3. 7. 2015

ID: 98102

Zákon o kybernetické bezpečnosti (č. 181/2014) - Komentář

eFocus

Zákon o kybernetické bezpečnosti upravuje práva a povinnosti osob, jakož i pravomoc a působnost orgánů veřejné moci, a to v oblasti kybernetické bezpečnosti. Jeho hlavním smyslem je ochrana funkčnosti kybernetického prostoru. S ohledem na vývoj moderních technologií a stále narůstající závislost společnosti na informačních systémech tak tento předpis představuje zcela zásadní úpravu.

Publikace předkládá systematickou a přehlednou prezentaci základního předpisu s prováděcími předpisy v souvislostech a na jednom místě. Tento způsob byl zvolen s ohledem na praktické užívání publikace při práci s předpisy s tím, že evropská směrnice, připojená v příloze, může napomoci k lepšímu porozumění úmyslu zákonodárce.

Zákon o kybernetické bezpečnosti (č. 181/2014) - Komentář
Martin Maisner, Barbora Vlachová
Vydalo nakladatelství Wolters Kluwer, 2015, 232 s.

Publikaci lze objednat >>> zde.

Z publikace vybíráme:

§ 8

Hlášení kybernetického bezpečnostního incidentu

(1) Orgány a osoby uvedené v § 3 písm. b) až e) jsou povinny hlásit kybernetické bezpečnostní incidenty v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury nebo významném informačním systému, a to bezodkladně po jejich detekci; tím není dotčena informační povinnost podle jiného právního předpisu[3)].
(2) Orgány a osoby uvedené v § 3 písm. b) hlásí kybernetické bezpečnostní incidenty provozovateli národního CERT.
(3) Orgány a osoby uvedené v § 3 písm. c) až e) hlásí kybernetické bezpečnostní incidenty Národnímu bezpečnostnímu úřadu (dále jen „Úřad“).
(4) Prováděcí právní předpis stanoví
a) typy a kategorie kybernetických bezpečnostních incidentů a
b) náležitosti a způsob hlášení kybernetického bezpečnostního incidentu.
[3)] Například § 98 odst. 4 a § 99 odst. 4 zákona č. 127/2005 Sb., ve znění pozdějších předpisů.

Z důvodové zprávy:

Navržené ustanovení zakládá vybraným orgánům a osobám povinnost hlásit kybernetické

bezpečnostní incidenty. Účelem tohoto ustanovení je umožnit NBÚ (respektive jeho součásti – vládnímu CERT) a národnímu CERT vykonávat jejich primární funkci, tj. koordinovat ochranu kritické informační infrastruktury, významných informačních systémů a významných sítí.

Vybrané orgány a osoby budou povinny hlásit kybernetické bezpečnostní incidenty, které se vyskytly v jejich významné síti, informačním nebo komunikačním systému kritické informační infrastruktury anebo ve významném informačním systému, bezodkladně po jejich zjištění, tj. po vyhodnocení kybernetické bezpečnostní události jako kybernetického bezpečnostního incidentu. Toto ustanovení je komplementární úpravou k existujícím informačním a ohlašovacím povinnostem, tj. splněním ohlašovací povinnostipodle toho ustanovení se orgány a osoby nezbavují informačních povinností založených jinými právními předpisy, např. zákonem o elektronických komunikacích.

Vzhledem k zásadní důležitosti informačních a komunikačních systémů zařazených do kritické informační infrastruktury a významných informačních systémů jsou jejich správci povinni hlásit výskyt kybernetických bezpečnostních incidentů NBÚ, respektive jím provozovanému vládnímu CERT. Kybernetické bezpečnostní incidenty ve významných sítích jsou vybrané orgány a osoby povinny hlásit národnímu CERT.

Účelem tohoto ustanovení je založit povinnost hlásit kybernetické bezpečnostní incidenty detekované na základě povinnosti založené v předchozím ustanovení. Tato ustanovení však nevylučují možnost hlášení kybernetických bezpečnostních událostí nebo možnost obracet se na národní CERT nebo NBÚ (respektive jeho součást – vládní CERT) s podněty anebo jinými oznámeními souvisejícími s kybernetickou bezpečností nemajícími charakter kybernetického bezpečnostního incidentu.

Vzhledem k tomu, že je třeba upravit technické podrobnosti k výkonu povinnosti hlásit kybernetické bezpečnostní incidenty, tj. zejména je třeba v návaznosti na technický vývoj a na aktuální poznatky z oboru informatiky průběžně defi novat konkrétní technické parametry typů a kategorií hlášených kybernetických bezpečnostních incidentů, jakož i stanovovat technické náležitosti a způsob jednotlivých hlášení, je v tomto ustanovení rovněž provedeno zákonné zmocnění NBÚ k vydání prováděcího předpisu.

K odst. 1

1. Zákon o kybernetické bezpečnosti určuje, které osoby a orgány stíhá povinnost hlásit kybernetické bezpečnostní incidenty. Kybernetické bezpečnostní incidenty je nutné hlásit bezodkladně po detekci kybernetické bezpečnostní události, která je vyhodnocena jako kybernetický bezpečnostní incident. Kybernetický bezpečnostní incident, který je detekován ve významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury nebo významném informačním systému, mají povinnost hlásit:
a) orgány nebo osoby zajišťující významnou síť,
b) správci informačního nebo komunikačního systému kritické informační infrastruktury,
c) správci významného informačního systému.

2. Splnění povinnosti hlásit zjištěné kybernetické bezpečnostní incidenty nezbavuje tyto osoby povinnosti plnit úkoly stanovené jinými právními předpisy. Zákon o kybernetické bezpečnosti konkrétně odkazuje na § 98 odst. 4 a § 99 odst. 4 zák. o elektronických komunikacích.

3. Ustanovení § 98 odst. 4 zák. o elektronických komunikacích stanoví podnikatelům zajišťujícím veřejnou komunikační síť nebo poskytujícím veřejně dostupnou službu elektronických komunikací povinnost informovat bezodkladně Národní bezpečnostní úřad o závažném narušení bezpečnosti a ztrátě integrity sítě či rozsahu a důvodech přerušení poskytování služby nebo odepření přístupu k ní. Dále musí úřad informovat o přijatých opatřeních a o předpokládaném termínu odstranění příčiny

tohoto narušení či přerušení. Narušení bezpečnosti a ztráta integrity sítě jakož i přerušení poskytování služby mohou být způsobeny zejména vlivem velkých provozních havárií nebo živelních pohrom.

4. V § 99 je upravena povinnost podnikatelů zajišťujících veřejnou komunikační síť nebo poskytujících veřejně dostupnou službu elektronických komunikací zajistit integritu sítě a inoperabilitu služby za krizového stavu.[19] Dle odstavce 4 je podnikatel za krizových ostavu povinen informovat Národní bezpečnostní úřad o ohrožení nebo narušení bezpečnosti a integrity své sítě a bezpečnosti služeb. Dále musí sdělit přijatá nebo zamýšlená opatření k nápravě a předpokládaný termín odstranění příčiny.
[19] VANÍČEK, Z. Zákon o elektronických komunikacích: komentář. 2. aktualiz. a dopl. vyd. Praha: Linde, 2014, s. 378 stavu povinen informovat Národní bezpečnostní úřad o ohrožení nebo narušení bezpečnosti a integrity své sítě a bezpečnosti služeb. Dále musí sdělit přijatá nebo zamýšlená opatření k nápravě a předpokládaný termín odstranění příčiny.

K odst. 2

5. Druhý odstavec ukládá orgánům a osobám, které zajišťují významné sítě, povinnost hlásit kybernetické bezpečnostní incidenty provozovateli národního CERT (k pojmu „národní CERT“ srov. komentář k § 17). Hlavním úkolem národního CERT je přijímání oznámení a sdílení údajů o kybernetické bezpečnosti na národní a mezinárodní úrovni. Provozovatelem národního CERT je právnická osoba, se kterou uzavírá Národní bezpečnostní úřad veřejnoprávní smlouvu.

6. Osoby zajišťující významné sítě budou většinou osoby soukromého práva. Povinnost hlásit kybernetické bezpečnostní incidenty národnímu CERT je v souladu se zákonným principem minimální zátěže směrem k osobám soukromého práva. Naproti tomu správci informačních a komunikačních systémů kritické informační infrasturktury jsou povinni hlásit kybernetické bezpečnostní incidenty NBÚ, respektive tzv. vládnímu CERT.

K odst. 3

7. Správci významných informačních systémů, informačních systémů kritické informační infrastruktury a komunikačních systémů kritické informační infrastruktury mají taktéž povinnost hlásit kybernetické bezpečnostní incidenty. Na rozdíl od osob a orgánů zajišťujících významné sítě, které hlásí kybernetické bezpečnostní incidenty národnímu CERT, správci těchto informačních a komunikačních systémů hlásí kybernetické bezpečnostní incidenty Národnímu bezpečnostnímu úřadu, respektive vládnímu CERT, který je jeho součástí (k pojmu „vládní CERT“ srov. komentář k § 20).

K odst. 4

8. Odstavec 4 obsahuje zmocnění k vydání prováděcího předpisu. Typy a kategorie kybernetických bezpečnostních incidentů, jakož i náležitosti a způsob hlášení kybernetického bezpečnostního incidentu stanovuje vyhláška č. 316/2014 Sb., kterou vydal Národní bezpečnostní úřad.

9. V § 30 a § 31 této vyhlášky jsou uvedeny typy a kategorie kybernetických bezpečnostních incidentů. Typy kybernetických bezpečnostních incidentů se rozlišují jednak podle příčin, kterými byly způsobeny, a jednak podle dopadů, které tyto incidenty způsobily.

10. Příčiny kybernetických bezpečnostních incidentů mohou být následující:
a) kybernetický útok nebo jiná událost vedoucí k průniku do informačního nebo komunikačního systému nebo k omezení dostupnosti služeb;

b) škodlivý kód;
c) překonání technických opatření;
d) porušení organizačních opatření;
e) projev trvale působící hrozby;
f) ostatní kybernetické útoky.

11. Mezi možné dopady kybernetických bezpečnostních incidentů patří:
a) narušení důvěrnosti aktiv – např. know-how, obchodního tajemství, osobních údajů;
b) narušení integrity aktiv – celistvost aktiv, jejichž narušení může vést k ohrožení zájmu osob;
c) narušení dostupnosti aktiv – pro ochranu dostupnosti jsou využívány především různé zálohovací systémy; d) kombinace a) až c).

12. Vedle typů kybernetických bezpečnostních incidentů se tyto dělí dle závažnosti do tří kategorií, a to na velmi závažný kybernetický incident, závažný kybernetický incident a méně závažný kybernetický incident. Povinnost zařadit kybernetické bezpečnostní incidenty do jedné z uvedených kategorií mají správci významných informačních systémů, správci informačních systémů kritické informační infrastruktury, jakož i správci komunikačních systémů kritické informační infrastruktury. Při kategorizaci je nutné zohlednit zejména důležitost dotčených aktiv, dopady na poskytované služby a dopady na služby poskytované jinými informačními systémy.

13. V § 32 vyhlášky č. 316/2014 Sb. je určen způsob hlášení kybernetických bezpečnostních incidentů pro správce informačních systémů kritické informační infrastruktury, komunikačních systémů kritické informační infrastruktury, jakož i správce významných informačních systémů. Pro orgány a osoby zajišťující významné sítě není forma hlášení kybernetických bezpečnostních incidentů národnímu CERT explicitně stanovena.

14. Správci informačních a komunikačních systémů kritické informační infrastruktury a významných informačních systémů mohou kybernetické bezpečnostní incidenty hlásit v listinné formě pouze tehdy, pokud nejde využít formu elektronickou. Elektronickou podobou se rozumí zaslání e-mailem, do datové schránky nebo pomocí určeného datového rozhraní.

15. Náležitosti hlášení jsou uvedeny v příloze č. 5 k vyhlášce č. 316/2014 Sb., kde nalezneme vzor formuláře. Vedle kontaktních údajů se zaměřuje především na detaily kybernetického bezpečnostního incidentu – popis incidentu, typ a kategorie incidentu, současný stav jeho zvládání, počet zasažených systémů nebo počet dotčených uživatelů, jakož i systémové detaily (host, IP, funkce hosta).

Související ustanovení:
§ 7 – vymezení kybernetické bezpečnostní události a kybernetického bezpečnostního incidentu, § 17 – národní CERT, § 20 – vládní CERT

Související předpisy:
§ 98, § 99 zák. o elektronických komunikacích, – § 30, § 31, § 31, příloha č. 1, příloha č. 5 vyhlášky č. 316/2014 Sb.

Další články:

- Recenze publikace: Chalupa, R. Zákon směnečný a šekový – komentář směnečné části. Zákon o mezinárodním právu soukromém – komentář směnečné části. Praha: Leges, 2021, 646 s.
- Recenzia
- Budoucnost je v technologiích i udržitelnosti
- Anotační recenze: Vyvlastnění a vyvlastňovací řízení
- Věznice jsou přeplněné a věznění příliš drahé. Knihou Tresty budoucnosti chce INFO.CZ otevřít diskuzi o změnách
- Recenze na knihu: Zdeňková, V., Seidlová, M., Čornejová, H.,Peterová H.: Jak správně vytvářet a využívat FKSP: Jak postupovat při poskytování příspěvku na stravování.
- Recenze na knihu: Zuzana Strnadová: Co by měl vědět příjemce dotace. 1.vyd. Praha: GRADA Publishing, a.s., 2019, ISBN: 978-80-247-3076-9
- Ondřej Chmela: Zrušení poplatku za podnět k ÚOHS lze považovat za správné
- Anotační recenze: Koudelka, Z., Průcha, P., Zwyrtek Hamplová, J.: Zákon o obcích (obecní zřízení) – Komentář. Praha: Leges, 2019, 480s
- Pražské finále osmého ročníku konferencí Soukromé právo
- Recenze: Jakub Tomšej a kolektiv – Zaměstnávání cizinců v České republice