Nový zákon o kybernetické bezpečnosti a Portál NÚKIB

Neveřejný web – Portál NÚKIB v2023 – Portál NÚKIB v2024 (v2025)

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

23. ledna 2024, Zlín

TLP:CLEAR

Tomáš Pekař
Vládní CERT, NÚKIB

1. NÚKIB, Vládní CERT a jeho role
2. Neveřejný web (v2021) – Portál NÚKIB (v2023)
3. Nový zákon o kybernetické bezpečnosti (nZKB)
4. Portál NÚKIB (v2024/2025)

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB a Vládní CERT

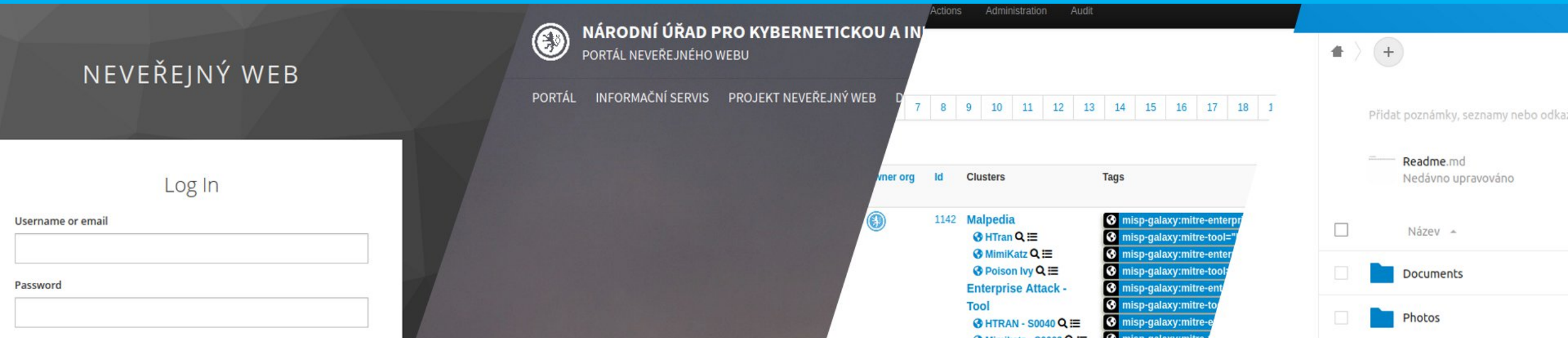
- Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je ústředním správním orgánem pro **kybernetickou bezpečnost** včetně ochrany utajovaných informací…

- Součástí Úřadu je i **Vládní CERT**, jehož úkoly jsou zejména:
  - Příjem hlášení o kybernetických bezpečnostních incidentech
  - Vyhodnocení informací o KBU a KBI z KII, informačního systému základní služby, VIS a dalších informačních systémů veřejné správy
  - Poskytování metodické podpory a pomoci
  - Poskytování součinnosti při výskytu KBI a KBU
  - Provádění hodnocení zranitelností v oblasti kybernetické bezpečnosti
  - A další úkoly ze ZoKB

- Úkolem Vládního CERT je tak zejména **pomáhat** (primárně povinným osobám) a **poskytovat informace** pro zabezpečení informační infrastruktury (upozornění na hrozby a zranitelnosti)

~~Neveřejný web~~ Portál NÚKIB

Neveřejný web je (byl) platformou Národního úřadu pro kybernetickou a informační bezpečnost, jehož prostřednictvím plní (plnil) NÚKIB některé jemu svěřené úkoly v oblasti kybernetické bezpečnosti.



NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Portál NÚKIB v2023 (1)

- Prostřednictvím Portálu plní NÚKIB některé jemu svěřené povinnosti a úkoly v oblasti KB

- Účelem této platformy je především sdílení informací k zabezpečení kybernetického prostoru mezi NÚKIB a následujícími orgány či osobami:
  1. spadajícími do působnosti NÚKIB,
  2. kterým NÚKIB na základě ZoKB poskytuje služby či spolupracuje v oblasti KB,
  3. partnery NÚKIB, jako jsou orgány a osoby působící v oblasti KB,
  4. vykonávajícími působnost v oblasti KB v zahraničí.

Upozorňujeme na hrozbu Terrapin útoku mířícího na SSH protokol

Na konci prosince 2023 došlo ke zveřejnění nového druhu útoku mířícího na SSH protokol – útok Terrapin, který využívá zranitelnosti CVE-2023-48795 (CVSS 5.9). Jedná se o prefix truncation attack, kdy útočník manipuluje daty při ustanovování komunikace tzv. handshake. Tím zapříčiní použití méně bezpečných algoritmů a deaktivaci některých bezpečnostních protiopatření.

Důležitým předpokladem je, aby byl útočník v pozici MitM (Man in the Middle). Spojení musí být zároveň zabezpečeno šifrou ChaCha20-Poly1305 nebo jakoukoliv CBC šifrou v kombinaci s Encrypt-then-Mac, které jsou velmi rozšířené.

V prostředí internetu je složité dostat se do pozice MitM. Proto útočníci často kompromitují síťovou infrastrukturu a vyčkávají na okamžik, kdy se objeví podobné zranitelnosti, aby mohli do infrastruktury proniknout hlouběji.

Bezpečnostní organizace Shadowserver Foundation nalezla rozsáhlým skenováním internetu skoro 11 milionů zranitelných SSH serverů. Informaci sdílela např. na sociální síti X (https://x.com/Shadowserver/status/1742482640815419653?s=20). Neznamená to, že jsou všechny tyto servery v nebezpečí, ale poukazuje to na rozsáhlost zranitelnosti.

Skener zranitelnosti na Terrapin útok od Ruhr-Universität Bochum: https://github.com/RUB-NDS/Terrapin-Scanner.

Mitigace

Většina vývojářů SSH klientů již vydala bezpečnou verzi, na kterou doporučujeme aktualizovat server i klienta. U některých se ale zatím jedná o beta-verzi např. WinSCP. Podrobný přehled zde: https://terrapin-attack.com/patches.html.

Pokud ještě není vydána aktualizace, doporučujeme v konfiguraci SSH pro klienta i server zakázat používání šifry Chacha20-Poly1305, jakékoliv Encrypt-then-MAC (EtM) a ověřit, že nejsou využívány žádné aes(128|192|256)-cbc. Příklad zakázání v /etc/ssh/ssh_config:

```
Ciphers -chacha20-poly1305@openssh.com
```

K nastavování konfigurace SSH doporučujeme přistupovat s opatrností, protože nesprávná konfigurace může způsobit ztrátu spojení se serverem.

Zdroje

- SSH Prefix Truncation Vulnerability Used in Terrapin Attacks (CVE-2023-48795) – Qualys ThreatPROTECT
- SSH shaken, not stirred by Terrapin downgrade vulnerability • The Register
- SSH protects the world's most sensitive networks. It just got a lot weaker | Ars Technica
- Nearly 11 million SSH servers vulnerable to new Terrapin attacks (bleepingcomputer.com)
- SSH Protocol Flaw CVE-2023-48795 Terrapin Attack: All You Need To Know (jfrog.com)
- CVE-2023-48795- Red Hat Customer Portal

KLASIFIKACE

TLP:CLEAR

AUTOR

Národní úřad pro kybernetickou a informační bezpečnost

DATUM

05. 01. 2024

OBSAH

Mitigace
Zdroje

REAKCE

Zatím žádné reakce na článek

REAGOVAT

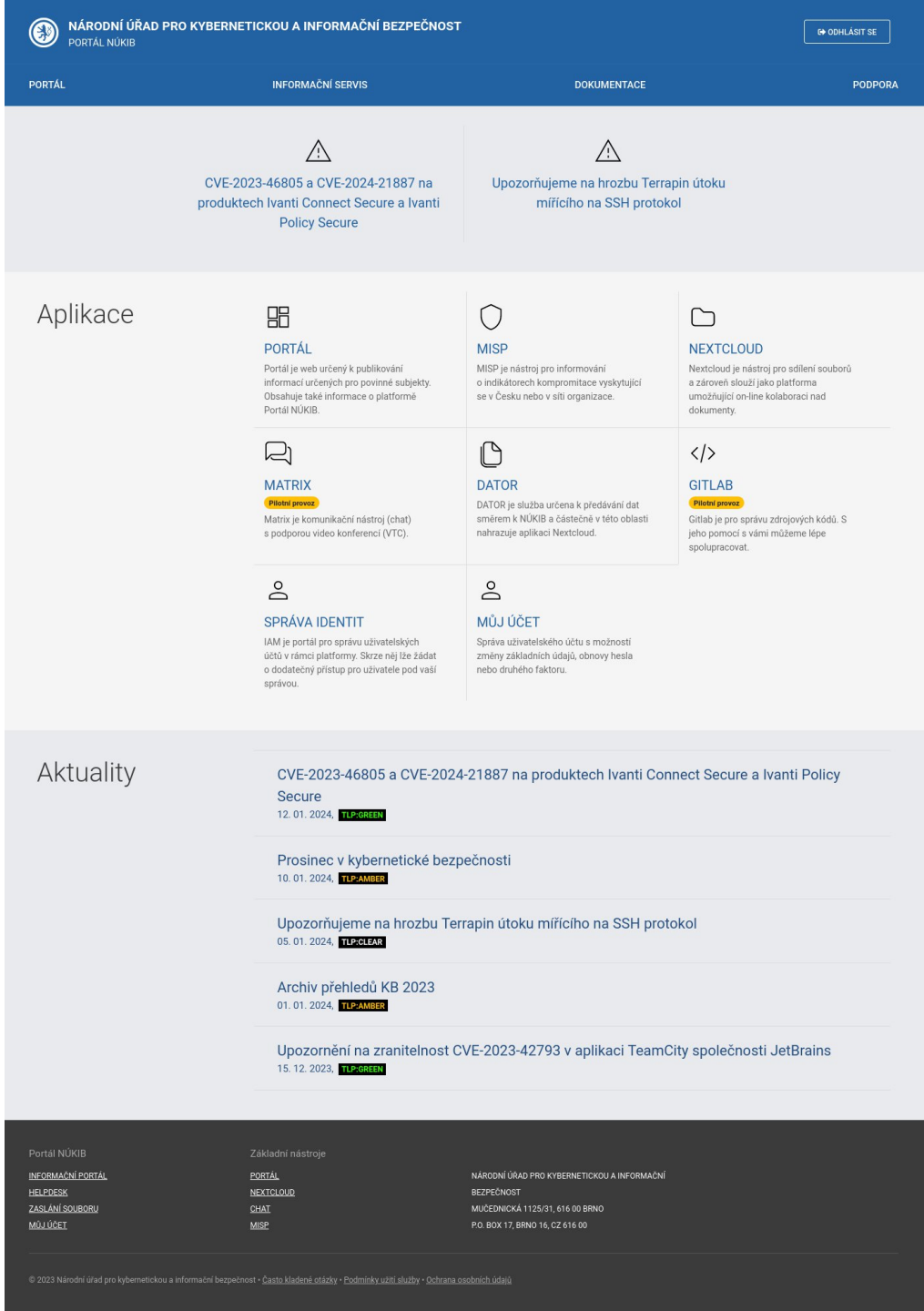
NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Portál NÚKIB v2023 (2)

- NÚKIB platformu (~~Neveřejný web~~/Portál NÚKIB) pro sdílení informací provozuje **od poloviny roku 2021**
- Koncem roku 2023 byl Neveřejný web **„rebrandován“ na Portál NÚKIB**, právě vzhledem k plánům rozšířit tuto platformu o nové administrativní funkce v souvislosti s nZKB

- Nyní jsou do Portálu zapojeny primárně organizace spravující systémy typu KII a pracuje se na zapojení organizací spravující systémy typu VIS
- Registrace do Portálu je zcela **dobrovolná**

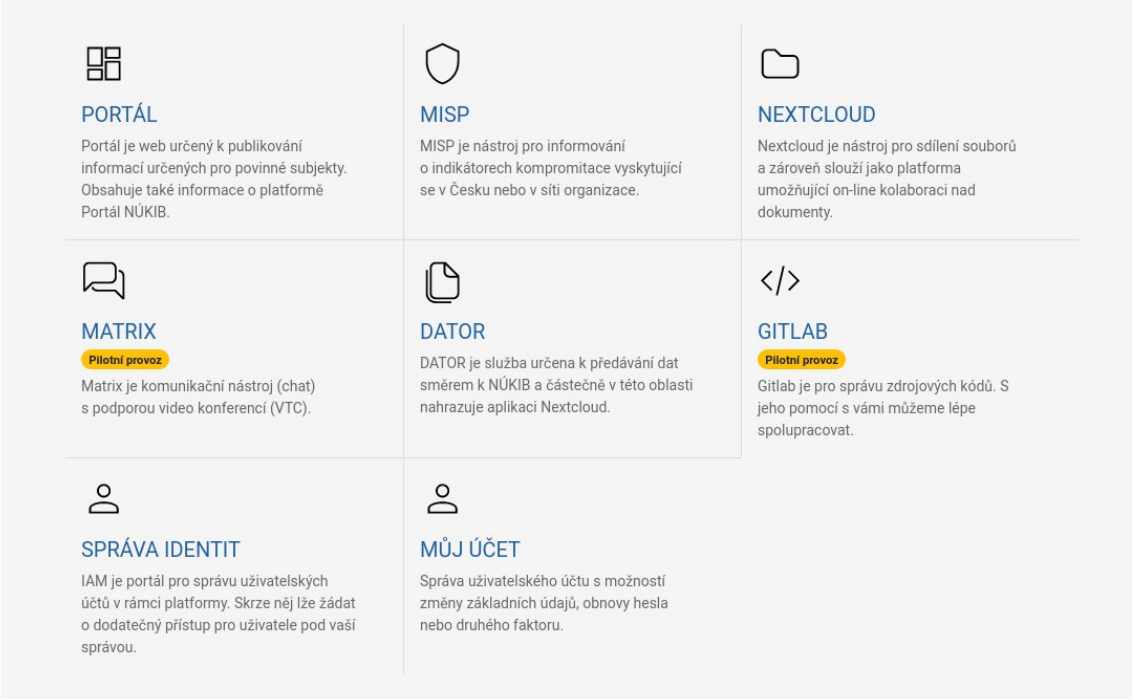


NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Portál NÚKIB v2023 (3)

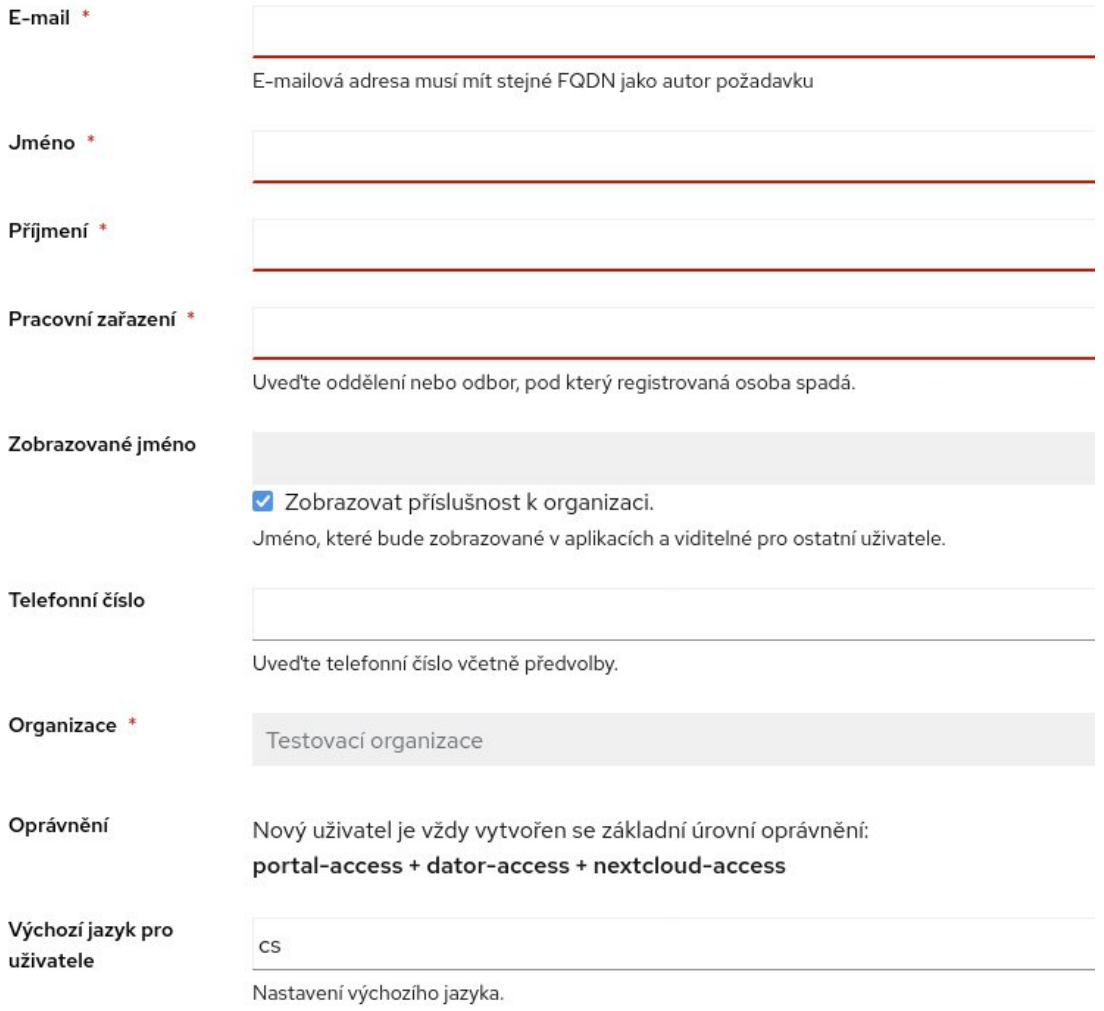
- **PORTÁL** – slouží jako rozcestník (uživatel vidí, jaké služby Portálu jsou mu přístupné); slouží jako informační portál (aktuality, analýzy nebo aktuální hrozby)
- **MISP** – sdílení informací o hrozbách; sdílení indikátorů kompromitace (IoC)
- **NEXTCLOUD** – sdílení souborů a dat; nástroj pro podporu spolupráce
- **MATRIX** – služba pro okamžité zasílání zpráv a služba pro videokonference (pilotní provoz od Února 2024)



Portál NÚKIB v2023 (4)

- **DATOR** – slouží k předávání dat výhradně NÚKIB a data předávaná pomocí služby Dator je možné zaslat pouze zaměstnancům Úřadu; slouží pro předání dat z incidentů (logy, obrazy disků, obrazy paměti), vzorků škodlivého kódu nebo jiných dat

- **SPRÁVA IDENTIT** – slouží pro správu identit a řízení přístupu; každá organizace si řídí správu uživatelských účtů sama



Nový zákon o kybernetické bezpečnosti nabude účinnosti

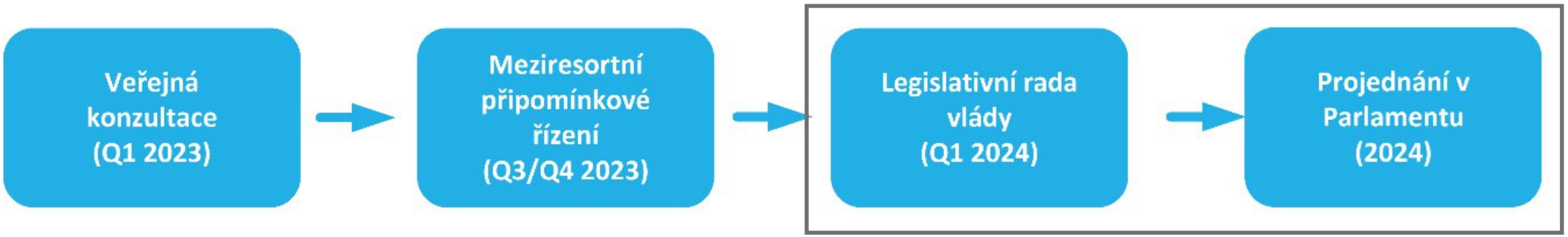
18. října 2024

(návrh zákona předložen Legislativní radě vlády 22. prosince 2023)

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Nový zákon o kybernetické bezpečnosti – sumarizace

- Ke konci roku 2024 vejde v platnost nová regulace – nový zákon o kybernetické bezpečnosti – navrhovaná platnost zákona: 18. října 2024
- Nová regulace dopadne přibližně na více jak 6 000 organizací – jste jednou z nich?
- Dva režimy – **režim nižších nebo vyšších povinností** pro regulované organizace
- Povinnost provést registraci **do 30 dnů** ode dne, kdy subjekt zjistí, že naplnil kritéria pro identifikaci regulované služby; nejpozději však do 90 dnů ode dne, kdy k naplnění kritérií pro identifikaci regulované služby došlo



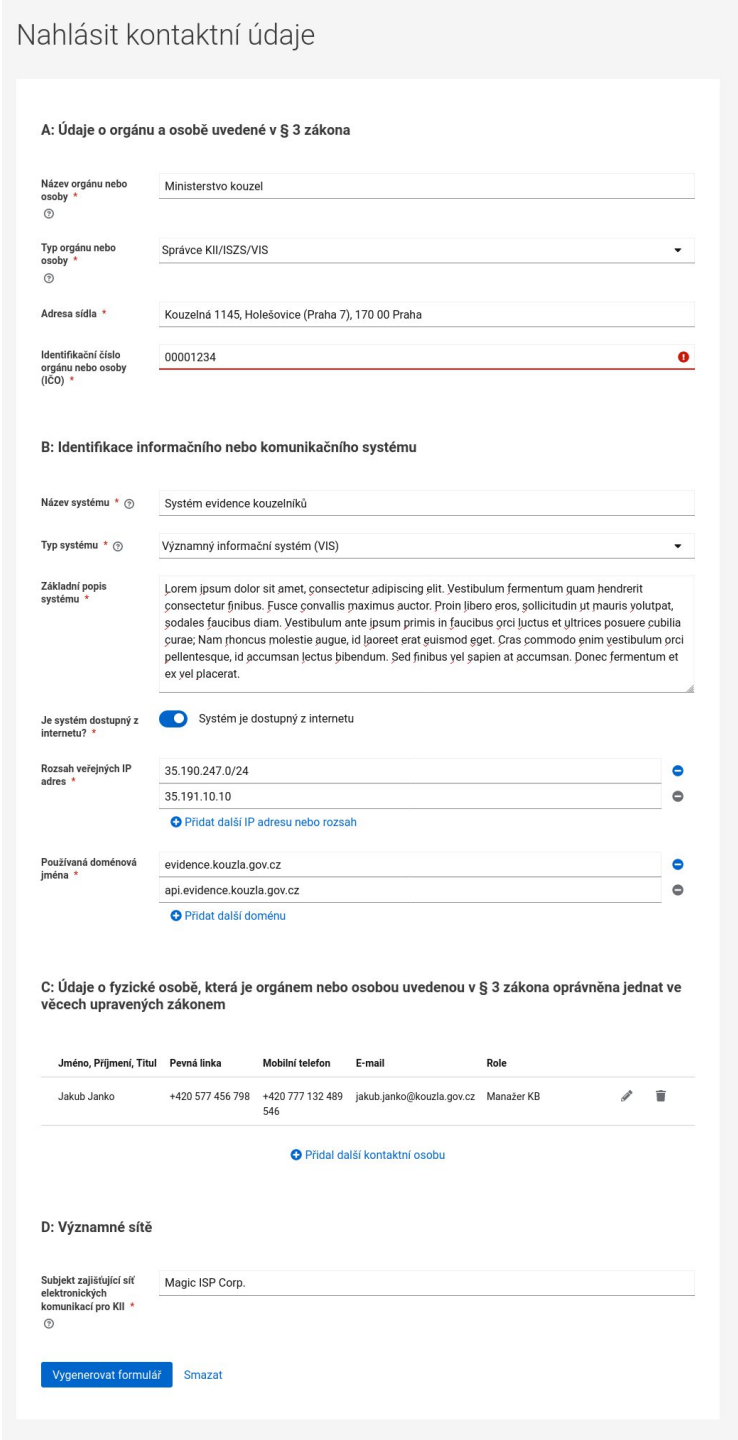
NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

nZKB a Portál NÚKIB v2024

- Primárním nástrojem pro veškerou komunikaci ze strany poskytovatelů regulovaných služeb s NÚKIB **bude Portál NÚKIB**

- Úkony prováděné skrze Portál NÚKIB:
  - registraci regulované služby podle § 8 zákona,
  - změnu registrace regulované služby podle § 9 zákona,
  - žádost o výmaz z evidence regulovaných služeb podle § 11 zákona,
  - hlášení údajů podle § 12 zákona,
  - hlášení incidentů podle § 16 a 17 zákona,
  - hlášení provedení protiopatření podle § 21 zákona,
  - hlášení informací o dodavatelích podle § 33 zákona, a
  - hlášení provedení nápravného opatření podle § 59 zákona.



Poskytovatel regulované služby povinen provádět **výlučně elektronicky** s využitím dálkového přístupu prostřednictvím formulářových podání.

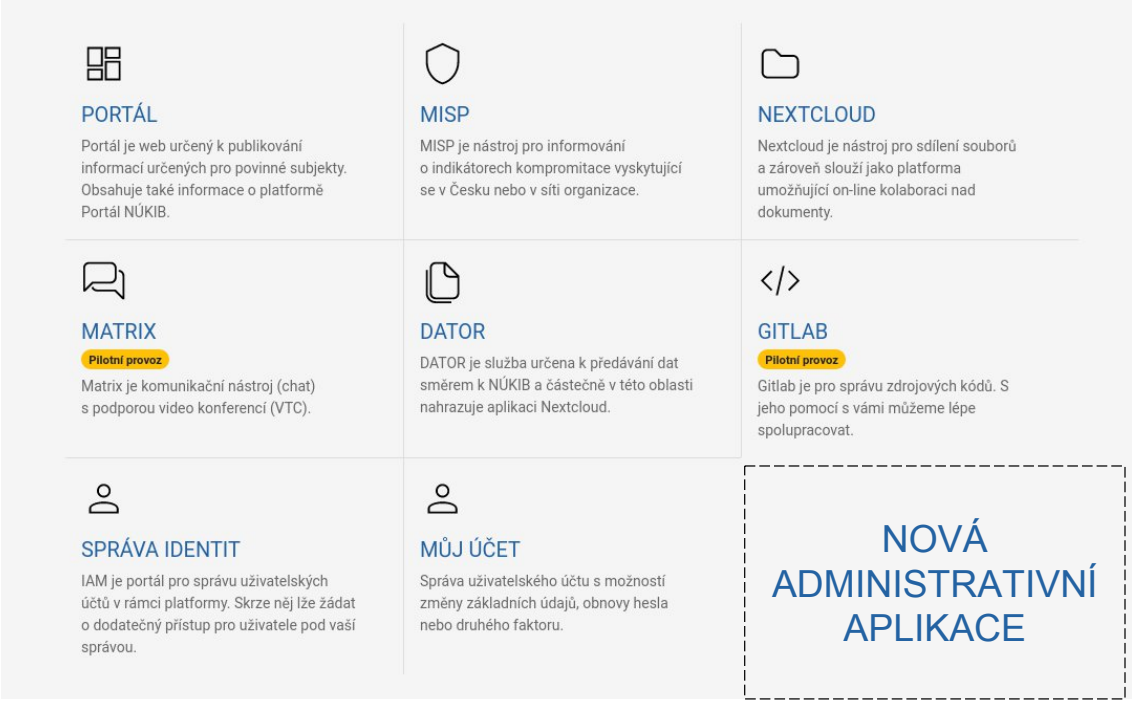
Jiným způsobem lze tyto úkony provést pouze tehdy, připouští-li to odpovídající ustanovení tohoto zákona a není-li z objektivních příčin možné využít k provedení úkonu Portál Úřadu (Portál NÚKIB).

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Portál NÚKIB v2024/2025 (1)

- Portál NÚKIB by měl sloužit jako **samoobslužný** portál, jehož prostřednictvím by měly povinné osoby snadno provádět veškeré standardizované úkony předpokládané návrhem zákona

- Fakticky dojde k rozšíření stávající platformy o **nové funkcionality** stávajících aplikací, **nový administrativní modul** a také **novou veřejnou část platformy** (nyní je platforma plně přístupná pouze autorizovaným uživatelům)



Identita občana

CAAIS

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Portál NÚKIB v2024/2025 (2)

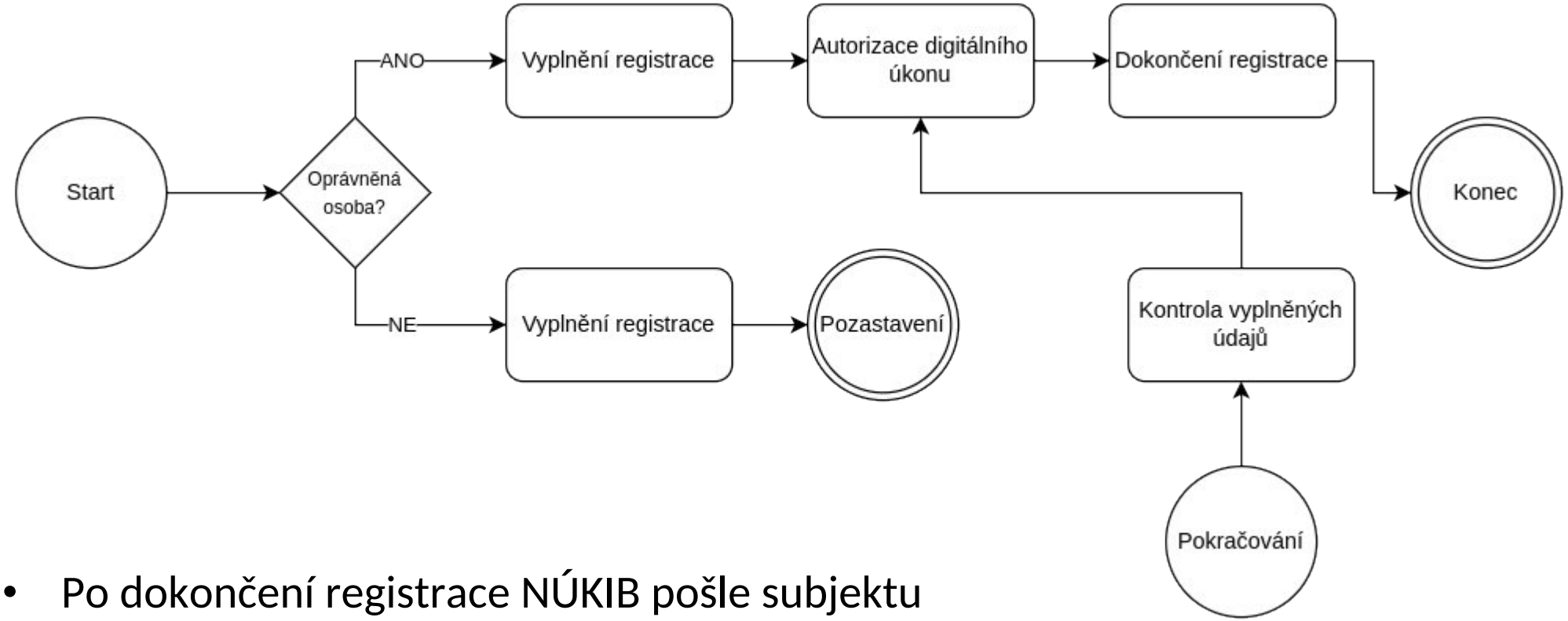
- Portál bude nově rozdělen na veřejnou a neveřejnou část:
  - Veřejná část bude obsahovat základní informace o Portálu NÚKIB (popis, návody), veřejně dostupné elektronické formuláře a další informace
  - Neveřejná část bude přístupná pouze autorizovaným uživatelům na základně určení pověřené osoby (správce uživatelských účtů), neveřejná část bude obsahovat stejné formuláře jako veřejná část, veškeré dostupné informace budou předvyplněny

- Cílem nového administrativního modulu je automatizovat co možná nejvíce úkonů předpokládaných návrhem zákona

- Využití některých funkcionalit Portálu a poskytování vybraných informací (např. informace o instalovaném SW a verzích) bude stále dobrovolné, nicméně tyto informace mohou lépe zacílit varování před hrozbami

- **Aplikační rozhraní** pro práci s Portálem? Ano, ale pravděpodobně až ve verzi v2025

Příklad: registrace regulované služby

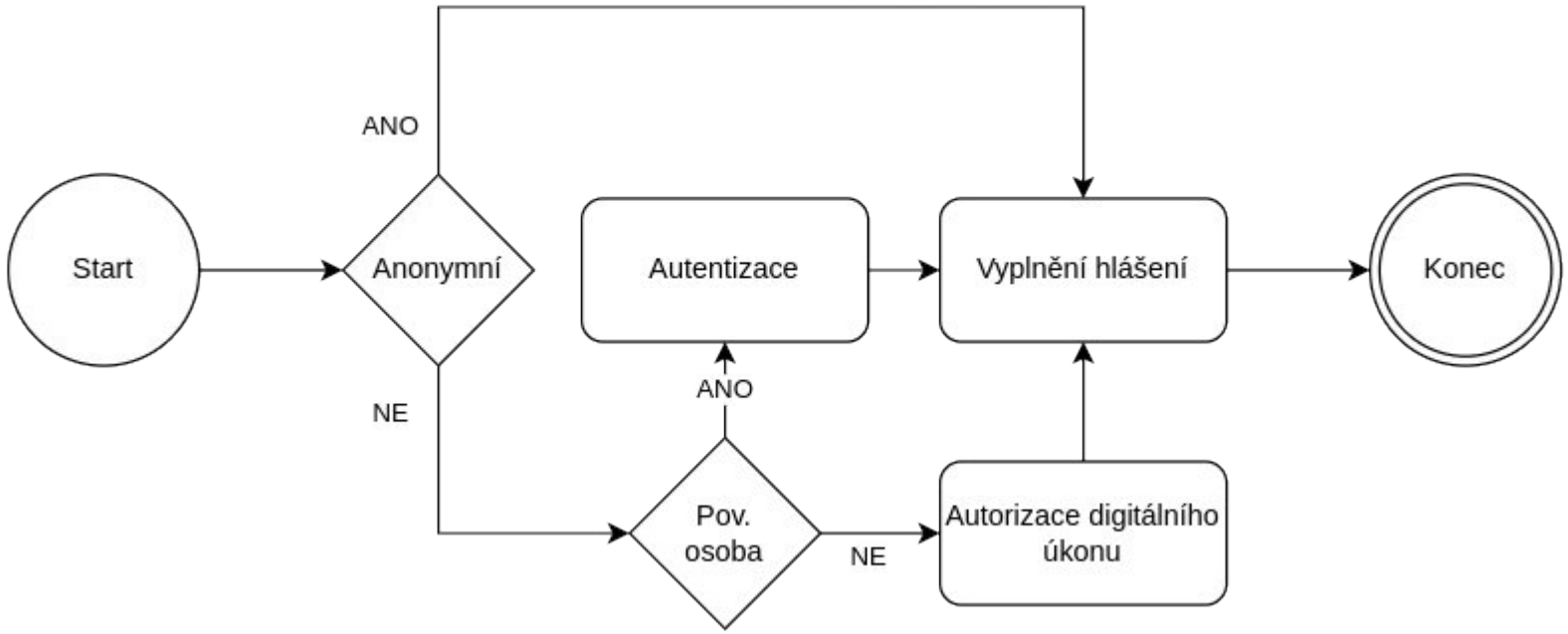


- Po dokončení registrace NÚKIB pošle subjektu vyrozumění o zápisu regulované služby a organizaci jsou zřízeny první uživatelské účty s přístupem do Portálu NÚKIB (další účty už si pak vytváří sama organizace)

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

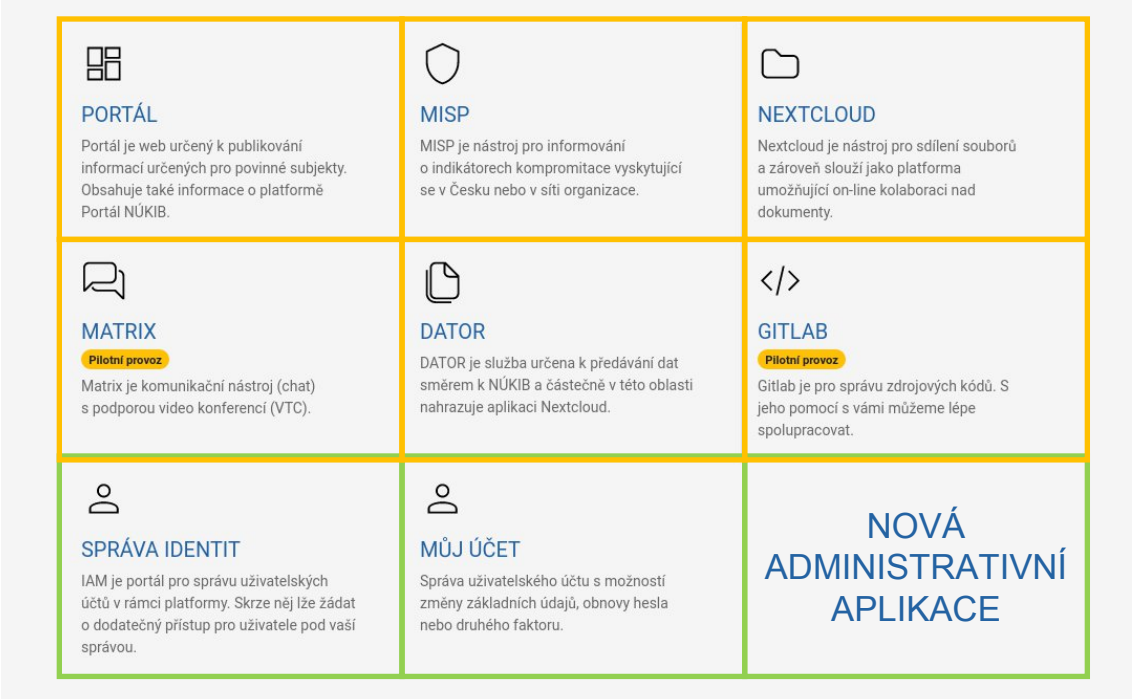
Příklad: hlášení incidentu



- NÚKIB poskytovateli regulované služby ve vyšším režimu po prvotním hlášení oznámí (skrze Portál), zda má incident významný dopad (pokud je incident bez významného dopadu, tímto krokem hlášení pro organizaci končí).
- Bez zbytečného odkladu, nejpozději do 72 hodin (poskytovatel služeb vytvářejících důvěru do 24 hodin) po zjištění incidentu poskytovatel regulované služby aktualizuje informace z prvotního hlášení (opět již skrze Portál).

Režim nižších povinností a Portál NÚKIB

- Portál NÚKIB bude plně přístupný všem uživatelům organizací spadajících do režimu vyšších povinností
- Nyní ještě není rozhodnuto, zda budou mít uživatelé organizací spadajících do režimu nižších povinností přístupné všechny aplikace platformy
- Přístupné bude určitě rozhraní nové administrativní aplikace a systémy pro správu uživatelských účtů



I přesto, že máme plný backlog...

...budeme rádi za vaše podněty.

Zavádění nových funkcionalit Portálu NÚKIB

- V rámci Portálu NÚKIB chceme vylepšit sběr zpětné vazby a upravit stávající formuláře
- V průběhu roku 2024, předtím než vejde v platnost nový zákon, chceme nasadit a zpřístupnit dílčí prototypy za účelem získání zpětné vazby
- Některé prototypy budou veřejně přístupné, jiné budou k dispozici pouze pro stávající uživatele Portálu NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB

HLAŠENÍ KONTAKTNÍCH ÚDAJŮ

Prvotní hlášení

A: Údaje o orgánu a osobě uvedené v § 3 zákona

Název orgánu nebo osoby:	Ministerstvo kouzel
Typ orgánu nebo osoby:	Správce KII/ISZS/VIS
Adresa sídla:	Kouzelná 1145, Holešovice (Praha 7), 170 00 Praha
Identifikační číslo orgánu nebo osoby (IČO):	00001234

B: Identifikace informačního nebo komunikačního systému

Název systému:	Systém evidence kouzelníků
Typ systému:	Významný informační systém (VIS)
Základní popis systému:	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vestibulum fermentum quam hendrerit consectetur finibus. Fusce convallis maximus auctor. Proin libero eros, sollicitudin ut mauris volutpat, sodales faucibus diam. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia curae; Nam rhoncus molestie augue, id laoreet erat euismod eget. Cras commodo enim vestibulum orci pellentesque, id accumsan lectus bibendum. Sed finibus vel sapien at

nukib.gov.cz
kariera.nukib.gov.cz
nis2.nukib.gov.cz

Dotazy?

Tomáš Pekař

Referent bezpečnosti státu, Vládní CERT

E-mail: Tomas.Pekar@nukib.gov.cz
Telefon: +420 721 911 705
PGP: 7CB1 C024 7CA1 1617 43AE 54EB 2FFF 9AE6 C5DA 5635