Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – SETTEMBRE 2016

****

Newsletter mensile con novità su 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- Normativa: Nuovo CAD

Con il D.Lgs. 179 del 2016 è stato modificato il D.Lgs. 82 del 2005, ossia il CAD, ossia il Codice dell'amministrazione digitale, importante perché regola la gestione dei documenti digitali, non solo nella PA. Le modifiche sono necessarie per allineare il CAD al Regolamento eIDAS (EU 910/2014).

È possibile leggere il nuovo CAD ricercandolo su www.normattiva.it.

Grazie ai tweet di Daniele Tumietto, che segnala questo articolo di analisi:
- http://www.mysolutionpost.it/blogs/socialmediamente/ragone/2016/09/codice-amministrazione-digitale.aspx.

Andrea Caccia, invece, analizza gli impatti che il nuovo CAD ha sulla PEC. Non sembrano impatti positivi:
- https://www.linkedin.com/pulse/pec-la-fine-dellincantesimo-andrea-caccia.

Altri articoli usciranno nei prossimi giorni e ne darò notizia.

****

02- Normativa: Firme elettroniche nel mondo

Stefano Ramacciotti mi ha segnalato (commentandola come non molto scientifica né approfondita, ma comunque interessante) la seguente presentazione relativa alle firme elettroniche nel mondo:
- https://www.esignlive.com/resource-center/electronic-signature-laws-around-the-world/.

Se non riuscite a sopportare il fatto che si tratta di una presentazione commerciale o se volete confrontarvi direttamente con le legislazioni nazionali, segnalo che la presentazione riporta il seguente sito:
- http://193.62.18.232/dbtw-wpd/textbase/esiglaws.htm.

Il problema di questo sito è che elenca sì la normativa nazionale pertinente per ogni Paese (anche se per l'Italia mancano tutti i provvedimenti tecnici), ma non dice come consultarla. Però faccio i complimenti al Institute of Advanced Legal Studies (IALS), School of Advanced Study, University of London, che ha avviato questo lavoro.

Per quanto riguarda la presentazione, Andrea Caccia mi ha segnalato che, quando tratta delle "certificate signature", sostiene erroneamente l'equivalenza tra una firma elettronica basata su certificato e la firma qualificata.

****

03- Normativa: Garante privacy e "strumenti per rendere la prestazione lavorativa

Massimo Cottafavi di SNAM e Pierfrancesco Maistrello di Vecomp mi hanno segnalato (quasi in contemporanea) questa sentenza del Garante privacy. La situazione è simile a tante altre: i dipendenti di un'azienda (un'università, in questo caso) si lamentano dei monitoraggi relativi alla navigazione Internet:
- http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/5408460.

Però qui il Garante parla degli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa", di cui si parla nel nuovo (del 2015) articolo 4 dello Statuto dei lavoratori (Legge 300 del 1970) e di cui ho parlato in precedenza. Il punto chiave del Provvedimento del Garante è il 4.3.

Se ho capito giusto, il Garante dice che gli strumenti di monitoraggio e tracciamento dell'uso dei servizi Internet non sono da considerare "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" e pertanto non possono essere utilizzati senza accordi sindacali o autorizzazione della Direzione territoriale del lavoro.

****

04- Standardizzazione: ISO 22301 in italiano

Questa volta sembra proprio che la notizia sia vera: è finalmente uscita la versione ufficiale UNI in italiano della ISO 22301:2012, ossia la norma dedicata alla continuità operativa (o "business continuity", per chi è abituato all'ingelse):
- http://store.uni.com/magento-1.4.0.1/index.php/uni-en-iso-22301-2014.html.

Mi chiedo perché ci siano voluti 4 anni per pubblicare questo testo, ma ora è una domanda inutile. Buona lettura e grazie a Franco Ferrari di DNV GL per la notizia!

****

05- Standardizzazione: ISO/IEC 20000-6

Tony Coletta mi ha segnalato la prossima pubblicazione della ISO/IEC 20000-6 dal titolo "Requirements for bodies providing audit and certification of service management systems". In altre parole, si tratta delle regole per gli organismi di certificazione che offrono certificazioni ISO/IEC 20000-1. Ora lo standard si trova in stato di bozza finale:
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=64681.

Lettura consigliata solo agli organismi di certificazione.

****

06- Attenzione a Internet!

Non avrei voluto scrivere del caso di Tiziana Cantone: una persona che ha inviato via Internet un suo film hard a degli amici, che a loro volta l'hanno diffuso fin tanto che tale film è diventato di pubblico dominio e la sua protagonista non ha retto la situazione (complici anche gli sberleffi di ogni tipo e un giudice che le ha chiesto 20mila euro di spese processuali quando lei ha chiesto ai social network di cancellare i video) e alla fine si è suicidata.

Ne scrivo perché si tratta di un caso che ci riguarda tutti perché troppo spesso usiamo Internet e i suoi servizi senza renderci veramente conto di quanto siano pubblici e pervasivi.

Ricordiamo in futuro questo caso, non per sbeffeggiare una persona che ha fatto sì una sciocchezza ma l'ha pagata troppo cara, ma per ricordarci e ricordare che ogni foto e ogni video e ogni commento e ogni post che lasciamo su Internet o inviamo via email è come se fosse appeso in una bacheca accessibile al pubblico e che a pagarla sono sempre i meno forti (vi ricordate uno dei casi della Sony, di cui parlai quasi due anni fa su http://blog.cesaregallotti.it/2015/01/una-riflessioen-sullattacco-alla-sony.html, che ha visto la diffusione delle email degli impiegati "normali"?).

E però sembra che qualcosa stia cambiando, forse finalmente una nuova sensibilità si sta diffondendo: una 18enne ha accusato i suoi genitori perché avevano pubblicato le sue foto da bambina su Facebook:
- http://fusion.net/story/347880/sue-your-parents-for-embarrassing-you-on-facebook/.

****

07- Linee guida NIST sul BYOD

Il NIST ha pubblicato due documenti dedicato al BYOD e, in generale, al lavoro da remoto.

La prima è la SP 800-46 Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. Il link diretto:
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf.

La seconda è la SP 800-114 Revision 1, User's Guide to Telework and Bring Your Own Device (BYOD) Security. Il link diretto:
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf.

La pagina web dove sono annunciate queste due pubblicazioni:
- http://csrc.nist.gov/news_events/#pub2and3.

La prima è rivolta alle aziende, la seconda ai "lavoratori remoti". Mi chiedo quali "lavoratori remoti" si possano leggere il malloppo tecnico di 44 pagine proposto dal NIST.

Io sono un estimatore delle SP del NIST: chiare ed esaustive. Purtroppo negli ultimi anni non posso aggiungere l'aggettivo "sintetiche".

Intendiamoci: sono ottime per chi non conosce l'argomento. Ma chi lo conosce già, e vorrebbe verificare la completezza delle proprie competenze, è costretto ad affrontare un testo molto didattico e poco sintetico (e anche i "riassumento" sono un po' troppo verbosi).

Comunque sia, chiunque si occupa di sicurezza delle informazioni dovrebbe leggerle.

****

08- NIST e l'autenticazione via SMS

Da Crypto-gram di Bruce Schneier leggo che il NIST ora "depreca" l'uso degli SMS per l'autenticazione a due fattori nella bozza della nuova versione della SP 800-63:
- https://pages.nist.gov/800-63-3/sp800-63b.html.

Nella newsletter Bruce Schneier fornisce alcuni link ad alcuni articoli:
- https://techcrunch.com/2016/07/25/nist-declares-the-age-of-sms-based-2-factor-authentication-over/;
- http://www.eweek.com/security/nist-says-sms-based-two-factor-authentication-isnt-secure.html;
- https://threatpost.com/nist-recommends-sms-two-factor-authentication-deprecation/119507/;
- http://fortune.com/2016/07/26/nist-sms-two-factor/.

Alcuni di questi articoli citano come alternative (ma dovrei capire meglio quanto sono ancora in fase di studio) il Code Generator di Facebook o il Google Authenticator o il Google Promt. Ovviamente ci sono anche il RSA SecurID (con token o meno), i dongle (un po' difficili da usare sui dispositivi mobili) e le caratteristiche biometriche (anch'esse difficili da usare su molti dispositivi).

Vedremo. Per intanto è brutto vedere che una misura di sicurezza che positivamente ma lentamente si stava diffondendo è già obsoleta.

****

09- Cambiare password è improduttivo

Avevo già segnalato un articolo contrario al troppo frequente cambio di password.

Ma in agosto Bruce Schneier ha asserito che è una cosa che dice da anni e segnala il seguente articolo:
- http://arstechnica.com/security/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/.

Io lo dico solo da qualche mese, ma penso sia il caso di rifletterci.

Ovviamente, le password che non si cambiano devono essere accompagnate da meccanismi quali: blocco (o allarme che si possa distinguere dal phishing) dopo pochi tentativi sbagliati, lunghezza di almeno 16 caratteri, complessità elevata.

****

10- Schneier e IoT

Trovo sempre piacevole leggere Bruce Schneier. Questo è un suo articolo sui rischi dell'Internet of Things:
- https://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster.

Credo dica cose originali e interessanti. Certamente ignorate dai produttori e utilizzatori di dispositivi (anche se non capisco perché entusiasmarsi per una lavatrice che posso governare a distanza).

PS: Pier Francesco Massida su LinkedIn mi ha fatto notare come i rischi dell'IoT siano al centro del nuovo romanzo giallo di Jeffrey Deaver "The steel kiss". Non apprezzo molto Deaver (indulge in troppi finti finali), ma apprezzo il fatto che abbia colto il problema.