Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Manažerské shrnutí
Vyhláška o Portálu NÚKIB navazuje na ustanovení v novém Zákoně o kybernetické bezpečnosti a upravuje technické a procesní náležitosti technického řešení automatizace a elektronizace procesů Úřadu, které jsou spojeny s výkonem většiny agend podle nového Zákona o kybernetické bezpečnosti.
Tento dokument slouží jako rozpracované teze budoucí vyhlášky a je proto podkladem k další diskuzi. Může se měnit a to v závislosti jak na obsahu připomínek odborné veřejnosti, tak na obsahu připomínek v průběhu legislativního procesu.

Návrh

VYHLÁŠKA

ze dne dd.mm.rrrr,

o technických a organizačních podmínkách používání Portálu NÚKIB a požadavcích na úkony vykonávané prostřednictvím Portálu NÚKIB (vyhláška o Portálu NÚKIB)

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § X zákona č. X, o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti):

ČÁST PRVNÍ
PORTÁL NÚKIB A NÁLEŽITOSTI ÚKONŮ

HLAVA I
PORTÁL NÚKIB

§ 1
Přístup do Portálu NÚKIB a úkony v něm

1) Přístup do portálu NÚKIB a jeho následné používání se provádí prostřednictvím internetové stránky Úřadu. Portál NÚKIB je neveřejný a přihlašuje se do něj prostřednictvím přidělených přihlašovacích údajů.
2) Úřad v rámci Portálu NÚKIB zpřístupní formuláře pro
   a) registraci poskytovatele regulované služby podle § X *[Registrace poskytovatele regulované služby]* zákona,
   b) změna registrace poskytovatele regulované služby podle § X *[Změna registrace poskytovatele regulované služby]* zákona,
   c) pověření osoby,

d) hlášení údajů podle § X *[Hlášení údajů poskytovatelem regulované služby]* zákona,
e) hlášení incidentů podle § X *[Hlášení kybernetických bezpečnostních incidentů]* zákona,
f) hlášení provedení protiopatření podle § X *[Protiopatření]* zákona,
g) hlášení provedení nápravného opatření podle § X *[Nápravná opatření]* zákona,
h) žádost o výmaz z evidence poskytovatelů regulovaných služeb podle § X *[Výmaz z evidence poskytovatelů regulovaných služeb]* zákona,
i) hlášení informací o dodavatelích dle § X *[Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce]* zákona.

3) Úkony podle § X *[Hlášení údajů poskytovatelem regulované služby]*, § X *[Protiopatření]*, § X *[Nápravná opatření]* § X *[Výmaz z evidence poskytovatelů regulovaných služeb],* § X *[Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce]* zákona může provést pouze oprávněná či pověřená osoba, a to po své identifikaci a autentizaci s využitím prostředku elektronické identifikace prostřednictvím kvalifikovaného systému elektronické identifikace alespoň s úrovní záruky značná, nebo po přihlášení skrze autentizační informační systém podle zákona o základních registrech[1] (dále jen „autentizační informační systém").
4) Není-li oprávněná nebo pověřená osoba občanem České republiky, musí Úřadu prokázat své oprávnění jednat za poskytovatele regulovaných služeb náhradním způsobem.

§ 2
Osoby přistupující do Portálu NÚKIB

1) Oprávněnou osobou se rozumí fyzická osoba, která je podle referenčních údajů vedených v základních registrech[2] nebo údajů v autentizačním informačním systému
   a) členem statutárního orgánu poskytovatele regulovaných služeb,
   b) zastupuje právnickou osobu, která je členem statutárního orgánu poskytovatele regulovaných služeb,
   c) podnikající fyzickou osobou poskytující regulované služby, nebo
   d) nositelem odpovídající role v rámci orgánu veřejné moci, který je poskytovatelem regulované služby.
2) Pověřenou osobou se rozumí fyzická osoba, která byla v rámci Portálu NÚKIB pověřena oprávněnou osobou k provádění veškerých činností a úkonů podle zákona o kybernetické bezpečnosti.
3) Uživatelem se rozumí kdokoliv, komu byl v rámci Portálu NÚKIB vytvořen uživatelský účet.

[1] § 56a zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.
[2] § 26 zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů..

§ 3
Druhy hlášených údajů

1) Registračními údaji se rozumí
   a) identifikační údaje poskytovatele regulované služby, jimiž se rozumí jeho název, identifikační číslo, adresa sídla, a případně hlavní provozovny a dalších provozoven v jiných členských státech Evropské unie,
   b) seznam poskytovaných regulovaných služeb naplňujících kritéria pro identifikaci regulovaných služeb a kritéria naplněná poskytovatelem regulované služby podle vyhlášky o regulovaných službách,
2) Kontaktními údaji se rozumí jméno a příjmení a případně další údaje umožňující jednoznačnou identifikaci oprávněné nebo pověřené osoby, její role či pracovní pozice vůči poskytovateli regulované služby, její telefonní číslo a e-mailová adresa.
3) Doplňujícími údaji se rozumí jména domén, čísla autonomních systémů (ASN) a rozsahy IP adres, které jsou využívány k poskytování regulované služby, pokud takové existují, informace o geografickém rozšíření regulované služby, jejím přeshraničním poskytování a vlastnické struktuře poskytovatele regulované služby.

HLAVA II
NÁLEŽITOSTI VYBRANÝCH ÚKONŮ

§ 4
Registrace poskytovatele regulované služby

1) Fyzická osoba může přistoupit k registraci nebo potvrdit registraci poskytovatele regulované služby skrze Portál NÚKIB pouze po své identifikaci a autentizaci s využitím prostředku elektronické identifikace prostřednictvím kvalifikovaného systému elektronické identifikace alespoň s úrovní záruky značná, nebo po přihlášení skrze autentizační informační systém.
2) Není-li registrující fyzická osoba oprávněnou osobou, musí být registrace poskytovatele regulované služby potvrzena oprávněnou osobou.
3) Formulář pro registraci poskytovatele regulované služby obsahuje registrační údaje.

§ 5
Změna registrace poskytovatele regulované služby

1) Změnu registrace provádí oprávněná či pověřená osoba po své identifikaci a autentizaci s využitím prostředku elektronické identifikace prostřednictvím kvalifikovaného systému elektronické identifikace alespoň s úrovní záruky značná, nebo po přihlášení skrze autentizační informační systém, pokud
   a) poskytovatel regulované služby naplní kritéria pro identifikaci jakékoliv další regulované služby podle § X odst. 1 *[Změna registrace poskytovatele regulované služby]* zákona,

b) v rámci naplnění kritérií pro identifikaci regulované služby dojde ke změně režimu poskytovatele regulované služby podle § X odst. 2 *[Změna registrace poskytovatele regulované služby]* zákona.

2) Formulář pro změnu registrace poskytovatele regulované služby obsahuje registrační údaje.

§ 6
Pověření osoby

3) Pověření osoby může provést pouze oprávněná osoba po své identifikaci a autentizaci s využitím prostředku elektronické identifikace prostřednictvím kvalifikovaného systému elektronické identifikace alespoň s úrovní záruky značná, nebo po přihlášení skrze autentizační informační systém.
4) Formulář pro pověření osoby obsahuje
   a) identifikační údaje poskytovatele regulované služby,
   b) kontaktní údaje pověřené osoby,
   c) informaci o pověření pověřované osoby.

§ 7
Hlášení kybernetického bezpečnostního incidentu

1) Formulář hlášení kybernetického bezpečnostního incidentu poskytovatelem regulované služby obsahuje
   a) identifikační údaje poskytovatele regulované služby včetně výčtu jím poskytovaných regulovaných služeb,
   b) kontaktní údaje,
   c) doplňující údaje zasažených systémů a služeb,
   d) informace o kybernetickém bezpečnostním incidentu, zejména datum a čas zjištění, stav incidentu, pravděpodobnou příčinu incidentu, obecný popis incidentu, indikátory kompromitace, jsou-li tyto informace dostupné,
   e) informace vymezující dopad incidentu, zejména funkční dopad, odhad rozsahu a počtu zasažených systémů, strojů, aktiv či osob, čas a zdroje potřebné k obnově poskytování zasažené služby, lokaci incidentu a citlivost zasažených dat a případný přeshraniční dopad incidentu, jsou-li tyto informace dostupné,
   f) informace o reakci na kybernetický bezpečnostní incident, zejména požadovaná podpora ze strany Úřadu, přijatá a probíhající opatření ke zmírnění následků a subjekty, které byly v souvislosti s incidentem informovány.
2) Skrze formulář hlášení kybernetického bezpečnostního incidentu může poskytovatel regulované služby provést
   a) prvotní hlášení podle § X odst. 1 *[Náležitosti hlášení kybernetických bezpečnostních incidentů]* zákona,
   b) oznámení incidentu podle § X odst. 3 písm. a) *[Náležitosti hlášení kybernetických bezpečnostních incidentů]* zákona,

c) podání průběžné zprávy podle § X odst. 3 písm. b) *[Náležitosti hlášení kybernetických bezpečnostních incidentů]* zákona,
d) podání závěrečné zprávy podle § X odst. 3 písm. c) *[Náležitosti hlášení kybernetických bezpečnostních incidentů]* zákona,
e) podání zprávy o pokroku podle § X odst. 4 *[Náležitosti hlášení kybernetických bezpečnostních incidentů]* zákona.

3) Hlásí-li poskytovatel regulované služby kybernetický bezpečnostní incident v souladu s § X *[Hlášení kybernetických bezpečnostních incidentů]* zákona jinak než prostřednictvím Portálu NÚKIB, uplatní se obsahové náležitosti podle odstavce 1 obdobně.
4) Hlásí-li kybernetický bezpečnostní incident prostřednictvím internetových stránek Úřadu dobrovolný ohlašovatel podle § X odst. 5 *[Hlášení kybernetických bezpečnostních incidentů]* zákona, který není poskytovatel regulované služby, obsahuje formulář
   a) identifikační a kontaktní údaje ohlašovatele či jiné kontaktní osoby,
   b) identifikace informačního systému nebo služby zasažených kybernetickým bezpečnostním incidentem,
   c) informace o kybernetickém bezpečnostním incidentu zejména datum a čas zjištění, druh hrozby nebo základní příčinu, která incident pravděpodobně spustila, odhad rozsahu zasažených systémů, odhad počtu zasažených uživatelů, podrobný popis incidentu a případný přeshraniční dopad incidentu, jsou-li tyto informace dostupné,
   d) informace o reakci na kybernetický bezpečnostní incident zejména stav zvládání incidentu, přijatá a probíhající opatření ke zmírnění následků.

§ 8
Obsahové náležitosti dalších úkonů

1) Formulář pro hlášení údajů obsahuje
   a) identifikační údaje poskytovatele regulované služby včetně výčtu jím poskytovaných regulovaných služeb,
   b) kontaktní údaje,
   c) doplňující údaje.

2) Formulář hlášení provedení protiopatření obsahuje
   a) identifikační údaje poskytovatele regulované služby včetně výčtu jím poskytovaných regulovaných služeb,
   b) kontaktní údaje,
   c) doplňující údaje relevantní s ohledem na obsah protiopatření,
   d) identifikace protiopatření,
   e) informaci o provedení protiopatření a jeho výsledku.

3) Formulář hlášení provedení nápravného opatření obsahuje

a) identifikační údaje poskytovatele regulované služby včetně výčtu jím poskytovaných regulovaných služeb,
b) kontaktní údaje,
c) doplňující údaje relevantní s ohledem na obsah nápravného opatření,
d) identifikace nápravného opatření,
e) informaci o provedení nápravného opatření a jeho výsledku.

4) Formulář žádosti o výmaz poskytovatele regulované služby z evidence poskytovatelů regulovaných služeb obsahuje
a) registrační údaje poskytovatele regulované služby,
b) odůvodnění žádosti o výmaz.

5) Formulář žádosti o výmaz regulované služby obsahuje
a) registrační údaje poskytovatele regulované služby,
b) odůvodnění žádosti o výmaz.

6) Formulář hlášení informací o dodavatelích obsahuje
a) identifikační údaje poskytovatele regulované služby,
b) identifikační údaje dodavatele bezpečnostně významné dodávky,
c) identifikace bezpečnostně významné dodávky,
d) identifikace kritické části rozsahu,
e) identifikace regulované služby, k níž se váže bezpečnostně významná dodávka,
f) informace o přímém či nepřímém vztahu s dodavatelem.

ČÁST DRUHÁ
ÚČINNOST

§ 9
Účinnost

Tato vyhláška nabývá účinnosti dnem dd.mm.rrrr.

Ředitel:
Ing. Lukáš Kintr v. r.