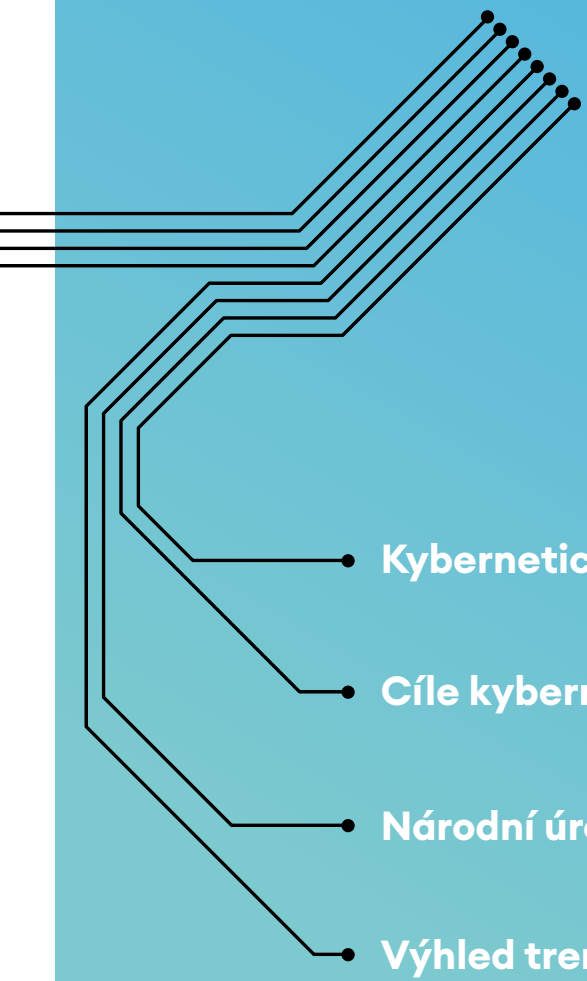
# Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2023



- Kybernetické hrozby a aktéři
- Cíle kybernetických útoků
- Národní úroveň kybernetické bezpečnosti
- Výhled trendů na roky 2024 a 2025

# Úvodní slovo ředitele




Vážené dámy, vážení pánové,
je mi potěším Vám předložit Zprávu o stavu kybernetické bezpečnosti České republiky za uplynulý rok. Stejně tak mi dovolte Vám i poděkovat za Váš zájem o kybernetickou bezpečnost naší země.

Z pohledu počtu a povahy incidentů se rok 2023 nesl zejména ve znaku hacktivismu a kyberkriminality. Donedávna, ne příliš významný fenomén hacktivismu se v reakci na agresi Ruska proti Ukrajině v posledních dvou letech stal organizovanějším a do určité míry i sofistikovanějším. Mnoho hacktivistických skupin má své působení silně spjaté s konkrétním státem a operuje ve shodě se zájmy konkrétních vlád. Česká republika tak čelila vysokému počtu DDoS útoků, což významně navýšilo celkový počet incidentů řešených naším úřadem na rekordních **262**.

Zintenzivnila se také činnost kyberkriminálních aktérů, zřetelná z nárůstu množství tohoto druhu kriminality evidované Policií České republiky. Útočníci přitom profesionalizují své aktivity v kyberprostoru, což lze nejvíce vidět v oblasti různých forem phishingu. Využívání umělé inteligence poskytuje stále lepší výchozí pozice pro útočníky k efektivní manipulaci obětí, přičemž lze očekávat, že tento trend bude i nadále akcelerovat.
S partnery jsme se proto v uplynulém roce zaměřili na intenzivnější osvětu v této oblasti. U všech forem phishingu je totiž nejúčinnější obranou prevence a vzdělávání uživatelů.

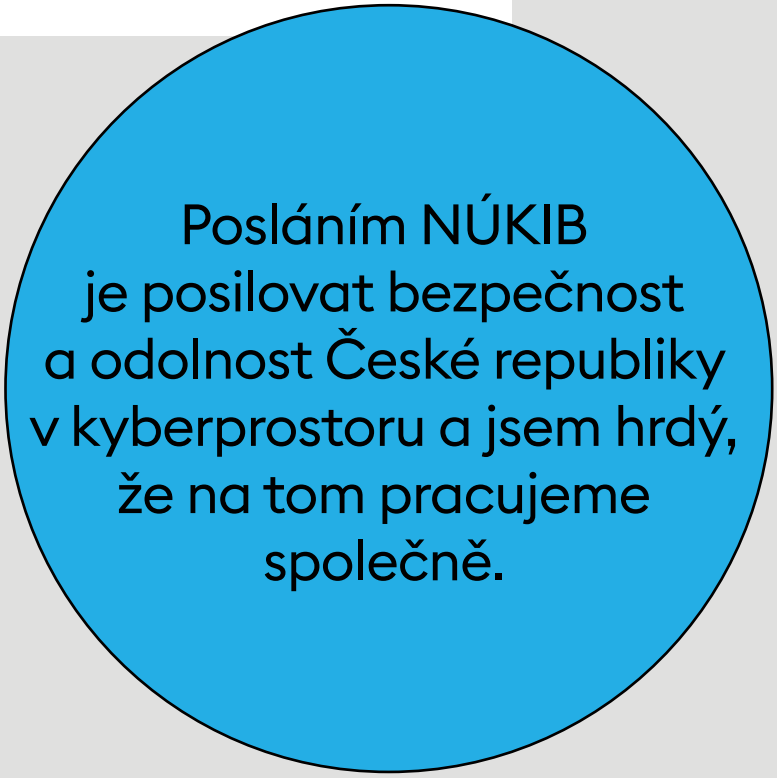
Uplynulý rok taktéž potvrdil dlouholetý zájem aktérů napojených zejména na Ruskou federaci a Čínskou lidovou republiku o skryté působení v sítích českých strategických institucí. V uplynulém roce lze hovořit o minimálně čtyřech separátních pokusech či úspěšných průnicích do sítí těchto organizací. Ve všech případech byla velmi pravděpodobně cílem kybernetická špionáž proti České republice.

Poznatky našeho úřadu dále ukazují, že v posledních letech stagnují rozpočty vynakládané na kybernetickou bezpečnost u značného počtu organizací, což dlouhodobě představuje jeden z hlavních problémů stavu kyberbezpečnosti v naší zemi. Stejně tak přetrvávají i problémy s nedostatkem odborníků na kybernetickou bezpečnost, zejména v rámci veřejného sektoru. Bez nich se přitom může stát situace výhledově nezvladatelnou. Kamenem úrazu jsou však možnosti a schopnosti státu takové lidi najmout, zaplatit a dlouhodobě udržet. Řada těchto oblastí je navíc ovlivněna neoptimální ekonomickou situací a růstem životních nákladů. Zcela srovnat platové podmínky se soukromým sektorem lze jen těžce a v případě státu to ani nemůže být cílem. Nicméně se dostáváme do stavu, kdy jsou státní instituce prakticky zcela nekonkurenceschopné a nedisponují kritickým množstvím odborníků nutných k pokrytí jejich kyberbezpečnostních a IT potřeb, a to ani při zapojení externích dodavatelů.

**Ing. Lukáš Kintr**
Ředitel Národního úřadu pro kybernetickou a informační bezpečnost

Pokud se tedy chceme posunout vpřed, musíme v brzké budoucnosti přistoupit ke změnám. Z mého pohledu je nutné přivřít čím dál více rozevřené nůžky u platového ohodnocení státních odborníků v oblasti IT a kybernetické bezpečnosti. Chceme-li bezpečný, odolný, inovativní a konkurenceschopný stát, musí tomu rámcově odpovídat podmínky pro ty, kteří jej budují. Jsem přesvědčen, že z dlouhodobého hlediska se přiměřená investice do těchto zaměstnanců státu mnohokrát vyplatí.

Závěrem bych chtěl tradičně poděkovat všem **423** organizacím, které se formou odpovědí na naše dotazy přímo podílely na vzniku Zprávy o stavu kybernetické bezpečnosti za rok 2023. Počet respondentů meziročně narostl o více jak **100** organizací, čímž je tato zpráva opět o něco přesnější.



# Obsah


## 2 Úvod

2 Úvodní slovo ředitele
6 O dokumentu
7 Seznam použitých zkratek
8 2023: Kybernetická bezpečnost ČR v datech
9 Shrnutí Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2023

## 10 Kybernetická bezpečnost ČR v roce 2023 z pohledu NÚKIB

11 Shrnutí dění v kyberprostoru za rok 2023 pohledem NÚKIB
14 Klasifikace kybernetických incidentů nahlášených NÚKIB
15 Incidenty pohledem subjektů
17 Finance vynaložené na kybernetickou bezpečnost
18 Odborníci
20 Uživatelé

## 21 Kybernetické hrozby a aktéři

22 Pokračující pokusy ruských a čínských aktérů o průnik do sítí strategických institucí
23 Severokorejský zájem o obranný sektor, nižší aktivita Íránu
24 Ransomware: útočníci inovují způsoby k dosažení zaplacení výkupného
25 Phishing: rostoucí četnost i sofistikovanost, zachyceny byly i nové podoby hrozby
27 Vývoj kyberkriminality v ČR

## 29 Cíle kybernetických útoků

30 Veřejný sektor
32 Finanční sektor
33 Průmysl a energetika
34 Zdravotnictví
36 Vzdělávací sektor

## 38 Časová osa vybraných varování a upozornění NÚKIB v roce 2023

## 39 Národní úroveň kybernetické bezpečnosti

40 Projekt BIVOJ
40 Bezpečnost dodavatelského řetězce
40 Předcházení kvantové hrozbě
41 Koordinované zveřejňování zranitelností
41 Legislativní ukotvení
41 Nový zákon o kybernetické bezpečnosti
41 Evropská certifikační schémata kybernetické bezpečnosti
42 Dozorová činnost NÚKIB v roce 2023
43 Cvičení kybernetické bezpečnosti
44 Prevence, osvěta a vzdělávání v kybernetické bezpečnosti v ČR
45 Mezinárodní spolupráce
46 Činnost Vládního CERT

## 47 Výhled trendů v kybernetické bezpečnosti v ČR na roky 2024 a 2025

47 Kybernetické útoky skrze dodavatelský řetězec
47 Geopoliticky motivované kybernetické útoky
47 Generativní umělá inteligence a velké jazykové modely (LLM)

## 48 Příloha 1: Vyhodnocení plnění cílů Národního plánu výzkumu a vývoje v kybernetické a informační bezpečnosti za rok 2023

## 49 Příloha 2: Naplňování Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025

## 50 O NÚKIB

# O dokumentu

## Dotazníkové šetření

NÚKIB na začátku roku 2024 rozeslal dotazník se 63 otázkami, a to jak subjektům regulovaným dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti, ZKB), ve znění pozdějších předpisů, tak i řadě dalších klíčových institucí a organizací, které zákonem o kybernetické bezpečnosti regulovány nejsou. Otázky se týkaly širokého záběru témat, například kybernetických útoků, nákladů na kybernetickou bezpečnost, personálních kapacit v oblasti kybernetické bezpečnosti, uživatelů, technologií i zavedených procesů. Dotazník vyplnilo celkem 423 subjektů, z toho 339 regulovaných a 84 neregulovaných. Ze získaných dat NÚKIB čerpal informace pro potřeby Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2023 (dále také jen „Zpráva“). Veškeré údaje z dotazníků jsou anonymizovány.

## Dotazníkové šetření

Hodnocení stavu kybernetické bezpečnosti v ČR je založeno na analytickém procesu, který zahrnuje kvantitativní i kvalitativní vyhodnocení dat z vyplněných dotazníků, poznatky NÚKIB, informace poskytnuté partnery a další dostupné informace z otevřených zdrojů. NÚKIB neměl možnost data poskytnutá respondenty kontrolovat, ani hlouběji ověřovat uvedená tvrzení. Analytické závěry obsažené ve Zprávě jsou založeny na premise, že odpovědi v dotaznících nejsou zkresleny. K vyjádření analytického hodnocení používáme pravděpodobnostní výrazy (viz níže).

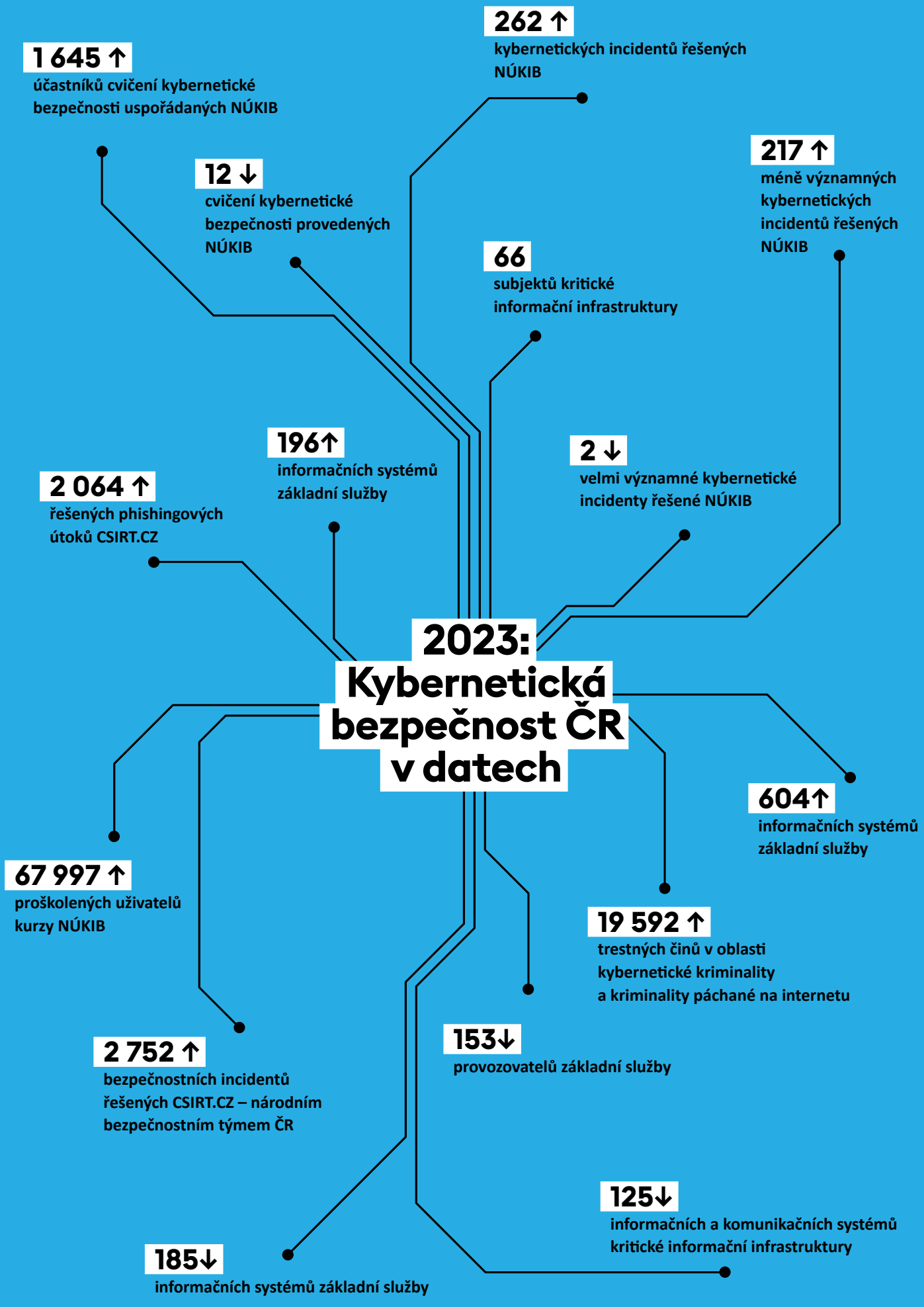
Zpráva neposkytuje vyčerpávající seznam všech aktivit v oblasti kybernetické bezpečnosti. Účelem dokumentu je popsat a vyhodnotit hrozby v kybernetickém prostoru, s nimiž se ČR v roce 2023 potýkala, stejně jako aktivity, které napomáhají jejich zmírnění.

## Pravděpodobnostní výrazy použité ve Zprávě o stavu kybernetické bezpečnosti České republiky za rok 2023

| | |
|---|---|
| Téměř jistě | 90–100 % |
| Velmi pravděpodobně | 75–85 % |
| Pravděpodobně | 55–70 % |
| Nelze vyloučit / Reálná možnost | 25–50 % |
| Nepravděpodobně | 15–20 % |
| Velmi nepravděpodobně | 0–10 % |

# Seznam použitých zkratek

| | |
|---|---|
| AI | umělá inteligence (artificial intelligence) |
| CZ PRES | Předsednictví České republiky v Radě Evropské unie |
| ČLR | Čínská lidová republika |
| ČR | Česká republika |
| DIA | Digitální a informační agentura |
| DoS/DDoS | Denial of Service / Distributed Denial of Service |
| ENISA | Agentura Evropské unie pro kybernetickou bezpečnost |
| EU | Evropská unie |
| GRU | Hlavní správa generálního štábu Ozbrojených sil Ruské federace (Главное управление Генерального штаба Вооружённых Сил России) |
| LLM | velké jazykové modely (Large Language Models) |
| MPSV | Ministerstvo práce a sociálních věcí |
| NATO | Severoatlantická aliance |
| NCTEKK | Národní centrála proti terorismu, extremismu a kybernetické kriminalitě |
| NIS 2 | (směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii) |
| NÚKIB | Národní úřad pro kybernetickou a informační bezpečnost |
| PCSC | Prague Cyber Security Conference |
| RGB | Generální úřad pro průzkum (Reconnaissance General Bureau) |
| SVR | Služba vnější rozvědky (Служба Внешней Разведки) |
| TTPs | taktiky, techniky a procedury (Tactics, Techniques, and Procedures) |
| ZKB | zákon o kybernetické bezpečnosti |




*Vizualizace 1: Kybernetická bezpečnost ČR v datech*

# Shrnutí Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2023

## 80% nárůst kybernetických incidentů

**Během roku 2023 došlo proti loňskému roku téměř k 80% nárůstu kybernetických bezpečnostních incidentů evidovaných NÚKIB, a to ze 146 na 262.** Za nárůstem stojí zejména opakované vlny DDoS útoků ruskojazyčných hacktivistických skupin. Došlo taktéž k řadě útoků ransomwarových aktérů vůči některým českým strategickým institucím či firmám. **Celkově se však meziročně snížil počet významných a velmi významných kybernetických incidentů.**

## Nejčastější typy kyberútoků a jejich kontext

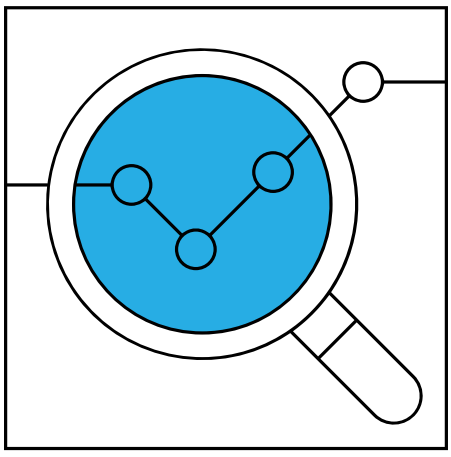
**Mezi nejčastější typy kyberútoků během roku 2023 patřily zejména různé druhy phishingu, jako je spearphishing, vishing či nově častěji i quishing a podvodné CEO e-maily. Dále také DDoS útoky, a to primárně vůči veřejnému a finančnímu sektoru.** Řada evidovaných incidentů souvisela s ruskou agresí na Ukrajině, v několika málo případech pak i s izraelsko-palestinským konfliktem.

## Hrozby kybernetické špionáže

Dále u minimálně čtyř separátních aktérů hrozeb NÚKIB spolu s partnery detekoval pokusy či úspěšné průniky do sítí strategických institucí českého státu. Ve všech případech byla velmi pravděpodobně (75–85 %) cílem útočníků kybernetická špionáž.

## Práce na zlepšení legislativy a bezpečnostních opatřeních

**Další významnou činností NÚKIB byla příprava nového zákona o kybernetické bezpečnosti. Jedná se pokračování úsilí NÚKIB zajistit odpovídající legislativní rámec kybernetické bezpečnosti v ČR, které navazuje na publikaci směrnice NIS 2 během českého předsednictví v Radě Evropské unie v roce 2022.** Rok 2023 se tedy obdobně jako předchozí rok nesl ve znamení projednávání a vytváření návrhu nového zákona, konzultace se zainteresovanými subjekty (regulovanými osobami a gestory regulovaných odvětví) stejně jako s širokou veřejností a zahájení formálního legislativního procesu.



## Projekt BIVOJ: Zvyšování odolnosti ČR

**V roce 2023 NÚKIB ve spolupráci s partnery pokračoval v práci na Projektu BIVOJ.** Cílem je vytvoření jednotné, funkční a bezpečné sdílené platformy poskytující bezpečnostní a komunikační služby, do které budou postupně připojeny instituce veřejného sektoru.

## GOV.CZ

**Jedním z letošních výsledků projektu je například migrace ústředních orgánů státní správy na jednotnou státní doménu gov.cz.** Tato jednotná doména zvýší uživatelskou přívětivost pro občany, právní jistotu a zvýší odolnost proti DDoS útokům.

## Osvětová činnost a cvičení pro lepší ochranu

**V neposlední řadě NÚKIB taktéž pokračoval v osvětové činnosti a organizaci cvičení kybernetické bezpečnosti.** To zahrnuje například spolupráci na tvorbě a implementaci rámcových vzdělávacích programů na základních a středních školách, ale i snaha zviditelnit kybernetickou bezpečnost v rámci systému rekvalifikačního vzdělávání. V kontextu cvičení během loňska proběhlo například sektorové cvičení TELCO23 zaměřené na poskytovatele telekomunikačních služeb, naopak zástupci NÚKIB se účastnili mezinárodních cvičení kybernetické bezpečnosti Locked Shields či Cyber Coalition.

## Co nás čeká v následujících letech?

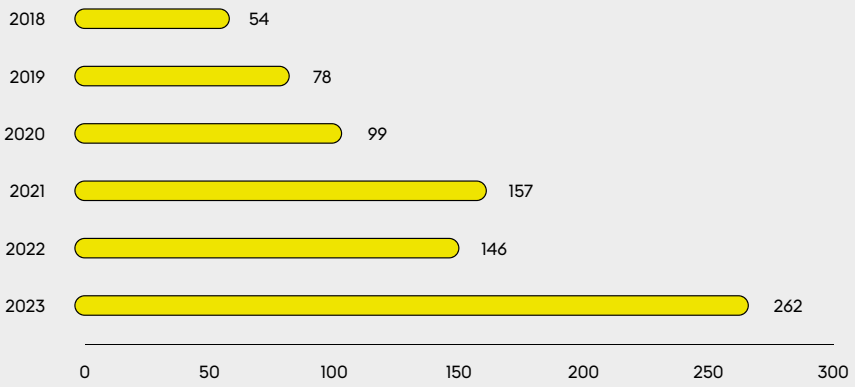
**Mezi hlavní trendy pro následující dva roky NÚKIB ve svém výhledu řadí zejména kybernetické útoky skrze dodavatelský řetězec, geopoliticky motivované kyberútoky či posilující vliv umělé inteligence na kybernetickou bezpečnost.**

# 1 Kybernetická bezpečnost ČR v roce 2023 z pohledu NÚKIB[1]



[1] Prezentované informace vycházejí ze zdrojů NÚKIB a z vyhodnocení 423 dotazníků (viz část O dokumentu).

**NÚKIB v roce 2023 evidoval celkem 262 kybernetických bezpečnostních incidentů, což je dosud nejvyšší zaregistrovaná hodnota.**

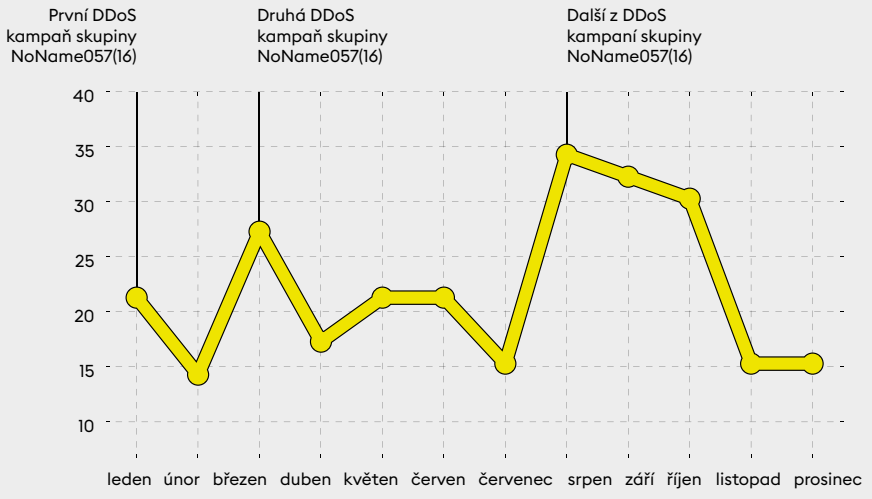



*Graf 1: Vývoj počtu incidentů evidovaných NÚKIB v letech 2018–2023*

Oproti roku 2022, kdy bylo evidováno 146 incidentů, tak došlo k téměř 80% nárůstu.

Za tímto nárůstem stojí primárně opakované vlny DDoS útoků vedené zejména ruskojazyčnými hacktivistickými skupinami.

**DDoS útoky tvořily významnou část všech evidovaných incidentů v roce 2023. Jednoznačně nejčastějším původcem těchto útoků byla skupina NoName057(16), která na české cíle útočila pravidelně.**



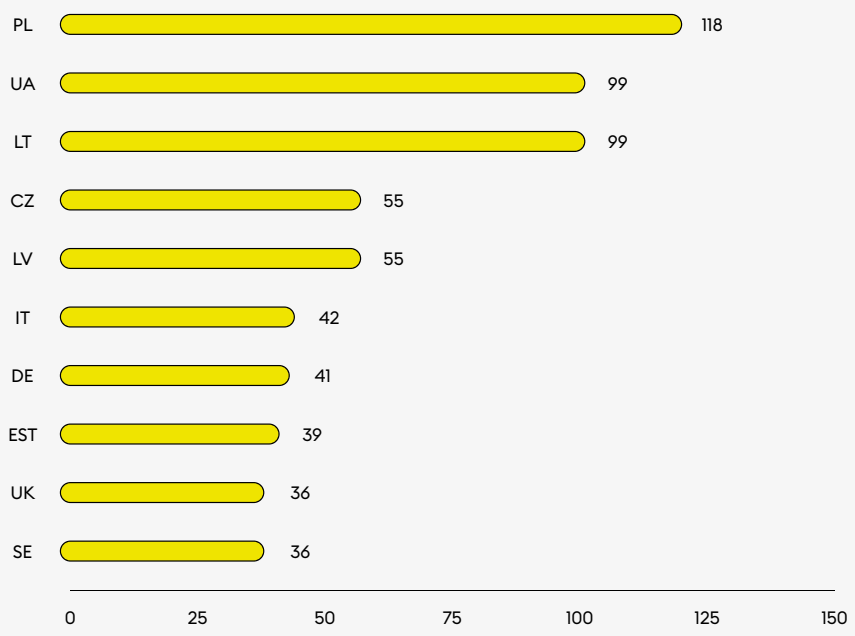

**Celkem 262 incidentů**

*Graf 2: Vývoj počtu incidentů řešených NÚKIB v roce 2023*

Kampaně NoName057(16) vůči českým cílům zpravidla probíhaly v návaznosti na dění či výroky spojené s konfliktem na Ukrajině či jiné významné události. Zmínit lze například útoky v reakci na oznámení materiální či jiné pomoci Kyjevu nebo některá vyjádření českých politických představitelů v souvislosti s ukrajinským konfliktem. Česká republika zároveň patřila mezi nejzasaženější státy Evropy tímto aktérem (viz Graf 3).

**Zaznamenané útoky však neměly závažnější dopady a v naprosté většině vedly pouze k dočasné nedostupnosti webových stránek napadených subjektů. DDoS útoky obecně zahlcují provoz na webových stránkách a službách přístupných z internetu, interní informační systémy organizací však nekompromitují.**

## Počet deklarovaných DDoS útoků skupinou NoName057(16) proti evropským státům v roce 2023




*Graf 3*

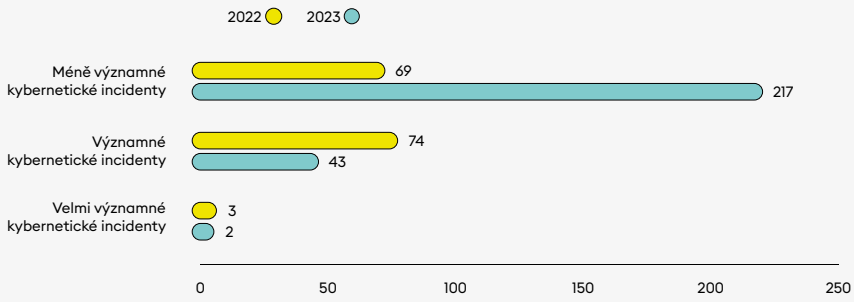
NÚKIB v roce 2023 mimo jiné evidoval také řadu DDoS útoků, u nichž nebyl identifikován jejich původce.

Jedním z případů byla kampaň interně nazvaná DNS NXDOMAIN, podle použité techniky DNS NXDOMAIN flood. Tato kampaň byla specifická zejména tím, že u ní nebyl zřetelný vzorec, kdy by jednotlivé útoky byly vázány např. na geopolitické dění nebo činnost napadených obětí a umožňovaly tak objasnit útočníkovy aktivity. Jediným vodítkem tak kromě využívaných technik a infrastruktury zůstává specifická viktimologie, v rámci které NÚKIB zaznamenal útoky cílené výhradně na české státní instituce.

**Ransomwarové útoky se mezi incidenty NÚKIB objevují pravidelně od roku 2018. Zejména v průběhu června však NÚKIB zaznamenal zvýšený zájem ransomwarových aktérů o některé české strategické cíle, což vedlo k vydání upozornění na zvýšené riziko ransomwarových útoků.** Nejvýrazněji se pak do statistik propsaly aktivity gangů PLAY a LockBit, což zrcadlí i globální trend. Mimo výše uvedené NÚKIB registroval také řadu phishingových kampaní, jak ze strany státem podporovaných aktérů, tak kyberkriminálních skupin.

Během června NÚKIB vydal varování před zvýšeným rizikem ransomwarových útoků, přičemž zdůraznil zejména zájem útočníků o české strategické cíle.

## Zatímco méně významných incidentů přibylo více než trojnásobně, významných incidentů ubylo o třetinu.



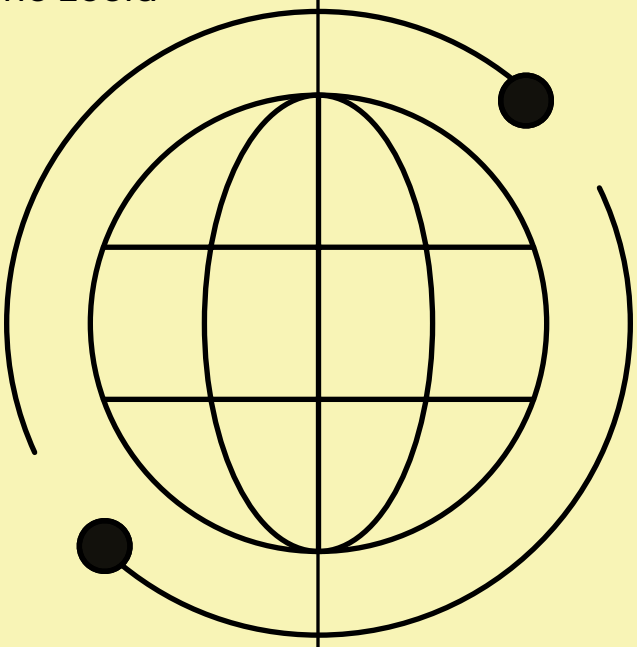

*Graf 4 : Meziroční srovnání závažnosti incidentů evidovaných NÚKIB v letech 2022–2023*

Z pohledu závažnosti evidovaných incidentů bylo možné sledovat pozitivní vývoj, kdy navzdory výraznému nárůstu počtu incidentů došlo k meziročnímu snížení počtu významných a velmi významných kybernetických incidentů (viz Graf 4). Nárůst počtu a pokles závažnosti evidovaných incidentů lze vysvětlit opakovanými DDoS útoky vůči českým cílům, které se významně propsaly do statistik NÚKIB, nicméně zpravidla neměly významnější a dlouhodobější dopady.

**V krátkodobém výhledu následujících tří let lze předpokládat pokračování některých nastolených trendů.**

### Kybernetické útoky v reakci na geopolitické události

I nadále bude pravděpodobně (55–70 %) docházet ke kybernetickým útokům v reakci na geopolitické dění či jiné politicky citlivé události, a to ne zcela nutně pouze v souvislosti s ukrajinským konfliktem.



### Zapojení hacktivistických skupin

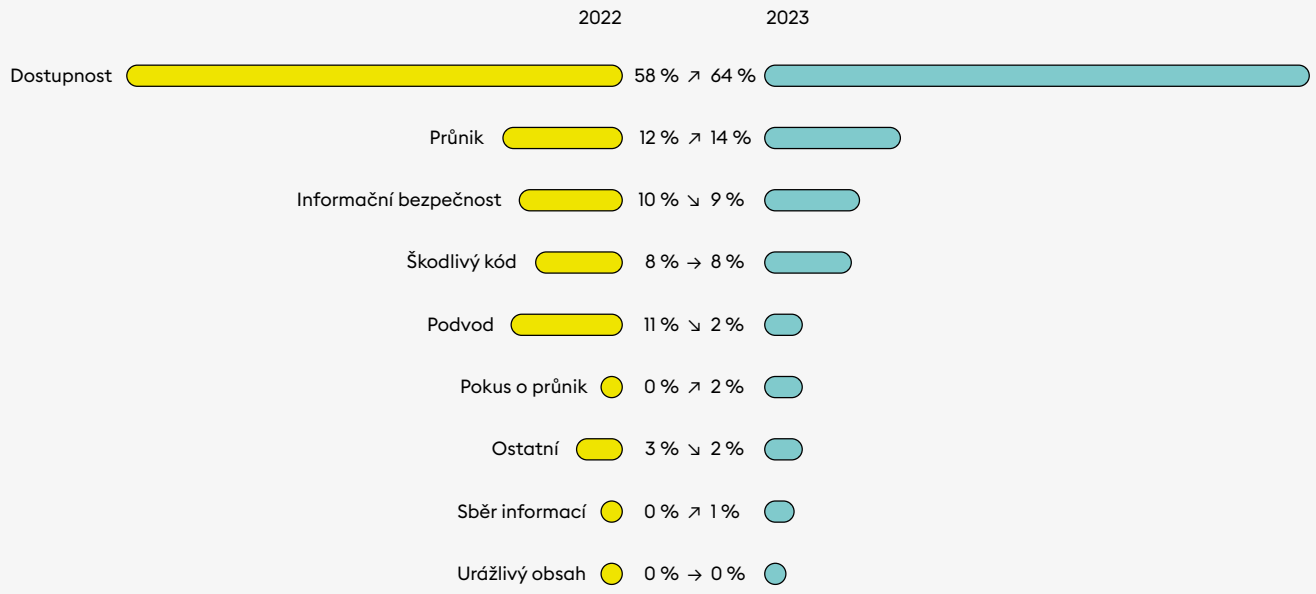
V těchto případech lze očekávat zapojení zejména různých hacktivistických skupin, nelze však vyloučit (25–50 %) ani působení jiných typů aktérů.

### Phishingové kampaně a ransomwarové útoky

Podobně jako v uplynulých letech pak bude taktéž velmi pravděpodobně (75–85 %) docházet k plošným phishingovým kampaním vůči státním i soukromým subjektům, ale také ransomwarovým útokům napříč odvětvími.

# Klasifikace kybernetických incidentů nahlášených NÚKIB [2]

## Procentuální zastoupení v incidentech




**Dostupnost** - např. narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží
**Průnik** - např. kompromitace aplikace nebo uživatelského účtu
**Informační bezpečnost** - např. neautorizovaný přístup k datům, neautorizovaná změna informace
**Škodlivý kód** - např. virus, červ, trojský kůň, dialer, spyware
**Podvod** - např. phishing, krádež identity nebo neoprávněné využití ICT
**Pokus o průnik** - např. pokus o zneužití zranitelnosti, pokus o přihlášení apod.
**Sběr informací** - např. skenování, sniffing, sociální inženýrství

*Vizualizace 2: Klasifikace kybernetických incidentů nahlášených NÚKIB*

**Z hlediska klasifikace incidentů nejvíce převažovaly incidenty cílící na dostupnost (např. webových stránek či služeb), což odpovídá vysokému počtu zaznamenaných DDoS útoků.** Tato kategorie nicméně obsahuje také řadu incidentů, za kterými nestojí útoky, ale například technické chyby vedoucí k výpadku systémů.[3]

**Druhou nejpočetnější pak byla kategorie průnik.** Sem spadaly zpravidla útoky využívající metod sociálního inženýrství, nejčastěji phishingové útoky vedoucí ke kompromitaci e-mailových či jiných účtů. **Třetí nejčastěji evidovanou pak byla kategorie informační bezpečnost, v rámci které převládaly ransomwarové útoky.**

---

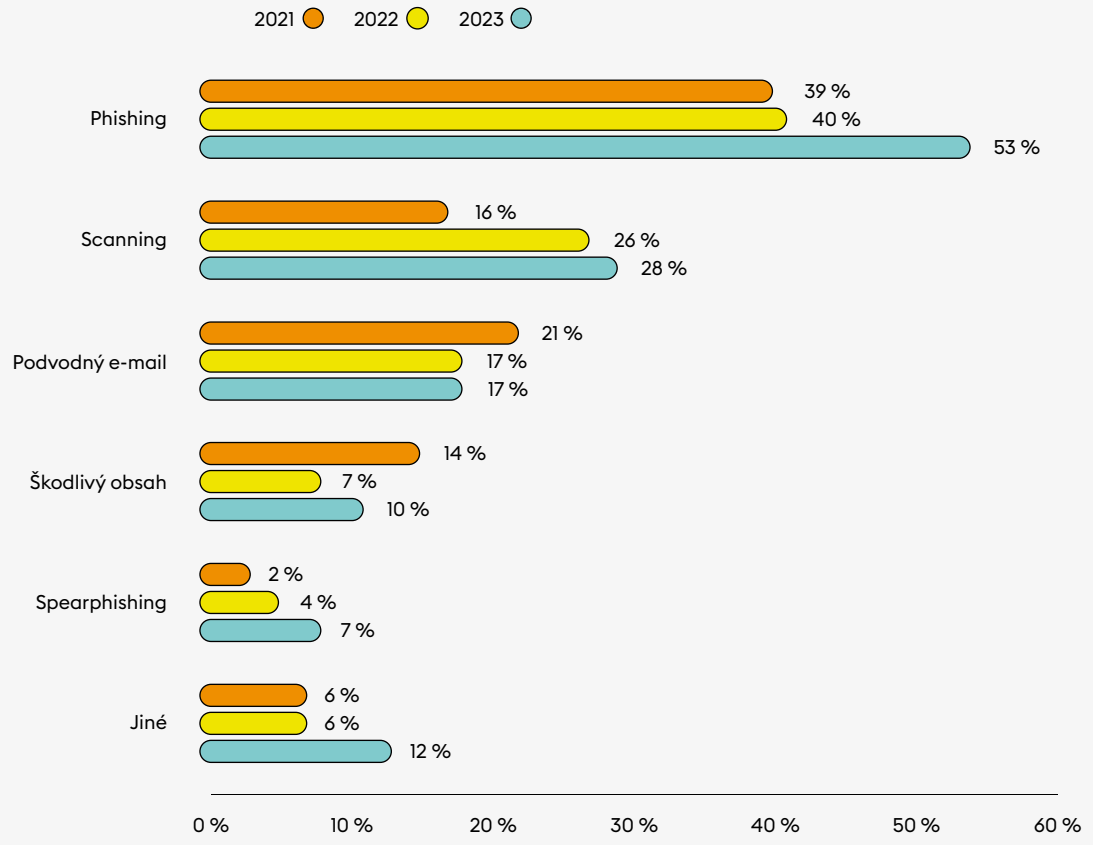
[2] Klasifikace kybernetických incidentů je založena na taxonomii ENISA: Reference Incident Classification Taxonomy — ENISA (europa.eu).
Dle současného znění ZKB jsou regulované subjekty povinny hlásit veškeré kybernetické incidenty, tj. narušení bezpečnosti

[3] Informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.

# Incidenty pohledem subjektů

## Rostoucí četnost a sofistikovanost phishingu

**Pohledem dotazovaných společností dominuje statistikám kybernetických útoků dlouhodobě phishing, nicméně z letošních dat vyplývá, že se využívání této techniky oproti minulým rokům stupňuje.**



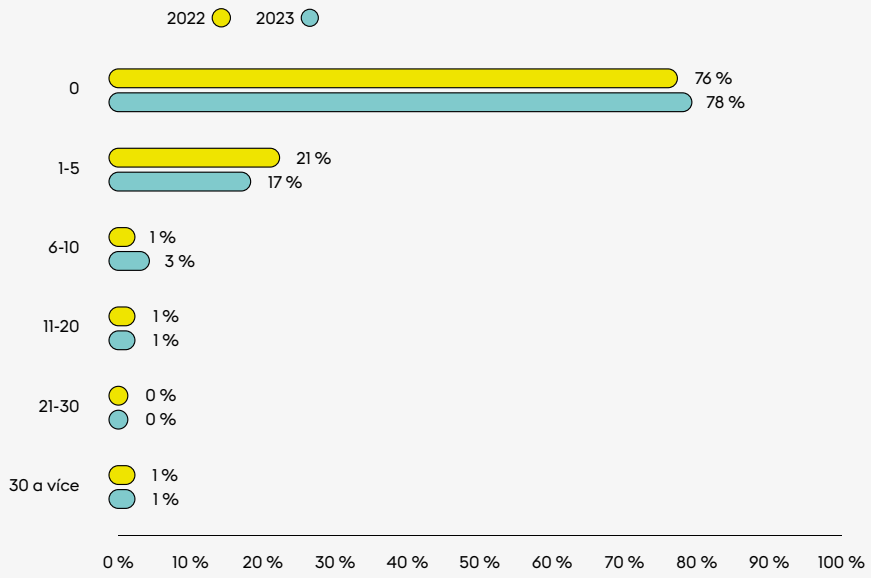

*Graf 5 : Kategorie nejčastějších typů kybernetických útoků v letech 2021–2023 (% respondentů)*

Během roku 2023 lze vidět výrazný nárůst této kategorie, kterou jako nejčastější typ útoku či pokus o něj označila více než polovina respondentů (viz Graf 5). **Nárůst lze vidět taktéž v kategorii cílených spear-phishingových útoků, což odpovídá obecnému trendu rostoucí četnosti i kvality phishingu, který vyplývá i z dalších poznatků činnosti NÚKIB.**

# Celkový počet incidentů na úrovni z minulých let

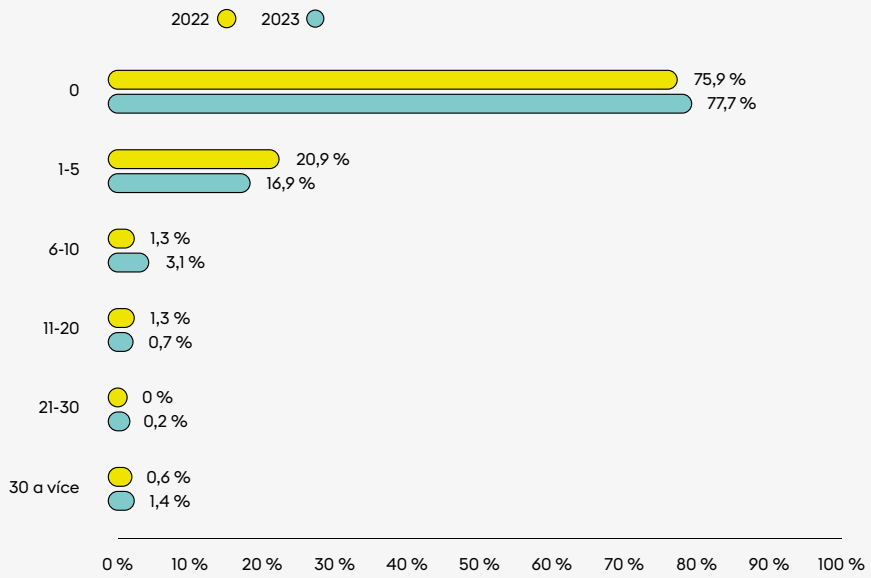
Pohledem četnosti pokusů o kybernetický útok, které vyústily v kybernetický incident, zůstává meziročně situace takřka totožná (viz Graf 6), stejná situace platí taktéž pro podíl úspěšných pokusů o kyberútok ústící v kybernetický incident (viz Graf 7).

**Počet pokusů o kybernetický útok, které vyústily v kybernetický incident v roce 2023 (% respondentů)**




*Graf 6*

**Srovnání zaznamenaných kybernetických útoků či pokusů o ně v roce 2022 a 2023 (% respondentů)**

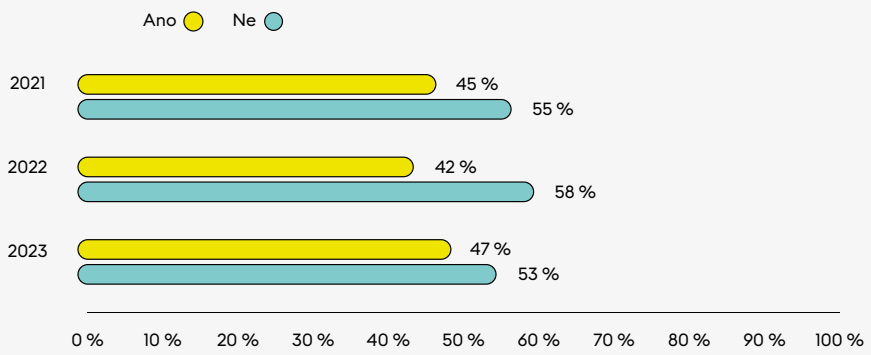



*Graf 7*

Je tudíž pozitivní zprávou, že navzdory zlepšení technik útočníků toto nemá výrazný vliv na kybernetickou bezpečnost subjektů.

# Finance vynaložené na kybernetickou bezpečnost: Rozpočty organizací stagnovaly

**Považujete vyčleněné finance na zajištění kybernetické bezpečnosti své organizace za dostatečné?**




*Graf 8*

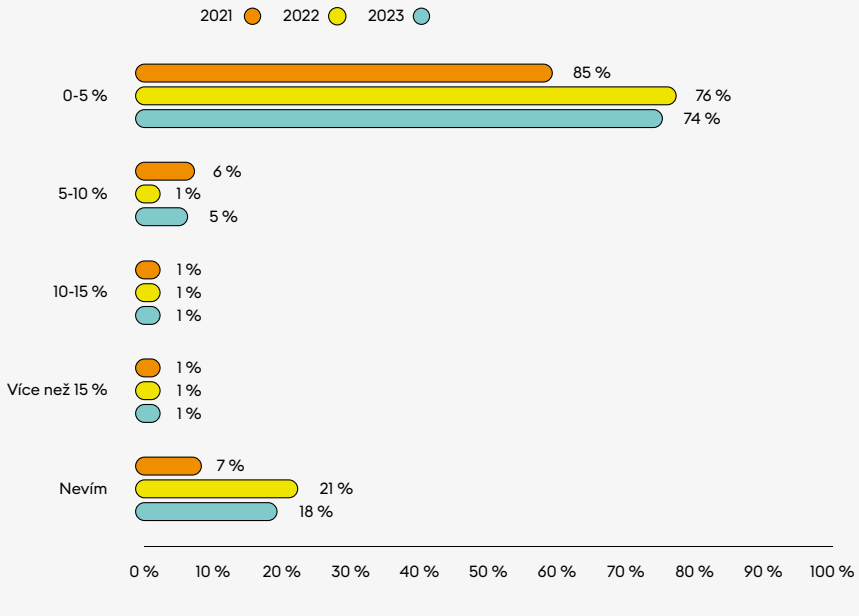
**Jedním z trendů, který je patrný v uplynulých dvou letech, je stagnace rozpočtů alokovaných na kybernetickou bezpečnost jednotlivých organizací**. Z dotázaných organizací 47 % deklarovalo, že svůj rozpočet navýšilo, což představuje 3% meziroční růst. V kontextu navýšení rozpočtů, které je pravděpodobně meziročně porovnáváno v nominálních částkách, je však třeba brát v potaz i vliv vysoké inflace z posledních dvou let. Navýšení rozpočtů tak pravděpodobně (55–70 %) spíše dorovnávalo inflační tlaky a růst cen, přičemž více než polovina respondentů žádné navýšení rozpočtů neuvedla.

**Odpovídá tomu i meziročně téměř neměnný podíl organizací, které považují svůj rozpočet na kybernetickou bezpečnost za dostačující (viz Graf 8)**. I nadále nadpoloviční většina respondentů hodnotí finance vynaložené na kybernetickou bezpečnost za nedostatečné.

Podíl rozpočtu vynaloženého na kybernetickou bezpečnost z celkového rozpočtu je navzdory deklarovanému navýšení rozpočtů srovnatelný s loňskými výsledky, kdy tři čtvrtiny organizací dedikují 0–5 % svého rozpočtu na bezpečnost v kyberprostoru (viz Graf 9).

Do budoucna indikuje další plánovaná zvýšení financí do kybernetické bezpečnosti celkem 55 % respondentů, v závislosti na ekonomické situaci je tak možné, že trend stagnace v budoucnu přejde v mírný nárůst rozpočtů.

**Podíl rozpočtu alokovaného na kybernetickou bezpečnost z celkového rozpočtu organizací v letech 2021–2023**



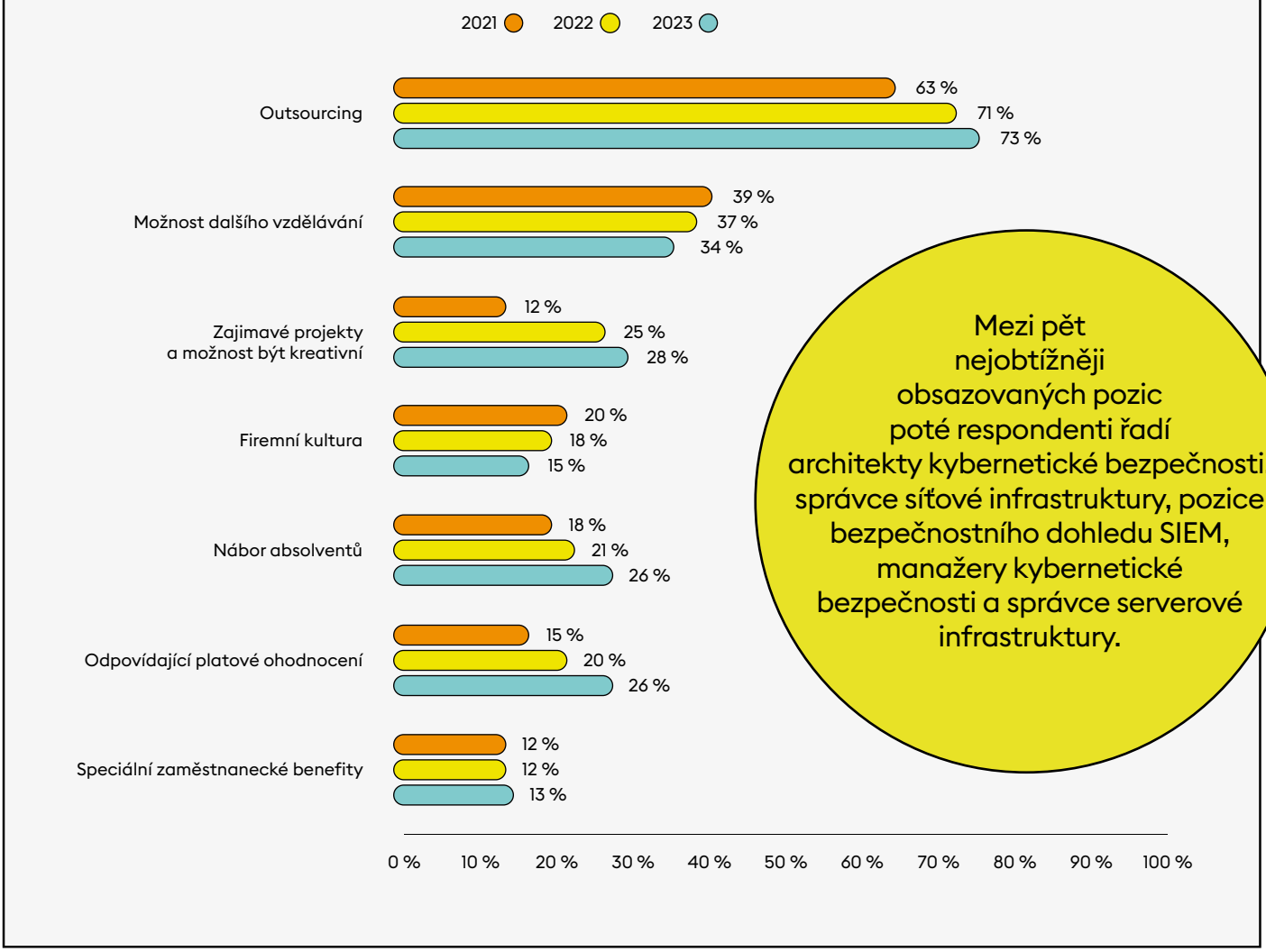

*Graf 9*

# Odborníci: více outsourcingu a snaha o zajištění adekvátního platového ohodnocení

**Nedostatek odborníků na kybernetickou bezpečnost zůstává i nadále jedním z hlavních problémů a výzev pro české instituce a organizace.** Problémem, který rovněž představuje dlouhodobý trend, je nedostatečné finanční ohodnocení zaměstnanců.

Dotazované organizace tuto problematiku řeší několika různými způsoby, přičemž během posledních tří let lze identifikovat obecnější pokračující trendy (viz Graf 10).

## Jak se organizace v letech 2020–2023 snažily vypořádat s nedostatkem odborníků (% respondentů)




*Graf 10*

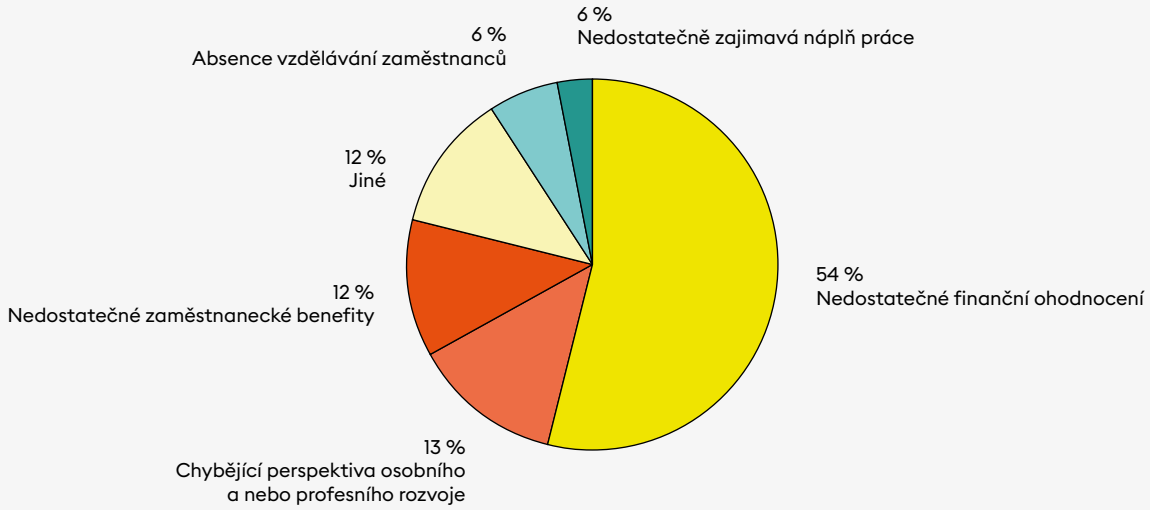
Nadále například roste podíl organizací, které svůj nedostatek v oblasti odborníků na kybernetickou bezpečnost řeší outsourcingem.

Ačkoliv růst tohoto přístupu zpomaluje, je stále dominantním, a setrvale roste již od roku 2020. Klesá oproti tomu volba možností dalšího vzdělávání. Přestože se stále jedná o druhé nejčastější řešení, je možné sledovat od roku 2020 jeho konstantní pokles.

Setrvalý pozvolný nárůst lze identifikovat také v náboru absolventů, který za poslední tři roky stoupl o osm procent.

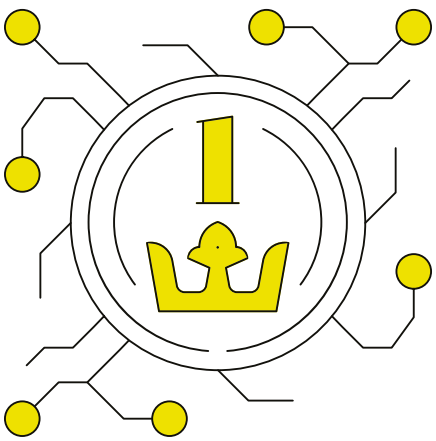
Setrvale stoupá i snaha o navyšování platového ohodnocení, které za poslední tři roky narostlo o více jak 60 %. **I přesto však respondenti uvádějí ve více jak polovině případů nedostatečné platové ohodnocení jako primární faktor komplikující obsazování klíčových pozic.** (viz Graf 11).

## Nejzásadnější faktory, které dle respondentů odrazují uchazeče při náborech na místa v oblasti kybernetické bezpečnosti (% respondentů)



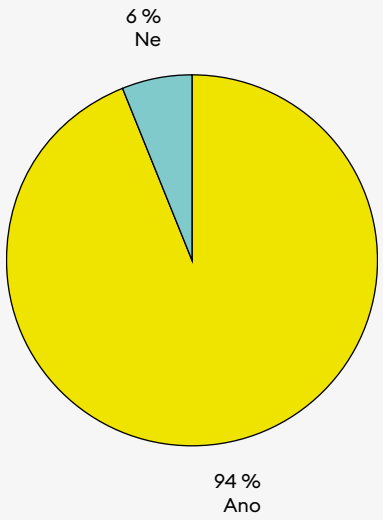

*Graf 11*

Více než polovina (54 %) respondentů uvedla, že nároky na finanční ohodnocení představují nejzásadnější faktor, který odrazuje uchazeče.



# Uživatelé: pozitivní posun v testování odolnosti proti kybernetickým hrozbám oproti minulému roku

## Podíl organizací, které své zaměstnance školí na kybernetickou bezpečnost a těmi, které je neškolí (% respondentů)



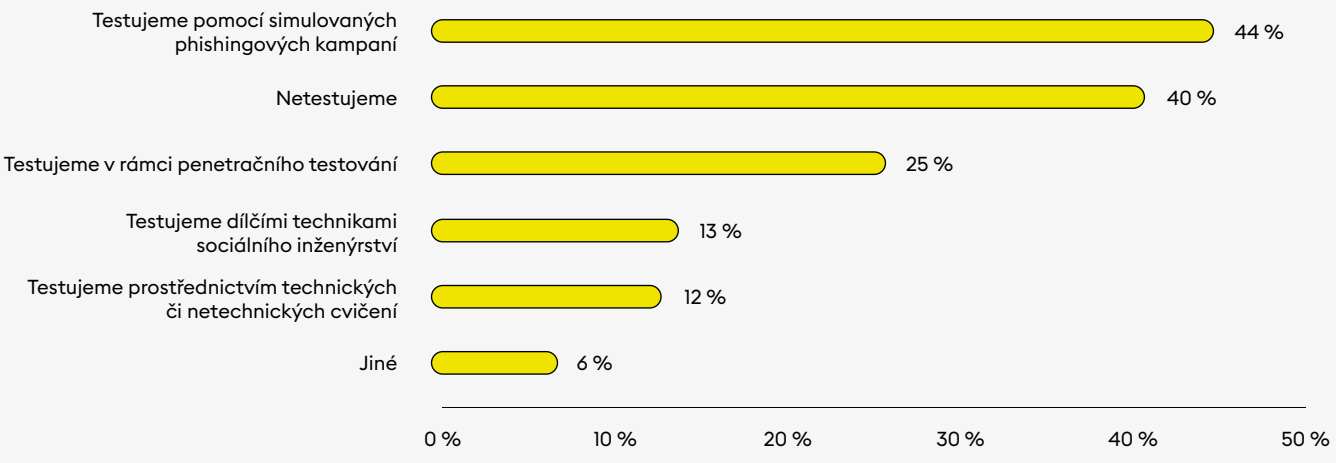

*Graf 12*

Dotazované organizace napříč všemi sektory své zaměstnance školí na kybernetickou bezpečnost či je seznamují s aktuálními kybernetickými hrozbami nejčastěji jednou za rok. Pouze 6 % respondentů své zaměstnance neškolí vůbec (viz Graf 12).

Nejrozšířenější školící metodou je informování zaměstnanců (formou e-mailu či interních portálů), kterou využívají skoro dvě třetiny dotazovaných.

Nejméně školí organizace nacházející se ve zdravotnickém a vzdělávacím sektoru, kde pořádá školení přibližně 85 % dotazovaných organizací.

## Způsob testování odolnosti zaměstnanců proti kybernetickým hrozbám v organizacích za rok 2023 (% respondentů)

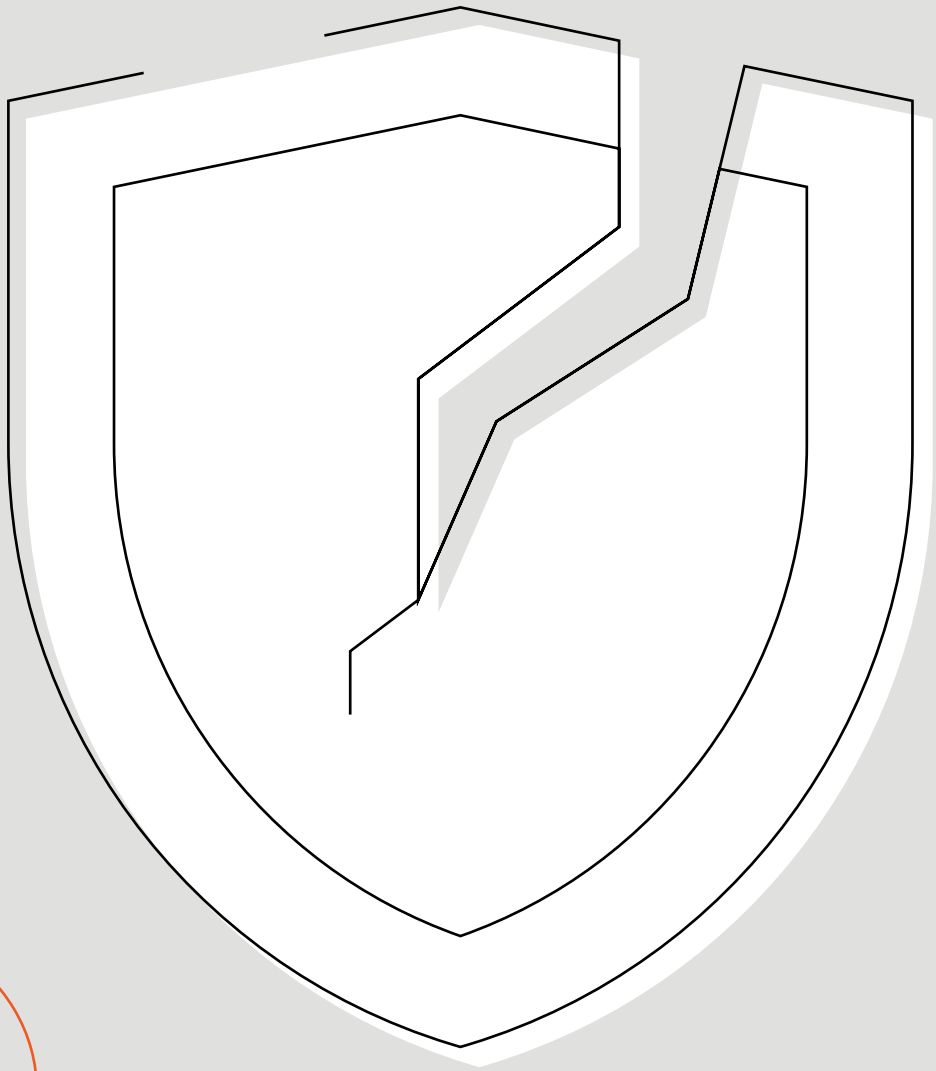



Nejčastější formou testování jsou poté simulované phishingové kampaně.

V kontextu testování zaměstnanců je naopak mnohem vyšší podíl organizací (40 %), které žádný způsob testování neprovádí.

*Graf 13*

# Kybernetické hrozby a aktéři



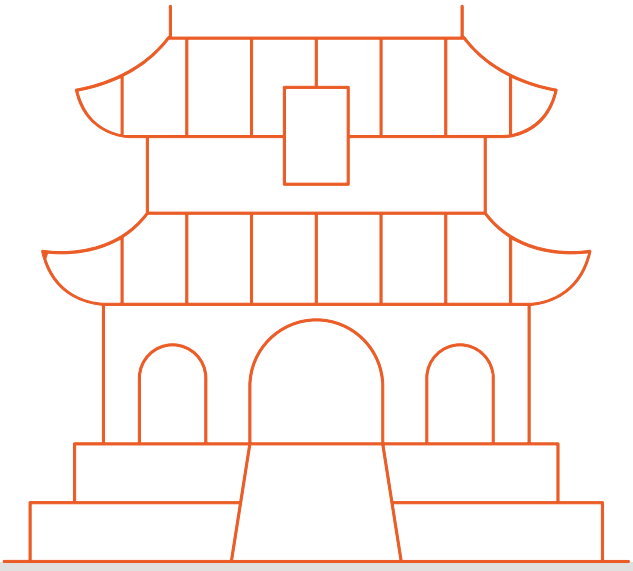
2

# Pokračující pokusy ruských a čínských aktérů o průnik do sítí strategických institucí

U minimálně čtyř separátních aktérů hrozeb detekoval NÚKIB ve spolupráci s partnery pokusy či úspěšné průniky do sítí strategických institucí. Ve všech případech byla podle viktimologie a TTPs velmi pravděpodobným (75–85 %) cílem kybernetická špionáž.

Z hlediska státem podporovaných hrozeb čelí ČR dlouhodobě velmi podobným hrozbám jako spojenci v NATO/EU.

**Daní aktéři usilují v tuzemském případě zejména o vytvoření dlouhodobé přítomnosti (tzv. persistence) v zájmové síti, zejména u strategických institucí.** Tomu odpovídají jejich TTPs, kdy jejich primárním cílem bývá zpravidla kybernetická špionáž.





## Ruské aktivity spojené se skupinami APT29 a APT28

U aktérů spojovaných s Ruskou federací šlo téměř jistě (90–100 %) o aktivity, které byly součástí dlouhodobých kampaní, jež zasáhly i spojence. **Detekovány byly škodlivé aktivity útočníků, jejichž operační postupy (tzv. tradecraft), motivace a cíle se do významné míry překrývají se skupinami APT29 (dále známá jako Midnight Blizzard, BlueBravo či Cozy Bear) a APT28 (dále známá jako Forest Blizzard, BlueDelta či Fancy Bear).** První jmenovaný aktér je spojován s ruskou Službou vnější rozvědky (SVR) a druhý pak s ruským vojenským zpravodajstvím (GRU).[4]



## Zvýšená aktivita aktérů spojených s ČLR

Během posledních několika let NÚKIB detekuje také zvýšené operační tempo aktérů spojovaných s Čínskou lidovou republikou (ČLR), mj. v důsledku jejich většího zaměření na evropské cíle v kontextu války na Ukrajině. **V roce 2023 byl identifikován průnik do sítě strategické instituce, kdy velmi pravděpodobným (75–85 %) útočníkem byla skupina čínského původu.** Dále pak byla detekována phishingová kampaň skupiny Mustang Panda (dále známá jako RedDelta), která minimálně od ruské invaze na Ukrajinu směřuje značnou část svých aktivit proti evropským cílům, včetně těch českých.



## Severokorejský zájem o obranný sektor

Česká republika byla v minulém roce terčem severokorejské skupiny Lazarus (dále známá jako Diamond Sleet či Labyrinth Chollima). **Ta měla kompromitovat společnosti činné v obranném průmyslu, a to nejenom v tuzemsku, nýbrž i dalších zemích NATO/EU.** Daný aktér je spojován se zpravodajským Generálním úřadem pro průzkum (RGB).[5] **Daná kampaň potvrzuje zájem vybraných aktérů hrozeb o specifická odvětví českého průmyslu.**



## Nižší aktivita Íránu

**Ve srovnání s minulostí byla aktivita sofistikovaných aktérů operujících v souladu se zájmy Teheránu nižší.** V kontextu eskalace izraelsko-palestinského konfliktu byly detekovány také aktivity íránských aktérů, která směřovaly například vůči technologiím konkrétních výrobců ve vodohospodářském sektoru.

---

[4] Viz např.: SVR cyber actors adapt tactics for initial cloud access - NCSC.GOV.UK / BlueBravo Adapts to Target Diplomatic Entities with GraphicalProton Malware | Recorded Future / Office of Public Affairs | Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU) | United States Department of Justice / Vojenské zpravodajství | Tiskové zprávy - Vojenské zpravodajství provedlo aktivní zásah v kybernetickém prostoru (vzcr.cz)

[5] Viz např.: Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups | U.S. Department of the Treasury / Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations | Mandiant

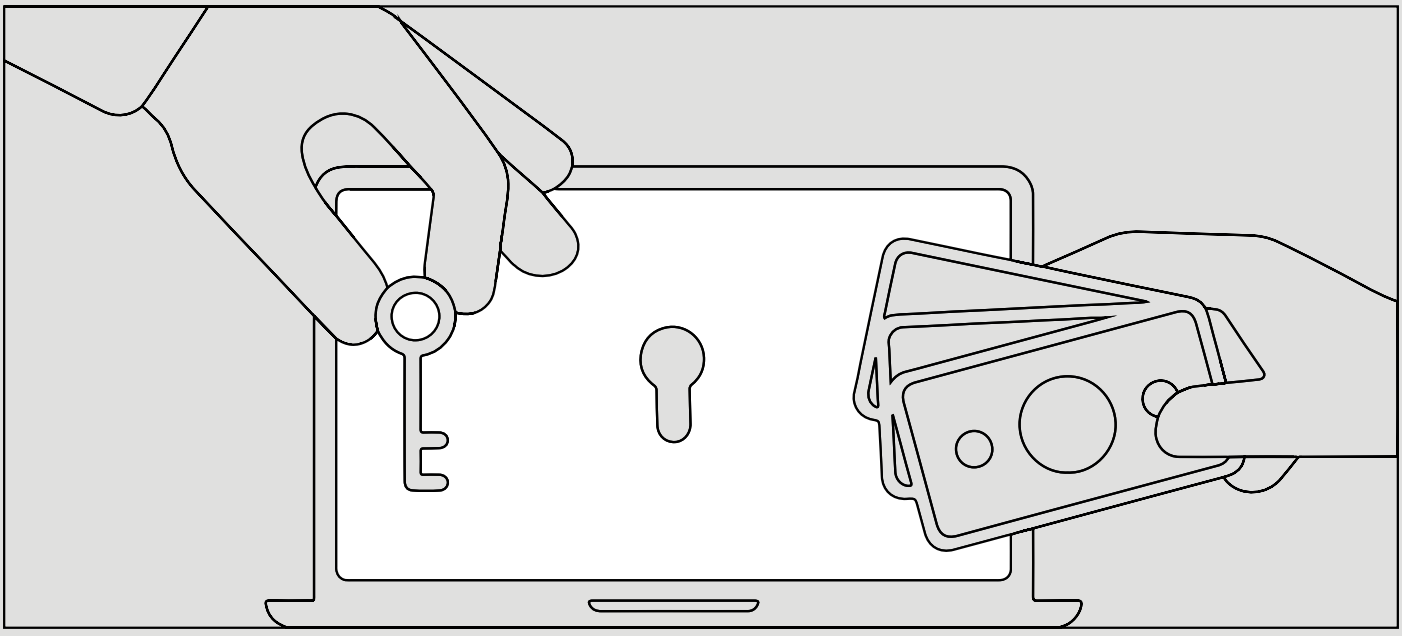
# **Ransomware:** útočníci inovují způsoby k dosažení zaplacení výkupného

Ransomwarové útoky jsou dlouhodobým trendem, pro který je typický vývoj směrem k takovým taktikám a technikám, jež by zvýšily pravděpodobnost, že bude útočníkům zaplaceno výkupné. **V minulém roce NÚKIB zaznamenal první případ ransomwarového útoku, který využíval tzv. „extortion-only" přístup, kdy data oběti nebyla útočníkem zašifrována, nýbrž pouze exfiltrována a útočník vydíral oběť jejich zveřejněním.** Jedná se o posun již ustálené taktiky dvojitého, popřípadě vícenásobného, vydírání, jež se skládá z exfiltrace dat a výhružek jejich zveřejněním. Konstantní výskyt je zaznamenán taktéž u modelu ransomware-as-a-service, tedy ransomwaru nabízeného ve formě služby.

Je velmi pravděpodobné (75–85 %), že útočníci budou přicházet s inovativními způsoby, jak získat výkupné.

**Platba výkupného však nikdy nezaručuje vyřešení incidentu ani obnovení dat, přičemž zároveň podporuje útočníky v další škodlivé činnosti.**

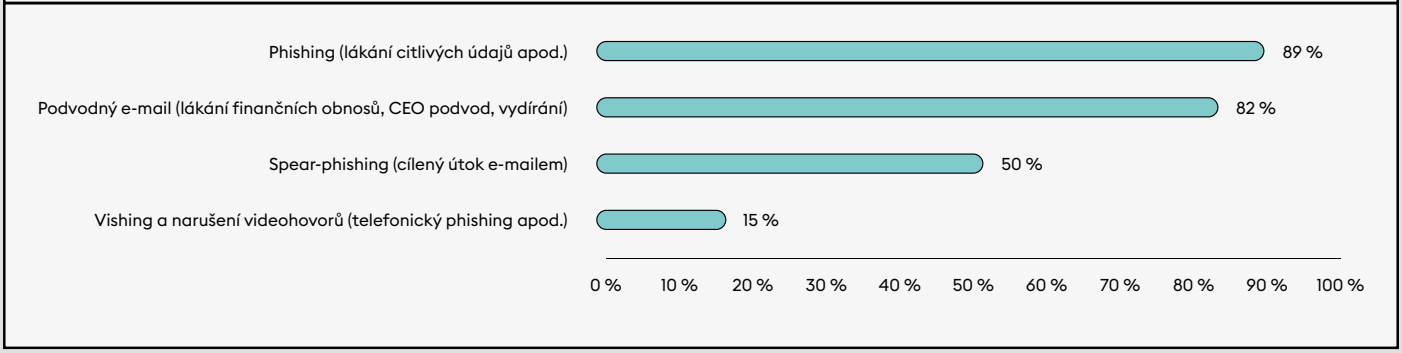
Snaha o prosazení neplacení výkupného vykrystalizovala mj. v prohlášení Counter Ransomware Initiative o zavázání se neplatit výkupné, ke kterému se připojila i Česká republika.



# Phishing: rostoucí četnost i sofistikovanost, zachyceny byly i nové podoby hrozby

**Phishing a jeho různé podoby dlouhodobě představují nejrozšířenější techniku útočníků.** I během roku 2023 se s touto hrozbou potýkala naprostá většina dotazovaných subjektů (viz Graf 14). **Často zmiňované jsou taktéž novější formy phishingu, zejména tzv. vishing, smishing či quishing.**

## Různé druhy phishingu, které respondenti během roku 2023 zaznamenali (% respondentů)




*Graf 14*

Mezi nově zaznamenané trendy pak řada respondentů řadí podvodné CEO e-maily, tedy snahu útočníků autorizovat převod finančních prostředků pod falešnou identitou ředitele společnosti, přičemž několik subjektů tento druh hrozby označilo za nejvýznamnější incident roku 2023.

**V jedné z vishingových kampaní poté došlo i ke zneužití identity NÚKIB** (viz kapitola Finanční sektor)**.**

Obecně lze také říci, že kvalita všech druhů phishingu se opět meziročně zdokonalila.

**Podle výpovědí respondentů phishingové pokusy vypadají věrohodněji, mají často bezchybnou češtinu či velmi konkrétní znalosti o oběti, případně dané společnosti.**

**Je pravděpodobné (55–70 %), že k nárůstu kvality přispívá i dostupnost nástrojů umělé inteligence (artificial intelligence, AI) či proliferace specifických phishingových nástrojů na tzv. dark webu** (viz kapitola Výhled trendů v kybernetické bezpečnosti v ČR na roky 2024 a 2025).

# Phishing

**Podvodné jednání útočníků s cílem získat citlivé informace svých obětí, případně je přimět k určité akci.**

### Vishing

Využití telefonického či internetového hovoru, mohou být zneužita i čísla reálných organizací (tzv. spoofing), jména jejich reálných představitelů či dokonce jejich hlas za pomocí AI

### Smishing

Využívá SMS zprávy, opět často pod falešnou identitou různých institucí, jako jsou banky, dopravní společnosti apod.

### Spear-phishing

Využívá konkrétní znalosti oběti či prostředí, ve kterém oběť pracuje nebo žije

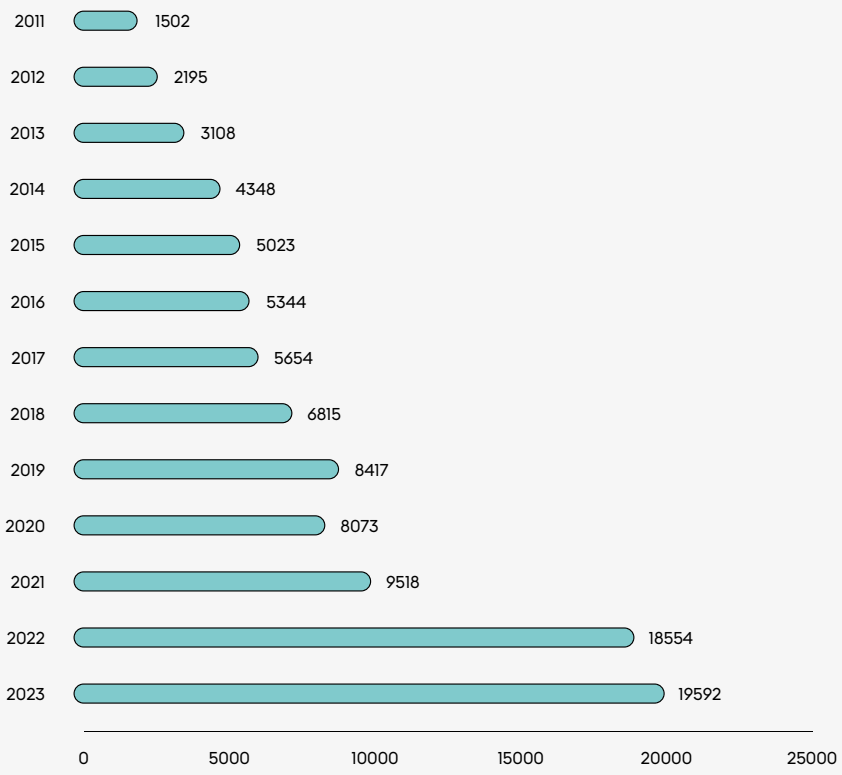
### Quishing

Tato poměrně nová technika zneužívá QR kódy k šíření škodlivých odkazů. Existují případy jejich šíření např. skrze vizitky na společenských akcích

*Vizualizace 3: Představení různých podob phishingu*

# Vývoj kyberkriminality v ČR: pokračující růst trestné činnosti v kyberprostoru

**Podle dat Policie České republiky (PČR) proběhlo v ČR 19 592 skutků trestné činnosti páchané v kyberprostoru, což představuje asi 6% meziroční nárůst.**




**V roce 2022 došlo k výraznému zlomu, kdy meziroční nárůst těchto skutků je téměř dvojnásobný.**

*Graf 15 : Vývoj registrovaných skutků trestné činnosti v kyberprostoru Policií České republiky mezi lety 2011-2023*

Podle vyjádření a dat PČR poskytnutých NÚKIB lze mezi lety 2011 až 2021 hovořit o pozvolném růstovém trendu počtu trestných činů páchaných v kyberprostoru. **V roce 2022 ale došlo k výraznému zlomu, kdy meziroční nárůst těchto skutků je téměř dvojnásobný.** Zatímco v roce 2011 představovala trestná činnost páchaná v kyberprostoru pouze 0,5 % celkové registrované kriminality a v roce 2020 dosahovala 5 %, v roce 2022 dosáhla již podílu více než 10 % (z celkového počtu 181 991 skutků). V roce 2023 pokračoval růstový trend, nicméně došlo k jeho stabilizaci a vývoj celkového počtu trestných činů spáchaných v kyberprostoru se vrací k pozvolnému meziročnímu nárůstu.

Preventivním působením došlo ke zvýšení pozornosti potenciálních obětí vůči aktivitám pachatelů i ke zmenšení zájmu o některé rizikové formy elektronické komunikace (např. u prodejů použitého zboží na bazarových internetových serverech).

Zploštění nárůstu trestné činnosti páchané v kyberprostoru považuje PČR za výsledek mnohačetných preventivních aktivit upozorňujících především na nejčastější formy tzv. ostatní kriminality v kyberprostoru.

# Policejní statistiky kybernetické kriminality se dělí na:

## Komentář PČR

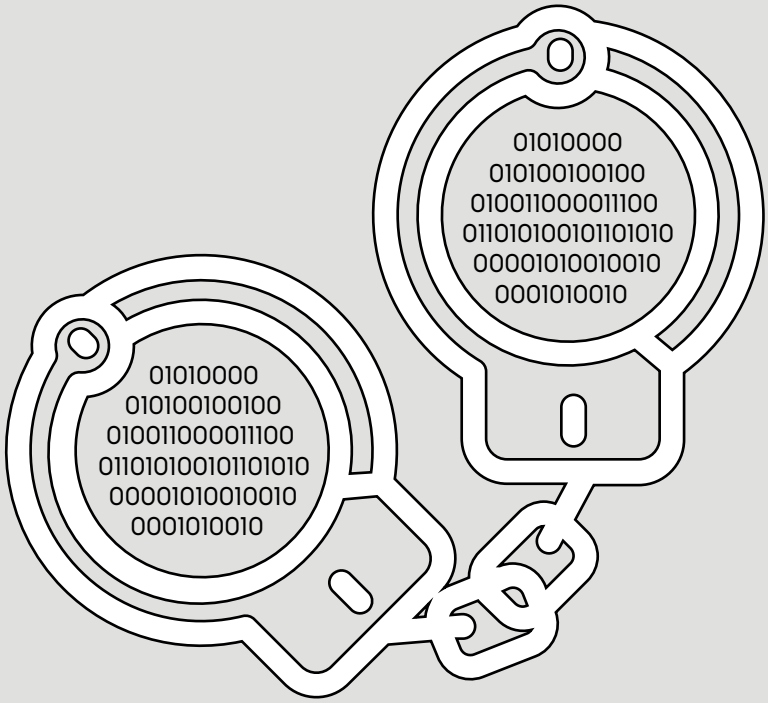
Celková statistická data shromažďovaná od roku 2011 zahrnují obě oblasti trestné činnosti páchané v kyberprostoru, do kterých je v Policii ČR tato oblast od roku 2020 definičně rozdělena.

**Kybernetická kriminalita**

Kriminalita směřující proti informačním a komunikačním technologiím a v nich obsaženým datům. Toto jednání lze označit za „hacking“ páchaný „hackery“, který z dlouhodobého hlediska představuje technologicky velmi náročnou výzvu, ohrožující občanskou i národní bezpečnost. V anglickém jazyce se pro tento druh kriminality užívá označení „cyber-dependent crime“.

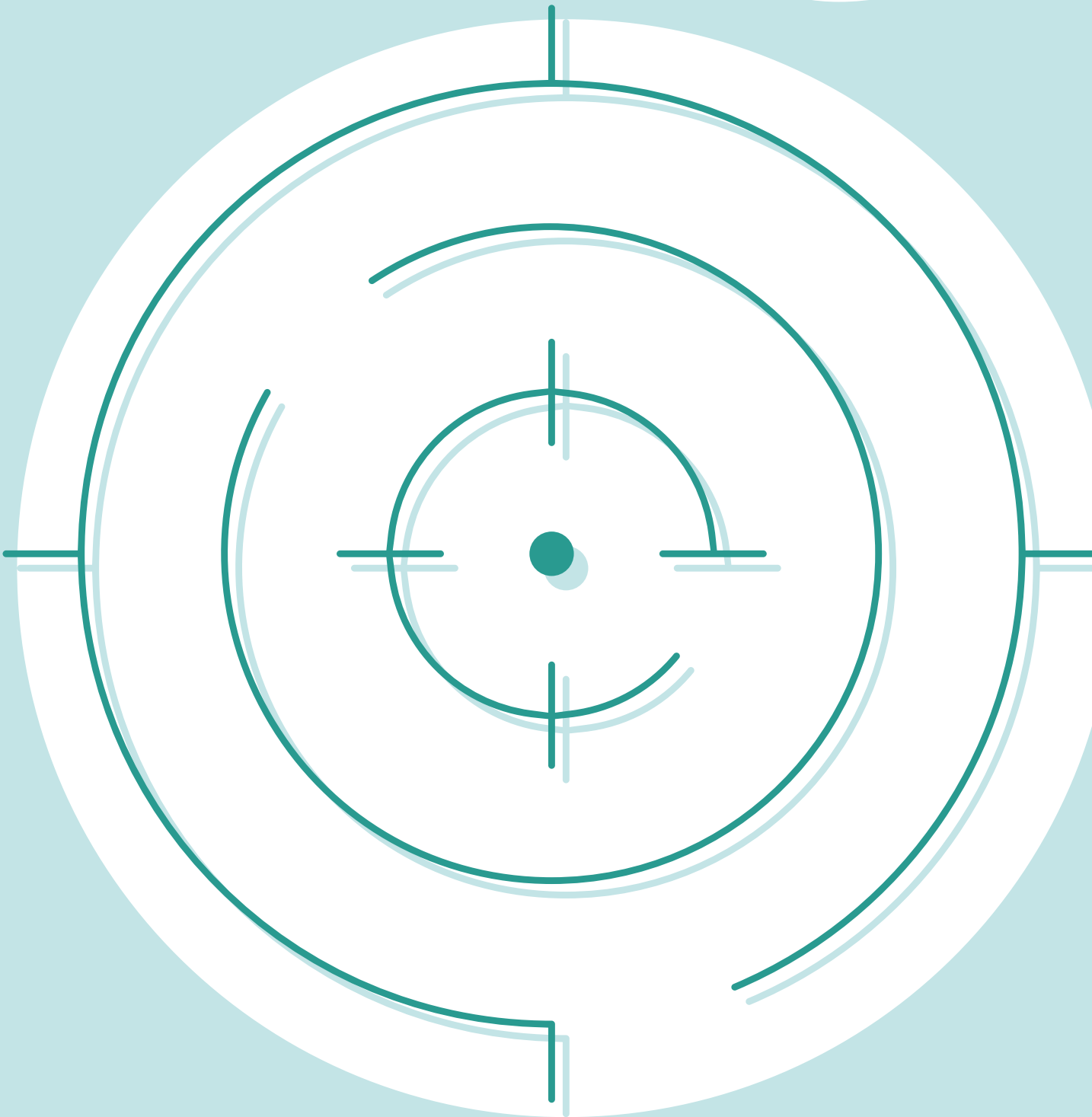
**Ostatní kriminalita páchaná v kyberprostoru**

Zjednodušeně „běžná obecná a hospodářská kriminalita“ ve formě například podvodů, vydírání, nenávistných projevů, sexuálního zneužívání, distribuce drog a dalších, ke které je informačních a komunikačních technologií (počítačů či mobilních telefonů) pouze využito jako prostředku jejich spáchání. I v tomto případě se může jednat o kriminální činnost komplikovanou, zejména často jejím zacílením na obrovské množství poškozených či zacílením na významné subjekty, za využití moderních způsobů anonymizované komunikace atd.



# Cíle kybernetických útoků

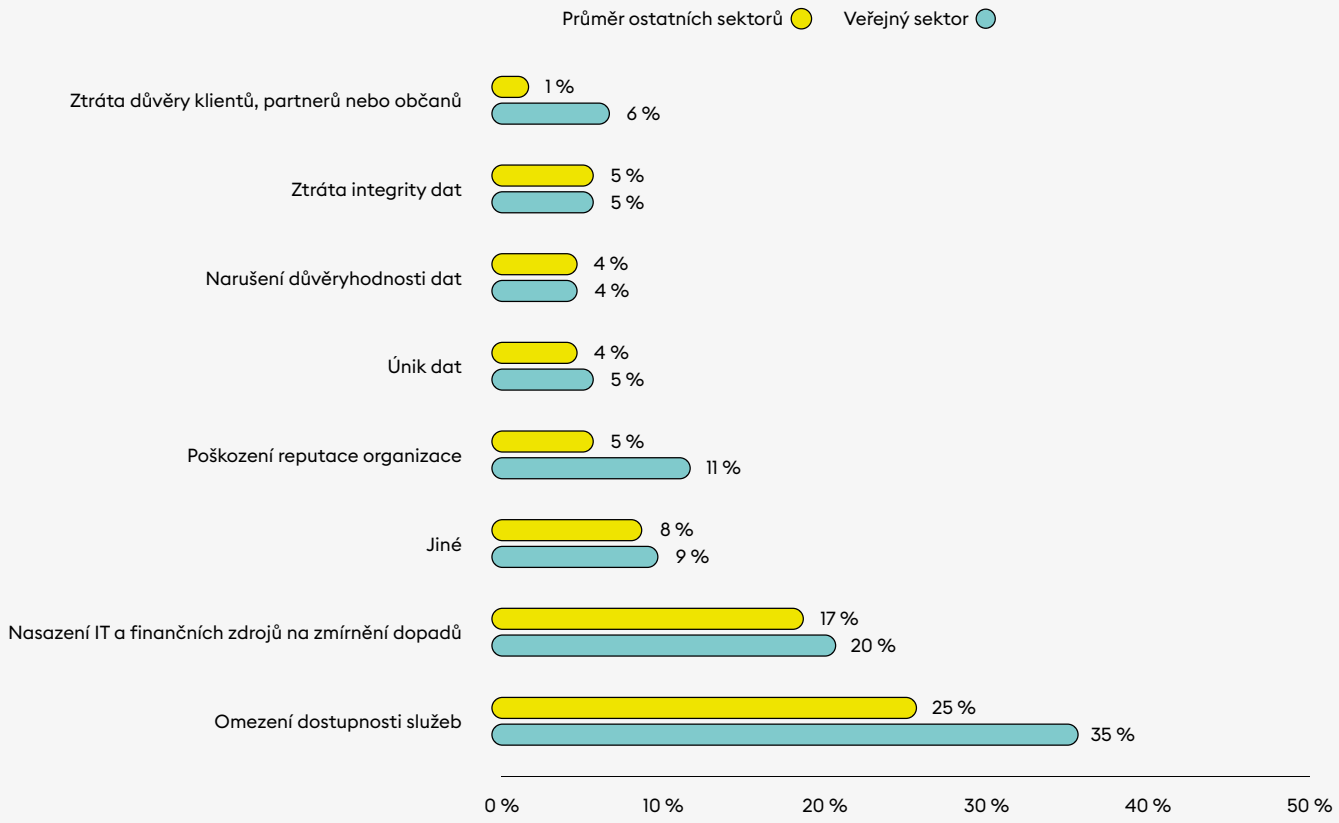
3



# Veřejný sektor: útočníci chtějí především omezit dostupnost dat a služeb

Veřejný sektor se dlouhodobě řadí k těm exponovanějším a tento trend pokračoval i v roce 2023. Letos byl evidován nárůst počtu pokusů o útok i kyberbezpečnostních incidentů. Meziročně však klesla jejich závažnost, což se promítlo též do dopadů incidentů.

**Dopady kybernetických incidentů, srovnání výpovědí respondentů veřejného sektoru oproti průměru (% respondentů)**



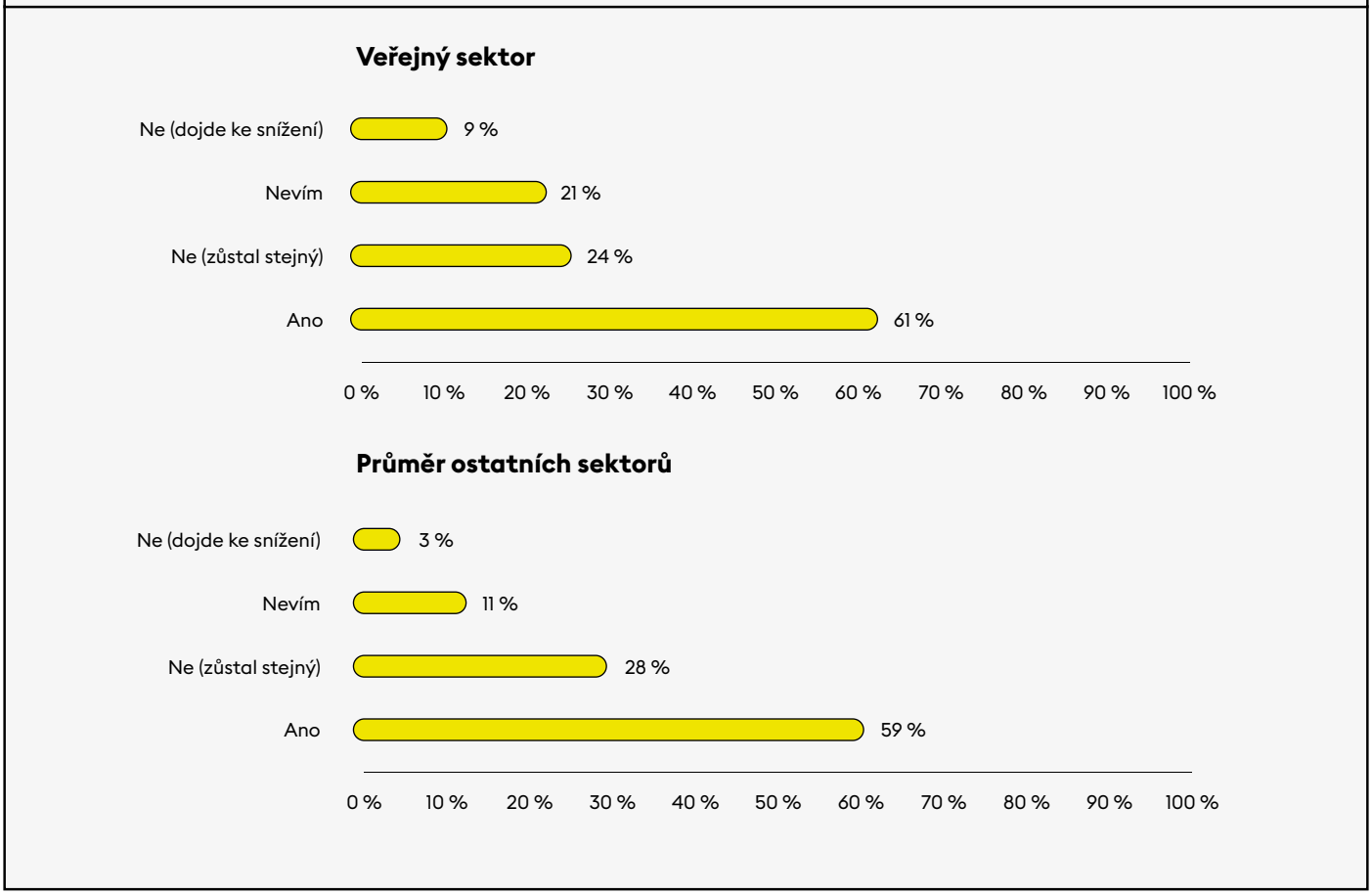

**Největší počet kybernetických útoků směřoval na dostupnost dat, a to ve větší míře než u ostatních sektorů.**

*Graf 16*

Hlavní příčinou byly DDoS kampaně, vedené proti českým vládním a veřejným institucím. Oproti minulému roku poklesla jejich přímá vazba na konkrétní kroky České republiky v souvislosti s podporou Ukrajiny, ale i přesto je většinu těchto kampaní možné přisoudit ruskojazyčným aktérům. **Stejně jako v minulém roce se však jednalo o méně sofistikované útoky, jež byly limitované v reálných dopadech.**

Veřejný sektor se dlouhodobě potýká s nedostatkem financí na kybernetickou bezpečnost. Více než polovina respondentů hodnotí finance vyčleněné na kybernetickou bezpečnost jako nedostatečné.

**Plánuje Vaše organizace zvýšit pro příští rok rozpočet alokovaný na kybernetickou bezpečnost? Srovnání veřejného sektoru oproti průměru (% respondentů)**




*Graf 17*

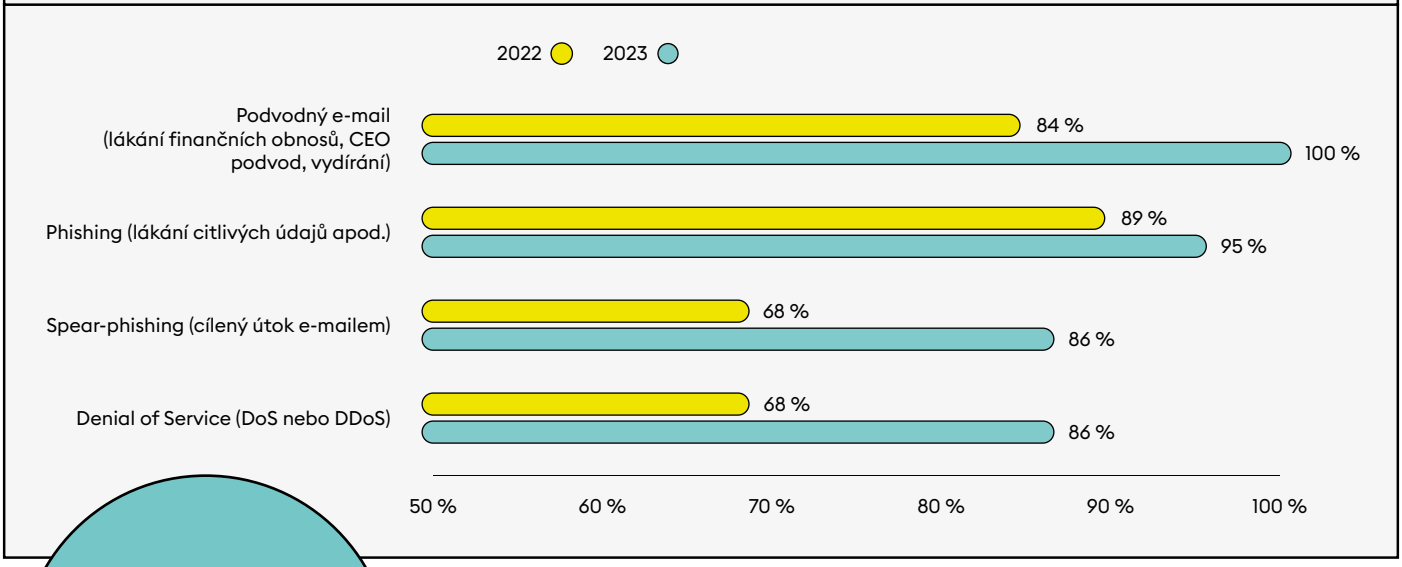
Pohled na očekávanou výši rozpočtu na kybernetickou bezpečnost veřejných institucí ukazuje, že o šest procent více respondentů oproti národnímu průměru indikuje jeho snížení (viz Graf 17). Drobným pozitivem může být, že jeho zvýšení očekává většina respondentů, a to dokonce o dvě procenta větší, než je průměr ostatních sektorů. Stále zde však platí, že toto navýšení může být pouze snahou vyrovnat historické inflační tlaky.

Hlavním faktorem negativně ovlivňujícím výšku rozpočtu pak byl velmi pravděpodobně (75–85 %) vládní konsolidační balíček, který mimo jiné snižuje finanční prostředky dostupné veřejnému sektoru.

# Finanční sektor: útoky na dostupnost bankovních služeb či pokročilé podvody na klienty

Finanční sektor, stejně jako sektor veřejný z předchozí kapitoly, byl v uplynulém roce zasažen nárůstem DDoS útoků ruskojazyčných hacktivistů. Veřejný sektor podobné hrozbě čelil již během roku 2022, zatímco pro sektor finanční, zejména banky, se jednalo spíše o nový trend útoků v kontextu konfliktu na Ukrajině.

**Počet respondentů finančního sektoru, kteří zaznamenali různé formy phishingu či útoků na dostupnost (% respondentů)**




*Graf 18*

Počet respondentů, kteří se s DDoS útoky v roce 2023 setkali, vzrostl téměř o 20 %

Téměř dvě třetiny respondentů z finančního sektoru zároveň uvedly, že útoky měly vliv na dostupnost služeb. **Jednalo se zejména o různé aplikace či funckionality internetového bankovnictví či webové stránky, nicméně jejich výpadky trvaly řádově maximálně hodiny. Přibližně polovina subjektů zároveň uvedla DDoS útok jako nejzávažnější incident roku.**

## Podvodná telefonická kampaň zneužívající mj. identitu NÚKIB

V rámci jedné z podvodných kampaní, na níž NÚKIB upozornil v srpnu roku 2023, došlo také ke zneužití identity NÚKIB spolu s několika bankovními institucemi. **Útočníci se vydávali buď přímo za zaměstnance NÚKIB, včetně podvržení reálných telefonních čísel (tzv. spoofing) či za zaměstnance bankovní instituce pouze s odkazem na zaměstnance NÚKIB.** V obou případech se podvodníci snaží pod časovým nátlakem přesvědčit své oběti, že kvůli různým hrozbám je potřeba převést finanční částku z jejich bankovních účtů na „rezervní záložní účet". Zastřešují se při tom mj. tím, že celá transakce je pod dozorem NÚKIB. Pro větší důvěryhodnost pak používají útočníci jména zaměstnanců úřadu, která čerpají z veřejně dostupných zdrojů. Jedním z jejich podpůrných argumentů je, že si lze jméno zaměstnance ověřit telefonicky přímo u NÚKIB nebo ze zmíněných veřejně dostupných zdrojů.

Kontinuální hrozbu pro finanční sektor dlouhodobě představují taktéž různé formy phishingu či podvodných e-mailů. **Hrozba se přitom týká nejen zaměstnanců daných společností, ale i jejich klientů, kdy řada respondentů potvrzuje obecný trend rostoucího počtu i sofistikovanosti phishingových útoků s cílem vylákat z obětí finanční prostředky.**

# Průmysl a energetika: sofistikovanější metody phishingu používané pravděpodobně za pomoci umělé inteligence

S ohledem na velké množství navázaných služeb je energetika mimořádně kritickým sektorem. Pravděpodobnost jejího zacílení byla v roce 2023 dále zvýšena pokračujícím konfliktem na Ukrajině a snahami Evropské unie přeorientovat se na dovoz energetických produktů z jiných trhů (např. Norsko, USA, Ázerbájdžán nebo země Perského zálivu). V návaznosti na izraelsko-palestinský konflikt se stal minulý rok terčem kyberútoků i český vodohospodářský sektor.

V roce 2023 čelilo 63 % dotazovaných organizací z energetického a průmyslového sektoru pokusům o kybernetický útok.

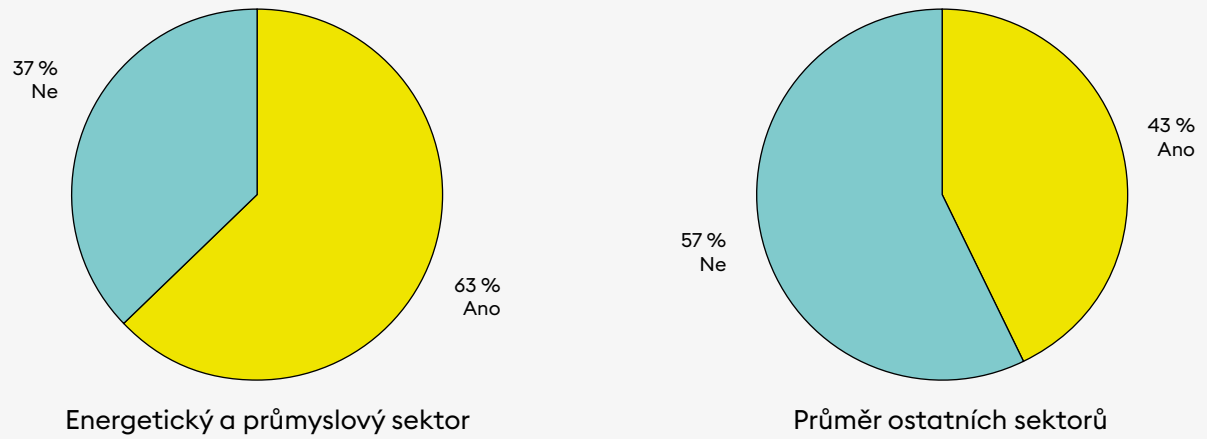
## Proíránský aktér cílil na subjekty používající technologie izraelské společnosti Unitronics

V minulém roce bylo několik subjektů působících ve vodohospodářském sektoru zacíleno proíránskou skupinou. Stalo se tak v rámci globální kampaně útočící na subjekty používající přístroje izraelské společnosti Unitronics. Ačkoliv se útoky do chodu zařízení výrazněji nepromítly, tato kampaň představuje příklad, jakým způsobem může mít mezinárodní konflikt dopad na české subjekty.

**Energetický a průmyslový sektor se taktéž liší od zbytku sektorů spokojeností s financemi alokovanými do kybernetické bezpečnosti.** Přibližně 63 % respondentů z energetického a průmyslového sektoru je s financemi spokojeno, přičemž více než 60 % plánuje ještě dále rozpočet navyšovat i v příštím roce. V ostatních sektorech souhrnně je spokojeno pouze 43 %, přičemž navýšení očekává zhruba polovina (viz Graf 19).

Ačkoliv je dlouhodobě nejčastějším typem útoků phishing, v loňském roce byl nově pozorovaným trendem, podobně jako ve finančním sektoru, především nárůst v sofistikovanosti těchto útoků. Důvěryhodnost a propracovanost phishingových e-mailů respondenti přičítají používání nástrojů umělé inteligence. Simulované phishingové kampaně však v roce 2023 přesto prováděla méně než polovina dotazovaných organizací v energetickém a průmyslovém sektoru, přičemž 35 % neprovádělo jakékoliv testy vůči kybernetickým hrozbám. Tato situace může souviset s tím, že respondenti tento typ útoků vnímají jako méně závažný. Nicméně právě phishing často bývá prvotním vektorem kybernetických útoků.

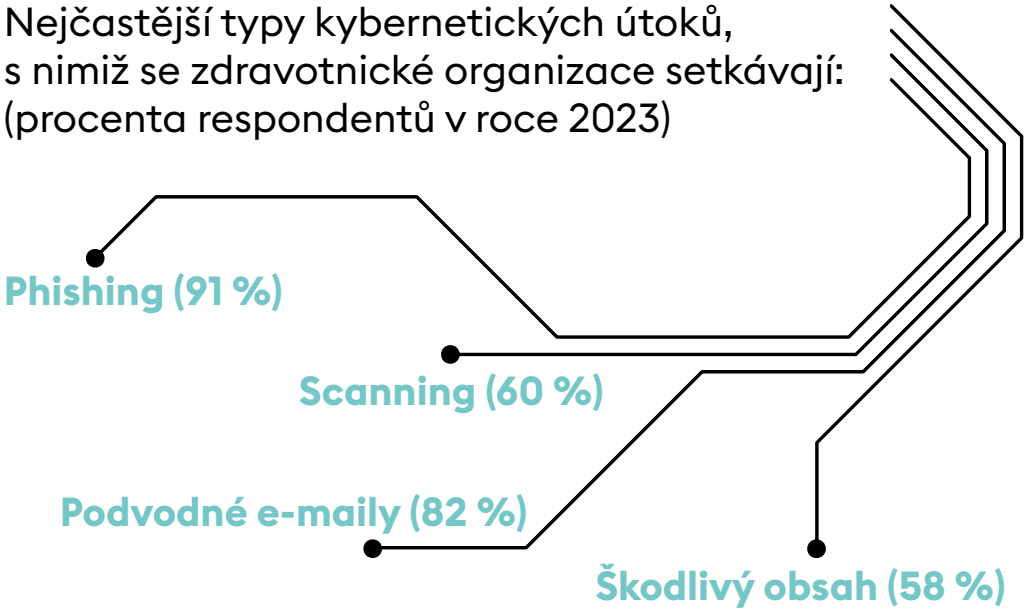
**Spokojenost s výší rozpočtu na kybernetickou bezpečnost, srovnání energetického a průmyslového sektoru oproti průměru (% respondentů)**



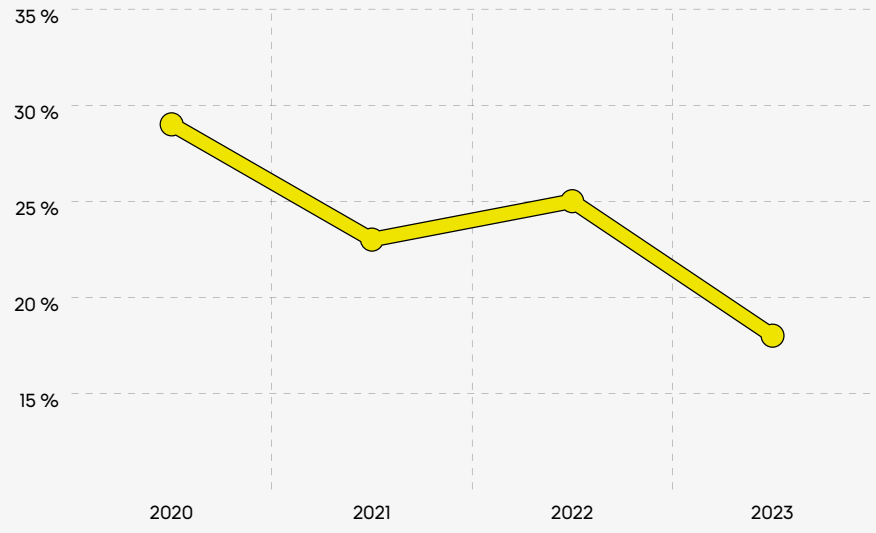

*Graf 19*

# Zdravotnictví: nejčastější hrozbou je phishing a podvodné e-maily, ransomwarových útoků bylo zachyceno nejméně od roku 2020

Nejčastější typy kybernetických útoků, s nimiž se zdravotnické organizace setkávají: (procenta respondentů v roce 2023)




**Počet ransomwarových útoků ve zdravotnickém sektoru zaznamenalo 18 % respondentů, což poukazuje na pozvolný dlouhodobý pokles.**

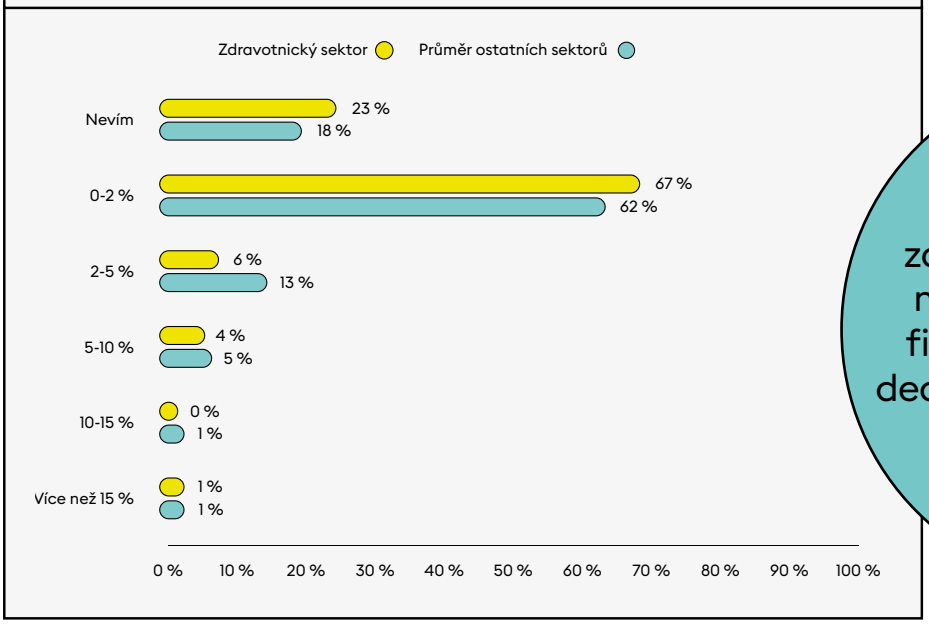



*Graf 20: Vývoj podílu respondentů zdravotnického sektoru, kteří za daný rok zaznamenali ransomware (ať už pokus či úspěšný útok), data 2020-2023 (% respondentů)*

## Navzdory přetrvávajícím hrozbám však stále téměř polovina institucí ve zdravotnickém sektoru své zaměstnance proti útokům netestuje.

Oproti roku 2022, kdy své zaměstnance netestovalo 53 % dotazovaných institucí, tak v uplynulém roce došlo k mírně pozitivnímu vývoji, nicméně 47 % organizací stále neprovádí žádná testování, ať už formou simulovaných phishingových kampaní či penetračním testováním.

## Podíl financí vyčleněných na kybernetickou bezpečnost z celkového rozpočtu zůstává jako v předchozích letech převážně v nízkých jednotkách procent, kdy 67 % organizací vynakládá 0–2 %.

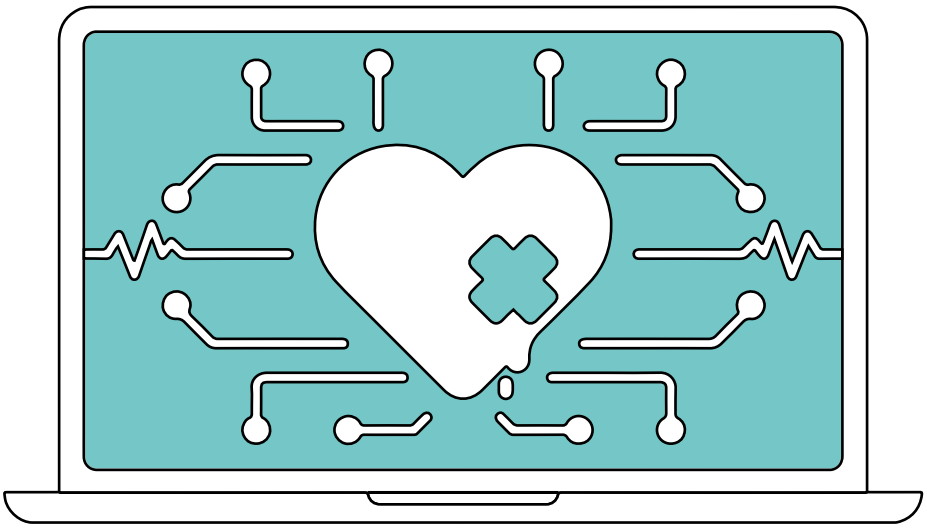



*Graf 21: Podíl rozpočtu alokovaného na kybernetickou bezpečnost z celkového rozpočtu organizací, srovnání zdravotnického sektoru oproti průměru (% respondentů)*

**Při pohledu na podíl vyčleněných financí na kybernetickou bezpečnost zdravotnický sektor zaostává za národním průměrem (viz Graf 21).**

Celých 61 % respondentů zdravotnického sektoru nepovažuje vyčleněné finance své organizace dedikované na kybernetickou bezpečnost za dostatečné.

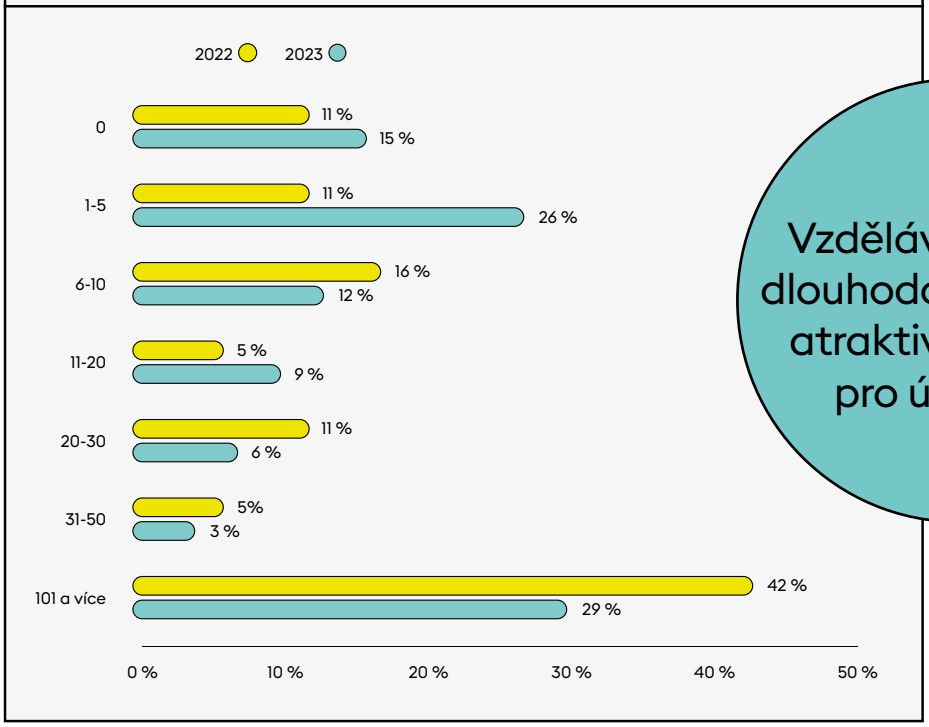
Drobnou pozitivní zprávou je, že celkem 87 % respondentů indikovalo zlepšení úrovně kyberbezpečnosti ve své organizaci oproti roku 2022 (38 % určitě ano, 49 % spíše ano), což může signalizovat postupné navyšování kyberbezpečnosti napříč celým sektorem.



# Vzdělávací sektor: exponovaný sektor, na který cílí kyberzločinci i státem podporovaní aktéři

Akademický výzkum představuje hodnotný cíl pro státem sponzorované skupiny a jejich kampaně se nevyhýbají ani českým univerzitám. Nejméně jedna česká vzdělávací instituce zaznamenala a v roce 2023 mitigovala následky kampaně, kterou připsala státem podporovanému aktérovi.

**Srovnání počtu zaznamenaných pokusů o kybernetický útok respondenty vzdělávacího sektoru (% respondentů)**




*Graf 22*

Daný sektor pak vykazuje větší podíl pokusů o kybernetický incident než ostatní sektory, a to i přes zlepšení ve srovnání s loňským rokem (viz Graf 22). Toto lze pozorovat především v krajních hodnotách škály.

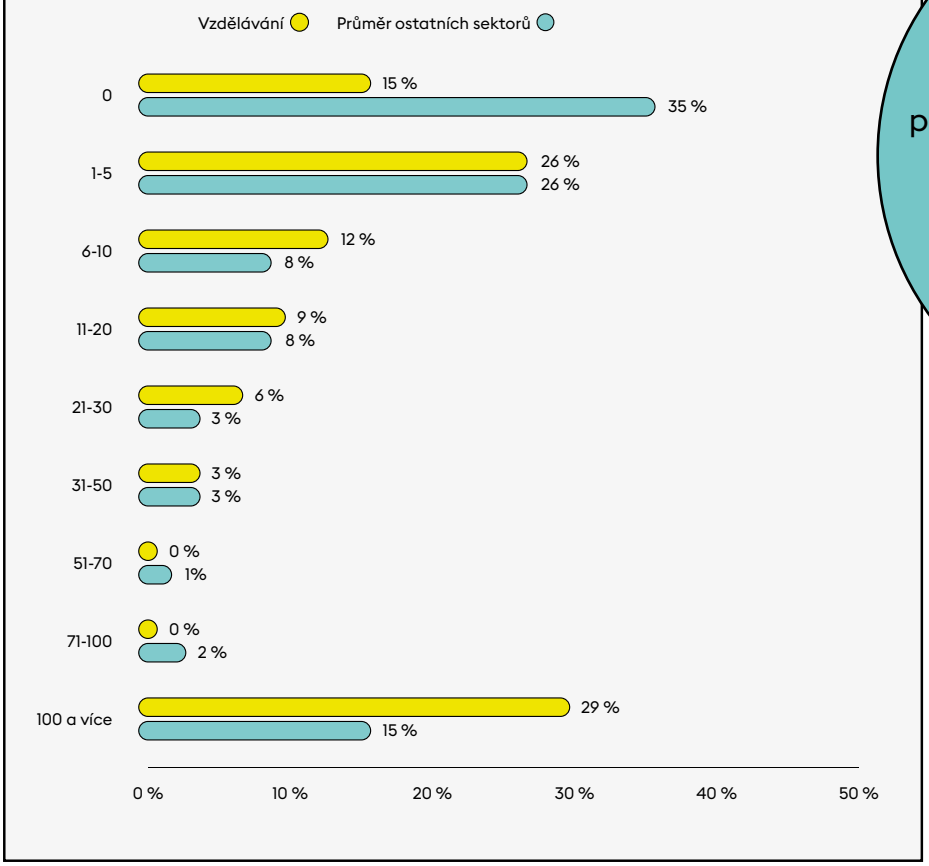
Vzdělávací sektor dlouhodobě zůstává atraktivním cílem pro útočníky.

Jak v krajní kategorii 101 a více, která o 13 % převyšuje průměr, tak skrze množství respondentů ze vzdělávacího sektoru, kteří uvedli, že se nestali cílem žádného pokusu o útok (a jsou tak přibližně o 4 % pod průměrem)(viz Graf 23).

**Medializovaným incidentem v sektoru vzdělávání byl ransomwarový útok kyberzločineného aktéra Monti vedený proti Univerzitě obrany v Brně (UNOB), který byl poprvé detekován 11. září.**

Kromě zašifrování dat použila skupina takzvané dvojité vydírání (double extortion), kdy docházelo k výhrůžkám, že v případě nezaplacení výkupného budou data zároveň zveřejněna na internetu. **Potom co univerzita odmítla se tak skutečně stalo a mezi zveřejněnými dokumenty byly například osobní údaje vyučujících důstojníků, zápisy z porad nebo studijní plány.** Vzhledem k povaze instituce mohou být tyto informace cenné i pro státní aktéry. Univerzitě se sice podařilo zašifrovaná data obnovit ze záloh, nicméně jejich krádež proto představuje závažný incident.

## Počet zaznamenaných pokusů o kybernetický útok respondenty vzdělávacího sektoru oproti průměru (% respondentů)

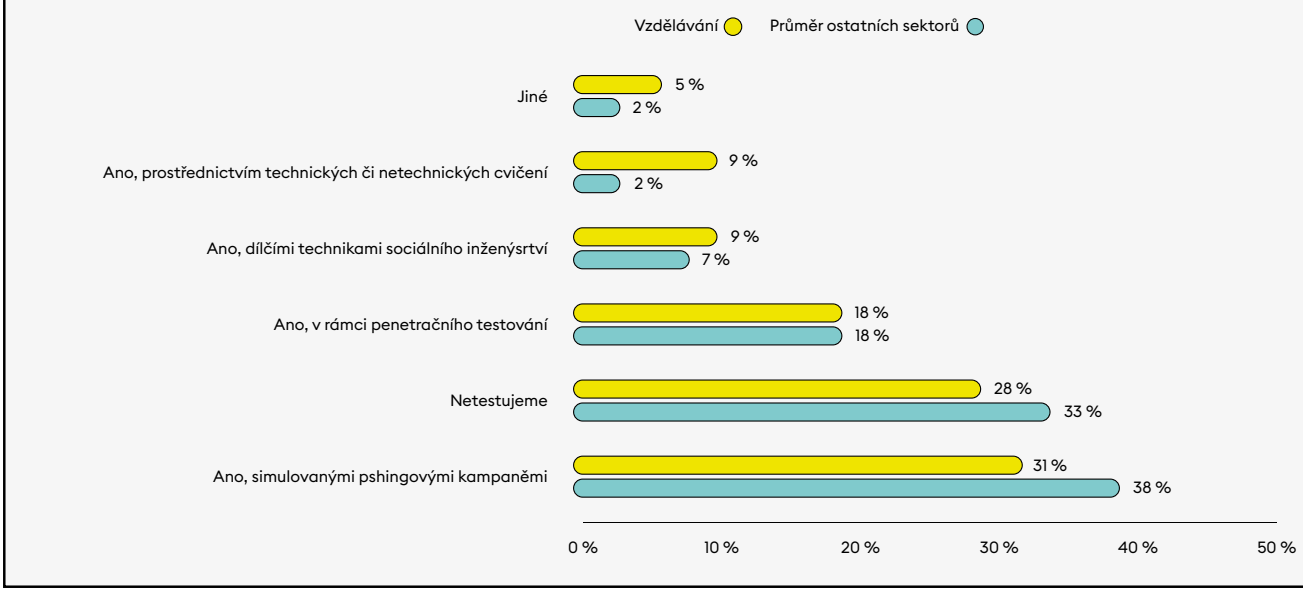



*Graf 23*

Pokračujícím trendem je pak převaha phishingu a podvodných e-mailů. Ty jakožto nejčastější metoda o pokus o průnik do sítě tvoří téměř dvě třetiny všech forem zaznamenaných pokusů.

Ke snížení tohoto rizika může přispět mj. i testování odolnosti uživatelů pomocí simulovaných phishingových kampaní. Oproti minulému roku zde došlo k mírnému zlepšení, kdy více organizací v sektoru začalo tyto kampaně provádět (viz Graf 24). Respondenti ze vzdělávacího sektoru dále uvedli, že více jak 67 % všech pokusů o útok nevedlo k žádnému incidentu. I v tomto ohledu ovšem vzdělávací sektor mírně zaostává za průměrem a vykazuje tak svou exponovanost.

## Srovnání přístupu k testování zaměstnanců vůči kybernetickým hrozbám organizací vzdělávacího sektoru oproti průměru (% respondentů)




*Graf 24*

# Časová osa vybraných varování a upozornění NÚKIB v roce 2023

## Únor

**Upozornění na zneužití dokumentů OneNote ke stahování malware**

První upozornění roku 2023 vydal NÚKIB v únoru. Varovalo před aktivní phishingovou kampaní zneužívající aplikaci Microsoft OneNote. Útočníci konkrétně zneužívali funkcionality OneNote, která po spuštění souboru dovolí aktivovat i skript. Ten poté stáhne malware zajišťující vzdálený přístup útočníka.

## Březen

**Varování před hrozbou aplikace TikTok**

NÚKIB v březnu vydal varování před hrozbou spočívající v instalaci a používání aplikace TikTok. K vydání tohoto varování vedla NÚKIB kombinace vlastních poznatků a zjištění spolu s informacemi od partnerů. Obava z možných bezpečnostních hrozeb vyplývá především z množství shromažďovaných dat o uživatelích a způsobu, jakým jsou sbírána, nakládání s nimi a v neposlední řadě také z právního a politického prostředí Čínské lidové republiky.

## Červen

**Upozornění před zvýšeným rizikem ransomwarových útoků**

Červnové upozornění poté reagovalo na zvýšenou aktivitu kyberzločineckých skupin používajících ransomware. Součástí upozornění byl seznam útočníky využívaných zranitelností, ale i popis dalších obvyklých vektorů kompromitace. V kontextu upozornění došlo též k aktualizaci dokumentu Ransomware: Doporučení pro mitigaci, prevenci a reakci, který obsahuje ucelený přehled informací v kontextu této hrozby.

## Červenec

**Upozornění na zranitelnost MikroTik RouterOS**

V červenci došlo ke zveřejnění zranitelnosti routerů s operačním systémem MikroTik RouterOS. CVE-2023-30799 umožňovala útočníkům potenciální eskalaci privilegií pomocí brute-force útoku na kombinaci login:heslo. NÚKIB na tuto hrozbu upozornil a doporučil i sadu mitigačních opatření.

## Říjen

**Upozornění na zranitelnosti Cisco IOS XE**

V říjnu byly odhaleny dvě zranitelnosti rozhraní operačního systému Cisco IOS XE. První z nich (CVE-2023-20198) měla nejvyšší možné hodnocení závažnosti 10, druhá (CVE-2023-20273) poté 7,2. Před oběma NÚKIB vydal **upozornění**.

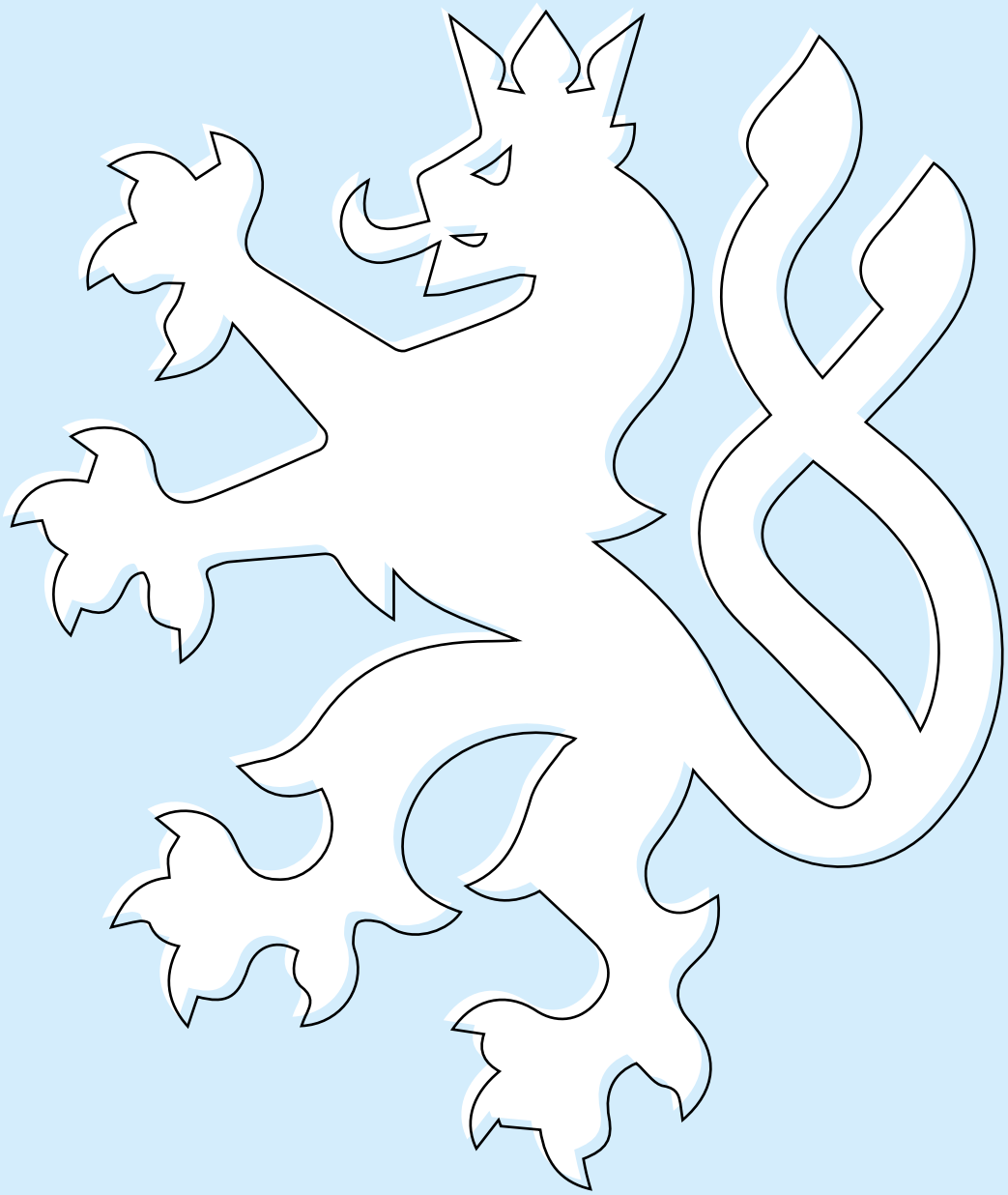
## Listopad

**Upozornění na hrozbu spojenou s aplikací WeChat společnosti Tencent**

Koncem roku vydal NÚKIB **upozornění** před hrozbou v oblasti kybernetické bezpečnosti spočívající v používání mobilní aplikace WeChat a její čínské verze Weixin společnosti Tencent. Obdobně jako v případě aplikace TikTok je hrozbou kombinace velkého objemu sbíraných uživatelských dat, jejichž množství a způsob sběru mohou sloužit k přesnému zacílení kybernetických útoků, působení v právním prostředí Čínské lidové republiky (ČLR) a vlivové působení ČLR v České republice vede k důvodné obavě ze zneužití dat, která aplikace shromažďuje.

# Národní úroveň kybernetické bezpečnosti

4



# Projekt BIVOJ

V roce 2023 NÚKIB ve spolupráci s partnery pokračoval v práci na Projektu BIVOJ.

Cílem je vytvoření jednotné, funkční a bezpečné sdílené platformy poskytující bezpečnostní a komunikační služby, do které budou postupně připojeny instituce veřejného sektoru. Ačkoliv je Projekt stále ve fázi strategického rozpracování, již nyní se daří naplňovat některé jeho části.

Za koordinace místopředsedy vlády pro digitalizaci a blízké součinnosti NÚKIB probíhá migrace ústředních orgánů státní správy na jednotnou státní doménu gov.cz.
Tato jednotná doména zvýší uživatelskou přívětivost pro občany, právní jistotu a zvýší odolnost proti DDoS útokům.

# Bezpečnost dodavatelského řetězce

V důsledku zavedení mechanismu by mělo dojít k významnému omezení dopadu hrozeb plynoucích z dodavatelského řetězce pro nejvýznamnější ICT infrastruktury státu, mezi které patří například narušení bezpečnosti dodávek prostřednictvím vlivu cizích států na dodavatele.

Na základě pověření Bezpečnostní rady státu z června roku 2022 připravuje NÚKIB mechanismus prověřování bezpečnosti dodavatelského řetězce, který by státu umožnil prověřovat a omezovat rizika spojená s dodavateli technologií do strategicky významné infrastruktury.

Mechanismus je připravován jako součást návrhu nového zákona o kybernetické bezpečnosti a sestává se ze dvou částí – oprávnění NÚKIB a dalších relevantních orgánů státu dodavatele prověřovat a oprávnění omezit ICT dodávky těch dodavatelů, kteří budou v důsledku prověření vyhodnoceni jako vysoce rizikoví.

Navrhovaný proces prověřování a omezování hrozeb dopadá pouze na bezpečnostně nejkritičtější dodávky a obsahuje řadu nástrojů pro zamezení nežádoucího dopadu mechanismu, jako je možnost správců dotčené infrastruktury připomínkovat návrh omezení dodavatele nebo výjimky z omezení dodavatelů nenahraditelných technologií. Návrh mechanismu byl v roce 2023 společně se zbytkem zákona finalizován a po dokončení meziresortního připomínkového řízení předložen do dalších fází legislativního procesu.

# Předcházení kvantové hrozbě

Kvantové počítače v současné době zaznamenávají velký rozmach a s tím spojený zájem ze strany odborné i laické veřejnosti. S rozvojem schopností kvantových počítačů ovšem nabývá konkrétnějších rozměrů také hrozba prolomení současných kryptografických standardů zajišťující informační a kybernetickou bezpečnost.

V reakci na to NÚKIB vydal sadu podpůrných materiálů (přehledový dokument, minimální požadavky na kryptografické algoritmy a příloha k minimálním požadavkům) s cílem jednak objasnit povahu této hrozby, jednak popsat kroky, jež bude v následujících letech třeba podniknout, aby bylo této hrozbě předejito ve vztahu ke kryptografické ochraně a celkově kybernetické bezpečnosti.

# Koordinované zveřejňování zranitelností

NÚKIB finalizoval podobu návrhu národní politiky koordinovaného zveřejňování zranitelností (CVD), včetně detailní právní analýzy relevantních právních aspektů CVD. Na přelomu roku 2022 a 2023 vstoupila v platnost směrnice NIS 2, která mj. zavádí konkrétní povinnosti pro členské státy Evropské unie ve vztahu k CVD[6].

Ty NÚKIB zohlednil do návrhu nového zákona o kybernetické bezpečnosti, zejména v určení vládního CERT jakožto koordinátora pro účely CVD a výslovného zakotvení, že každá osoba může i anonymně koordinátorovi hlásit nalezené zranitelnosti v ICT produktech.

[6] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148

## Legislativní ukotvení:

# Nový zákon o kybernetické bezpečnosti

Na konci roku 2022 byla publikována směrnice Evropského parlamentu a Rady EU NIS 2. Ta významným způsobem prohlubuje harmonizaci regulace kybernetické bezpečnosti v Evropské unii, přičemž vyžaduje významné změny v dosavadním pojetí zákonné regulace kybernetické bezpečnosti v České republice.

**S ohledem na množství změn, které NIS 2 přináší a které je nutné propsat do národního práva, a v zájmu zajištění přehlednosti a srozumitelnosti zákonné úpravy, bylo přistoupeno k sepsání nového zákona o kybernetické bezpečnosti namísto pouhé novelizace stávajícího.** NÚKIB využil této příležitosti a do návrhu nového zákona včlenil též dosavadní zkušenosti s aplikací zákona č. 181/2014 Sb. a relevantní podněty subjektů, které se ustanoveními aktuálního zákona řídí.

Rok 2023 se tedy obdobně jako předchozí rok nesl ve znamení projednávání a vytváření návrhu nového zákona, konzultace se zainteresovanými subjekty (regulovanými osobami a gestory regulovaných odvětví) stejně jako s širokou veřejností a zahájení formálního legislativního procesu. Paralelně s tím NÚKIB pokračuje v intenzivní informační kampani k návrhu zákona (zejm. prostřednictvím dedikovaných internetových stránek, přednáškové činnosti a reakci na četné dotazy).

# Evropská certifikační schémata kybernetické bezpečnosti

**Zavedení evropských certifikačních schémat kybernetické bezpečnosti představuje krok směrem ke sjednocení a posílení bezpečnostních standardů v digitálním prostoru Evropské unie.**

Momentálně na evropské úrovni vznikají tři certifikační schémata – EUCC (European Common Criteria-based cybersecurity certification scheme), EUCS (European Cybersecurity Certification Scheme for Cloud Services) a EU5G (EU 5G Cybersecurity certification scheme).
Během roku 2023 práce pokročila a na konci ledna 2024 byl publikován implementační akt ke schématu EUCC (IA EUCC). U návrhu kandidátského schématu EUCS probíhají diskuze na úrovni ECCG (Evropská skupina pro certifikaci kybernetické bezpečnosti). Kandidátské schéma pro 5G bude teprve představeno, snad v průběhu roku 2024.

# Dozorová činnost NÚKIB v roce 2023

Rok 2023, stejně jako rok 2022, byl z pohledu kontrolní a auditní činnosti ovlivněn eskalací geopolitické situace ve světě. I v tomto roce jsme proto pokračovali prověřováním kybernetické bezpečnosti klíčových subjektů, zajišťujících základní fungování státu, a především služeb občanům.

Celkem bylo v roce 2023 provedeno 20 auditů a kontrol podle zákona o kybernetické bezpečnosti, respektive jeho prováděcí vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů.

**Nad rámec standardních auditů a kontrol byl taktéž vykonán tzv. komplexní audit, který zahrnuje nejenom samotné ověření stavu organizace formou auditu, v rámci kterého jsou prováděny rozhovory a případné ukázky reálného nastavení některých zařízení, ale i penetrační testování, skenování zranitelností a table top cvičení.**

Na komplexním auditu se podílí několik odborů NÚKIB (Odbor kontroly, Odbor vládní CERT, Odbor cvičení a vzdělávání). Takto provedený komplexní audit poskytuje organizaci úplnou zpětnou vazbu o stavu kybernetické bezpečnosti a její připravenosti čelit případným kybernetickým bezpečnostním incidentům.

Dále byl ve spolupráci se sdružením CZ.NIC na základě usnesení vlády České republiky ze dne 11. ledna 2023 č. 23 o záměru migrace na jednotnou doménu a vytvoření jednotné vizuální identity ústředních orgánů státní správy proveden audit domény gov.cz.

# Cvičení kybernetické bezpečnosti:

**12**
**Národní cvičení**

**1645**
**Počet účastníků**

**3**
**Mezinárodní cvičení**

## TELCO23

V roce 2023 se NÚKIB v oblasti cvičení zaměřil mimo jiné na sektor telekomunikací a v říjnu uspořádal cvičení TELCO23 – netechnické table-top cvičení, jehož se zúčastnili zástupci vybraných poskytovatelů telekomunikačních služeb.

Cvičení se zaměřilo na ověření, zda jsou bezpečnostní procesy nastavené tak, aby došlo k minimalizaci potenciálních škod způsobených kybernetickým útokem, nebo na to, jak řešit komunikaci směrem k veřejnosti, médiím ale i dovnitř organizace samotné. Jednalo se o dvoudenní aktivitu, při které se setkali zástupci státní správy se zástupci regulovaných subjektů a diskutovali o zajišťování kybernetické bezpečnosti v sektoru telekomunikací a možnostech spolupráce.

## Comm Czech 2023

V srpnu proběhlo komunikační cvičení Comm Czech 2023, jehož cílem bylo ověřit dosažitelnost určených kontaktních osob subjektů regulovaných podle zákona o kybernetické bezpečnosti.

Aktuálnost a dostupnost kontaktních údajů je důležitá především pro případ krize, kdy by vyvstala potřeba s regulovanými subjekty rychle a účinně komunikovat, a tudíž předejít četným škodám.

## Locked Shields

Také v roce 2023 proběhla cvičení s mezinárodním přesahem, mezi něž již tradičně patří cvičení Locked Shields pořádané NATO Cooperative Cyber Defence Centre of Excellence v estonském Tallinnu, které se konalo v dubnu.

## Cyber Coalition

Dále též Cyber Coalition, které proběhlo v listopadu a představuje mezinárodní cvičení kybernetické bezpečnosti, které je pravidelně pořádáno NATO.

# Prevence, osvěta a vzdělávání v kybernetické bezpečnosti v ČR

Stejně jako v předchozím roce, prevence, osvěta a vzdělávání v oblasti kybernetické bezpečnosti byly důležitými tématy při zajišťování kybernetické bezpečnosti a zvyšování odolnosti společnosti v souladu s cíli Národní strategie kybernetické bezpečnosti 2021-2025.

**Potřeba připravenosti občanů ČR k bezpečnému používání digitálních technologií a pohybu v online světě napříč všemi sociálními skupinami nadále přetrvává.**

## Základní školy

Na úrovni základního školství v roce 2023 proto probíhala implementace revidovaného rámcového vzdělávacího programu pro základní vzdělávání. Základní školy měly za povinnost zahájit výuku podle revidovaných RVP obsahující novou informatiku na prvních stupních nejpozději k 1. září 2023.

## Vysoké školy

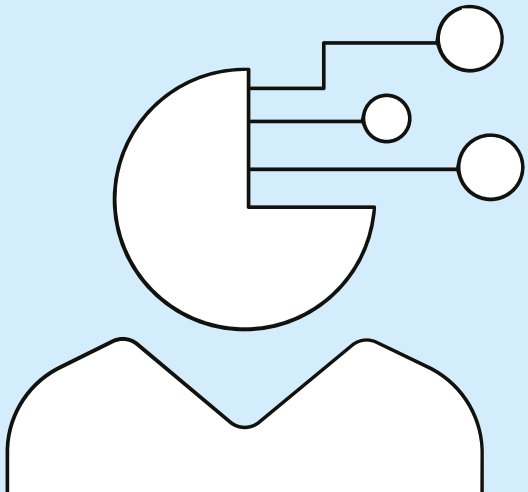
U vysokých škol pokračuje trend mírného růstu počtu studentů studijních programů informačních a komunikačních technologií. Naopak přetrvávajícím negativním trendem je i nadále nedostatečný nárůst počtu připravovaných nebo otevíraných studijních programů zaměřených na kybernetickou bezpečnost.

## Střední odborné školy

V rámci středního odborného vzdělávání došlo s účinností k 1. září 2023 ke změně rámcových vzdělávacích programů, kdy bylo podobně jako u základního vzdělávání a u gymnázií aplikováno nové pojetí informatického vzdělávání (jehož součástí je i kybernetická bezpečnost).

## Rekvalifikační vzdělání

Pozitivní změny proběhly v systému rekvalifikačního vzdělávání. Ministerstvo práce a sociálních věcí (MPSV) zveřejnilo databázi rekvalifikací, ve které je soustředěna nabídka rekvalifikací na jednom místě (včetně kurzů kybernetické bezpečnosti), čímž se usnadňuje orientace a přístup ke potřebnému vzdělání zájemcům o práci v oblasti kybernetické bezpečnosti.



## Konference CyberCon 2023

V září 2023 uspořádal NÚKIB na půdě Fakulty sociálních studií Masarykovy univerzity a v prostorách Provozně ekonomické fakulty Mendelovy univerzity již devátý ročník konference CyberCon.

Hlavním cílem konference je poskytnout prostor pro propojení veřejného, akademického a soukromého sektoru v oblasti kybernetické bezpečnosti. Během třídenního programu si přibližně 350 účastníků mohlo poslechnout přednášky a diskuse reflektující technické, politické i právní aspekty kybernetické bezpečnosti.

Na základě kladných ohlasů z loňského roku byl na začátek konference opět zařazen úvodní workshopový den. Druhý den konference byl věnován novinkám z oblasti regulace, novému zákonu o kybernetické bezpečnosti, analýze rizik veřejných zakázek a dalším tématům z oblasti činnosti povinných osob NÚKIB. Třetí den byl věnován tématu veřejných politik a mimo jiné v rámci něj byly představeny nové státní instituce (DIA, NCTEKK) a proběhla diskuse oslovených politických představitelů nad aktuálními tématy v kyberbezpečnosti.

# Mezinárodní spolupráce:

## Navázání na úspěchy CZ PRES

V roce 2023 NÚKIB navázal na úspěchy českého předsednictví v Radě EU (dále CZ PRES) dalším rozvinutím závěrů Rady EU k bezpečnosti dodavatelských řetězců informačních a komunikačních technologií, které povedou k vytvoření tzv. ICT Supply Chain Toolboxu. Ten bude obsahovat soubor obecných opatření ke snížení kritických rizik dodavatelských řetězců ICT.

NÚKIB v EU projednával návrh nařízení, kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie a které bylo na konci roku 2023 přijato.

Dále byl přijat obecný přístup Rady k návrhu Aktu o kybernetické odolnosti a začala vyjednávání k novým návrhům, Aktu o kybernetické solidaritě a aktualizaci Aktu o kybernetické bezpečnosti; rovněž u obou posledně zmíněných návrhů Rada na konci roku 2023 přijala svůj mandát pro další vyjednávání.

## EU-CyCLONe

Současně s účinností NIS 2 byla zformalizovaná síť styčných úředníků a relevantních úřadů řešících kybernetické krizové řízení (EU-CyCLONe), do níž je NÚKIB zapojen.

## ENISA Support Action

NÚKIB dále zastává roli kontaktního místa pro unijní agenturu pro kybernetickou bezpečnost ENISA a v roce 2023 zprostředkovával pilotní projekt ENISA Support Action k podpoře kybernetické bezpečnosti regulovaných subjektů na území ČR.

## Counter Ransomware Initiative

Úřad pokračoval v zapojení do Counter Ransomware Initiative, v jejímž rámci bylo mj. na podzim 2023 přijato společné prohlášení více než 40 států včetně ČR proti platbám výkupného při ransomwarových útocích. Významnou měrou se NÚKIB zapojil také do přípravy národní pozice k aplikaci mezinárodního práva veřejného v kyberprostoru, kterou připravilo MZV. S MZV také probíhá spolupráce na poli prosazování zahraniční politiky v EU i OSN.

## Prague Cyber Security Conference

V roce 2023 byly zahájeny přípravy na další ročník Prague Cyber Security Conference (PCSC), a to realizací červnové virtuální události Prague Cyber Security Meeting s mezinárodní účastí. PCSC jakožto mezinárodní konference plánovaná na první čtvrtletí 2024 naváže na předchozí ročníky, přičemž se očekává účast širokého globálního publika.

**NÚKIB prostřednictvím svých kyberatašé hájí zájmy ČR v oblasti kybernetické bezpečnosti nejen v EU, ale také ve Výboru pro kybernetickou obranu NATO, a dále pak přispívá k činnosti NATO Cooperative Cyber Defence Centre of Excellence.**

V rámci významného rozvoje bilaterálních vztahů se uskutečnila řada setkání nejen na úrovni ředitele Úřadu. Zahraniční aktivity NÚKIB v Indo-Pacifiku nově pokrývá kyberatašé sídlící v australské Canberře. Nadále pokračoval rozvoj bilaterálních vztahů s klíčovými partnery v EU, USA či Izraeli. Významně se také rozvíjí spolupráce s Ukrajinou a daří se navyšovat účast NÚKIB v projektech rozvojové spolupráce. Pracovníci Vládního CERT taktéž navštívili Bosnu a Hercegovinu, kde realizovali několik školení na téma počítačové bezpečnosti. NÚKIB se tak například podílí na rozvojovém projektu Cybervac, který připravuje MZV.

# Činnost Vládního CERT:

## Rozvoj síťového Threat Huntingu

V roce 2023 NÚKIB nadále pracoval na projektech k navýšení kybernetické a informační bezpečnosti ČR.

**Novinkou bylo zprovoznění služby Síťového Threat Huntingu, v rámci kterého je na základě smlouvy po omezenou dobu vykonávaná proaktivní detekce škodlivé aktivity a provozních nedostatků v rámci infrastruktury partnerů.**

Po finalizaci interního testování proběhlo pilotní nasazení sondy u povinného subjektu a na základě zkušeností jsou rozvíjeny související procesy. V roce 2023 se začala koncepčně rozvíjet i služba Threat Huntingu na koncových stanicích (Host Threat Hunting), aby mohlo v příštím roce dojít ke spuštění pilotního projektu.

## Budování kapacit v oblasti průmyslových a řídicích systémů

**Vzhledem k válečnému konfliktu na Ukrajině a Blízkém východě NÚKIB pokračoval v dlouhodobém budování kapacit specializujících se na oblast průmyslových a řídicích systémů.**

V roce 2023 se zaměřil na auditní a kontrolní činnost v oblastech plynárenství, telekomunikací a energetiky. Poskytoval technické konzultace i k soukromým subjektům, které budou v budoucnu pravděpodobně určeny jako součást kritické informační infrastruktury. V návaznosti na tuto činnost se specialisté z NÚKIB účastnili i interních cvičení daných organizací, kde se podíleli na ověření funkčnosti interních bezpečnostních politik.

## Rozvoj a rebrandování Portálu NÚKIB

**V roce 2023 NÚKIB pokračoval i v rozvoji platformy Neveřejný web, včetně jejího rebrandování na Portál NÚKIB.**

Jedná se o platformu, která slouží k poskytování neveřejných informací regulovaným subjektům a partnerům. V tomto roce byly do platformy zapojeny další orgány veřejné moci nebo subjekty, které jsou správci kritické informační infrastruktury nebo významných informačních systémů.

Jednalo se především o subjekty z oblasti dopravy, univerzity, krajské úřady a úřední státní orgány. Celkem se jednalo o 71 organizací, přičemž nadále budou zapojovány další.

## Rozvoj forenzních analýz

**V oblasti rozšiřování technických služeb NÚKIB došlo na začátku roku 2023 k certifikaci analytického informačního systému, který umožňuje forenzně analyzovat nahlášené incidenty, které se týkají utajovaných informací.**

Zároveň byly budovány nové schopnosti techniků v oblasti forenzní analýzy, zejména v oblastech mobilních zařízení a cloudových technologií.

## Posílení penetračního testování

**V minulém roce NÚKIB posílil i oblast penetračního testování. Kromě zdokonalení používaných technik představil novou službu fyzických penetračních testů, která ověřuje fyzické zabezpečení organizace, chování pracovníků a zabezpečení budovy.** Zároveň zkvalitnil službu průběžného skenování zranitelností, při které jsou dlouhodobě monitorovány zapojené subjekty z hlediska přítomnosti nejznámějších zranitelností, a to zejména za pomoci automatizovaných skenovacích nástrojů.

# Výhled trendů v kybernetické bezpečnosti v ČR na roky 2024 a 2025

## Kybernetické útoky skrze dodavatelský řetězec

Ve Zprávě za rok 2021 bylo ve stejné kapitole uvedeno, že kybernetické útoky proti dodavatelským řetězcům budou pokračovat, nabírat na síle a zasáhnou i Českou republiku. **Tato předpověď se naplnila a je téměř jisté (90–100 %), že tento vektor útoku bude pro útočníky i nadále velmi atraktivní.**[7] Zvláštní pozornost by tomuto vektoru měla být věnována u organizací, které jsou závislé na jednom klíčovém dodavateli.

**Velmi pravděpodobně (75–85 %) bude ve větší míře než dosud docházet ke kompromitaci sekundárních a terciálních dodavatelů konečné oběti, a nikoli jen těch primárních.** S ohledem na potřebnou sofistikovanost budou velmi pravděpodobně (75–85 %) tento vektor využívat především státní aktéři.

## Geopoliticky motivované kybernetické útoky

Kybernetické útoky proti státním institucím a kritické infrastruktuře ze strany státních aktérů jsou téměř vždy motivované děním ve fyzickém světě a nejde jen o zneužití slabého zabezpečení či o finanční zisk. V předchozích letech NÚKIB zaznamenal řadu podobných kybernetických útoků ze strany státních aktérů, které byly spojeny s politickým směřováním České republiky či s konkrétními událostmi (např. DDoS útoky stran ruskojazyčných hacktivistů).

**Je téměř jisté (90–100 %), že tento vývoj bude pokračovat a převažujícím motivem útočníků bude zisk informací. Nelze vyloučit (25–50 %), že někteří ze škodlivých aktérů budou usilovat i o infiltraci sítí významných organizací a firem s cílem zneužít přístupu pro další aktivity (např. destruktivní) v případě konfliktu.**

## Generativní umělá inteligence a velké jazykové modely (LLM)

**Rok 2023 se nesl ve znamení generativní umělé inteligence (AI), konkrétně chatbotů na bázi velkých jazykových modelů (LLM).** Po spuštění přelomové služby ChatGPT následovaly brzy další.[8] AI chatboti a od nich odvozené produkty se začali téměř okamžitě používat ve všech typech organizací. **Stejně rychle se ale objevily metody k jejich zneužití, ať už ke generování phishingu nebo psaní škodlivého kódu.** Přestože se provozovatelé těchto služeb snažili do chatbotů nainstalovat limity na poskytování škodlivých odpovědí, potenciál k překonání těchto zábran (tzv. jailbreak) se zatím vždy ukázal větší.

**V roce 2024 lze téměř jistě (90–100 %) očekávat nárůst ve všech ohledech.** Mají být spuštěny nové služby a zároveň budou dále narůstat schopnosti těch stávajících. Nelze předpokládat, že by se v roce 2024 výrazně zvýšila schopnost provozovatelů filtrovat škodlivé dotazy, a proto lze očekávat nárůst schopností útočníků. Konkrétně lze očekávat větší poměr výstupů které nebudou pouze ve formě textu. **Stoupá dostupnost dalších generativních výstupů, jako obrázky, zvuk, nebo videa a deepfakes. Chatboti navíc stále více tyto schopnosti implementují i do svých funkcí. Proto lze očekávat především nárůst audiovizuálních forem phishingu, jako vishing, a jejich různých kombinací v sofistikovaných phishingových schématech.**

---

7 Za zmínku stojí např. kompromitace poskytovatele autentifikačních služeb Okta, softwarové společnost JetBrains či firmy Microsoft. V posledních dvou případech stáli za škodlivými aktivitami státem sponzorovaní aktéři.

8 ChatGPT byl sice spuštěn již na konci listopadu roku 2022, ale masivní nárust jeho popularity lze datovat až k začátku roku 2023.

# Příloha 1:

# Vyhodnocení plnění cílů Národního plánu výzkumu a vývoje v kybernetické a informační bezpečnosti za rok 2023

## Zapojení do programů EU a podpora výzkumných projektů

V roce 2023 pokračovala podpora prioritních výzkumných témat v oblasti kybernetické a informační bezpečnosti v rámci národních programů podpory aplikovaného výzkumu a experimentálního vývoje. Na úrovni Evropské unie se NÚKIB podílel na přípravě pracovních programů Digitální Evropa a Horizont Evropa s cílem zajistit stabilní podporu v oblasti rozvoje kvantových technologií, umělé inteligence a dalších klíčových oblastí.

Z pozice aplikačního garanta NÚKIB podpořil několik výzkumných projektů financovaných z programů veřejných soutěží MV ČR a TA ČR s cílem zvýšit uplatnitelnost výsledků výzkumu a vývoje v praxi.

## Rozvoj  informačního zázemí a propojení komunity v oblasti výzkumu a vývoje kybernetické bezpečnosti

NÚKIB se rovněž podílel na budování informačního zázemí a komunity v oblasti výzkumu a vývoje. Na webových stránkách NÚKIB jsou pravidelně publikovány newslettery „Aktuality ve výzkumu a vývoji v kybernetické bezpečnosti“ a byla vytvořena informační stránka zaměřena na přehled činností a služeb Národního koordinační centra výzkumu a vývoje v kybernetické bezpečnosti.

Posilování vazeb mezi akademickým, veřejným a soukromým sektorem bylo realizováno prostřednictvím pravidelných setkání Platformy pro výzkum a vývoj v kybernetické a informační bezpečnosti.

## Mezinárodní aktivity a spolupráce - PROPED

Na mezinárodním poli NÚKIB spoluorganizoval tři výzkumné mise v rámci nástroje podpory ekonomické diplomacie PROPED. První mise směřovala do Německa a zaměřovala se na prohloubení spolupráce mezi akademickou a veřejnou sférou v oblasti bezpečnosti optických sítí. Následně se uskutečnil Česko-bavorský networkingový seminář o kybernetické bezpečnosti v Řezně, kde proběhla diskuse na témata implementace unijní směrnice NIS 2 a aktuálních výzev v oblasti využití nástrojů umělé inteligence.

Cílem cesty do Singapuru pak byla především výměna zkušeností a navázání kontaktů mezi českými a singapurskými subjekty, mimo jiné i v oblasti detekce kybernetických hrozeb.

## Posun vývoje Národního koordinačního centra

NÚKIB dále pokračoval v budování Národního koordinačního centra dle Nařízení Evropského parlamentu a Rady č. 2021/887. Zkvalitnění služeb v oblastech budování informačního zázemí, poradenství a šíření výsledků výzkumu a vývoje v rámci ČR bude podpořeno ze dvou grantů EU, které NÚKIB získal z programu Digitální Evropa.

V rámci těchto projektů tak bude možné poskytnout finanční podporu subjektům působícím v kybernetické bezpečnosti prostřednictvím dotací.

# Příloha 2:

# Naplňování Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025

Rok 2023 byl třetím rokem vyhodnocování Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025 (dále jen „Akční plán“).

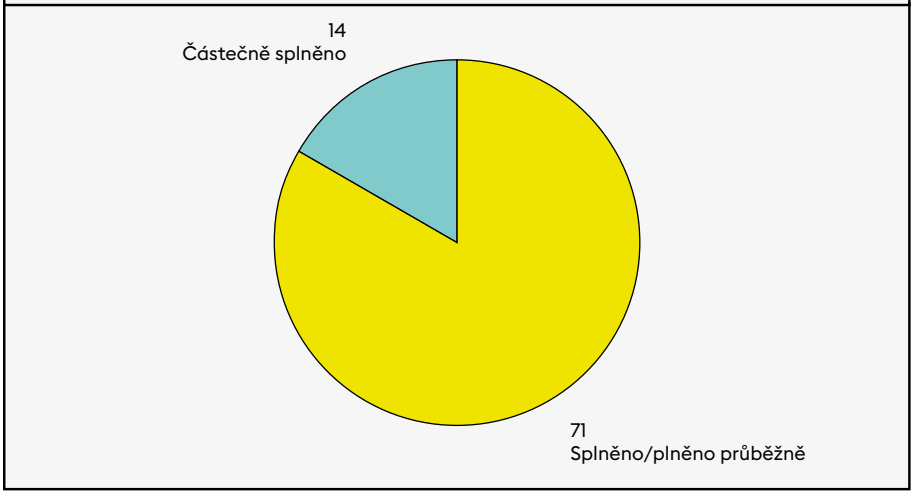
NÚKIB nejenže koordinuje vyhodnocení celého Akčního plánu, ale podílí se z pozice gestora/spolupracujícího subjektu na plnění 101 z celkových 105 úkolů.

Faktorů negativně ovlivňujících míru plnění Akčního plánu může být několik. V rámci Akčního plánu částečně existuje určitá prioritizace úkolů, dle časových a kapacitních možností gestorů. Dále můžou mít vliv další různé dílčí faktory, jako například finanční možnosti či další interně-organizační problémy jednotlivých gestorů či spolupracujících subjektů.

**Za rok 2023 bylo vyhodnocováno 85 úkolů.**

**71 z nich bylo v roce 2023 splněno či plněno průběžně, 14 úkolů bylo splněno pouze částečně, a jejich plnění bude přeneseno do roku 2024. Ve srovnání s rokem 2022, kdy bylo částečně splněno 9 úkolů, se jedná o dílčí pokles v úspěšnosti plnění úkolů.**

**V roce 2023 nebyl žádný úkol vyhodnocen jako nesplněný.**



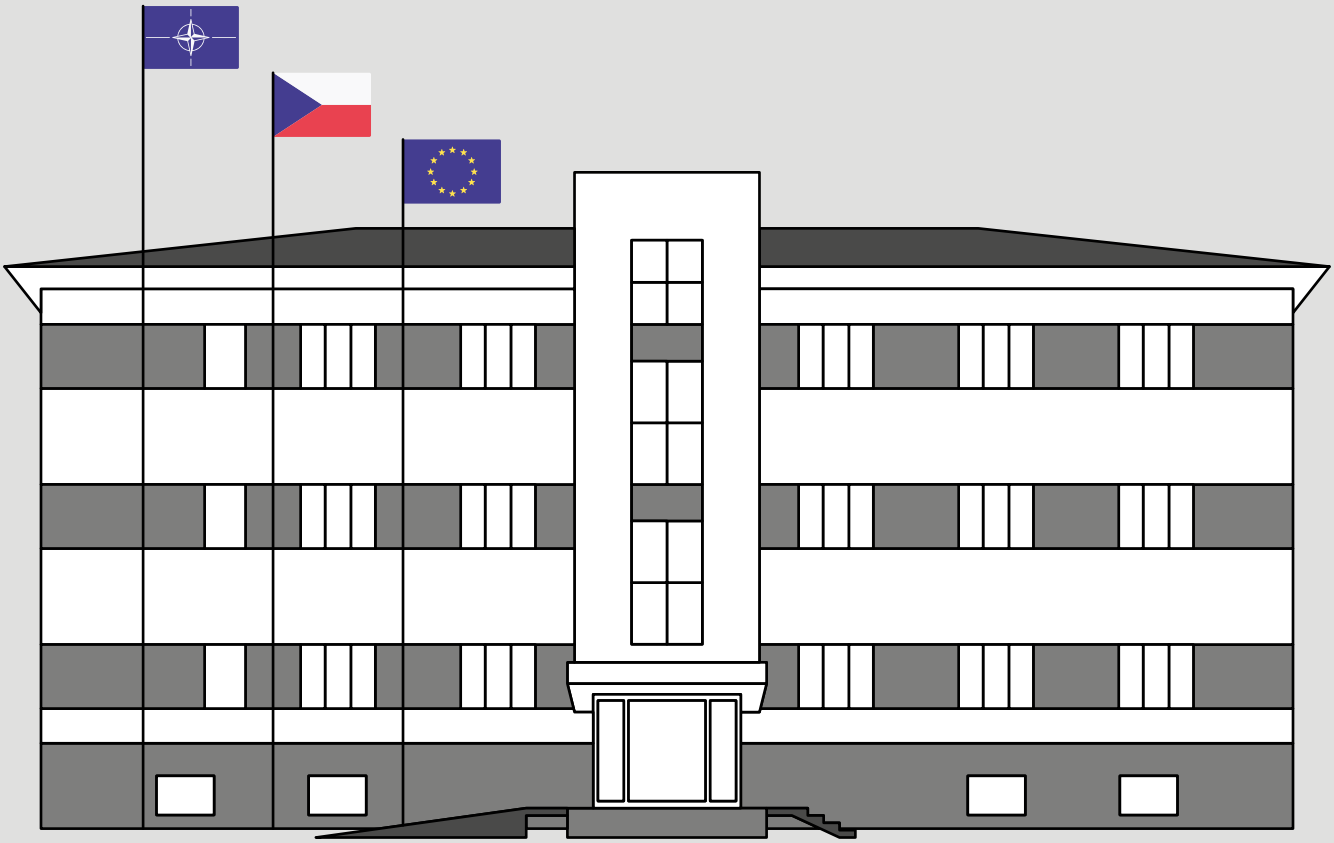

*Graf 25: Vyhodnocení Akčního plánu za rok 2023*

**Příkladem úkolu terminovaného a splněného v roce 2023 je úkol č. 40** *„Provést právní revizi stavu kybernetického nebezpečí v kontextu dalších krizových stavů a připravit návrhy pro případné legislativní změny.“* V rámci návrhu nového ZKB došlo u tohoto úkolu k přepracování stavu kybernetického nebezpečí, a to i ve vztahu k revizi krizové legislativy a ve spolupráci s gestorem krizového řízení, kterým je Generální ředitelství Hasičského záchranného sboru ČR. Právní úprava stavu kybernetického nebezpečí byla nově formulována.

**Příkladem úkolu pouze částečně splněného je úkol č. 83** „Vypracovat koncepci ochrany neutajovaných informací citlivé povahy.“. Po zpracování analýzy stávajícího stavu a po diskusi s interními a externími partnery zpracoval NÚKIB interní návrh Koncepce ochrany neutajovaných informací, avšak dosud nedošlo k jejímu schválení. Plnění úkolu bude přeneseno do dalšího roku, kdy proběhne projednání návrhu s externími subjekty a předložení BRS.

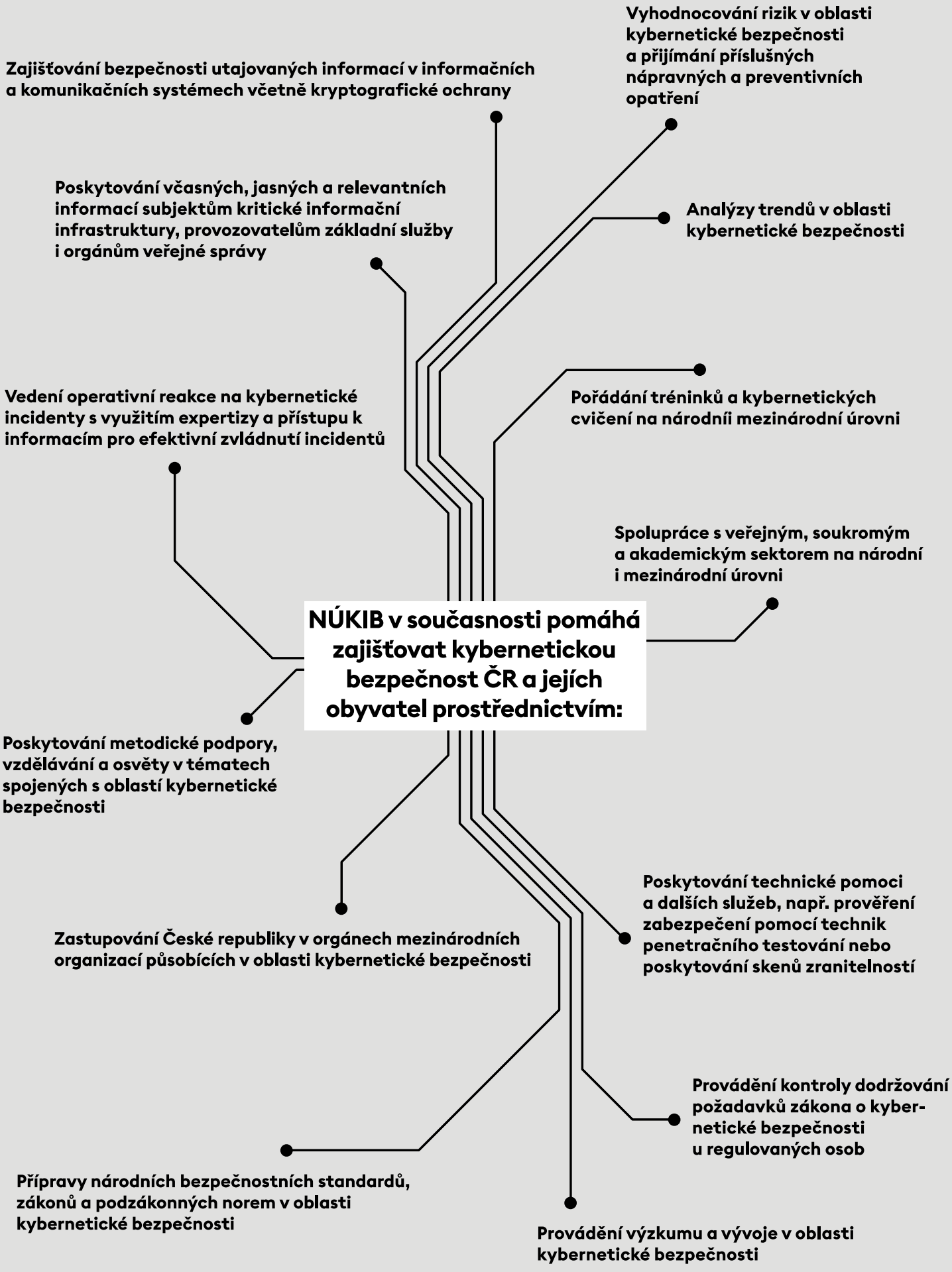
**V Akčním plánu jsou také úkoly průběžné, které jsou vyhodnocovány každý rok. Jedná se například o úkol č. 67** „Účastnit se a aktivně participovat na organizaci, přípravě a provádění mezinárodních cvičení a prostřednictvím společných kybernetických cvičení aktivně posilovat síť významných partnerů v oblasti kybernetické bezpečnosti“. V roce 2023 se ČR skrze NÚKIB a další subjekty podílela na organizaci, ale i exekuci několika mezinárodních cvičení (např. Cyber Coalition, NATO CMX 2023), přičemž v těchto aktivitách bude nadále pokračovat.

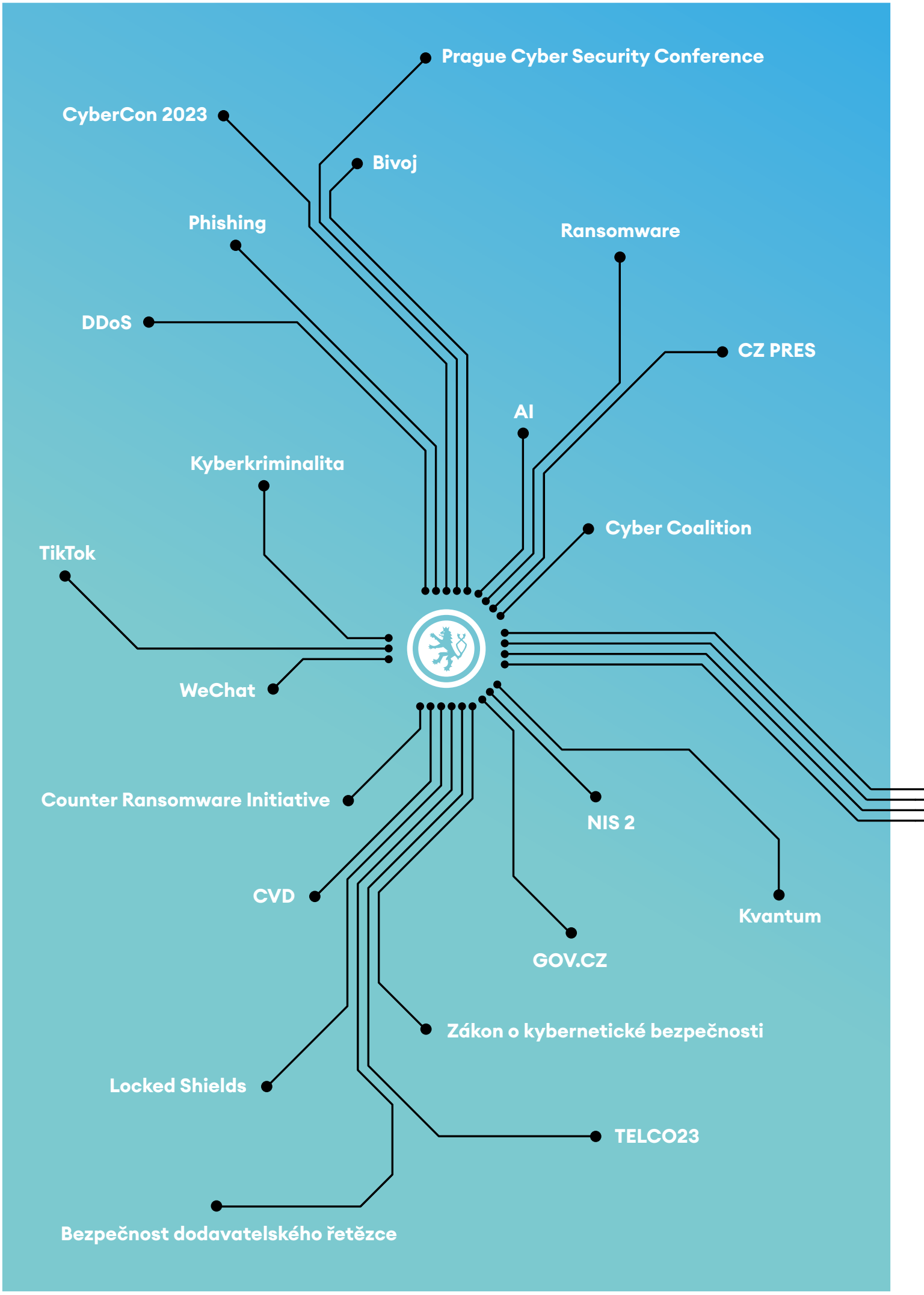
# O NÚKIB



**NUKIB je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku veřejně regulované služby v rámci družicového systému Galileo. NÚKIB vznikl 1. srpna 2017 na základě zákona č. 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).**

Pro více informací o NÚKIB navštivte naše webové stránky www.nukib.gov.cz nebo sledujte aktuality z oblasti kybernetické bezpečnosti v ČR na našich sociálních sítích X, LinkedIn, Facebook nebo Instagram. Záznamy z některých akcí, které NÚKIB pořádá, nebo se jich účastní jeho zástupci, pak najdete na YouTube kanálu NÚKIB.


Zajišťování bezpečnosti utajovaných informací v informačních a komunikačních systémech včetně kryptografické ochrany
Vyhodnocování rizik v oblasti kybernetické bezpečnosti a přijímání příslušných nápravných a preventivních opatření
Poskytování včasných, jasných a relevantních informací subjektům kritické informační infrastruktury, provozovatelům základní služby i orgánům veřejné správy
Analýzy trendů v oblasti kybernetické bezpečnosti
Vedení operativní reakce na kybernetické incidenty s využitím expertizy a přístupu k informacím pro efektivní zvládnutí incidentů
Pořádání tréninků a kybernetických cvičení na národníi mezinárodní úrovni
Spolupráce s veřejným, soukromým a akademickým sektorem na národní i mezinárodní úrovni
NÚKIB v současnosti pomáhá zajišťovat kybernetickou bezpečnost ČR a jejích obyvatel prostřednictvím:
Poskytování metodické podpory, vzdělávání a osvěty v tématech spojených s oblastí kybernetické bezpečnosti
Zastupování České republiky v orgánech mezinárodních organizací působících v oblasti kybernetické bezpečnosti
Poskytování technické pomoci a dalších služeb, např. prověření zabezpečení pomocí technik penetračního testování nebo poskytování skenů zranitelností
Provádění kontroly dodržování požadavků zákona o kyber-netické bezpečnosti u regulovaných osob
Přípravy národních bezpečnostních standardů, zákonů a podzákonných norem v oblasti kybernetické bezpečnosti
Provádění výzkumu a vývoje v oblasti kybernetické bezpečnosti


Prague Cyber Security Conference
CyberCon 2023
Bivoj
Phishing
Ransomware
DDoS
CZ PRES
AI
Kyberkriminalita
Cyber Coalition
TikTok
WeChat
Counter Ransomware Initiative
NIS 2
CVD
Kvantum
GOV.CZ
Zákon o kybernetické bezpečnosti
Locked Shields
TELCO23
Bezpečnost dodavatelského řetězce