ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2018

Vyhlásené: 14. 6. 2018 Vyhlásená verzia v Zbierke zákonov Slovenskej republiky

Obsah dokumentu je právne záväzný.

166

VYHLÁŠKA
Národného bezpečnostného úradu

z 1. júna 2018

o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov

Národný bezpečnostný úrad podľa § 32 ods. 1 písm. a) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) ustanovuje:

§ 1

Táto vyhláška ustanovuje podrobnosti technického, technologického a personálneho vybavenia jednotky pre riešenie kybernetických bezpečnostných incidentov (ďalej len „jednotka CSIRT“), ktorých náležitosti a spôsob splnenia sa preukazujú na účely akreditácie jednotky CSIRT podľa § 13 zákona.

§ 2

(1) Požadované vybavenie jednotky CSIRT podľa § 14 písm. a) zákona sa preukazuje splnením

a) technických podmienok, ktoré zahŕňajú technicko-organizačné podmienky a technicko-procesné podmienky,

b) personálnych podmienok a

c) technologických podmienok.

(2) Splnenie podmienok podľa odseku 1 sa preukazuje dokumentom tak, že k takému dokumentu má prístup a je s ním preukázateľne oboznámený každý pracovník jednotky CSIRT, ktorý plní úlohy tejto jednotky CSIRT, a to vo forme záväzného interného predpisu vydaného orgánom verejnej moci podľa § 4 písm. b) zákona.

(3) Dokument podľa odseku 2 je súčasťou dokumentácie preukazujúcej splnenie podmienok akreditácie jednotky CSIRT podľa § 14 zákona.

§ 3

(1) Technické podmienky, ktoré zahŕňajú technicko-organizačné podmienky, zahŕňajú

a) určenie mandátu jednotky CSIRT,

b) definovanie subjektov v rámci sektora a podsektora podľa prílohy č. 1 zákona, ktoré využívajú služby jednotky CSIRT alebo sú na ňu napojené (ďalej len „zákazník“),

c) definovanie právomocí jednotky CSIRT,

d) definovanie úloh jednotky CSIRT,

e) definovanie služieb poskytovaných jednotkou CSIRT,

f) definovanie reakčného času služieb poskytovaných jednotkou CSIRT,

g) klasifikáciu kybernetických bezpečnostných incidentov riešených jednotkou CSIRT,

h) definovanie organizačnej štruktúry jednotky CSIRT,

i) definovanie bezpečnostnej politiky jednotky CSIRT.

(2) Technicko-organizačná podmienka podľa odseku 1 písm. a) určuje zriadenie a prevádzkovanie jednotky CSIRT v zmysle § 9 ods. 2 zákona.

(3) Technicko-organizačná podmienka podľa odseku 1 písm. b) znamená, že jednotka CSIRT má jasne zadefinovanú zákaznícku štruktúru, ktorej poskytuje svoje služby.

(4) Technicko-organizačná podmienka podľa odseku 1 písm. c) znamená, že jednotka CSIRT má zadefinované práva, ktoré je oprávnená vo vzťahu ku svojej zákazníckej štruktúre vykonávať.

(5) Technicko-organizačná podmienka podľa odseku 1 písm. d) znamená, že jednotka CSIRT plní úlohy v súlade s § 15 zákona.

(6) Technicko-organizačná podmienka podľa odseku 1 písm. e) znamená, že jednotka CSIRT má vymedzené služby podľa § 15 ods. 2 a 3 zákona, ktoré poskytuje svojej zákazníckej štruktúre.

(7) Technicko-organizačná podmienka podľa odseku 1 písm. f) znamená, že jednotka CSIRT má určený čas odozvy na prijaté informácie ako dobu prijatia kyberneticky relevantnej informácie (o incidente, hrozbe alebo zraniteľnosti) počas začatia prvých úkonov zo strany jednotky CSIRT. Pri reakcii na kybernetický bezpečnostný incident je maximálny reakčný čas dva pracovné dni od prijatia kyberneticky relevantnej informácie.

(8) Technicko-organizačná podmienka podľa odseku 1 písm. g) znamená, že jednotka CSIRT má vytvorenú schému pre klasifikáciu a triedenie kybernetických bezpečnostných incidentov do jednotlivých kategórií podľa osobitného predpisu.[1])

(9) Technicko-organizačná podmienka podľa odseku 1 písm. h) znamená, že jednotka CSIRT má určenú organizačnú štruktúru s vymedzením jednotlivých pracovísk a rolí a má vymedzený vzťah a postavenie jednotky CSIRT v rámci ústredného orgánu alebo vo vzťahu k ústrednému orgánu, ktorý má plniť úlohy jednotky CSIRT.

(10) Technicko-organizačná podmienka podľa odseku 1 písm. i) znamená, že jednotka CSIRT má vytvorenú bezpečnostnú politiku, ktorá je založená na všeobecne záväzných právnych predpisoch Slovenskej republiky a na medzinárodných bezpečnostných štandardoch. Bezpečnostnou politikou sa rozumie súhrn bezpečnostných požiadaviek na riešenie bezpečnosti na všetkých dotknutých úrovniach organizácie jednotky CSIRT.

§ 4

(1) Technické podmienky, ktoré zahŕňajú technicko-procesné podmienky, sú definovanie

a) eskalačných procesov na úroveň manažmentu,

b) eskalačných procesov na úrovni mediálnej komunikácie,

c) procesu prevencie kybernetických bezpečnostných incidentov,

d) procesu detekcie kybernetických bezpečnostných incidentov,

e) procesu riešenia kybernetických bezpečnostných incidentov,

f) procesu riešenia incidentov, ktoré nie sú kybernetickým bezpečnostným incidentom podľa § 3 písm. j) zákona, ale svojou povahou môžu narušiť bezpečnosť siete alebo informačného systému,

g) procesu auditu a kontroly jednotky CSIRT,

h) procesu dostupnosti poskytovania služieb v stave núdze,

i) procesu manipulácie s e-mailovými kontami a webovými stránkami,

j) procesu bezpečnej manipulácie s informáciami,

k) procesu získavania a manipulácie s informačnými zdrojmi,

l) procesu aktívnej pomoci zákazníckej štruktúre,

m) procesu komunikácie s ústredným orgánom, ktorý plní úlohy jednotky CSIRT,

n) procesu vytvárania a zdieľania štatistík,

o) procesu interných stretnutí jednotky CSIRT,

p) procesu spolupráce s partnerskými organizáciami.

(2) Technicko-procesná podmienka podľa odseku 1 písm. a) znamená, že jednotka CSIRT má vymedzené eskalačné procesy na úroveň manažmentu jednotky CSIRT, na úroveň manažmentu ústredného orgánu, ktorý má plniť úlohy jednotky CSIRT a na úroveň národnej jednotky CSIRT.

(3) Technicko-procesná podmienka podľa odseku 1 písm. b) znamená, že jednotka CSIRT má vymedzené eskalačné procesy pre potreby mediálnej komunikácie o informáciách získaných v rámci činnosti jednotky CSIRT.

(4) Technicko-procesná podmienka podľa odseku 1 písm. c) znamená, že jednotka CSIRT má vymedzené postupy, akým spôsobom v rámci svojej zákazníckej štruktúry predchádza vzniku kybernetických bezpečnostných incidentov, a to najmä budovaním bezpečnostného povedomia.

(5) Technicko-procesná podmienka podľa odseku 1 písm. d) znamená, že jednotka CSIRT má vymedzené postupy, akým spôsobom v rámci svojej zákazníckej štruktúry detekuje a vyhodnocuje kybernetické bezpečnostné incidenty.

(6) Technicko-procesná podmienka podľa odseku 1 písm. e) znamená, že jednotka CSIRT má vymedzené postupy, akým spôsobom v rámci svojej zákazníckej štruktúry reaguje na kybernetické bezpečnostné incidenty a rieši kybernetické bezpečnostné incidenty.

(7) Technicko-procesná podmienka podľa odseku 1 písm. f) znamená, že jednotka CSIRT má vymedzený postup, akým spôsobom v rámci svojej zákazníckej štruktúry reaguje na kybernetické bezpečnostné incidenty a rieši kybernetické bezpečnostné incidenty, ktoré nemožno vyriešiť štandardným postupom.

(8) Technicko-procesná podmienka podľa odseku 1 písm. g) znamená, že jednotka CSIRT má vymedzený postup, akým sa nastavujú kontrolné mechanizmy v rámci jednotky CSIRT a akým spôsobom a ako často sa vykonávajú kontroly.

(9) Technicko-procesná podmienka podľa odseku 1 písm. h) znamená, že jednotka CSIRT má definovaný postup, akým reaguje na kybernetické bezpečnostné incidenty alebo kyberneticky relevantné informácie v stave núdze, a to aj v čase mimo pracovnej doby.

(10) Technicko-procesná podmienka podľa odseku 1 písm. i) znamená, že jednotka CSIRT má definovaný postup, akým sú vytvárané e-mailové kontá, akým spôsobom je s nimi manipulované a kto má k týmto e-mailovým kontám prístup, aké informácie sú dostupné na webových stránkach jednotky CSIRT, akým spôsobom je webová stránka menená a aktualizovaná.

(11) Technicko-procesná podmienka podľa odseku 1 písm. j) znamená, že jednotka CSIRT má definované postupy na klasifikáciu, ochranu, uchovávanie a likvidáciu informácií a riadenie prístupu k nim.

(12) Technicko-procesná podmienka podľa odseku 1 písm. k) znamená, že jednotka CSIRT má definovaný postup, akým získava a verifikuje informačné zdroje.

(13) Technicko-procesná podmienka podľa odseku 1 písm. l) znamená, že jednotka CSIRT má definovaný postup komunikácie so svojou zákazníckou štruktúrou a zdieľa s ňou informácie.

(14) Technicko-procesná podmienka podľa odseku 1 písm. m) znamená, že jednotka CSIRT má definovaný postup komunikácie s ústredným orgánom a akým spôsobom mu odovzdáva informácie o svojej činnosti.

(15) Technicko-procesná podmienka podľa odseku 1 písm. n) znamená, že jednotka CSIRT má vymedzený postup, akým vytvára a s kým zdieľa štatistiky, ktoré vznikajú z jej činnosti.

(16) Technicko-procesná podmienka podľa odseku 1 písm. o) znamená, že jednotka CSIRT má vymedzený postup, ako často a na akej úrovni organizuje porady zamestnancov jednotky CSIRT.

(17) Technicko-procesná podmienka podľa odseku 1 písm. p) znamená, že jednotka CSIRT má vymedzený postup, ako často a na akej úrovni komunikuje a zdieľa informácie so svojimi partnerskými organizáciami a inými jednotkami CSIRT.

§ 5

(1) Personálne podmienky zahŕňajú

a) kódex správania sa a kódex praktického výkonu činností v jednotke CSIRT,

b) dostupnosť pracovníkov jednotky CSIRT,

c) kvalifikačné predpoklady pre pracovníkov jednotky CSIRT,

d) pravidlá interných školení pre pracovníkov jednotky CSIRT,

e) pravidlá externých technických školení pre pracovníkov jednotky CSIRT,

f) pravidlá externých komunikačných školení pre pracovníkov jednotky CSIRT,

g) pravidlá externých stretnutí pracovníkov jednotky CSIRT.

(2) Personálna podmienka podľa odseku 1 písm. a) znamená, že pre jednotku CSIRT je vydaný kódex správania sa a kódex praktického výkonu činností v jednotke CSIRT alebo iný porovnateľný dokument, ktorý obsahuje zásady práce a správania sa.

(3) Personálna podmienka podľa odseku 1 písm. b) znamená, že jednotka CSIRT disponuje minimálnym počtom aspoň troch pracovníkov, ktorí zabezpečujú plnenie úloh jednotky CSIRT.

(4) Personálna podmienka podľa odseku 1 písm. c) znamená, že jednotka CSIRT má vytvorený rámec kvalifikačných predpokladov na pracovníkov, ktorí plnia úlohy jednotky CSIRT, a ktorý zahŕňa

a) preukázanie znalosti anglického jazyka jazykovým certifikátom aspoň na úrovni B1 Spoločného európskeho referenčného rámca pre cudzie jazyky minimálne jedným pracovníkom jednotky CSIRT a

b) preukázanie vzdelania v oblasti informačných technológií aspoň dvoma pracovníkmi jednotky CSIRT v rozsahu podľa osobitného predpisu.

(5) Personálna podmienka podľa odseku 1 písm. d) znamená, že jednotka CSIRT má vytvorený program interných školení pracovníkov s uvedením ich zamerania a pravidelnosti.

(6) Personálne podmienky podľa odseku 1 písm. e) a f) znamenajú, že jednotka CSIRT má vytvorený program pre externé technické a externé komunikačné školenia spolu s uvedením ich zamerania a pravidelnosti.

(7) Personálna podmienka podľa odseku 1 písm. g) znamená, že jednotka CSIRT má vymedzené možnosti účasti na externých stretnutiach jednotiek CSIRT v rámci existujúcich komunít a skupín jednotiek CSIRT.

§ 6

(1) Technologické podmienky zahŕňajú

a) spôsob zberu údajov o aktívnych zákazníkoch a zoznam aktív zákazníkov,

b) zoznam informačných zdrojov,

c) konsolidovaný e-mailový systém,

d) systém sledovania incidentov,

e) dostupnosť telefonických služieb,

f) dostupnosť e-mailových služieb,

g) dostupnosť prístupu do siete internet,

h) nástroje na prevenciu incidentov.

(2) Technologická podmienka podľa odseku 1 písm. a) znamená, že jednotka CSIRT má vymedzený spôsob a periodicitu zberu údajov o aktívach zákazníkov a evidenciu týchto aktív. Zber údajov a zoznam aktív slúži na adresné zasielanie upozornení a varovaní a efektívnejšie informovanie zákazníkov pri špecifických kyberneticky relevantných informáciách.

(3) Technologická podmienka podľa odseku 1 písm. b) znamená, že jednotka CSIRT má vytvorený a vedený zoznam informačných zdrojov, z ktorých čerpá kyberneticky relevantné informácie, ktoré môžu mať vplyv na kybernetickú bezpečnosť.

(4) Technologická podmienka podľa odseku 1 písm. c) znamená, že jednotka CSIRT disponuje zabezpečeným e-mailovým systémom, ktorý umožňuje pracovníkom jednotky CSIRT prístup ku všetkým e-mailovým kontám jednotky CSIRT, ktoré sú potrebné na plnenie úloh jednotky CSIRT.

(5) Technologická podmienka podľa odseku 1 písm. d) znamená, že jednotka CSIRT disponuje systémom, ktorý umožňuje v rámci riešenia kybernetických bezpečnostných incidentov zaznamenávať priebeh incidentu a jeho riešenia, vykonávať zmeny a udržiavať všetky potrebné informácie o tomto incidente.

(6) Technologická podmienka podľa odseku 1 písm. e) znamená, že jednotka CSIRT disponuje redundantným pripojením do telekomunikačnej siete, ktoré má zabezpečiť kontinuálnosť plnenia úloh jednotky CSIRT.

(7) Technologické podmienky podľa odseku 1 písm. f) a g) znamenajú, že jednotka CSIRT disponuje redundantným pripojením do siete internetu, ktoré má zabezpečiť kontinuálnosť plnenia úloh jednotky CSIRT.

(8) Technologická podmienka podľa odseku 1 písm. h) znamená, že jednotka CSIRT disponuje systémami, ktoré technologicky slúžia na predchádzanie kybernetických bezpečnostných

incidentov.

§ 7

(1) Technické, technologické a personálne vybavenie jednotky CSIRT nemožno preukazovať splnením iných alebo náhradných podmienok, ktoré nie sú v tejto vyhláške uvedené.

(2) Žiadosť o posúdenie zhody jednotky CSIRT s podmienkami akreditácie jednotky CSIRT podľa § 13 ods. 1 zákona obsahuje

a) označenie orgánu verejnej moci podľa § 4 písm. b) zákona,

b) meno a priezvisko osoby zodpovednej za správnosť žiadosti,

c) dokumentáciu alebo zmenu v dokumentácii,

d) dátum a podpis žiadateľa.

§ 8

Touto vyhláškou sa preberajú právne záväzné akty Európskej únie uvedené v prílohe.

§ 9

Táto vyhláška nadobúda účinnosť 15. júna 2018.

Jozef Magala v. r.

l) § 2 ods. 2 vyhlášky Národného bezpečnostného úradu č. 165/2018, ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov.

Príloha
k vyhláške č. 166/2018 Z. z.

ZOZNAM PREBERANÝCH PRÁVNE ZÁVÄZNÝCH AKTOV EURÓPSKEJ ÚNIE

Smernica 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 (Ú. v. EÚ L 194, 19. 7. 2016).

Vydavateľ Zbierky zákonov Slovenskej republiky, správca obsahu a prevádzkovateľ právneho a informačného portálu Slov-Lex dostupného na webovom sídle www.slov-lex.sk je
Ministerstvo spravodlivosti Slovenskej republiky, Župné námestie 13, 813 11 Bratislava,
tel.: 02 888 91 137, fax: 02/52442853, e-mail: helpdesk@slov-lex.sk.