VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2018/151

z 30. januára 2018,

ktorým sa stanovujú pravidlá uplatňovania smernice Európskeho parlamentu a Rady (EÚ) 2016/1148, pokiaľ ide o bližšiu špecifikáciu prvkov, ktoré musia poskytovatelia digitálnych služieb zohľadňovať pri riadení rizík v oblasti bezpečnosti sietí a informačných systémov, a parametrov na posudzovanie toho, či má incident závažný vplyv

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na smernicu Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii ([1]), a najmä na jej článok 16 ods. 8,

keďže:

(1) V súlade so smernicou (EÚ) 2016/1148 majú poskytovatelia digitálnych služieb právo slobodne prijímať technické a organizačné opatrenia, ktoré považujú za vhodné a primerané na riadenie rizík v oblasti bezpečnosti ich sietí a informačných systémov, pokiaľ takéto opatrenia zabezpečujú primeranú úroveň bezpečnosti a zohľadňujú prvky stanovené v uvedenej smernici.

(2) Pri určovaní vhodných a primeraných technických a organizačných opatrení by poskytovateľ digitálnych služieb mal pristupovať k bezpečnosti informácií systematicky a využívať pritom prístup založený na posúdení rizík.

(3) V záujme zaistenia bezpečnosti systémov a zariadení by poskytovatelia digitálnych služieb mali vykonávať postupy posudzovania a analýzy. Tieto činnosti by sa mali týkať systematického riadenia sietí a informačných systémov, fyzickej a environmentálnej bezpečnosti, bezpečnosti dodávok a kontrol prístupu.

(4) Pri vykonávaní analýzy rizík v rámci systematického riadenia sietí a informačných systémov by poskytovatelia digitálnych služieb mali byť podnecovaní k tomu, aby identifikovali špecifické riziká a kvantifikovali ich význam napríklad tým, že identifikujú hrozby pre kľúčové aktíva a ich prípadný vplyv na operácie, a pritom stanovia spôsob, ako uvedené hrozby čo najlepšie zmierňovať na základe súčasných kapacít a požiadaviek na zdroje.

(5) Politiky v oblasti ľudských zdrojov by sa mohli zamerať na riadenie zručností vrátane aspektov súvisiacich s rozvojom zručností v oblasti bezpečnosti a so zvyšovaním informovanosti. Pri rozhodovaní o primeranom súbore politík v oblasti bezpečnosti prevádzky by poskytovatelia digitálnych služieb mali byť podnecovaní k tomu, aby zohľadňovali aspekty riadenia zmeny, riadenia zraniteľnosti, formalizácie prevádzkových a administratívnych postupov a mapovania systémov.

(6) V rámci politík v oblasti bezpečnostnej štruktúry by mohlo dôjsť najmä k oddeleniu sietí a systémov a mohli by zahŕňať osobitné bezpečnostné opatrenia pre kľúčové operácie, akými sú napr. administratívne operácie. Oddelenie sietí a systémov by poskytovateľovi digitálnych služieb umožnilo rozlišovať medzi prvkami, ako sú toky údajov a počítačové zdroje, ktoré patria klientovi, skupine klientov, poskytovateľovi digitálnych služieb alebo tretím stranám.

(7) Opatreniami prijatými so zreteľom na fyzickú a environmentálnu bezpečnosť by sa mali zabezpečiť siete a informačné systémy organizácie proti škodám spôsobeným incidentmi, ako sú napríklad, krádež, požiar, povodeň alebo iné poveternostné vplyvy, ako aj zlyhania telekomunikácií alebo výpadky elektrického prúdu.

(8) Bezpečnosť dodávok, ako napríklad elektrickej energie, pohonných hmôt alebo chladenia, by mohla zahŕňať bezpečnosť dodávateľského reťazca, v ktorej je začlenená najmä bezpečnosť vonkajších dodávateľov a subdodávateľov a ich riadenie. Vysledovateľnosťou kľúčových dodávok sa rozumie schopnosť poskytovateľa digitálnych služieb identifikovať a zaznamenávať zdroje takýchto dodávok.

(9) Medzi používateľov digitálnych služieb by mali patriť fyzické a právnické osoby, ktoré sú zákazníkmi alebo predplatiteľmi na online trhu alebo využívajú služby cloud computingu, alebo ktoré navštívili webové sídlo internetového vyhľadávača na účely vyhľadávania pomocou kľúčových slov.

([1]) Ú. v. EÚ L 194, 19.7.2016, s. 1.

(10) Pri vymedzovaní závažnosti vplyvu incidentu by sa prípady stanovené v tomto nariadení mali považovať za neúplný zoznam závažných incidentov. Bolo by vhodné využiť poznatky získané pri vykonávaní tohto nariadenia a z práce skupiny pre spoluprácu, pokiaľ ide o zbieranie informácií o najlepších postupoch v súvislosti s rizikami a incidentmi a diskutovanie o spôsoboch informovania o oznámených incidentoch, ako sa uvádza v článku 11 ods. 3 písm. i) a m) smernice (EÚ) 2016/1148. Výsledkom by mohli byť komplexné pokyny o kvantitatívnych prahových hodnotách parametrov na oznamovanie incidentov, ktoré by mohli viesť k aktivácii povinnosti poskytovateľov digitálnych služieb oznamovať incidenty podľa článku 16 ods. 3 smernice (EÚ) 2016/1148. Komisia by v prípade potreby mohla takisto zvážiť preskúmanie prahových hodnôt, ktoré sú v súčasnosti stanovené v tomto nariadení.

(11) Aby príslušné orgány mohli byť informované o potenciálnych nových rizikách, mali by byť poskytovatelia digitálnych služieb podnecovaní k tomu, aby dobrovoľne informovali o akomkoľvek incidente, ktorého charakteristiky im neboli predtým známe, ako napr. nové spôsoby zneužitia, vektory útoku alebo aktér hrozby, zraniteľnosti a nebezpečenstvá.

(12) Toto nariadenie by sa malo uplatňovať odo dňa nasledujúceho po dni, ktorým uplynie lehota na transpozíciu smernice (EÚ) 2016/1148.

(13) Opatrenia stanovené v tomto nariadení sú v súlade so stanoviskom Výboru pre bezpečnosť sietí a informačných systémov uvedeného v článku 22 smernice (EÚ) 2016/1148,

PRIJALA TOTO NARIADENIE:

Článok 1

Predmet úpravy

Týmto nariadením sa bližšie špecifikujú prvky, ktoré musia poskytovatelia digitálnych služieb zohľadňovať pri identifikovaní a prijímaní opatrení na účely zaistenia úrovne bezpečnosti sietí a informačných systémov, ktoré využívajú pri poskytovaní služieb uvedených v prílohe III k smernici (EÚ) 2016/1148, a parametre, ktoré sa majú zohľadňovať pri posudzovaní toho, či incident má závažný vplyv na poskytovanie uvedených služieb.

Článok 2

Bezpečnostné prvky

1. Bezpečnosťou systémov a zariadení podľa článku 16 ods. 1 písm. a) smernice (EÚ) 2016/1148 sa rozumie bezpečnosť sietí a informačných systémov a ich fyzického prostredia a zahŕňa tieto prvky:

a) systematické riadenie sietí a informačných systémov, t. j. mapovanie informačných systémov a vytvorenie súboru vhodných politík v oblasti riadenia bezpečnosti informácií vrátane analýzy rizík, ľudských zdrojov, bezpečnosti operácií, bezpečnostnej štruktúry, bezpečného riadenia životného cyklu údajov a systémov a v prípade potreby šifrovania a jeho riadenia;

b) fyzickú a environmentálnu bezpečnosť, t. j. dostupnosť súboru opatrení na ochranu bezpečnosti sietí a informačných systémov poskytovateľov digitálnych služieb pred poškodením na základe prístupu založeného na posúdení všetkých rizík, v rámci ktorého sa zohľadňuje napríklad zlyhanie systému, zlyhanie ľudského faktora, zlomyseľné konanie alebo prírodné javy;

c) bezpečnosť dodávok, t. j. vytvorenie a udržiavanie príslušných politík na účely zabezpečenia dostupnosti a v prípade potreby vysledovateľnosti kľúčových dodávok používaných pri poskytovaní služieb;

d) kontroly prístupu k sieťam a informačným systémom, t. j. dostupnosť súboru opatrení na zabezpečenie toho, aby bol fyzický a logický prístup k sieťam a informačným systémom vrátane administratívnej bezpečnosti sietí a informačných systémov povolený a obmedzený na základe obchodných a bezpečnostných požiadaviek.

2. Pokiaľ ide o riešenie incidentov podľa článku 16 ods. 1 písm. b) smernice (EÚ) 2016/1148, opatrenia prijaté poskytovateľmi digitálnych služieb zahŕňajú:

a) udržiavanie a testovanie procesov a postupov odhaľovania incidentov na účely včasného a náležitého informovania o výskyte anomálií;

b) postupy a politiky týkajúce sa oznamovania incidentov a identifikácie nedostatkov a slabých stránok a v ich informačných systémoch;

c) reakciu v súlade so zavedenými postupmi a podávanie správ o výsledkoch prijatých opatrení;

d) posúdenie závažnosti incidentu, zdokumentovanie poznatkov z analýzy incidentu a zhromaždenie príslušných informácií, ktoré môžu slúžiť ako dôkazy a podklady pri procese neustáleho zlepšovania.

3. Riadenie kontinuity činnosti podľa článku 16 ods. 1 písm. c) smernice (EÚ) 2016/1148 predstavuje schopnosť organizácie udržiavať alebo v prípade potreby obnovovať poskytovanie služieb na prijateľnej a vopred určenej úrovni po rušivom incidente a zahŕňa:

a) vypracovanie a používanie pohotovostných plánov založených na analýze vplyvu na podnikateľskú činnosť na zabezpečenie kontinuity služieb poskytovaných poskytovateľmi digitálnych služieb, ktoré sa musia pravidelne vyhodnocovať a testovať napríklad prostredníctvom cvičení;

b) spôsobilosť obnoviť prevádzku po núdzovej udalosti, ktorá sa musí pravidelne vyhodnocovať a testovať napríklad prostredníctvom cvičení.

4. Monitorovanie, audit a skúšanie podľa článku 16 ods. 1 písm. d) smernice (EÚ) 2016/1148 zahŕňajú vytvorenie a udržiavanie politík týkajúcich sa:

a) vykonávania plánovanej postupnosti pozorovaní alebo meraní na posúdenie toho, či siete a informačné systémy fungujú tak, ako sa plánovalo;

b) inšpekcií a overení na účely kontroly toho, či sa dodržiavajú normy alebo súbory pokynov, či sú záznamy presné a či sa plnia ciele v oblasti účinnosti a účelnosti;

c) procesu zameraného na odhaľovanie nedostatkov bezpečnostných mechanizmov siete a informačného systému, ktoré chránia údaje a udržiavajú funkčnosť tak, ako sa plánovalo. Tento proces zahŕňa technické postupy a zamestnancov zapojených do toku prevádzky.

5. Medzinárodné normy podľa článku 16 ods. 1 písm. e) smernice (EÚ) 2016/1148 predstavujú normy prijaté medzinárodným normalizačným orgánom, ako sa stanovuje v článku 2 ods. 1 písm. a) nariadenia Európskeho parlamentu a Rady (EÚ) č. 1025/2012 ([1]). Podľa článku 19 smernice (EÚ) 2016/1148 sa môžu použiť európske alebo medzinárodne uznávané normy a špecifikácie, ktoré sú relevantné pre bezpečnosť sietí a informačných systémov, vrátane existujúcich vnútroštátnych noriem.

6. Poskytovatelia digitálnych služieb zabezpečujú, že majú k dispozícii dostatočnú dokumentáciu, ktorá príslušnému orgánu umožní overiť súlad s bezpečnostnými prvkami uvedenými v odsekoch 1, 2, 3, 4 a 5.

Článok 3

Parametre, ktoré sa majú zohľadňovať pri posudzovaní toho, či má incident závažný vplyv

1. Vzhľadom na počet používateľov postihnutých incidentom, najmä používateľov využívajúcich danú službu na účely poskytovania vlastných služieb podľa článku 16 ods. 4 písm. a) smernice (EÚ) 2016/1148, poskytovateľ digitálnych služieb musí byť schopný odhadnúť jeden z týchto údajov:

a) počet fyzických a právnických osôb postihnutých incidentom, s ktorými uzavrel zmluvu o poskytovaní služby, alebo

b) počet postihnutých používateľov, ktorí službu použili, a to najmä na základe predchádzajúcich údajov o prevádzke.

2. Dĺžkou trvania incidentu podľa článku 16 ods. 4 písm. b) sa rozumie obdobie od narušenia riadneho poskytovania služby z hľadiska dostupnosti, pravosti, integrity alebo dôvernosti až po obnovenie poskytovania služby.

3. Pokiaľ ide o geografický rozsah oblasti postihnutej incidentom podľa článku 16 ods. 4 písm. c) smernice (EÚ) 2016/1148, poskytovateľ digitálnych služieb musí byť schopný určiť, či incident má vplyv na poskytovanie jeho služieb v určitých členských štátoch.

4. Stupeň narušenia fungovania služby podľa článku 16 ods. 4 písm. d) smernice (EÚ) 2016/1148 sa meria na základe jednej alebo viacerých týchto charakteristík, ktoré boli narušené incidentom: dostupnosť, pravosť, integrita alebo dôvernosť údajov alebo súvisiacich služieb.

([1]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 z 25. októbra 2012 o európskej normalizácii, ktorým sa menia a dopĺňajú smernice Rady 89/686/EHS a 93/15/EHS a smernice Európskeho parlamentu a Rady 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES a 2009/105/ES a ktorým sa zrušuje rozhodnutie Rady 87/95/EHS a rozhodnutie Európskeho parlamentu a Rady č. 1673/2006/ES (Ú. v. EÚ L 316, 14.11.2012, s. 12).

5. Pokiaľ ide o rozsah vplyvu na hospodárske a spoločenské činnosti podľa článku 16 ods. 4 písm. e) smernice (EÚ) 2016/1148, poskytovateľa digitálnych služieb musí byť schopný posúdiť na základe údajov, ako je napríklad povaha jeho zmluvných vzťahov so zákazníkom alebo v prípade potreby potenciálny počet postihnutých používateľov, či incident spôsobil používateľom závažné materiálne alebo nemateriálne škody, napr. v súvislosti so zdravím, bezpečnosťou alebo poškodením majetku.

6. Na účely odsekov 1, 2, 3, 4 a 5 sa nevyžaduje, aby poskytovatelia digitálnych služieb zhromažďovali ďalšie informácie, ku ktorým nemajú prístup.

Článok 4

Závažný vplyv incidentu

1. Za incident, ktorý má závažný vplyv, sa považuje incident, pri ktorom nastala aspoň jedna z týchto situácií:

a) služba poskytovaná poskytovateľom digitálnych služieb bola nedostupná v rozsahu väčšom než 5 000 000 používateľských hodín, pričom pojem používateľská hodina sa týka počtu postihnutých používateľov v Únii počas šesťdesiatich minút;

b) incident viedol k strate integrity, pravosti alebo dôvernosti uchovávaných, zasielaných alebo spracovávaných údajov alebo súvisiacich služieb ponúkaných alebo prístupných prostredníctvom siete alebo informačného systému poskytovateľa digitálnych služieb, čo malo vplyv na viac ako 100 000 používateľov v Únii;

c) incident viedol k vzniku rizika pre verejný poriadok či verejnú bezpečnosť alebo k strate života;

d) incident viedol k vzniku materiálnej škody v prípade aspoň jedného používateľa v Únii, pričom škoda spôsobená tomuto používateľovi presahuje 1 000 000 EUR.

2. Na základe najlepších postupov zhromaždených skupinou pre spoluprácu pri výkone jej úloh podľa článku 11 ods. 3 smernice (EÚ) 2016/1148 a na základe diskusií podľa článku 11 ods. 3 písm. m) uvedenej smernice Komisia môže preskúmať prahové hodnoty stanovené v odseku 1.

Článok 5

Nadobudnutie účinnosti

1. Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

2. Uplatňuje sa od 10. mája 2018.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 30. januára 2018

Za Komisiu

predseda

Jean-Claude JUNCKER