Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – DICEMBRE 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

Breve editoriale per augurare a tutti i lettori delle Buone Feste, sperando che il 2015 sia migliore del 2014.

****
01- Legale: Regolamento UE 910 del 2014 e CAD

Franco Ferrari del DNV GL mi ha segnalato il Regolamento UE 910 del 2014 "in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la

direttiva1999/93/CE". Esso è noto anche come eIDAS "electronic IDentification Authentication and Signature" e disciplina le modalità di apposizione della firma elettronica a convalida di documenti con valore probatorio. Il regolamento è entrato in vigore dal 17 settembre e sarà applicabile dal 1° luglio 2016.

I "servizi fiduciari" riguardano il mutuo riconoscimento attraverso mezzi elettronici e sono: firme elettroniche, sigilli elettronici, marche temporali, servizi di consegna, autenticazione di siti web".

Su http://eur-lex.europa.eu/ è possibile ricercarlo e scaricarlo.

Ho chiesto aiuto a Franco Ruggieri che mi ha scritto quanto segue. << La UE ha fatto una cosa buona: adeguare le normative sulla firma elettronica, stabilite nel lontano 1999 con la Direttiva 1999/993/CE. Con questo Regolamento UE 910/2014 si aggiorna qualche cosa sulle firme elettroniche, si inseriscono i "sigilli elettronici", cioè le firme elettroniche delle persone giuridiche, si apre la strada a qualcosa che assomiglia alla nostra PEC, si parla di time stamping, di authentication, e roba del genere.

Inoltre, sulla base dei pasticci dovuti alle diverse interpretazioni della Direttiva 1999/93/CE, hanno deciso di emettere un Regolamento. A differenza di una Direttiva, che deve essere recepita dagli Stati Membri della UE, un Regolamento entra in vigore automaticamente in tutti gli EUMS, il che dovrebbe consentire finalmente l'interoperabilità. E, poiché un Regolamento non può che essere una specie di legge primaria, stanno già lavorando intensamente agli implementing acts (atti attuativi). >>

A questo punto gli ho chiesto cosa ne sarebbe stato del Dlgs 82/2005, ossia il CAD (Codice dell'Amministrazione Digitale). La risposta: << Il CAD non sarà abrogato, perché tratta sì di eIDAS, ma anche di altre cose. Alcune parti dovranno essere eliminate o modificate. Dobbiamo avere notizie da AgID>>.

Ho chiesto lumi anche ad Andrea Caccia, nella speranza di mettere insieme più risposte e, forse, capirci qualcosa. Andrea dice che <<se il Parlamento non modifica il CAD, dal 1 luglio 2016 ci penserà il Regolamento a farne uno spezzatino: resterà in vigore solo ciò che non è in contrasto col Regolamento>>.

Andrea ha anche illustrato, in occasione della 10a riunione del SC27 di UNINFO alcune slide, confermando la partecipazione ai lavori di ETSI (ai cui lavori partecipa, tra gli altri, proprio Andrea Caccia).

Anche il sotto-comitato ISO/IEC JTC1 SC27 ha stabilito di occuparsi della materia con l'aggiornamento di un vecchio Technical Report del WG4, il TR14516 col nuovo titolo "Guidelines for use and management of Trust Service Provider"

Una cosa che mi sono segnato dalla presentazione di Andrea Caccia è questa: in base all'articolo 20 del Regolamento, "I prestatori di servizi fiduciari qualificati sono sottoposti, a proprie spese almeno ogni 24 mesi, a una verifica da parte di un organismo di valutazione della conformità" ... "ai sensi... del regolamento (CE) n. 765/2008 accreditato a... effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati", "in base agli standard che la Commissione indicherà nei propri decreti attuativi in base all'articolo 20 (3)".

In Italia, quindi, Accredia dovrebbe promuovere questo schema di certificazione dei Trust service providers (TSP). Nulla impedisce di affidarsi ad organismi accreditati da altri organismi non italiani. EA (European Cooperation for Accreditation), a cui Accredia aderisce, ha già approvato un piano di

migrazione predisposto da ETSI. Gli organismi di accreditamento si devono predisporre tra novembre 2014 e maggio 2015, mentre gli organismi di certificazione dovranno migrare da giugno 2015 a luglio 2016 (si preferiscono organismi con già esperienza di certificazioni rilasciate su standard ETSI). Ne vedremo delle belle...

Per intanto, Andrea suggerisce di leggere la presentazione di Riccardo Bianconi del 1 dicembre, che si può trovare a questo link (poi cliccare su "Convegno - Roma, 1 e 2 dicembre 2014"; anche le altre presentazioni sono di interesse):
- http://www.euronotaries.eu/news-ed-eventi/rassegna-stampa/

****

02- Legale: Social Network assimilato a luogo pubblico

Segnalo questo articolo a sua volta segnalatomi da Pasquale Stirparo sulla lista di discussione della DFA:
- http://thinkinginforensics.net/2014/11/social-network-assimilato-ad-un-luogo-aperto-al-pubblico/

In sintesi: La Corte di Cassazione ha assimilato una pagina (visibile a chiunque sia registrato) di un social network come un luogo aperto al pubblico, quindi idoneo alla configurabilità del reato di molestie o disturbo alle persone.

Non è la prima volta che segnalo questa notizia (e, anzi, penso sia lo stesso caso attraverso i vari gradi di giudizio), ma questa volta la sentenza è della Corte di Cassazione.

****

03- Legale: Aggiornamento sul Regolamento europeo sulla privacy

Alessandro Cosenza di BTicino mi ha segnalato il seguente articolo:
- http://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2014-12-11/regolamento-europeo-privacy-ancora-discussione-162857.php

Riassumo: bisogna aspettare e non fare nulla, al momento, poiché l'entrata in vigore richiederà almeno 2 anni e mezzo. Insomma, le stesse cose che vado dicendo da tempo, ma in modo molto più preciso.

Comunque, se e quando sarà approvato questo Regolamento, spero che tutti si ricordino dei cosiddetti esperti che ne hanno annunciato l'approvazione nel 2013, poi a inizio 2014, poi a fine 2014, e così via. Tutto per vendere corsi e consulenze basate sul "forse".

****

04- Legale: Provvedimento Garante biometria (e firma grafometrica)

Mi segnala Pierfrancesco Maistrello di Vecomp che è appena uscito il Provvedimento definitivo del Garante privacy su biometria:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3556992

Pierfrancesco commenta: "è scomparso il riferimento alla ISO/IEC 15408 per i sistemi di firma grafometrica, ma è comparso un interessante modulino di notifica data breach".

Io invece ho notato il seguente periodo: "I titolari dotati di certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) secondo la norma tecnica UNI CEI ISO/IEC 27001:2005 e successive modificazioni..." perché la norma citata non è mai esistita (esitono invece la ISO/IEC 27001:2005 e la UNI

CEI ISO/IEC 27001:2006), cosa che segnalai quando si potevano inviare commenti. Ma io mi chiedo: chi sono i consulenti del Garante? perché il Garante non si interfaccia con UNINFO? perché questa autoreferenzialità? Comunque oggi bisognerà usare la ISO/IEC 27001:2013 (o la UNI CEI ISO/IEC 27001:2014).

Segnalo anche questo articolo di riassunto:
- http://lamiaprivacy.wordpress.com/2014/12/07/provvedimento-e-linee-guida-in-materia-di-biometria-12-11-2014/

****

05- Legale: Privacy e Dossier sanitario

Dal gruppo Clusit di LinkedIn è stato segnalato questo articolo che riguarda le difficoltà di un'azienda sanitaria (AS9 ad adeguarsi alle disposizioni del Garante privacy in materia di fascicolo sanitario elettronico (FSE) fino a dire che si dovrà tornare alle cartelle di carta:
- http://altoadige.gelocal.it/bolzano/cronaca/2014/12/13/news/privacy-si-torna-alle-cartelle-di-carta-1.10493365.

In realtà, l'articolo aiuta molto poco a capire. Ma si può consultare il Provvedimento del Garante relativo a questa AS:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3325808

La storia: si scopre che una dipendente dell'ospedale consultava le cartelle cliniche del proprio reparto, fino a diffondere la notizia della sieropositività di un'altra collega. C'è un processo e si scopre che nella AS non c'è alcuna segregazione delle autorizzazioni di accesso alle cartelle cliniche. Il Garante privacy, a luglio 2014 ha imposto all'AS il recepimento delle misure di sicurezza per i fascicoli sanitari elettronici, come previsto dalle "Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario" del 16 luglio 2009 [doc web 1634116]. L'AS ha poi chiesto una proroga dei tempi al Garante e ora sembra che non sia in grado di completare l'attuazione delle misure.

La notizia mi ha colpito perché, nel Provvedimento del Garante, è scritto che l'AS ha chiesto aiuto ad una società di consulenza nel 2013 (4 anni dopo la pubblicazione delle linee guida e 6 anni dopo la costituzione dell'AS dalla fusione di 4 AS pre-esistenti!): certamente la privacy non è stata una priorità!

Altra notizia molto simile mi è arrivata da CINDI e riguarda invece l'Emilia Romagna:
- http://www.privacyofficer.pro/dossier-sanitario-elettronico-a-prova-di-privacy/

****

06- Certificazioni privacy e Europa

Alessandro Cosenza di BTicino mi ha segnalato il Bando di concorso dell'Ufficio europeo di selezione del personale (EPSO) per amministratori (AD 6) nel settore della protezione dei dati:
- http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=OJ:C:2014:391A:FULL&from=EN

La cosa interessante è la richiesta di formazione. E' infatti richiesta "Una formazione certificata in materia di protezione dei dati (IAPP, EIPA, GDD o equivalente, conseguita a seguito di esami)".

Ma poi tutto è lasciato all'interpretazione, oltre a ridurre gli organismi di certificazione a 3 (come interpretare il termine "equivalente"?).

Il primo è l'IAPP che offre ben 3 certificazioni ed è un'associazione USA (non europea!):
- https://privacyassociation.org/certify/programs/

Il secondo è l'EIPA, forse il più istituzionale, supportato economicamente dall'Unione Europea (ma temo sia un organismo privato). Il catalogo presenta diversi corsi, il cui più interessante potrebbe essere quello per "Training and Certification Programme for Data Protection Officers and Other Data Protection Professionals - Basic and Advanced Module".
- http://www.eipa.eu/en/pages/display/&tid=152

L'ultimo (GDD) è la German Association for Data Protection and Data Security. E questo la dice lunga su come è orientata l'Europa, anche per quanto riguarda la sicurezza delle informazioni. Io poi sul sito non ho trovato proposte di certificazione:
- https://www.gdd.de/international/english

****

07- Standard: UNI EN ISO 22301:2014 - Errata corrige

Franco Ferrari di DNV GL mi ha fatto notare che la UNI EN ISO 22301:2014 non è in italiano, ma solo in inglese. Pertanto è uguale alla ISO 22301:2012.

Mi scuso per l'errore. Avevo dato per scontato che il recepimento italiano della norma comprendesse la traduzione, visto che so che alcune persone ci stavano lavorando.

****

08- Standard: ISO/IEC 27018 - Code of practice for PII protection in public clouds acting as PII processors

L' Istituto Italiano Privacy e Alessandro Cosenza di BTicino mi hanno informato dell'uscita dello standard ISO/IEC 27018 "Code of practice for PII protection in public clouds acting as PII processors". L'articolo dell'Istituto:
- http://www.istitutoitalianoprivacy.it/it/dati-personali-e-cloud-computing-adesso-la-nuvola-ha-il-suo-standard/

La ISO/IEC 27018 presenta alcuni requisiti aggiuntivi rispetto alla ISO/IEC 27002 applicabili ai fornitori di servizi cloud.

Personalmente, non mi pare un documento particolarmente illuminante. Ma è un'opinione personale.

****

09- Standard: ISO/IEC 27040 - Storage security

A breve sarà pubblicata la ISO/IEC 27040 dal titolo "Information technology – Security techniques — Storage security". Si tratta di un libro di 122 pagine in totale, con molte cose tecniche interessanti.

Si potrà trovare sul sito dell'ISO: www.iso.org

****

10- Standard: NIST SP 800-53 - Assessing Security

Il NIST ha pubblicato la versione 4 della "Special Publication (SP) 800-53 A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans".

Il link:
- http://csrc.nist.gov/publications/PubsSPs.html#800-53ar4

Si tratta di un librone in pdf di 487 pagine. Di queste, quasi 400 costituiscono l'elenco dei controlli da verificare. Si tratta quindi di una lettura quanto meno esaustiva.

****

11- Richieste di responsabili sicurezza

Dal Crypto-gram di dicembre, segnalo questa notizia che traduco:
<< Questo articolo segnala che le richieste di Chief Information Security Officers eccede di gran lunga l'offerta:
- http://www.usatoday.com/story/tech/2014/12/02/sony-hack-attack-chief-information-security-officer-philip-reitinger/19776929/ o http://tinyurl.com/pha3sqp >>.

Non ho neanche verificato l'articolo, ma mi pare interessante il commento di Bruce Schneier, che sottoscrivo per quanto mi riguarda: << Non mi sorprende. E' un lavoro duro: budget sempre insufficiente, e si è sempre criticati quando si è inevitabilmente attaccati. E richiede un insieme difficile di competenze: abbastanza competenze tecniche per capire la sicurezza IT e sufficienti abilità gestionali per navigare tra i dirigenti. Non vorrei mai un lavoro così>>.

Quindi: tanti auguri ai CISO presenti e futuri!

****

12- VA, sicurezza e OWASP - Commenti

Stefano Ramacciotti commenta il mio articolo "I VA sono la sicurezza applicativa?":
- http://blog.cesaregallotti.it/2014/11/i-va-sono-la-sicurezza-applicativa.html

Stefano, leggendo il mio commento "in molti riducono il tutto non solo ai VA, ma alle sole vulnerabilità Top 10 segnalate da OWASP", commenta quanto segue:

“la cosa ancora più grave è che OWASP si riferisce alle sole web applications, ma se un'applicazione non è web? Ci sarebbero i "CWE/SANS TOP 25 Most Dangerous Software Errors" (http://www.sans.org/top25-software-errors/), e potrebbe essere d’aiuto l’elenco su http://www.hpenterprisesecurity.com/vulncat/en/vulncat/index.html, ma in molti sembrano non conoscerli.

Con questo nessuno vuole disconoscere l’enorme importanza di OWASP. Diciamo solo che di OWASP se ne avvantaggiano i soli sviluppatori web, che forse sono anche la maggioranza, ma non tutti gli altri.

Inoltre ci si dimentica che la Top 10 di OWASP elenca solo le prime dieci vulnerabilità, ma non è che ce ne siano solo 10, in realtà ce ne sono molte di più. Lo stesso sito di OWASP ne riporta anche altre che però sono meno visibili e forse meno tenute in considerazione dagli sviluppatori".

Enos D'Andrea, in merito alle mie piccole critiche sull'uso di OWASP e, soprattutto, sul fatto che la sicurezza applicativa si riduce ai test, mi ha segnalato una pagina dell'OWASP Top 10 dal titolo "What's Next for Organizations".

Qui sono scritte cose molto interessanti che richiedono appunto di non ridurre ai soli test la sicurezza applicativa. Infatti richiede di "porre delle basi solide", e tra queste vi sono "politiche e standard per gli sviluppatori, guide per la progettazione e lo sviluppo, formazione". Nella pagina "What's Next for Developers" si richiede di "progettare la sicurezza fin dall'inizio".

Raccomando quindi di rileggere la "OWASP Top 10 - 2013" senza fermarsi a pagina 16, ma proseguendo fino a pagina 27. Trovate la guida sul sito dell'OWASP:
- https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

****

13- Tecniche di sicurezza: Sicurezza IT nel settore energia

Dal Gruppo Clusit su LinkedIn segnalo questo whitepaper dedicato alla sicurezza informatica nel settore "produzione":
- http://download.schneider-electric.com/library/downloads/WW/en/document/998-2095-07-21-14AR0_EN

Ovviamente, è concentrato sul settore energia. Colgo allora l'occasione per ricordare il Quaderno Clusit numero 7 dal titolo "Introduzione alla protezione di reti e sistemi di controllo e automazione (DCS, SCADA, PLC, ecc.)", che ho riletto recentemente e mi è sembrato molto utile, anche se del 2007. Lo si può scaricare dal seguente link:
- http://www.clusit.it/download/index.htm

****

14- Tecniche di sicurezza: Certificati digitali gratuiti

Su Crypto-Gram del 15 dicembre, Bruce Schneier ha segnalato una nuova Certification Authority che fornisce certificati digitali gratuiti: Let's Encrypt, progetto a cui partecipano EFF, Mozilla, Cisco, Akamai e l'Università del Michigan.

Leggendo il blog di Bruce Schneier, alcuni partecipanti (con toni ovviamente critici, come si conviene quando si partecipa a forum!) hanno segnalato altre CA gratuite. Ecco quindi l'elenco:
- Let's Encrypt: https://letsencrypt.org;
- CAcert: http://wiki.cacert.org;
- StartSSL: https://cert.startcom.org.

Tutte offrono certificati per web server (Let's Encrypt propone anche l'aggiornamento automatico); CAcert permette anche di usare dei certificati per l'e-mail. Ovviamente non si tratta di certificati digitali utili per apporre firme digitali come previsto dalla normativa italiana in vigore.

Qualche breve riflessione:
1- forse saranno meno numerosi i siti web con i certificati scaduti; c'è da chiedersi perché vengono inizialmente attivate delle funzionalità di sicurezza (cifratura con certificato digitale) per poi non mantenerle;

2- oggi quasi nessuno si preoccupa più di cifrare le e-mail e quindi, ahinoi, non farà notizia la disponibilità di certificati digitali gratuiti per questo servizio.

****

15- Errata corrige: Poodle non Poddle

Enos D'Andrea mi ha fatto notare che ho scritto più volte Poddle al posto di Poodle. Me ne scuso con i lettori.

Enos aggiunge anche che, per contrastare Poodle, la soluzione in SSL3 consiste nel disabilitare i block cyphers e lasciare solo gli stream cyphers.