Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – FEBBRAIO 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- Privacy, timbrature e GPS

Ringrazio Pierfrancesco Maistrello di Vecomp per avermi segnalato questo recente Provvedimento del Garante dal titolo "Verifica preliminare. Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone per finalità di rilevazione delle presenze":
- http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/5497522.

In poche parole, il Garante ha autorizzato l'uso di un sistema alternativo al cartellino per la rilevazione presenze di dipendenti e collaboratori: la persona usa una app dello smartphone per selezionare "entrata" e "uscita"; la app, con il GPS, registra anche la posizione della persona, in modo da verificare che la segnalazione avvenga veramente sul posto di lavoro.

La sentenza è interessante perché stabilisce alcune misure da considerare: aggiornamento dell'informativa, rapporti con il fornitore, tempi di conservazione dei dati (5 anni per le timbrature, il minimo indispensabile per la posizione), la notifica al Garante stesso.

****

02- Privacy: Codice deontologico per informazione commerciale

Segnalo che il Garante privacy ha pubblicato il "Codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale":
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4298343.

Questo codice deontologico copre un'area non ancora trattata nell'ambito delle comunicazioni commerciali e di marketing, ossia il caso in cui i dati personali siano stati forniti direttamente dagli interessati, magari nell'ambito di altre operazioni.

****

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

Avevo dato notizia del Provvedimento del Garante privacy che trattava, tra gli altri, degli "strumenti per rendere la prestazione lavorativa":
- http://blog.cesaregallotti.it/2016/09/garante-privacy-e-strumenti-per-rendere.html.

Mi è arrivata notizia della disponibilità del materiale dell'incontro organizzato da Tech & Law Center dal titolo "Controllo del lavoratori, cyber espionage e tutela del segreto industriale":
- http://techandlaw.net/ita-13-settembre-2016-controllo-del-lavoratori-cyber-espionage-e-tutela-del-segreto-industriale/.

Io ho apprezzato soprattutto il materiale di Jacopo Giunta.

Quando diedi la notizia, commentai il punto relativo agli "strumenti per rendere la prestazione lavorativa". Su questo ho scambiato delle opinioni con Giuseppe Bava di Data Management.

Giuseppe intanto mi ha segnalato che il Provvedimento ricorda anche che:
- l'indirizzo MAC è da ritenersi una dato personale;
- le strutture IT non devono memorizzare dati senza finalità precise e plausibili e non devono conservarli per un tempo troppo lungo.

Ma alla fine abbiamo convenuto che sarebbe auspicabile che il Garante aggiorni le Linee guida sull'uso dell'email e Internet sul posto di lavoro, in modo da fornire ulteriore chiarezza sul tema.

****

04- Wi-fi pubblico e responsabilità

Segnalo questo articolo dal titolo auto-esplicativo "Chi offre al pubblico un servizio Wi-Fi gratuito non è responsabile per le attività degli utenti":
- http://www.filodiritto.com/articoli/2016/10/chi-offre-al-pubblico-un-servizio-wi-fi-gratuito-non-e-responsabile-per-le-attivita-degli-utenti.html.

Si tratta di una decisione recente della Corte di Giustizia dell'Unione Europea.

****

05- Analisi del nuovo CAD

Segnalo questa serie di articoli del Forum PA dal titolo "Dossier: Speciale Cad. Inizia la fase attuativa, l'analisi di FPA e dei nostri esperti":
- http://www.forumpa.it/speciale-cad-inizia-la-fase-attuativa-lanalisi-di-fpa-e-dei-nostri-esperti.

Segnalo anche questo articolo sul nuovo CAD (grazie a Franco Ferrari di DNV GL):
- http://www.agendadigitale.eu/egov/c-era-una-volta-la-pec-la-norma-cad-la-svaluta_2526.htm.

Andrea Caccia riassume le ragioni delle modifiche al Codice dell'amministrazione digitale (CAD) e si concentra sul futuro della PEC.

****

06- Standardizzazione: ISO 37001 sui sistemi anti frode

Massimo Cottafavi di SNAM mi informa della pubblicazione della ISO 37001:2016 dal titolo "Anti-bribery management systems - Requirements with guidance for use":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=65034.

Al momento non ne so altro se non quanto riportato da questo post su LinkedIn (sempre segnalato da Massimo):
- https://www.linkedin.com/pulse/pubblicata-la-norma-iso-370012016-diretta-streaming-di-ciro-strazzeri.

****

07- Assicurazioni sulla sicurezza ICT

Segnalo questo articolo dal titolo "Le nuove polizze di copertura assicurativa sul Cyber Risk":
- www.altalex.com/documents/news/2016/09/23/le-nuove-polizze-di-copertura-assicurativa-sul-cyber-risk.

Sono sempre perplesso in merito a questo tipo di assicurazioni, e ne ho già scritto in passato (http://blog.cesaregallotti.it/2016/03/studio-sulle-assicurazioni-informatiche.html, http://blog.cesaregallotti.it/2015/12/lo-stato-delle-cyber-assicurazioni.html, http://blog.cesaregallotti.it/2015/10/assicurazione-si-rifiuta-di-pagare-dopo.html, http://blog.cesaregallotti.it/2014/07/le-assicurazioni-relative-agli.html e http://blog.cesaregallotti.it/2012/08/assicurazioni-e-sicurezza-informatica.html).

Questo articolo ha il pregio di presentare degli esempi reali di polizze (anche se mi pare di vedere anche un po' di pubblicità).

****

08- Vendor Security Alliance

Da Dark Reading Weekly leggo che società come Uber, Dropbox e Twitter hanno costituito la Vendor Security Alliance (VSA):
- http://www.darkreading.com/vulnerabilities---threats/vulnerability-management/uber-dropbox-other-tech-leaders-team-up-to-boost-vendor-security-/d/d-id/1326926?.

L'idea sembrava buona, ma poi leggo che "ogni anno, VSA collaborerà con degli esperti per pubblicare un questionario in modo che le società possano determinare il proprio livello di rischio".

Un altro questionario? Ancora? Secondo me, non servirà a niente. Però potremo leggerlo dal 1 ottobre sul loro sito:
- https://www.vendorsecurityalliance.org/.

Dico questo perché non è il fornitore che deve valutare il proprio livello di rischio, ma sei tu che devi valutarlo e sulla base di questo stabilire le misure di sicurezza da chiedere ai fornitori. E quindi non bisogna inviare un questionario ai fornitori, ma istruzioni precise, e poi agire opportunamente (cambiando il fornitore, dando al fornitore il tempo di adeguarsi, accettare la situazione) nel caso il fornitore non attui quanto richiesto.

****

09- NIST e l'autenticazione via SMS - Precisazioni

Giampiero Raschetti della Banca Popolare di Sondrio mi ha scritto in merito al post che segnalava che il NIST ora "depreca" l'uso degli SMS per l'autenticazione a due fattori nella bozza della nuova versione della SP 800-63. Il mio post:
- http://blog.cesaregallotti.it/2016/08/nist-e-lautenticazione-via-sms.html.

Giampiero mi ricorda che il testo del NIST "depreca" l'uso di SMS o voce attraverso rete PSTN, vista la sua vulnerabilità. Se non capisco male, quindi, l'uso di SMS via GSM non è da scoraggiare.

Giampiero mi ricorda i rischi relativi all'utilizzo di SMS via cellulare, che sono comuni a tutti gli strumenti di autenticazione a due fattori basati su dispositivi mobili, inclusi dunque anche OTP di qualsivoglia natura.

Lo ringrazio per la precisazione.

****

10- Misure minime di AgID per la PA

Più di uno (cito Pierfrancesco Maistrello di Vecomp, ma anche la mailing list di sikurezza.org e Franco Ferrari di DNV GL) mi hanno segnalato la pubblicazione delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" dell'AgID:
- http://www.agid.gov.it/notizie/2016/09/26/misure-minime-sicurezza-informatica-pubbliche-amministrazioni.

Le ho lette e non mi sono piaciute. Innanzi tutto perché sono ricavate dal Cyber Security Framework (CSF) del NIST, su cui ho già espresso delle perplessità. Poi perché ritengo che queste "misure minime" siano un riassunto mal fatto dei controlli del CSF.

Infatti, come mi dice Pierfrancesco:
1- queste misure minime non sono veramente "minime" e contengono cose oggi irrealizzabili (e, aggiungo io, forse inutili) come il DLP;
2- propone una valutazione delle misure per un livello "minimo", "standard" e "alto" senza indicare esattamente come stabilirlo.

Infine io aggiungo una cosa già detta tempo fa: negli anni, con fatica, la Pubblica amministrazione si è avvicinata alla ISO/IEC 27001; non capisco che senso abbia aggiungere un altro schema.

****

11- IoT Security framework

Dal SANS NewsBites del 20 settembre trovo la notizia che il Industrial Internet Consortium (IIC) ha pubblicato un Industrial Internet Security Framework (IISF). Questo documento riporta indicazioni per sviluppatori e utenti.

Il documento lo trovate qui:
- http://www.iiconsortium.org/IISF.htm.

Ho cominciato a leggerlo, ma l'ho trovato molto verboso e con poche indicazioni veramente pratiche. Vedo anche molti controlli "organizzativi" (politiche, processi). Intendiamoci: il documento è pieno di spunti interessanti, ma una maggiore sintesi e schematicità avrebbe giovato.

****

12- Neuroscienza e leadership

Ho avuto modo di leggere sul numero Q3 2016 di "Continuity", rivista del BCI, due articoli interessanti:
- The neuroscience of crisis leadership;
- Making the call.

Li segnalo perché mettono in ordine gli errori più frequenti che facciamo, non necessariamente in occasione di crisi:
- atteggiamento di attacco e difesa per paura di sbagliare;
- incapacità di prendere decisioni perché la realtà è troppo diversa da quanto previsto;
- impulsività, che è certo utile, ma deve essere mitigata dal calcolo;
- cattiva comunicazione.

Il secondo articolo elenca un insieme alternativo di errori personali:
- pregiudizio causato dalle aspettative (expectancy bias);
- pregiudizio orientato alla conferma (confirmation bias);
- decisioni prese sulla base di quanto già nelle nostre menti (availability heuristic);

e di gruppo (ricerca del consenso, sottovalutazione dei meno esperti, carisma di un leader).

Per leggere questi articoli (e anche altri, che però mi sono sembrati meno interessanti), è necessario scaricare il pdf della rivista da questa pagina:
- http://www.thebci.org/index.php/continuity.

****

13- Report semestrale Cisco sulla sicurezza

Segnalo il "Report semestrale sulla cybersecurity 2016" di Cisco del luglio 2016 (mi diverto a segnalare che la data è solo nell'ultima pagina):
- http://www.cisco.com/c/m/it_it/offers/sc04/2016-midyear-cybersecurity-report/index.html.

Nulla di nuovo, molto tecnico e con qualche pubblicità. Però ritengo sia fatto bene e vale la lettura. Ho trovato particolarmente interessante le pagine dal titolo "Gli attacchi di ransomware nella sanità servono da lezione per tutti i settori" e "Consigli per la sicurezza": due brevi riassunti delle vulnerabilità e delle azioni più importanti.