Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – OTTOBRE 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- Privacy: Statuto dei lavoratori - Modificato articolo 4

Come molte volte preannunciato, è stato modificato l'articolo 4 della Legge 300 del 1970.

Segnalo questo articolo, dove si trovano il link al D. Lgs. 151 del 2015 (articolo 23) che modifica l'articolo 4, il link al commento del Garante privacy (polemico e non certo risolutivo):
- http://www.webnews.it/2015/09/24/controllo-distanza-lavoro/.

Tra l'altro, il Garante non ricorda (e poteva farlo!) le sue "Linee-guida per il trattamento di dati dei dipendenti privati", che rimangono applicabili:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1364099.

Segnalo anche la comunicazione del Ministero del lavoro del 18 giugno 2015:
- http://www.lavoro.gov.it/Notizie/Pages/2015_06_18-Controlli-a-distanza.aspx.

Segnalo anche questo articolo di Gabriele Faggioli in merito:
- www.clusit.it/docs/faggioli_app_controllo.pdf.

Io ho letto e ho qualche dubbio. Provo a riassumere cosa dice il provvedimento e scrivo qualche commento tratto dalla lettura degli articoli sopra riportati (ricordo però che non sono un legale e la colpa di inesattezze è mia).

Il comma 1 dice, in sostanza, che è possibile utilizzare strumenti di controllo purché si abbiano le opportune autorizzazioni. Gli strumenti di controllo possono essere installati solo per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale. Deduco che le "esigenze produttive" non includano il controllo delle prestazioni del singolo lavoratore, ma solo quelle "generali". Ad ogni modo, l'unica vera novità riguarda l'aggiunta della finalità di "tutela del patrimonio aziendale".

Il comma 2 dice che le autorizzazioni non sono necessarie quando la raccolta dati (e quindi il potenziale controllo) avviene tramite gli "attrezzi di lavoro" (detti "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa") e gli strumenti di registrazione degli accessi e delle presenze. Da notare:
- gli strumenti di controllo accessi sono principalmente quelli fisici, relativi alle presenze; Faggioli include anche gli strumenti di controllo degli accessi ai sistemi informatici;
- tra gli attrezzi di lavoro sono da includere sicuramente pc, tablet e cellulari; secondo me, sono anche da aggiungere i sistemi informatici nel loro complesso; in altre parole, il "gestionale aziendale" (tipo SAP, per intenderci, che raccoglie log su chi ha modificato un documento o un record) e l'e-mail sono anch'essi attrezzi di lavoro;
- la raccolta dati tramite gli "attrezzi di lavoro" prevista da questo comma non comprende gli "attrezzi di lavoro modificati"; in altre parole, se ad un pc o smartphone si aggiungono software di monitoraggio o di localizzazione, questi richiedono autorizzazione.

Il comma 3 ricorda che è comunque applicabile la normativa privacy e quindi i lavoratori devono essere adeguatamente informati in merito agli strumenti di controllo (anche quelli inclusi nel comma 2). Un mio dubbio:
- se un lavoratore dovesse richiedere il blocco del trattamento, su quale base è possibile continuare il controllo? Forse perché c'è qualche disposizione contrattuale in merito?

Gabriele Faggioli ricorda inoltre delle sentenze della Cassazione dicendo (se riassumo correttamente): se il controllo dei log e delle registrazioni non avviene in modo continuativo (quindi "preventivo", come se fossero delle telecamere), ma solo quando ve ne è la necessità, per esempio a seguito di segnalazione di illecito (quindi "reattivo"), allora questo è permesso (purché questo aspetto sia incluso nell'informativa).

Le sentenze della Cassazione citate da Faggioli con le mie conclusioni:
- la 4746 del 2002, che validava la prova sull'uso illecito del cellulare aziendale da parte di un lavoratore; oggi questa sentenza rimarrebbe valida in quanto la verifica è stata effettuata ad hoc su una persona precisa (quindi non con strumenti specifici di monitoraggio dell'uso dei cellulari) e solo analizzando gli accessi non autorizzati allo strumento aziendale;

- la 15892 del 2007, che invalidava delle prove raccolte filtrando con strumenti specifici tutti gli accessi del personale; oggi forse queste prove sarebbero state ritenute valide, purché il personale sia stato adeguatamente informato;
- la 4375 del 2010, che invalidava delle prove raccolte attraverso strumenti di analisi del traffico Internet; anche oggi queste prove non sarebbero state ritenute valide in quanto gli strumenti usati erano ulteriori a quelli "di base" e non autorizzati (segnalo che da un punto di vista sicurezza sarebbe stato meglio bloccare direttamente i siti web, non raccogliere dati);
- la 2722 del 2012, che validava delle prove raccolte grazie a meccanismi "di base" dei sistemi informatici (nel caso particolare, l'archiviazione delle e-mail); anche oggi queste prove sarebbero ritenute valide.

Spero di ricevere ulteriori contributi, soprattutto per rispondere alle mie domande.

****

02- Privacy: Safe Harbour non è più valido

Con sentenza del 6 ottobre, la Corte di giustizia dell'UE ha dichiarato nulli gli accordi di Safe Harbour.

La sentenza la trovate nella pagina web con il commento del nostro Garante:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4308245.

Per chi non avesse seguito la questione in passato: gli accordi Safe Harbour prevedevano che se un'azienda USA dichiarava la propria adesione a questi accordi, automaticamente era consentito il trasferimento di dati personali dalla UE a questa azienda. Molte di queste aziende sono data centre in cui imprese europee archiviano i propri dati (la lista delle aziende Safe Harbour è liberamente accessibile: https://safeharbor.export.gov/list.aspx).

Questi accordi non sono più ritenuti validi perché non impediscono, per esempio e come dimostrato dal caso Snowden, la sorveglianza da parte di entità quali NSA.

Ora cosa succede? Facendo riferimento ad un articolo segnalatomi da Daniela Quetti di Lispa (http://uk.businessinsider.com/european-court-of-justice-safe-harbor-ruling-2015-10), ora le organizzazioni europee dovranno seguire le indicazioni delle autorità garanti nazionali. A quanto mi risulta non abbiamo ancora un Provvedimento del nostro Garante privacy.

Comunque già ora ci sono delle regole, previste dal nostro Codice privacy (D.lgs 196/2003) che richiedono, tra l'altro, il consenso esplicito da parte degli interessati.

In alternativa, si possono applicare le "clausole tipo" previste dall'autorizzazione del Garante del 2010 (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1728496).

Stessa conclusione si trova nell'articolo di Gabriele Faggioli in merito:
- www.clusit.it/docs/faggioli_ue_inval_safe_harbor.pdf.

Segnalo altri articoli di cui ho trovato riferimento su Twitter:
- http://www.reuters.com/article/2015/10/07/us-eu-ireland-privacy-idUSKCN0S00NT20151007;
- http://www.lastampa.it/2015/10/06/tecnologia/la-sentenza-shock-della-corte-ue-sulla-privacy-spiegata-in-punti-bpu45K0Ha8FRNOYvnbZ5TO/pagina.html.

****

03- Privacy: Accordo USA-UE per i dati personali

Franco Ferrari mi ha segnalato il recente Umbrella agreement, accordo USA-UE per la protezione dei dati personali scambiati con la finalità di prevenzione, rilevazione, indagine e gestione dei procedimenti legali di reati, incluso il terrorismo:
- http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm.

Da quanto capisco:
- per essere adottato in Europa deve essere ancora approvato dalla Commissione;
- l'accordo non introduce elementi peggiorativi della situazione attuale; forse la migliora;
- buffo che sia stato siglato pochi giorni prima della sentenza a proposito di Safe Harbour.

****

04- Privacy: Riflessione sulle sanzioni

Pierfrancesco Maistrello di Vecomp, mi ha reso partecipe di qualche sua riflessione.

Anche lui ha notato la scarsa comprensione dei requisiti normativi vigenti presso alcune PA.

Relativamente ad un sistema biometrico, per far comprendere il problema ad un suo committente, ha pensato di utilizzare il vecchio e consumato asso nella manica del conto della serva: Violazione del 162, comma2-ter, cioè 30mila-180mila Euro.

E il data breach, nei conti della serva? Considerando anche le ipotesi aggravate dell'art.164-bis, l'ammontare è attorno ai 50-60mila Euro. Con le migliori delle attenuanti non si scende sotto i 12mila €.

Pierfrancesco mi chiede: chi compra o commissiona soluzioni biometriche o grafo-metriche lo ha capito?

Rispondo: probabilmente no, perché sperano sempre nello stellone o nell'inefficienza della giustizia italiana (a individuare i reati e sanzionarli).

****

05- Privacy: PA e adempimenti

Fabrizio Bottacin, dopo aver letto il mio post in merito al Provvedimento del Garante privacy sul data breach (http://blog.cesaregallotti.it/2015/08/privacy-comunicazione-compromissioni.html), mi ha comunicato alcune sue considerazioni che riassumo nel seguito.

Il Provvedimento è un po' monco rispetto al D.Lgs. 82 del 2005 (Codice per l'Amministrazione Digitale). Questo riporta delle misure non applicabili solo dalla PA, ma anche da altri soggetti.

I gestori dei servizi pubblici, quindi PA o altri soggetti, devono adempiere ai dettami in materia di continuità Operativa (art. 50bis), sicurezza dei dati (art. 51), fruibilità del dato (art. 58), organizzazione dei servizi in rete (art. 63).

Ci sarebbero due riflessioni da fare, quindi:
- molti (come sappiamo) non sanno nemmeno che sono tenuti a questi adempimenti;
- il Provvedimento del Garante poteva essere esteso ai "gestori di servizi pubblici" e non solo alle PA.

****

06- Standardizzazione: Pubblicata la ISO/IEC 27006:2015

Il 30 settembre è stata pubblicata la nuova versione della ISO/IEC 27006 dal titolo "Requirements for bodies providing audit and certification of information security management systems":
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62313.

Si applica solo agli organismi di certificazione.

Non sono pienamente soddisfatto del risultato raggiunto perché:
- la versione del SOA (o Dichiarazione di applicabilità) deve comunque essere presente nei "documenti di certificazione"; in questo caso la dicitura è più vaga, ma l'idea di riportare la versione del SOA sul certificato, ahinoi, è rimasta;
- le giornate uomo minime previste non sono diminuite; qualcuno ha visto margini per essere "creativi" nel calcolo delle giornate uomo, ma la base di partenza è comunque troppo elevata.

****

07- Standardizzazione: Uscita la nuova ISO 9001:2015

Il 23 settembre è infine uscita la ISO 9001:2015 (anche se la data riportata dalla norma è il 15 settembre), di cui ho già parlato in altri post.

La pagina dell'ISO:
- http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62085.

La pagina UNI per la versione italiana (già disponibile):
- http://store.uni.com/magento-1.4.0.1/index.php/uni-en-iso-9001-2015.html.

Complimenti al BSI e al BSI Italia per la celerità con cui hanno inviato la notizia.

Per quanto riguarda i tempi di transizione: il 15 settembre 2018 tutti i certificati ISO 9001:2008 non saranno più validi e quindi le organizzazioni dovranno adeguarsi entro quella data. Gli Organismi di certificazione dovranno rendere disponibili regolamenti con maggiori dettagli.

Segnalo (grazie a Franco Ferrari di DNV GL) anche la seguente pagina di Accredia con molti chiarimenti:
- http://www.accredia.it/news_detail.jsp?ID_NEWS=1962&areaNews=95&GTemplate=default.jsp.

Nella pagina Accredia trovate anche dei documenti, in inglese, di chiarimento elaborati dal gruppo ISO (ISO/TC 176/SC 2) responsabile dello sviluppo della ISO 9001. Gli stessi documenti si trovano anche nella ISO TC/176/SC2 Home Page (che però è meno chiara della pagina Accredia):
- http://isotc.iso.org/livelink/livelink/open/tc176SC2public.

Ci tengo a sottolineare che questi documenti riportano pochi chiarimenti su come effettuare l'analisi del rischio richiesta dalla ISO 9001. Pertanto non esiste una "via giusta". Vedere anche un altro post: http://blog.cesaregallotti.it/2015/09/iso-9001-e-risk-thinking.html.

****

08- ISO 9001 e "risk thinking"

Con la nuova ISO 9001, si richiede di identificare e "affrontare" i rischi, senza però fornire dettagli.

Ho avuto l'occasione di raccogliere alcune indicazioni da Nicola Gigante, rappresentante italiano presso il ISO/TC176/SC2/WG24 (ossia il gruppo che ha elaborato la ISO 9001:2015), basate sulle indicazioni fornite da ISO e maturate nel corso della scrittura della norma stessa.

Si premette che la norma non richiede esplicitamente di documentare i rischi e le opportunità individuate; in altre parole, non è richiesto che le organizzazioni predispongano un'analisi dei rischi, ma che lo sviluppo, mantenimento e valutazione del sistema di gestione sia orientato da un approccio che metta la valutazione dei rischi al primo posto.

La norma non impone alcun approccio strutturato per affrontare rischi e opportunità: saranno le organizzazioni a decidere, con il rischio (!) che vi possa essere una generale banalizzazione del requisito.

Tuttavia va considerato che, come spesso accade a causa della natura "sistemica" della norma, anche in questo caso esiste una "circolarità": in altri termini, stabilire, da parte dell'organizzazione, con quale livello di approfondimento debba essere affrontata la gestione del rischio è essa stessa una operazione "risk-based", come tale soggetta a giustificazione e a valutazione di efficacia. Questo dovrebbe essere il primo effetto di un corretto orientamento al rischio.

In generale, organizzazioni semplici, di piccole dimensioni, con tecnologie consolidate e caratterizzate da un contesto stabile, non avranno effettivamente bisogno di strumenti sofisticati per mettere in pratica il "risk-based thinking". In tali realtà potrebbe essere sufficiente "lavorare" sugli atteggiamenti mentali di ciascuno, affinché ogni decisione - a livello strategico, tattico, e operativo - sia determinata da una sia pure intuitiva valutazione della concatenazione dei possibili eventi.

Nelle organizzazioni più grandi e complesse, invece, l'approccio al rischio dovrà verosimilmente essere di tipo più strutturato e potrebbe comportare la messa in atto di metodi, infrastrutture e competenze mirate. In caso contrario, cioè in presenza di un approccio riduttivo al tema del rischio, l'auditor chiederà ragione di ciò all'organizzazione, che dovrà fornire spiegazioni convincenti (cioè oggettivamente sostenibili).

In ogni caso l'efficacia dell'approccio dovrà essere dimostrata dall'organizzazione (vedere per esempio, al riguardo, il p.to 9.3.2 e, relativo al riesame di Direzione) e all'auditor spetterà valutare l'adeguatezza delle dimostrazioni (anche se rappresentate solo da argomentazioni).

E' evidente che questo "gioco" è possibile se vi sono competenze adeguate da entrambe le parti (organizzazione e auditor).

Mio (di Cesare Gallotti) parere personale: forse qualche indicazione in più sarebbe stata utile. Ora correremo il rischio (!) di vedere auditor imporre valutazioni del rischio molto dettagliate, altri accontentarsi di un'analisi SWOT generale e poi chissà che altro, con il risultato che le aziende, ancora una volta, non capiranno le motivazioni della ISO 9001, non ne coglieranno i benefici e, anzi, la rifiuteranno ancora di più.

Infine: ringrazio Nicola per avermi consentito la pubblicazione.

****

09- Articolo su eIDAS

Come noto da precedenti post, eIDAS, il Regolamento europeo relativo ai servizi fiduciari, è un argomento che trovo interessante e degno di attenzione.

Ricordo qui i miei post precedenti:
- http://blog.cesaregallotti.it/2014/12/regolamento-ue-910-del-2014-e-cad_11.html;
- http://blog.cesaregallotti.it/2015/03/spid-identita-digitale.html;
- http://blog.cesaregallotti.it/2015/03/novita-legali-spid-precisazione.html.

A questo punto segnalo un articolo di Andrea Caccia e Daniele Dumietto che, secondo me, rende più chiara la situazione:
- http://www.ildocumentodigitale.com/regolamento-europeo-eidas/.

****

10- EN 319403 per i servizi fiduciari

È stata pubblicata la EN 319 403, dal titolo " Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers":
- http://uninfo.it/index.php/news/focus/item/pubblicata-la-norma-en-319403-nasce-l-accreditamento-per-la-conformita-dei-servizi-fiduciari.

È applicabile ai fornitori di servizi che vorranno ottenere dall'AgID lo status di servizio qualificato. Tra questi servizi vi sono quelli relativi a:
- firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi;
- certificati di autenticazione di siti web;
- conservazione di firme, sigilli o certificati elettronici relativi a tali servizi.

Grazie ad Andrea Caccia per la segnalazione.

****

11- Per AgID l'informatica è ferma agli anni Novanta

Per AgID l'informatica è ferma agli anni Novanta, forse. Forse agli Ottanta.

Mi spiego. La Circolare AgID 65 del 2014 riguarda l'accreditamento per le attività di conservazione dei documenti informatici e non distingue tra i 3 elementi fondamentali di un servizio IT: attività burocratiche e amministrative, sviluppo e manutenzione dell'applicazione, conduzione dei sistemi informatici.

La circolare stabilisce: "Il conservatore può affidare ad altro conservatore accreditato le attività a supporto del processo di conservazione limitatamente a quelle che riguardano le infrastrutture per la memorizzazione, trasmissione ed elaborazione dei dati".

In altre parole, se un'azienda conosce il processo e mantiene l'applicazione non può usare i servizi di amministrazione dei sistemi (e il CED) di un esterno, a meno che questo non sia accreditato a sua volta come conservatore. Quindi, questo professionista esterno deve essere bravo a gestire il CED, ad

amministrare i sistemi, a sviluppare un'applicazione complessa, a gestire un processo di conservazione sostitutiva.

Oggi, però, le aziende sono spesso specializzate in un solo di questi compiti (chi conosce le aziende specializzate nello sviluppo sa bene che, spesso, una delle prime cose da fare per migliorarne la sicurezza è proprio quella di far gestire i sistemi ad altri).

Pensate che io sia paranoico? Pensate che in realtà quelli di AgID non la pensino così? Purtroppo questa mia accusa nasce da casi reali.

Ulteriore considerazione: la medesima disposizione non si applica allo sviluppatore del software. Sebbene l'applicazione sia fondamentale, chi la mantiene non deve essere necessariamente accreditato, a differenza di chi gestisce i sistemi. Come negli anni Ottanta-Novanta, quando le vulnerabilità applicative erano poco considerate.

La circolare di AgID, quindi, doveva essere scritta decisamente meglio, tenendo conto di un concetto che oggi si applica a quasi tutti i settori: la catena di fornitura.

Nota finale: non penso che i conservatori accreditati ad oggi siano deboli in uno dei settori indicati. Ma le aziende di questo tipo sono necessariamente molto poche.

****

12- Rapporti di sicurezza informatica

In questo periodo ho ricevuto notizia di diversi rapporti di sicurezza informatica.

Il primo è "Annual Incident reports 2014" di ENISA, l'agenzia europea per la sicurezza informatica, relativo ai sistemi di telecomunicazione:
- https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2014.

La segnalazione è arrivata da Claudio Telmon, attraverso il gruppo Clusit di LinkedIn. Il suo commento: Ci sono molti dati interessanti, ma uno mi ha colpito particolarmente, da pag. 15 del Report: le gravi interruzioni dovute ad azioni malevole (9%, quasi un decimo) hanno superato quelle dovute ad eventi naturali (5%); e mentre il secondo valore è in calo, il primo è in crescita. Per completezza, la causa principale (66%) sono "system failures". Non che si possano trarre delle conclusioni statistiche "certe" anche per altri contesti, ma noto però che nei piani di BC/DR continuo a vedere tanta attenzione agli eventi naturali, e poca a quelli malevoli.

Il secondo è "The Internet Organised Crime Threat Assessment (IOCTA) 2015" a cura di Europol:
- https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015.

La segnalazione è arrivata da Mattia Epifani, via mailing list di www.perfezionisti.it. Ad avviso di Mattia, dopo una prima veloce lettura, i fatti salienti sono:
- valutazione della situazione nelle tre aree ritenute di maggiore interesse da Europol (Cyber Attacks, Online Child Exploitation e Payment Fraud);
- analisi dei malware che hanno avuto maggiore effetto nell'ultimo anno;
- grande spazio ai ransomware ma attenzione anche sui RAT; è strano vedere che Dark Comet (che è oramai vecchiotto) e le sue varianti siano ritenute ancora un High Risk (pagina 27);
- preoccupazione per lo sviluppo delle criptomonete e delle darknet per le attività illegali.

Il terzo è l'aggiornamento del rapporto Clusit 2015:
- http://clusit.it/rapportoclusit/

Io avevo già la versione di marzo 2015 e non ho notato cambiamenti. Ad ogni modo, chi non dovesse averlo ancora letto, dovrebbe farlo.

Infine, Vito Losacco mi ha segnalato il Report McAfee Labs sulle minacce" dell'Agosto 2015:
- http://www.mcafee.com/it/mcafee-labs.aspx?view=legacy (versione italiana);
- http://www.mcafee.com/it/resources/reports/rp-quarterly-threats-aug-2015.pdf (link diretto alla versione italiana);
- https://blogs.mcafee.com/mcafee-labs/malware-trend-continues-relentless-climb/ (versione inglese).

In realtà questo report propone delle riflessioni su alcuni temi e alcuni casi di interesse.

****

13- iOS Security paper

La Apple ha pubblicato recentemente un documento dl titolo " iOS Security: iOS 9.0 or later":
- http://www.apple.com/iphone/business/it/security.html.

Gli appassionati di tecnologia lo troveranno interessante.

Io però sono interessato ad un'altra cosa: la cura con cui la Apple ha preparato questo documento. Certamente si tratta di marketing. Ma non è solo questo: è una presentazione dei meccanismi di sicurezza di un sistema hardware e software.

È vero che la Apple dispone di personale preparato e dedicato a questo tema, ma certamente il loro esempio dovrebbe essere considerato dalle aziende produttrici e clienti di hardware e software.

Ringrazio Mattia Epifani per la segnalazione e i link.

****

14- Il computer a scuola non aiuta ad imparare il digitale

Questo argomento è lievemente fuori tema rispetto ai soliti qui trattati:
- http://www.techeconomy.it/2015/09/15/ocse-computer-scuola-non-aiuta-ad-imparare-digitale/.

In sintesi: non è detto che gli alunni con maggiore accesso ai sistemi informatici siano più bravi ad utilizzarli. La conclusione: è necessario non solo mettere a disposizione gli strumenti informatici e il tempo per utilizzarli, ma anche "un rilevante livello di preparazione degli insegnanti" su come gestire questo tempo in modo efficace.

Penso che sia il caso di riflettere su questi aspetti perché forse la questione non si ferma alle scuole: nelle aziende, il personale, di qualunque età, usa i sistemi informatici in modo continuativo, ma non per questo ne capisce tutte le potenzialità, i limiti e, ovviamente, i rischi.

****

15- Valutatori e competenze

Prendo lo spunto da questo post di Paolo Perego:
- https://codiceinsicuro.it/blog/premetto-io-non-sono-uno-sviluppatore/.

Riassunto: chi fa i vulnerability assessment delle applicazioni dovrebbe avere un po' di esperienza di programmazione; in caso contrario le raccomandazioni per il miglioramento non possono essere pienamente adeguate.

Estendo e penso a auditor, assessor e alcuni consulenti (detti "advisor"), che spesso non hanno mai scritto una riga di procedura da condividere con tutte le parti interessate. Ho notato che sono spesso prodighi di "buoni consigli", senza però alcuna idea della loro fattibilità nel contesto di riferimento.

Piccolo aneddoto: recentemente ho seguito un audit. L'auditor si è proclamato ex programmatore. Ha fornito suggerimenti su tutto, con molto entusiasmo, ma senza chiedersi se fossero realmente applicabili e utili per l'azienda in cui si trovava (tra le tante: ha suggerito di usare diagrammi causa-effetto per individuare le cause di OGNI non conformità, ha chiesto di vedere un'analisi del rischio di ogni processo, ha suggerito di adottare ITIL per la gestione dei sistemi e della rete, malgrado le persone coinvolte fossero 8).

Per un solo settore non ha dato consigli: lo sviluppo delle applicazioni (eppure qualche idea sarebbe stata utile).

Perché? Perché incompetente in materia o perché capiva che, per quel contesto, era stato fatto il massimo? Forse la seconda.

****

16- Assicurazione si rifiuta di pagare dopo un attacco

Sono sempre stato perplesso in merito alle assicurazioni relative agli attacchi informatici.

Questo caso, conseguente all'attacco a BitPay, sembra confermare la mia prudenza:
- http://www.networkworld.com/article/2984989/security/cyber-insurance-rejects-claim-after-bitpay-lost-1-8-million-in-phishing-attack.html.

Faccio la sintesi del caso. BitPay è una società che gestisce Bitcoin. Un hacker invia una mail al CFO di BitPay con un link fraudolento a Google. Il CFO usa il link, si connette alla propria e-mail su Google e, ovviamente, l'hacker da quel momento dispone delle credenziali dell'e-mail del CFO. Quindi, con le credenziali del CFO, invia una mail al CEO chiedendogli di inviare dei bitcoin ad un certo conto. Il CEO esegue e, ancora ovviamente, l'hacker si vedere recapitare i bitcoin sul proprio conto.

L'assicurazione si è rifiutata di pagare BitPay perché l'attacco non è avvenuto sui sistemi di gestione dei bitcoin, oggetto dell'assicurazione, ma sul sistema di e-mail.

****

17- Caso Volkswagen

Il caso è molto marginale per gli argomenti di questo blog:
- http://www.pressreader.com/italy/corriere-della-sera/20150923/281685433644490/TextView.

Però due riflessioni le faccio:
- se questi hanno fatto dei test tarocchi su un'automobile, perché stupirci quando gli sviluppatori di software meno critici fanno lo stesso?
- smettiamo di parlare male dell'Italia e degli italiani quando emergono queste cose: non è un problema di cultura nazionale, è un problema di cultura imprenditoriale. Tradotto: smettiamo di dire "qui è difficile applicare certe procedure perché siamo italiani" e cominciamo a dire "qui è difficile applicare certe procedure perché alla Direzione non interessa". Chissà che avere ben chiara la causa del problema renda meno difficile risolverlo.