PORTÁL NÚKIB

Hlášení kybernetických bezpečnostních incidentů

TLP:CLEAR

8. června 2026

Verze 1.2

Národní úřad
pro kybernetickou
a informační bezpečnost

Obsah

1 Co se dozvím v tomto dokumentu?

Co je kybernetickým bezpečnostním incidentem? Co je kybernetickou bezpečnostní událostí? Kdo má povinnost je hlásit? Jakým způsobem je hlásí? Hrozí za jejich opožděné ohlášení či neohlášení postih?

Odpovědi na tyto otázky nabízí následující materiál Národního úřadu pro kybernetickou a informační bezpečnost (dále jen jako „Úřad“). Čtenář tohoto materiálu se v následujících kapitolách dozví, jak postupovat při plnění povinností podle zákona, č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „ZKB“), a jeho vyhlášek.

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

2 Definice kybernetického bezpečnostního incidentu

Podle § 2 odst. 2 písm. f) ZKB je **kybernetickým bezpečnostním incidentem** „*narušení bezpečnosti informací v kybernetickém prostoru*“. Kybernetickým bezpečnostním incidentem je tak v zásadě každé neplánované narušení důvěrnosti, integrity nebo dostupnosti informací a dat[1] v souboru sítí elektronických komunikací a dalších technologií, ve kterém dochází ke zpracování informací a dat v elektronické podobě.[2]

Jak lépe rozumět pojmům důvěrnost, integrita a dostupnost?

Důvěrnost je porušena, pokud je informace zpřístupněna neoprávněným osobám: k informacím či datům se dostal někdo, kdo se k nim dostat neměl.

Integrita je porušena, pokud je informace neoprávněným zásahem pozměněna nebo smazána: informace či data vypadají jinak, než vypadat měly.

Dostupnost je porušena, pokud je informace nedostupná: informace či data nejsou k dispozici v době, kdy k dispozici být měly.

Definiční znak **neplánovanosti** se projeví tak, že za kybernetický bezpečnostní incident nelze považovat plánované (co do způsobu provedení a doby trvání) zásahy do informačních systémů (servisní okna, plánované výpadky či odstávky).

Specifickým znakem je **autenticita** informací a dat, kterou v rámci posuzování incidentu vnímáme jako součást obecnější integrity a důvěrnosti.

[1] Podle § 2 odst. 2 písm. b) ZKB se bezpečností informací rozumí „zajištění důvěrnosti, integrity a dostupnosti informací a dat“.
[2] Podle § 2 odst. 2 písm. a) ZKB se kybernetickým prostorem rozumí „soubor sítí elektronických komunikací a dalších technologií, ve kterém dochází ke zpracování informací a dat v elektronické podobě“.

3 Kdo kybernetické bezpečnostní incidenty hlásí

Povinnost hlásit kybernetické bezpečnostní incidenty ukládá § 15 ZKB pouze **poskytovatelům regulované služby**, další osoby mohou incidenty hlásit dobrovolně. Poskytovatelé regulované služby hlásí kybernetické bezpečnostní incidenty, které

1. se projevily ve stanoveném rozsahu (viz materiál Stanovení rozsahu řízení kybernetické bezpečnosti),[3]
2. mají původ v kybernetickém prostoru, a
3. nelze u nich bez zbytečného odkladu, nejpozději do 24 hodin, vyloučit úmyslné zavinění.

Není tedy dána povinnost hlásit provozní a operativní incidenty, u nichž lze vyloučit úmyslné zavinění.

Poskytovatelé regulované služby v režimu nižších povinností hlásí jen ty, které mají významný dopad na poskytování regulované služby. Významnost dopadu kybernetického bezpečnostního incidentu si poskytovatel regulované služby v režimu nižších povinností posuzuje sám podle kritérií uvedených v § 14 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.

Poskytovatelé regulované služby v režimu vyšších povinností hlásí všechny kybernetické bezpečnostní incidenty splňující výše uvedené znaky.

4 Způsob hlášení kybernetických bezpečnostních incidentů

Prvotní hlášení o kybernetickém bezpečnostním incidentu je poskytovatel regulované služby povinen provést **bez zbytečného odkladu, nejpozději do 24 hodin**. V praxi se tato lhůta počítá od okamžiku, kdy u konkrétního subjektu osoba k tomu pověřená (například manažer kybernetické bezpečnosti) vyhodnotí zjištěnou událost jako kybernetický bezpečnostní incident.

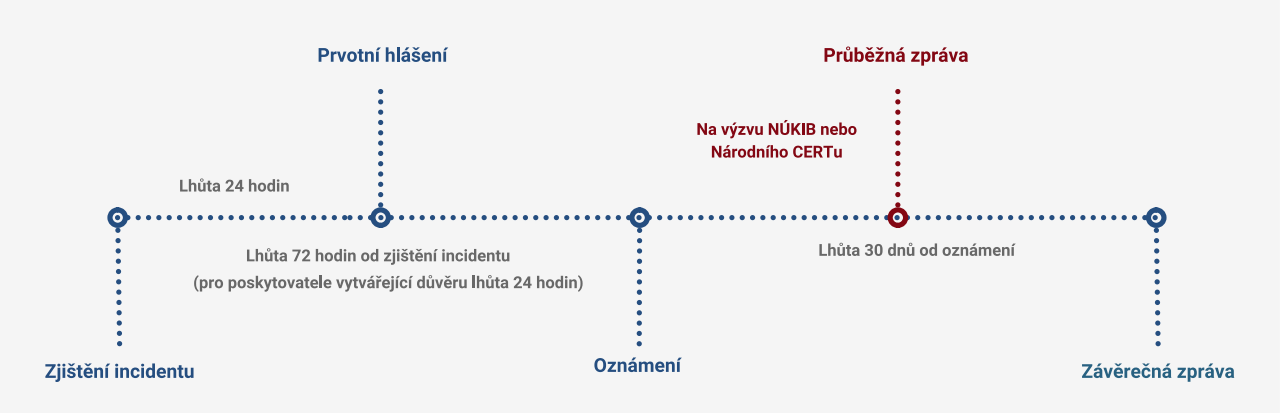
Je však potřeba mít na paměti, že kybernetický bezpečnostní incident má jasně danou definici a pověřená osoba nerozhoduje o tom, co sama za incident považuje (subjektivní pohled), ale o tom, zda je naplněna definice (objektivní skutečnost). Zároveň je potřeba, aby vyhodnocení zjištěné kybernetické bezpečnostní události proběhlo v rámci subjektu co nejrychleji. Pokud se má prvotní hlášení provést bez zbytečného odkladu, tím spíše to platí pro vyhodnocení případného incidentu.

K hlášení kybernetických bezpečnostních incidentů je určen **Portál NÚKIB**, který uživatelům umožňuje elektronickou komunikaci s Úřadem. Pokud není možné přistoupit k Portálu NÚKIB (např. to neumožní probíhající kybernetický bezpečnostní incident), lze ohlásit kybernetický bezpečnostní incident **e-mailem nebo datovou schránkou** podle § 16 odst. 4 ZKB.

[3] Stanoveným rozsahem se rozumí rozsah řízení kybernetické bezpečnosti, v podrobnostech viz § 12 ZKB.

5 Průběh hlášení kybernetických bezpečnostních incidentů

Hlášení incidentů může u **méně závažných** incidentů poskytovatelů regulované služby v režimu vyšších povinností končit již po **prvotním hlášení**, zatímco u incidentů s **významným dopadem** zahrnuje proces hlášení **několik kroků** a končí závěrečnou zprávou. Průběh celého hlášení znázorňuje tato časová osa:



Prvotní hlášení: NÚKIB poskytovateli regulované služby ve vyšším režimu po prvotním hlášení oznámí, zda má incident významný dopad. Pokud je incident **bez významného dopadu**, tímto krokem hlášení pro organizaci končí.

Oznámení incidentu: Podrobnější **posouzení incidentu**, dopad incidentu, indikátory kompromitace.

Průběžná zpráva: Průběžná zpráva o podstatných **změnách stavu** zvládání incidentu.

Závěrečná zpráva: Podrobný popis incidentu, jeho závažnosti a dopadu, druh hrozby, pravděpodobná příčina incidentu, učiněná a probíhající opatření ke zmírnění následků a případný přeshraniční dopad incidentu. Pokud incident stále trvá, předloží organizace po uplynutí lhůty průběžnou zprávu o aktuálním stavu zvládání incidentu, a po jeho vyřešení nejpozději **do 30 dnů závěrečnou zprávu o vyřešení incidentu**.

6 Hlášení kybernetických bezpečnostních incidentů vybraných poskytovatelů digitálních služeb

Ve vztahu k následujícím službám se uplatňují speciální pravidla týkající se hlášení incidentů:

- služba systému překladu doménových jmen,
- služba vytvářející důvěru[4],
- služba správy a provozu registru domény nejvyšší úrovně,

[4] Dle nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, v platném znění.

- služba cloud computingu,
- služba datového centra,
- služba sítě pro doručování obsahu,
- služba on-line tržiště,
- služba internetového vyhledávače,
- služba platformy sociální sítě,
- řízená služba,
- řízená bezpečnostní služba.

Poskytovatelé výše uvedených služeb v případě hlášení incidentů u těchto služeb postupují podle **prováděcího nařízení Komise (EU) 2024/2690** ze dne 17. října 2024, nezávisle na svém režimu povinností. Způsob hlášení incidentů zůstává stejný jako pro všechny ostatní subjekty (Portál NÚKIB, termíny), mění se pouze vymezení hlášených incidentů. Prováděcí nařízení stanovuje, který incident se považuje za významný a je ho potřeba hlásit. Obecná kritéria jsou v čl. 3 a 4 prováděcího nařízení a specifická kritéria pro jednotlivé služby pak v čl. 5–13 prováděcího nařízení.

V případě jiných, výše nevyjmenovaných, regulovaných služeb poskytovatel regulované služby hlásí kybernetické bezpečnostní incidenty běžným postupem podle § 15 a § 16 ZKB.

7 Neohlášení kybernetického bezpečnostního incidentu

Samotná skutečnost, že se povinné osobě kybernetický bezpečnostní incident stal, není přestupkem. Na druhé straně se za přestupek považuje, pokud povinná osoba ve stanovené lhůtě, či vůbec neohlásí kybernetický bezpečnostní incident, který ohlásit měla.

Obdobně lze za přestupek považovat situaci, kdy poskytovatel regulované služby v režimu vyšších povinností provede prvotní hlášení, Úřad tento incident vyhodnotí jako významný, načež poskytovatel přestane komunikovat a neprovede další úkony zmíněné v kapitole 5, případně odmítne poskytnout součinnost pro zvládání incidentu podle § 17 odst. 3 ZKB. Viz skutkové podstaty přestupků podle § 59 odst. 1 písm. h) či i), § 59 odst. 2 písm. h) a i).

Ohlášení kybernetického bezpečnostního incidentu bezprostředně nezakládá důvod pro provedení následné kontroly dotčené organizace. Úřad si totiž uvědomuje, že vznik incidentu se automaticky nerovná zanedbání povinnosti zavádět bezpečnostní opatření. Kybernetický bezpečnostní incident se může vyskytnout také u skvěle zabezpečené organizace, protože bezpečnost nikdy není stoprocentní.

8 Definice kybernetické bezpečnostní události

Podle § 2 odst. 2 písm. e) ZKB je **kybernetickou bezpečnostní událostí** „*událost, která může vyústit v kybernetický bezpečnostní incident*“. Jedná se tedy o událost s potenciálem přerůst v kybernetický bezpečnostní incident. **V případě jakékoliv nejistoty je vždy lepší domnělý incident nahlásit.**

Hlášení kybernetických bezpečnostních událostí je dobrovolné a stejně jako u kybernetického bezpečnostního incidentu jej lze provést prostřednictvím Portálu NÚKIB, v případě nemožnosti přistoupit k portálu také e-mailem či datovou schránkou (viz kapitola 4).

9 Co je kybernetickým bezpečnostním incidentem a co událostí

V této kapitole si ukážeme příklady kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů. U kybernetických bezpečnostních incidentů současně rozdělíme ty, které splňují definici kybernetického bezpečnostního incidentu, ovšem Úřadu se nehlásí, a kybernetické bezpečnostní incidenty, které splňují všechny znaky popsané v kapitole 3 tohoto podpůrného materiálu a musí být Úřadu nahlášeny.

***Situace 1**: E-mailový server organizace nezachytil phishingový e-mail, který tak doputoval až k samotnému uživateli, ten jej ale ihned nahlásil, nekliknul na žádný odkaz ani nikam nezadal žádná data.*

V této situaci se jedná o **kybernetickou bezpečnostní událost**. Nedošlo ke kliknutí na žádný škodlivý odkaz, nebyl stažen žádný potenciálně škodlivý soubor, nebyly zadány přihlašovací údaje na žádné útočníkovy stránky ani formuláře. Hovoříme pouze o výše uvedeném potenciálu vyústit v kybernetický bezpečnostní incident.

***Situace 2**: E-mailový server organizace nezachytil phishingový e-mail, který tak doputoval až k samotnému uživateli. Uživatel klikl na odkaz v e-mailu a na útočníkův formulář zadal přihlašovací údaje, které používá v souvislosti se svou pracovní agendou v organizaci.*

V této situaci se jedná o **kybernetický bezpečnostní incident, který je nutno hlásit**. V důsledku úmyslného jednání útočníka došlo přinejmenším k porušení důvěrnosti dat (vyzrazení přihlašovacích údajů útočníkovi).

***Situace 3:** Během stanoveného časového okna upgradu nastala nedostupnost technického aktiva, která však bylo v plánovaném rozsahu řízené změny.*

V této poslední situaci hovoříme o **kybernetickém bezpečnostním incidentu, který není nutno hlásit**. Přestože došlo k narušení dostupnosti informací či dat, v daném případě můžeme vyloučit úmysl, neboť se jednalo o schválenou a plánovanou změnu.

10 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**
20. října 2025	1.0	OREG	Vytvoření dokumentu
10. března 2026	1.1	OREG	Drobné doplnění kapitol 3 a 7
8. června 2026	1.2	OREG	Do výčtu v kapitole 6 doplněni poskytovatelé služeb vytvářejících důvěru