Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – GIUGNO 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 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- Rischi: OWASP Top 10 - 2013

OWASP ha pubblicato il 12 giugno l'aggiornamento delle "OWASP Top 10", ossia delle 10 vulnerabilità più critiche delle applicazioni web. L'edizione precedente è del 2010.

La notizia l'ho avuta dal gruppo Clusit su LinkedIn, ed è accompagnata dal seguente commento: "sono le stesse del 2010; questo vuol dire che bisognerebbe iniziare a fare i compiti". Credo si riferisca al fatto che se le vulnerabilità più critiche sono sempre le stesse, vuol dire che in 3 anni nulla è stato fatto per ridurle.

In realtà l'elenco è leggermente diverso da quello del 2010, ma si tratta di un rimescolamento delle stesse cose. Viene data maggiore evidenza ai software riutilizzati, spesso non ben gestiti e aggiornati.

Trovo la lettura delle Top 10 un po' ostica, probabilmente a causa degli accorpamenti fatti e della sintesi con cui i vari problemi sono trattati. Sto quindi aspettando la nuova edizione della OWASP Guide, prevista per il 2013.

Potete scaricare la Top 10 dal seguente link:
- https://www.owasp.org/index.php/Top10

****

02- Rischi: Il mercato delle vulnerabilità - Parte 2

Un anno fa avevo scritto un breve articolo sul mercato delle vulnerabilità:
- http://blog.cesaregallotti.it/2012/06/il-mercato-delle-vulnerabilita.html

Nel numero del 30 maggio 2013, l'Economist tratta l'argomento più diffusamente, ma senza commenti:
- http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade

Commento io: trovo allarmante che esistano tante imprese legalmente riconosciute il cui obiettivo è vendere vulnerabilità senza comunicarle ai produttori. Certamente io sono uno sciocco, visto che i prezzi variano tra i 20.000 e 250.000 dollari!

****

03- Rischi: Il Governo USA raccoglie dati personali

La notizia è molto nota e molto diffusa e la traduco direttamente dal sito del Washington Post (segnalato dal SANS NewsByte): la National Security Agency e l'FBI stanno effettuando intercettazioni direttamente dai server di 9 delle più importanti aziende USA fornitrici di servizi Internet (Microsoft, Apple, Yahoo!, Google, Facebook, Skype, YouTube, PalTalk, AOL) per analizzare audio, video chiamate, fotografie, e-mail, documenti e connessioni. Questo per controllare alcuni obiettivi stranieri.

Il progetto si chiama Prism ed è anche disponibile una presentazione dell'NSA:
- http://www.washingtonpost.com/www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Sul giornale del 8 giugno, Obama conferma la notizia:
- http://www.corriere.it/esteri/13_giugno_07/inchiesta-usa-nsa_e2fdc50e-cf7e-11e2-b6a8-ee7758ca2279.shtml

Lo sapevamo già da Echelon che una roba così era fattibile e quasi sicuramente fatta. Il successo di telefilm come Person of interest dimostra anche quanto tutto ciò fosse già da tempo nel nostro immaginario. E' dagli anni '90 che in tutte le aziende ci si racconta che i sistemisti guardano le e-mail del personale.

Ora abbiamo la certezza che tutto ciò è realtà. E finché sono i "buoni" a fare certe cose, possiamo anche accettarlo. Ma le stesse tecnologie sono anche in mano ai "cattivi" (lascio ai lettori scegliere a quale delle tue categorie appartengono NSA e FBI) o ai "furbi" che ci inondano di pubblicità.

Non ci rimane che guardare se questa notizia avrà degli impatti sui nostri comportamenti personali e sulla società nel suo complesso. Forse un po' più di attenzione alla riservatezza non potrà guastare.

****

04- Rischi: Byod, la ricetta non vale per tutti

Enzo Ascione di Intesa Sanpaolo mi scrive:
"ti segnalo un articolo che parla di quanto il BYOD sia in crescita, ma non per tutte le tipologie di azienda. Da non sottovalutare, inoltre, i rischi per la sicurezza, visto che molto presto si farà luce anche il Byoa (per non farci mancare nulla come sigle), Bring your own app, ossia 'usate il vostro software'".

L'articolo:
- http://www.corrierecomunicazioni.it/tlc/21351_milanesi-byod-la-ricetta-non-vale-per-tutti.htm

****

05- Novità legali: Regole tecniche sulle firme elettroniche (AgID e Garante privacy)

Il 2 febbraio è stato approvato il Decreto del Presidente del Consiglio dei Ministri dal titolo "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali [...]", che sostituisce quello del 30 marzo 2009.

Il DPCM si trova nella pagina del sito dell'AgID:
- http://www.digitpa.gov.it/firme-elettroniche-certificatori

Ringrazio Daniela Quetti che ha postato l'informazione sulla newsletter di DFA.

Sul Sole 24 Ore si trova anche un interessante articolo che segnala come la maggiore novità sia l'estensione delle regole alla firma elettronica avanzata, non solo digitale, e il riconoscimento della piena validità giuridica dei documenti informatici (tranne in alcuni casi):
- http://www.ilsole24ore.com/art/norme-e-tributi/2013-05-22/firma-elettronica-funzioni-064353.shtml?uuid=AbrUL1xH
- http://www.ilsole24ore.com/art/norme-e-tributi/2013-05-22/vecchia-grafia-diventa-spendibile-064416.shtml?uuid=AbUaL1xH

Ad aprile il Garante aveva già dato il permesso ad un paio di banche ad introdurre la possibilità per i clienti di firmare su lettori digitali anziché su carta; sebbene richiesto dalla normativa, il commento mi è sembrato inutile e forse dannoso. Infatti stabilisce che le firme autografe sono dati personali biometrici con rischio di palesare lo stato di salute del firmatario (attenzione quindi a chiedere documenti firmati!):
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2381240#1

****

06- Novità legali: Contrassegno elettronico e Linee guida

L'Agenzia per l'Italia Digitale ha emanato la Circolare n. 62/2013 relativa alle Linee guida per il contrassegno generato elettronicamente.

Copiando dalla Circolare: " La copia analogica del documento amministrativo informatico su cui è apposto il contrassegno elettronico sostituisce a tutti gli effetti di legge la copia analogica sottoscritta con firma autografa e pertanto non può essere richiesta all'amministrazione la produzione di altro tipo di copia analogica".

Inoltre: "Il contrassegno non assicura di per sé la "corrispondenza" della copia analogica al documento amministrativo informatico originale contenuto nel contrassegno stesso o conservato dall'amministrazione che lo ha prodotto, ma costituisce uno strumento mediante il quale è possibile effettuare la verifica della suddetta corrispondenza secondo modalità oggetto delle presenti linee guida".

I contrassegni elettronici più diffusi sono quelli visibili come quelle specie di codici a barre a punti (PDF417, 2D-Plus, WR Code) o di quadrati a punti (Maxicode, DataMatrix, Dataglyph, QR Code).

La circolare si trova sul sito dell'AgID:
- http://www.digitpa.gov.it/notizie/contrassegno-elettronico-online-circolare-sulle-linee-guida

****
07- Novità legali (privacy): Vademecum privacy del Garante

Il Garante della privacy ha pubblicato un opuscolo dal titolo "La privacy dalla parte dell'impresa - Dieci pratiche aziendali per migliorare il proprio business". Secondo il comunicato stampa esso "ha l'obiettivo di aiutare le imprese a valorizzare il proprio patrimonio dati, trasformando la privacy da costo a risorsa, senza per questo ridurre le tutele dei diritti fondamentali della persona".

In realtà non dice alcunché di nuovo. Alcuni titoli della normativa vigente sono riscritti in italiano più accessibile. E' un opuscolo utile solo a coloro che non hanno mai affrontato l'argomento privacy.

In particolare, l'opuscolo non affronta i problemi più spinosi che le imprese devono affrontare: come nominare i propri fornitori se si è titolari di un trattamento (un professionista dovrebbe nominare Telecom Italia come responsabile del trattamento ed esercitare il controllo sul suo operato?), come nominare i propri fornitori se si è responsabili di un trattamento, cosa si intende per amministratore di sistema e come devono essere svolte le verifiche sul suo operato.

Peccato: un'altra occasione persa. Per chi volesse verificare:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2445101

****

08- Novità legali (privacy): Binding corporate rules: un parere

Max Cottafavi di Reply mi segnala questo articolo di sintesi sul parere positivo dell'Art 29 WP sul ricorso alle Binding Corporate Rules (BCR) da parte dei responsabili esterni del trattamento (c.d. "BCR for Processors"):
- http://livinginaglassworld.com/2013/05/21/binding-corporate-rules-per-i-responsabili-del-trattamento-i-chiarimenti-dellart-29-working-party/

Il commento di Max Cottafavi è "non credo molto nelle BCR e trovo estremamente difficile che società di uno stesso gruppo multinazionale, operante in contesti e nazioni totalmente differenti tra loro, riescano a metterle in piedi e a rispettarle. I casi virtuosi ci sono ma di essi si parla proprio perché rappresentano delle eccezioni".

Ricordo che l'Art 29 WP, come dichiarato sul sito web della Commissione Europea (http://ec.europa.eu/justice/data- protection/article-29/), ha un ruolo di consulenza.

****

09- Novità legali: Fattura elettronica obbligatoria per la PA: pubblicato il regolamento

Ci sono cose che fanno piacere: la fattura elettronica è ora obbligatoria per la Pubblica Amministrazione grazie al DM 55 del Ministero dell'economia e delle finanze del 3 aprile 2013 con titolo "Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche [...]".

Se pensiamo che ci sono aziende private che ancora inviano fatture in formato cartaceo e si rifiutano anche di riceverle in formato elettronico, possiamo sperare che anche loro si evolvano.

L'articolo su CINDI, con il link alla normativa:
- http://www.cindi.it/fattura-elettronica/

****

10- Sky e la gestione delle vulnerabilità

Sandro Sanna mi ha segnalato questo articolo di Panorama:
- http://mytech.panorama.it/sicurezza/bug-sito-sky-hacker

In poche parole, tale Fabio Natalucci (in gergo, il "finder") ha segnalato una vulnerabilità a Sky. Sky ha poi negato e il Natalucci ne ha scritto assai sul suo blog:
- http://www.fabionatalucci.it/la-bella-risposta-di-sky/
- http://www.fabionatalucci.it/per-sky-hackingsky/

Non che la notizia sia diversa da tante altre, ma mi ha ricordato che sono in lavorazione i seguenti standard in merito al "Vulnerability handling":
- ISO/IEC 29147 - Responsible vulnerability disclosure (fornisce linee guida per la divulgazione delle potenziali vulnerabilità nei prodotti e servizi online);
- ISO/IEC 30111 - Vulnerability handling processes (descrive i processi per i vendor della gestione della segnalazioni di potenziali vulnerabilità nei prodotti e nei servizi online).

Sono tutti e due in stato di DIS e se non ci sono intoppi dovrebbero essere pubblicati tra un anno circa.

Per quanto riguarda il caso Sky, ecco alcuni punti non rispettati dai due contendenti:
- il fornitore di servizi o prodotti (Sky) avrebbe dovuto rendere disponibile un canale sicuro attraverso cui un "finder" può comunicare le vulnerabilità e mantenere i contatti reciproci per le analisi opportune;
- il "finder" non dovrebbe mai rendere disponibile l'exploit, ma solo un resoconto (per esempio sul modello dei Microsoft Buletin).

Si dice anche che il "finder" potrebbe comunicare la vulnerabilità ad un CERT, ma sembra che in Italia continui a non esistere...

****

11- Quante volte al giorno controlli l'email?

Segnalo questo interessante articolo dal titolo "Quante volte al giorno controlli l'email?".
- http://www.achab.it/blog/index.cfm/2013/4/quante-volte-al-giorno-controlli-lemail.htm

In pochissime parole: se controllate le vostre e-mail più di 4 volte al giorno, siete improduttivi.

Credo di essere un brutto esempio su questa materia.

****

12- ITIL "venduto" ad una joint venture

La notizia è in giro da qualche tempo: il Governo UK ha "venduto" ITIL e Prince2 ad una nuova società a cui lo stesso Governo UK partecipa con il 49%. Il 51% è di una società denominata Capita.

Alcuni sono molto critici perché temono un'eccessiva futura commercializzazione di ITIL:
- http://www.itsmportal.com/news/itil-goes-commercial

Altri sono invece soddisfatti perché ora la nuova joint venture si occuperà di svolgere funzioni di arbitro e controllore imparziale dei fornitori di formazione e certificazioni ITIL, mentre in precedenza APMG svolgeva il suo incarico di arbitro e controllore in regime di conflitto di interessi, in quanto fornitore di certificazioni essa stessa.

In realtà, nel Gruppo Capita, una piccola società è fornitrice di formazione ITIL, ma è stato dichiarato che i suoi servizi sono svolti principalmente all'interno del Gruppo e che non vi sono piani di un suo sviluppo come concorrente degli altri fornitori di formazione (ATO, accredited training organization). Mi chiedo se però poi a Capita non verrà un po' di appetito.

Le dichiarazioni in merito al futuro del "sistema ITIL", seppure ancora molto possibiliste, le trovate sul sito ufficiale:
- http://www.best-management-practice.com/?di=637187

****

13- La formazione sulla sicurezza è utile? (risposte)

In aprile avevo scritto che " la formazione degli utenti sulla sicurezza informatica non è generalmente utile".

Enzo Ascione di Intesa Sanpaolo mi ha risposto con una mail interessante che riporto:

<< Ciò che affermi è giustissimo nella misura in cui continuiamo a pensare che la società in cui viviamo non sia perfettibile.

Da qualche tempo faccio parte di un'associazione composta da volontari che insegna ai ragazzi nelle scuole l'utilizzo di Internet in modo consapevole. Ovvero, oltre l'uso anche le insidie che si nascondono interagendo nel mondo virtuale. L'associazione si chiama: Icaro ce l'ha fatta (www.associazioneicaro.org).

Inoltre, stiamo emettendo a livello banca una serie di regole sullo sviluppo sicuro del software, ma più si va avanti e più ci si accorge che non esiste un "codice sicuro".

La profilazione dei propri device è comunque qualcosa a cui stanno reagendo bene gli utenti… forse accoppiandola a regole di comportamento (etico e non) può rappresentare una buona scappatoia>>.

Ringrazio Enzo. Mi permetto di dare due risposte:
- utilissima la formazione svolta anche sui ragazzi per l'uso consapevole delle tecnologie (ringrazio quanti fanno questa attività, spesso volontaria, che ha anche l'effetto di rendere Internet un posto un po' più sicuro);
- i comportamenti a livello aziendale sono purtroppo condizionati da altre cose (fretta, efficienza, contenimento dei costi) e queste spesso sono ritenute più importanti della sicurezza.

Altra risposta molto interessante da Stefano Brambilla di Intesa Sanpaolo:

<< La mia esperienza vissuta in quest'ultimo periodo con la ISO/IEC 27001 mi porta a pensare che la formazione è utile. Infatti per le persone che lavorano sui sistemi in ambito di certificazione ho tenuto un corso di formazione di un'ora per dal titolo "Dal Cobit alla ISO/IEC 27001: implicazioni pratiche per gli operatori tecnici".

Non ho (per ora) una "misurazione di efficacia" quantitativa che lo possa dimostrare, ma vedo nel comportamento delle 35 persone a cui ho fatto il corso che ne tengono conto, anche se non tutti, non del tutto, e con attenzione decrescente nel tempo.... Però se non avessi fatto formazione avrei avuto comportamenti mediamente peggiori. Quindi la mia risposta secca alla domanda "La formazione sulla sicurezza è utile?" è "Sì, è utile".>>