PORTÁL NÚKIB

Informační povinnost podle § 19 zákona o kybernetické bezpečnosti

TLP:CLEAR

17. října 2025

Verze 1.0

Národní úřad pro kybernetickou a informační bezpečnost

Obsah

1 Co se dozvím v tomto dokumentu? ... 3
2 Manažerské shrnutí dokumentu ... 3
3 Úvod ... 4
4 Informování o kybernetickém bezpečnostním incidentu s významným dopadem ... 6
4.1 Rozbor jednotlivých pojmů ... 6
4.1.1 Řádné poskytování regulované služby ... 6
4.1.2 Vhodnost oznámení a negativní ovlivnění poskytování služby ... 6
4.1.3 Způsoby oznámení ... 7
4.1.4 Uživatel regulované služby ... 7
4.1.5 Kybernetický bezpečnostní incident s významný dopadem ... 8
5 Rozhodnutí o povinnosti nebo zákazu informovat uživatele ... 9
6 Informování o krocích vůči významné hrozbě ... 9
6.1 Rozbor jednotlivých pojmů ... 9
6.1.1 Významná hrozba ... 9
6.1.2 Bez zbytečného odkladu ... 10
7 Následek nesplnění povinností ... 11
8 Otázky a odpovědi ... 12
9 Podmínky využití informací ... 13

1 Co se dozvím v tomto dokumentu?

Dokument představuje informační povinnost poskytovatele regulované služby vůči uživatelům jeho služby vyplývající z ustanovení § 19 zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jako „**zákon o kybernetické bezpečnosti**“). Dále se zabývá oprávněním Národního úřadu pro kybernetickou a informační bezpečnost (dále jako „**Úřad**“) rozhodnout o uložení povinnosti nebo zákazu o kybernetickém incidentu s významným dopadem informovat.

Pokud máte jakékoliv další otázky, podívejte se na www.portal.nukib.gov.cz nebo nám napište na regulace@nukib.gov.cz.

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

2 Manažerské shrnutí dokumentu

- Poskytovatel regulované služby má povinnost uživatele své služby **o kybernetickém incidentu s významným dopadem**.
- **Úřad může správním rozhodnutím** uložit povinnost informovat o incidentu s významným dopadem, nebo toto informování zakázat.
- Poskytovatel regulované služby má povinnost informovat uživatele regulované služby, který může být ovlivněn **významnou hrozbou, o možných preventivních či nápravných krocích.**
- Informování musí proběhnout **bez zbytečného odkladu** a musí být srozumitelné, cílené, rychlé a efektivní (tzn. využití správných informačních kanálů např. e-mail, web, SMS). Při informování se zohledňuje jazyk a místo pobytu uživatelů služby.
- Nesplnění informační povinnosti uložené rozhodnutím Úřadu může být posouzeno jako **přestupek**.

3 Úvod

Poskytovatel regulované služby je povinen informovat uživatele jím poskytované regulované služby o kybernetickém incidentu s významným dopadem a o krocích, které mohou být učiněny proti významné kybernetické hrozbě. Shledá-li to poskytovatel regulované služby za vhodné, informuje uživatele své služby i o samotné významné hrozbě.

Úplné znění § 19 zákona o kybernetické bezpečnosti

(1) Pokud to poskytovatel regulované služby považuje z důvodu zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv za vhodné, oznámí bez zbytečného odkladu uživatelům regulované služby kybernetický bezpečnostní incident s významným dopadem, který by mohl negativně ovlivnit poskytování této služby. Úřad může poskytovateli regulované služby, který je dotčen kybernetickým bezpečnostním incidentem s významným dopadem, uložit povinnost nebo zákaz informovat uživatele regulované služby o tomto incidentu. V rozhodnutí o uložení povinnosti nebo zákazu informovat podle předchozí věty stanoví Úřad rozsah informační povinnosti nebo rozsah zákazu.

(2) Poskytovatel regulované služby je povinen bez zbytečného odkladu vhodným a srozumitelným způsobem informovat uživatele regulované služby, který může být ovlivněn významnou hrozbou, o takových krocích, které může uživatel učinit v reakci na tuto hrozbu, aby byl případný dopad její realizace na tohoto uživatele co nejmenší. V případě, že je to možné a vhodné, informuje poskytovatel regulované služby uživatele také o této významné hrozbě.

Poskytovatel regulované služby musí uživatele bez zbytečného odkladu a srozumitelně informovat o kybernetických incidentech s významným dopadem nebo o krocích proti významné hrozbě. Dopad může spočívat v narušení služby, finanční ztrátě nebo jiné (hmotné či nehmotné) újmě.

Významný dopad se u incidentu posuzuje podle § 15 zákona o kybernetické bezpečnosti:

- v režimu vyšších povinností rozhoduje o významnosti Úřad,
- v režimu nižších povinností hodnotí významnost sám poskytovatel regulované služby.

Významná hrozba je taková, u níž lze na základě jejích technických charakteristik předpokládat, že má potenciál závažně ovlivnit aktiva poskytovatele regulované služby nebo uživatele regulované služby natolik, že způsobí značnou újmu.

Úřad může rozhodnutím uložit povinnost informovat, případně naopak rozhodnout o zákazu informovat. Při rozhodování zohledňuje veřejný zájem, bezpečnostní i reputační rizika.

Tabulka: základní přehled ustanovení § 19 zákona o kybernetické bezpečnosti

§ 19	KDO INFORMUJE	O ČEM INFORMUJE	KOHO INFORMUJE	JE INFORMOVÁNÍ POVINNOST?	DOPLNĚNÍ
§ 19 odst. 1 věta první	Poskytovatel regulované služby	O **kybernetickém bezpečnostním incidentu** s významným dopadem, který může negativně ovlivnit poskytování služby	Uživatele regulované služby	Ano, pokud je to vhodné z důvodu zajištění služby a bezpečnosti aktiv	Bez zbytečného odkladu
§ 19 odst. 1 věta druhá	Poskytovatel regulované služby na základě rozhodnutí Úřadu	O **kybernetickém bezpečnostním incidentu** s významných dopadem; může být rozhodnuto o zákazu informovat o tomto incidentu	Uživatele regulované služby	Ano, na základě rozhodnutí Úřadu	Rozsah informační povinnosti nebo zákazu stanoví Úřad
§ 19 odst. 2	Poskytovatel regulované služby	O reakčních **krocích**, které lze učinit proti významné kybernetické **hrozbě.** O samotné významné **hrozbě**	Uživatele regulované služby, který může být hrozbou ovlivněn	Ano, musí informovat o krocích. Je-li to možné a vhodné, informuje o hrozbě samotné.	Bez zbytečného odkladu, vhodným a srozumitelným způsobem

4 Informování o kybernetickém bezpečnostním incidentu s významným dopadem

4.1 Rozbor jednotlivých pojmů

4.1.1 Řádné poskytování regulované služby

Řádné poskytování regulované služby podle zákona o kybernetické bezpečnosti znamená, že služba je poskytována bezpečně, spolehlivě a s připraveností reagovat na kybernetické bezpečnostní události a incidenty. Podle směrnice o opatřeních k zajištění vysoké společenské úrovně kybernetické bezpečnosti v Unii (dále jako „**směrnice NIS2**“) se za řádné poskytování považuje takové, které není negativně ovlivněno.

Obecně lze říci, že řádné poskytování regulované služby je takové, které je včasné, odpovídá smluvním i zákonným požadavkům, je bez vad a zajišťuje důvěrnost, dostupnost a integritu. Zajišťuje také kontinuální a bezpečný provoz.

Každý poskytovatel regulované služby je odpovědný za vlastní vymezení řádného poskytování s ohledem na specifika organizace a potřeby uživatelů.

4.1.2 Vhodnost oznámení a negativní ovlivnění poskytování služby

Posouzení, zda je vhodné informovat o incidentu s významným dopadem, **vždy závisí na konkrétní situaci, okolnostech a uvážení poskytovatele regulované služby**. Zákon nestanovuje přesná kritéria, kdy oznámení je či není vhodné. Vhodnost informování se posuzuje ve vztahu k zajištění řádného poskytování služby a kybernetické bezpečnosti aktiv. Informování je vhodné, např. z toho důvodu, bude-li uživateli informace přínosná (např. může si změnit hesla při úniku jeho dat) nebo pokud bylo zasaženo do jeho práv.

Při posuzování vhodnosti musí mít poskytovatel služby na paměti, že cílem informační povinnosti je zvýšení transparentnosti a možnosti reakce uživatele na incident. Zákon o kybernetické bezpečnosti neumožňuje neinformování uživatelů o incidentu čistě z důvodu obav o reputaci poskytovatele regulované služby. Prioritou je zajištění bezpečnosti na straně uživatelů, a tedy včasnost a transparentnost.

Negativní ovlivnění poskytování regulované služby se může projevit nejen výpadkem regulované služby, ale např. i dopadem na finanční prostředky nebo ekonomickou činnost, a jakoukoliv možnou újmou na straně uživatele v důsledku incidentu. Ke vzniku informační povinnosti postačí samotná **možnost** negativního ovlivnění poskytované služby, tedy **nemusí skutečně dojít k dopadu na uživatele.** Infomační povinnost vzniká už v okamžiku, kdy existuje důvodná obava, že incident s významným dopadem může negativně ovlivnit poskytování regulované služby.

Dojde-li k negativnímu ovlivnění řádného poskytování regulované služby, bude negativně ovlivněn i její uživatel (to obdobně platí i pro možnost negativního ovlivnění). Informační povinnost vznikne až v situaci, kdy bude informování vyhodnoceno poskytovatelem jako vhodné (viz výše).

Postup hodnocení probíhá ve čtyřech krocích:

1. určení, zda jde o kybernetický bezpečnostní incident,
2. posouzení jeho významnosti (v závislosti na režimu povinností),
3. vyhodnocení, zda incident může negativně poskytování regulované služby,
4. posouzení vhodnosti informovat.

Příklad negativního ovlivnění: Samotný únik přihlašovacích údajů uživatele představuje negativní ovlivnění poskytování regulované služby dopadající na uživatele této služby. Ke vzniku informační povinnosti nemusí vůbec dojít ke skutečnému zneužití uniklých údajů.

4.1.3 Způsoby oznámení

Při volbě **způsobu informování o incidentu s významným dopadem** musí poskytovatel regulované služby zohlednit zejména povahu incidentu, jeho dopad a počet dotčených uživatelů. Důležité je i to, že uživatelé nemusí být pouze v České republice, proto jazyk oznámení musí odpovídat jejich jazykové vybavenosti.

Cílem oznámení není jen formální splnění povinnosti, ale skutečné **poskytnutí užitečných informací**. Uživatel musí obsahu oznámení rozumět a být schopen vyhodnotit, jaké důsledky pro něj incident má.

Možné formy oznámení:

- e-mail,
- zveřejnění na webových stránkách poskytovatele,
- oznámení v mobilní aplikaci (push notifikace, in-app zprávy),
- SMS zpráva,
- příspěvek na sociálních sítích apod.

4.1.4 Uživatel regulované služby

Definice uživatele regulované služby není uvedena přímo v zákoně o kybernetické bezpečnosti, najdeme ji ve vyhláškách k bezpečnostním opatřením pro vyšší i nižší režim. Uživatelem regulované služby může být **kdokoliv**, tedy fyzická nebo právnická osoba či orgán veřejné moci, kdo využívá **aktiva regulované služby**.

Uživatelem regulované služby může být jak **interní zaměstnanec organizace**, včetně administrátorů podílejících se na správě aktiv, tak **externí zákazník využívající regulovanou službu**.

Při plnění informační povinnosti musí poskytovatel vždy vyhodnotit, **které uživatele incident s významným dopadem potenciálně negativně ovlivní**. V některých případech bude nutné informovat přímo koncové uživatele služby, jindy postačí informovat pouze vybrané uživatele v rámci organizace. Je na poskytovateli regulované služby, aby si okruh relevantních uživatelů určil.

Pokud o povinnosti informovat **rozhodne Úřad**, určí v rozhodnutí i rozsah této povinnosti.

4.1.5 Kybernetický bezpečnostní incident s významný dopadem

Poskytovatel regulované služby musí informovat uživatele o **kybernetických bezpečnostních incidentech s významným dopadem**. Bližší informace o samotných kybernetických incidentech a jejich hlášení jsou dostupné v podpůrném materiálu na Portálu NÚKIB.

Významný dopad incidentu

Podle § 15 odst. 3 zákona o kybernetické bezpečnosti má incident významný dopad, pokud **způsobil nebo může způsobit**:

- závažné narušení služeb,
- finanční ztrátu poskytovateli,
- značnou újmu jiným osobám.

Tato definice platí pro oba režimy povinností, způsob určení významnosti se mezi nimi liší.

Tabulka: určování významnosti kybernetického bezpečnostního incidentu

KDO?	JAK URČUJE VÝZNAMNOST
Poskytovatel regulované služby v režimu vyšších povinností	Významnost dopadu incidentu neposuzuje sám poskytovatel. Tuto vlastnost incidentu určí **Úřad**, a to rovněž bez zbytečného odkladu, nejpozději do 24 hodin od nahlášení incidentu.
Poskytovatel regulované služby v režimu nižších povinností	Významnost dopadu incidentu posuzuje **sám poskytovatel** na základě své metodiky. Incident je významný, přesáhne-li únosnou míru (§ 15 vyhlášky o BO pro nižší režim)
Poskytovatel služby v odvětví digitální infrastruktura a služby	Významnost dopadu incidentu posuzuje **sám poskytovatel** na základě prováděcí nařízení Komise (EU) 2024/2690.

5 Rozhodnutí o povinnosti nebo zákazu informovat uživatele

Za oznamování incidentů s významným dopadem odpovídají primárně poskytovatelé regulované služby. Úřad však může ve správním řízení rozhodnout, že poskytovateli **uloží povinnost** informovat uživatele o incidentu, nebo naopak **uloží zákaz** informovat.

V rozhodnutí Úřad vždy stanoví **rozsah informační povinnosti nebo zákazu**. Při rozhodování Úřad zvažuje bezpečnostní otázky, tedy zájem na informování o incidentech, nikoliv obchodní zájmy poskytovatelů.

6 Informování o krocích vůči významné hrozbě

Poskytovatel regulované služby musí bez zbytečného odkladu vhodným a srozumitelným způsobem informovat uživatele, který může být významnou hrozbou ovlivněn, **o krocích, které může učinit**, aby se minimalizoval její dopad. Pokud je to možné a vhodné, má poskytovatel informovat i o samotné hrozbě.

Informace musí být poskytovány zdarma, transparentně, srozumitelně a musí být snadno dostupné. Splnění této povinnosti vyžaduje maximální úsilí ze strany poskytovatele. Smyslem je předcházet tomu, aby se hrozby proměnily v incidenty. Proaktivní přístup je zásadní součástí řízení kybernetických rizik. Pokud je pravděpodobné, že se hrozba naplní, poskytovatel má uživatele informovat o opatřeních i o samotné hrozbě.

Tato povinnost nezbavuje poskytovatele odpovědnosti **přijmout na vlastní náklady přiměřená a okamžitá opatření** k odstranění hrozby a k obnovení bezpečné úrovně služby.

6.1 Rozbor jednotlivých pojmů

6.1.1 Významná hrozba

Definice hrozby a významné hrozby je obsažena v § 2 písm. c) a d) zákona o kybernetické bezpečnosti.

- **Hrozba** je jakákoliv potenciální okolnost, událost nebo jednání, které mohou způsobit kybernetickou událost či incident a poškodit, narušit nebo jinak nepříznivě ovlivnit aktiva, jejich uživatele nebo jiné osoby.
- **Významná hrozba** je taková, u níž lze podle jejích technických charakteristik předpokládat, že může závažně ovlivnit aktiva poskytovatele regulované služby nebo jeho uživatelů natolik, že způsobí značnou újmu (hmotnou či nehmotnou).

Podle recitálu 101 směrnice NIS2 se posouzení, zda jde o značnou újmu, vždy odvíjí od konkrétních okolností. Tento pojem nijak nesouvisí s terminologií trestního zákoníku, který „značnou škodu“ vymezuje finanční hranicí.

Posouzení významnosti hrozby je do značné míry subjektivní. Při hodnocení lze mimo jiné zohlednit:

- možné dopady: počet potencionálně zasažených uživatelů, povahu potencionálně dotyčných dat (citlivost, osobní údaje atd.), finanční dopady, geografické rozšíření dotčené regulované služby;
- závažnost hrozby: CVE rating konkrétní zranitelnosti se kterou hrozba souvisí,
- kontext a systémová rizika: ohrožení dalších regulovaných organizací využívajících dotčenou regulovanou službu (včetně kritické infrastruktury či státních orgánů).

Příklady hrozeb lze nalézt v příloze č. 4 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností. Může jít o zneužití identity, neoprávněná modifikace informací, škodlivý kód atp.

Konkrétní hrozbou může být existence **falešné webové stánky**, jejíž tvůrce se snaží napodobit vzhled webové stránky poskytovatele regulované služby. Podvržená stránka slouží k získání informací a finančních prostředků od uživatelů, kteří se domnívají, že nakupují službu u poskytovatele regulované služby. Informování o krocích proti významné hrozbě (doporučení nakupovat na ověřené webové stránce) nebo o hrozbě samotné (existence falešné webové stránky) je možné provést na oficiálních webových stránkách poskytovatele regulované služby, prostřednictvím e-mailu či SMS zprávami.

6.1.2 Bez zbytečného odkladu

Jednotná definice pojmu „bez zbytečného odkladu“ v právním řádu neexistuje. Jde o neurčitý právní pojem, který se vykládá podle kontextu konkrétní právní normy a okolností případu. Obecně znamená, že úkon musí být proveden **co nejdříve, jakmile to okolnosti dovolí, bez zbytečného prodlení**. Ve vztahu ke kybernetickým hrozbám a incidentům tak „bez zbytečného odkladu“ představuje **nejrychlejší možnou reakci** odpovídající závažnosti hrozby a reálným možnostem organizace.

V oblasti kybernetické bezpečnosti může tento pojem znamenat **okamžité jednání**, případně reakci v řádu hodin. Vodítkem je i lhůta pro prvotní ohlášení incidentu podle § 16 zákona o kybernetické bezpečnosti, která je limitována 24 hodinami.

Za informování bez zbytečného odkladu zpravidla nelze považovat situace, kdy se poskytovatel rozhodne informovat o incidentu či hrozbě až po nechtěném zveřejnění relevantních informací (např. na základě whistleblowingu či běžného únik informací do médií). To neplatí absolutně, může docházet k situacím, kdy bezprostřední informování o incidentu či hrozbě nebude vhodné, ale únik informací způsobí nutnost určité reakce ze strany poskytovatele regulované služby.

7 Následek nesplnění povinností

Zákon o kybernetické bezpečnosti nespojuje s nesplněním povinnosti informovat o významném incidentu s žádnou sankci. Je to proto, že poskytovatel regulované služby má informovat uživatele „pokud to považuje za vhodné“, což je do značné míry subjektivní. To ale neznamená, že by tato povinnost mohla být zcela ignorována, absence sankce není omluvou pro její neplnění. Řádné splnění veřejnoprávní povinnosti je důležité také z hlediska soukromoprávní odpovědnosti za případnou újmu způsobenou uživatelům služby.

Pokud Úřad poskytovateli rozhodnutím uloží povinnost informovat a ta není splněna, jde o přestupek. Sankce hrozí také v případě, že poskytovatel neinformuje o krocích proti významné hrozbě.

Výše pokut

- **Režim vyšších povinností**: pokuta až 250 mil. Kč, nebo až 2 % čistého ročního obratu podniku (podle toho, co je vyšší).
- **Režim nižších povinností**: pokuta až 175 mil. Kč, nebo až 1,4 % čistého ročního obratu podniku (podle toho, co je vyšší).

Výše uvedené částky představují **maximální hranice**. O skutečné výši rozhoduje Úřad ve správním řízení, kde zohledňuje polehčující a přitěžující okolnosti.

8 Otázky a odpovědi

Má poskytovatel regulované služby informační povinnost i v případě propojených nebo partnerských podniků?

Informační povinnost se vždy vztahuje na konkrétního poskytovatele regulované služby. Vazby na partnerské nebo propojené podniky jsou důležité jen pro posouzení významnosti dopadu incidentu, nikoli pro samotnou informační povinnost.

Pokud je regulovaným poskytovatelem i partnerský či propojený podnik, každý subjekt musí incident vyhodnotit samostatně a plní svou informační povinnost nezávisle na ostatních. Zákon nevylučuje, aby poskytovatelé regulované služby, kteří jsou v holdingu, koordinovali svá oznámení, vždy je však nutné správně identifikovat všechny ovlivněné uživatelé všech poskytovatelů.

Má informační povinnost podle zákona o kybernetické bezpečnosti i dodavatel poskytovatele regulované služby?

Ne, informační povinnost se vztahuje pouze na poskytovatele regulované služby, nikoli na jeho dodavatele. Proto je vhodné smluvně zajistit, aby dodavatel informoval poskytovatele o incidentech, které mají dopad na poskytovanou službu. Poskytovatel pak nese odpovědnost oznámit incident s významným dopadem uživatelům a informovat je také o krocích, které mohou učinit vůči významné hrozbě.

Jak se uplatňuje informační povinnost při přeshraničních dopadech a vůči uživatelům ve více členských státech EU?

Pokud je poskytovatel pod jurisdikcí České republiky, musí splnit informační povinnost vůči uživatelům své služby bez ohledu na to, kde se tito uživatelé nacházejí. Informace o významném incidentu nebo o krocích proti významné hrozbě musí být srozumitelné, jasné, přiměřené a poskytnuté v jazyce uživatelů (nebo v jazyce služby). Při významných incidentech spolupracují a sdílejí informace i národní týmy CSIRT v jednotlivých členských státech.

9 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
TLP:RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP:AMBER+STRICT	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
TLP:CLEAR	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
17. října 2025	1.0	OREG	Vytvoření dokumentu