Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – NOVEMBRE 2018

****

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

Come alla fine di ogni anno, mi prendo un piccolo spazio per fare gli auguri di Buone feste a tutti i miei lettori.

Quindi: auguri!

****

01- Sicurezza da dilettanti

Bruce Schneier, nell'ultimo numero di Crypto-Gram, ha pubblicato un breve articolo dal titolo "Worst-Case Thinking Breeds Fear and Irrationality":
- https://www.schneier.com/blog/archives/2018/11/worst-case_thin_1.html.

Ha colto l'idea da una notizia da Brighton: un tizio vede un adulto e una bambina e chiama la polizia dicendo di aver visto un adulto rapire una bambina; la polizia interviene con tutto l'armamentario del caso e poi scoprire che si trattava di un padre con la propria figlia.

Ultimamente sto notando l'ansia eccessiva intorno ai bambini e non mi stupisce che ci siano persone che o ne approfittano o dimostrano ulteriore ansia.

Bruce Schneier conclude dicendo che se ci si rivolge ai dilettanti, non bisogna stupirsi se poi si fa una sicurezza da dilettanti. Mi sembra un'ulteriore riflessione degna di nota.

Io invece rifletto che le statistiche sono poche (pare che negli USA si parli di 105 casi all'anno; ma non ho trovato ricerche che diano dettagli sulle età, sui diversi tipi di sparizione, sulla certezza delle cause di sparizione, eccetera) e quasi nessuno legge le poche a disposizione; crescono le notizie false, i conseguenti allarmi falsi e la successiva ansia ingiustificata. Questo succede anche nella sicurezza delle informazioni (e lo si è visto con la "corsa al GDPR").

Osservate per esempio le notizie di questo mese, come di ogni mese. Alcune sono relative a linee guida sulle misure di sicurezza, spesso formulate in modo generico oppure in formato di "rapporto di audit". Altre notizie riguardano rapporti di sicurezza che in realtà riportano percezioni, non dati. Altre notizie ancora riguardano incidenti, senza però un'attenta analisi delle cause (nella migliore delle ipotesi insegnano a installare gli aggiornamenti).

Eppure queste notizie sono inoltrate, ri-twittate, ri-linkedinate, cuoricinate, pollice-in-su-ate, mi-piacie-ate eccetera (anche da me). Creano solo tanto rumore e insegnano poco.

Il risultato è sotto gli occhi di tutti: enti regolatori che richiedono sempre più documenti sempre più verbosi anche se non molto interessanti, auditor che si ostinano a richiedere cose inutili da un punto di vista gestionale (per esempio, misurazioni) e tecnico (per esempio, firmare un modulo di ingresso alle sale macchine), esperti che ripetono a pappagallo cose oggi ritenute superate (per esempio, il cambio periodico delle password per evitare che vengano indovinate o la cancellazione sicura in 37 passaggi), esperti privacy che si interrogano ancora della sparizione dei responsabili interni, degli incaricati e delle nomine.

C'è un metodo per migliorare? Per me sì, ed è selezionare. Anzi: leggere, capire, decidere se la notizia dice qualcosa di nuovo, se sì, inoltrare. Anche a costo di avere pochi follower, amici o contatti.

Personalmente, sicuramente dovrò ridurre il numero di notizie (e già lo faccio, evitando di parlare delle violazioni di catene alberghiere, compagnie aeree o simili, visto che gli articoli che ho trovato si dilungano sul nulla).

****

02- OWASP per applicazioni per dispositivi mobili

OWASP ha recentemente pubblicato due documenti interessanti sulla sicurezza delle applicazioni per dispositivi mobili. Sono gratuiti e si possono trovare sul sito di OWASP:
- https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide.

Segnalo in particolare il pdf per la "Mobile Security Testing Guide (MSTG)" - 1.1.0 Release (406 pagine):
- https://github.com/OWASP/owasp-mstg/releases.

La "Mobile App Security Requirements and Verification" è ora alla versione 1.1 ed è di più rapida lettura (30 pagine). Si può scaricare direttamente dal sito di OWAS (dalla prima pagina indicata in questo post).

Le tabelle della "Mobile App Security Requirements and Verification" sono disponibili anche in Excel:
- https://github.com/OWASP/owasp-mstg/tree/master/Checklists.

****

03- Sviluppo sicuro: tipi di scansione

Segnalo questo articolo su ICT Security Magazine dal titolo "Sviluppo sicuro del codice… 4 semplici domande a 3 strati di una cipolla":
- https://www.ictsecuritymagazine.com/articoli/sviluppo-sicuro-del-codice-4-semplici-domande-a-3-strati-di-una-cipolla/.

Mi pare che questo articolo faccia chiarezza sulle 3 analisi di sicurezza del codice:
- scansione statica del codice, da fare con strumenti automatici in ambiente di sviluppo e test;
- scansione dinamica del codice, da fare con strumenti parzialmente automatici in ambiente di test;
- penetration test, da fare con vari strumenti in ambiente di produzione.

Mi piacciono le argomentazioni proposte, anche se mi rimangono alcune domande:
- la scansione dinamica va fatta coinvolgendo specialisti o può essere fatta dagli stessi sviluppatori (osservando che i PT rientrano nel primo caso)?
- quali strumenti sono oggi ritenuti più interessanti per le scansioni statiche e dinamiche?

****

04- Guida per la sicurezza informatica sulle navi

Dal SANS NewsBites del 14 dicembre, segnalo la notizia della pubblicazione, del documento "The guidelines on cyber security onboard ships":
- https://iumi.com/news/blog/bimco-the-guidelines-on-cyber-security-onboard-ships.

L'articolo di ZDnet suggerito dal SANS NewsBites si concentra troppo sugli incidenti registrati negli ultimi anni:
- https://www.zdnet.com/article/ships-infected-with-ransomware-usb-malware-worms/.

L'esercizio sugli attacchi è interessante non tanto per l'impatto giornalistico, ma perché evidenzia lo sforzo di analisi fatto. Questo sforzo si riflette anche sulla descrizione delle misure e sulle altre parti del documento, che ripetono sì le "solite cose", ma ben personalizzate per l'ambiente di riferimento. Questo include una breve riflessione sulla differenza tra i sistemi informatici tradizionali (IT system) e quelli industriali o, nel caso, della nave (Operational system o OT system).

Segnalo poi, accanto alla completezza, la sinteticità del documento: 56 pagine.

****

05- Pentesting

Pentesting (con un piccolo e divertente gioco di parole):
- https://nymag.com/strategist/article/best-pens-gel-ballpoint-rollerball-felt-fountain.html.

E' vero: non c'entra niente con le notizie che do di solito. Però è divertente.

****

06- Sicurezza nei sistemi missilistici USA

Giulio Boero su LinkedIn mi ha consigliato questa notizia dal lungo titolo "Security Controls at DoD Facilities for Protecting Ballistic Missile Defense System Technical Information DODIG-2019-034":
- http://www.dodig.mil/reports.html/Article/1713611/security-controls-at-dod-facilities-for-protecting-ballistic-missile-defense-sy/.

Gli ispettori del US Department of Defense (DOD) Office of Inspector General (OIG) hanno elencato le carenze in materia di sicurezza informatica presso l'US ballistic missile defense systems (BMDS).

In sintesi:
- non è presente un meccanismo di autenticazione a 2 fattori;
- le vulnerabilità di rete non sono state mitigate;
- i rack non sono chiusi a chiave;
- i media rimovibili non sono sufficientemente monitorati e protetti;
- le trasmissioni non sono cifrate;
- non è attivo un IDS sulla rete classificata;
- non sono disponibili giustificazioni scritte per elevare i privilegi degli utenti.

Nulla di nuovo o di specifico. Certamente alcune cose fanno paura.

Però segnalo che tutto manca di contesto. Per esempio: i rack non sono chiusi a chiave, ma l'accesso al data centre è controllato? quali vulnerabilità di rete non sono state mitigate e si tratta di vulnerabilità visibili all'esterno della rete?

Alcune cose, però, sono ingiustificabili, come per esempio l'assenza di 2FA e di trasmissioni cifrate.

Insomma: notizia che mi ha impressionato soprattutto perché vedo che negli USA rendono pubbliche queste cose.

****

07- Linee guida ENISA per gli audit NISD

Franco Vincenzo Ferrari di DNV GL mi ha segnalato questa pubblicazione di ENISA dal titolo "Guidelines on assessing DSP security and OES compliance with the NISD security requirements":
- https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements.

Si tratta di una guida per gli audit interni per i "Digital service provider" (DSP) e gli operatori di servizi essenziali (OES) che vogliono conformarsi ai requisiti della Direttiva NIS e per gli audit che potrebbero condurre le autorità nazionali (national competent authorities o NCA o, in Italia, le "autorità competenti NIS") sempre sulle società a cui è indirizzata la NIS.

Della NIS ne parlai tempo fa:
- http://blog.cesaregallotti.it/2018/06/direttiva-nis-in-vigore-veramente.html.

Ho trovato alcuni punti confusi qua e là (mi chiedo, per esempio, perché usare la definizione di audit dell'ISACA, che non richiama la conformità, e non altre, perché confondano metodologie di valutazione del rischio come il CRAMM con altri documenti come la ISO/IEC 27001; perché citino il CRAMM non più mantenuto dal 2003 o perché usino il termine "ecosistema"). Però ho trovato molto interessanti i due elenchi di misure da considerare perché presentano un elenco di misure che possiamo considerare come "minime" nell'ambito NIS.

Confermo quello che ho scritto: apprezzo questo lavoro che parte dalle basi e ne suggerisco la lettura.

****

08- Articolo sulla blockchain

Mi ero ripromesso di non occuparmi più di blockchain, dopo aver visto che si tratta, nei casi che riguardano il mio lavoro, di una bufala. Ma come fare? Troppi articoli e troppa pubblicità; troppi venditori di fumo o, per chi apprezza l'importazione, di snakeoil.

Allora rilancio con un articolo dal programmatico titolo di "La blockchain è una tecnologia scadente e una pessima idea per il futuro":
- https://thevision.com/innovazione/blockchain/.

Segnalo ulteriori perplessità su questa tecnologia, riportate da un articolo che avevo segnalato ad agosto (https://medium.com/@kaistinchcombe/decentralized-and-trustless-crypto-paradise-is-actually-a-medieval-hellhole-c1ca122efdec).

****

09- NIST Risk management framework

Il NIST ha pubblicato la rev. 2 del SP 800-37 dal titolo "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy":
- https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

Solitamente apprezzo le pubblicazioni del NIST, ma questa mi pare un rifacimento di cose vecchie. In particolare ripropone una valutazione del rischio basata sugli asset senza ulteriori riflessioni.

Dal NIST, poi, speravo di ricevere un maggior numero di esempi, che invece non ci sono.

Come pragmatismo, infine, non posso non notare quanto si aggrovigli sui concetti di "autorizzazione", dedicandoci anche due appendici per un totale di 32 pagine. Se ho capito correttamente, si tratta di "approvazione del rischio residuo e del piano di trattamento" e, quindi, parte delle riflessioni riguardano le responsabilità dei sistemi, visto che spesso si intrecciano in forme non facilmente discernibili.

****

10- Standard: Pubblicata la ISO/IEC 29101 "Privacy architecture framework"

E' stata pubblicata la seconda edizione della ISO/IEC 29101 "Privacy architecture framework":
- https://www.iso.org/standard/75293.html.

Questa versione del 2018 sostituisce quella del 2013.

Nella prefazione è detto che la modifica più significativa è l'eliminazione dell'Appendice D, dove i "controlli privacy" erano correlati ai "controlli della ISO/IEC 27001:2005".

Personalmente pensavo che la versione del 2013 fosse una roba inutile. Continuo a pensarlo della versione del 2018.

****

11- Cyber lexicon

Enrico Luigi Toso mi ha segnalato questo Cyber Lexicon:
- http://www.fsb.org/2018/11/cyber-lexicon/.

E' stato preparato dall'FSB, quindi è indirizzato al settore finanziario. Però può essere di interesse per tutti.

****

12- Executive Perspectives on Top Risks for 2019 di Protiviti

Segnalo questo documento di Protiviti dal titolo "Executive Perspectives on Top Risks for 2019":
- https://www.protiviti.com/IT-it/insights/protiviti-top-risks-survey.

Io ho molte perplessità di fronte a queste indagini, visto che sono palesemente guidate. Inoltre trovo eccessivamente pomposo il sottotitolo "Key Issues Being Discussed in the Boardroom and C-Suite".

Però trovo interessante il lavoro preparatorio di selezione di 30 rischi da sottoporre agli intervistati. Sono convinto si tratti di una selezione condotta tra i vari consulenti e che quindi sia maggiormente significativa delle successive analisi sui 10 rischi "più significativi".

Molti sono rischi non operativi (per la qualità o la sicurezza delle informazioni), ma fanno parte del "contesto" di cui tanto si parla con gli standard relativi ai sistemi di gestione e basati sull'HLS (ISO 9001:2015, ISO/IEC 27001:2013, ISO/IEC 20000-1:2018 e così via). Consiglio quindi una lettura della tabella 1 (pagine 4, 5 e 6).

****

13- Privacy: Libro "European Data Protection" di IAPP

Per prepararmi all'esame CIPP/E dell'IAPP ho letto il libro ufficiale dell'IAPP.

Ne consiglio la lettura perché mi pare scritto bene e in modo pragmatico, anche se si tratta sempre di un libro teorico.

Riporto il commento di Pierfrancesco Maistrello: "Mi ha insegnato cose che non sapevo, e ogni tanto fa sintesi concettuali che in italia o te le fai da solo, se hai tempo e sei capace, o te le scordi".

Penso che in Italia si paghino gli interventi troppo concettuali di questi anni.

Comunque... il libro si trova in versione digitale e cartacea sul sito dell'IAPP:
- (digitale) https://iapp.org/store/books/a191a000002FJK5AAO/;
- (cartacea) https://iapp.org/store/books/a191a000002F94uAAC/.

****

14- Privacy: Linea Guida EDPB sull'applicazione territoriale del GDPR

Questa "Guidelines 3/2018 on the territorial scope of the GDPR" dell'EDPB la segnalo perché l'applicazione territoriale del GDPR mi ha dato da pensare in un paio di occasioni:
- https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-32018-territorial-scope-gdpr-article-3_en.

Al momento è solo in inglese.

Non l'ho ancora letta, ma il testo di accompagnamento del nostro Garante copre i miei punti di attenzione:
- https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9065814#3.

****

15- Privacy: Regolamento UE contro il geo-blocking

Ivo Trotti di Kantar Italia, visto il mio interesse in materia di accessibilità, mi ha segnalato questo:
- https://www.consorzionetcomm.it/notizie/entra-in-vigore-il-regolamento-sul-geoblocking.kl.

E' quindi possibile accedere alla pagina ufficiale della UE sulla materia:
- https://ec.europa.eu/digital-single-market/en/faq/geo-blocking.

In sostanza, da quando entrerà in vigore il Regolamento, non sarà più possibile, per i siti di uno Stato membro, bloccare l'accesso o i pagamenti a utenti di altri Stati membri, pratica che è invece vista come discriminante.

****

16- Servizi fiduciari: PEC o SERCQ? Scenari dal 1 gennaio 2019

Franco Vincenzo Ferrari di DNV GL mi ha segnalato questo articolo dal titolo "Dalla PEC al domicilio digitale, il passaggio nel 2019: ecco che può succedere":
- https://www.agendadigitale.eu/documenti/fatturazione-elettronica/dalla-pec-al-domicilio-digitale-il-passaggio-nel-2019-ecco-che-puo-succedere/.

In sostanza, la PEC non sarà più regolamentata ai sensi dell'articolo 48 del CAD. Quindi ci sarà una migrazione verso il Servizio di recapito certificato (SERC), regolamentato invece dal Regolamento eIDAS.

Nell'articolo sono presentati dei possibili scenari futuri. A mio parere, per chi non deve qualificarsi esperto della materia, è importante sapere che ci sarà una migrazione ed evitare, quando ci sarà, di fare la faccia stupita.

****