Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – LUGLIO 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

****

00- Editoriale

Come sempre prima delle vacanze (per alcuni) estive e invernali, ne approfitto per salutarvi e augurarvi il meglio possibile, qualunque cosa facciate.

Questo mese la mail arriva in ritardo così non ne sentirete la mancanza ad agosto. Riprenderò con la newsletter di metà settembre.

È anche più lunga per la stessa ragione (se vi annoiate in spiaggia, avete qualche lettura in più).

****

01- Standard: Pubblicata la ISO/IEC 27042 su digital evidence

Segnalo che è stata pubblicata la ISO/IEC 27042 dal titolo "Guidelines for analysis and interpretation of digital evidence". In precedenza avevo dato notizie inesatte sul suo stato di approvazione e me ne scuso. In questo caso, ho visto la notizia della pubblicazione dalla newsletter del BSI.

Le norme ISO/IEC dedicate alla digital forensics sono quindi:
- ISO/IEC 27035 (molto parzialmente) - Information security incident management;
- ISO/IEC 27037 - Guidelines for identification, collection, acquisition, and preservation of digital evidence;
- ISO/IEC 27041 - Guidance on assuring suitability and adequacy of incident investigative method;
- ISO/IEC 27042 - Guidelines for analysis and interpretation of digital evidence;
- ISO/IEC 27043 - Incident investigation principles and processes.

Prego notare che costa 85 Euro e consta di 14 pagine. La sua lettura, inoltre, è impossibile senza 27037 e 27041. Non commento...

****

02- Standard: FDIS ISO 9001:2015

È disponibile la FDIS della futura ISO 9001. Ringrazio Franco Ferrari di DNV GL per avermelo segnalato. Ci saranno quindi le votazioni e ne è prevista la pubblicazione finale per il 22 novembre.

Le novità rispetto alla ISO 9001:2008 sono tante. E ne segnalo solo alcune.

La prima è relativa alla "valutazione del rischio", che sostituisce le azioni preventive. Il testo non è di facilissima comprensione (anche se chi ha già lavorato sulla ISO/IEC 27001:2013 lo conosce bene). Richiederà qualche aggiustamento al sistema di gestione per la qualità e all'approccio al sistema stesso. Come per gli "indicatori" introdotti dalla ISO 9001:2000, ci vorrà un po' di tempo perché organizzazioni, consulenti e auditor trattino queste novità correttamente. Nel frattempo, spero che nessuno faccia danni introducendo troppo fuffaware.

Altre novità riguardano la terminologia: "persone" al posto di "risorse umane", "informazioni documentate" al posto di "procedure documentate" e "registrazioni" e così via.

In alcuni casi, queste novità danno luogo a difficoltà di lettura. Per esempio, bisogna stare attenti a distinguere tra il mantenimento di informazioni documentate (ossia avere procedure documentate) e la conservazione di informazioni documentate (ossia avere registrazioni).

In molti si stupiranno della riduzione di procedure e registrazioni. In realtà bisogna prestare attenzione a non esagerare ed eliminare tutti i documenti. Forse però questa novità imporrà di vedere le procedure qualità come vere procedure o istruzioni e non come carta da fare per la certificazione. D'altra parte, sono numerosi i casi in cui le "vere" istruzioni non coincidono con le procedure presentate agli auditor. D'ora in avanti, sarà sempre più evidente la differenza tra la "carta per gli auditor" e i "documenti necessari".

Altra eliminazione importante è il manuale qualità, che negli ultimi anni era diventato sempre più un esempio di "carta da auditor" che non diceva nulla, frutto di un'errata interpretazione della norma.

Ulteriore eliminazione è il responsabile della qualità, in realtà già assente dalle ultime versioni, che richiedevano la presenza di un membro dell'Alta Direzione come referente per la qualità (mentre spesso il Responsabile per la qualità, nella migliore delle ipotesi, era un quadro o un primo livello). La responsabilità del sistema di gestione per la qualità è la Direzione, punto e basta.

Non ho accennato a molte cose. La norma è impostata in modo molto diverso da prima e un breve articolo non può esaurire l'elenco delle novità. Usciranno libri, si faranno corsi e presentazioni, si scriveranno articoli. Ancora una volta: tutti da leggere o seguire con attenzione, anche per evitare di incappare in interpretazioni fantasiose.

****

03- Standard: BSI PAS 555 sul Cyber security risk

Franco Ferrari di DNV GL mi ha segnalato la pubblicazione da parte del BSI della PAS 555, risalente in realtà al 2013. Questo standard nazionale ha titolo "Cyber security risk – Governance and management – Specification".

Ho trovato molte cose negative e una cosa positiva in questo standard.

Comincio da quella positiva: l'importanza data agli strumenti di raccolta di informazioni relative a minacce e al monitoraggio preventivo.

Le cose negative sono diverse:
- il fatto che questa norma, più limitata rispetto alla ISO/IEC 27001 (come ho già avuto modo di scrivere in precedenza: blog.cesaregallotti.it/2015/03/cyber-che.html), ma non più semplice, si metta in concorrenza con essa senza alcuna ragione se non quella di portare più entrate al BSI;
- la confusione che questa norma può generare in merito ai sistemi di gestione perché non è basata sul HLS;
- il fatto che i rappresentanti inglesi (quindi del BSI), in fase di redazione della ISO/IEC 27001:2013, siano stati tra i più pugnaci a voler togliere dalla stessa ISO/IEC 27001 ogni riferimento a asset, minacce e vulnerabilità, per poi, attraverso questa PAS 555, richiedere di valutare il rischio basandosi proprio su asset, minacce e vulnerabilità e per poi ancora presentare in appendice una "risk impact matrix" basata su minacce, conseguenze e verosimiglianza.

****

04- Standard: ISO/IEC 38500 su IT governance

Franco Ferrari di DNV GL mi ha segnalato la recente pubblicazione della nuova edizione del 2015 della ISO/IEC 38500 dal titolo "Governance of IT for the organization".

Ad una prima e veloce lettura, non mi sembra né tanto diversa né tanto più utile della precedente ISO/IEC 38500:2008 (però non mi offenderei se qualcuno mi contraddicesse).

Segnalo però che la nuova norma fa riferimento ad una ISO/IEC 38501:2015 dal titolo "Governance of IT -- Implementation guide"; forse questa è più interessante, ma non ho avuto alcuna possibilità di leggerla.

****

05- Privacy: Linee guida in materia di Dossier sanitario

Pierfrancesco Maistrello mi ha segnalato le nuove "Linee guida in materia di Dossier sanitario" (4 giugno 2015) emanate dal Garante privacy:
- http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/4084632.

Una domanda che ci siamo fatti tutti e due riguarda i rapporti tra queste nuove linee guida e le "Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario" del 16 luglio 2009:
- http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/1634116.

Dovremmo leggerci con attenzione ambedue i provvedimenti e capire quali punti sono stati aggiornati.

Altra riflessione riguarda il termine "Linee guida": visto che poi sono usate come "normative", ci chiediamo perché non le titoli come "prescrizioni".

****

06- Privacy impact assessment

Del Privacy impact assessment (PIA) si parla sempre più diffusamente.

La vigente Direttiva 95/46 richiede di "ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi..." (secondo il testo del nostro Dlgs 196/2003). Il nostro sistema normativo prevedeva inoltre di redigere un Documento programmatico per la sicurezza con un'analisi del rischio relativo alla privacy.

Oggi le bozze di Regolamento Europeo in materia di privacy citano esplicitamente il Privacy impact assessment e alcuni lo stanno già prendendo in considerazione più seriamente dell'analisi del rischio prevista dal famigerato DPS (chissà perché).

Non conosco l'origine del termine, ma una breve ricerca su Google mi ha portato a leggere quelli della Homeland security USA. Essi, anche degli anni 2005-2006 sembrano delle informative estese:
- http://www.dhs.gov/privacy-impact-assessments

In Europa, per quello che è di mia conoscenza, si parla dei PIA dal 2009, quando la Commissione Europea ha emesso "Commission recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio- frequency identification (notified under document number C(2009) 3200) - (2009/387/EC)" in cui si chiede agli operatori di applicazioni RFID di predisporre una "sintesi delle valutazioni degli impatti su privacy e dati " e di descrivere i "rischi

verosimili relativi alla privacy, se esistenti, e all'uso di tag nelle applicazioni RFID e le misure che gli individuo possono prendere per mitigare quei rischi":
- https://ec.europa.eu/digital-agenda/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles

A quel punto, il Art. 29 WP (gruppo collegato alla Commissione Europea) ha emanato delle raccomandazioni per realizzare i PIA, complicando le cose, chiedendo un risk assessment e proponendo una sorta di linea guida abbastanza incompleta ma con una direzione precisa: identificare dei rischi (è proposta una lista di 15 minacce), valutarne gli impatti e la verosimiglianza, assegnare loro un livello (alto, medio, basso), descrivere i controlli di sicurezza, correlarli ai rischi (minacce) e specificare se il rischio risultante è accettable. La documentazione, del 12 gennaio 2011, si trova tra i documenti del WP 29; particolarmente importante è il " Annex: Privacy and Data Protection Impact Assessment Framework for RFID Applications":
- http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

La situazione è ancora accettabile. Poi la Commissione Europea è passata alle smart grid e nel 2014 ha promosso un modello per realizzare i PIA. Un malloppo di 74 pagine, che promuove una distinzione tra "eventi temuti" e "minacce" (lo studioso che è in me rabbrividisce) e una loro valutazione basata su parametri quali: facilità di identificazione degli interessati, impatti sugli interessati, facilità di riuscita di un attacco, capacità delle minacce di sfruttare le vulnerabilità. Questo per fornire un livello di rischio su 4 livelli, descrivere i controlli e stabilire se sono sufficienti. I documenti (incluso il DPIA template) si trovano qui:
- http://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters

Le cose peggiorano ancora. Il CNIL (Garante privacy francese), a luglio 2015, ha proposto le proprie linee guida, ovviamente basate sul modello più complicato (quello per le smart grid), anticipando l'analisi dei controlli rispetto all'analisi dei rischi e non fornendo indicazioni utili per correlare rischi e controlli. Sono in francese e in inglese:
- http://www.cnil.fr/linstitution/actualite/article/article/etude-dimpacts-sur-la-vie-privee-suivez-la-methode-de-la-cnil/;
- http://www.cnil.fr/english/news-and-events/news/article/privacy-impact-assessments-the-cnil-publishes-its-pia-manual/.

Ultimo attore: il ISO/IEC JTC1 SC27 WG5 che sta redigendo la ISO/IEC 29134, ora in stato di Committee Draft (cioè, nella migliore delle ipotesi, richiede altre 2 riletture tecniche e uscirà a fine 2016). Questa proposta ha un grande pregio: torna a chiedere un'analisi del rischio basata su due parametri (verosimiglianza e impatto).

Procedo con le conclusioni. Sono convinto della necessità delle analisi del rischio, ma quando vedo un eccesso di complicazione rabbrividisco perché capisco che la teoria (o la furbizia) sta prendendo il sopravvento sulla pratica. Spero che in questo campo non prendano troppo piede le interpretazioni "sbagliate" (come, per esempio, sono state quelle sulla custodia delle password e sul DPS iper-complicato, per citare quelle più ovvie).

Ringrazio Alessandro Cosenza di BTicino, che mi ha fornito molti dei riferimenti sopra citati.

Nota: ho proposto questo stesso articolo per europrivacy.info (di cui parlo nel seguito).

****

07- europrivacy.info

Alessandro Vallega di Oracle mi ha segnalato il sito http://europrivacy.info.

Si tratta di un osservatorio sul nuovo Regolamento EU sulla protezione dei dati personali promosso da AUSED, Clusit e la Oracle Community for Security.

Lo raccomando perché mi sembra un'iniziativa seria (conosco Alessandro personalmente e non posso pensare a qualcosa di meno) perché si tratta di un sito di aggiornamento e non di vendita di servizi basati sul nulla.

Gli stessi articoli sono seri. Per esempio, quanti di voi hanno letto che il DPO (Data protection officer), nell'ultima versione (bozza!) del Regolamento, non è più obbligatorio? Io l'ho scoperto proprio da questo sito:
- http://europrivacy.info/2015/06/20/data-protection-officer-no-more-mandatory

Un solo appunto: spero attivino al più presto l'RSS Feed del blog, in modo da poter essere aggiornato tempestivamente dei nuovi articoli.

Post scriptum: scrissi questo articolo su europrivacy.info prima che mi chiedessero di scrivere un articolo (aggratis). Quindi, non ci ho guadagnato nulla da tutto ciò. Peccato ;-)

****
08- DPO e il nuovo testo del Regolamento Privacy

Francesco Maistrello di Vecomp S.p.A., dopo aver letto il mio post su europrivacy.info, ha aggiunto informazioni in merito al fatto che ora la figura del DPO sembra non sarà più obbligatoria.

Francesco mi dice che il testo con DPO "non obbligatorio" è uno dei 3 testi che dovrebbero essere fusi insieme durante il trilogo, quello più morbido.

Francesco mi fornisce anche due link.

Il primo è di Viviane Reading, molto critica:
- http://www.euractiv.com/sections/infosociety/more-data-protection-better-less-315404.

Il secondo è il commento del WP art.29, di solito finora abbastanza ascoltato in materia; in particolare bisogna leggere a pagina 18:
- http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary.pdf.

Per i completisti, si faccia riferimento ai documenti della press release del WP art. 29 del 19 giugno:
- http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/index_en.htm

Ci tengo a ricordare una cosa: tutte queste questioni riguardano la bozza del regolamento, interessanti per chi, come me e Francesco, si interessa alla materia. Le aziende non dovrebbero fare nulla, visto che le tempistiche sono incerte (come per tutti i percorsi legislativi) e, comunque, per adottare i nuovi requisiti sarà previsto un periodo di transizione. Rimane il mio solito consiglio: non ascoltare chiunque cerca di vendere servizi relativi al futuro Regolamento privacy (uso "non ascoltare" per evitare polemiche; ma vorrei usare termini più duri).

AGGIUNTA. Francesco mi ha ricordato anche il rovescio della medaglia: quelli che avevano mappato i trattamenti e poi hanno abbandonato il lavoro fatto perché "tanto cambia la normativa". Dovremmo ricordare loro che comunque è da lì che si ripartirà. Inoltre questa mappa è utile con la normativa attuale: è un buon punto di partenza per fare della vera sicurezza delle informazioni (non sono informatica e non solo cyber) e le sanzioni non sono scomparse miracolosamente perché in futuro la normativa cambierà.

****

09- Industriale: standard e linee guida per la sicurezza IT

Dalla newsletter di HSC segnalo questa pubblicazione del Clusif dal titolo "Cybersécurité des systèmes industriels: par où commencer? Panorama des référentiels et synthèse des bonnes pratiques":
- http://www.clusif.fr/fr/production/ouvrages/pdf/CLUSIF-2014-SCADA-Panorama-des-referentiels.pdf.

Il documento è in francese (e usa troppo il termine "cybersécurité" al posto di "sicurezza informatica"). Il lavoro è notevole: hanno analizzato più di 50 documenti dedicati alla sicurezza informatica in ambito industriale e li hanno categorizzati (in settori industriali, in base al livello di specializzazione, in base al livello tecnico o gestionale, in documenti base o di approfondimento).

Nel documento sopra segnalato sono rappresentati i 21 documenti ritenuti più rappresentativi. In un altro documento sono invece analizzati tutti uno per uno:
- http://www.clusif.fr/fr/production/ouvrages/pdf/CLUSIF-2014-SCADA-Annexes-Fiches-de-lecture.pdf.

"Merci" ai colleghi francesi.

****

10- NIST SP 800-171 sulla protezione delle informazioni non classificate

Il NIST ha pubblicato la SP 800-171 dal titolo "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations":
- http://csrc.nist.gov/publications/PubsSPs.html#800-171

Si tratta di 76 pagine, ma quasi tutte inutili. Le pagine interessanti sono quelle del capitolo 3 (6 pagine) perché riportano un insieme di misure minime di sicurezza da adottare.

****

11- Slide DFA Open Day 2015 (digital forensics)

Segnalo che sono disponibili le presentazioni del DFA Open Day del 2 luglio 2015:
- http://www.perfezionisti.it/proposte-formative/dfa-open-day-2015/

Alcuni argomenti: i PIN dei cellulari, VoIP Forensics, investigazione di immagini digitali, profilazione online, applicazioni mobile di dating, diritto all'oblio, NodeXL, applicazioni mobile nell'ambito sanitario, standard europeo per lo scambio di digital evidence, Forensic Acquisition of Website.

Buona lettura!

****

12- Deep & Dark Web

Dal Security Summit di Roma segnalo la presentazione "Deep & Dark Web" di Stefano Ramacciotti e Pierluigi Paganini del G.d.L. "Educazione alla Sicurezza Informatica" del ISC2 chapter Italy:
-
https://www.securitysummit.it/static/files/ATTI%20ROMA%202015/10%20GIUGNO/10.06.2015_RAMACCIOTTI-PAGANIN.pdf

Interessante e inquietante.

****

13- User experience Vs. Design

Grazie a Marco Fabbrini per avermi segnalato questa meravigliosa foto sulle sfide tra user experience e design:
- https://twitter.com/arjunsethi/status/613473156469145600

****

14- DevOps e Microsoft

Stefano Ramacciotti mi ha segnalato il test dal titolo: "DevOps Self-Assessment: Moving you to the second decade of agile":
- https://profile.microsoft.com/RegSysProfileCenter/wizardnp.aspx?wizid=ba58aa87-54dc-4ffe-8066-05de46edb8a2

Il commento di Stefano è "anche se è targato MS mi sembra una cosa interessante".

In effetti, Microsoft è criticabile da molti punti di vista, ma il loro lavoro è sicuramente notevole se pensiamo alle complessità che devono affrontare.

Ho provato a fare il test, ma è certamente per persone (manager) che si occupano di sviluppo.

Per chi non volesse fare il test (anche perché non si fida a dare la propria e-mail a Microsoft, come se non ce l'avesse già...), può leggersi la loro pubblicazione di 21 pagine dal titolo "From Agile to DevOps at Microsoft Developer Division" (io però non l'ho ancora letto):
- https://www.microsoft.com/en-us/download/details.aspx?id=46920

****

15- Cisco Security Report 2015

Franco Ferrari di DNV GL mi ha segnalato la pubblicazione del Cisco Security Report 2015:
- http://www.cisco.com/c/en/us/products/security/annual_security_report.html.

Confesso che non ci ho trovato novità per me rilevanti, visto che è molto focalizzato su malware e attacchi dall'esterno.

Ho notato però un dato interessante: il 59% dei CISO (ossia i "dirigenti" della sicurezza) ritengono che i processi di sicurezza della propria azienda siano "ottimizzati". Questa sembra un'esagerazione, soprattutto se "solo" il 46% dei SecOps manager (ossia persone con mansioni più operative) ritiene la

stessa cosa. Trovo interessante questa diversa percezione mano a mano che si scende la scala gerarchica. Ad ogni modo mi sembrano comunque troppo ottimisti questi officier e questi manager.

****

16- Ransomware as-a-service

Dal gruppo Italian Security Professional di Linkedin segnalo questo articolo di McAfee:
- https://blogs.mcafee.com/mcafee-labs/meet-tox-ransomware-for-the-rest-of-us

Dalla rete TOR si accede ad un sito web attraverso il quale creare del ransomware, stabilire la quota del riscatto, gestire i proventi dell'attività, eccetera. Inquietante.

La cosa interessante: per contrastare questo tipo di malware, i normali antivirus non sono sufficienti; è invece necessario prevedere dei sistemi di intrusion prevention, whitelisting e sandboxing. Ci sono ancora molti che usano il proprio pc con privilegi di amministratore...

****

17- Cronaca: Black out informatico in Sicilia

Sandro Sanna mi ha segnalato la seguente notizia:
http://palermo.repubblica.it/cronaca/2015/06/15/news/stop_informatico_alla_regione_caos_nelle_asp_e_negli_uffici-116894666/

In sintesi: apparentemente, a seguito di debiti contestati, la società che ha in gestione i sistemi informatici della Regione Sicilia ha staccato la spina.

Il commento di Sandro: Sarei curioso di sapere come la Regione ha gestito il piano di business continuity...

****

18- Cronaca: Hacking Team

Può un blog o una newsletter o un twittatore che si occupano di sicurezza informatica non parlare di Hacking Team? Quindi lo faccio brevemente.

Segnalo un articolo in italiano e sintetico:
- http://www.massimomelica.net/hacking-team-spy-che-storia-di-cacca/

Quindi riassumo:
- un'azienda italiana vende armi (informatiche) a Governi anche non democratici;
- un'azienda di sicurezza informatica è stata vittima di un riuscito attacco informatico;
- sono disponibili su Internet dei nuovi exploit (ossia programmi che automatizzano alcuni attacchi informatici).

C'è qualche novità degna di discussione in blog, newsletter o tweet? Mi pare di no.

Certamente si può parlare di etica ("non si lavora con governi non democratici!"), di sociologia ("come è possibile che degli italiani brava gente lavorino per dei governi non democratici?"), di situazioni comico-avventurose ("lo spione è stato spiato con le sue stesse armi, ah ah ah") o della diffusione incredibile di

tecniche di attacco informatico (per questo ho già segnalato la presentazione di Ramacciotti e Paganini). Ma sono tutti argomenti o non pertinenti o troppo ribaditi per dedicarci altro tempo.

Qualche lezione, comunque, è emersa. Per esempio che alcuni exploit di Hacking Team si applicavano a smartphone sbloccati (a seguito di jailbreak) e quindi è sconsigliato fare il jailbreak (per iPhone) e il rooting (per Android) del proprio smartphone. Ma anche questa è cosa nota è stra-nota.

Segnalo le cose interessanti che ho visto su Twitter collegate a questa notizia:
- @DanielaQuetti segnala un'utilità della vicenda: "Per fortuna c'è Hacking Team l'estate era diventata noiosa tra caldo e Grecia...;-)";
- un articolo di Francesco Paolo Micozzi sulla valenza giuridica dei software spia (il pezzo ha titolo "Il caso Hacking Team e il rinnovato interesse per i captatori informatici" e si trova qui: http://www.huffingtonpost.it/francesco-paolo-micozzi/caso-hacking-team-captatori-informatici_b_7775152.html);
- Firefox blocca l'avvio automatico di Flash per evitare che le sue vulnerabilità vengano sfruttate (http://twib.in/l/5LkqoMgMG9G);
- @SwiftOnSecurity ricorda i prodotti da installare per evitare gli attacchi: Microsoft EMET; MalwareBytes Anti-Exploit; HitmanPro.Alert (lo sta valutando).

E anch'io ho scritto troppo su questa storia. A meno che qualcuno non voglia segnalarmi degli articoli un po' più interessanti di quelli che ho già visto.

****

19- Cronaca: Lombardia Informatica e privacy

Marco Fabbrini mi ha segnalato questo articolo:
- http://www.ilfattoquotidiano.it/2015/06/22/sanita-lombardia-appalti-milionari-poca-sicurezza-il-lato-oscuro-della-privacy-digitale/1782904/

In poche parole, un rapporto riservato di audit è uscito dalla società Lombardia Informatica; questo rapporto riguarda il sub-fornitore Santer e riporta 56 non conformità anche piuttosto gravi.

Ci ho messo un po' a capire come commentare questa notizia per almeno due motivi. Il primo è un conflitto di interessi che non intendo spiegare; il secondo è che l'articolo è evidentemente scandalistico e volevo capire meglio quanto prenderlo per buono. Osservate, per dirne una, che la Regione Lombardia paga a Santer 600 mila Euro al mese per il servizio, che comunque deve avere dei costi elevati a causa dei volumi del lavoro, mentre l'articolo li fa risultare dedicati alla sicurezza.

La diffusione di un rapporto del genere, inoltre, mi fa pensare a manovre di potere che poco hanno a che fare con la sicurezza delle informazioni. Chiunque ha le (poche) competenze per interpretare gli estratti del rapporto capisce che non tutti i rilievi sono necessariamente gravi (per esempio, nessuna delle mancanze è in realtà prescritta dalle misure minime dell'allegato B del Codice privacy, ma così viene fatto credere).

Che dire poi la nota finale sul fatto che l'audit è stato fatto pagare a Santer Reply? Ottima per il "uomo della strada", ma ridicola per chi mastica la materia e sa perché il rischio si "condivide" con i fornitori, non si "trasferisce" ai fornitori.

L'effetto, quindi, è quello di vedere un bambino che urla come un ossesso per un taglietto al dito. La situazione, seppure non così drammatica, rimane inquietante e spero ritorni sotto controllo (essendo io stesso lombardo e sapendo che i veri risultati, non quelli riportati dall'articolo, non vanno sottovalutati).

****

20- Cronaca: La guerra sulla crittografia

Segnalo questo lungo articolo (in inglese) su un argomento di attualità:
- http://www.dailydot.com/politics/encryption-crypto-war-james-comey-fbi-privacy/

In poche parole: l'FBI richiede ai produttori di software che fanno uso di meccanismi crittografici di mettere a disposizione delle forze dell'ordine una backdoor.

Ovviamente non è una buona idea (perché la backdoor potrebbe essere individuata anche dai "cattivi", perché ogni porta aperta è una vulnerabilità in più, perché nelle forze dell'ordine ogni tanto si trova una mela marcia, eccetera).

Questo articolo, quindi, ripercorre la vicenda attuale e il passato, citando Zimmerman, Clipper chip e altro.

****

21- Storia dell'insicurezza su Internet

Una serie di tre interessanti articoli del Washington Post sulla storia dell'insicurezza di Internet:
- http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/;
- http://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/;
- http://www.washingtonpost.com/sf/business/2015/06/22/net-of-insecurity-part-3/.

Certo: è giornalismo, quindi l'attenzione è più sulle storie (la nascita di Internet, il protocollo BGP e il gruppo L0pht), ma il tutto è accurato e interessante.

A chi piacciono gli schemi, segnalo anche questo elenco di "date importanti":
- http://www.washingtonpost.com/graphics/national/security-of-the-internet/history/.

Prego di notare la ragione di fondo dell'insicurezza di Internet: volevano fare le cose in fretta e che funzionassero e la sicurezza era vista come un ostacolo; alla peggio, si sarebbero fatte le correzioni necessarie in un secondo tempo. Ancora oggi, purtroppo, questo è l'approccio.

****

22- Multitasking e produttività

Da Twitter (@A1SiteSolutions), segnalo questo articolo su come il multitasking uccida la produttività:
- https://blog.todoist.com/2014/05/13/how-multitasking-slows-your-brain-and-kills-your-productivity/

Trovo interessanti le premesse, ma non tutte le conclusioni (avere due schermi non mi sembra una buona idea; bloccare l'e-mail o i siti social non credo sia efficace: bisognerebbe proprio spegnerli). Ognuno può trovare il metodo che ritiene più opportuno (la pagina segnalata riporta dei link), ma credo sia opportuno essere consapevoli dei problemi del multitasking.

****

23- Gruppi e fiducia

Segnalo questo post:
- http://share-coach.com/ita/articoli.php?id=52&read=storia

La trovo una bella sintesi sul buon funzionamento di un gruppo. Spesso ci dimentichiamo come sicurezza e qualità si basino prevalentemente sulle persone e che le persone agiscono mosse anche dal gruppo di cui fanno parte.

Sì... l'articolo è di mia sorella. Ma questo non è familismo. È la presa di coscienza che spesso parlo di tecniche, standard e tecnologia, ma è fondamentale non perdere di vista il lato decisamente umano delle materie di cui mi occupo, oltre ai soliti slogan ("la sicurezza e la qualità la fanno le persone"; "le persone sono fondamentali"; "il punto debole della sicurezza sono le persone").

****

24- Millennials, Generazione Z e sicurezza informatica.

Stefano Ramacciotti di (ISC)2 Italian Chapter (associazione promotrice, tra le altre cose, di interventi di sensibilizzazione, o awareness, sulla sicurezza informatica per studenti delle scuole, che finora ha raggiunto 13.000 persone) risponde al mio post dal titolo "I bambini possono insegnarci la sicurezza delle informazioni":
- http://blog.cesaregallotti.it/2015/05/i-bambini-possono-insegnarci-la.html

Riporto nel seguito le sue parole.
<<
Dalla mia esperienza personale, i nati dopo il 1980 sono messi veramente male a competenze di sicurezza. Sono infatti bravissimi ad usare i computer, ma sulla sicurezza sono, in genere, messi peggio delle persone più anziane.

Sono nati connessi, o quasi, e non sopportano le regole, a meno che non siano insegnate loro alle elementari (è per quello che preferisco fare lezione a quelli fino a 10 anni).

E' vero anche che le statistiche non sono "pesate" in base alla fascia d'età, ma è lecito supporre che le nuove generazioni, per la loro naturale necessità di essere sempre connessi, commettano grossolani errori a scuola e nelle aziende in cui sono stati da poco assunti.

Aggiungo che il termine Millennials è un termine che riguarda le persone nate tra il 1980 e il 2000, non quelle nate dopo il 2000, spesso indicate come parte della "Generazione Z".

Segnalo qualche articolo nel seguito.

Sui benefici di assumere le nuove generazioni
http://securityintelligence.com/security-management-embracing-millennials-in-your-security-program/#.VYGKlEbtPcB;

Why Millennials Are an Information-Security Threat
http://blogs.wsj.com/experts/2015/04/20/why-milliennials-are-an-information-security-threat/;

Do Millennials Believe in Data Security?
https://hbr.org/2014/02/do-millennials-believe-in-data-security/;

Millennials becoming known as Generation Leaky
http://www.csoonline.com/article/2884638/security-awareness/millennials-becoming-known-as-generation-leaky.html

Building the security bridge to the Millennials
http://www.csoonline.com/article/2134359/strategic-planning-erm/building-the-security-bridge-to-the-millennials.html

How security smart is Generation Y?
http://www.csoonline.com/article/2133845/strategic-planning-erm/how-security-smart-is-generation-y-.html

Will Millennials Be The Death Of Data Security?
http://www.darkreading.com/operations/wiil-millennials-be-the-death-of-data-security-/a/d-id/1318806

Are Millennials a greater security threat than other staff?
http://www.itworldcanada.com/post/are-millennials-a-greater-security-threat-than-other-staff

Are Millennials the Latest Security Threat?
http://www.softwareadvice.com/security/industryview/millennial-threat-report-2015/

Millennials And Smartphone Apps: Your Security Nightmare
http://www.informationweek.com/mobile/mobile-applications/millennials-and-smartphone-apps-your-security-nightmare/d/d-id/1320841
>>

Io chiudo ringraziando Stefano per il suo contributo.