Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS - FEBBRAIO 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: Privacy e AdS applicativi

Con il mio lettore Matteo Bonfanti di Lutech ho scambiato qualche opinione sul come considerare gli utenti di un'applicazione con privilegi speciali, principalmente quelli di gestione delle utenze.

Nel dubbio, Matteo Bonfanti ha contattato l'Ufficio del Garante dal quale ha ricevuto la risposta: "il Provvedimento del 27 novembre 2008 non riguarda gli utenti applicativi anche se questi hanno privilegi speciali, a meno che non possano agire direttamente sullo schema del database".

Prendo atto e lo ringrazio molto.

Occupandomi anche di sicurezza delle informazioni oltre alla privacy, rimango sempre nel dubbio che:
- elencare tali AdS non dovrebbe essere un problema,
- garantire la loro esperienza, capacità e affidabilità non dovrebbe essere un problema,
- l'applicazione dovrebbe registrare le azioni di tali AdS (anche se ci sono applicazioni che ahimé non lo fanno)
- i log non dovrebbero essere accessibili in scrittura agli AdS applicativi, ma solo a quelli sistemistici

Purtroppo ci sono applicazioni che non generano log e, ogni volta che le vedo, continuo a stupirmi.

****

02- Legale: Governo e sicurezza informatica

Sandro Sanna mi ha segnalato questa comunicazione del Governo italiano: "è stato firmato il decreto per dotarsi della prima definizione di un'architettura di sicurezza cibernetica nazionale e di protezione delle infrastrutture critiche".

Si parla di "un'architettura istituzionale che assicuri coerenza d'azione per ridurre le vulnerabilità dello spazio cibernetico, accrescere le capacità d'individuazione della minaccia e di prevenzione dei rischi e aumentare quelle di risposta coordinata in situazioni di crisi":
- http://www.governo.it/Presidenza/Comunicati/dettaglio.asp?d=70337

Il Decreto sarà pubblicato prossimamente in Gazzetta Ufficiale.

Confesso che non ho capito se si tratta del CERT nazionale previsto dall'Agenda digitale europea e di cui avevo scritto a dicembre:
- http://blog.cesaregallotti.it/2012/12/cert-italia.html

Non rimane altro che osservare.

****
03- Legale: Legge 4/2013 sulle "professioni non organizzate"

E' stata pubblicata la Legge 4/2013 dal titolo "Disposizioni in materia di professioni non organizzate".

Essa riguarda "l'attività economica, anche organizzata, volta alla prestazione di servizi o di opere a favore di terzi, esercitata abitualmente e prevalentemente mediante lavoro intellettuale [...]" con l'esclusione delle professioni già regolamentate in ordini e collegi (avvocati, ingegneri, eccetera). Insomma, riguarda l'attività di consulenti, auditor e formatori in molte discipline.

La Legge prevede che "La professione è esercitata in forma individuale, in forma associata, societaria, cooperativa o nella forma del lavoro dipendente".

All'articolo 2 sono regolamentate le associazioni professionali (codici deontologici, promozione della formazione permanente, sportello per fornire informazioni ai cittadini e utenti, eccetera). L'elenco delle associazioni che si auto-certificano come conformi alla Legge 4/2013 sarà disponibile sul sito del Ministero dello sviluppo economico.

Agli articoli 4 e 5 sono forniti ulteriori requisiti per le associazioni professionali, il primo delle quali riguarda la pubblicazione delle norme e regolamenti, inclusi, se pertinenti, quelli relativi al riconoscimento delle competenze dei propri associati, che le governano. E' anche consigliata, ma non obbligatoria, la certificazione ISO 9001 per le associazioni.

Ritengo che l'articolo 6 sia importante: "promuove l'autoregolamentazione volontaria" basata su norme tecniche "UNI ISO, UNI EN ISO, UNI EN e UNI". Sarà a questo punto importante (vedere anche l'articolo 9) quali saranno queste "norme tecniche UNI definite per ciascuna professione" per le quali un organismo di certificazione potrà rilasciare una certificazione: spero non si tratti della ISO 9001, visto che nei casi di singoli professionisti la sua applicazione sarebbe quanto meno discutibile.

Anche gli articoli 7 e 8 sono importanti perché specificano come un'associazione può rilasciare attestazioni relative alle competenze dei propri partecipanti.

Concludo dicendo che questa norma è importante. Forse qualche punto mi è ancora oscuro, ma sarà certamente chiarito con la sua applicazione.

Ho avuto notizia di questa Legge (ma senza il suo riferimento numerico!) dal CEPAS:
- http://www.cepas.it/legge_professioni.asp

Segnalo anche il link dal sito di Accredia:
- http://www.accredia.it/news_detail.jsp?ID_NEWS=1133&areaNews=95>emplate=default.jsp

La norma non è ancora disponibile su www.normattiva.it, ma è reperibile sulla Gazzetta Ufficiale 22 del 26 gennaio 2013 (http://www.gazzettaufficiale.it)

****

04- Ricerca: Furto di dati aziendali

Claudio Nasti di Chantecler mi ha segnalato questo interessante articolo dal titolo "Dati aziendali, sottrarli non è ritenuto sbagliato":
-
http://www.lineaedp.it/articolo/0000095971/30/8/Dati_aziendali_sottrarli_non_e_ritenuto_sbagliato.html#.UR1ChvJdCSp

Ecco alcuni dati di un recente studio di Symantec: il 50% dei dipendenti che lasciano un'azienda copia i dati dell'azienda stessa e, nel 40% dei casi, prevede di riutilizzarli dal suo nuovo datore di lavoro; solo il 38% dei dipendenti afferma che il loro manager vede la protezione dei dati come una priorità di business.

Brevissimo articolo che vale la pena di leggere (a patto di ricordarsi che, in questo contesto, IP non è l'Internet protocol, ma la intellectual property, e che probabilmente si tratta di una ricerca in ambito USA; cosa che non ho fatto ad una prima lettura).

Confesso che non sono un innocente. Ma mi è anche accaduto (ormai millenni or sono) di trovare qualcuno che mi chiedesse se potevo passargli documenti di un mio precedente datore di lavoro o di un mio ex cliente. Come se ormai fossero documenti pubblici. Ovviamente mi sono rifiutato. Ma la cosa fa pensare.

Per chi volesse approfondire il tema da un punto di vista legale, suggerisco di partire da Legge 633/1941 sul Diritto d'autore, Dlgs 30/2005 sulla proprietà industriale e CCNL.

****

05- Tecnologia: Quaderno su vulnerability assessment e penetration test

Isaca Venice Chapter ha pubblicato il suo primo quaderno dal titolo "Vulnerability Assessment e Penetration Test - Linee guida per l'utente di verifiche di terze parti sulla sicurezza ICT".

Ritengo sia un documento interessante perché ricorda una serie di argomenti che non sempre sono chiari ai responsabili di sicurezza informatica:
- differenza tra VA e PT
- normativa applicabile
- metodologie e tipi di PT
- requisiti per commissionare un PT
- schema di contratto

Una piccola e probabilmente inutile critica: troppa focalizzazione sui PT (i VA, ad un certo punto, sono quasi dimenticati).

Ringrazio Daniela Quetti di DFA per la segnalazione.

****

06- Tecnologia: Google, le password e i token

La notizia sta circolando: Google sta studiando un metodo per sostituire il meccanismo di identificazione e autenticazione degli utenti basato sulla sola coppia userid e password.

Sandro Sanna mi ha segnalato un articolo che ho trovato chiaro e completo:
- http://bits.blogs.nytimes.com/2013/01/17/critical-infrastructure-systems-seen-as-vulnerable-to-attack/?src=rechp

Segnalo anche due articoli ripresi dalla newsletter SANS NewsBytes:
-
https://www.computerworld.com/s/article/9235971/Google_sees_one_password_ring_to_rule_them_all?taxonomyId=17
- http://www.wired.com/wiredenterprise/2013/01/google-password/?cid=5394044

Da una parte, Google sta intraprendendo una bella iniziativa che potrà educare tutti gli utenti all'uso di meccanismi un po' più complessi ma più sicuri (da buon cittadino, trovo interessanti i film americani in cui gli abitanti di alcuni paesi non chiudono la porta a chiave, gesto per me consueto e banale).

Dall'altra parte, non posso fare a meno di notare che il meccanismo si baserebbe inizialmente su chiavi USB e Chrome, ricordandomi la guerra tra Google e Apple e il sospetto che ambedue vogliano tutti i nostri dati personali e che l'invio di un token a casa renderebbe ancora più sicura l'identificazione dell'utente e dell'autenticità dei suoi dati.

Ho il dubbio di star diventando paranoico...

PS: dal Clusit Group di LinkedIn ho avuto notizia di altri (Paypal in prima linea) che si muovono nella stessa direzione:
- http://www.computerweekly.com/news/2240177869/IT-industry-group-releases-password-killing-standard

****
07- Minacce e attacchi: Sistemi delle infrastrutture critiche

Le notizie sui sistemi IT delle infrastrutture critiche e non informatiche (soprattutto distributori d'acqua, elettricità, combustibile, energia) stanno aumentando. In parte perché questi mercati sono un obiettivo ancora non completamente presidiato da chi si occupa di sicurezza ("cherchez l'argent", mi viene da parafrasare), in parte perché le notizie di attacchi a questi sistemi (il più famoso è Stuxnet) hanno evidenziato le loro carenze.

Uno degli ultimi articoli l'ho trovato segnalato dalla newsletter SANS NewsBites e ha titolo "Critical Infrastructure Systems Seen as Vulnerable to Attack".

La notizia sconcertante è che il 91% degli attacchi inizia con una e-mail con allegato codice nocivo. Un esperimento condotto da una società di consulenza ha dimostrato che il 26% dei destinatari ha aperto l'allegato (su un campione di 70 persone, come viene onestamente dichiarato). Altro dato interessante: molti attacchi sono condotti dopo una breve ricerca su LinkedIn per creare e-mail fasulle il cui (falso) mittente è un contatto del destinatario.

Ho avuto modo di vedere aziende in cui i sistemi di controllo sono su una rete indipendente da quella utilizzata per lo scambio di e-mail e la navigazione sul web; ho visto aziende in cui i computer del personale sono bloccati rispetto a qualsiasi installazione di nuovo software; ho visto aziende in cui quasi tutti gli allegati alle e-mail sono sono bloccati così come le porte USB; ho visto aziende in cui il personale può ricevere e-mail solo su computer specifici. Ho visto cose che certi umani non possono immaginare, eppure dimostrano che non è tecnologicamente difficile fare sicurezza nei settori critici. Molti sono però frenati dal fatto che il personale potrebbe risentirsene. Forse, una maggiore consapevolezza del fatto che si lavora in settori critici potrebbe aiutare.

L'articolo:
- http://bits.blogs.nytimes.com/2013/01/17/critical-infrastructure-systems-seen-as-vulnerable-to-attack/?src=rechp

****
08- Minacce e attacchi: Alla sicurezza non sfugge (quasi) niente

Enzo Ascione di Intesa Sanpaolo mi ha segnalato questa interessante notizia:
- http://www.corriere.it/tecnologia/13_gennaio_17/softwerista-assenteista-lavoro-marchetti_5ff3373e-60b1-11e2-bd7d-debf946ea0b6.shtml

In poche parole: un programmatore, dipendente di un'azienda e con contratto di telelavoro, aveva in realtà subappaltato la propria attività ad un'azienda cinese. Nel tempo libero si dedicava al proprio hobby.

Enzo, ironicamente, dice "Beh però almeno il lavoro veniva fatto, no?".

L'articolo non fornisce indicazioni utili per capire a quali dati il programmatore aveva dato accesso a dei fornitori non autorizzati.