Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – MARZO 2017
****

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- Aggiornamento libro "Sicurezza delle informazioni"

Ho aggiornato il mio libro "Sicurezza delle informazioni". Maggiori dettagli si trovano in questa pagina: http://www.cesaregallotti.it/libro.html.

Segnalo che le modifiche non sono molto numerose. Ho ovviamente aggiornato i riferimenti alla normativa privacy e al Regolamento eIDAS e ho introdotto qualche nuovo esempio. Tutte le modifiche sono comunque frutto di aggiornamenti che ho segnalato sul blog e sulla newsletter.

In altre parole: se avete già comprato una copia della precedente edizione, oltre a ringraziarvi, vi invito a non acquistare la nuova edizione. A meno che non vogliate avere la mia foto del Perito Moreno (ma in quel caso vi prego di scrivermi e ve la mando).

Per questa edizione ringrazio Pierfrancesco Maistrello e Francesca Lazzaroni per una rilettura delle bozze e i loro suggerimenti. Ancora di più ringrazio Stefano Ramacciotti, che anche per questa edizione si è prodigato di consigli e suggerimenti (oltre a continuare a regalarmi l'appendice sui Common Criteria e altre parti di testo).

****

02- Privacy e accessi degli AdS

Pierfrancesco Maistrello (ormai mio spacciatore ufficiale di novità dal Garante) mi ha segnalato questa "Ordinanza di ingiunzione nei confronti di Planetel s.r.l. - 22 dicembre 2016": http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/6032975.

Il punto importante riguarda una prassi solitamente seguita per l'autenticazione degli AdS, ossia: accesso con credenziali personali ad un desktop remoto, successivo accesso con credenziali condivise al sistema da amministrare. Questa prassi si basa sul fatto che l'accesso al desktop remoto permette di risalire a chi è poi acceduto ai sistemi con credenziali condivise (in modo simile al comando "su" dei sistemi Unix e Linux).

Il Garante ha detto che questa prassi non è conforme alle misure minime.

Scrive Pierfrancesco: "Servirà a convincere i, tuttora molti, riottosi all'assegnazione univoca di credenziali amministrative?". Non saprei rispondergli.

L'ordinanza riporta altre violazioni, a mio parere meno interessanti e quindi non le evidenzio in questa occasione.

****

03- Privacy: Provvedimento su trattamenti dati sul posto di lavoro

Interessante Provvedimento del Garante privacy del 22 dicembre: http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/5958296.

Un ex dipendente di una società ha fatto reclamo per trattamento non idoneo dei dati personali.

Ecco alcune lezioni che ne ho tratto:
- quando qualcuno lascia la società, la casella di email va disabilitata senza permettere la ricezione e l'invio di messaggi;
- conservare le email per 10 anni è eccessivo, a meno che non tale termine non sia giustificato (in generale, però, andrebbe sempre giustificato il tempo di conservazione, anche se di molto inferiore ai 10 anni);
- se la Capogruppo gestisce servizi informatici per tutte le società del Gruppo, tali società devono nominare Responsabile la Capogruppo.

****

04- Privacy, call centre e protezionismo

Pierfrancesco Maistrello mi ha segnalato anche questa. La legge di stabilità 2017 cerca di proteggere i call centre italiani. Per questo anche il Garante privacy ha aumentato le pratiche burocratiche per lo spostamento dei call centre all'estero.

Un articolo in merito alle novità sui call centre:
http://www.publicpolicy.it/analisi-%e2%80%8bcall-center-privacy-protezionista-lavoratori-67376.html.

La nota informativa del Garante privacy "Nuove disposizioni normative concernenti le attività di call center":
http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/6029202.

****

05- Norma italiana per DPO

Mi informa Fabio Guasconi che è in fase di inchiesta pubblica la bozza di norma tecnica UNI/UNINFO che definisce i profili e le competenze dei professionisti che lavorano nella privacy, inclusi quindi DPO:
http://www.uni.com/index.php?option=com_content&view=article&id=5802:data-protection-officer-finalmente-uno-schema-per-la-certificazione-unificato-e-non-solo&catid=171&Itemid=2612.

Scadenza: 25 marzo.

****

06- Diritto d'autore e produzione software

Una vera coincidenza: la sera un cliente mi chiede informazioni sul diritto d'autore del software prodotto dal personale e il mattino dopo la newsletter di Filodiritto riporta una sentenza proprio su questo argomento:
http://www.filodiritto.com/articoli/2017/03/a-chi-spetta-il-diritto-di-sfruttamento-economico-del-software-il-caso-del-software-commissionato-da-una-societa-ad-un.html.

Mi sembra molto chiaro e quindi lo segnalo.

****

07- Imprese: informazioni di carattere non finanziario

Il Decreto legislativo 254/2016 riguarda la comunicazione di informazioni di carattere non finanziario e sulla diversità. Esso recepisce la direttiva 2014/95/UE riguardante la comunicazione di informazioni di carattere non finanziario di imprese e gruppi di grandi dimensioni.

La Fondazione nazionale dei commercialisti ha pubblicato una panoramica di queste nuove disposizioni:
http://www.fondazionenazionalecommercialisti.it/node/1201.

La materia mi è largamente ignota. Capisco che la normativa richiede di pubblicare informazioni: di carattere ambientale, di carattere sociale, inerenti alla gestione del personale, inerenti alla tutela dei diritti umani, riguardanti la lotta contro la corruzione. E quindi tutto ciò non è pertinente alle materie di cui mi occupo.

Però... magari in questo documento potrebbero trovare posto considerazioni sulla qualità, la sicurezza delle informazioni e i processi del sistema di gestione. Viceversa, da un documento così si potrebbero ricavare informazioni utili per l'analisi dei "rischi e opportunità" richiesti dagli standard ISO. E forse questo può rendere l'adozione degli standard ISO ancora meno formale e più pratica.

Queste sono solo riflessioni personali. Se altri possono fornire contributi, ne sarò lieto.

****

08- Linee guida ENISA per la valutazione del rischio per le PMI

Pierfrancesco Maistrello mi ha segnalato le "Guidelines for SMEs on the security of personal data processing" di ENISA:
https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing.

Presenta un metodo semplificato di valutazione del rischio per il trattamento dei dati personali. Ritengo sia da considerare anche per altre finalità, come per esempio la certificazione ISO/IEC 27001 (in altre parole, mi sembra un metodo ancora più semplice del mio VERA).

Inoltre ENISA elenca un insieme di contromisure, tratte dalla ISO/IEC 27001, da attuare per il controllo del rischio.

Forse l'ho già detto, ma lo ripeto: mi pare che ENISA stia facendo quello che il NIST ha smesso di fare, ossia scrivere documenti semplici ma pragmatici e rigorosi.

****

09- Linee guida ENISA per la sicurezza dei Digital Service Providers

ENISA ha pubblicato un documento dal titolo "Technical Guidelines for the implementation of minimum security measures for Digital Service Providers":
https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/.

La pagina di presentazione è:
https://www.enisa.europa.eu/news/enisa-news/security-measures-for-digital-service-providers.

Mi sembra ben fatto e di facile lettura. Forse ENISA sta facendo quello che il NIST ha smesso di fare, ossia documenti di semplice lettura.

Forse non sentivo la mancanza di un altro documento con le misure di sicurezza.

Da un tweet di @Silvia_Mar_

****

10- Certificazione conservatori (nuove regole)

Accredia ha pubblicato le nuove regole per la certificazione dei conservatori: http://www.accredia.it/extsearch_documentazione.jsp?area=55&ID_LINK=331&page=113&IDCTX=5418&id_context=5418.

Rispetto alle precedenti regole, le giornate si sono ridotte arrivando, in prima certificazione, a circa 8 (prima erano 13 o 11). Preferisco non commentare.

Non sono invece state fornite le scadenze entro le quali vanno effettuate le verifiche secondo il nuovo schema. Tali informazioni dovranno essere comunicate da Agid.

Grazie a Simona Montinari di DNV GL per la segnalazione.

****

11- Controlli Essenziali di Cybersecurity

Stefano Ramacciotti mi ha segnalato la pubblicazione di CINI dal titolo "2016 Italian Cybersecurity Report: Controlli Essenziali di Cybersecurity" che si può scaricare da qui: http://www.cybersecurityframework.it/.

Non mi sembra male, anche se ho sempre delle riserve per chi promuove uno schema made in USA al posto di uno di livello internazionale (le ISO/IEC 27001, come invece fa ENISA) e per chi usa il termine "cibernetica" in modo scorretto.

Altra perplessità: sullo stesso sito si fa riferimento alle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni", pubblicate di recente, che sono diverse dai "Controlli essenziali". Il tutto mi sembra possibile fonte di confusione.

Comunque, se questa iniziativa può servire a migliorare la cultura in materia di sicurezza, ben venga.

****

12- Le 7 tecniche di attacco più pericolose

Il titolo è decisamente troppo enfatico. È una proposta del SANS, presentata a RSA 2017, di lista: https://www.sans.org/the-seven-most-dangerous-new-attack-techniques.

Questa lista diventerà famosa oppure no? Per intanto, elenco gli attacchi:
- ransomware;
- uso del IoT per gli attacchi;
- ransomware per IoT (ti bloccano l'automobile e tu devi pagare per sbloccarla);
- attacchi ai sistemi industriali di controllo (ICS);
- compromissione dei canali cifrati a causa di deboli generatori di numeri casuali;
- attacchi dovuti all'uso di servizi web esterni usati come componenti software;
- attacchi ai database noSQL.

E quindi cosa fare? Non lo dicono.

****

13- Configurare il browser in modo sicuro

Questa pagina (da un retweet di @pstirparo) di istruzioni su come configurare il browser per una navigazione sicura mi sembra interessante:
https://gist.github.com/atcuno/3425484ac5cce5298932.

Mi pare possa essere utile da segnalare quando qualcuno mi chiede come configurare un pc.

****

14- BCI Horizon Scan 2017

Inizio anno, tempo di rapporti sulla sicurezza, con tutti i loro punti positivi e negativi. L'Horizon Scan è quello del BCI:
- http://www.thebci.org/index.php/download-the-horizon-scan-2017.

Trovo ci siano troppe minacce informatiche per essere un rapporto non solo di tipo informatico.