REGOLAMENTO DI ESECUZIONE (UE) 2018/151 DELLA COMMISSIONE

del 30 gennaio 2018

recante modalità di applicazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio per quanto riguarda l'ulteriore specificazione degli elementi che i fornitori di servizi digitali devono prendere in considerazione ai fini della gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi e dei parametri per determinare l'eventuale impatto rilevante di un incidente

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

vista la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione ([1]), in particolare l'articolo 16, paragrafo 8,

considerando quanto segue:

(1) Conformemente alla direttiva (UE) 2016/1148, i fornitori di servizi digitali rimangono liberi di adottare le misure tecniche e organizzative che ritengono adeguate e proporzionate alla gestione dei rischi che corre la sicurezza delle loro reti e dei loro sistemi informativi, purché tali misure garantiscano un adeguato livello di sicurezza e tengano conto degli elementi previsti da detta direttiva.

(2) Nell'individuazione delle misure tecniche e organizzative adeguate e proporzionate, il fornitore di servizi digitali dovrebbe affrontare la questione della sicurezza informatica in modo sistematico, ricorrendo a un approccio basato sui rischi.

(3) Al fine di garantire la sicurezza dei sistemi e degli impianti, i fornitori di servizi digitali dovrebbero effettuare procedure di valutazione e di analisi. Tali attività dovrebbero riguardare la gestione sistematica delle reti e dei sistemi informativi, la sicurezza fisica e dell'ambiente, la sicurezza delle forniture e i controlli dell'accesso.

(4) Nello svolgimento di un'analisi dei rischi nell'ambito della gestione sistematica delle reti e dei sistemi informativi, i fornitori di servizi digitali dovrebbero essere incoraggiati a individuare i rischi specifici e a quantificarne l'importanza, ad esempio individuando le minacce alle risorse critiche e il modo in cui incidono sulle operazioni, e determinando il modo migliore per attenuare tali minacce sulla base delle capacità correnti e delle esigenze in termini di risorse.

(5) Le politiche in materia di risorse umane potrebbero fare riferimento alla gestione delle competenze, inclusi gli aspetti connessi allo sviluppo delle competenze correlate alla sicurezza e alla sensibilizzazione. Nel decidere in merito a una serie di politiche adeguate in materia di sicurezza di funzionamento, i fornitori di servizi digitali dovrebbero essere incoraggiati a tener conto degli aspetti relativi alla gestione dei cambiamenti, alla gestione delle vulnerabilità, alla formalizzazione delle pratiche operative e amministrative e alla mappatura del sistema.

(6) Le politiche in materia di architettura di sicurezza potrebbero comprendere in particolare la segregazione delle reti e dei sistemi, nonché misure di sicurezza specifiche per le operazioni critiche quali ad esempio le operazioni amministrative. La segregazione delle reti e dei sistemi potrebbe consentire ai fornitori di servizi digitali di distinguere elementi quali i flussi di dati e le risorse informatiche appartenenti a un cliente, a un gruppo di clienti, al fornitore di servizi digitali o a terzi.

(7) Le misure adottate per quanto riguarda la sicurezza fisica e dell'ambiente dovrebbero garantire la protezione delle reti e dei sistemi informativi dell'organizzazione dai danni causati da incidenti quali furti, incendi, inondazioni o altre condizioni meteorologiche, problemi di telecomunicazione o interruzioni di corrente.

(8) La sicurezza dell'erogazione, ad esempio per quanto riguarda l'energia elettrica, il combustibile o il raffreddamento, potrebbe includere la sicurezza della catena di approvvigionamento che comprende, in particolare, la sicurezza dei contraenti e subcontraenti terzi e la loro gestione. La tracciabilità delle forniture critiche si riferisce alla capacità del fornitore di servizi digitali di identificare e registrare le fonti delle forniture.

(9) Gli utenti dei servizi digitali dovrebbero comprendere le persone fisiche e giuridiche che sono clienti o abbonati di un mercato online o di un servizio di *cloud computing*, o che visitano il sito web di un motore di ricerca online allo scopo di effettuare ricerche con parole chiave.

([1]) GU L 194 del 19.7.2016, pag. 1.

(10) Nel definire la rilevanza dell'impatto di un incidente, i casi previsti dal presente regolamento dovrebbero essere considerati un elenco non esaustivo di incidenti rilevanti. Occorre trarre insegnamenti dall'attuazione del presente regolamento e dal lavoro del gruppo di cooperazione per quanto riguarda la raccolta di informazioni sulle migliori pratiche in relazione ai rischi e agli incidenti e le discussioni sulle modalità di comunicazione delle notifiche di incidenti di cui all'articolo 11, paragrafo 3, lettere i) e m), della direttiva (UE) 2016/1148. Potrebbero risultarne orientamenti esaustivi sulle soglie quantitative dei parametri di notifica atte a far scattare l'obbligo di notifica per i fornitori di servizi digitali a norma dell'articolo 16, paragrafo 3, della direttiva (UE) 2016/1148. Se del caso, la Commissione può anche vagliare l'opportunità di rivedere le soglie attualmente stabilite nel presente regolamento.

(11) Al fine di consentire alle autorità competenti di essere informate circa eventuali nuovi rischi, i fornitori di servizi digitali dovrebbero essere incoraggiati a segnalare su base volontaria eventuali incidenti dalle caratteristiche precedentemente sconosciute, ad esempio nuovi exploit, vettori di attacco e autori di minacce, vulnerabilità e pericoli.

(12) Il presente regolamento dovrebbe applicarsi a partire dal giorno successivo alla scadenza del termine di recepimento della direttiva (UE) 2016/1148.

(13) Le disposizioni di cui al presente regolamento sono conformi al parere del comitato per la sicurezza delle reti e dei sistemi informativi, istituito dall'articolo 22 della direttiva (UE) 2016/1148,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Oggetto

Il presente regolamento specifica ulteriormente gli elementi che i fornitori di servizi digitali devono prendere in considerazione nell'identificazione e nell'adozione delle misure volte a garantire un livello di sicurezza delle reti e dei sistemi informativi che essi utilizzano nel contesto dell'offerta di servizi di cui all'allegato III della direttiva (UE) 2016/1148; esso precisa ulteriormente anche i parametri da prendere in considerazione al fine di determinare se un incidente ha un impatto rilevante sulla fornitura di tali servizi.

Articolo 2

Elementi di sicurezza

1. La sicurezza dei sistemi e degli impianti di cui all'articolo 16, paragrafo 1, lettera a), della direttiva (UE) 2016/1148 è riferita alla sicurezza delle reti e dei sistemi informativi e del loro ambiente fisico e comprende i seguenti elementi:

a) la gestione sistematica delle reti e dei sistemi informativi, ossia la mappatura dei sistemi informativi e la definizione di una serie di politiche adeguate in materia di gestione della sicurezza informatica, comprese l'analisi dei rischi, le risorse umane, la sicurezza delle operazioni, l'architettura di sicurezza, la gestione del ciclo di vita dei dati e dei sistemi protetti e, se del caso, la crittografia e la sua gestione;

(b) la sicurezza fisica e dell'ambiente, ossia la disponibilità di una serie di misure volte a proteggere le reti e i sistemi informativi dei fornitori di servizi digitali dai danni attraverso il ricorso a un approccio globale ai pericoli basato sui rischi, che affronti ad esempio gli errori di sistema, gli errori umani, gli atti dolosi o i fenomeni naturali;

c) la sicurezza delle forniture, ossia la definizione e il mantenimento di politiche adeguate al fine di assicurare l'accessibilità e, se del caso, la tracciabilità delle forniture critiche utilizzate nella prestazione dei servizi;

d) i controlli dell'accesso alle reti e ai sistemi informativi, ossia la disponibilità di una serie di misure volte ad assicurare che l'accesso fisico e logico alle reti e ai sistemi informativi, ivi inclusa la sicurezza amministrativa di tali reti e sistemi, sia autorizzato e limitato sulla base di esigenze aziendali e di sicurezza.

2. Per quanto riguarda il trattamento degli incidenti di cui all'articolo 16, paragrafo 1, lettera b), della direttiva (UE) 2016/1148, le misure adottate dal fornitore di servizi digitali comprendono:

a) il mantenimento e la prova di processi e procedure di individuazione per assicurare l'individuazione tempestiva e idonea degli eventi anomali;

b) i processi e le politiche per la segnalazione degli incidenti e l'individuazione delle debolezze e vulnerabilità nei propri sistemi informativi;

c) una risposta conforme alle procedure stabilite e la comunicazione dei risultati ottenuti con la misura adottata;

d) la valutazione della gravità dell'incidente, la documentazione delle conoscenze acquisite grazie all'analisi dell'incidente e la raccolta di informazioni pertinenti da utilizzare eventualmente come prova e per sostenere un processo di costante miglioramento.

3. La gestione della continuità operativa di cui all'articolo 16, paragrafo 1, lettera c), della direttiva (UE) 2016/1148 è la capacità di un'organizzazione di mantenere o, se del caso, ripristinare l'erogazione di servizi a livelli predefiniti accettabili in seguito a un incidente perturbatore e comprende:

a) la definizione e l'uso di piani di emergenza basati sull'analisi dell'impatto sulle attività aziendali volti a garantire la continuità dei servizi erogati dai fornitori di servizi digitali e valutati e testati regolarmente, ad esempio mediante esercitazioni;

b) la capacità di ripristino di emergenza, valutata e testata regolarmente, ad esempio mediante esercitazioni.

4. Il monitoraggio, l'audit e i test di cui all'articolo 16, paragrafo 1, lettera d), della direttiva (UE) 2016/1148 comprendono la definizione e il mantenimento di politiche relative:

a) alla conduzione di una sequenza pianificata di osservazioni o misurazioni per valutare se le reti e i sistemi informativi funzionano come previsto;

b) all'ispezione e alla verifica per controllare se una norma o una serie di orientamenti sono applicati, se le registrazioni sono accurate e se gli obiettivi di efficienza ed efficacia sono raggiunti;

c) a un processo finalizzato a rivelare i difetti dei meccanismi di sicurezza di una rete o di un sistema informativo che proteggono i dati e mantengono la funzionalità prevista. Tale processo comprende i processi tecnici e il personale coinvolto nel flusso di operazioni.

5. Le norme internazionali di cui all'articolo 16, paragrafo 1, lettera e), della direttiva (UE) 2016/1148 sono le norme adottate da un organismo di normazione internazionale di cui all'articolo 2, paragrafo 1, lettera a), del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio ([1]). Secondo l'articolo 19 della direttiva (UE) 2016/1148 possono essere utilizzate anche le norme e le specifiche europee o accettate a livello internazionale relative alla sicurezza delle reti e dei sistemi informativi, comprese le norme nazionali esistenti.

6. I fornitori di servizi digitali provvedono a rendere disponibile la documentazione adeguata per consentire all'autorità competente di verificare la conformità con gli elementi di sicurezza di cui ai paragrafi 1, 2, 3, 4 e 5.

Articolo 3

Parametri da prendere in considerazione al fine di determinare se l'impatto di un incidente è rilevante

1. Per quanto riguarda il numero di utenti interessati da un incidente, in particolare gli utenti che dipendono dal servizio per la fornitura dei propri servizi di cui all'articolo 16, paragrafo 4, lettera a), della direttiva (UE) 2016/1148, il fornitore di servizi digitali è in grado di stimare:

a) il numero di persone fisiche e giuridiche interessate con cui è stato concluso un contratto per la fornitura del servizio, o

b) il numero di utenti interessati che hanno utilizzato il servizio in particolare in base ai precedenti dati sul traffico.

2. La durata dell'incidente di cui all'articolo 16, paragrafo 4, lettera b), della direttiva (UE) 2016/1148 è il periodo tra la perturbazione della regolare prestazione del servizio in termini di disponibilità, autenticità, integrità o riservatezza e il momento del ripristino.

3. Per quanto riguarda la diffusione geografica relativamente all'area interessata dall'incidente di cui all'articolo 16, paragrafo 4, lettera c), della direttiva (UE) 2016/1148, il fornitore di servizi digitali è in grado di stabilire se l'incidente influisce sulla fornitura dei suoi servizi in determinati Stati membri.

4. La portata della perturbazione del funzionamento del servizio di cui all'articolo 16, paragrafo 4, lettera d), della direttiva (UE) 2016/1148 è misurata per una o più delle seguenti caratteristiche compromesse dall'incidente: disponibilità, autenticità, integrità o riservatezza dei dati o dei servizi correlati.

([1]) Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio (GU L 316 del 14.11.2012, pag. 12).

5. Per quanto riguarda la portata dell'impatto sulle attività economiche e sociali di cui all'articolo 16, paragrafo 4, lettera e), della direttiva (UE) 2016/1148, il fornitore di servizi digitali è in grado di dedurre, sulla base di indicazioni quali la natura delle sue relazioni contrattuali con il cliente o, se del caso, il numero potenziale di utenti interessati, se l'incidente ha causato importanti perdite materiali o immateriali per gli utenti, ad esempio in relazione alla salute e alla sicurezza o danni materiali.

6. Ai fini dei paragrafi 1, 2, 3, 4 e 5, i fornitori di servizi digitali non sono tenuti a raccogliere ulteriori informazioni alle quali non hanno accesso.

Articolo 4

Impatto rilevante di un incidente

1. Un incidente è considerato come avente un impatto rilevante se si verifica almeno una delle seguenti situazioni:

a) il servizio fornito da un fornitore di servizi digitali non è stato disponibile per oltre 5 000 000 di ore utente, dove per ore utente si intende il numero di utenti interessati nell'Unione per una durata di sessanta minuti;

b) l'incidente ha provocato una perdita di integrità, autenticità o riservatezza dei dati conservati, trasmessi o trattati o dei relativi servizi offerti o accessibili tramite una rete e un sistema informativo del fornitore di servizi digitali che ha interessato oltre 100 000 utenti nell'Unione;

c) l'incidente ha generato un rischio per la sicurezza pubblica, l'incolumità pubblica o in termini di perdite di vite umane;

d) l'incidente ha provocato danni materiali superiori a 1 000 000 di EUR per almeno un utente nell'Unione.

2. Sulla base delle buone pratiche raccolte dal gruppo di cooperazione nello svolgimento dei suoi compiti a norma dell'articolo 11, paragrafo 3, della direttiva (UE) 2016/1148 e delle discussioni di cui all'articolo 11, paragrafo 3, lettera m), della medesima direttiva, la Commissione può riesaminare le soglie di cui al paragrafo 1.

Articolo 5

Entrata in vigore

(1) Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

(2) Esso si applica a decorrere dal 10 maggio 2018.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 30 gennaio 2018

Per la Commissione

Il presidente

Jean-Claude JUNCKER