315

VYHLÁŠKA

ze dne 24. srpna 2021

o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 28 odst. 2 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 205/2017 Sb., (dále jen „zákon“):

§ 1

Předmět úpravy

Tato vyhláška stanoví bezpečnostní úrovně pro využívání cloud computingu orgány veřejné moci podle § 6 písm. e) zákona.

§ 2

Vymezení pojmů

Pro účely této vyhlášky se rozumí

a) poptávaným cloud computingem informační nebo komunikační systém jako celek nebo jeho část, které mohou být provozovány pomocí cloud computingu a které je orgán veřejné moci povinen zařadit do bezpečnostní úrovně,

b) částí informačního nebo komunikačního systému taková část tohoto systému, která je jednoznačně oddělitelná, zabezpečuje cílevědomou a systematickou informační činnost[1]), může být provozována pomocí cloud computingu a je definována z hlediska funkčních kategorií, architektury, provozního modelu a bezpečnosti,

c) oblastí dopadu vymezená oblast, v rámci které může mít dopad kybernetického bezpečnostního incidentu na poptávaný cloud computing vliv na bezpečnost a zdraví lidí, ochranu osobních údajů, trestněprávní řízení, veřejný pořádek, mezinárodní vztahy, řízení a provoz, důvěryhodnost, finanční model nebo zajišťování služeb,

d) úrovní dopadu nízká, střední, vysoká nebo kritická hodnota, která odpovídá dopadu kybernetického bezpečnostního incidentu na poptávaný cloud computing v každé oblasti dopadu.

§ 3

Bezpečnostní úrovně

Bezpečnostní úroveň pro využívání cloud computingu orgány veřejné moci vyjadřuje možné dopady kybernetického bezpečnostního incidentu na poptávaný cloud computing. Bezpečnostní úrovně jsou nízká, střední, vysoká nebo kritická.

§ 4

Zařazení poptávaného cloud computingu do bezpečnostní úrovně

(1) Zařazení poptávaného cloud computingu do bezpečnostní úrovně provede orgán veřejné moci podle přílohy k této vyhlášce. Orgán veřejné moci zhodnotí naplnění úrovně dopadu, které je poptávaný cloud computing schopen dosáhnout v rámci každé oblasti dopadu. Úroveň dopadu je v rámci každé oblasti dopadu dána nejhorším možným dopadem kybernetického bezpečnostního incidentu.

(2) Při zjišťování nejhoršího možného dopadu kybernetického bezpečnostního incidentu zohlední orgán veřejné moci možné narušení důvěrnosti, integrity a dostupnosti poptávaného cloud computingu a povahu informačního nebo komunikačního systému, který je poptávaným cloud computingem, jako celku. V případě, že je poptávaným cloud computingem pouze určitá část informačního nebo komunikačního systému, zohlední také vztah této části k bezpečnostní úrovni informačního nebo komunikačního systému jako celku.

(3) Bezpečnostní úroveň pro využívání poptá-

[1]) § 2 písm. a) zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.

vaného cloud computingu orgánem veřejné moci je shodná s nejvyšší úrovní dopadu, které poptávaný cloud computing dosáhne při hodnocení jednotlivých oblastí dopadu.

(4) Informační nebo komunikační systém, který je významným informačním systémem podle zákona, odpovídá vysoké bezpečnostní úrovni, pokud je poptávaným cloud computingem tento informační nebo komunikační systém jako celek, a pokud nebude orgánem veřejné moci postupem podle předchozích odstavců zařazen do kritické bezpečnostní úrovně.

(5) Informační nebo komunikační systém, který je kritickou informační infrastrukturou podle zákona, odpovídá kritické bezpečnostní úrovni, pokud je poptávaným cloud computingem tento informační nebo komunikační systém jako celek.

(6) Nejvyšší stanovená bezpečnostní úroveň informačního nebo komunikačního systému jako celku musí být stanovena alespoň pro jednu část informačního nebo komunikačního systému, který je poptávaným cloud computingem.

(7) O procesu stanovení bezpečnostní úrovně poptávaného cloud computingu podle předchozích odstavců provede orgán veřejné moci písemný záznam. Vzor písemného záznamu zveřejní Národní úřad pro kybernetickou a informační bezpečnost na svých internetových stránkách.

§ 5

Účinnost

Tato vyhláška nabývá účinnosti dnem následujícím po dni jejího vyhlášení.

Ředitel:

Ing. **Řehka** v. r.

Úrovně a oblasti dopadu pro zařazení poptávaného cloud computingu do bezpečnostní úrovně

Úroveň dopadu	Oblast dopadu								
	A. Bezpečnost a zdraví lidí	B. Ochrana osobních údajů	C. Trestněprávní řízení	D. Veřejný pořádek	E. Mezinárodní vztahy	F. Řízení a provoz	G. Důvěryhodnost	H. Finanční model	I. Zajišťování služeb
1. Nízká	Nemůže vést ke zranění jednotlivce ani skupiny lidí.	Nemůže ovlivnit poptávaný cloud computing, nebo může negativně ovlivnit poptávaný cloud computing, který naplňuje nejvýše dvě kritéria z první skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů.	Nemůže vytvořit podmínky pro páchání trestných činů přisvojení pravomoci úřadu, zneužití pravomoci úřední osoby nebo padělání a pozměnění veřejné listiny ani nemůže ztížit jejich vyšetřování.	Nemůže zapříčinit hromadné nepokoje nebo jinak narušit veřejný pořádek.	Nemůže negativně ovlivnit obraz České republiky v zahraničí.	Nemůže narušit řádné fungování nebo řízení ani části orgánu veřejné moci, nebo může narušit řádné fungování části nebo celého orgánu veřejné moci, avšak nemůže závažně omezit nebo zastavit provádění důležitých činností orgánu veřejné moci.	Nemůže negativně ovlivnit vztahy s jinými částmi orgánu veřejné moci, jinými organizacemi nebo vztahy s veřejností, nebo může vztahy s nimi negativně ovlivnit, avšak negativní následky mohou být nejvýše lokální.	Nemůže ani nepřímo vést k finančním ztrátám, nebo může vést k finančním ztrátám menším než 1 % běžných výdajů ročního rozpočtu orgánu veřejné moci.	Nemůže způsobit omezení, narušení nebo nedostupnost žádných poskytovaných služeb, nebo může způsobit omezení, narušení nebo nedostupnost poskytovaných služeb pro 5 000 a méně osob.
2. Střední	Může vést ke zranění jednotlivce nebo skupiny nejvíce 100 lidí.	Může negativně ovlivnit poptávaný cloud computing, který naplňuje tři a více kritérií z první skupiny kritérií nebo jedno kritérium z druhé skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů.	Může vytvořit podmínky pro páchání trestných činů přisvojení pravomoci úřadu, zneužití pravomoci úřední osoby nebo padělání a pozměnění veřejné listiny nebo může ztížit jejich vyšetřování.	Může zapříčinit hromadné nepokoje nebo jinak narušit veřejný pořádek s lokálními dopady.	Může negativně ovlivnit obraz České republiky v sousedních státech.	Může narušit řádné fungování části nebo celého orgánu veřejné moci, přičemž může závažně omezit nebo zastavit provádění důležitých činností orgánu veřejné moci.	Může negativně ovlivnit vztahy s jinými částmi orgánu veřejné moci, jinými organizacemi nebo vztahy s veřejností, avšak negativní následky mohou být nejvýše regionální.	Může vést k finančním ztrátám ve výši mezi 1 % a 5 % běžných výdajů ročního rozpočtu orgánu veřejné moci a tyto ztráty odpovídají částce 100 000 Kč a vyšší. V případě, že výše finanční ztráty odpovídá částce nižší než 100 000 Kč, použije se úroveň dopadu nízká.	Může způsobit omezení, narušení nebo nedostupnost služeb pro více než 5 000, nejvíce však 50 000 osob.

3. Vysoká	Může vést ke zranění skupiny více než 100 lidí a nejvíce 2 500 lidí nebo přímému ohrožení nebo ztrátě života jednotlivce nebo skupiny nejvíce 250 lidí.	Může negativně ovlivnit poptávaný cloud computing, který naplňuje dvě a více kritérií z druhé skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů.	Může vést k narušení vyšetřování trestné činnosti nebo soudního řízení v rámci orgánů činných v trestním řízení.	Může zapříčinit hromadné nepokoje nebo jinak závažně narušit veřejný pořádek s regionálními dopady.	Může negativně ovlivnit obraz České republiky ve světě.	Může narušit řádné fungování části nebo celého orgánu veřejné moci, přičemž může závažně omezit nebo zastavit provádění důležitých činností orgánu veřejné moci a narušit řízení, poškodit rozvoj nebo poškodit prosazování cílů a zájmů orgánu veřejné moci.	Může negativně ovlivnit vztahy s jinými částmi orgánu veřejné moci, jinými organizacemi nebo vztahy s veřejností, avšak negativní následky mohou být nejvýše celostátní nebo krátkodobě mezinárodní.	Může vést k finančním ztrátám ve výši přesahující 5 % a maximálně 10 % běžných výdajů ročního rozpočtu orgánu veřejné moci a tyto ztráty odpovídají částce 1 000 000 Kč a vyšší, nebo může způsobit hospodářské ztráty státu ve výši mezi 0,1 % a 0,5 % hrubého domácího produktu. V případě, že výše finanční ztráty odpovídá částce nižší než 1 000 000 Kč, použije se úroveň dopadu střední.	Může způsobit omezení, narušení nebo nedostupnost služeb pro více než 50 000 osob.
4. Kritická	Může vést ke zranění skupiny více než 2 500 lidí nebo přímému ohrožení nebo ztrátě života skupiny více než 250 lidí.	Může vést k omezení nebo narušení zpracování osobních údajů, které je nezbytné pro zajišťování obranných a bezpečnostních zájmů České republiky.	Může vést k závažnému a dlouhodobému narušení schopnosti vyšetřovat trestnou činnost nebo zpochybnění soudního řízení v rámci orgánů činných v trestním řízení.	Může být dotčen prvek kritické infrastruktury provozovaný orgánem veřejné moci, který poptávaný cloud computing zařazuje do bezpečnostní úrovně, a může zapříčinit hromadné nepokoje nebo jinak závažně narušit veřejný pořádek s celostátními dopady.	Může negativně ovlivnit nebo poškodit diplomatické vztahy České republiky.	Může být dotčen prvek kritické infrastruktury provozovaný orgánem veřejné moci, který poptávaný cloud computing zařazuje do bezpečnostní úrovně, a může narušit řádné fungování části nebo celého orgánu veřejné moci, přičemž může závažně omezit nebo zastavit provádění důležitých činností orgánu veřejné moci a narušit řízení, poškodit rozvoj nebo poškodit prosazování cílů a zájmů orgánu veřejné moci.	Může být dotčen prvek kritické infrastruktury provozovaný orgánem veřejné moci, který poptávaný cloud computing zařazuje do bezpečnostní úrovně, a může negativně ovlivnit vztahy s jinými částmi orgánu veřejné moci, jinými organizacemi nebo vztahy s veřejností a negativní následky mohou být dlouhodobě mezinárodní.	Může vést k finančním ztrátám přesahujícím 10 % běžných výdajů ročního rozpočtu orgánu veřejné moci a tyto ztráty odpovídají částce 10 000 000 Kč a vyšší, nebo může způsobit hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu. V případě, že výše finanční ztráty odpovídá částce nižší než 10 000 000 Kč, použije se úroveň dopadu vysoká.	Může být dotčen prvek kritické infrastruktury provozovaný orgánem veřejné moci, který poptávaný cloud computing zařazuje do bezpečnostní úrovně, a může dojít k rozsáhlému omezení poskytování nezbytných služeb nebo jinému závažnému zásahu do každodenního života postihujícího více než 125 000 osob.

Skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů

(1) První skupinu kritérií tvoří tato kritéria:

a) zpracovávají se osobní údaje umožňující bez dalšího vystupovat nebo jednat jménem subjektu údajů v souvislostech znamenajících poškození cti, pověsti nebo charakteru nebo umožňující na účet subjektu údajů odebírat služby, zboží, popřípadě vybírat peníze nebo jiné majetkové hodnoty,

b) zpracovávají se osobní údaje, podle kterých je subjekt údajů zařaditelný jako člen skupiny s časově omezenou nebo situačně danou zranitelností,

c) dochází ke zpracování osobních údajů, kterým je dotčeno nebo lze důvodně předpokládat, že bude dotčeno 5 000 až 10 000 subjektů údajů,

d) osobní údaje jsou veřejně přístupné neomezenému počtu orgánů nebo osob a

e) jedná se o zpracování osobních údajů systémem s propojením na jiná zpracování prováděná stejným správcem osobních údajů nebo se jedná o osobní údaje získané od jiných správců osobních údajů.

(2) Druhou skupinu kritérií tvoří tato kritéria:

a) zpracovávají se zvláštní kategorie osobních údajů nebo údaje vysoce osobní povahy, zejména finanční údaje o stavu majetku, výši finančních prostředků, dluzích nebo půjčkách nebo platební morálce, záznamy o historii soukromých volání subjektů údajů, údaje z elektronické pošty subjektů údajů a podobně,

b) dochází ke zpracování osobních údajů, kterým je dotčeno nebo lze důvodně předpokládat, že bude dotčeno více než 10 000 subjektů údajů a

c) dochází k automatizovanému rozhodování, které se dotýká subjektu údajů.