REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2018/151 AL COMISIEI

din 30 ianuarie 2018

de stabilire a normelor de aplicare a Directivei (UE) 2016/1148 a Parlamentului European și a Consiliului în ceea ce privește aducerea unor precizări suplimentare cu privire la elementele care trebuie să fie luate în considerare de către furnizorii de servicii digitale pentru gestionarea riscurilor la adresa securității rețelelor și a sistemelor informatice, precum și cu privire la parametrii necesari pentru a se determina dacă un incident are un impact substanțial

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune ([1]), în special articolul 16 alineatul (8),

întrucât:

(1) În conformitate cu Directiva (UE) 2016/1148, furnizorii de servicii digitale au libertatea de a lua măsurile tehnice și organizatorice pe care le consideră adecvate și proporționale pentru a gestiona riscurile la adresa securității rețelelor și a sistemelor lor informatice, atât timp cât aceste măsuri asigură un nivel adecvat de securitate și țin seama de elementele prevăzute în directiva respectivă.

(2) Atunci când identifică măsurile tehnice și organizatorice adecvate și proporționale, furnizorul de servicii digitale ar trebui să abordeze chestiunea securității informațiilor în mod sistematic, utilizând o abordare bazată pe riscuri.

(3) Pentru a garanta securitatea sistemelor și a instalațiilor, furnizorii de servicii digitale ar trebui să efectueze proceduri de evaluare și analiză. Aceste activități ar trebui să se refere la gestionarea sistematică a rețelelor și a sistemelor informatice, la securitatea fizică și a mediului, la securitatea aprovizionării și la controlul accesului.

(4) Atunci când efectuează o analiză de risc în cadrul gestionării sistematice a rețelelor și a sistemelor informatice, furnizorii de servicii digitale ar trebui să fie încurajați să identifice riscurile specifice și să cuantifice importanța acestora, de exemplu prin identificarea amenințărilor la adresa bunurilor critice și a modului în care acestea pot afecta operațiunile și prin definirea celor mai bune modalități de a atenua aceste riscuri pe baza capacităților existente și a resurselor necesare.

(5) Politicile privind resursele umane ar putea să se refere la gestionarea competențelor, inclusiv la aspectele legate de dezvoltarea competențelor în materie de securitate și de creșterea informării în acest domeniu. Atunci când decid cu privire la un set adecvat de politici privind securitatea operațiunilor, furnizorii de servicii digitale ar trebui să fie încurajați să aibă în vedere aspectele legate de gestionarea schimbărilor, gestionarea vulnerabilității, formalizarea practicilor operaționale și administrative, precum și cartografierea sistemului.

(6) Politicile privind arhitectura de securitate ar putea cuprinde separarea rețelelor și a sistemelor, precum și măsuri specifice de securitate pentru operațiunile critice, cum ar fi operațiunile de administrare. Separarea rețelelor și a sistemelor ar putea permite unui furnizor de servicii digitale să facă distincția între elemente precum fluxurile de date și resursele informatice care aparțin unui client, unui grup de clienți, furnizorului de servicii digitale propriu-zis sau părților terțe.

(7) Măsurile luate cu privire la securitatea fizică și a mediului ar trebui să asigure securitatea rețelelor și a sistemelor informatice ale unei organizații pentru a le proteja împotriva daunelor cauzate de incidente cum ar fi furturile, incendiile, inundațiile sau alte fenomene meteo și deficiențele din sectorul telecomunicațiilor sau al energiei electrice.

(8) Securitatea aprovizionării – de exemplu cu energie electrică, combustibil sau energie pentru răcire – ar putea include securitatea lanțului de aprovizionare, care include în special securitatea contractanților și subcontractanților terți, precum și securitatea de la nivelul conducerii acestora. Trasabilitatea bunurilor critice se referă la capacitatea furnizorului de servicii digitale de a identifica sursele bunurilor respective și de a ține evidența acestora.

(9) Categoria utilizatorilor de servicii digitale ar trebui să includă și persoanele fizice și juridice care sunt clienți sau abonați ai unei piețe online sau ai unui serviciu de cloud computing ori care vizitează un site web al unui motor de căutare online pentru a efectua căutări după cuvinte-cheie.

([1]) JO L 194, 19.7.2016, p. 1.

(10) Atunci când se determină în ce măsură impactul unui incident este substanțial, lista de incidente substanțiale prevăzută în prezentul regulament ar trebui să fie considerată drept neexhaustivă. Ar trebui să se tragă învățăminte din punerea în aplicare a prezentului regulament și din lucrările grupului de cooperare în ceea ce privește colectarea informațiilor referitoare la cele mai bune practici privind riscurile și incidentele și discuțiile privind modalitățile de raportare a notificărilor incidentelor menționate la articolul 11 alineatul (3) literele (i) și (m) din Directiva (UE) 2016/1148. Rezultatul ar putea fi formularea unor orientări cuprinzătoare cu privire la pragurile cantitative ale parametrilor de notificare care ar putea declanșa obligația de notificare pentru furnizorii de servicii digitale în temeiul articolului 16 alineatul (3) din Directiva (UE) 2016/1148. Dacă este cazul, Comisia ar putea, de asemenea, să aibă în vedere revizuirea pragurilor prevăzute actualmente de prezentul regulament.

(11) Pentru ca autoritățile competente să poată fi informate cu privire la noi riscuri potențiale, furnizorii de servicii digitale ar trebui să fie încurajați să semnaleze în mod voluntar orice incident ale cărui caracteristici le erau anterior necunoscute, cum ar fi noi exploit-uri, vectori de atac, entități răuvoitoare, vulnerabilități și pericole.

(12) Prezentul regulament ar trebui să se aplice în ziua următoare expirării termenului de transpunere a Directivei (UE) 2016/1148.

(13) Măsurile prevăzute de prezentul regulament sunt conforme cu avizul Comitetului pentru securitatea rețelelor și a sistemelor informatice instituit în temeiul articolului 22 din Directiva (UE) 2016/1148,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Obiect

Prezentul regulament precizează mai în detaliu elementele care trebuie luate în considerare de către furnizorii de servicii digitale atunci când identifică și iau măsuri pentru a asigura un anumit nivel de securitate a rețelelor și a sistemelor informatice pe care le utilizează în contextul furnizării serviciilor menționate în anexa III la Directiva (UE) 2016/1148 și descrie mai detaliat parametrii care trebuie luați în considerare pentru a stabili dacă un incident are un impact substanțial asupra furnizării serviciilor respective.

Articolul 2

Elemente de securitate

(1) Securitatea sistemelor și a instalațiilor menționată la articolul 16 alineatul (1) litera (a) din Directiva (UE) 2016/1148 înseamnă securitatea rețelelor și a sistemelor informatice și a mediului fizic al acestora și include următoarele elemente:

(a) gestionarea sistematică a rețelelor și a sistemelor informatice, care înseamnă cartografierea sistemelor informatice și stabilirea unui set de politici adecvate privind gestionarea securității informațiilor, incluzând analiza riscurilor, resursele umane, securitatea operațiunilor, arhitectura securității, securitatea datelor și gestionarea ciclului de viață al sistemului, precum și, dacă este cazul, criptarea și gestionarea acesteia;

(b) securitatea fizică și a mediului, care înseamnă existența unui set de măsuri menite să protejeze securitatea rețelelor și a sistemelor informatice ale furnizorilor de servicii digitale împotriva daunelor, cu ajutorul unei abordări bazate pe riscuri care să țină seama de toate tipurile de pericole, printre care deficiențele sistemului, erorile umane, acțiunile răuvoitoare și fenomenele naturale;

(c) securitatea aprovizionării, care înseamnă instituirea și menținerea unor politici adecvate pentru a asigura accesibilitatea și, după caz, trasabilitatea bunurilor critice utilizate în furnizarea serviciilor;

(d) controlul accesului la rețele și la sistemele informatice, care înseamnă existența unui set de măsuri prin care să se asigure că accesul fizic și logic la rețele și la sistemele informatice, incluzând securitatea administrativă a rețelelor și a sistemelor informatice, este autorizat și restricționat pe baza unor cerințe operaționale și de securitate.

(2) În ceea ce privește gestionarea incidentelor menționată la articolul 16 alineatul (1) litera (b) din Directiva (UE) 2016/1148, printre măsurile luate de furnizorul de servicii digitale se numără:

(a) procesele și procedurile de detectare menținute și testate pentru a asigura identificarea adecvată și în timp util a evenimentelor anormale;

(b) procesele și politicile referitoare la raportarea incidentelor și identificarea punctelor slabe și a vulnerabilităților în propriile sisteme informatice;

(c) un răspuns conform cu procedurile instituite și raportarea rezultatelor măsurilor luate;

(d) o evaluare a gravității incidentului, cu documentarea concluziilor trase din analiza incidentului și colectarea informațiilor relevante care ar putea servi drept mijloace de probă și ar putea sprijini procesul de îmbunătățire continuă.

(3) Gestionarea continuității activității menționată la articolul 16 alineatul (1) litera (c) din Directiva (UE) 2016/1148 înseamnă capacitatea unei organizații de a menține sau, dacă este cazul, de a restabili furnizarea de servicii la nivelurile acceptabile predefinite, în urma unui incident perturbator. Aceasta cuprinde:

(a) crearea și utilizarea de planuri de urgență pe baza unei analize a impactului asupra activității, pentru asigurarea continuității serviciilor oferite de furnizorii de servicii digitale; acestea trebuie evaluate și testate periodic, de exemplu prin exerciții;

(b) capacități de redresare în caz de dezastru, care trebuie evaluate și testate periodic, de exemplu prin exerciții.

(4) Monitorizarea, auditarea și testarea menționate la articolul 16 alineatul (1) litera (d) din Directiva (UE) 2016/1148 includ stabilirea și menținerea unor politici privind:

(a) efectuarea unei serii planificate de observații sau măsurători pentru a evalua dacă rețelele și sistemele informatice funcționează în mod corespunzător;

(b) inspecții și verificări pentru a determina dacă un anumit standard sau set de orientări este respectat, dacă evidențele sunt exacte și dacă obiectivele în materie de eficiență și eficacitate sunt atinse;

(c) o procedură menită să scoată la iveală deficiențele din mecanismele de securitate ale unei rețele sau ale unui sistem informatic destinate să protejeze datele și să mențină funcționalitatea preconizată. O astfel de procedură include procesele tehnice și personalul implicat în fluxul operațional.

(5) Standardele internaționale menționate la articolul 16 alineatul (1) litera (e) din Directiva (UE) 2016/1148 înseamnă standardele care sunt adoptate de către un organism de standardizare internațional, astfel cum sunt menționate la articolul 2 alineatul (1) litera (a) din Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului ([1]). În temeiul articolului 19 din Directiva (UE) 2016/1148, pot fi, de asemenea, utilizate standardele și specificațiile europene sau cele acceptate la nivel internațional relevante pentru securitatea rețelelor și a sistemelor informatice, inclusiv standardele naționale existente.

(6) Furnizorii de servicii digitale se asigură că dispun de documentația adecvată care să îi permită autorității competente să verifice conformitatea cu elementele de securitate stabilite la alineatele (1), (2), (3), (4) și (5).

Articolul 3

Parametrii care trebuie luați în considerare pentru a determina dacă impactul unui incident este substanțial

(1) În ceea ce privește numărul de utilizatori afectați de un incident, în special utilizatori care se bazează pe serviciul în cauză pentru furnizarea propriilor servicii, menționat la articolul 16 alineatul (4) litera (a) din Directiva (UE) 2016/1148, furnizorul de servicii digitale trebuie să fie în măsură să estimeze unul dintre următoarele elemente:

(a) numărul de persoane fizice și juridice afectate cu care s-a încheiat un contract pentru furnizarea serviciului respectiv sau

(b) numărul de utilizatori afectați care au utilizat serviciul respectiv, pe baza datelor de transfer anterioare.

(2) Durata unui incident menționată la articolul 16 alineatul (4) litera (b) din Directiva (UE) 2016/1148 înseamnă perioada cuprinsă între momentul perturbării furnizării adecvate a serviciului în ceea ce privește disponibilitatea, autenticitatea, integritatea sau confidențialitatea și momentul reluării activității.

(3) Distribuția geografică în ceea ce privește zona afectată de incident menționată la articolul 16 alineatul (4) litera (c) din Directiva (UE) 2016/1148 se referă la faptul că furnizorul de servicii digitale trebuie să fie în măsură să determine dacă incidentul afectează furnizarea serviciilor sale în anumite state membre.

(4) Amploarea perturbării funcționării serviciului menționată la articolul 16 alineatul (4) litera (d) din Directiva (UE) 2016/1148 se măsoară în ceea ce privește una sau mai multe dintre următoarele caracteristici afectate de un incident: disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor sau a serviciilor conexe.

([1]) Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului (JO L 316, 14.11.2012, p. 12).

(5) În ceea ce privește amploarea impactului asupra activităților economice și societale menționată la articolul 16 alineatul (4) litera (e) din Directiva (UE) 2016/1148, furnizorul de servicii digitale trebuie să fie în măsură să concluzioneze, pe baza unor factori cum ar fi natura relațiilor sale contractuale cu clientul sau, dacă este cazul, numărul potențial al utilizatorilor afectați, dacă incidentul a provocat daune materiale sau morale semnificative pentru utilizatori, de pildă în ceea ce privește sănătatea și siguranța ori deteriorarea proprietății.

(6) În sensul alineatelor (1), (2), (3), (4) și (5), furnizorii de servicii digitale nu au obligația de a colecta informații suplimentare la care nu au acces.

Articolul 4

Impactul substanțial al unui incident

(1) Se consideră că un incident are un impact substanțial în cazul în care a survenit cel puțin una dintre următoarele situații:

(a) serviciul oferit de un furnizor de servicii digitale a fost indisponibil timp de mai bine de 5 000 000 de ore-utilizator; termenul „oră-utilizator” se referă la un utilizator afectat în Uniune pe o durată de șaizeci de minute;

(b) incidentul a avut ca rezultat o pierdere a integrității, autenticității sau confidențialității datelor stocate, transmise ori prelucrate sau a serviciilor conexe oferite de rețeaua sau sistemul de informații al furnizorului de servicii digitale sau accesibile prin intermediul rețelei sau al sistemului respectiv care afectează mai mult de 100 000 de utilizatori din Uniune;

(c) incidentul a creat un risc la adresa ordinii sau a siguranței publice ori în ceea ce privește pierderea de vieți omenești;

(d) incidentul i-a provocat daune materiale cel puțin unui utilizator din Uniune, dacă dauna cauzată acestuia depășește 1 000 000 EUR.

(2) Bazându-se pe cele mai bune practici colectate de grupul de cooperare în exercitarea sarcinilor sale conferite în temeiul articolului 11 alineatul (3) din Directiva (UE) 2016/1148 și pe discuțiile purtate în temeiul articolului 11 alineatul (3) litera (m), Comisia poate revizui plafoanele prevăzute la alineatul (1).

Articolul 5

Intrarea în vigoare

(1) Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

(2) Se aplică de la 10 mai 2018.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 30 ianuarie 2018.

Pentru Comisie

Președintele

Jean-Claude JUNCKER