Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – OTTOBRE 2017
****

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.

La newsletter è inviata via MailUp, offerta da Team Quality S.r.l.

Per iscriversi, cancellarsi e leggere l'informativa privacy: http://www.cesaregallotti.it/Newsletter.html.

Sulla stessa pagina è possibile consultare l'informativa sul trattamento dei dati personali.

****
Indice

****
00- Editoriale (newsletter, spam e link)

Il mese scorso l'invio della newsletter con MailUp non è andato molto bene: a molti è finita nello spam e i link non funzionavano (curiosamente venivano modificati dal sistema).

Per lo spam non so che dire (anche se MailUp dovrebbe proprio prevenire questo evento). Per i link, in questo numero semplicemente non li ho inseriti; quindi, a seconda del client di posta, alcuni non avranno il link e altri sì. Mi spiace. Io non riesco a trovare soluzioni (tranne cambiare fornitore).

Ogni altro suggerimento è benvenuto.

****

01- Linee guida WP 29 sulla DPIA

Premetto che, come spesso succede ultimamente, devo ringraziare Pierfrancesco Maistrello per la segnalazione e lo scambio di idee.

La notizia è che il Art. 29 WP ha pubblicato le sue linee guida sulla DPIA (Data privacy impact assessment). Si trovano alla pagina seguente, con il lungo titolo di "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01":
- http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

L'Art. 29 WP è paragonabile al "centro studi europeo sulla privacy", è collegato alla Commissione europea e i suoi pareri sono molto importanti.

Meglio ricordare che non tutti i titolari (o responsabili) devono predisporre una DPIA. La linea guida fornisce una tabella molto interessante in cui elenca alcuni trattamenti e se per loro è necessaria o meno una DPIA. E' bene comunque ricordare che è previsto che il Garante pubblichi un elenco più esaustivo di trattamenti per cui predisporre una DPIA.

Per il resto, il documento non specifica "come" fare una DPIA (per quello fornisce dei riferimenti in Annex 1), ma solo alcuni principi generali. Importante comunque l'Annex 2, che propone una lista delle caratteristiche che deve avere la DPIA.

Il messaggio, in sostanza, sembra essere: fatela come volete, purché rispetti i punti dell'Annex 2.

In questi giorni il WP 29 ha pubblicato le bozze di altre linee guida (sul data breach e sulla profilazione). Non le commento perché, appunto, sono in bozza.

****
02- Riconoscimento facciale e video porno

Letta da un certo punto di vista, la notizia (da Crypto-Gram di ottobre) è divertente: Pornhub vuole attivare un software per riconoscere gli attori (così gli utenti possono seguire i loro favoriti) e le posizioni:
- https://motherboard.vice.com/en_us/article/a3kmpb/facial-recognition-for-porn-stars-is-a-privacy-nightmare-waiting-to-happen.

Il problema sono gli attori amatoriali: un software del genere potrebbe collegarli alla loro identità reale.

Problema simile (sempre da Crypto-Gram) riguarda le persone che hanno due identità su Facebook. Il caso specifico riguarda chi offre servizi di sesso con un'identità e poi vive il resto della vita con un'altra. Facebook riesce comunque a capirlo e suggerisce ai contatti di un'identità di connettersi anche all'altra:
- https://gizmodo.com/how-facebook-outs-sex-workers-1818861596.

Certo, a molti questo fa sorridere. Ma software che sanno riconoscere le facce e software che sanno collegare cose tra loro scollegate su Internet (ma collegate nella vita reale)... pensiamoci...

****

03- ISO/IEC 27007 per gli audit ISO/IEC 27001

E' stata pubblicata la nuova edizione della ISO/IEC 27007 dal titolo "Guidelines for information security management systems auditing":
- https://www.iso.org/standard/67398.html.

Il documento riporta requisiti aggiuntivi rispetto alla ISO 19011. Le pagine sono tante perché è stata aggiunta un'Appendice con interpretazioni di alcuni requisiti della ISO/IEC 27001, compito svolto già dalla ISO/IEC 27003.

Parere personale: non la trovo utile.

****

04- Mio articolo sui requisiti di sicurezza delle applicazioni

Questo, dal titolo " Sviluppo sicuro delle applicazioni: i requisiti" l'ho scritto io:
https://www.ictsecuritymagazine.com/articoli/sviluppo-sicuro-delle-applicazioni-requisiti/.

****

05- Mio articolo sulle nuove specifiche NIST per le password

Considerazioni sulle nuove specifiche NIST per le password le avevo già scritte il mese scorso.

Sullo stesso argomento ho scritto un articolo per ICT Security Magazine un poco più lungo del post originario. L'articolo ha titolo "Nuove specifiche NIST per le password":
https://www.ictsecuritymagazine.com/articoli/nuove-specifiche-nist-le-password/.

****

06- Contratti fornitori - una presentazione

Segnalo questa presentazione del Club 27001 dal titolo "Contrôle des prestataires: Erreurs à ne pas commettre" (in francese):
- http://www.club-27001.fr/precedentes-reunions/paris/214-21-septembre-2017-transparents.html

L'ho trovata interessante soprattutto per quanto riguarda le riflessioni sul "diritto di audit". In effetti, spesso troviamo sui contratti una clausola molto generica e semplice. Invece la presentazione ci ricorda di considerare:
- quanti audit prevedere ciascun anno (e possibilità di cambiare la frequenza);
- tempi di preavviso e casi di audit straordinari o a sorpresa;
- garanzie sulla riservatezza delle informazioni raccolte durante l'audit;
- modalità di gestione dei rilievi di audit;
- conseguenze delle non conformità (fino alla rescissione del contratto.

Ho trovato altre cose interessanti nella presentazione e quindi la segnalo.

****

07- Il caso Equifax

Il primo a darmi notizia del caso Equifax è stato Sandro Sanna:
- http://money.cnn.com/2017/09/08/technology/equifax-hack-qa/.

Questo è un articolo più approfondito di Bloomberg (grazie a un tweet di @carolafrediani):
- https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros.

Equifax è un'azienda che raccoglie dati da varie compagnie (carte di credito, banche, eccetera) e fornisce valutazioni sulla situazione economica delle persone. Immagino sia ad una centrale del rischio.

Da quello che ho capito, gli attaccanti hanno sfruttato una vulnerabilità nota e pericolosa di Apache e sono riusciti ad accedere al sistema informatico di Equifax, ossia ai dati di 143 milioni di cittadini USA (pare ci siano anche dati di cittadini UK e chissà di chi altro).

Il caso è ovviamente esploso anche perché hanno scoperto che il responsabile della sicurezza informatica era una persona senza competenze tecnologiche (grazie ad Alberto Viganò per questa segnalazione):
- http://www.marketwatch.com/story/equifax-ceo-hired-a-music-major-as-the-companys-chief-security-officer-2017-09-15.

Alberto ha subito pensato ai nostri futuri DPO, spesso con competenze incerte.

Il caso, secondo me, è molto semplice, anche se la semplicità è nascosta dal polverone mediatico. Bisogna aggiornare dei server, ma nessuno lo fa perché bisogna interrompere il servizio per qualche tempo, richiede tempo, è noioso, ci sono cose più interessanti da fare. Il responsabile della sicurezza (anche se con competenze inadeguate), magari ha segnalato il problema, ha chiesto soldi per segmentare meglio la rete, ha telefonato ogni giorno ai sistemisti perché facessero gli aggiornamenti, ha chiesto ogni giorno ai "capi" di autorizzare l'interruzione del servizio per un'oretta. Ma tutti avevano cose più interessanti da fare e la manutenzione della "macchina IT" aveva priorità bassissima.

Anche noi, nel nostro piccolo, non abbiamo voglia di portare l'automobile a fare il tagliando o la revisione periodica e neanche il cambio gomme stagionale. Però lo facciamo perché sappiamo che è importante per la nostra sicurezza e perché le forze dell'ordine potrebbero bloccarci la macchina.

Semplicemente, i "capi" delle aziende non sono consapevoli di questo. Non si rendono conto che i sistemi informatici sono oggetti potentissimi ma anche delicatissimi e che richiedono manutenzione.

Semplice. L'avevo già detto, ma lo sappiamo tutti (basta parlare per qualche minuto di IT con qualunque manager italiano o straniero). E quindi la notizia dov'è? Solo nei numeri elevati di questo ennesimo caso.

****

08- Il caso dello spesometro

Da un tweet di @a_oliveri segnalo questo breve articolo sul "caso spesometro" che è finito anche sui giornali:
- https://www.avvenire.it/economia/pagine/spesometro-bloccato-il-sito.

Come è noto non riporto solitamente notizie di attacchi. Ma questa mi permette di ricordare che è corretto pensare agli attacchi e agli hacker e alle intrusioni da Internet, ma è necessario pensare anche agli interni o ai fornitori che fanno errori o che installano aggiornamenti dei software. Anzi, forse questi sono i più difficili da controllare ("dagli amici mi guardi Iddio, che ai nemici ci penso io").

****

09- Attacco a CCleaner

Un altro attacco che ho trovato interessante è quello a CCleaner:
- https://www.bleepingcomputer.com/news/security/ccleaner-compromised-to-distribute-malware-for-almost-a-month/;
- https://www.bleepingcomputer.com/news/security/avast-publishes-full-list-of-companies-affected-by-ccleaner-second-stage-malware/.

CCleaner è un'utilità che facilita la pulizia di disco, memoria e configurazioni di Windows. Qualcuno si è introdotto nei server di sviluppo e ha inserito del codice dannoso nei sorgenti di CCleaner.

Certamente gli attacchi possono essere più numerosi verso chi sviluppa prodotti di sicurezza (anche se CCleaner non è propriamente un prodotto di sicurezza), ma questo poteva capitare a tanti. Soprattutto in pochi, a differenza del produttore di CCleaner (da poco acquisito da Avast), si sarebbero accorti del problema.

Quindi: prestare attenzione ai prodotti che si installano sui propri pc e sulla propria rete. Soprattutto attenzione, come purtroppo fanno molti sistemisti, a installare prodotti in prova sulla rete aziendale.

L'attacco è stato rilevato grazie alla "recente" installazione del prodotto Morphisec della Cisco. Quindi ho un dubbio di quale sia la causa e quale l'effetto. Ma mi rendo conto che sto esagerando. Forse ;-)

****

10- Attacco a Verizon (e ai server sul cloud)

In questi giorni le notizie di attacco sono numerose.

Una su Deloitte: http://money.cnn.com/2017/09/25/technology/deloitte-hack-cybersecurity-guardian/index.html (da tweet di @stevedeft; probabilmente per un server DNS non in completa sicurezza con servizi RDP aperti su Internet);
Una sulla SEC: http://money.cnn.com/2017/09/21/news/sec-edgar-hack/index.html?iid=EL.

La più interessante, a mio parere, è quello di Verizon (dal Sans NewsBites):
http://www.zdnet.com/article/another-verizon-leak-exposed-confidential-data-on-internal-systems/.

Infatti l'attacco a Verizon è avvenuto su server sul cloud AWS. Uno studio più ampio (accennato su https://www.cyberscoop.com/verizon-wireless-s3-bucket-public-access-kromtech/) dimostra che sono tantissimi i server S3 non correttamente configurati.

Qui ripeto quanto già detto in altre occasioni e con altre parole: il cloud non è il bene né il male; purtroppo molti comprano server in cloud senza capire di cosa si tratta; pensano di risparmiare, fino a pensare di non avere più bisogno di sistemisti capaci di fare il loro lavoro (ho visto casi del genere). Invece un server in cloud va configurato e mantenuto come gli altri, senza poter risparmiare chissà quali cifre.