PORTÁL NÚKIB

Protiopatření podle nového zákona o kybernetické bezpečnosti

TLP:CLEAR

3. listopadu 2025

Verze 1.0

Národní úřad pro kybernetickou a informační bezpečnost

Obsah

1 Co se dozvím v tomto dokumentu?

Protiopatření jsou aktivní úkony Národního úřadu pro kybernetickou a informační bezpečnost (dále také „NÚKIB“), které provádí v mimořádných situacích. Jejich cílem je ochrana aktiv před hrozbou nebo před zneužitím zranitelností, případně před kybernetickým bezpečnostním incidentem. Mezi protiopatření patří výstraha, varování a reaktivní protiopatření. Tento dokument popisuje specifika jednotlivých druhů protiopatření.

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

- Zákon o kybernetické bezpečnosti ukládá poskytovatelům regulovaných služeb povinnost zavádět bezpečnostní opatření a plnit další povinnosti podle ZKB. Plnění těchto povinností je ponecháno v zákonných mezích na uvážení jednotlivých poskytovatelů regulovaných služeb. Stát si však ponechává možnost tuto autonomii v mimořádných situacích omezit prostřednictvím tzv. **protiopatření.**
- Existuje několik typů protiopatření: **výstraha, varování a reaktivní protiopatření**.
- **Výstraha** je veřejné upozornění na závažný incident nebo porušení povinností konkrétním poskytovatelem. Cílem je chránit bezpečnost státu, veřejný pořádek, zdraví či majetek.
- **Varování** je deklarace závažné hrozby nebo zranitelnosti, která může mít širší dopady. Poskytovatelé v režimu vyšších povinností jej musí zohlednit v řízení rizik.
- **Reaktivní protiopatření** je nástroj, ukládá konkrétní technická nebo organizační opatření k odvrácení nebo zmírnění incidentu, případně k navýšení bezpečnosti aktiv.

3 Protiopatření obecně

Jednou ze základních povinností v rámci ZKB je povinnost zavádět a provádět bezpečnostní opatření uvedená v § 13 a § 14 zákona, v míře nezbytné pro zajištění kybernetické bezpečnosti regulované služby. Zavádění bezpečnostních opatření je spojeno s vysokou mírou autonomie regulované organizace – je to ona, kdo si řízeným způsobem stanovuje, jaká bezpečnostní opatření zavede a v jaké míře.

Protiopatření jsou nástrojem státu, jak ve specifických situacích a za mimořádných okolností tuto autonomii při zavádění bezpečnostních opatření omezit a dosáhnout dalšího zvýšení kybernetické

bezpečnosti. Protiopatřeními jsou tzv. výstraha, varování a reaktivní protiopatření. Každý ze tří typů protiopatření dosahuje výše uvedeného cíle jiným způsobem.

Obecně u každého typu protiopatření platí, že každý je **povinen poskytovat NÚKIB nezbytnou součinnost** při zajišťování podkladů pro vydání protiopatření. Požadovaná součinnost nemusí být poskytnuta, brání-li v tom zákonná nebo státem uznaná povinnost mlčenlivosti nebo plnění jiné zákonné povinnosti.

4 Výstraha

Úplné znění § 21 odst. 1 zákona o kybernetické bezpečnosti:

„Úřad může po konzultaci s dotčeným poskytovatelem regulované služby z důvodu ochrany bezpečnosti České republiky, vnitřního pořádku, života a zdraví nebo majetkové hodnoty informovat veřejnost formou výstrahy o kybernetickém bezpečnostním incidentu nebo o porušování povinností stanovených tímto zákonem, nebo dotčenému poskytovateli regulované služby rozhodnutím uložit, aby tak učinil sám.“

NÚKIB informace o kybernetických bezpečnostních incidentech, ani o porušování povinností stanovených ZKB standardně nezveřejňuje a řeší tyto problémy pouze s dotčenými regulovanými osobami (formou reaktivních protiopatření, nápravných opatření nebo pokut).

Veřejná výstraha slouží k možnosti **informovat obecnou veřejnost** o nastalém kybernetickém bezpečnostním incidentu, případně o tom, že určitý poskytovatel regulované služby závažným způsobem porušuje své povinnosti stanovené ZKB. Důvodem takového informování musí být ochrana bezpečnosti České republiky, vnitřního pořádku, života, zdraví nebo majetkové hodnoty.

Zveřejnění informace může buď provést NÚKIB sám prostřednictvím svým internetových stránek, nebo vydat rozhodnutí, ve kterém dotčenému poskytovateli regulované služby uloží povinnost informování veřejnosti provést.

Pokud zveřejnění provede sám NÚKIB, bude se jednat o **úkon podle části čtvrté správního řádu**. Podstatnou částí takového procesu je povinnost konzultovat zveřejnění informace s dotčeným poskytovatelem regulované služby. Dotčeným poskytovatelem regulované služby je typicky ten, u koho se stal kybernetický bezpečnostní incident nebo u koho kontrola NÚKIB zjistila, že závažným způsobem porušuje své povinnosti vyplývající ze ZKB. Dotčeným poskytovatelem regulované služby může být jak poskytovatel v režimu vyšších povinností, tak i poskytovatel v režimu nižších povinností.

K vydání výstrahy může při splnění zákonných požadavků dojít i v případě, že s tím dotčený poskytovatel regulované služby v rámci konzultace **nesouhlasí**. Podstatou konzultace je vzájemná koordinace a možnost vysvětlit si před zveřejněním vzájemné pohledy na danou

situaci. NÚKIB informuje veřejnost prostřednictvím svých internetových stránek prostým zveřejněním informace. Míra a detail informování není zákonem stanovena a bude odpovídat každé konkrétní situaci. Bude-li to vhodné může NÚKIB informovat také další poskytovatele regulovaných služeb prostřednictvím Portálu NÚKIB.

Pokud zveřejnění výstrahy nebude provádět sám NÚKIB, může dotčenému poskytovateli regulované služby **uložit povinnost**, aby informování provedl sám. V takovém případě se bude jednat o klasické správní řízení, na jehož konci dojde k vydání rozhodnutí. Od klasického správního řízení se řízení o uložení povinnosti informovat veřejnost liší pouze v tom, že rozhodnutí může být prvním úkonem ve věci a rozklad podaný proti němu nemá odkladný účinek. Na rozdíl od informační povinnosti podle § 19 ZKB směřuje výstraha vůči široké veřejnosti, nejen vůči uživatelům regulované služby.

5 Varování

Úplné znění § 22 odst. 1 zákona o kybernetické bezpečnosti:

„Úřad vydá varování, dozví-li se o závažné hrozbě nebo zranitelnosti v oblasti kybernetické bezpečnosti.“

NÚKIB má ze ZKB pravomoc vydávat varování, dozví-li se o **závažné hrozbě nebo zranitelnosti v oblasti kybernetické bezpečnosti**. V praxi to znamená, že NÚKIB za mimořádných okolností určitou hrozbu nebo zranitelnost veřejně označí a uvede k ní bližší informace. Historicky NÚKIB vydal již několik varování. Všechna tato varování jsou zveřejněna na elektronické úřední desce NÚKIB.

Varování podle ZKB je samo o sobě deklarace stavu – něco je hrozba, nebo zranitelnost. Není samo o sobě spojeno s uložením konkrétní povinnosti subjektu, jedná se stejně jako v případě výstrahy o úkon podle části čtvrté správního řádu.

Podle starého zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále také „starý zákon o kybernetické bezpečnosti“) se nerozlišovalo mezi režimem nižších a vyšších povinností a varování vstupovala do procesu řízení rizik jakožto bezpečnostního opatření podle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, a to dle míry hrozby, která byla ve varování uvedena.

U poskytovatele regulované služby v **režimu vyšších povinností** podle ZKB varování stejně tak vstupuje do procesu řízení rizik, protože to výslovně stanovuje vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností jako jedno z bezpečnostních opatření.

U poskytovatele regulované služby v **režimu nižších povinností** podle ZKB není zohlednění varování povinné. Zohlednění varování může být pro poskytovatele regulované služby přeneseně povinné v případě, kdy je možné jej zohlednit ve smlouvě s dodavateli. Zajištění relevantních požadavků ve smlouvách s dodavateli je jedním z bezpečnostních opatření poskytovatele regulované služby v režimu nižších povinností.

Varování standardně neřeší kybernetické bezpečnostní hrozby specifické pro jeden konkrétní subjekt, které nemají potenciál mít významnější dopad na fungování společnosti jako celku. Naopak je využíváno především v situacích, kdy je **hrozba společná pro širší okruh osob** a její realizace by měla závažné dopady přesahující zájmy jedné regulované osoby.

6 Reaktivní protiopatření

Úplné znění § 23 odst. 1 zákona o kybernetické bezpečnosti:

„Úřad vydá rozhodnutí, ve kterém uloží poskytovateli regulované služby povinnost provést reaktivní protiopatření

a) k řešení hrozícího nebo probíhajícího kybernetického bezpečnostního incidentu,

b) k zabezpečení aktiv před kybernetickým bezpečnostním incidentem, nebo

c) za účelem zvýšení ochrany aktiv na základě analýzy již vyřešeného kybernetického bezpečnostního incidentu.“

Účelem reaktivního protiopatření je **okamžitá reakce** na výskyt kybernetického bezpečnostního incidentu. Reaktivní protiopatření obsahuje povinnost provést konkrétní úkony nutné k odvrácení kybernetického bezpečnostního incidentu nebo ke zmírnění jeho následků. Může nabývat jak podoby preventivní, kdy kybernetický bezpečnostní incident hrozí, nebo čistě reaktivní, kdy incident právě probíhá, či následně preventivní. Následně preventivní reaktivní opatření je využíváno v situacích, kdy incident proběhl, byl vyřešen a je vhodné provést úkony, které budou výskytu tohoto incidentu u vymezeného dotčeného okruhu poskytovatelů regulovaných služeb dostatečně předcházet.

Mezi protiopatření nově řadíme také původní institut „ochranného opatření” ze starého znění zákona o kybernetické bezpečnosti. To lze nově nalézt právě mezi reaktivními protiopatřeními, došlo tak ke sloučení těchto nástrojů. Jeho účelem je navrhnout na základě analýzy a zkušeností z již vyřešeného kybernetického bezpečnostního incidentu vhodné kroky vedoucí ke zvýšení ochrany aktiv u poskytovatelů regulovaných služeb.

Zatímco výstraha a varování jsou instituty spíše informativní, **reaktivní protiopatření ukládá konkrétní technická nebo organizační opatření**, která je potřeba zavést nebo provést. Míra detailu a síly v daných opařeních tedy bude oproti zbytku protiopatření standardně vyšší. Vzhledem ke své povaze je pak reaktivní protiopatření prostředkem *ultima ratio*.

Rozsah reaktivního protiopatření je dostatečně široký na to, aby jím bylo možné nařídit **zákaz použití některých aktiv** daného poskytovatele do doby odstranění nedostatků, které byly při kontrole nalezeny.

Reaktivní protiopatření může mít dvě formy, a to **rozhodnutí, nebo opatření obecné povahy**. Reaktivní protiopatření lze ve formě rozhodnutí vydat v případě výskytu kybernetického

bezpečnostního incidentu v rámci určité organizace. Takové rozhodnutí konkrétně specifikuje povinnosti pro určeného adresáta – poskytovatele regulované služby. Naopak ve formě opatření obecné povahy lze reaktivní protiopatření vydat při výskytu incidentu, jehož rozsah je větší nebo jehož rozsah nelze kvůli složitosti incidentu nebo jeho rychlému vývoji přesně určit. Takové opatření obecné povahy bude specifikovat konkrétní povinnosti k odvrácení daného incidentu neurčitému okruhu poskytovatelů regulované služby. Tento okruh bude definován za užití generických znaků odpovídajících charakteru tohoto okruhu poskytovatelů.

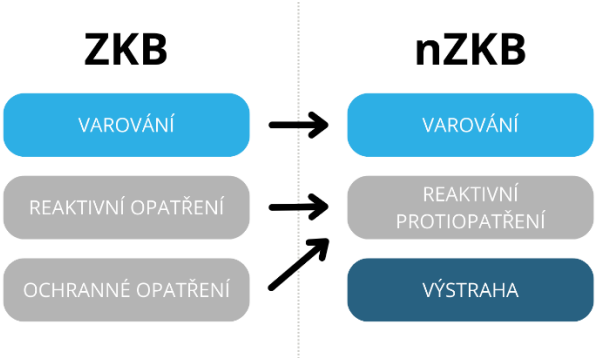
Reaktivní protiopatření je povinné pro všechny poskytovatele regulované služby. Konkrétní reaktivní protiopatření však může stanovit odlišný okruh adresátů, a to podle povahy kybernetického bezpečnostního incidentu, na který reaguje – často může být ohroženo pouze konkrétní odvětví a podobně.

Poskytovatelé regulované služby, kterých se reaktivní protiopatření týká, mají zákonnou povinnost informovat NÚKIB o jeho provedení ve lhůtě v něm uvedené, **není-li v konkrétním protiopatření stanoveno jinak**.

Opatření obecné povahy je **účinné okamžikem zveřejnění na úřední desce NÚKIB**. O vydání protiopatření NÚKIB informuje poskytovatele prostřednictvím Portálu NÚKIB.

7 Přechodná ustanovení a protiopatření

Zákon o kybernetické bezpečnosti v § 71 odst. 3 a 4 uvádí, že varování, reaktivní a ochranná opatření, vydaná za účinnosti starého zákona č. 181/2014 Sb., o kybernetické bezpečnosti, **zůstávají v platnosti i podle nového zákona a jsou nadále závazná**. Varování jsou i nadále varováními, reaktivní a ochranná opatření jsou považována za reaktivní protiopatření.



Zohlednění varování vstupuje do bezpečnostních opatření:

- **Poskytovatel v režimu vyšších povinností**: varování vstupuje do procesu řízení rizik.
  - Je-li subjekt v režimu vyšších povinností nově regulován nebo má varování zohlednit v nově regulovaných částech své organizace, uplatní se pro zohlednění varování roční přechodná lhůta.
- **Poskytovatel v režimu nižších povinností**: zohlednění varování **není** v rámci řízení rizik povinné. Povinné však může být, pokud je možné je promítnout do smluv s dodavateli.

Reaktivní a ochranná opatření ukládají konkrétní technická nebo organizační opatření, která je potřeba zavést nebo provést. Vydaná reaktivní a ochranná opatření odpovídají nastavení regulace podle starého zákona o kybernetické bezpečnosti. Postupně bude docházet k jejich přizpůsobování a výkladu tak, aby je bylo možné uplatnit v prostředí nové právní úpravy.

8 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**
3. listopadu 2025	1.0	OREG	Vytvoření dokumentu