IZVEDBENA UREDBA KOMISIJE (EU) 2018/151

z dne 30. januarja 2018

o določitvi pravil za uporabo Direktive (EU) 2016/1148 Evropskega parlamenta in Sveta v zvezi z dodatno specifikacijo elementov, ki jih morajo upoštevati ponudniki digitalnih storitev pri obvladovanju tveganj za varnost omrežij in informacijskih sistemov, in parametrov za določanje, ali ima incident pomemben vpliv

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Direktive (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji ([1]) ter zlasti člena 16(8) Direktive,

ob upoštevanju naslednjega:

(1) V skladu z Direktivo (EU) 2016/1148 bi morali ponudnikom digitalnih storitev omogočiti, da se sami odločijo za sprejetje tehničnih in organizacijskih ukrepov, ki so po njihovem mnenju ustrezni in sorazmerni za obvladovanje tveganj za varnost njihovih omrežij in informacijskih sistemov, če navedeni ukrepi zagotavljajo ustrezno raven varnosti in upoštevajo elemente iz navedene direktive.

(2) Pri določanju ustreznih in sorazmernih tehničnih in organizacijskih ukrepov bi moral ponudnik digitalnih storitev obravnavati informacijsko varnost na sistematičen način in pri tem uporabiti pristop, ki temelji na tveganju.

(3) Za zagotovitev varnosti sistemov in zmogljivosti bi morali ponudniki digitalnih storitev izvajati ocenjevalne in analitske postopke. Te dejavnosti bi morale zadevati sistematsko upravljanje omrežij in informacijskih sistemov, fizično in okoljsko varnost, zanesljivost oskrbe in nadzor dostopa.

(4) Pri izvajanju analize tveganj znotraj sistematskega upravljanja omrežij in informacijskih sistemov bi bilo treba ponudnike digitalnih storitev spodbujati, da določijo specifična tveganja in količinsko opredelijo njihov pomen, na primer z opredelitvijo tveganj za kritična sredstva in načinov, kako lahko ta vplivajo na dejavnosti, in določijo najboljši način za zmanjšanje navedenih tveganj na podlagi trenutnih sposobnosti in zahtev glede virov.

(5) Kadrovske politike bi se lahko nanašale na upravljanje veščin, vključno z vidiki, povezanimi z razvojem veščin glede varnosti in ozaveščanjem. Pri odločanju o ustreznem sklopu politik v zvezi z varnostjo izvajanja dejavnosti bi bilo treba ponudnike digitalnih storitev spodbujati, da upoštevajo vidike upravljanja sprememb, upravljanja ranljivosti, formalizacije postopkov izvajanja dejavnosti in upravnih postopkov ter organizacije sistema.

(6) Politike na področju varnosti bi lahko obsegale zlasti ločevanje med omrežji in sistemi ter posebne varnostne ukrepe za ključne dejavnosti, kot so upravne dejavnosti. Z ločevanjem med omrežji in sistemi bi se lahko ponudnikom digitalnih storitev omogočilo razlikovanje med elementi, kot so podatkovni tokovi in računalniški viri, ki pripadajo stranki, skupini strank, ponudniku digitalnih storitev ali tretjim stranem.

(7) Ukrepi, sprejeti v zvezi s fizično in okoljsko varnostjo, bi morali zagotoviti varovanje omrežij in informacijskih sistemov organizacije pred škodo, ki jo povzročijo incidenti, kot so kraja, požar, poplava ali druge vremenske razmere ter telekomunikacijske napake ali izpadi oskrbe z električno energijo.

(8) Zanesljivost oskrbe npr. z električno energijo, gorivom ali hlajenjem bi lahko vključevala varnost oskrbovalne verige, ki vključuje zlasti varnost tretjih izvajalcev in podizvajalcev ter njihovega vodstva. Sledljivost kritične oskrbe pomeni sposobnost ponudnika digitalnih storitev, da določi in evidentira vire navedene oskrbe.

(9) Uporabniki digitalnih storitev bi morali zajemati fizične in pravne osebe, ki so stranke ali naročniki spletnega trga ali storitve računalništva v oblaku ali ki so obiskovalci spletne strani preko spletnega iskalnika z namenom iskanja po ključnih besedah.

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

(10) Pri določanju pomembnosti vpliva incidenta bi morali primeri, določeni v tej uredbi, veljati za neizčrpen seznam pomembnih incidentov. Pridobiti bi bilo treba izkušnje pri izvajanju te uredbe in delu skupine za sodelovanje, kar zadeva zbiranje informacij o najboljših praksah v zvezi s tveganji in incidenti ter obravnavo načinov poročanja o priglasitvah incidentov iz člena 11(3)(i) in (m) Direktive (EU) 2016/1148. Tako bi lahko nastale celovite smernice o količinskih pragih parametrov za priglasitev, ki bi lahko sprožili obveznost priglasitve za ponudnike digitalnih storitev v skladu s členom 16(3) Direktive (EU) 2016/1148. Kadar je to primerno, lahko Komisija prav tako razmisli o pregledu pragov, določenih v tej uredbi.

(11) Da bi bili pristojni organi obveščeni o možnih novih tveganjih, bi bilo treba ponudnike digitalnih storitev spodbujati, da prostovoljno poročajo o vseh incidentih, katerih značilnosti so jim bile prej neznane, npr. novi načini izkoriščanja, vektorji napada ali akterji, ki predstavljajo nevarnost, ranljivosti in tveganja.

(12) Ta uredba bi se morala uporabljati od dneva po poteku roka za prenos Direktive (EU) 2016/1148.

(13) Ukrepi, predvideni s to uredbo, so v skladu z mnenjem Odbora za varnost omrežij in informacijskih sistemov iz člena 22 Direktive (EU) 2016/1148 –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Predmet urejanja

Ta uredba dodatno opredeljuje elemente, ki jih morajo ponudniki digitalnih storitev upoštevati pri določanju in sprejemanju ukrepov za zagotovitev določene ravni varnosti omrežij in informacijskih sistemov, ki jih uporabljajo pri zagotavljanju storitev iz Priloge III k Direktivi (EU) 2016/1148 in dodatno opredeljuje parametre, ki jih je treba upoštevati pri določanju, ali ima incident pomemben vpliv na zagotavljanje navedenih storitev.

Člen 2

Varnostni elementi

1. Varnost sistemov in zmogljivosti iz člena 16(1)(a) Direktive (EU) 2016/1148 pomeni varnost omrežij in informacijskih sistemov ter njihovega fizičnega okolja in vsebuje naslednje elemente:

(a) sistematično upravljanje omrežij in informacijskih sistemov, kar pomeni razporejanje informacijskih sistemov in določitev niza ustreznih politik glede upravljanja informacijske varnosti, vključno z analizo tveganja, človeškimi viri, varnostjo izvajanja dejavnosti, varnostno arhitekturo, varovanjem podatkov in upravljanjem življenjskega cikla sistema ter, kjer je to primerno, šifriranjem in njegovim upravljanjem;

(b) fizično in okoljsko varnost, kar pomeni razpoložljivost niza ukrepov za zaščito varnosti omrežij in informacijskih sistemov ponudnikov digitalnih storitev pred škodo z uporabo pristopa upoštevanja vseh nevarnosti, ki temelji na tveganju, s katerim se obravnavajo na primer sistemske napake, človeške napake, zlonamerna dejanja ali naravni pojavi;

(c) zanesljivost oskrbe, kar pomeni vzpostavitev in ohranjanje ustreznih politik za zagotovitev dostopnosti do kritične oskrbe, ki se uporablja pri zagotavljanju storitev, in po potrebi njene sledljivosti;

(d) nadzor dostopa do omrežij in informacijskih sistemov, kar pomeni razpoložljivost niza ukrepov za zagotovitev, da je fizični in logični dostop do omrežij in informacijskih sistemov, vključno z upravno varnostjo omrežij in informacijskih sistemov, dovoljen in omejen na podlagi poslovnih in varnostnih zahtev.

2. Kar zadeva obvladovanje incidentov iz člena 16(1)(b) Direktive (EU) 2016/1148, ukrepi, ki jih je sprejel ponudnik digitalnih storitev, vključujejo:

(a) procese in postopke odkrivanja, ki se ohranjajo in preskušajo, da bi se zagotovilo pravočasno in ustrezno odkrivanje neobičajnih dogodkov;

(b) procese in politike v zvezi s poročanjem o incidentih ter ugotovljenih šibkih točkah in ranljivostih v njihovih informacijskih sistemih;

(c) odziv v skladu z vzpostavljenimi postopki in poročanje o rezultatih sprejetih ukrepov;

(d) oceno pomembnosti incidenta z dokumentacijo izsledkov analize incidenta in zbiranje ustreznih informacij, ki lahko služijo kot dokaz in podpirajo proces stalnega izboljševanja.

3. Upravljanje neprekinjenega poslovanja iz člena 16(1)(c) Direktive (EU) 2016/1148 pomeni sposobnost organizacije, da po incidentu z negativnim vplivom ohrani ali po potrebi ponovno vzpostavi zagotavljanje storitev na sprejemljivih vnaprej določenih ravneh in vključuje:

(a) pripravo in uporabo načrtov izrednih ukrepov, ki temeljijo na analizi poslovnega učinka za zagotovitev stalnosti storitev, ki jih zagotavljajo ponudniki digitalnih storitev ter se redno ocenjujejo in preskušajo, na primer z vajami;

(b) sanacijske zmogljivosti po incidentih, ki se redno ocenjujejo in preskušajo, na primer z vajami.

4. Spremljanje, revidiranje in preskušanje iz člena 16(1)(d) Direktive (EU) 2016/1148 vključuje oblikovanje in ohranjanje politik o:

(a) izvajanju načrtovanega zaporedja opazovanj ali meritev za oceno, ali omrežja in informacijski sistemi delujejo, kot je bilo predvideno;

(b) inšpekcijskih pregledih in preverjanjih z namenom, da se preveri, ali se standard ali niz smernic upošteva, ali so evidence točne ter ali so cilji učinkovitosti in uspešnosti izpolnjeni;

(c) postopku za odkrivanje pomanjkljivosti v varnostnih mehanizmih omrežij in informacijskih sistemov, ki varujejo podatke in ohranjajo funkcije, kot je bilo predvideno. Tak proces vključuje tehnične postopke in osebje, vključeno v tok upravljanja.

5. Mednarodni standardi iz člena 16(1)(e) Direktive (EU) 2016/1148 pomenijo standarde, ki jih sprejme mednarodni organ za standardizacijo iz člena 2(1)(a) Uredbe (EU) št. 1025/2012 Evropskega parlamenta in Sveta ([1]). V skladu s členom 19 Direktive (EU) 2016/1148 se lahko uporabijo tudi evropski ali mednarodno sprejeti standardi in specifikacije, pomembni za varnost omrežij in informacijskih sistemov, vključno z obstoječimi nacionalnimi standardi.

6. Ponudniki digitalnih storitev zagotovijo, da imajo na voljo ustrezno dokumentacijo, ki pristojnemu organu omogoči preverjanje skladnosti z varnostnimi elementi iz odstavkov 1, 2, 3, 4 in 5.

Člen 3

Parametri, ki jih je treba upoštevati pri določanju, ali ima incident pomemben vpliv

1. Glede na število prizadetih uporabnikov, zlasti uporabnikov, ki so od storitve odvisni pri zagotavljanju lastnih storitev iz člena 16(4)(a) Direktive (EU) 2016/1148, je ponudnik digitalnih storitev sposoben, da oceni eno od naslednjih:

(a) število prizadetih fizičnih in pravnih oseb, s katerimi je bila sklenjena pogodba za zagotavljanje storitve ali

(b) število preteklih prizadetih uporabnikov storitve, ki temelji zlasti na podatkih o preteklem prometu.

2. Trajanje incidenta iz člena 16(4)(b) pomeni časovno obdobje od prekinitve ustreznega zagotavljanja storitve v smislu razpoložljivosti, avtentičnosti, celovitosti ali zaupnosti do trenutka njene ponovne vzpostavitve.

3. Kar zadeva geografsko razširjenost območja, na katerega vpliva incident iz člena 16(4)(c) Direktive (EU) 2016/1148, je ponudnik digitalnih storitev sposoben ugotoviti, ali incident vpliva na zagotavljanje njegovih storitev v določenih državah članicah.

4. Obseg, v katerem je moteno delovanje storitve iz člena 16(4)(d) Direktive (EU) 2016/1148, se izmeri glede na eno ali več od naslednjih značilnosti, oslabljenih zaradi incidenta: razpoložljivost, avtentičnost, celovitost ali zaupnost podatkov ali povezanih storitev.

([1]) Uredba (EU) št. 1025/2012 Evropskega parlamenta in Sveta z dne 25. oktobra 2012 o evropski standardizaciji, spremembi direktiv Sveta 89/686/EGS in 93/15/EGS ter direktiv 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES in 2009/105/ES Evropskega parlamenta in Sveta ter razveljavitvi Sklepa Sveta 87/95/EGS in Sklepa št. 1673/2006/ES Evropskega parlamenta in Sveta (UL L 316, 14.11.2012, str. 12).

5. Kar zadeva obseg vpliva na gospodarske in družbene dejavnosti iz člena 16(4)(e) Direktive (EU) 2016/1148, je ponudnik digitalnih storitev zmožen, da na podlagi kazalnikov, kot je narava njegovih pogodbenih razmerij s stranko ali, kjer je to primerno, morebitno število prizadetih uporabnikov, ugotovi, ali je incident uporabnikom povzročil veliko materialno ali nematerialno škodo, na primer v zvezi z zdravjem, varnostjo ali škodo na premoženju.

6. Za namene odstavkov 1, 2, 3, 4 in 5 se od ponudnikov digitalnih storitev ne bi smelo zahtevati, da zbirajo dodatne informacije, do katerih nimajo dostopa.

Člen 4

Pomemben vpliv incidenta

1. Za incident se šteje, da ima pomemben vpliv, če velja vsaj ena od naslednjih okoliščin:

(a) storitev, ki jo zagotavlja ponudnik digitalnih storitev, ni bila na voljo več kot 5 000 000 uporabniških ur, pri čemer se pojem „uporabniška ura“ nanaša na število prizadetih uporabnikov v Uniji v obdobju šestdesetih minut;

(b) incident je povzročil izgubo celovitosti, avtentičnosti ali zaupnosti shranjenih ali prenesenih ali obdelanih podatkov ali povezanih storitev, ki jih ponujajo omrežja in informacijski sistemi ponudnika digitalnih storitev ali so dostopni prek njih, pri čemer je bilo prizadetih več kot 100 000 uporabnikov v Uniji;

(c) incident predstavlja tveganje za javno varnost in smrtno nevarnost;

(d) incident je povzročil materialno škodo vsaj enemu uporabniku v Uniji in ta presega 1 000 000 EUR.

2. Na podlagi dobre prakse, ki jo je skupina za sodelovanje zbrala pri izvajanju svojih nalog v skladu s členom 11(3) Direktive (EU) 2016/1148, in obravnav iz člena 11(3)(m) Direktive lahko Komisija pregleda prage, določene v odstavku 1.

Člen 5

Začetek veljavnosti

(1) Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

(2) Uporablja se od 10. maja 2018.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 30. januarja 2018

Za Komisijo

Predsednik

Jean-Claude JUNCKER