PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2018/151

ze dne 30. ledna 2018,

kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na směrnici Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii [1], a zejména na čl. 16 odst. 8 uvedené směrnice,

vzhledem k těmto důvodům:

(1) V souladu se směrnicí (EU) 2016/1148 mají poskytovatelé digitálních služeb možnost přijímat technická a organizační opatření, jež považují za vhodná a přiměřená z hlediska řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, pokud uvedená opatření zajišťují odpovídající úroveň bezpečnosti a zohledňují prvky stanovené v uvedené směrnici.

(2) Při určování vhodných a přiměřených technických a organizačních opatření by poskytovatelé digitálních služeb měli přistupovat k bezpečnosti informací systematicky a využívat přitom přístup založený na posouzení rizik.

(3) Za účelem zajištění bezpečnosti systémů, budov a zařízení by poskytovatelé digitálních služeb měli provádět postupy posuzování a analýzy. Tyto činnosti by se měly týkat systematického řízení sítí a informačních systémů, fyzické a environmentální bezpečnosti, bezpečnosti dodávek a kontrol přístupu.

(4) Při provádění analýzy rizik v rámci systematického řízení sítí a informačních systémů by poskytovatelé digitálních služeb měli být vybízeni k tomu, aby určili specifická rizika a kvantifikovali jejich významnost, například určením hrozeb pro klíčová aktiva a jejich případného dopadu na provoz, a přitom stanovili způsob, jak uvedeným hrozbám co nejlépe zabránit na základě stávajících kapacit a požadavků na zdroje.

(5) Politiky v oblasti lidských zdrojů by mohly odkazovat na řízení získávání dovedností, včetně aspektů souvisejících s rozvojem dovedností souvisejících s bezpečností a zvyšováním informovanosti. Při rozhodování o přiměřeném souboru politik v oblasti bezpečnosti provozu by poskytovatelé digitálních služeb měli být vybízeni k tomu, aby zohlednili aspekty řízení změn, řízení zranitelností, formalizace provozních a správních postupů a mapování systémů.

(6) Politiky v oblasti bezpečnostní architektury by mohly zahrnovat zejména oddělení sítí a systémů, jakož i zvláštní bezpečnostní opatření pro kritické operace, jako je například správa. Oddělení sítí a systémů by mohlo poskytovatelům digitálních služeb umožnit rozlišovat prvky, jako jsou např. toky dat a výpočetní zdroje, které patří klientovi, skupině klientů, poskytovateli digitálních služeb nebo třetím stranám.

(7) Opatření přijatá v souvislosti s fyzickou a environmentální bezpečností by měla zajistit bezpečnost sítí a informačních systémů organizace před poškozením v případě výskytu incidentů, jako jsou například krádež, požár, zatopení nebo jiné povětrnostní vlivy, jakož i telekomunikační selhání či výpadky proudu.

(8) Bezpečnost dodávek, jako např. elektrické energie, pohonných hmot či chlazení, by mohla zahrnovat bezpečnost dodavatelského řetězce, což zahrnuje zejména bezpečnost vnějších dodavatelů a subdodavatelů a jejich řízení. Sledovatelností kritických dodávek se rozumí schopnost poskytovatele digitálních služeb určit a zaznamenat zdroje uvedených dodávek.

(9) Uživatelé digitálních služeb by měli zahrnovat fyzické a právnické osoby, které jsou zákazníky internetového tržiště nebo služby cloud computingu či účastníky ve vztahu k internetovému tržišti nebo službě cloud computingu nebo navštívily stránku internetového vyhledávače za účelem vyhledávání pomocí klíčových slov.

[1] Úř. věst. L 194, 19.7.2016, s. 1.

(10) Při definování významnosti dopadu incidentu by se případy stanovené v tomto nařízení měly považovat za demonstrativní výčet významných incidentů. Je zapotřebí využít zkušeností získaných z provádění tohoto nařízení a z činnosti skupiny pro spolupráci v rámci shromažďování informací o osvědčených postupech, pokud jde o rizika a incidenty, a jednání o způsobech hlášení incidentů, jak je uvedeno v čl. 11 odst. 3 písm. i) a m) směrnice (EU) 2016/1148. Výsledkem by mohly být komplexní pokyny o kvantitativních mezních hodnotách parametrů hlášení, které by mohly vést k aktivaci ohlašovací povinnosti poskytovatelů digitálních služeb podle čl. 16 odst. 3 směrnice (EU) 2016/1148. Komise by v příslušných případech mohla rovněž zvážit přezkum mezních hodnot, které jsou v současné době stanoveny v tomto nařízení.

(11) Aby příslušné orgány mohly být informovány o potenciálních nových rizicích, měli by poskytovatelé digitálních služeb být vybízeni k tomu, aby dobrovolně hlásili jakékoli incidenty, jejichž charakteristiky jim předtím nebyly známy, např. nové způsoby zneužití zranitelností (tzv. exploits), nové cesty vedení útoku nebo aktéry ohrožení, zranitelnosti a nebezpečí.

(12) Toto nařízení by se mělo použít od prvního dne po uplynutí lhůty k provedení směrnice (EU) 2016/1148.

(13) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem Výboru pro bezpečnost sítí a informačních systémů uvedeného v článku 22 směrnice (EU) 2016/1148,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Předmět

Toto nařízení blíže upřesňuje prvky, které musí poskytovatelé digitálních služeb zohlednit při určování a přijímání opatření za účelem zajištění úrovně bezpečnosti sítí a informačních systémů, které využívají v souvislosti s nabízením služeb uvedených v příloze III směrnice (EU) 2016/1148, a blíže upřesňuje parametry, které je nutné zvážit při posouzení toho, zda má incident významný dopad na poskytování uvedených služeb.

Článek 2

Bezpečnostní prvky

1. Bezpečností systémů a zařízení podle v čl. 16 odst. 1 písm. a) směrnice (EU) 2016/1148 se rozumí bezpečnost sítí a informačních systémů a jejich fyzického prostředí a zahrnuje tyto prvky:

a) systematické řízení sítí a informačních systémů, což znamená mapování informačních systémů a vytvoření souboru vhodných politik v oblasti řízení bezpečnosti informací, včetně analýzy rizik, lidských zdrojů, bezpečnosti operací, bezpečnostní architektury, bezpečného řízení životního cyklu dat a systémů, případně šifrování a jeho řízení;

b) fyzickou a environmentální bezpečnost, což znamená dostupnost souboru opatření za účelem ochrany bezpečnosti sítí a informačních systémů poskytovatelů digitálních služeb před poškozením na základě přístupu založeném na posouzení rizik, který zohledňuje například selhání systému, lidské chyby, svévolné zásahy nebo přírodní jevy;

c) bezpečnost dodávek, což znamená vytvoření a udržování příslušných politik za účelem zajištění dostupnosti a případně sledovatelnosti kritických dodávek používaných při poskytování služeb;

d) kontroly přístupu k sítím a informačním systémům, což znamená dostupnost souboru opatření za účelem zajištění, že fyzický a logický přístup k sítím a informačním systémům, včetně administrativní bezpečnosti sítí a informačních systémů, je autorizován a omezen na základě obchodních a bezpečnostních požadavků;

2. Pokud jde o řešení incidentů podle čl. 16 odst. 1 písm. b) směrnice (EU) 2016/1148, opatření přijatá poskytovateli digitálních služeb zahrnují:

a) udržování a testování postupů a procesů pro detekci za účelem zajištění včasného a dostatečného informování o výskytu anomálií;

b) postupy a politiky týkající se ohlašování incidentů a identifikace slabých stránek a zranitelností v jejich informačních systémech;

c) reakci v souladu se stanovenými postupy a podávání zpráv o výsledcích přijatých opatření;

d) posouzení závažnosti incidentu, zdokumentování znalostí z analýzy incidentu a shromáždění příslušných informací, které mohou sloužit jako důkaz a podpora procesu neustálého zlepšování.

3. Řízení kontinuity provozu podle čl. 16 odst. 1 písm. c) směrnice (EU) 2016/1148 znamená schopnost organizace udržovat či případně obnovovat poskytování služeb na přijatelné, předem definované úrovni následně po rušivém incidentu a zahrnuje:

a) vypracování a používání krizových plánů na základě analýzy dopadu na podnikatelskou činnost za účelem zajištění kontinuity služeb poskytovaných poskytovateli digitálních služeb, které musí být pravidelně posuzovány a testovány například prostřednictvím cvičení;

b) schopnosti pro obnovení provozu po mimořádné události, které musí být pravidelně posuzovány a testovány například prostřednictvím cvičení.

4. Monitorování, audity a testování podle čl. 16 odst. 1 písm. d) směrnice (EU) 2016/1148 zahrnují vypracování a udržování politik týkajících se:

a) provádění plánované série pozorování či měření za účelem posouzení, zda sítě a informační systémy fungují zamýšleným způsobem;

b) inspekcí a ověřování za účelem kontroly, zda jsou dodržovány normy nebo soubory pokynů, zda záznamy jsou přesné a zda jsou plněny cíle v oblasti účinnosti a účelnosti;

c) procesu pro odhalování nedostatků v bezpečnostních mechanismech sítě a informačního systému, které chrání data a udržují zamýšlenou funkcionalitu. Tento proces zahrnuje technické postupy a pracovníky zapojené do provozu.

5. Mezinárodními normami uvedenými v čl. 16 odst. 1 písm. e) směrnice (EU) 2016/1148 se rozumí normy přijaté mezinárodním normalizačním orgánem, jak stanoví čl. 2 odst. 1 písm. a) nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ([1]). Podle článku 19 směrnice (EU) 2016/1148 se mohou použít evropské nebo mezinárodně uznávané normy a specifikace upravující bezpečnost sítí a informačních systémů, včetně stávajících vnitrostátních norem.

6. Poskytovatelé digitálních služeb zajistí, že budou mít k dispozici odpovídající dokumentaci, aby příslušný orgán mohl ověřit dodržování bezpečnostních prvků uvedených v odstavcích 1, 2, 3, 4 a 5.

Článek 3

Parametry, které musí být zohledněny při posuzování toho, zda je dopad incidentu významný

1. S ohledem na počet uživatelů postižených incidentem, zejména těch uživatelů, kteří na službu spoléhají při poskytování vlastních služeb, jak je uvedeno v čl. 16 odst. 4 písm. a) směrnice (EU) 2016/1148, musí být poskytovatel digitálních služeb schopen odhadnout jeden z těchto počtů:

a) počet fyzických a právnických osob postižených incidentem, s nimiž uzavřel smlouvu na poskytování služeb nebo

b) počet dotčených uživatelů, kteří službu použili, založený zejména na předchozích údajích o provozu.

2. Délkou trvání incidentu uvedenou v čl. 16 odst. 4 písm. b) se rozumí časové období od narušení řádného poskytování služby ve smyslu dostupnosti, autenticity, integrity nebo důvěrnosti až po obnovení služby.

3. Pokud jde o zeměpisný rozsah oblasti dotčené incidentem uvedený v čl. 16 odst. 4 písm. c) směrnice (EU) 2016/1148, musí být poskytovatel digitálních služeb schopen určit, zda se incident dotýká poskytování jeho služeb v určitých členských státech.

4. Rozsah, v jakém bylo narušeno fungování služby, uvedený v čl. 16 odst. 4 písm. d) směrnice (EU) 2016/1148 se posuzuje na základě alespoň jedné z těchto charakteristik, které byly narušeny incidentem: dostupnost, autenticita, integrita nebo důvěrnost dat či souvisejících služeb.

([1]) Nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ze dne 25. října 2012 o evropské normalizaci, změně směrnic Rady 89/686/EHS a 93/15/EHS a směrnic Evropského 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 kterým se ruší rozhodnutí Rady 87/95/EHS a rozhodnutí Evropského parlamentu a Rady č. 1673/2006/ES (Úř. věst. L 316, 14.11.2012, s. 12).

5. Pokud jde o rozsah dopadu na společenské a ekonomické činnosti uvedený v čl. 16 odst. 4 písm. e) směrnice (EU) 2016/1148, poskytovatel digitálních služeb musí být na základě ukazatelů, jako je například povaha jeho smluvních vztahů se zákazníkem či případně potenciální počet dotčených uživatelů, schopen určit, zda incident způsobil uživatelům závažné materiální či nemateriální škody, např. ve vztahu ke zdraví, bezpečnosti nebo poškození majetku.

6. Pro účely odstavců 1, 2, 3, 4 a 5 se nepožaduje, aby poskytovatelé digitálních služeb shromažďovali další informace, k nimž nemají přístup.

Článek 4

Významný dopad incidentu

1. Za incident, který má významný dopad, se považuje incident, u nějž nastala alespoň jedna z těchto situací:

a) služba poskytovaná poskytovatelem digitálních služeb byla nedostupná v rozsahu větším než 5 000 000 uživatelských hodin, přičemž pojmem uživatelská hodina se vztahuje k počtu uživatelů v Unii, kteří byli dotčeni po dobu šedesáti minut;

b) incident vedl ke ztrátě integrity, autenticity nebo důvěrnosti uchovávaných, předávaných nebo zpracovávaných dat nebo souvisejících služeb, které nabízejí sítě nebo informační systémy poskytovatele digitálních služeb nebo které jsou jejich prostřednictvím přístupné, a ovlivněno bylo více než 100 000 uživatelů v Unii;

c) incident vytvořil riziko pro veřejnou bezpečnost a ochranu nebo ztrátu života;

d) incident způsobil materiální škodu alespoň jednomu uživateli v Unii, přičemž škoda způsobená uvedenému uživateli překračuje 1 000 000 EUR;

2. Na základě osvědčených postupů shromážděných skupinou pro spolupráci v rámci svých úkolů podle čl. 11 odst. 3 směrnice (EU) 2016/1148 a na základě jednání podle čl. 11 odst. 3 písm. m) uvedené směrnice, může Komise přezkoumat mezní hodnoty uvedené v odstavci 1.

Článek 5

Vstup v platnost

1. Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

2. Použije se ode dne 10. května 2018.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 30. ledna 2018.

Za Komisi

předseda

Jean-Claude JUNCKER