PROVEDBENA UREDBA KOMISIJE (EU) 2018/151

od 30. siječnja 2018.

o utvrđivanju pravila za primjenu Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća u odnosu na dodatne specifikacije elemenata koje pružatelji digitalnih usluga moraju uzeti u obzir u upravljanju rizicima kojima je izložena sigurnost njihovih mrežnih i informacijskih sustava i parametara za utvrđivanje ima li incident znatan učinak

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Direktivu (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije ([1]), a osobito njezin članak 16. stavak 8.

budući da:

(1) U skladu s Direktivom (EU) 2016/1148 pružatelji digitalnih usluga i dalje mogu slobodno poduzimati tehničke i organizacijske mjere koje smatraju prikladnima i uravnoteženima za upravljanje rizicima kojima su izloženi njihovi mrežni i informacijski sustavi, pod uvjetom da se tim mjerama osigura odgovarajuća razina sigurnosti i uzmu u obzir elementi predviđeni u toj Direktivi.

(2) Pri utvrđivanju odgovarajućih i uravnoteženih tehničkih i organizacijskih mjera pružatelj digitalnih usluga trebao bi sustavno pristupati sigurnosti informacija služeći se pristupom koji se temelji na riziku.

(3) Kako bi se osigurala sigurnost sustava i objekata, pružatelji digitalnih usluga trebali bi provesti ocjenjivanje i analizu. Te aktivnosti trebale bi se odnositi na sustavno upravljanje mrežnim i informacijskim sustavima, fizičku sigurnost i sigurnost okoliša, sigurnost opskrbe i kontrolu pristupa.

(4) Pri provođenju analize rizika u okviru sustavnog upravljanja mrežnim i informacijskim sustavima pružatelje digitalnih usluga trebalo bi poticati da utvrđuju posebne rizike i kvantificiraju njihovu težinu, na primjer, utvrđivanjem prijetnji ključnoj imovini i njihova mogućeg utjecaja na poslovanje i utvrđivanjem najboljih načina za ublažavanje tih prijetnji na temelju trenutačnih sposobnosti i zahtjeva u pogledu resursa.

(5) Politike u području ljudskih resursa mogle bi se odnositi na upravljanje vještinama, uključujući aspekte koji se odnose na razvoj vještina povezanih sa sigurnošću i osvješćivanjem potrebe za sigurnošću. Pri odlučivanju o odgovarajućem skupu politika o sigurnosti operacija, pružatelje digitalnih usluga trebalo bi poticati da uzmu u obzir aspekte upravljanja promjenama, upravljanja osjetljivošću, formalizacije operativnih i administrativnih postupaka te sistemskog planiranja.

(6) Politike o arhitekturi sigurnosti mogle bi obuhvaćati razdvajanje mreža i sustava, kao i posebne sigurnosne mjere za ključne djelatnosti kao što su aktivnosti upravljanja. Razdvajanjem mreža i sustava omogućilo bi se pružateljima digitalnih usluga razlikovanje elemenata kao što su prijenos podataka i računalni resursi koji pripadaju jednom korisniku, skupini korisnika, pružatelju digitalnih usluga ili trećim stranama.

(7) Mjerama poduzetima u odnosu na fizičku sigurnost i sigurnost okoliša trebalo bi zajamčiti sigurnost mrežnih i informacijskih sustava organizacije od štete izazvane incidentima kao što su krađa, požar, poplava ili druge vremenske nepogode, telekomunikacijski problemi ili prekidi opskrbe električnom energijom.

(8) Sigurnost opskrbe, npr. električnom energijom, gorivom ili sredstvima za hlađenje, mogla bi obuhvatiti sigurnost opskrbnog lanca koja posebno uključuje sigurnost nepovezanih izvođača i podizvođača te njihova rukovodstva. Sljedivost ključnih materijala odnosi se na sposobnost pružatelja digitalnih usluga da utvrdi i zabilježi izvore tih materijala.

(9) Korisnici digitalnih usluga trebali bi obuhvaćati fizičke i pravne osobe koje su korisnici internetskog tržišta ili su pretplatnici na internetsko tržište ili usluge računalstva u oblaku, ili koji su posjetitelji internetske tražilice radi pretraživanja s pomoću ključnih riječi.

([1]) SL L 194, 19.7.2016., str. 1.

(10) Pri utvrđivanju težine učinka incidenta slučajeve navedene u ovoj Uredbi ne bi trebalo smatrati konačnim popisom znatnih incidenata. Trebalo bi izvući pouke iz provedbe ove Uredbe i iz rada skupine za suradnju u vezi s prikupljanjem informacija o najboljoj praksi u pogledu rizika i incidenata, te iz rasprava o modalitetima za slanje obavijesti o incidentima iz članka 11. stavka 3. točaka (i) i (m) Direktive (EU) 2016/1148. Tako bi mogle nastati sveobuhvatne smjernice o kvantitativnim pragovima parametara za obavještavanje koji kod pružatelja digitalnih usluga mogu aktivirati obvezu obavještavanja u skladu s člankom 16. stavkom 3. Direktive (EU) 2016/1148. Kada je to prikladno, Komisija bi mogla preispitati pragove utvrđene ovom Uredbom.

(11) Kako bi se nadležnim tijelima omogućilo da budu informirana o mogućim novim rizicima, pružatelje digitalnih usluga trebalo bi poticati da dragovoljno izvještavaju o svakom incidentu čije im značajke prethodno nisu bile poznate, kao što su novi načini iskorištavanja, vektori napada ili akteri prijetnje, ranjivosti i opasnosti.

(12) Ova Uredba trebala bi se primjenjivati sljedećeg dana nakon isteka roka za prijenos Direktive (EU) 2016/1148.

(13) Mjere predviđene u ovoj Uredbi u skladu su s mišljenjem Odbora za sigurnost mrežnih i informacijskih sustava iz članka 22. Direktive (EU) 2016/1148,

DONIJELA JE OVU UREDBU:

Članak 1.

Predmet

Ovom se Uredbom dodatno utvrđuju elementi koje pružatelji digitalnih usluga moraju uzeti u obzir pri utvrđivanju i poduzimanju mjera kako bi se osigurala određena razina sigurnosti mrežnih i informacijskih sustava kojima se služe u okviru pružanja usluga iz Priloga III. Direktivi (EU) 2016/1148, a nadalje se određuju i parametri koje treba uzeti u obzir za određivanje ima li incident znatan učinak na pružanje tih usluga.

Članak 2.

Sigurnosni elementi

1. Sigurnost sustava i objekata iz članka 16. stavka 1. točke (a) Direktive (EU) 2016/1148 znači sigurnost mrežnih i informacijskih sustava i njihova fizičkog okruženja i uključuju sljedeće elemente:

(a) sustavno upravljanje mrežnim i informacijskim sustavima, što znači pregled informacijskih sustava i utvrđivanje odgovarajućih politika za upravljanje sigurnošću informacija, uključujući analizu rizika, ljudske potencijale, sigurnost poslovanja, sigurnosnu arhitekturu, upravljanje životnim ciklusom zaštićenih podataka i sustava i, prema potrebi, šifriranje i upravljanje šifriranjem;

(b) fizička sigurnost i sigurnost okoliša, što znači dostupnost skupa mjera za zaštitu mrežnih i informacijskih sustava pružatelja digitalnih usluga od štete primjenom globalnog pristupa koji se temelji na riziku radi rješavanja primjerice kvara sustava, ljudskih pogrešaka, zlonamjernog djelovanja ili djelovanja prirodnih fenomena;

(c) sigurnost opskrbe, što znači uspostava i održavanje odgovarajućih politika za osiguravanje dostupnosti i, prema potrebi, sljedivosti ključnih materijala koji se upotrebljavaju u pružanju usluga;

(d) kontrola pristupa mrežnim i informacijskim sustavima, što znači dostupnost niza mjera kojima se osigurava ovlašten i ograničen fizički i logički pristup mrežnim i informacijskim sustavima, uključujući administrativnu sigurnost mrežnog i informacijskog sustava, na temelju poslovnih i sigurnosnih zahtjeva.

2. U pogledu rješavanja incidenata iz članka 16. stavka 1. točke (b) Direktive (EU) 2016/1148, mjere koje poduzima pružatelj digitalnih usluga uključuju:

(a) održavanje i testiranje procesa i postupaka detekcije radi pravovremene i odgovarajuće informiranosti o neuobičajenim događajima;

(b) postupke i politike za prijavljivanje incidenata i otkrivanje nedostataka i slabosti u njihovim informacijskim sustavima;

(c) odgovor u skladu s utvrđenim postupcima i obavještavanje o rezultatima poduzetih mjera;

(d) procjenu ozbiljnosti incidenta, dokumentiranje spoznaja iz analize incidenta i prikupljanje relevantnih podataka koji mogu poslužiti kao dokaz i pridonijeti kontinuiranom procesu poboljšanja.

3. Upravljanje kontinuitetom poslovanja iz članka 16. stavka 1. točke (c) Direktive (EU) 2016/1148 znači sposobnost organizacije da pruža ili po potrebi ponovno uspostavi pružanje usluga na unaprijed utvrđenoj prihvatljivoj razini nakon incidenta koji je izazvao prekid u radu, što uključuje:

(a) uspostavu i uporabu kriznih planova na temelju analize učinka na poslovanje radi osiguranja kontinuiteta pružanja usluga pružatelja digitalnih usluga; te planove treba redovito procjenjivati i testirati, primjerice kroz vježbe;

(b) sposobnost za oporavak od katastrofa; koju treba redovito procjenjivati i testirati, primjerice kroz vježbe.

4. Praćenje, revizija i testiranje iz članka 16. stavka 1. točke (d) Direktive (EU) 2016/1148 uključuje uspostavljanje i održavanje politike o:

(a) provođenju planiranog niza promatranja ili mjerenja kako bi se procijenilo funkcioniraju li mrežni i informacijski sustavi na predviđeni način;

(b) inspekcijama i provjerama kako bi ocijenilo slijedi li se određeni standard ili skup smjernica, je li evidencija točna, a ciljevi učinkovitosti i djelotvornosti ostvareni;

(c) postupku kojemu je svrha otkriti nedostatke u sigurnosnim mehanizmima mrežnog i informacijskog sustava, čime se štite podaci i održava njihova pravilna funkcija. Taj postupak uključuje tehničke postupke i osoblje uključeno u rad.

5. Međunarodne norme iz članka 16. stavka 1. točke (e) Direktive (EU) 2016/1148 znače norme koje je donijelo međunarodno normizacijsko tijelo kao što je navedeno u članku 2. stavku 1. točki (a) Uredbe (EU) br. 1025/2012 Europskog parlamenta i Vijeća ([1]). U skladu s člankom 19. Direktive (EU) 2016/1148 dopuštena je i primjena europskih ili međunarodno priznatih normi i specifikacija relevantnih za sigurnost mrežnih i informacijskih sustava, uključujući postojeće nacionalne standarde.

6. Pružatelji digitalnih usluga dužni su nadležnom tijelu osigurati dostup do odgovarajuće dokumentacije na temelju koje će ono provjeriti usklađenost sa sigurnosnim elementima iz stavaka 1., 2., 3., 4. i 5.

Članak 3.

Parametri na temelju kojih se utvrđuje je li učinak incidenta znatan

1. S obzirom na broj korisnika na koje incident utječe, osobito korisnika koji se oslanjaju na tu uslugu za pružanje vlastitih usluga iz članka 16. stavka 4. točke (a) Direktive (EU) 2016/1148, pružatelj digitalnih usluga mora biti u mogućnosti procijeniti jedno od sljedećeg:

(a) broj pogođenih fizičkih i pravnih osoba s kojima je sklopljen ugovor o pružanju usluga; ili

(b) broj pogođenih korisnika koji su se koristili tom uslugom, osobito na temelju podataka o prethodnom prometu.

2. Trajanje incidenta iz članka 16. stavka 4. točke (b) znači razdoblje od trenutka kad je normalno pružanje usluge poremećeno, u pogledu dostupnosti, autentičnosti, cjelovitosti ili povjerljivosti, do trenutka nastavka pružanja usluge.

3. Što se tiče veličine zemljopisnog područja na koje utječe incident iz članka 16. stavka 4. točke (c) Direktive (EU) 2016/1148, pružatelj digitalnih usluga mora biti u mogućnosti utvrditi utječe li taj incident na pružanje usluga u određenim državama članicama.

4. Opseg poremećaja u funkcioniranju usluge iz članka 16. stavka 4. točke (d) Direktive (EU) 2016/1148 mjeri se u odnosu na jednu ili više sljedećih značajki kojima je vrijednost umanjena zbog incidenta: dostupnost, autentičnost, cjelovitost ili povjerljivost podataka ili srodnih usluga.

([1]) Uredba (EU) br. 1025/2012 Europskog parlamenta i Vijeća od 25. listopada 2012. o europskoj normizaciji, o izmjeni direktiva Vijeća 89/686/EEZ i 93/15/EEZ i direktiva 94/9/EZ, 94/25/EZ, 95/16/EZ, 97/23/EZ, 98/34/EZ, 2004/22/EZ, 2007/23/EZ, 2009/23/EZ i 2009/105/EZ Europskog parlamenta i Vijeća te o stavljanju izvan snage Odluke Vijeća 87/95/EEZ i Odluke br. 1673/2006/EZ Europskog parlamenta i Vijeća (SL L 316, 14.11.2012., str. 12.).

5. S obzirom na opseg učinka na gospodarske i društvene aktivnosti iz članka 16. stavka 4. točke (e) Direktive (EU) 2016/1148, pružatelj digitalnih usluga, na temelju pokazatelja kao što su priroda njegovih ugovornih odnosa s klijentom ili, eventualno, potencijalni broj pogođenih korisnika, mora moći zaključiti je li incident uzrokovao znatne materijalne ili nematerijalne gubitke za korisnike, npr. u odnosu na zdravlje, javnu sigurnost ili oštećenje imovine.

6. Za potrebe stavaka 1., 2., 3., 4. i 5. pružatelji digitalnih usluga nemaju obvezu prikupljanja dodatnih informacija kojima nemaju pristup.

Članak 4.

Znatan učinak incidenta

1. Smatra se da incident ima znatan učinak ako je nastala najmanje jedna od sljedećih situacija:

(a) usluga koju pruža pružatelj digitalnih usluga nije bila dostupna više od 5 000 000 korisničkih sati, pri čemu se izraz korisnički sat odnosi na broj pogođenih korisnika u Uniji u trajanju od šezdeset minuta;

(b) incident koji je doveo do gubitka integriteta, autentičnosti ili povjerljivosti pohranjenih ili prenesenih ili obrađenih podataka ili srodnih usluga koje nudi pružatelj digitalnih usluga ili su dostupne putem njegovih mrežnih i informacijskih sustava utjecao je na više od 100 000 korisnika u Uniji;

(c) incident je stvorio opasnost za javnu sigurnost, javnu zaštitu ili gubitak ljudskih života;

(d) incident je uzrokovao materijalnu štetu za barem jednog korisnika u Uniji, pri čemu šteta za tog korisnika prelazi 1 000 000 EUR.

2. Oslanjajući se na najbolje prakse koje je prikupila skupina za suradnju u izvršavanju svojih zadaća u skladu s člankom 11. stavkom 3. Direktive (EU) 2016/1148 i na rasprave u skladu s njezinim člankom 11. stavkom 3. točkom (m), Komisija može preispitati pragove utvrđene u stavku 1.

Članak 5.

Stupanje na snagu

1. Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

2. Primjenjuje se od 10. svibnja 2018.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 30. siječnja 2018.

Za Komisiju

Predsjednik

Jean-Claude JUNCKER