Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – GENNAIO 2014
****

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

****
00- Editoriale

Questo brevissimo editoriale per augurare a tutti un buon 2014, sperando anche di uscire dalla crisi economica e morale in cui siamo caduti in questi anni.

Io vedo anche crisi di segnalazioni e quindi vi invito a farmele: molte cose mi sfuggono.

Vi informo che ho deciso di inviare la newsletter dal mio indirizzo personale e professionale e non più dal “generico” 'IT Service Management News': ho scoperto che in molti non lo collegano a questa newsletter e la cestinano. Temo però che alcuni filtri antispam non apprezzino questa newsletter e la blocchino. Vedremo.

****

01- Standardizzazione: Annex SL o Annex JC o MSS HLS?

Come già detto altrove, la ISO ha promosso uno schema unico per scrivere gli standard relativi ai sistemi di gestione.

Al momento, sono stati pubblicati sei standard aderenti allo schema unico: ISO 30301, ISO 22301, ISO 20121, ISO 39001, ISO 14298 e ISO/IEC 27001. Nove standard sono in fase di redazione e aderenti allo schema: ISO 9001, ISO 14001, ISO 18420, ISO 19228, ISO 19600, ISO 21101, ISO 34001, ISO 37101, ISO 55001).

Lo schema unico ha un titolo: "High level structure, identical core text, common terms and core definitions" ed era parte dell'Annex SL delle "ISO/IEC Directives, Part 1 - Consolidated ISO Supplement — Procedures specific to ISO".

L'ISO/IEC ha emesso le nuove direttive del 2014 e l'Annex SL si chiama ora... Annex JC!

Ottimo... io l'ho sempre chiamato Annex SL, ma da oggi lo chiamerò, come fanno in molti, MSS HLS (Management system standards - High level structure), in modo che la prossima revisione delle direttive ISO non mi colga impreparato

****

02- Normativa: Privacy e call center extra-UE (riflessioni - parte 2 con errata corrige)

In merito ai call-center Extra-UE ho scritto un post e una riflessione nei mesi scorsi:
- http://blog.cesaregallotti.it/2013/10/privacy-e-call-center-extra-ue.html
- http://blog.cesaregallotti.it/2013/12/privacy-e-call-center-extra-ue.html

Giuseppe Bava di ASPErience mi ha fatto notare che ho fatto un errore e lo ringrazio.

In particolare, dicevo che il provvedimento si applica "a tutti i soggetti che svolgono in qualità di titolare del trattamento un'attività di call center in maniera prevalente". In realtà ciò non è vero.

Giuseppe mi ha segnalato che, nel Provvedimento, inizialmente il Garante richiama una circolare del Ministero del lavoro e delle politiche sociali, dedicata alle "aziende che svolgono in via assolutamente prevalente un'attività di call center", ma poi dice che le sue disposizioni sono rivolte a tutte le aziende, INDIPENDENTEMENTE dalla prevalenza o meno dell'attività di call center.

****

03- Minacce e attacchi: Microsoft Security Intelligence Report 15

Dal gruppo infotechlegale.it di LinkedIn vedo che Microsoft ha pubblicato il suo "Microsoft Security Intelligence Report", relativo al periodo gennaio-giugno 2013.

Come molti altri report, presenta molti esempi e casi registrati da Microsoft, con indicazioni su come sono stati trattati:
- http://www.microsoft.com/security/sir/default.aspx

****

04- Minacce e attacchi: Le backdoor dell'NSA

Volutamente, non ho quasi parlato del caso NSA. Già in troppi si sono dedicati. Bruce Schneier, purtroppo, non parla quasi d'altro. Però, questi due articoli del Der Spiegel segnalati dal gruppo Italian security professional di LinkedIn sono interessanti:
- http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html
- http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html

In pochissime parole, sembra che l'NSA disponesse di un gruppo (TAO), che a sua volta utilizzava le tecnologie messe a disposizione dal gruppo ANT, per compromettere qualsiasi tipo di dispositivo. In particolare, sembra che l'ANT avesse pubblicato un catalogo in cui apparivano più o meno tutte le marche dei prodotti di gestione delle reti informatiche.

Da una parte è certamente inquietante che i servizi di spionaggio degli USA possano accedere a qualsiasi tipo di dispositivo e intercettare quasi ogni comunicazione (ma quando guardiamo certi telefilm come Person of Interest ne siamo affascinati!). Io confesso di essere più turbato dal fatto che se lo possono fare gli USA, lo possono fare anche gli altri.

Per i fan del genere: anche le linee intercontinentali di comunicazione erano spiate:
- http://www.repubblica.it/tecnologia/2013/12/30/news/datagate_nsa_cavo_sottomarino_piratato-74789471/

****

05- Minacce e attacchi: Attacchi DDoS via NTP

SANS NewsBites riporta la notizia dell'aumento di attacchi DDoS basati su una vulnerabilità del Network Time Protocol (NTP):
- http://www.darkreading.com/attacks-breaches/attackers-wage-network-time-protocol-bas/240165063
- https://isc.sans.edu/forums/diary/NTP+reflection+attack/17300

Il problema del NTP è che spesso viene configurato dagli sviluppatori e dagli amministratori di rete e poi dimenticato. Quindi, le vulnerabilità sono ignorate da produttori e utilizzatori.

Questo ricorda la necessità di tenersi sempre aggiornati sui prodotti che si usano.

****

06- Minacce e attacchi: Attacco a OpenSSL

La notizia di Capodanno, ricevuta dal SANS NewsBites, è l'attacco al sito di OpenSSL:
- http://arstechnica.com/security/2014/01/openssl-site-defacement-involving-hypervisor-hack-rattles-nerves/

La cosa interessante è il comunicato finale del 29 dicembre, in cui si dice che l'attacco ha sfruttato una password debole utilizzata per l'accesso all'hypervisor:
- http://www.openssl.org/news/secadv_hack.txt

Insomma: il solito caro vecchio errore nella gestione delle password!