Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – FEBBRAIO 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- Legale Cassazione Penale - legittimo l'utilizzo di telecamere per provare i furti dei dipendenti

Questa sentenza, che analizza anche il famoso articolo 4 dello Statuto dei lavoratori, mi pare interessante. In sintesi, l'enunciato è il seguente: " le norme dello Statuto tutelano sì la riservatezza dei lavoratori ma non fanno divieto dei cosiddetti "controlli difensivi" del patrimonio aziendale e non vietano il loro utilizzo in sede processuale.".

L'articolo di Filodiritto:
- http://www.filodiritto.com/news/2015/cassazione-penale-legittimo-lutilizzo-di-telecamere-per-provare-i-furti-dei-dipendenti.html.

La sentenza non è ancora su www.cortedicassazione.it.

****

02- Legale: Lecito registrare il colloquio telefonico con il capo (parte 2)

Roberto Bonalumi mi ha risposto in merito alla notizia per cui la registrazione di un colloquio intercorsa tra due persone può essere effettuata nel caso in cui si preveda possa essere spendibile in un processo civile o per difesa:
- http://blog.cesaregallotti.it/2015/01/lecito-registrare-il-colloquio.html

In quella occasione mi lamentavo di non poter leggere la sentenza. Roberto mi ha quindi fornito la soluzione: "andare su www.cassazione.it, selezionare il servizio "SentenzeWeb" e poi effettuare la ricerca tra le sentenze civili della Cassazione".

C'è ovviamente anche quella oggetto di discussione e sembra proprio che è legittimo registrare conversazioni, purché solo quando questo possa essere ritenuto utile, in un futuro, per difesa.

Spero di aver capito correttamente, visto che la sentenza è scritta in modo inutilmente complicato.

****

03- Standardizzazione: ISO/IEC TR 90006

Franco Ferrari mi ha segnalato l'esistenza della ISO/IEC TR 90006 dal titolo "Guidelines for the applications of ISO 9001:2008 to the IT service management and its integration wirh ISO/IEC 20000-1:2011".

La norma è del 2013 e non la leggerò. Forse mi sfuggirà qualcosa, ma ho sempre dei dubbi su queste norme di confronto per due motivi: il primo è che se qualcuno conosce già le due norme (di poche pagine ciascuna!), dovrebbe essere capace di confrontarle agevolmente; il secondo è che solitamente il documento finale risulta composta di una serie di ovvietà, a causa della natura stessa degli standard internazionali (troppi autori contribuiscono a eliminare qualsiasi contributo originale e in una norma non si possono scrivere cose troppo originali).

****

04- NSA Information Assurance guidance

Stefano Ramacciotti mi ha segnalato la pagina "Information Assurance guidance" della NSA:
- https://www.nsa.gov/ia/mitigation_guidance/

Io avevo già visitato questo sito ma non l'avevo segnalato. Quindi ringrazio Stefano del richiamo. Infatti ho fatto male perché la NSA, nonostante sia associata a spionaggio e controllo delle persone, ha persone valide e la loro lista delle 10 misure di sicurezza più importanti ("Top 10 IA Mitigation Strategies") dovrebbe essere considerata.

Si tratta di misure tecniche spesso non considerate dalle solite raccomandazioni in circolazione. Insomma, non si tratta delle solite misure generali ("scrivete una politica di sicurezza", "fate un risk assessment", "fate gli audit", eccetera) e neanche di processo ("stabilite un processo di gestione delle utenze", "stabilite un processo di gestione degli incidenti", eccetera). Sono anche forniti consigli tecnici molto pratici.

Purtroppo non hanno fatto un volumetto di 20 pagine, ma 10 documenti di due pagine ciascuno.

****

05- NIST SP 800-163 sui test per le apps

Il NIST ha pubblicato questa guida dal titolo SP 800-163 " Vetting the Security of Mobile Applications". Si scopre che "vetting" è usato al posto di "evaluating" (Oxford Dictionary lo traduce come "verifica del passato di un individuo" e mi chiedo perché non abbiano usato "evaluating"... forse la solita introduzione di un gergo inutile e ridicolo che crea confusione e fa sembrare bravi e competenti?).

La guida si trova a questo link: http://csrc.nist.gov/publications/PubsSPs.html#800-163.

La guida dovrebbe essere accompagnata dalla NIST SP 800-124 "Guidelines for Managing the Security of Mobile Devices in the Enterprise". Insieme forniscono indicazioni per lo sviluppo delle apps, sulle quali transitano sempre più dati critici e, pertanto, dovrebbero essere sviluppate attentamente.

****

06- Game of hacks per il codice sicuro

Stefano Ramacciotti mi ha segnalato una bella iniziativa: un quiz di 5 domande per verificare la capacità di riconoscere le vulnerabilità di programmazione e, quindi, imparare a sviluppare codice più sicuro.

Ecco un articolo di presentazione (in inglese):
- https://www.checkmarx.com/2015/01/20/secure-coding-with-game-of-hacks

Ecco il gioco, nella versione gratuita: http://www.gameofhacks.com/.

Sembra che proporranno una versione a pagamento per le attività aziendali di formazione e sensibilizzazione; mi viene quasi voglia di obbligare i miei clienti a fare il test. Stefano, invece, dice di suggerire questo gioco agli sviluppatori, in sostituzione della PlayStation.

****

07- Enisa Threat Landscape 2014

A inizio gennaio 2015 avevo segnalato l'Enisa "Threat Landscape and Good Practice Guide for Internet Infrastructure": http://blog.cesaregallotti.it/2015/01/enisa-threat-landscape-of-internet.html.

Questa volta, sempre dal gruppo Italian Security Professional di LinkedIn, segnalo l'ENISA "Threat Landscape 2014" che ha come sottotitolo "Overview of current and emerging cyber-threats":
- http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014.

Si tratta di un'analisi e un ordinamento delle minacce informatiche più diffuse, secondo quanto raccolto da numerosi (più di 400) studi liberamente disponibili su Internet. In altre parole, quelli di Enisa si sono studiati i materiali disponibili e preparati da altri e quindi, con un metodo che mi è oscuro, hanno elencato le 15 minacce più diffuse. Malgrado i miei dubbi, la lettura è interessante. I più pigri possono solo consultare pagina iv, dove si trova la "Table 1: Overview of Threats and Emerging Trends of the ENISA Threat Landscape 2014".

I mediamente pigri possono accontentarsi di un articolo riassuntivo:
- http://securityaffairs.co/wordpress/32777/cyber-crime/enisa-threat-landscape-2014.html

****

08- Rapporto sulla sicurezza nelle PA

Andrea Praitano di Business-e mi ha segnalato il "Cyber Security Report 2014" del CIS dell'Università La Sapienza di Roma. Questo report riporta i risultati dell'osservatorio che hanno fatto sulle Pubbliche Amministrazioni, classificate in PA centrali, locali, ASL, ecc.

La presentazione, da sola, è di difficile comprensione, mentre il report, riportando la descrizione dei vari grafici, è chiaro:
- http://www.cis.uniroma1.it/csr2014

La mia veloce lettura mi ha permesso di trarre preoccupazione dallo stato della sicurezza della nostra PA, ma ben pochi insegnamenti (spero però ne traggano i responsabili delle strutture). Comunque, copio e incollo nel seguito il commento di Andrea e lo sottoscrivo.

<<
Il report nel complesso è interessante anche se ha diversi aspetti che a me non piacciono perché analizza più il "che cosa hanno" più che entrare nel merito del "come lo utilizzano". Per esempio, è stato chiesto agli intervistati se hanno il firewall, non se ne gestiscono le regole in modo efficace.

Però un osservatorio, gioco forza, fa analisi abbastanza "ad alto livello" non riuscendo o potendo entrare nel dettaglio.

Ha comunque degli spunti e conclusioni interessanti che sono anche delle conferme. A mio avviso andrebbero approfondite le PA che hanno risposto di non aver subito attacchi, in quanto a me personalmente sembra poco probabile: forse non si sono accorte di essere state sotto attacco e questo sarebbe grave.
>>

****

09- Ospedali e continuità operativa

Sandro Sanna mi ha segnalato il seguente articolo:
- http://www.agendadigitale.eu/infrastrutture/1316_in-tre-ospedali-su-quattro-i-pazienti-sono-alla-merce-dei-crash-informatici.htm

Diciamo che i toni dell'articolo sono un po' troppo "giornalistici".

Però ci sono cose interessanti, come la riflessione sul cloud per trovare soluzioni di DR e la differenza tra grandi e piccole aziende (e quindi, tra diverse disponibilità economiche grazie alla differenza di scala).

Forse un'ulteriore riflessione dovrebbe riguardare: quanti dei servizi informatici degli ospedali sono già gestiti da fornitori esterni? Con tutto quello che ne consegue (disponibilità di un DR, controllo degli accessi, eccetera).

****

10- Sicurezza IT nel settore energia - 3

Stefano Ramacciotti, dopo le prime due puntate sulla sicurezza IT nel settore energia, mi ha segnalato il "Energy sector cybersecurity framework implementation guidance" del U.S. Department of energy, uscito giusto a gennaio 2015:
- http://www.energy.gov/oe/downloads/energy-sector-cybersecurity-framework-implementation-guidance

Si tratta di un bel volume di 53 pagine di tipo tecnico (per quanto un framework possa esserlo), dopo le precedenti segnalazioni di pubblicazioni molto più divulgative.

Diciamo che non dice nulla di particolarmente nuovo (ma sono pronto ad essere smentito), ma è certamente molto chiaro e molto pragmatico. Può essere letto anche da chi non si occupa di settore energetico, visto che si tratta di raccomandazioni facilmente applicabili a tutti i settori.

Per chi volesse approfondire, nel capitolo 3 si trovano ulteriori link, incluso uno al " NISTIR 7628 Revision 1: Guidelines for Smart Grid Cybersecurity. Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements" di ben 668 pagine (mi sono rifiutato di leggerlo perché non sto seguendo lavori nel settore energia; e poi mi chiedo quanto dovrebbe essere lungo il documento che tratta dei requisiti a basso livello).

Sicuramente queste pubblicazioni così pragmatiche mi sembrano più interessanti di altre che trattano di sicurezza come se fosse metafisica. Quindi ringrazio Stefano della segnalazione.

****

11- Sandbox sui pc

Dalla newsletter di Achab inoltro questa notizia: Dell prevede, nella sua installazione OEM per i pc business, la messa a disposizione di un programma di sandboxing:
- https://www.achab.it/achab.cfm/it/blog/achablog/dell-introduce-una-sandbox-sui-pc-business

In poche parole, l'utente può decidere quali programmi utilizzare nella sandbox, senza che invece lavorino direttamente sul sistema operativo, con tutti i rischi del caso, in particolare se si tratta di browser o programmi con livello di sicurezza non completamente noto.

Ovviamente, quello annunciato non è l'unico prodotto di sandboxing (vedo che il più noto è Sandboxie, e poi c'è questo BufferZone Pro della Trustware gratuito per scopi non commerciali, ma il loro sito oggi non funziona). Questa tecnologia mi pare interessante e spero di poterla approfondire nel futuro.

****