Parte I

Recepimento degli Orientamenti dell'EBA in materia di segnalazione dei gravi incidenti del 19 dicembre 2017 (EBA/GL/2017/10)

Con riferimento al Cap. 4 – Sez. 1 – Par. 3 – Definizioni - definizione di "grave incidente di sicurezza informatica*"[… è probabile che derivi*…], si evidenzia oltre all'incremento del numero degli eventi da segnalare anche l'introduzione di una sorta di misurazione in termini di probabilità a differenza di quanto espresso in termini di "potenziali impatti" utilizzato in altre parti della presente normativa. In considerazione dei fini statistici della raccolta da parte del Regulator si chiede di eliminare la parola probabile e limitarsi solo agli incidenti con un reale impatto.

Recepimento degli Orientamenti dell'EBA sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento del 12 gennaio 2018 (EBA/GL/2017/17)

Con riferimento al Cap. 4 Sez. 7 Par. 1 – Sicurezza dei servizi di pagamento – 2^ linea punto a) *[…in termini di* ***criticità*** *…*], si chiede di meglio definire il significato di "criticità."

Con riferimento al Cap. 5 – Sez. 2 – Par. 1 E Par. 2 – Nota 1 e Nota 2, si chiede di spiegare meglio in che misura il piano di continuità si debba attenere agli orientamenti dell'EBA sulla sicurezza dei pagamenti via Internet e sulle misure di sicurezza per i rischi operativi come recepiti nel Cap. 4, inteso come ampliamento del concetto di scenario di crisi vs. un concetto di indisponibilità del servizio

Con riferimento al Cap. 5 – Sez. 2 – Par. 3.5 Le verifiche, si chiede se il primo comma *[… gli intermediari sottopongono… processi critici*] possa essere ricompreso a livello di principio nel concetto di verifiche complessive già incluso nel comma 3 o se manifesti un differente approccio operativo e quindi una modifica sostanziale dell'approccio alle verifiche.

Stante la Sez. VII – 2 – Disposizioni transitorie
"*Le banche che prestano servizi di pagamento mediante uso del canale internet applicano le disposizioni degli "Orientamenti finali in materia di sicurezza dei pagamenti via internet" secondo il regime transitorio delineato dall'ABE nella "Opinion on the transition from PSD1 to PSD2" del 19 dicembre 2017 e fino 14 settembre 2019, data di applicazione del Regolamento delegato della Commissione del 27 novembre 2017 n. 2018/389 riguardante le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri previsti dall'articolo 98, paragrafo 4, della direttiva 2015/2366/UE (PSD2)*."

Riteniamo che le definizioni incluse nella Sez I- 3 – Definizioni (in particolare le voci "autenticazione", "autorizzazione", "credenziali") debbano rispettare tale disposizione transitoria e quindi tenere conto delle "nuove" definizioni incluse nella Direttiva 2015/2366/UE (PSD2) (Rif. Articolo 4 – Definizioni), che differiscono dalle precedenti.

Più in generale, segnaliamo che il 13 dicembre u.s. sono state pubblicate in consultazione da EBA, delle nuove linee guida (Guidelines on ICT and security risk management) che, viene indicato, integrano quanto previsto dai precedenti Orientamenti EBA sulle misure di sicurezza per i rischi operativi e per la sicurezza dei servizi di pagamento (EBA/GL/2017/17), che pertanto saranno abrogati al momento dell'entrata in vigore di quelle attualmente in consultazione.

Con la presente si intende chiedere se Banca d'Italia, nel predisporre il presente aggiornamento della Circolare 285, abbia già tenuto conto del testo in consultazione relativo agli Orientamenti in materia di gestione del rischio informatico e di sicurezza, o se tali nuovi orientamenti saranno considerati successivamente.

Altresì, si chiede conferma che l'aggiornamento della Circolare 285 attualmente in consultazione, sempre con riferimento agli Orientamenti EBA sulle misure di sicurezza per i rischi operativi e per la sicurezza dei servizi di pagamento (EBA/GL/2017/17), non subirà slittamenti dovuti alla loro prevista succitata abrogazione.

Parte II

Recepimento delle Raccomandazioni dell'EBA in materia di esternalizzazione a fornitori di servizi cloud del 28 marzo 2018 (EBA/REC/2017/03)

Nessuna osservazione.

Parte III

Recepimento delle "Guidelines on the conditions to be met to benefit from an exemption from contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC)" dell'EBA (EBA/GL/2018/07)

Nessuna osservazione.