Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – APRILE 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: Accesso ai pc per antiterrorismo

In questi giorni c'è dibattito in merito al "provvedimento antiterrorismo". E' bene ricordare che si tratta ancora di una bozza di Decreto Legge non ancora approvata.

In poche parole: il decreto consentirebbe "l'intercettazione del flusso di comunicazioni anche attraverso l'impiego di strumenti o programmi informatici per l'acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico. In pratica, anche per ragioni non legate all'antiterrorismo, le Forze dell'ordine sarebbero autorizzate a installare malware sui pc a scopi di intercettazione.

Il problema è quindi che si introdurrebbero misure di indagine, nascondendole dietro l'anti terrorismo.

Per saperne di più, segnalo un articolo del Corriere della Sera e un post del deputato Stefano Quintarelli:
- http://www.corriere.it/cronache/15_marzo_25/decreto-antiterrorismo-polizia-potra-accedere-pc-italiani-66eea4e2-d319-11e4-9209-9dd80f8535a2.shtml;
- http://stefanoquintarelli.tumblr.com/post/114529278225/una-svista-rilevante-nel-provvedimento.

Pochi giorni dopo la notizia, il Governo ha fatto marcia indietro:
- http://www.corriere.it/politica/15_marzo_26/renzi-stralcia-antiterrorismo-norme-computer-3e07c838-d3a5-11e4-9231-aa2c4d8b5ec3.shtml

Materia certamente da seguire, che permette di riflettere sul livello di libertà che siamo disposti a perdere per essere più sicuri.

Grazie alla mailing list dei "perfezionisti" per la notizia.

****

02- Legale: Escrow agreement

Si parla spesso di contratti escrow per garantire la disponibilità del codice sorgente di un fornitore o di chiavi crittografiche.

Questo articolo mi sembra spieghi bene questo strumento:
-
http://www.altalex.com/index.php?idu=264948&cmd5=021c46ab76df2fd7050bbc8c56ed7fe1&idnot=70619

****

03- Novità legali: SPID (precisazione)

Una precisazione da Andrea Caccia di Kworks a seguito dell'articolo sullo SPID:
- http://blog.cesaregallotti.it/2015/03/spid-identita-digitale.html

Copio e incollo quanto segnalatomi da Andrea e lo ringrazio.

"Il Regolamento UE eIDAS non introduce realmente un sistema per la gestione dell'identità di gitale, ma un sistema di mutuo riconoscimento per gli schemi nazionali di gestione dell'identità digitale che diventerà operativo però solo con l'emanazione dei previsti atti esecutivi da parte della Commissione. In Italia il sistema di chiama "Sistema Pubblico per la gestione dell'Identità Digitale - Spid" e nasce con ambizioni europee ed evolverà in modo da poter essere riconosciuto anche dagli altri Stati membri dell'Unione."

Attualmente i decreti attuativi sono dal GarantePrivacy per la necessaria approvazione".

****

04- Standardizzazione: ISO/IEC 27041 e 27043

Dalla newsletter del BSI, vi segnalo l'avvenuta pubblicazione della norma ISO/IEC 27043:2015 dal titolo "Incident investigation principles and processes".

Mi sembra molto interessante l'estensione data alla preparazione pre-incidente, che richiede, tra le altre cose, di identificare le potenziali fonti di dati e le modalità di raccolta dei dati perché siano utilizzabili come prova.

Provvedo io a segnalare che, probabilmente, sarà pubblicata a breve la ISO/IEC 27041 dal titolo "Guidance on assuring suitability and adequacy of incident investigative method" e dedicata ai metodi e processi per investigare gli incidenti di sicurezza.

****

05- CIO si lamentano dell'inutilità dei report

Sul SANS NewsBites del 3 aprile trovo la seguente notizia: secondo un'indagine del Government Accountability Office (GAO) presso responsabili dell'IT (CIO, Chief Information Officer) di 24 agenzie federali tra le più grandi, i report richiesti dal Office of Management and Budget (OMB) sono in gran parte inutili e costosi:
- http://www.nextgov.com/cio-briefing/2015/04/survey-cios-say-many-it

Si tratta certamente di cose molto specifiche, ma il report del GAO mi ha incuriosito:
- http://www.gao.gov/assets/670/669434.pdf

Se ho capito correttamente, i report richiesti sono 36 e riguardano la pianificazione strategica, la pianificazione capitale e degli investimenti, la sicurezza IT, l'acquisizione e integrazione dei sistemi IT e altre iniziative. Solo 4 di questi sono reputati utili e riguardano la pianificazione strategica e la pianificazione capitale e degli investimenti. Tra i report "moderatamente significativi" si trovano quelli sulle "significative debolezze di sicurezza" e sulle "metriche di sicurezza IT".

Perché la sicurezza è "moderatamente significativa"? In parte, sul report si legge che si tratta di report con dati ridondanti l'uno con gli altri o con dati da inserire manualmente da diverse fonti. In parte immagino che molte misure non siano ritenute effettivamente significative e questo è uno dei problemi della sicurezza: si può misurare il numero di incidenti e poco più. Il resto serve solo a dare un'illusione di controllo "oggettivo".

****

06- I costi dei fornitori IT

Segnalo questo brevissimo articolo di @ISACA del 25 marzo 2015 dal titolo "The True Cost of Cost Savings When Outsourcing IT":
- http://www.isaca.org/About-ISACA/-ISACA-Newsletter/Pages/@-isaca-volume-6-25-march-2015.aspx

Traduco liberamente (l'articolo mi sembra troppo coinciso e non so se ho capito bene): secondo il "Global Information Security Survey 2015" di Pricewaterhouse Coopers, le minacce più elevate di sicurezza informatica sono originate, in ordine, da personale interno, ex dipendenti, fornitori di servizi IT, consulenti e collaboratori. Quindi, dare in outsourcing i servizi IT non è molto economico, se si

aggiungono, alle tariffe dei fornitori, i costi delle misure di sicurezza da adottare per ridurre i rischi originati dai fornitori stessi.

In base alla mia esperienza non saprei se avallare questa affermazione. Però posso affermare con forza una cosa: la questione della sicurezza nei rapporti con i fornitori è ignorata o sottovalutata. A meno che il servizio non sia "cloud"; in quel caso si accendono tanti (troppi) allarmi. Ma dell'eccessiva attenzione al cloud e della sottovalutazione degli altri fornitori ne parlo da tanto (troppo) tempo.

****

07- I 17 principi del COSO Integrated Framework

A maggio 2013, è stato pubblicato il "Internal Control – Integrated Framework" del COSO. Questo è composto da tre libri del costo di 175 dollari.

Non l'ho letto, ma ho letto questa serie di articoli dedicati ai 17 principi del framework (ad oggi sono solo 11):
- http://www.bestgrc.com/leverage-compliance/insights-revised-coso-integrated-framework-revised-coso-series/

Li ho trovati molto interessanti, anche perché applicabili in diversi contesti, anche se il punto di vista dell'autore è soprattutto quello delle medio-grandi imprese statunitensi.

****

08- Controllo del codice

Sulla mailing list ml di Sikurezza.org, un partecipante ha chiesto consigli sugli strumenti di controllo automatico del codice.

Gli altri partecipanti hanno fornito diverse indicazioni: Fortify, ZAproxy, pylint (per Python), Brakeman, Dawnscanner (per Ruby), Coverity (C++), Veracode (su cloud).

Ancora più interessante è il link alla pagina del NIST, con una serie di strumenti:
- http://samate.nist.gov/index.php/Source_Code_Security_Analyzers.html

In molti hanno segnalato alcuni problemi di questi strumenti, soprattutto i falsi positivi e la necessità di valutarne i risultati con la dovuta cautela, visto che ogni prodotto ha le sue specificità.

In questi anni, lo confesso, ho sempre ignorato questi strumenti, usati sia per il controllo della qualità sia della sicurezza del codice. Credo che invece siano da prendere in considerazione.

****

09- La scatola degli attrezzi per la sicurezza applicativa

Stefano Ramacciotti, sempre molto gentile, sa bene quanto mi interessi la sicurezza applicativa (anche perché devo approfondirla).

Questa volta mi ha segnalato un articolo interessante dal titolo "The Web AppSec How-to: The Defenders' Toolbox":
- https://www.checkmarx.com/white_papers/the-defenders-toolbox/

Se almeno uno di questi strumenti vi risulta sconosciuto, ne raccomando la lettura (l'articolo è molto breve e di tipo introduttivo; ma da qualche parte bisogna pur iniziare):
- Penetration testing;
- Web Application Firewall (WAF);
- Dynamic Application Security Testing (DAST);
- Static Application Security Testing (SAST);
- Interactive Application Security Testing (IAST).

****

10- Sviluppo - Worst practice

Mi è capitato un caso interessante. Visto che fatturo (poco) all'estero, devo produrre dichiarazioni doganali. Da www.agenziadogane.it devo usare un servizio "Intrastat". Ogni anno mi dà dei problemi e ogni anno devo chiamare
l'assistenza.

Vi segnalo quindi la pagina con le istruzioni per quest'anno (ogni anno cambiano, ovviamente):
- http://assistenza.agenziadogane.it/SRVS/CGI-BIN/WEBCGI.EXE?St=274,E=0000000000249617387,K=5081,Sxi=17,Solution=1946,t=Solution

Per chi non ha voglia di leggersi il documento, ecco cosa bisogna fare:
- usare una versione obsoleta di JRE;
- abbassare il livello di sicurezza del Java;
- abbassare il livello di sicurezza di Internet Explorer.
- osservare che i certificati usati sono auto-firmati.

Aggiungo che il mio pc con Windows 8, nonostante tutte queste cose, ha fatto cilecca e ho dovuto usare un "vecchio" Windows Vista.

Questo è decisamente un caso di "worst practice" relativa allo sviluppo.

Un'ulteriore considerazione: l'assistenza mi ha risposto in modo molto veloce e puntuale (anche se poi ho comunque dovuto cambiare pc). Questo mi porta a credere che il fornitore dell'Agenzia delle Dogane ha un sistema gestionale per cui l'assistenza (reattiva) funziona bene, ma la qualità (preventiva) funziona molto male (la navigazione del sito è anch'essa molto discutibile, con informazioni sparse in modo apparentemente casuale). C'è di che pensar male (o perché la Direzione non sa fare il suo lavoro, oppure perché così può risparmiare su una serie di elementi ma farsi pagare di più a causa di altri).

****

11- Rapporto Clusit 2015

A metà marzo è stato pubblicato il "Rapporto Clusit 2015 sulla sicurezza ICT in Italia". Per averlo, bisogna seguire le istruzioni su www.clusit.it

Confesso che l'ho trovato un po' meno interessante degli anni scorsi, ma rimane fondamentale leggere la "Analisi dei principali attacchi a livello internazionale" e la "Analisi degli attacchi italiani".

Il "Focus on 2015", su diversi argomenti come l'Internet of things, Bitcoin, Cloud e sicurezza, Return on security investment, eccetera, propone articoli introduttivi a temi importanti. Il termine "introduttivi" lo

uso con dispiacere, perché mi piacerebbe vedere più coraggio negli articoli pubblicati in Italia. Forse sbaglio, ma, se continuiamo a essere superficiali, il livello di sicurezza rimarrà superficiale.

****

12- Italiano o inglese

Il 14 marzo avevo annunciato la pubblicazione della nuova versione della norma italiana UNI 10459 sui professionisti della "security":
- http://blog.cesaregallotti.it/2015/03/uni-104592015-professionista-della.html

In quell'occasione mi ero lamentato dell'uso del termine "security" in una norma italiana.

Franco Ruggieri, che ringrazio molto, mi risponde che non concorda e lo cito.

<<
Avendo visto la emetica traduzione in italiano del Regolamento (EU) 910/2014, oltre ad altre iniziative di UNI, tra cui la traduzione dello ISO/IEC 27001, preferisco che si utilizzi l'inglese.

Io faccio da decenni un ragionamento: i medici si sono inventati termini ostici per noi mortali, ma chiarissimi per loro del mestiere. Perché nell'informatica, dove non dobbiamo inventarci nulla in quanto gli americani/inglesi hanno de facto già creato un vocabolario tecnico, dobbiamo disintegrarci il cervello alla ricerca di termini italiani che, poi, risultano essere, nella migliore delle ipotesi, ambigui? E tieni conto che io per 5 anni circa sono stato in una Direzione IBM dove ci si occupava di tradurre i programmi e le dispense IBM, quindi so di che cosa parlo.
>>

Credo che Franco, per gentilezza, abbia evitato di ricordarmi che l'italiano "sicurezza" può tradurre sia "safety" (ossia la sicurezza delle persone) sia "security" (ossia la sicurezza dei beni o del patrimonio) e che usare il titolo "Professionista della sicurezza" sarebbe stato scorretto.

In parte condivido l'approccio di Franco. Certamente quando alcuni termini anglosassoni non hanno un equivalente condiviso in italiano (come "firewall"; sarebbe buffo chiamarlo "muro di fuoco"), oppure ce l'hanno ma poco usato (come "computer", che potrebbe essere tradotto con "elaboratore"). In altri casi, però, io mi ostino a cercare di usare l'italiano; vorrei citare quelli che usano "action plan" al posto di "piano di azioni" (perché fa "competente" usare termini in inglese a casaccio).

In effetti, sul termine "security" sospendo il giudizio.

D'altra parte condivido anche la sua idea (la deduco soltanto) che forse è inutile tradurre certe cose. Mi chiedo spesso come ci si possa occupare di sicurezza delle informazioni senza leggere l'inglese, visto che le pubblicazioni più interessanti (con l'ovvia eccezione del mio libro!) sono tutte in inglese. Purtroppo alcune risposte le ho già, ma mi intristiscono.

****

13- Sul web

Mi rendo conto che questa notizia non c'entra nulla. Ma appaio per un secondo (il quinto) in questo spot di McDonald's e mi sembra ancora incredibile (ovviamente, mi hanno chiesto il permesso):
- http://www.ilpost.it/2015/04/15/hamburger-mcdonalds-blind-taste-milano-italia/