PORTÁL NÚKIB

Stanovení významnosti incidentu v režimu nižších povinností

TLP:CLEAR

24. února 2026

Verze 1.0

Národní úřad pro kybernetickou a informační bezpečnost

Obsah

1 Co se dozvím v tomto dokumentu?

Poskytovatelé regulované služby v režimu nižších povinností jsou povinni vyhodnotit významnost dopadu kybernetického bezpečnostního incidentu. Tento materiál slouží jako vodítko, jak k tomuto procesu přistoupit.

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

Tento dokument 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 K čemu slouží stanovení významnosti dopadu

Samotné stanovení významnosti dopadu je proces, který podmiňuje hlášení incidentů v režimu nižších povinností, kdy vyhodnocení provádí sám poskytovatel regulované služby. Oproti tomu v režimu vyšších povinností vyhodnocuje významnost dopadu kybernetického bezpečnostního incidentu Národní úřad pro kybernetickou a informační bezpečnost (“NÚKIB”), který výsledek tohoto vyhodnocení následně sdělí poskytovateli regulované služby.

2.1 Právní úprava hlášení incidentů

Poskytovatelé regulovaných služeb v režimu nižších povinností hlásí podle § 15 odst. 2 zákona č. 264/2025 Sb., o kybernetické bezpečnosti („ZKB“), pouze kybernetické bezpečnostní incidenty, které se projevily ve stanoveném rozsahu, mají původ v kybernetickém prostoru, mají **významný dopad na poskytování regulované služby** a nelze u nich vyloučit úmyslné zavinění.

Významný dopad na poskytování regulované služby má podle § 15 odst. 3 incident, který poskytovateli regulované služby způsobil nebo může způsobit závažné provozní narušení služeb nebo finanční ztráty nebo způsobil nebo může způsobit jiným osobám značnou újmu.

Samotné stanovení významnosti dopadu incidentu je upraveno v § 14 vyhlášky č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulovaných služeb v režimu nižších povinností („vyhláška“).

Podrobnější výklad naleznete v materiálu Hlášení kybernetických bezpečnostních incidentů.

3 Stanovení významnosti dopadu

V této kapitole jsou vysvětleny jednotlivé kroky stanovení významnosti dopadu v souladu s § 14 vyhlášky.

V první řadě je nutné stanovit **únosnou míru újmy** způsobenou incidentem. Únosná míra újmy je souhrn nejvyšší škody a nemajetkové újmy vzniklé v souvislosti s kybernetickým bezpečnostním incidentem:

- **nejvyšší škoda** = celková finanční ztráta nebo náklady, které vzniknou v důsledku incidentu,
- **nemajetková újma** = nepřímá finanční ztráta, tedy škody, které mohou zahrnovat poškození reputace, ztrátu důvěry zákazníků nebo jiné formy nehmotných ztrát.

Následuje vymezení oblastí pro posouzení významnosti dopadu kybernetických bezpečnostních incidentů na organizaci:

- provozní dopad kybernetického bezpečnostního incidentu na povinnou osobu a její schopnost poskytovat regulovanou službu,
- množství uživatelů regulované služby a jiných orgánů a osob zasažených kybernetickým bezpečnostním incidentem,
- časové, lidské a technické zdroje, které jsou potřebné k obnově poskytování zasažené regulované služby,
- typ a umístění aktiv dotčených kybernetickým bezpečnostním incidentem,
- citlivost informací a dat zasažených kybernetickým bezpečnostním incidentem a újma, jakou může narušení bezpečnosti těchto informací a dat způsobit povinné osobě nebo jinému orgánu nebo osobě, a
- přímá příčina kybernetického bezpečnostního incidentu, je-li povinné osobě známo, zda se jedná o lidskou chybu, technickou závadu nebo úmyslné jednání.

U každé oblasti by měla být stanovena prahová hodnota dopadu, při jejímž překročení lze dopad považovat za významný. Hodnoty uvedené v příkladech u jednotlivých oblastí mají vzestupnou tendenci, kdy 1= nejnižší dopad, 4 = nejvyšší dopad.

3.1 Provozní dopad

Provozním dopadem se rozumí dopad kybernetického bezpečnostního incidentu na povinnou osobu a její schopnost poskytovat regulovanou službu.

Příklad:

1. Dopady nejsou žádné nebo pouze zanedbatelné. Poskytování služby není ovlivněno.
2. Dopady jsou rozpoznatelné. Poskytování služby je ovlivněno, ale nedochází k výraznému narušení.
3. Dopady jsou významné. Poskytování služby je významně ovlivněno, nicméně nedochází k úplnému přerušení.
4. Dopady jsou extrémní. Dochází k úplnému přerušení poskytování služby.

3.2 Množství zasažených osob

Množství zasažených osob zahrnuje přímo zasažené uživatele regulované služby a jiné orgány a osoby zasažené kybernetickým bezpečnostním incidentem. Pokud je dostupný i přehled sekundárně zasažených uživatelů, lze jej také zahrnout.

Příklad:

1. Počet zasažených osob je do 5 % z celkového počtu.
2. Zasažena byla pouze lokální síť (např. pobočka), příp. počet zasažených osob je do 15 % z celkového počtu.
3. Počet zasažených osob je více než 25 % nebo má incident dopad na podnikatelský sektor.
4. Rozsáhlý dopad na celý subjekt nebo stát, kdy počet zasažených osob přesahuje 50 % z celkového počtu.

3.3 Zdroje potřebné pro obnovu

Zdroji potřebnými pro obnovu se rozumí časové, lidské a technické zdroje, které jsou potřebné k obnově poskytování zasažené regulované služby.

Příklad:

1. Informace/data/služba můžou být zcela obnoveny bez časové prodlevy pomocí zajištěných zdrojů.
2. Informace/data/služba můžou být obnoveny se zanedbatelnou časovou prodlevou a ztrátou informací za použití nových zdrojů, které pro subjekt nepředstavují významnou finanční zátěž.
3. Informace/data/služba můžou být obnoveny se ztrátou nekritických částí, časová prodleva je do 75 % maximální tolerovatelné doby prostojů za použití nových zdrojů, které představují významnou finanční zátěž subjektu.
4. Informace/data/služba nemůžou být obnoveny v akceptovatelném čase, nebo je lze obnovit s významnou ztrátou kritických částí (vyšší než cíl bodu obnovy).

3.4 Typ a umístění dotčených aktiv

V této oblasti se posuzuje typ a umístění aktiv dotčených kybernetickým bezpečnostním incidentem, která mohou být ovlivněna kybernetickým bezpečnostních incidentem, ale nebyla přímo zasažena.

Příklad:

1. Méně významný informační systém, uživatelské stanice, demilitarizovaná zóna („DMZ“) nebo místní uživatelský účet umožňující správu pouze méně významných technických aktiv.
2. Server s významnou službou, síťové aktivum zajišťující bezpečnost regulované služby (např. perimetrový firewall) nebo privilegovaný účet umožňující správu významných technických aktiv.
3. Privilegovaný účet správce domény.
4. Prvek řízení infrastruktury – virtualizační servery, síťová infrastruktura, řídicí systémy.

3.5 Citlivost zasažených informací a dat

Vedle citlivosti a důvěrnosti zasažených informací a dat se posuzuje i újma, jakou může narušení bezpečnosti těchto informací a dat způsobit povinné osobě nebo jinému orgánu nebo osobě.

Příklad:

1. Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby.
2. Aktiva nejsou veřejně přístupná, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.
3. Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje).
4. Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů).

3.6 Přímá příčina incidentu, je-li známa

Předmětem této oblasti je identifikace přímé příčiny kybernetického bezpečnostního incidentu, je-li povinné osobě známa, s určením, zda se jedná o lidskou chybu, technickou závadu nebo úmyslné jednání.

Příklad:

1. Technické selhání nebo lidská chyba bez úmyslu.
2. Úmyslný útok, útočník bez konkrétního cíle (středně sofistikovaný aktér) nebo lidská chyba bez úmyslu, která způsobila podstatné škody.
3. Úmyslný útok nebo útočník cílící na konkrétní infrastrukturu (sofistikovaný aktér, např. větší ransomware operátor nebo průmyslová špionáž).
4. Úmyslná sofistikovaná zločinecká nebo APT organizace cílící na celou organizaci.

4 Praktický příklad

Uvedené příklady jsou pouze ilustrační, jedná se o návrh způsobu vyhodnocení významnosti. Organizace může zvolit jakýkoliv odlišný způsob, který bude dávat smysl a bude dostatečně zdokumentovaný a opakovatelný.

1. krok – stanovení únosné míry újmy

Interně si sepište krátkou metodiku, kde určíte, co ve Vaší organizaci ještě považujete za únosné. Ideální je v rámci této metodiky určit také následující údaje:

- dobu obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb regulované služby, a
- bod obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání technického aktiva.

Tyto parametry se následně mohou promítnout do níže uvedených proměnných.

1.1. Základní definice

Únosná míra újmy je taková kombinace celkové finanční ztráty, reputační újmy, dopadu na klienty a provozní nedostupnosti, při které:

- není ohrožen život nebo zdraví osob a
- není ohrožena schopnost společnosti plnit své smluvní, zákonné a regulatorní závazky.

1.2. Praktická kvantifikace

Stanovte si stropy např. u níže uvedených oblastí, které dohromady tvoří „únosnou míru újmy“ – při jejich překročení je dopad potenciálně významný:

Oblast	**Únosná míra újmy**
Finanční ztráta	≤ 1 000 000 Kč za jeden incident
Nedostupnost služby	max. 4 hodiny nedostupnosti kritických částí regulované služby
Počet dotčených osob	max. 10 000 klientů / uživatelů
Právní dopady	bez rizika pokuty / žaloby / zásahu do licencí
Reputace	bez negativní publicity ve významných médiích

V metodice si pak napíšete například:

*Incident překračuje únosnou míru újmy, pokud alespoň **jeden** z uvedených limitů dané oblasti byl fakticky překročen nebo je rozumně očekávatelné, že bude překročen (na základě kvalifikovaného odhadu).*

2. krok – definice oblastí pro posouzení dopadu

Vyhláška vypočítává, co musíte minimálně zohlednit:

1. **Provozní dopad** na schopnost poskytovat regulovanou službu
2. **Počet a typ zasažených uživatelů / dalších osob**
3. **Zdroje** potřebné k obnově (čas, lidé, technologie)
4. **Typ a umístění dotčených aktiv**
5. **Citlivost dat / informací** a možnou újmu
6. **Příčinu incidentu** (lidská chyba, závada, úmysl)

V praxi můžete použít hodnoticí matici dopadu – např. stupnice 1–4:

- 1 = zanedbatelný/nízký
- 2 = střední
- 3 = vysoký
- 4 = kritický

Hodnoticí matice dopadu

A. Provozní dopad

- 1 – bez dopadu na regulovanou službu
- 2 – krátké omezení (< 1 h), bez vlivu na SLA
- 3 – omezení 1–4 h / drobné nesplnění SLA
- 4 – nedostupnost > 4 h / zásadní omezení poskytování služby

B. Počet a typ dotčených osob

- 1 – interní testovací prostředí, žádný uživatel (zákazník)
- 2 – max. 15 % uživatelů / pouze interní zaměstnanci
- 3 – max. 25 % uživatelů / významný interní dopad
- 4 – více než 50 % uživatelů / dopad na zvlášť zranitelné osoby (např. pacienti, kritická infrastruktura)

Obdobně můžete postupovat u dalších oblastí, příp. můžete využít příklady uvedené v kapitole 3.

V metodice pak popíšete, jak vyhodnocujete – když detekujete incident, posuzující osoba projde všechny oblasti a ke každé přiřadí 1–4.

3. krok – rozhodovací pravidlo („kdy je dopad významný“)

Vyhláška říká, že dopad je významný, pokud:

1. **přesáhne stanovenou únosnou míru újmy** (pokud ano, pokračujete bodem 2.),
2. **oblast pro posouzení dopadu je vyhodnocena jako významná**.

Pro zjištění, zda oblast pro posouzení splňuje kritérium významného dopadu, můžete využít různé postupy, např.:

- určit si, že pro splnění kritéria postačí, když alespoň jedna oblast dosáhne hodnoty 4 – kritická;
- stanovit hodnotu celkového skóre, při jehož překročení je naplněno kritérium významného dopadu, např. pokud alespoň tři oblasti dosáhnou hodnoty 3 – vysoká;
- vytvořit si algoritmus, ve kterém si definujete interní limity, například:

Významnost dopadu = váha vlivu oblasti x hodnota oblasti		Hodnota oblasti			
		1	2	3	4
Váha vlivu oblasti	1	1	2	3	4
	2	2	4	6	8
	3	3	6	9	12
	4	4	8	12	16

Při překročení nastaveného limitu (v tabulce vyznačeno červenou barvou) se dopad považuje za významný. Takto transparentně naplníte § 14 odst. 2 vyhlášky – máte omezenou únosnou míru újmy a jasný způsob, jak určíte, že oblast dopadu je významná.

4. Ilustrační příklad kybernetického bezpečnostního incidentu

Scénář 1:

- V pátek dopoledne dojde k selhání clusteru databáze kritické části regulované služby.
- Kritická funkcionalita (např. zadávání nových objednávek / smluv) je nedostupná 3 hodiny 50 minut.
- Většina klientů se během té doby nedostane k části služeb, ale základní náhled účtu funguje.
- Incident zasáhne cca 9 500 klientů (pod 10 000).
- Finanční dopad (SLA kredity, přesčasy, dočasný výpadek příjmů, technická podpora) je odhadnut na 900 000 Kč.
- Nedojde k úniku dat, nejde o útok, jde o technickou závadu.
- Incident se neobjeví ve velkých médiích, pouze pár stížností na sociálních sítích a na zákaznické lince.
- Právní / regulatorní dopad: žádné reálné riziko pokuty ani zásahu do licencí.

Hodnocení únosné míry újmy:

- Finanční ztráta: 900 000 Kč ≤ 1 000 000 Kč ✅
- Nedostupnost služby: 3 h 50 min ≤ 4 h ✅
- Počet dotčených osob: 9 500 ≤ 10 000 ✅
- Právní dopady: žádné riziko pokuty / žaloby / zásahu do licencí ✅
- Reputace: bez negativní publicity ve významných médiích ✅

Výsledek: Únosná míra újmy nebyla překročena – incident nemá významný dopad.

Scénář 2:

- Během víkendové noci dojde k úspěšnému útoku (např. kompromitovaný účet administrátora aplikace).
- Útočník si stáhne databázi s osobními údaji klientů regulované služby.
- Služba zůstává funkční, nedojde k nedostupnosti – klienti si ničeho nevšimnou.
- Únik se odhalí o pár dní později forenzní analýzou logů.
- Dotčeno je 10 500 klientů (tedy nad limitem 10 000).
- Finanční dopad: odhad cca 600 000 Kč (forenzní analýza, právní služby, notifikace klientů, posílení bezpečnostních opatření).
- Vzniká reálné riziko sankce ze strany dozorového orgánu (např. za porušení ochrany osobních údajů).
- O incidentu vyjde článek na velkém zpravodajském portálu, následně je krátká zmínka i v TV zpravodajství – reputační dopad je nepříjemný, ale ne likvidační.

Hodnocení únosné míry újmy:

- Finanční ztráta: 600 000 Kč ≤ 1 000 000 Kč ✅
- Nedostupnost služby: 0 h ≤ 4 h ✅
- Počet dotčených osob: 10 500 > 10 000 ❌
- Právní dopady: reálné riziko sankce regulátorem → limit překročen ❌
- Reputace: negativní publicita ve významných médiích → limit překročen ❌

Únosná míra újmy je překročena hned ve třech oblastech (počet osob, právní dopady, reputace).

Hodnocení oblastí:

A. Provozní dopad – 1

- ŽÁDNÁ nedostupnost, služba byla po celou dobu online
  → „bez dopadu na regulovanou službu“

B. Počet a typ dotčených osob – 4

- Dotčeno 10 500 klientů (tj. nad limitem 10 000, typicky významná část uživatelské základny)

C. Zdroje potřebné pro obnovu – 3

- Je potřeba:
  - forenzní analýza,
  - posílení opatření,
  - notifikace klientů,
  - zpracování s právníky a regulátorem.
- To znamená významnou časovou i finanční zátěž, i když samotná služba neběžela v režimu výpadku.

D. Typ a umístění dotčených aktiv – 3

- Zasažena produkční databáze s osobními údaji – typicky „server s významnou službou“ nebo i „prvek řízení infrastruktury“ (pokud je přístup širší).

E. Citlivost zasažených informací / dat – 3

- Osobní údaje klientů, jejichž zneužití může znamenat finanční ztráty, zneužití identity, žaloby, ztrátu obchodního tajemství.

F. Přímá příčina incidentu – 3

- Úmyslný útok, minimálně „úmyslný jednoduchý / středně sofistikovaný útok“.

Výsledek:

- **Únosná míra újmy: PŘEKROČENA (počet osob, právní dopady, reputace).**
- **V oblastech B, C, D, E a F jsou poměrně vysoké hodnoty (3–4).**

Incident má významný dopad ve smyslu § 14 vyhlášky a § 15 ZKB.

Pokud:

- má původ v kyberprostoru a
- nelze vyloučit úmyslné zavinění,

musíte jej hlásit podle § 15 odst. 2 ZKB Národnímu CERT prostřednictvím Portálu NÚKIB.

Dopad kybernetického bezpečnostního incidentu na poskytování regulované služby se považuje za významný, pokud překročí poskytovatelem regulované služby stanovenou únosnou míru újmy a zároveň byla překročena prahová hodnota u oblastí pro posouzení významnosti dopadu.

5 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**
24. února 2026	1.0	OREG/OK/CERT	Vytvoření dokumentu