione si percepisce nel settimo rischio che recita "la gestione della sicurezza delle informazioni richiede risorse significative".

Nota terminologica: Protiviti non usa il termine "rischio" come previsto dalle norme internazionali (ISO 31000, ISO/IEC 27001, eccetera). Ma, insomma, si capisce lo stesso.

Il secondo rapporto è il "Horizon Scan 2015" del Business Continuity Institute:
- http://www.thebci.org/index.php/obtain-the-horizon-scan-2015-document

Sintetizzo le 10 minacce ritenute più importanti: attacchi informatici, interruzioni dei sistemi informatici e delle infrastrutture, interruzioni nella filiera di fornitura, clima, malattie, fuoco, terrorismo. Interessante la preoccupazione relativa alla filiera di fornitura, che l'anno scorso era al sedicesimo posto e ora è al quinto: questo aspetto è finalmente considerato come importante. Raccomando, come minimo, la lettura dell'executive summary.

Un dato interessante per scopi polemici: le organizzazioni che dispongono di analisi e non le usano sono il 33%; mi chiedo se è perché sono commissionate a consulenti non capaci o perché sono commissionate solo per far bella figura (due dei mali che affliggono me e i miei colleghi). Un altro caso riguarda l'incapacità di rivedere le proprie decisione anche a fronte di analisi che portano a diverse conclusioni (un tipo di autoinganno molto diffuso: si "dimenticano" subito le posizioni contrarie alla nostra).

L'ultimo report è il "HP Cyber risk report 2015":
- http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/index.html

Di questo seleziono alcuni dei temi chiave riportati all'inizio del rapporto: sfruttamento di vulnerabilità note da tempo (a cui sono collegati gli annosi problemi di patch non installate e di correzioni mai prese in considerazione per il principio "funziona e quindi non si tocca"); configurazioni sbagliate, difetti di progettazione, sviluppo e codifica dei software (cose che, per essere risolte, richiedono persone competenti, e quindi costose, che dedicano del tempo, che costa, ad aggiornarsi e trovare soluzioni).

Alcune parti del rapporto sono divulgative, altre più tecniche (per esempio il capitolo sulle vulnerabilità).

****
08- Indagine sulle funzioni interne di audit e la cybersecurity

Protiviti ha pubblicato un documento dal titolo "From cybersecurity to collaboration: assessing the top priorities for internl audit functions: 2015 internal audit capabilities and needs surveys":
- http://www.protiviti.com/iASurvey

Il documento è abbastanza interessante, se escludiamo il solito abuso del termine "cyber security" per "sicurezza informatica".

Presento alcune cose degne di nota a mio personale giudizio, con, tra parentesi, i miei commenti:
- il 53% valuta il rischio di cybersecurity per elaborare il piano di audit (il 47%, quindi, non lo fa; e mi pare tanto; ma chissà se tutti usano il termine "cybersecurity" con lo stesso significato);
- le competenze più urgenti da migliorare riguardano "GTAG 16 - Data analysis technogies", "NIST cybersecurity framework", "Mobile applications", "Practice advisory 2320-4 - Continuous assurance"; The guide to to assessment of IT risk (GAIT)" (posto che non so di cosa parlano 3 degli elementi, noto che le necessità riguardano, tranne un caso, schemi di audit; deduco che chi non ha competenze sulla tecnologia (e sono in tanti) continua a non volerne sapere; la lista prevede 35 argomenti e di tecnico c'è solo e soltanto "Mobile applications"; interessante osservare che nella lista si trova anche al 21o posto la ISO 14001);
- per quanto riguarda le competenze relative alla conduzione degli audit, al quinto posto si trova "time management" (solitamente uno dei grandi problemi degli auditor).

Altri troveranno ulteriori elementi di interesse: buona lettura!

****

09- Cyber che?

La newsletter di HSC (Hervé Schauer Consultants) di febbraio 2015 propone un intervento di Béatrice Joucreau e Christophe Renard che riassumo (forse malamente; spero gli autori non me ne vogliano (o non se ne accorgano)).

<<
Nel mondo della sicurezza si sentono sempre di più i termini di cybersicurezza, cybercriminalità, cyberguerra, eccetera. Tutti questi termini nascono forse per distinguere la sicurezza delle informazioni (solitamente con finalità di protezione di un ente) dalla difesa da criminali che usano Internet come arma. Oggi si sono estesi per sostituire, in modo più breve e suggestivo, "sicurezza informatica", "sicurezza delle informazioni" o "gestione della sicurezza delle informazioni".

In realtà, i termini cyberx non sono molto moderni né appropriati: hanno origine (tranne "cibernetica") negli anni Ottanta nella letteratura di fantascienza (!) e sono costruiti usando una parola ("cyber", ossia "timone" in greco) che non è un prefisso (infatti "cybernetica", che vuol dire "studio dei sistemi di regolamento", non usa "cyber" come vero e proprio prefisso).

A parte queste considerazioni, c'è qualche differenza tra cybersecurity e sicurezza dei sistemi informatici? I testi definiscono solitamente come cybersecurity "lo stato per cui un sistema informatico resiste ad eventi provenienti dal cyberspazio" (ossia da Internet, intesa come rete mondiale); la cybersecurity, quindi, utilizza tecniche di sicurezza informatica per combattere il cybercrime e attuare la cyberdefence.

Questa definizione, quindi, escluderebbe un certo numero di minacce, ossia quelle non legate ad Internet (come per esempio l'ingegneria sociale, l'osservazione dello schermo del pc da parte di un malintenzionato, il furto di un pc), quelle originate da agenti interni, quelle di origine accidentale (errori) o non umana (eventi naturali). Ovviamente sono anche escluse le minacce non informatiche, come quelle legate ai documenti cartacei e all'intercettazione di conversazioni.

Questa distinzione è fatta raramente nella pratica, forse perché ritenuta non interessante.
>>

A questo punto aggiungo una nota personale: noto molto interesse nei confronti di convegni che si richiamano alla cybersecurity e questo mi preoccupa. Infatti rischiamo di tornare indietro di 25 anni, quando la sicurezza informatica era vista come distinta dalla "sicurezza delle altre informazioni"; rischiamo di concentrarci troppo sulle minacce informatiche (pure importantissime) e perdere di vista quelle altre.

Mi scuso per l'interruzione e vado avanti a tradurre (malamente).

<<
Perché, quindi, "cybersecurity"? Con questo termine bisogna vedere un tentativo di "vendere" la sicurezza delle informazioni. I più cinici non vedranno che movimenti opportunistici da parte dei commerciali. Ma, visto che la nostra dipendenza dai sistemi informatici è ormai irreversibile e totale, anche se la loro sicurezza è rimasta in gran parte misera, un richiamo (con qualche suggestione di panico) potrebbe fare uscire il tema della sicurezza delle informazioni dalla comunità di pochi professionisti.

Usare un termine che sembra anglofono (siber-secuiriti) forse potrà promuovere meglio la sicurezza delle informazioni presso un pubblico incapace di concentrarsi su termini di più di 6 sillabe. Adottare questa terminologia vuol dire ammettere che la sicurezza delle informazioni ha bisogno di cambiare costume per uscire dal suo ghetto.

Malgrado sia ridicolo, usare il termine "cyber" vuol dire fare comunicazione. I media dimostrano che il termine è ormai conosciuto. La "cybersecurity" riuscirà a far convergere professionalità e tecniche, istituzioni pubbliche e private, agenzie governative e associazioni industriali di peso, mentre la "sicurezza delle informazioni" è rimasta un affare per specialisti? Bisogna sperarlo (a quando un'Agenzia per la cybersecurity?).

PS: alcuni verificheranno che il termine "cyberspazio" è stato inventato da William Gibson, che lo definiva "un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione, da bambini a cui vengono insegnati i concetti matematici... Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità. Linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci di una città, che si allontanano". >>

Personalmente, cercherò di continuare a usare l'espressione "sicurezza delle informazioni". Tra qualche anno sarà giudicata un'altra mia mania linguistica (come il non usare "implementare" e "rilasciare" per il software o "invocare" per i piani di continuità).

****

10- Inganno e autoinganno

Segnalo questo libro che ho trovato molto interessante: "La follia degli stolti: La logica dell'inganno e dell'autoinganno nella vita umana", di Robert Trivers (editore Einaudi).

Quanto riportato su inganno e autoinganno ha impatti anche sul lavoro e gli ambienti di lavoro. Per esempio, pensiamo alle categorie dell'auto inganno:
- sopravvalutarsi (tutti ci sopravvalutiamo e poi facciamo errori);
- denigrare gli altri, distinguere tra "noi" e "loro", l'ipocrisia morale e le falsi narrazioni sociali (per cui giustifichiamo nostri comportamenti altrimenti non giustificabili);
- la corruzione del potere (anche un minuscolo potere riduce la capacità di empatia e di ascoltare gli altri);
- l'illusione del controllo.

Altra cosa interessante che mi sono appuntato è la nostra attitudine a mantenere la posizione nonostante tutto (per esempio, una volta negata una preferenza o un'azione, si tende a continuare a negarla, nonostante le prove contrarie).

Purtroppo il libro tratta alcune teorie in modo frettoloso (per esempio, non ho capito il "faccismo"); altre parti sono inutilmente lunghe (quella sui disastri aerei e spaziali) o inappropriate per gli scopi del libro (le critiche a Israele, l'attacco alla psicologia come pseudo-scienza, eccetera).

****

11- Misure di sicurezza: Internet of Things

Dopo aver fatto indigestione negli ultimi 5 o 6 anni con il "cloud", ora sembra che sia arrivato il turno del "Internet of things" o IoT. In pochissime parole, l'insieme di tutti i dispositivi che si connettono a Internet; non solo pc o simili, ma anche altri, tra cui sensori di autoveicoli, dispositivi medici, elettrodomestici, eccetera.

Gli oggetti rappresentano dei rischi perché non sempre sono programmati correttamente e gli aggiornamenti non sono previsti. Possono quindi essere sfruttati da malintenzionati per accedere ad una rete privata in modo ancora più semplice che se attaccassero dei pc.

Questa mia descrizione è troppo sintetica, ma è solo per introdurre l'argomento e segnalare la pubblicazione " Internet of things: Risk and value considerations" di ISACA, ottimo punto d'inizio per studiare la materia (tra l'altro, ISACA prevede di realizzare una serie di studi dedicati all'IoT):
- www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/internet-of-things-risk-and-value-considerations.aspx

Segnalo anche che il "HP Cyber risk report 2015" (già commentato in precedenza) dedica un paragrafo alla materia:
- http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/index.html

****

12- Misure di sicurezza: NISTIR 8023 per i "Replication devices"

Il NIST ha pubblicato un internal report dal titolo "Risk Management for Replication Devices":
- http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-8023

Il termine "Replication device" si riferisce a ogni strumento che riproduce (cioè copia, stampa, acquisisce digitalmente) documenti, immagini o oggetti da origine elettroniche o fisiche; tra di essi vi sono fotocopiatrici, stampanti, stampanti 3D, scanner, scanner 3D e macchine multifunzione (fotocopiatrice, stampante e scanner).

Si tratta spesso di oggetti sottovalutati dal punto di vista della sicurezza, tanto che raramente ne è fatta un'analisi preliminare su questo aspetto e, poi, ne è tenuto un censimento a scopi di monitoraggio.

Il documento del NIST è molto sintetico e, a mio avviso, può essere usato come base per valutare e gestire altri macchinari (inclusi quelli industriali) presenti in un'azienda.

****

13- Misure di sicurezza: Threat exchange

Questa notizia l'ho ricevuta inizialmente dal SANS NewsBites: alcune grandi aziende di informatica (Facebook, Tumblr, Pinterest, Twitter, Yahoo eccetera) utilizzano un sistema di scambio di informazioni sulle minacce a cui potrebbero essere sottoposte.

Un articolo:
- http://www.wired.com/2015/02/facebook-unveils-tool-sharing-data-malicious-botnets/

Il sito di Threat Exchange (grazie a Pasquale Stirparo, che ha anche commentato "onestamente non so quante aziende siano disposte a condividere certe informazioni... e soprattutto a darle in gestione a FaceBook"):
- https://threatexchange.fb.com

Grazie a Daniela Quetti per avermi ribadito la notizia (inizialmente l'avevo ignorata).

****

14- Attacco ai siti olandesi

Fabrizio Monteleone di DNV GL mi ha segnalato questo articolo (fa riferimento ad un attacco DOoS del 10 febbraio):
- http://in.reuters.com/article/2015/02/11/netherlands-government-websites-idINKBN0LF0OU20150211

Fabrizio mi sottolinea quanto segue: "Chi tiene alla reputazione o chi ritiene che il web sia un canale di comunicazione come tutti gli altri e come tale vada protetto, dovrebbe comportarsi come i genitori che mandano i figli a scuola da soli: spiegare di fare attenzione agli sconosciuti, non dare confidenza, chiamare la maestra. Se tutto questo non importa vale sempre l'assioma che se non si crea il bisogno (in questo caso di protezione) non si vende il prodotto/servizio, nè si giustificano la nascita e la crescita di National/Worldwide/Secret agencies...").

Io noto un'altra cosa interessante: la società che si occupa dei siti web attaccati ha rilasciato una dichiarazione: "I primi sintomi indicavano un problema tecnico interno, poi abbiamo capito che si trattava di un attacco dall'esterno". Uno specialista di sicurezza ha commentato: "Se stai subendo un attacco DDoS, lo sai".

Il mio corollario: "Ma che dichiarazione hanno fatto? Un minimo di piano di emergenza e di comunicazione ("piano di gestione delle crisi") ce l'avevano?". Faccio anche notare che l'attacco ha colpito le linee telefoniche: deduco fossero su VoIP e sulla stessa rete della linea dati... forse non la scelta migliore del mondo.

****

15- Chief Humor Officer (CHO)

La Commissione Europea, nell'ambito dell'iniziativa sull'agenda digitale, promuove il Chief Humor Officer (CHO):
- http://ec.europa.eu/information_society/newsroom/cf/dae/itemdetail.cfm?item_id=21001

Ringrazio itSMF per la notizia.

In poche parole: scherzare aiuta la motivazione, la creatività e la qualità del lavoro.

Non so bene cosa c'entri con l'agenda digitale o la sicurezza delle informazioni o le altre cose che segnalo, ma so che c'entra.