**VYKONÁVACIE NARIADENIA KOMISIE (EU).../...**

**z ....**

**ktorým sa stanovujú pravidlá uplatňovania smernice Európskeho parlamentu a Rady (EÚ) 2016/1148, pokiaľ ide o ďalšie špecifikácie prvkov, ktoré by mali brať do úvahy poskytovatelia digitálnych služieb na riadenie rizík, ktoré by mohli predstavovať hrozby pre bezpečnosť sieťových a informačných systémov a pre parametre na určenie podstatného vplyvu incidentu**

**EURÓPSKA KOMISIA**

So zreteľom na Zmluvu o fungovaní Európskej únie,

So zreteľom na smernicu Európskeho parlamentu a Rady (EÚ) č. 2016/1148 zo 6. júla 2016 o opatreniach na vysokú spoločnú úroveň bezpečnosti sietí a informačných systémov v Únii, a najmä na jej článok 16 ods. 8,

vzhľadom na to:

V súlade so smernicou (EÚ) 2016/1148 môžu poskytovatelia digitálnych služieb naďalej slobodne prijímať technické a organizačné opatrenia, ktoré považujú za primerané a adekvátne na riadenie rizík, ktoré predstavujú hrozby pre bezpečnosť ich sietí a informačných systémov, pokiaľ tieto opatrenia dokážu zabezpečiť primeranú úroveň bezpečnosti a zohľadniť prvky stanovené v uvedenej Smernici.

Pri určovaní vhodných a primeraných technických a organizačných opatrení by sa mal poskytovateľ digitálnych služieb systematicky orientovať na bezpečnosť informácií s využitím prístupu založeného na riadení rizík.

Aby sa zabezpečila bezpečnosť systémov a zariadení, poskytovatelia digitálnych služieb by mali vykonávať posudzovania a analýzy. Tieto činnosti by sa mali týkať fyzickej a environmentálnej bezpečnosti, bezpečnosti dodávok, kontroly prístupu a systematického riadenia sietí a informačných systémov. Opatrenia prijaté v súvislosti s fyzickou a environmentálnou bezpečnosťou by mali zabezpečiť bezpečnosť siete a informačných systémov organizácie pred poškodením spôsobeným incidentmi ako krádež, požiar, záplavy alebo iné poveternostné vplyvy, telekomunikácie alebo výpadky elektrickej energie.

Bezpečnosť dodávok, ako je elektrická energia, palivo alebo chladenie, by mohla zahŕňať bezpečnosť dodávateľského reťazca, ktorá zahŕňa najmä bezpečnosť tretích strán a to dodávateľov, subdodávateľov ich riadenie.

Pri vykonávaní analýzy rizika v rámci systematického riadenia sietí a informačných systémov by sa mali byť poskytovatelia digitálnych služieb sústrediť hlavne na to, aby identifikovali špecifické riziká a kvantifikovali ich význam, napríklad identifikovaním hrozieb pre kritické aktíva a spôsob, akým môžu ovplyvniť operácie, alebo ako najlepšie zmierniť tieto hrozby na základe súčasných schopností a požiadaviek týkajúcich sa zdrojových možností.

Politika ľudských zdrojov by sa mohla vzťahovať na riadenie zručností vrátane aspektov súvisiacich s rozvojom zručností týkajúcich sa bezpečnosti a zvyšovania povedomia. Pri rozhodovaní o vhodnom súbore bezpečnostných opatrení v prevádzke by sa mali poskytovatelia digitálnych služieb hlavne sústrediť na to, aby zohľadňovali aspekty riadenia zmien, riadenia zraniteľnosti, formalizácie prevádzkových a administratívnych postupov a systémového mapovania.

Politiky týkajúce sa bezpečnostnej infraštruktúry by mohli zahŕňať najmä oddelenie sietí a systémov, ako aj osobitné bezpečnostné opatrenia pre kritické operácie, ako aj administratívne operácie. Segregácia sietí a systémov by mohla umožniť poskytovateľovi digitálnych služieb rozlišovať medzi prvkami, ako sú toky údajov a výpočtové dátové zdroje, ktoré patria klientovi, skupine klientov, poskytovateľovi digitálnych služieb alebo tretím stranám.

Na účely posúdenia vplyvu incidentu vzhľadom na parametre uvedené v článku 16 ods. 4 smernice (EÚ) 2016/1148 by sa od poskytovateľov digitálnych služieb nemalo vyžadovať, aby zhromažďovali dodatočné informácie, ktoré presahujú dostupné informácie získané počas bežného vykonávania ich služieb.

Používatelia digitálnych služieb by mali zahŕňať fyzické a právnické osoby, ktoré sú zákazníkmi alebo sú účastníkmi internetového trhoviska alebo služby cloud computingu, alebo ktorí sú návštevníkmi internetovej stránky poskytujúcej vyhľadávacie nástroje pre účely vyhľadávania kľúčových slov.

Pri definovaní rozsahu vplyvu incidentu by sa prípady ustanovené v tomto nariadení mali považovať za neúplný zoznam závažných incidentov. Toto by malo slúžiť ako príklad poučenia sa z činnosti vzniknutej pri implementácii tohto nariadenia a z práce Skupiny pre spoluprácu, pokiaľ ide o zbieranie informácií o najlepších postupoch v súvislosti s rizikami a incidentmi a diskusie o spôsoboch informovania o oznámených incidentoch v bodoch i) a m) článku 11 ods. 3 smernice (EÚ) 2016/1148. Výsledkom by mohli byť komplexné usmernenia o kvantitatívnych prahových hodnotách oznamovacích parametrov, ktoré môžu viesť k oznamovacej povinnosti pre poskytovateľov digitálnych služieb podľa článku 16 ods. 3 smernice (EÚ) 2016/1148. V prípade potreby by Komisia mohla zvážiť aj preskúmanie prahových hodnôt stanovených v tomto nariadení.

Aby mohli byť príslušné orgány dostatočne informované o možných nových rizikách, poskytovatelia digitálnych služieb by mali byť silne motivovaní, aby dobrovoľne hlásili akýkoľvek incident, ktorého charakteristiky boli predtým neznáme, ako sú nové odhalenia, útoky, zraniteľnosti a riziká.

Opatrenia ustanovené 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**

Toto nariadenie ďalej špecifikuje prvky, ktoré majú brať do úvahy poskytovatelia digitálnych služieb pri určovaní a prijímaní opatrení na zabezpečenie úrovne bezpečnosti sietí a informačných systémov, ktoré používajú v súvislosti s ponukou služieb uvedených v prílohe III k smernici (EÚ) 2016/1148 a ďalej špecifikuje parametre, ktoré sa majú brať do úvahy pri určovaní, či má incident závažný vplyv na poskytovanie týchto služieb.

**Článok 2**

**Bezpečnostné prvky**

Bezpečnosť systémov a zariadení uvedených v článku 16 ods. 1 písm. a) smernice (EÚ) 2016/1148 znamená bezpečnosť sietí a informačných systémov a ich fyzického prostredia a zahŕňa tieto prvky:

fyzická a environmentálna bezpečnosť, čo znamená dostupnosť súboru opatrení na ochranu bezpečnosti sietí a informačných systémov poskytovateľov digitálnych služieb pred poškodením spôsobeným nehodami vzniknutými všetkými nebezpečenstvami a hrozbami, náhodnými alebo škodlivými, ľudskými alebo environmentálnymi;

bezpečnosť dodávok, čo znamená vytvorenie a udržiavanie vhodných politík s cieľom zabezpečiť dostupnosť a prípadne sledovateľnosť kritických dodávok používaných pri poskytovaní služieb;

kontroly prístupu do sietí a informačných systémov, čo znamená dostupnosť súboru opatrení na zabezpečenie toho, aby fyzický a logický prístup k sieťam a informačným systémom vrátane administratívnej bezpečnosti sietí a informačných systémov bol povolený a obmedzený na základe prevádzkových a bezpečnostných požiadaviek;

systematické riadenie sietí a informačných systémov, čo znamená mapovanie informačných systémov a vytvorenie súboru vhodných politík na riadenie bezpečnosti informácií, vrátane analýzy rizík, ľudských zdrojov, bezpečnosti operácií, bezpečnostnej infraštruktúry, zabezpečených údajov a systému riadenia životného cyklu a ak je to vhodné, šifrovanie a jeho riadenie.

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

udržiavané a testované procesy a postupy odhaľovania s cieľom zabezpečiť včasné a primerané vedomie o nezvyčajných udalostiach;

procesy a politiky týkajúce sa hlásenia incidentov v oblasti bezpečnosti informácií a už zistené nedostatky a zraniteľnosti v svojich informačných systémoch;

odpoveď v súlade s dokumentovanými postupmi a oznamovanie výsledkov prijatého opatrenia;

posúdenie závažnosti incidentu, zdokumentovanie poznatkov z analýzy incidentov a zhromažďovanie príslušných informácií, ktoré môžu slúžiť ako dôkaz a podpora pre proces neustáleho zlepšovania sa.

Riadenie kontinuity činností uvedených v článku 16 ods. 1 písm. c) smernice (EÚ) 2016/1148 znamená schopnosť organizácie po rušivom incidente zachovať alebo prípadne obnoviť poskytovanie služieb na prijateľnej vopred stanovenej úrovni zahŕňajú:

vytvorenie a používanie pohotovostných plánov založených na analýze prevádzkového dopadu s cieľom zabezpečiť kontinuitu služieb poskytovaných poskytovateľmi digitálnych služieb, ktoré sa pravidelne vyhodnocujú a testujú napríklad prostredníctvom cvičení;

schopnosť na obnovenie prevádzky po havárii, ktorá sa pravidelne posudzuje a testuje, napríklad prostredníctvom cvičení.

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

vykonávania plánovaných postupných pozorovaní alebo meraní s cieľom posúdiť, či siete a informačné systémy fungujú podľa plánu;

kontroly a overovania s cieľom skontrolovať, či sa dodržiavajú štandardné alebo stanovené usmernenia, a či sú záznamy presné a sú splnené ciele účinnosti a efektívnosti;

procesu zameraného na odhalenie nedostatkov bezpečnostných mechanizmov siete a informačného systému, ktoré chránia dáta a zachovávajú funkčnosť podľa plánu. Takýto proces zahŕňa technické procesy a personál zapojený do prevádzky.

Medzinárodné normy uvedené v článku 16 ods. 1 písm. e) Smernice (EÚ) 2016/1148 znamenajú normy prijaté medzinárodným normalizačným orgánom uvedeným v článku 2 ods. 1 písm. a) Nariadenia Európskeho parlamentu a Rady (EÚ) č. 1025/2012. Podľa článku 19 smernice (EÚ) 2016/1148 sa môžu použiť aj európske alebo medzinárodne uznávané normy a špecifikácie týkajúce sa bezpečnosti sietí a informačných systémov vrátane existujúcich vnútroštátnych noriem.

Opatrenia prijaté poskytovateľom digitálnych služieb v súlade s odsekmi 1, 2, 3, 4 a 5 sa zdokumentujú.

**Článok 3**

**Parametre, ktoré sa majú zohľadniť pri určovaní toho, či je dopad incidentu závažný**

Pokiaľ ide o počet užívateľov postihnutých incidentom, najmä užívateľov, ktorí využívajú službu na poskytovanie svojich vlastných služieb uvedených v článku 16 ods. 4 písm. a) smernice (EÚ) 2016/1148, poskytovateľ digitálnych služieb musí byť schopný odhadnúť niektorú z týchto možností:

počet postihnutých fyzických a právnických osôb, s ktorými bola uzatvorená zmluva o poskytnutí služby; alebo

počet používateľov, ktorí využívali službu, a to najmä na základe predchádzajúcich prevádzkových údajov.

Dĺžka trvania incidentu uvedenej v článku 16 ods. 4 písm. b) znamená časový úsek od prerušenia riadneho poskytovania služby z hľadiska dostupnosti, pravosti, integrity alebo dôvernosti až do času obnovenia.

Pokiaľ ide o geografické rozsah s ohľadom na oblasť postihnutú incidentom uvedeným v článku 16 ods. 4 písm. c) smernice (EÚ) 2016/1148, poskytovateľ digitálnych služieb musí byť schopný identifikovať či táto udalosť zasahuje do poskytovania jeho služieb v konkrétnych členských štátoch.

Stupňa narušenia fungovania služby uvedený v článku 16 ods. 4 písm. d) smernice (EÚ) 2016/1148 sa meria, pokiaľ ide o jednu alebo viaceré z nasledujúcich charakteristík poškodených nehodou: dostupnosť, pravosť, integrita alebo dôvernosť údajov alebo súvisiacich služieb.

Pokiaľ ide o rozsah vplyvu na hospodárske a spoločenské činnosti uvedené v článku 16 ods. 4 písm. e) smernice (EÚ) 2016/1148, poskytovateľ digitálnych služieb musí vedieť uviesť na základe údajov, ako sú povaha svojich zmluvných vzťahov so zákazníkom alebo prípadne potenciálny počet postihnutých používateľov, či incident spôsobil používateľom značné materiálne alebo nemateriálne straty, napríklad v súvislosti so zdravím, bezpečnosťou alebo majetkovou ujmou.

**Článok 4**

**Závažný vplyv incidentu**

Incident sa považuje za mimoriadne závažný, ak sa vyskytla aspoň jedna z týchto situácií:

ak služba poskytovaná poskytovateľom digitálnych služieb nebola dostupná viac ako 5 000 000 používateľských hodín, pričom pojem používateľská hodina sa vzťahuje na počet dotknutých používateľov po dobu šesťdesiatich minút,

ak incident spôsobil stratu integrity, pravosti alebo dôvernosti uložených alebo prenášaných alebo spracovaných údajov, alebo s tým súvisiacich služieb ponúkaných alebo prístupných prostredníctvom siete a informačného systému poskytovateľa digitálnych služieb, ktorý postihuje viac ako 100 000 užívateľov v Únii;

ak incident spôsobil ohrozenie verejnej bezpečnosti a verejného poriadku

ak incident spôsobil hmotnú škodu najmenej jednému užívateľovi kde výška škody prevýši 1 000 000 EUR

ak incident narušil dodanie služieb vo dvoch alebo viac členských krajinách

Na základe osvedčených postupov, ktoré získaných Skupinou pre spoluprácu pri výkone jej úloh podľa článku 11 ods. 3 Smernice (EÚ) 2016/1148 a na základe podnetov z diskusie podľa článku 11 ods. 3 písm. m), môže Komisia preskúmať prahové hodnoty stanovené v odseku 1.

**Článok 5**

**Nadobudnutie platnosti**

Toto nariadenie nadobúda platnosť dvadsiatym dňom po jeho uverejnení v Úradnom vestníku Európskej únie.

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

V Bruseli,

 Za Komisiu

 Predseda