Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – GIUGNO 2016
****

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- ISO/IEC 27000:2016 disponibile gratuitamente

La ISO/IEC 27000:2016, dal titolo "Information security management systems — Overview and vocabulary", è ora disponbile gratuitamente al seguente indirizzo:
- http://standards.iso.org/ittf/PubliclyAvailableStandards/.

Grazie a Luciano Quartarone per l'aggiornamento.

****
02- Il caos degli standard per l'IoT

Segnalo questo articolo dal titolo "Chaos Theory of Standardization in IOT":
- securityaffairs.co/wordpress/47079/iot/chaos-theory-standardization-iot.html.

La tesi è semplice: sono presenti troppi protocolli di comunicazione per l'IoT e questo non potrà che generare problemi di funzionalità e di sicurezza.

Ho i miei timori: il tentativo di standardizzazione, se mai riuscirà, porterà ad un compromesso al ribasso in termini di sicurezza.

****

03- Certificazioni IoT

Dal Sans NewsBites del 27 maggio leggo la notizia che ICSA (ossia Verizon) ha lanciato un programma di certificazione dei dispositivi IoT. Segnalo l'articolo di Computerworld (più serio e completo di quello di DarkReading):
- http://www.computerworld.com/article/3075438/security/iot-security-is-getting-its-own-crash-tests.html.

La pagina di ICSA non aiuta perché promuove i test ma non dà indicazioni su quali sono i requisiti da rispettare. Trovo poco serio leggere di "sicurezza dalla progettazione" e poi, ipocritamente, trovare approfondimenti solo sui test:
- https://www.icsalabs.com/technology-program/iot-testing.

Segnalo quindi l'iniziativa della Online Trust Alliance, che ha pubblicato 30 principi per dispositivi sicuri (si trova la sintesi in versione definitiva e la guida completa in bozza):
- https://otalliance.org/initiatives/internet-things.

PS: l'articolo di DarkReading non riporta link per approfondire la notizia. Inoltre usa "cyber" a sproposito e "ecosistema" per "sistema informatico"; due indicatori di competenza acquisita sulle brochure commerciali.

****

04- eIDAS: norme di sicurezza per dispositivi (precisazione)

Leggendo la mia notizia in merito alla pubblicazione della decisione di esecuzione 2016/650 del 25 aprile 2016 della Commissione europea relativa alle norme per la valutazione di sicurezza dei dispositivi per la creazione di una firma e di un sigillo qualificati a norma del Regolamento eIDAS, Andrea Caccia mi ha segnalato una precisazione importante: questa decisione di esecuzione 2016/650 si applica limitatamente ai dispositivi sotto il diretto controllo dell'utilizzatore degli stessi (smart card, token USB, micro SD, eccetera); non si applica dunque (ad esempio) ai dispositivi (HSM) di firma remota.

La mia notizia originale:
http://blog.cesaregallotti.it/2016/05/eidas-norme-di-sicurezza-per.html.

****

05- Altri Aggiornamenti su eIDAS

Il nuovo CAD, per allinearsi al Regolamento eIDAS, sarà modificato a breve. Per chi vuole approfondire lo stato dell'arte, segnalo questo articolo (da un tweet di @fpmicozzi):
- http://www.ilquotidianodellapa.it/_contents/news/2016/maggio/1463684793525.html.

ENISA (l'agenzia europea per la sicurezza informatica) ha pubblicato un report con raccomandazioni in merito all'uso di certificati digitali per i siti web:
- https://www.enisa.europa.eu/publications/qualified-website-authentication-certificates.

Il report riguarda soprattutto le strategie generali per l'Europa, la prima delle quali è orientata, nel breve periodo, all'aumento di siti web che usano certificati digitali, la seconda è migliorare il mercato dei certificati digitali per i siti web.

In questi giorni saranno pubblicate le regole di Accredia per essere "certificati" come Trust service provider (TSP) anche per la vendita di certificati digitali per i siti web. Il numero minimo di giornate di audit per ottenere la qualifica è decisamente elevato.

Certo è che se ai fornitori sono richiesti molti soldi per qualificarsi come fornitore qualificato, il costo di questi certificati sarà troppo elevato e, quindi, questa strategia non avrà successo. Parere mio, per quanto poco possa valere.

****

06- DevOps e SIAM - Integrazioni

A inizio maggio avevo scritto su DevOps e SIAM:
http://blog.cesaregallotti.it/2016/05/devops-e-siam.html.

Deborah Monaco di Quint Wellington Redwood mi ha scritto per DevOps è attiva la DevOps Agile Skills Association (DASA), dedicata allo sviluppo delle competenze DevOps e Agile.

Questa associazione ha l'obiettivo, tra gli altri, di definire un programma di qualifiche DevOps. Da metà giugno 2016 saranno disponibili le certificazioni.

Stefano Ramacciotti mi ha invece suggerito di considerare le certificazioni, di ISC2, CSSLP, ISSEP e CCSP. Esse hanno dei moduli dove parlano della parte sicurezza delle DevOps, o meglio dell'SDLC, e promuovono la sicurezza in ogni fase del SDLC, per evitare di aggiungerla ex post, come un add-on.

Secondo Stefano, le metodologie più classiche e consolidate garantiscono un livello di sicurezza decisamente superiore.

Stefano ha anche avuto la brutta esperienza, di avere incontrato giovani programmatori che non hanno alcuna idea della sicurezza né della sua importanza. Certificazioni non di sicurezza (come, appunto, quelle di DevOps) dovrebbero integrare la sicurezza.

****

07- Direttiva europea sulla sicurezza informatica

Da tempo si parla della Direttiva europea relativa alla sicurezza delle reti e delle informazioni (network and information security, NIS).

Credo sia il caso di tenere sotto controllo il suo percorso. Essa dovrebbe essere attiva da agosto 2016. Ma, per avere una vera validità in Italia, è necessario vengano emessi degli opportuni Decreti legislativi. Quindi spero che non si scateni il panico che abbiamo già visto per il Regolamento privacy.

Per saperne un po' di più, segnalo la pagina del Consiglio EU:
- http://www.consilium.europa.eu/en/press/press-releases/2016/05/17-wide-cybersecurity-rule-adopted/.

****

08- Privacy online

Segnalo questo interessante articolo dal titolo "Going dark: online privacy and anonymity for normal people" (da un tweet di @fpietrosanti):
- https://www.troyhunt.com/going-dark-online-privacy-and-anonymity-for-normal-people/.

Un articolo che spiega perché non è male cercare di restare anonimi online.

A questo problema era collegato il mio post sulle email temporanee:
- http://blog.cesaregallotti.it/2016/05/email-temporanee.html.

Una mia amica (anonimizzata) mi ha segnalato altri servizi di posta temporanea: emailtemporanea.net, spaml.com, bigstring.com, 2prong.com, rppkn.com, ominutemail.com, spambox.us, mailinator.com, veryrealemail.com, mytrashmail.com, tempemail.net, tempinbox.com.

La mia anonima amica mi segnala che alcuni siti non permettono la registrazione con queste.

Ne approfitto a segnalare una frase di Terry Pratchett (da @DailyPratchett), di cui sono un fan, appropriata a questo argomento: "Ah, the rights of the individual, a famous Ankh-Morpork invention, so they say. But what rights are they, really, and whence do they come?"

****

09- Banca d'Italia: sicurezza dei pagamenti via Internet

Enrico Toso di DB Consorzio mi ha segnalato che Banca d'Italia ha emesso l'aggiornamento 16 delle Disposizioni di Vigilanza per le Banche - circolare 285 dove ha recepito gli Orientamenti EBA sulla Sicurezza dei pagamenti via Internet. Era un atto formale atteso dallo scorso 3 agosto 2015.

Enrico ricorda che la temuta conversione delle best practice (incluse nell'allegato 1 degli orientamenti) in misure obbligatorie non c'è stata e che, a partire dal 30 settembre 2016, le formule di adeguamento potranno contemplare la sola clausola del "comply" poiché la precedente formula "comply or explain" non sarà verosimilmente più percorribile.

Personalmente, trovo molto interessante il fatto che vogliono migliorare le misure di pagamento elettronico. Forse questo migliorerà le misure anche degli altri siti che non c'entrano nulla con le banche (visto che si innalzerà la qualità desiderata degli utenti). Enrico però mi ricorda che sarà necessario valutare ogni transazione per dimensionare correttamente la robustezza della sicurezza richiesta.

Il testo integrale della nuova Circolare 285 è disponibile al seguente link (A pag 350 / 628 c'e' la sezione VII che riporta il testo dell'aggiornamento):
- http://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/Circ_285_16_Aggto_testo_integrale_segnalibri.pdf