Interní vývoj Portálu NÚKIB

Lenka Ondrysková

Petra Kajánková

Jakub Onderka

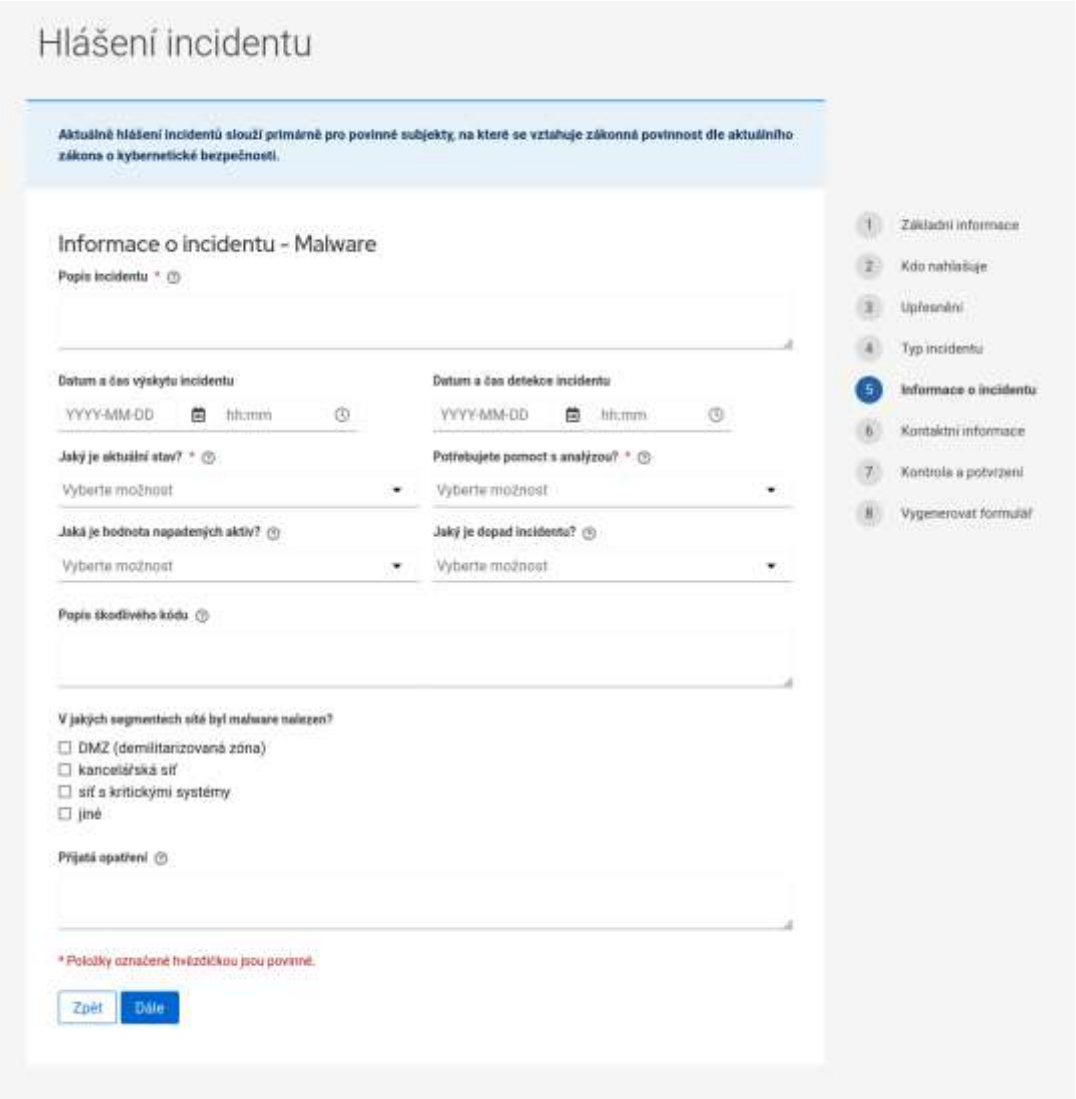
18.5.2026

Nový zákon o kybernetické bezpečnosti

- Od 1. listopadu 2025 se zákonné úkony provádí pouze prostřednictvím Portálu NÚKIB.

- Regulované organizace musí skrze Portál provádět následující:
  - ohlášení regulované služby,
  - hlášení údajů podle § 11 zákona
  - nebo hlášení incidentů podle §§ 16 a 17 zákona.

- Portál nicméně slouží nejen k plnění povinností, ale také ke sdílení informací.

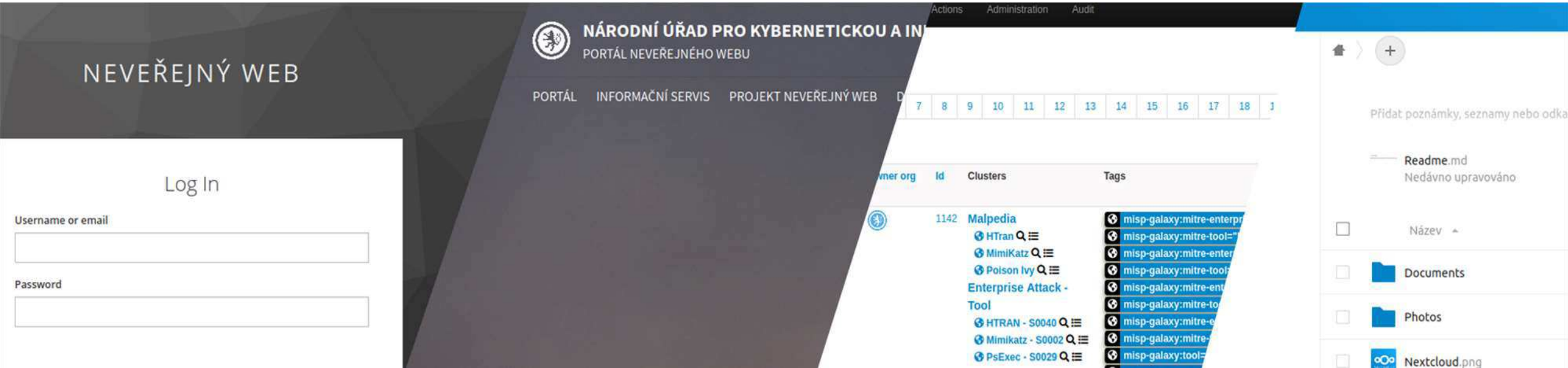


Vize Portálu NÚKIB

Komunikační a informační platforma usnadňující spolupráci mezi NÚKIB a zapojenými organizacemi s cílem zajistit **bezpečný a odolný kyberprostor** České republiky.

Proč jsme šli cestou interního vývoj?

- Již existující platforma Neveřejný web
- Interní tým vývojářů na NÚKIB
- Negativní zkušenost se spoluprací s dodavateli
- Zákon ani vyhlášky nebyly ve finální podobě – jak vytvořit specifikaci?



Interní vývoj na příkladu hlášení incidentů

- Konec 2022 – schválena evropská směrnice NIS2
- Konec 2023 – rebranding Neveřejného webu na Portál NÚKIB
- Červenec 2024 – schválení návrhu NZKB vládou
- 1. 8. 2024 – spuštění pilotní veřejné části Portálu jako náhrada původního informačního webu o směrnici NIS2

Přípravná fáze

- 11. 3. 2025 - nový Portál jako příprava na nové funkcionality
- Duben 2025 – schválení NZKB PSP

Implementace

- Srpen 2025 – vyhlášení NZKB ve Sbírce zákonů
- 1. 11. 2025 – účinnost NZKB a spuštění ohlašování regulované služby

Publikace

- 11. 2. 2026 – hlášení incidentů a správa regulovaných služeb

Rozvoj

- Dosud

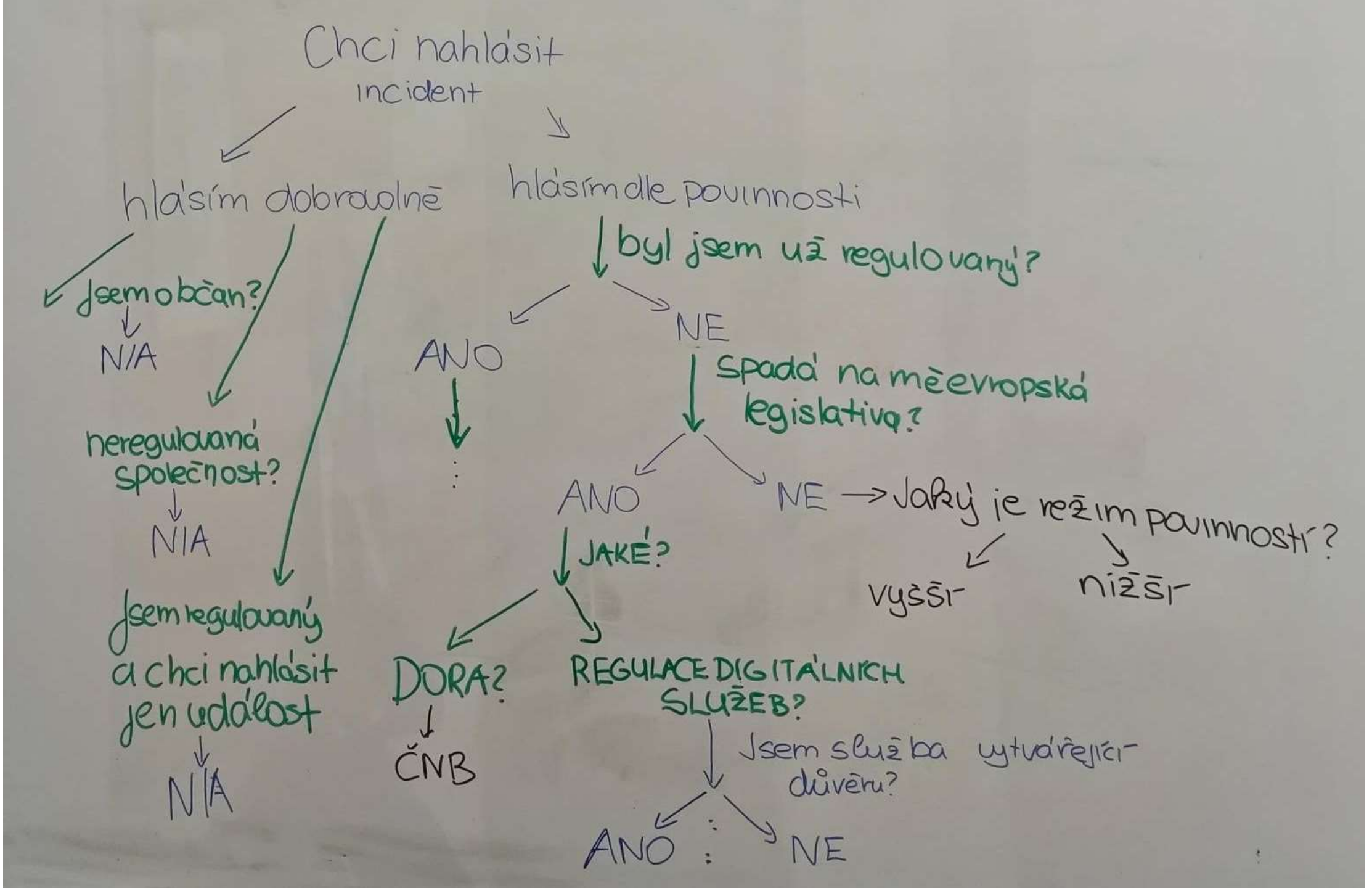
Přípravná fáze

Ujasnění specifik a komunikace

- Odbor regulace
  - Interpretace zákona, kontrola souladu
- Návrh procesu (první verze)
  - Návrh struktury incidentů
- Vládní CERT
  - Konzultace návrhu a ověření přístupu z pohledu praxe
- Úpravy návrhu
  - Zjednodušení pro uživatele, povinné subjekty a veřejnost
- Finální validace a kontrola souladu se zákonem

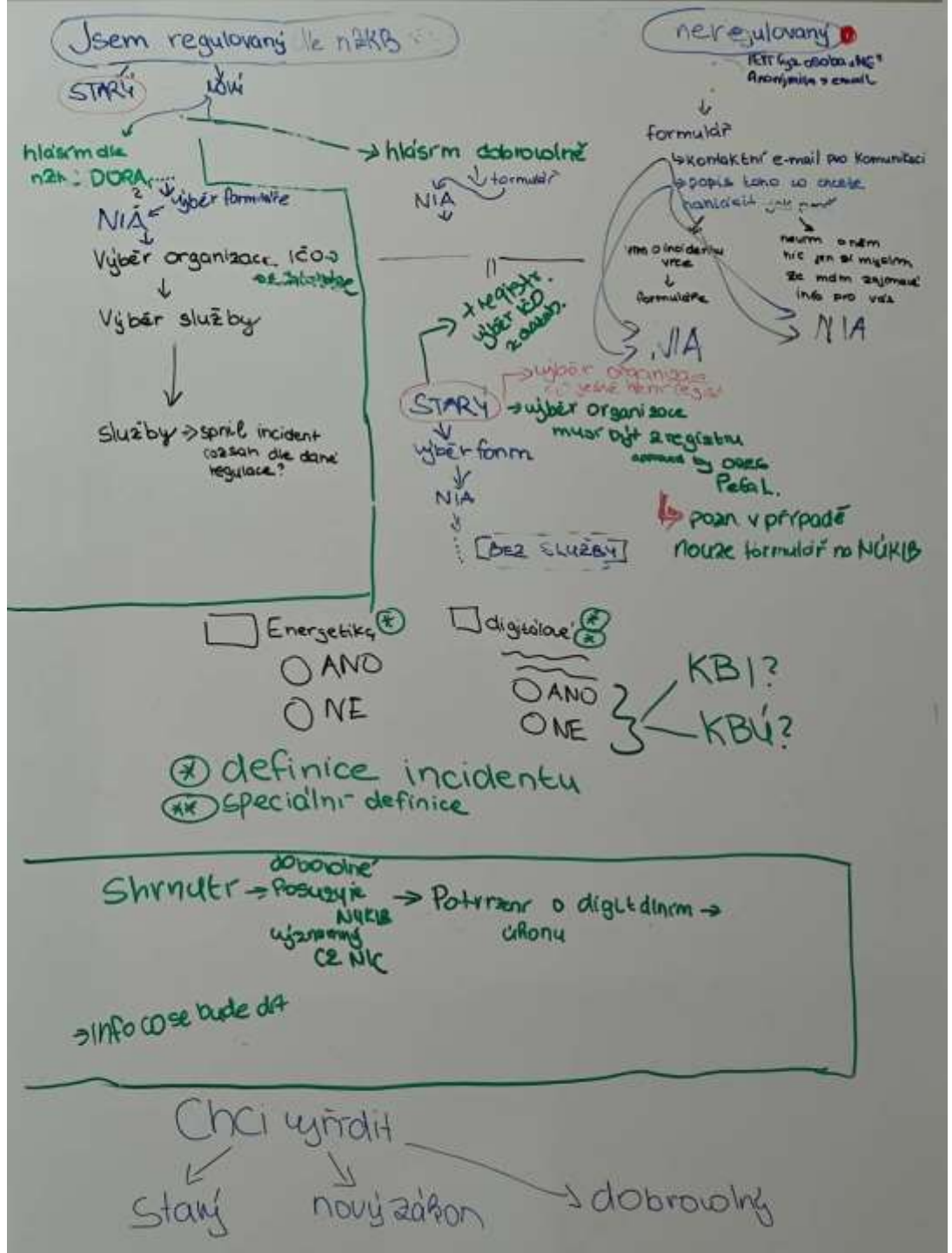
NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost



NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost



Interní vývoj

Výhody

- Reakce na nové požadavky a aktuální potřeby – vysoká flexibilita
- Můžeme zapracovat měnící se specifikaci na systém vycházející z legislativy

Nevýhody

- Náročná koordinace a komunikace napříč NÚKIB - zvýšená organizační zátěž na tým
- Nutnost mezioborových znalostí členů týmů

Implementace

Tvorba formulářů

- Implementace řešení
  - Naprogramování a technické zpracování návrhu
- Tvorba podpůrných materiálů
- Interní zpětná vazba
  - Testováno interními členy týmu, Vládní CERT
  - Ověřování funkcionalit a identifikace chyb
- Vliv evropské legislativy
  - Doplnění specifických procesů

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Work packages

+ Create | Include projects 1

TYPE	ID	SUBJECT
SPRINT GOAL	5620	Testování workflow hlášení incidentů
BUG	5625	Incidenty - co chybi v pdf
BUG	5626	Incidenty - co chybi ve formulari
BUG	5627	Incidenty - co chybi v textu e-mailu
BUG	5628	Incidenty - co chybi ve workflow

+ Create new work package

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Nadřazený: Testování workflow hlášení incidentů

BUG Incidenty - co chybi ve formulari

- [ ] ~~chybi otaznicek/vysvetleni u prijata opatreni (novy zakon/ransomware) --- predano --- není nikde, uzavírám za RO není potřeba~~
- [x] Pri pridavani prilohy - chybi info o omezeni velikosti ---- predáno RO
  - [x] info je na úvodní stránce, ale už není přímo u nahrávání souboru
- [x] V textech emailů jsou chybně Assets jako Incident
- [x] Pokračovací + záverecné -- do id tiketu jdou psát i písmena - vyresime v dalsi iteraci, todo BUG
- [x] Nahradit klíče polí jejich textem ???????? PŘEKLAD PROSÍM!
- [ ] ~~dá se zadat datum zjištění i výskytu v budoucnosti~~ - vyresime v dalsi iteraci low priprity BUG
- [x] Phishing - malfile dropper -> nedava smysl Specifika k phishingu/Stahli, zobrazili či spustili někteří uživatelé škodlivou přílohu? a v poli je defaultne je uvedno 'Pocet '
- [x] Útoky na perimetr - formulář nejde odeslat pokud vyberu 'Ano' a potom přepnu na 'Ne' u otázky jestli došlo k průniku (viz obrázek) ---- predano
- [ ] ~~přijatá opatření se dají vyplnit mezerou (" "), v PDF je potom "Nevyplněno"~~ - vyresime v dalsi iteraci, low priority BUG
- [x] Jiny typ (novy zakon) - vypnuje invalid date i kdyz se vyplni validni datum -> nepodarilo se odeslat formular
- [x] Jiny typ - pocet zasazenych lidi -1 asi? zpusobi chybu a nemoznost dokoncit formular -- fix nespadne už
- [ ] ~~oznameni -> vybral jsem oznameni, vybral spolecnost, pak je kde je kontakt je nazev formulare 'Průběžná zpráva (oznámení)', melo by byt pouze oznameni ne? --- predano~~ existije jen jeden formulář
- [x] na konci kde je moznost pridat prilohu je uvedena moznost jen zip,7zip a ne pdf (to je uvedneo jen na zacatku tech formularu) --- predano
- [x] Dobrovolne hlaseni za obcana konci chybou a neodesle se (ID chyby: aa30225760ec4dcf89d5e55d7e5cac75)
  - [x] Taktez za organizaci
- [x] DDos (stary zakon) nedovoli pokracovat dokud nedame Ano na oboje: "Došlo k výpadku zacíleného systému?" a "Aktivně spolupracujete s poskytovatelem na mitigaci DDoS?"
  - [x] Formular ale stejne nejde dokoncit ID chyby: 06d4b77c0fe440f4beec1ccd162394af
- [ ] ~~UI: textová pole jsou roztáhnout do nekonečna (viz obrázek)~~ - feature?
- [ ] ~~DDos, nizsi rezim, Oznámení -> ve shrnuti je uvedeno Navazuji hlaseni, melo by byt oznameni at je to jednotne.~~
- [x] Nedaří se provést validaci formuláře -- oznámení + průběžné + finální
- [ ] ~~Format datumu ve vyslednem PDF se lisi od formatu datumu ve shrnuti formulare (Novy zakon, vyssi, ransomware)~~ -> 3.2.. a 2/3/.... - vyresime v dalsi iteraci, BUG
- [x] chybí číslo jednací (viz obrázek) --- @jiri.valasek@nukib.gov.cz
- [x] jiny typ incidentu novyZ => Tento formulář slouží pro nahlášení kybernetického **bezpečnosntního** incidentu, který nelze hlásit využitím typových formulářů.
- [ ] ~~chybějící mezera v příloze --- text + "příloha"~~ - necham na dalsi iteraci, BUG
  - [ ] ~~Veta na dva radky - text hodnoty je v prvnim radku~~ - vyresime v dalsi iteraci, je to feature nebo bug?
- [x] u dobrovolneho hlaseni, pri zadani spravneho ICO, nedoplni to jmeno spolecnosti ani v pdf
  - [x] u dobrovolneho hlaseni pro organizaci, se v textu e-mailu v RT nezobrazi obsah formulare
- [x] u průběžných oznámení funguje ID jen jako číslo, pokud někdo zadá ID i s '#' tak se ticket nepřiřadí
- [ ] ~~po smazani povinneho pole dojde ke chvilkove validaci a je mozne v tomto okne dat dale, cimz se rozbije fomular~~ - budeme muset resit, ale ted se odlozi - BUG
- [ ] ~~japonske znaky se nepropisou do pdf~~ BUG

Interní vývoj

Výhody

- Odhalení chyb během testování a možnost opravy před spuštěním
- Změny oproti původní specifikaci bez dodatečných nákladů
- Důraz na uživatelskou přívětivost v celém procesu

Nevýhody

- Omezená kapacita týmu - změnami se posouvají jiné činnosti
- Menší zakázky na dodavatele nejsou vždy řešením
- Uživatelská přívětivost přináší nároky na návrh systému

Hlášení incidentu

Hlášení incidentu dle starého zákona

Hlášení kybernetického bezpečnostního incidentu podle starého zákona č. 181/2014 Sb.

Hlášení incidentu dle nového zákona

Hlášení kybernetického bezpečnostního incidentu podle nového zákona č. 264/2025 Sb.

Hlášení incidentu

Hlášení incidentu

Hlášení kybernetického bezpečnostního incidentu nebo události podle zákona o kybernetické bezpečnosti.

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Hlášení kybernetického bezpečnostního incidentu

Tato stránka slouží k **podání hlášení kybernetického bezpečnostního incidentu** podle zákona o kybernetické bezpečnosti.

Povinné hlášení incidentu pro regulované subjekty dle zákona

Použijte formulář Hlášení podle starého zákona, pokud:

- jste byli **regulovaní již dle starého zákona** - tento způsob hlášení je pro vás přechodně možný po dobu jednoho roku od doručení rozhodnutí o registraci podle nového zákona,
- na tato hlášení se nevztahují lhůty nového zákona,
- původně regulované subjekty mohou incident nahlásit i podle nového zákona, dle své volby.

Použijte formulář Hlášení podle nového zákona, pokud:

- jste se stali **regulovanými dle nového zákona** o kybernetické bezpečnosti - v tomto případě se **musíte řídit pravidly** dle **nového zákona**.
- jste byli **regulováni dle starého zákona** a **dobrovolně** volíte hlášení podle nového zákona.

Hlášení podle starého zákona

Hlášení kybernetického bezpečnostního incidentu podle starého zákona č. 181/2014 Sb.

Hlášení podle nového zákona

Hlášení kybernetického bezpečnostního incidentu podle nového zákona č. 264/2025 Sb.

Publikace

Příprava k publikaci

- Interní finální testování (2 dny)
  - Správné zařazení do front, zakládání spisů a ukládání osvědčení
  - Ověření funkčnosti, srozumitelnosti a uživatelské přívětivosti
- Finalizace navazujících procesů
  - Zpracování incidentů, spolupráce s CERT
- Příprava komunikace a odstávky
  - Dočasné omezení formulářů
- Go-live a první hlášení
  - První incident přijat do 15 minut, ověření funkčnosti

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Povinné hlášení incidentu pro regulované subjekty dle zákona

Použijte formulář Hlášení podle starého zákona, pokud:

- jste byli **regulovaní již dle starého zákona** - tento způsob hlášení je pro vás přechodně možný po dobu jednoho roku od doručení rozhodnutí o registraci podle nového zákona,
- na tato hlášení se nevztahují lhůty nového zákona,
- původně regulované subjekty mohou incident nahlásit i podle nového zákona, dle své volby.

Použijte formulář Hlášení podle nového zákona, pokud:

- jste se stali **regulovanými dle nového zákona** o kybernetické bezpečnosti - v tomto případě se **musíte řídit pravidly** dle **nového zákona**.
- jste byli **regulováni dle starého zákona** a **dobrovolně** volíte hlášení podle nového zákona.

Hlášení podle starého zákona

Hlášení kybernetického bezpečnostního incidentu podle starého zákona
č. 181/2014 Sb.

Hlášení podle nového zákona

Hlášení kybernetického bezpečnostního incidentu podle nového zákona
č. 264/2025 Sb.

Dobrovolné hlášení mimo zákonnou povinnost

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Typ nahlašovaného incidentu:

Ransomware

Útočník zašifroval anebo ukradl data a požaduje výkupné (u některých útoků nedochází k šifrování dat).

DDoS

Zahlcený server nebo služba vedoucí k omezení dostupnosti.

Malware

Nález škodlivého kódu v infrastruktuře, nestandardních procesů či podezřelých artefaktů

Phishing - malfile dropper

Podvodné e-maily s odkazy či přílohami, které stahují nebo spouštějí škodlivé soubory.

Phishing - credential harvester

Podvodné e-maily nebo stránky, které vyzývají k zadání hesla.

Útoky na perimetru

Útoky hrubou silou (bruteforce), invazivní skeny, exploitace zranitelností a další útoky po síti na exponované systémy.

Jiný typ incidentu

Nenašli jste vhodný formulář? Použijte tento.

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Ransomware

Tento formulář slouží pro nahlášení incidentu typu ransomware.

Jak vládní CERT hlášení incidentu řeší?

- V rámci řešení incidentu CERT plní roli koordinační autority na národní i mezinárodní úrovni.
- Náš tým je schopen poskytnout jak metodickou pomoc při zvládání krizových situací, tak analytickou pomoc v oblastech forenzní analýzy, analýzy síťového provozu, malware analýzy, CTI analýzy, analýzy bezpečnosti OT technologií či posouzení právních aspektů incidentu.
- Vaše hlášení incidentu zároveň přispívá do znalostní báze vládního CERT týmu. Díky tomu lze sledovat kyberbezpečnostní trendy ve větším měřítku. Umožňuje to také propojování jednotlivých případů mezi sebou, ať už v rámci trendů, globálních či sektorových událostí, nebo cílených útočných kampaní.

Kdy s incidentem pomáhá národní CSIRT?

- Na základě veřejnoprávní smlouvy jsou incidenty hlášené subjekty **v nižším režimu** primárně řešeny národním CSIRT týmem provozovaným sdružením CZ.NIC. V odůvodněných případech, zejména pokud to vyžaduje závažnost nebo charakter incidentu, lze do řešení zapojit také vládní CERT.

Jak předat data k analýze NÚKIBu?

- Menší soubory (do 5 MB) lze ve formátu (.zip, .7z, .pdf) nahrávat v rámci jednotlivých polí formuláře.
- Větší soubory (nad 5 MB) je třeba nahrát do služby DATOR skrze Portál NÚKIB. Služba DATOR je přístupná pro organizace, které mají zřízený účet v Portále NÚKIB. Pokud tento účet nemáte, tým CERT vám na základě vyplněného formuláře pošle potřebné informace pro zaslání souborů jinou cestou.

Položky označené hvězdičkou * jsou povinné. Kliknutím na tlačítko nápovědy ⓘ během vyplňování si zobrazíte více informací u požadovaných vstupních polí.

Dále

- Úvodní informace
- Výběr organizace
- Obecné informace k incidentu
- Detaily o aktivech
- Specifika k ransomwaru
- Shrnutí
- Odeslání a potvrzení

Interní vývoj

Výhody

- Kompletní přehled o fungování systému a úspěšnosti procesů
- Okamžitá reakce na chyby a provozní problémy

Nevýhody

- Nutnost sledovat, koordinovat a komunikovat odstávky
- Monitorování alertingu představuje další zátěž pro tým

Rozvoj

Další vývoj a zlepšování

- Zpětná vazba od uživatelů
- Focus groups
  - Průběžné úpravy formulářů - 41 požadavků
  - Úpravy podpůrných materiálů
  - Možnost zapojení portal@nukib.gov.cz
- Vznik nových návodů, videonávodů
- Průběžné ladění navazujících procesů
  - Spolupráce s Národním CERTem o předávání incidentů
  - Procesy spojené s odesláním incidentu – reakce o víkendu - automatizace
  - Zpětná vazba

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

jsem student kyberbezpečnosti a z tohoto pohledu mi tahle stránka přijde extrémně cool a je super, že poskytujete takového průvodce

Pokud chci dobrovolně nahlásit kyberntický podvod, tak přihlašování přes identitu občana je naprostá buzerace. Zjevně nechcete aby občané něco dobrovolně hlásili. jak chcete nasbírat dost dat aby jste mohli občany efektivně chránit?

Vyhozené peníze daňových poplatníků. Když jsem hlásil podvodný mail ohledně údajného dědictví z Anglie tak stačila jedna stránka a odkaz na mail kam mám ten podvodný mail poslat.

Díky za tento text. Považuji ho za výjimečný, protože by si mnoho dalších legislativních požadavků podobné texty zasloužilo 👍

Zbytečná buzerace

Interní vývoj

Výhody

- Sběr zpětné vazby uživatelů
- Průběžné zlepšování systému na základě reálného používání

Nevýhody

- Práce nekončí nasazením systému do provozu - potřeba vyčlenit kapacity
- Nutnost efektivně prioritizovat požadavky

Shrnutí interního vývoje ve státní správě

- Výhodou je vyšší flexibilita a kontrola nad výsledkem
- Nevýhodou je náročnější řízení celého produktu

- Dává smysl ve státní správě?
  - Určitě.
  - Stát ale musí nastavit podmínky, aby jej bylo možné využívat častěji.
  - Hybridní přístup = spolupráce se soukromým sektorem.

- Šli bychom do toho znovu?
  - Ano!

portal.nukib.gov.cz
kariera.nukib.gov.cz

Jakub Onderka
Product Owner Portálu NÚKIB
E-mail: jakub.onderka@nukib.gov.cz

Lenka Ondryskova
Produktová manažerka Portálu NÚKIB
E-mail: lenka.ondryskova@nukib.gov.cz

Petra Kajánková
Bezpečnostní analytička Portálu NÚKIB
E-mail: petra.kajankova@nukib.gov.cz

Dotazy?