Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – GENNAIO 2020

****

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

****

01- Attacco Idiot wind

Prendo a prestito il titolo di una canzone di Bob Dylan (di un grande album) per nominare il seguente tipo di attacco, successo veramente anche se anonimizzato (ringrazio la persona che me lo ha segnalato).

Una società produce molta documentazione cartacea. Quindi la raccoglie e la digitalizza (scansione). Quindi raccoglie la documentazione cartacea ormai digitalizzata e la distrugge con distruggi-documenti. Però un giorno succede che qualcuno apre la finestra e i documenti in attesa di essere distrutti volano via, in strada.

Salva la disponibilità e l'integrità delle informazioni (visto che i documenti erano già stati acquisiti), ma non la riservatezza.

Qualcuno mi ha detto che avrebbero dovuto distruggere i documenti appena acquisiti, ma bisogna stare attenti a dare soluzioni senza conoscere la realtà (neanche io la conosco). Forse le acquisizioni sono a lotti e questi lotti vanno verificati bene prima di procedere alla distruzione degli originali o forse la procedura solita bilanciava bene le esigenze di qualità ed efficienza o chissà.

****

02- Attacco "Loss of supplier"

Ad un mio cliente è successo: un fornitore di assistenza specialistica informatica ha chiuso i battenti da un giorno all'altro. Così il cliente, al primo incidente, ha impiegato molto più tempo del previsto a risolverlo e adesso teme che l'incidente si possa ripetere, visto che la correzione non è stata approvata dal fornitore.

L'errore del software ha mandato in errore altri apparati e anche questo incidente è stato risolto dopo molto più tempo del previsto perché il contratto prevedeva assistenza in orario lavorativo e non 24/7/365.

Lo segnalo per ricordarci che le "cose che non succedono mai" succedono.

Ho ovviamente anonimizzato il più possibile.

****

03- Red and blue team (seconda puntata)

Avevo scritto dei red e blue team, concludendo che mi sembravano nuovi nomi per vecchie cose:
- http://blog.cesaregallotti.it/2019/12/red-and-blue-team.html.

Niccolò Castoldi mi ha segnalato un articolo che dettaglia le differenze tra red team e penetration tester e tra blue team e SOC:
- https://danielmiessler.com/study/red-blue-purple-teams/.

In sintesi, l'articolo dice che il red team svolge attività continuative di test, mentre i penetration tester svolgono attività in tempi e ambiti predefinitivi; i blue team svolgono attività costante di ricerca e di miglioramento, mentre i SOC sono solo reattivi.

Come spesso succede nel campo dell'informatica (e non solo), bisogna sapere quali sono i termini in uso, essere consapevoli che non tutti li usano allo stesso modo e che bisogna chiarire con gli interlocutori cosa intendono con certi termini quando li usano (e aspettarsi di essere guardati con la faccia di chi pensa di dirti un'ovvietà e quindi di dovergli rispondere che non lo è).

****

04- Privacy: Articolo sullo stato delle certificazioni ISO/IEC 27701

Con Andrea Caccia e Fabio Guasconi ho scritto un articolo dal titolo "Stato delle certificazioni ISO/IEC 27701":
- https://www.cybersecurity360.it/soluzioni-aziendali/gdpr-e-certificazioni-tutto-sulla-norma-iso-iec-27701/.

Ora ha titolo "GDPR e certificazioni, tutto sulla norma ISO/IEC 27701" ma, insomma, l'articolo è quello.

****

05- Privacy: Due articoli sul GDPR (violazioni e sistema di gestione)

Daniele Santucci mi ha segnalato due suoi articoli sulla privacy.

Il primo ha titolo "Data breach e modelli preventivi di gestione delle non conformità: strategie di compliance":
- https://www.cybersecurity360.it/legal/privacy-dati-personali/data-breach-e-modelli-preventivi-di-gestione-delle-non-conformita-strategie-di-compliance/.

Il secondo ha titolo "Sistema di gestione privacy come modello per il controllo dei dati personali: una proposta operativa":
- https://www.cybersecurity360.it/legal/privacy-dati-personali/sistema-di-gestione-privacy-come-modello-per-il-controllo-dei-dati-personali-una-proposta-operativa/.

Si tratta di articoli abbastanza "di base", ma interessanti.

****