Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS - MARZO 2013

****

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 disiscriversi
- 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 - Novità: CAD e firma elettronica

La newsletter di DFA segnala questo articolo sulle novità introdotte nel CAD dal Decreto Sviluppo bis (DL 179 del 2012, convertito in Legge con modificazioni dalla L 221 del 2012):
- http://www.blogstudiolegalefinocchiaro.it/documento-informatico-e-firma-digitale/firma-elettronica-avanzata-rilevanti-novita-nel-d-l-sviluppo-bis/

Le novità segnalate sono due:
- adeguamento delle modalità con cui è possibile disconoscere la firma elettronica avanzata, in modo da considerare anche tecnologie quali la firma grafometrica su tavoletta

- l'estensione della validità della firma elettronica al posto di quella scritta per atti e contratti (con esclusione dei contratti aventi oggetto beni immobili).

L'articolo si conclude ricordando che l'aggiornamento delle regole tecniche, previsto per metà 2012, non è ancora stato pubblicato.

****

02- Legale - Novità: Ispezioni privacy agli operatori TLC

Agostino Oliveri mi ha segnalato la notizia del Garante dal titolo "Privacy: operazione Data Retention":
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2300180

La notizia presenta un breve resoconto sulle ispezioni della Guardia di Finanza in tutta Italia sul rispetto delle norme per la conservazione dei dati di traffico telefonico e telematico presso gli operatori TLC.

La sintesi è questa: in 9 casi (su 11) sono state accertate e contestate violazioni relativamente alla conservazione dei dati di traffico oltre i termini previsti, alla mancata adozione delle misure minime di sicurezza, e alla mancata adozione di alcune delle ulteriori misure di protezione prescritte dal provvedimento del Garante, quali l'uso di tecnologie di riconoscimento biometrico per selezionare l'accesso ai dati e la cifratura dei dati.

Mi sarebbe piaciuto avere maggiori dettagli sulle misure minime non adottate.

****

03- Legale - Novità: Repertorio delle normative sull'amministrazione digitale

Giovanni Francescutti mi segnala il sito di Digit@LEX "Tutte le Leggi sull'Amministrazione Digitale a portata di click":
- http://www.digita-lex.it/

Ho navigato un poco nel sito e bisogna dire che riporta moltissime cose e gli argomenti sono classificati in categorie.

Visto che sono sempre sospettoso dei siti realizzati da privati perché, in alcuni casi, dopo l'entusiasmo iniziale, gli aggiornamenti sono meno puntuali, raccomando di fare controlli incrociati con www.normattiva.it e il sito dell'AgID (www.digitpa.gov.it).

****

04- Legale - Novità: Siti web e dati societari

La notizia è vecchia e nota ed ero convinto di averla già pubblicata. Non trovandola tra i miei articoli, la scrivo ora.

Sui siti web (spazi elettronici destinati alla comunicazione collegati ad una rete telematica ad accesso pubblico) delle società soggette all'obbligo dell'iscrizione nel registro delle imprese (s.p.a., s.r.l. e s.a.p.a.), devono essere riportati:
- sede legale
- ufficio del registro delle imprese presso il quale la società è iscritta
- il numero d'iscrizione (ossia la partita IVA)
- capitale della società (somma effettivamente versata)
- se il socio è unico

Questo in virtù dell'articolo 2250 del Codice Civile, così come modificato dall'articolo 42 della Legge 88 del 2009.

****

05- Legale - Sentenze: Raccolta prove digitali - Un altro ricorso vinto

Dalla newsletter di DFA, rilancio un link ad un recente (ottobre 2012) provvedimento del Garante Privacy:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2149222

Ancora una volta, un'impresa si è dedicata ad effettuare analisi forensi di un pc di un dipendente, senza aver in precedenza pubblicato un disciplinare che riportasse i suoi poteri di controllo sui pc del personale.

****

06- Legale - Sentenze: Diffamazione su Facebook - Condanna

Questo articolo della associazione CINDI mi pare interessante:
- https://associazionecindi.wordpress.com/2013/02/28/diffamazione-facebook-giplivorno/

In realtà, si tratta di un argomento già noto: la diffamazione su un social network aperto al pubblico è vietata. Questa volta l'ha ribadito il GIP di Livorno.

Capisco che in quest'epoca in cui le modalità di comunicazione stanno cambiando, non tutti acquisiscono la corretta sensibilità su come usare certi mezzi. Ma anche prima di Internet, parlar male di qualcuno chiacchierando con qualche amico non aveva le stesse conseguenze dello scrivere male di qualcuno su uno o più manifesti affissi per strada.

****

07- Legale - Sentenze: UE - Rivendita online di licenze software

Dalla newsletter Ictlex-news, segnalo la seguente sentenza della Corte di Giustizia UE: una volta "venduto" un software via Internet ad un cliente, questi può a sua volta cedere la licenza a qualcun altro (ovviamente senza trattenere una copia del software per se) senza violare la legge sul diritto d'autore né i diritti del produttore.

Per chi vuole approfondire:
- http://www.ictlex.net/?p=1430

****
08- Legale: Privacy e AdS applicativi - Parte 2

Dopo l'articolo dal titolo "Privacy e AdS applicativi" in cui si riportavano le parole (verbali) di un rappresentante dell'ufficio del Garante in merito alle utenze applicative con poteri di amministrazione, Massimo Cottafavi di Reply mi ha segnalato un problema di interpretazione.

Come sappiamo, il Provvedimento sugli amministratori di sistema era seguito da delle FAQ. La FAQ 22 dà ragione all'interpretazione riportata:
- D: È corretto affermare che l'accesso a livello applicativo non rientri nel perimetro degli adeguamenti, in quanto l'accesso a una applicazione informatica è regolato tramite profili autorizzativi che disciplinano per tutti gli utenti i trattamenti consentiti sui dati?
- R: Si. L'accesso applicativo non è compreso tra le caratteristiche tipiche dell'amministratore di sistema

Evidentemente, visto che si tratta di un allegato al provvedimento sugli amministratori di sistema, è lecito esplicitare ulteriormente così: "L'accesso applicativo, *anche di power user*, non è compreso tra le caratteristiche tipiche dell'amministratore di sistema".

Però Max fa notare che questo è smentito dalla FAQ 1: "l'amministratore di sistema è assunto quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi [...] i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni".

Quando un'applicazione diventa complessa e quindi i suoi AdS sono da considerare AdS? Se un power user pasticcia con le utenze di un sistema Zucchetti per medie imprese non viene registrato, mentre quello del SAP sì?

I dubbi permangono, quindi.

L'articolo precedente:
- http://blog.cesaregallotti.it/2013/02/privacy-e-ads-applicativi.html

****

09- Legale: Google e privacy

Enzo Ascione di Intesa Sanpaolo, mi ha inviato questo articolo dal titolo "Google, Garanti Privacy Ue pronti ad azione repressiva":
- http://www.corrierecomunicazioni.it/it-world/19711_google-garanti-privacy-ue-pronti-ad-azione-repressiva.htm

Io continuo a temere questi fornitori di servizi, come ho già avuto modo di dire:
- http://blog.cesaregallotti.it/2013/01/google-le-password-e-i-token.html
- http://blog.cesaregallotti.it/2013/01/accordi-con-i-servizi-esterni-cloud-e.html

****

10- Tecnologia: Decalogo contro il phishing

L'associazione CINDI ha pubblicato un decalogo per proteggersi dal phishing:
- https://associazionecindi.wordpress.com/2013/01/23/phishing-postepay-regole-condott/

Lo trovo molto utile.

Alcuni elementi possono anche sembrare banali per chi si occupa di queste cose, ma sappiamo bene che non è così per tutti.

Visto che è facile dire cosa manca in un decalogo, lo faccio: avrei aggiunto "non cliccate mai su un link di una mail della vostra banca o carta di credito: scrivetelo ogni volta nella barra degli indirizzi".

****

11- Tecnologia: Programmare in... sicurezza

Dal Clust Group di LinkedIn, ho trovato la segnalazione di un articolo dal titolo "Programmare in... sicurezza":
-
http://programmazione.it/index.php?entity=eitem&idItem=48588&goback=.gde_54878_member_215687034

L'ho trovato molto interessante e ho trovato ancora più interessante l'articolo in inglese "Safeguard your code: 17 security tips for developers":
- https://www.infoworld.com/d/application-development/safeguard-your-code-17-security-tips-developers-211339?page=0,0

Ecco i titoli, ma vale la pena leggere tutto:
- 1: Test inputs rigorously
- 2: Store what you need, and not one bit more
- 3: Avoid trusting passwords more than necessary
- 4: Negotiate requirements
- 5: Add delays to your code
- 6: Use encryption more often than you think you should
- 7: Build walls
- 8: Tested libraries -- use them
- 9: Use internal APIs
- 10: Bring in outside auditors to critique your code

- 11: Code analyzers are your friend (con segnalato uno strumento)
- 12: Limit privilege
- 13: Model your threat
- 14: Trust goes both ways
- 15: Keep apprised of the latest threats
- 16: Deep research can pay off
- 17: Educate yourself

Come si vede, si tratta di suggerimenti tecnologici ben noti, di trucchi del mestiere e di pratiche organizzative. Quanti programmatori non seguono neanche una mailing list, quanti responsabili di progetto non hanno il coraggio di negoziare i requisiti!

****

12- Tecnologia: Errori di configurazione del Cisco IOS

Sul Clusit Group di LinkedIn, Aldo Ceccarelli ha segnalato un link ad un articolo dal titolo "Top 10 Cisco IOS Configuration Mistakes":
- http://www.petri.co.il/cisco-ios-configuration-mistakes.htm

Capisco che la configurazione di un firewall non è materia per principianti, ma mi chiedo come si possa immettere sul mercato (e vendere a caro prezzo) prodotti che hanno meccanismi che non richiedono la conferma della password, Telnet di default al posto di SSH, parametri di sicurezza SNMP minimali.

E dire che poco fa mi lamentavo della poca professionalità di troppi sviluppatori!

Voglio sperare che l'articolo si riferisca a prodotti ormai obsoleti.

****

13- Attacchi: Attacco al sito web del Tribunale di Milano

Sandro Sanna mi ha segnalato il giorno dopo l'accaduto del web defacing del sito del Tribunale di Milano il 15 febbraio:
- http://www.ansa.it/web/notizie/rubriche/cronaca/2013/02/16/Attacco-hacker-sito-tribunale-Milano_8259442.html

Volevo trasmettere la notizia solo perché io sono di Milano. In realtà, casi del genere capitano molto spesso e riguardano i soli siti web delle vittime: il minimo previsto quando si sviluppa un'architettura informatica è separare molto bene il server del sito web da quelli degli altri servizi; apparentemente, anche il Tribunale di Milano ha fatto così, anche se non ho trovato approfondimenti successivi il 17 febbraio.

C'è chi manifesta legalmente in piazza o su Internet e c'è anche chi manifesta illegalmente. Questa volta, facendo danni molto limitati e ottenendo un certo ritorno di immagine.

****

14- Attacchi: Backdoor (sui prodotti Barracuda)

La notizia è ormai vecchia di un mese, ma la riporto brevemente: diversi prodotti della Barracuda Network (firewall, VPN, filtri antispam) hanno una backdoor non documentata che permette l'accesso a degli apparati da remoto.

Questo è l'articolo segnalato da Crypto-Gram (ma ce ne sono molti altri):
- http://arstechnica.com/security/2013/01/secret-backdoors-found-in-firewall-vpn-gear-from-barracuda-networks/

Non sorprendiamoci troppo: basta andare in quasi qualunque reparto IT per vedere come la mentalità dell'artigiano (contrapposto, mi si perdoni, al "professionista") sia prevalente e come l'unica e sola guida sia il fatturato trimestrale.

****

15- Innovazione digitale (un caso pratico)

A pochi interesserà sapere che sono stato nominato Presidente di un seggio per le elezioni del 24 e 25 febbraio (a qualcuno in più interesserà sapere quanto si guadagna; non lo so; so che nel 2011, per 3 consultazioni e un totale di 7,5 giornate di lavoro ho guadagnato 340 Euro).

Fino al 2011, il Presidente di seggo riceveva una copia delle "Istruzioni per le operazioni degli uffici elettorali di sezione" almeno una settimana prima dell'inizio dei lavori, in modo che potesse prepararsi e garantire la speditezza delle operazioni.

Quest'anno non mi è arrivato nulla; ho telefonato all'Ufficio elettorale e mi hanno risposto che ora le istruzioni non sono più distribuite con anticipo (immagino per risparmiare sui lavori dei messi comunali): posso scaricarle dal sito del Ministero degli Interni.

Credo di essere un caso che si trova a metà tra quelli che ci erano arrivati da soli (magari con Google) e quelli che si presenteranno ai seggi senza un minimo di preparazione (i Presidenti che non hanno mai fatto questo mestiere) o senza quel poco ma necessario ripasso (i Presidenti con esperienza) utili a garantire l'auspicata speditezza delle operazioni.

Tutto questo per dire che questa piccola storia mi ha permesso di ripassare una nota, ma spesso dimenticata, lezione: "prima di introdurre innovazioni, è necessario istruire gli utenti per tempo".

Un'altra lezione che ho ripassato: il termine "istruire" non implica presentazioni in Powerpoint o filmati o grossi manuali o chissà che altro; nel caso specifico bastavano due righe sottolineate sulla lettera di nomina ("Il Presidente può consultare le Istruzioni per le operazioni degli uffici elettorali di sezione disponibili sul sito xxx").

****

Cesare Gallotti
Ripa Ticinese 75
20143 Milano (Italia)
Tel: +39.02.58.10.04.21
Mobile: +39.349.669.77.23
Web: http://www.cesaregallotti.it
Blog: http://blog.cesaregallotti.it
Mail: cesaregallotti@cesaregallotti.it

Cesare Gallotti

PEC: cesaregallotti@mailcert.it