Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – GENNAIO 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: Documenti informatici nella PA - Dpcm del 13 novembre 2014

Segnalo questo articolo di Bancaforte che annuncia le regole tecniche per la gestione dei documenti informatici presso le pubbliche amministrazioni:
- http://www.bancaforte.it/notizie/2015/01/pa-18-mesi-per-dire-addio-alla-carta

Non credo aggiunga alcunché per chi non si occupa di Pubblica Amministrazione.

****

02- Legale: Lecito registrare il colloquio telefonico con il capo

Dal Gruppo infotechlegale.it di LinkedIn, inoltro la seguente notizia: secondo la Corte di Cassazione, la registrazione di un colloquio intercorsa tra due persone assurge al rango di prova se è posta in essere da uno dei soggetti coinvolti nella conversazione; il dipendente può registrare il colloquio ancor prima dell'instaurazione di un eventuale procedimento civilistico o penalistico a suo carico, essendo detta attività orientata precisamente all'acquisizione di prove a suo favore:
- http://www.studiocataldi.it/news_giuridiche_asp/news_giuridica_17238.asp

Sarebbe interessante leggere la sentenza completa per vedere quali principi sono richiamati e in che modo sono limitati. Purtroppo non l'ho trovata. L'unico commento che ho trovato online finora è proprio quello del link segnalato.

****

03- Legale: Home banking - responsabilità parziale in caso di attacco

Enzo Ascione di Intesa Sanpaolo mi ha segnalato questa notizia: per il tribunale di Caltanisetta, il fatto che l'accesso all'home banking avvenga "solo" tramite user-id e password (nonostante comunque l'istituto bancario abbia sollecitato ai clienti l'adozione di un meccanismo di OTP), fa sì che un accesso abusivo al sistema sia da ritenere colpa dell'istituto bancario perché avrebbe potuto anche mettere a disposizione un servizio di SMS o simile.

Questo se ho capito correttamente gli articoli relativi alla sentenza. Ne propongo due; nel secondo è possibile trovare un link alla sentenza completa:
- http://www.quotidianodiritto.ilsole24ore.com/art/amministrativo/2014-11-26/colpa-parziale-se-cliente-non-nota-l-hacker--194747.php?uuid=ABZqZXIC;
- http://www.creditofinanzanews.it/2014/12/03/home-banking-responsabilita-parziale-del-cliente-che-non-nota-lhacker/

Trovo un po' inquietante il fatto che il giudice dica che la banca (ossia il fornitore del servizio informatico) "non aveva dimostrato che il cliente non aveva custodito con diligenza le credenziali d'accesso". Però, ancora una volta, si tratta di una sentenza che ribadisce la necessità di predisporre servizi sicuri sia tecnicamente che funzionalmente.

****

04- Standard: ISO/IEC 90003:2014

Franco Ferrari del DNV GL mi ha segnalato la pubblicazione della nuova edizione della ISO/IEC 90003 dal titolo "Guidelines for the application of ISO 9001:2008 to computer software". L'introduzione segnala che questa nuova edizione nasce per allineare la norma alla ISO 9001:2008, mentre la precedente si basava sulla ISO 9001:2000.

Visto che tra le due edizioni della ISO 9001 non ci sono notevoli differenze, immagino che non siano state apportate modifiche rilevanti alla ISO/IEC 90003. Se qualcuno più attento di me vuole però segnalarmele, sarò ben contento di condividerle.

Mi lascia perplesso anche la scelta di pubblicare questa norma oggi, a meno di un anno dalla prevista pubblicazione della nuova ISO 9001. Solo per questo motivo vorrei ignorarla.

****

05- Contromisure: NIST SP 800-88 Guidelines for Media Sanitization

Il NIST ha pubblicato la prima revisione della guida 800-88, dedicata alla "cancellazione sicura":
- http://csrc.nist.gov/publications/PubsSPs.html#800-88

Il titolo esatto è "sanitizzazione" (treccani.it lo dà come sinonimo di "sanificazione", ma questo è derivato dall'inglese "sanification") e riguarda tutti i dispositivi (carta e altri supporti inclusi).

Devo dire: un po' deludente perché è indicato precisamente come fare la cancellazione dei cellulari (con tanto di sequenza di comandi da seguire sui vari sistemi disponibili), ma non quella degli hard disk o delle memorie USB: non fornisce alcun suggerimento sugli strumenti da utilizzare e segnala di seguire dei forum o dei siti nei quali non c'è nulla. Forse sono io che ho sbagliato a cercare?

Dall'altra parte, segnalo che la maggior parte delle volte indica come sufficiente una passata di zeri; altre volte suggerisce due o tre passaggi.

E se lo dice il NIST, forse è il caso che i fautori delle 7, delle 20 e delle 37 volte si aggiornino (anche perché quella non è più "cancellazione", ma "distruzione" del supporto; opzione comunque da scegliere nei casi di dati particolarmente critici; ma un buon martello è più economico, più veloce e spiritualmente più soddisfacente).

****

06- Sicurezza IT nel settore energia - 2

Dopo la precedente segnalazione su sicurezza IT nel settore energia (http://blog.cesaregallotti.it/2014/12/sicurezza-it-nel-settore-energia.html), Stefano Ramacciotti mi ha segnalato un altro documento interessante (fino a pagina 10; le ultime 4 pagine sono pubblicità), dicendo " mi sembrano una discreta introduzione alla problematica per non addetti ai lavori, considerando che in Italia quasi nemmeno ci si pensa":

- http://www.appliedelectronics.com/documents/Design_Considerations_Real_Time_Operating_Centers_White_Paper.pdf

Per chi non vuole scaricarsi direttamente il pdf, lo può trovare a questo link con il titolo "Design Considerations for Real-Time Operating Centers":
- http://www.appliedelectronics.com/technical-papers

****

07- Attacchi e contromisure: ENISA Threat Landscape of Internet Infrastructure

Dal gruppo Italian Security Professional di LinkedIn vedo la notizia della pubblicazione da parte di Enisa del "Threat Landscape and Good Practice Guide for Internet Infrastructure":
- https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/iitl

La segnalazione riporta anche il link ad un articolo riassuntivo:
- http://securityaffairs.co/wordpress/32258/security/enisa-threat-landscape-report.html

Ho trovato più interessante la tabella del capitolo 7 (molto tecnica) piuttosto che le recommendations: queste ultime ripropongono le solite cose (fate risk assessment, formate le persone, eccetera).

****

08- Attacchi: Una riflessione sull'attacco alla Sony

L'ultimo numero di Crpyo-Gram presenta numerose riflessioni sull'attacco alla Sony. La sostanza è ovvia: state attenti, perché tutti possono subire un attacco mirato, condotto da persone competenti.

Quello che più mi ha colpito è un'altra riflessione (si trova quasi al termine dell'articolo di cui fornisco il link poco oltre): i dati pubblicati riguardano i "normali" impiegati della Sony, non i top manager né altra gente importante. Questi impiegati si sono scambiati e-mail e informazioni tra loro con anche battute e barzellette discutibili e ora sono alla berlina. Quindi: quando usate i sistemi informatici, anche se non c'entrate niente e non siete l'oggetto di un attacco, potreste subirne le conseguenze. Quindi (ancora): siate prudenti anche nelle vostre attività individuali.

Il link:
- http://www.wsj.com/articles/sony-made-it-easy-but-any-of-us-could-get-hacked-1419002701.

****
09- Attacchi: Attacco ad una conduttura turca (nel 2008)

A dicembre è stato noto un incidente occorso nel 2008: dopo un'intrusione ai sistemi informatici, è stata elevata la pressione di una conduttura di petrolio e questo ha generato un'esplosione:
- http://www.bloomberg.com/news/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.html

Sembra possa essere stato un attacco da parte della Russia verso la Georgia (devono aver sbagliato qualche calcolo e l'attacco è avvenuto in Turchia) quando la tensione politica era elevata.

La notizia, che traggo dal SANS NewsBites, è interessante perché sembra che, per l'intrusione, sia stata sfruttata una vulnerabilità del sistema di controllo delle telecamere o di un sistema di allarme:
- http://www.federalnewsradio.com/489/3769859/DoJs-new-cybersecurity-office-to-aid-in-worldwide-investigations

Trovo interessanti queste notizie perché mi ricordano la "filiera di fornitura ICT": gli addetti del condotto non sono esperti di informatica e fanno installare i sistemi senza pensare alla sicurezza; gli installatori di sistemi di allarme e/o di telecamere si preoccupano solo che i propri sistemi funzionino (magari con qualche patch mancante al sistema operativo e/o qualche porta del firewall aperta senza necessità perché "non si sa mai" e "meglio non toccare"); gli sviluppatori dei software di allarme e di gestione delle telecamere sanno "programmare" in Java o simile, ma senza saper "programmare in sicurezza", visto che poi la responsabilità di "configurare" sta negli installatori; gli addetti agli acquisti forse hanno pensato alla parola "sicurezza" solo per la salute dei lavoratori (spero almeno questa) e al costo dell'offerta.

Chissà chi avranno trovato come capro espiatorio, anche se la colpa è di tutti.

****

10- Attacchi: Ricerca sulla criminalità informatica nelle PMI

Dalla mailing list di Sikurezza.org, segnalo questa ricerca dal titolo "La criminalità informatica e i rischi per l'economia e le imprese a livello italiano ed europeo". Non credo che aggiunga molto a quanto già si sa e a studi già noti (peraltro la ricerca, molto correttamente, li cita), ma fornisce qualche spunto di riflessione sulle nostre aziende.

La presentazione sulla pagina web è in inglese, mentre la pubblicazione e la presentazione sono in italiano:
- http://www.unicri.it/in_focus/on/Cybercrime_risks_economy