UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ

2026

Analýza výsledkov dotazníka kybernetickej a informačnej bezpečnosti

(analytický materiál)

Projekt Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ (KCKB UPJŠ) financovaný Európskou úniou z prostriedkov Plánu obnovy a odolnosti Slovenskej republiky, kód projektu: 17R05-04-V01-00007.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

OBSAH

PREDSTAVENIE KC KB UPJŠ

Kompetenčné centrum kybernetickej bezpečnosti na Univerzite Pavla Jozefa Šafárika v Košiciach (KC KB UPJŠ) predstavuje kompetenčné centrum, v rámci ktorého sú realizované aktivity zamerané na vzdelávanie, výskum a expertnú činnosť v oblasti informačnej a kybernetickej bezpečnosti, ochrany dát, kyberkriminality a ochrany pred dezinformáciami. Súčasne KC KB UPJŠ realizuje medzinárodnú spoluprácu s akademickými partnermi zo zahraničia a poskytuje konzultácie pre možnosť prípravy a podania projektov v oblasti kybernetickej bezpečnosti.

Vytvorenie KC KB UPJŠ reflektuje viacero problémov, ktoré možno v súčasnosti identifikovať v oblasti informačnej a kybernetickej bezpečnosti (ďalej aj „KIB“):

- zvýšenie bezpečnostného povedomia relevantných subjektov zahŕňajúcich predovšetkým zamestnancov verejnej správy a študentov vysokoškolského a stredoškolského štúdia,
- vzdelávanie a výchova nových odborníkov pôsobiacich v tejto oblasti,
- výskum kybernetických hrozieb a identifikácia adekvátnych reakcií na tieto hrozby,
- zvýšenie operatívnej bezpečnosti v rámci verejnej správy poskytovaním expertných činností zo strany CSIRT tímu.

V rámci KC KB UPJŠ sa pripravoval študijný plán magisterského stupňa študijného programu aplikovaná informatika, ktorého jedna vetva sa zameriava na kybernetickú bezpečnosť. K tomuto študijnému plánu budú vytvorené, resp. modifikované viaceré predmety. Súčasne sa ako výstup kompetenčného centra vytvára ponuka **vzdelávania** pre rôzne cieľové skupiny zamestnancov verejnej správy.

V kontexte projektu sa súčasne posilňuje **spolupráca so strednými školami**, najmä vo forme činnosti **KyberTímov**, ich vzdelávania a následného zapojenia do šírenia bezpečnostného povedomia medzi širokou verejnosťou.

V rámci vzdelávacích aktivít sa sumarizujú nové poznatky a skúsenosti z oblasti KIB, ale aj príbuzných oblastí. Tie sú aktuálne doplnené o rôzne formy zážitkového vzdelávania.

V rámci **výskumnej** činnosti dochádza v už existujúcich výskumných oblastiach k publikovaniu viacerých vedeckých výstupov a k vytvoreniu nových možných výskumných spoluprác na posilnenie výskumného a vývojového potenciálu KC KB UPJŠ.

Nemenej dôležitým výstupom projektu je doplnenie výbavy a vzdelávanie univerzitného CSIRT tímu a možnosť poskytovania **expertných činností** pre akreditované CSIRT tímy v SR za účelom rýchlejšej a adekvátnejšej reakcie na kybernetické bezpečnostné incidenty.

1 ÚVOD

Táto analýza vychádza z dotazníka **„KCKB UPJŠ – dotazník kybernetickej bezpečnosti pre subjekty verejného sektora“**, ktorý bol realizovaný Kompetenčným centrom kybernetickej bezpečnosti UPJŠ. Do prieskumu sa zapojilo **83 organizácií verejného sektora**, prevažne obce a mestské časti. Cieľom prieskumu bolo komplexne zhodnotiť aktuálny stav kybernetickej a informačnej bezpečnosti (KIB), identifikovať slabé miesta, personálne a technologické nedostatky a pomenovať potreby organizácií v oblasti ďalšieho rozvoja.

Analýza kombinuje **kvantitatívne údaje (počty a percentá)** s **kvalitatívnou interpretáciou odpovedí**, pričom je zachované pôvodné číslovanie otázok dotazníka.

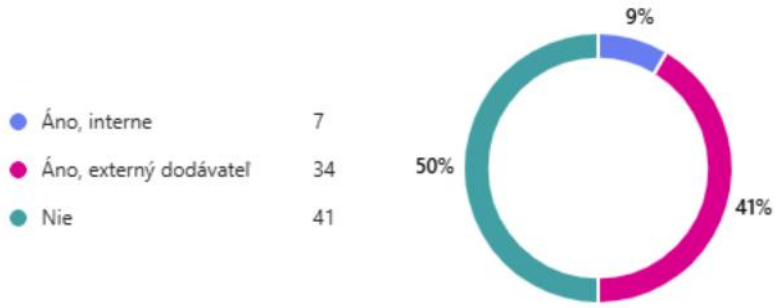
2 CHARAKTERISTIKA RESPONDENTOV (OTÁZKY 1–4)

Otázky 1 až 4 mali identifikačný charakter (názov organizácie, sídlo, pracovná pozícia respondenta). Respondentmi boli najmä **starostovia, primátori, vedúci pracovníci a administratívni zamestnanci**. Táto skutočnosť naznačuje, že problematika KIB je vo verejnom sektore často riešená popri iných povinnostiach a nie prostredníctvom špecializovaných odborných pozícií.

3 PERSONÁLNE ZABEZPEČENIE KYBERNETICKEJ BEZPEČNOSTI (OTÁZKY 5–6)

3.1 OTÁZKA 5: MÁ VAŠA ORGANIZÁCIA VYHRADENÚ ZODPOVEDNOSŤ ZA KIB?

Odpoveď	Počet	Podiel
Áno, interne	7	9 %
Áno, externý dodávateľ	34	41 %
Nie	41	50 %



Otázka zameraná na určenie zodpovednosti za kybernetickú a informačnú bezpečnosť patrí medzi kľúčové z hľadiska riadenia KIB. Výsledky ukazujú, že 50 **% organizácií nemá určenú žiadnu osobu ani tím zodpovedný za KIB**, čo predstavuje zásadný problém z pohľadu bezpečnostného riadenia a zodpovednosti.

Absencia určenej zodpovednosti znamená, že bezpečnosť nie je riadená systematicky, ale riešená len vtedy, keď nastane problém. Takýto prístup je typický pre menšie organizácie, kde je KIB vnímaná ako technická alebo okrajová agenda, a nie ako súčasť strategického riadenia organizácie. V praxi to vedie k tomu, že neexistuje jasný vlastník rizík, chýba dlhodobé plánovanie a bezpečnostné opatrenia sa zavádzajú nekoordinovane.

Zaujímavým zistením je, že **41 % organizácií využíva externého dodávateľa**. Hoci externá podpora môže byť prínosná, sama o sebe nenahrádza internú zodpovednosť. V mnohých prípadoch ide skôr o

outsourcing technickej správy IT infraštruktúry než o komplexné riadenie kybernetickej bezpečnosti. Organizácia bez interne určenej zodpovednej osoby zároveň nemá dostatočnú kapacitu na kontrolu kvality dodávaných služieb ani na strategické rozhodovanie v oblasti KIB.

Len 9 % organizácií má určenú internú zodpovednosť za KIB, čo poukazuje na nízku mieru inštitucionalizácie tejto oblasti vo verejnom sektore. Z pohľadu pripravovanej a postupne implementovanej legislatívy (napr. smernica NIS2) je však jasné, že určenie zodpovedných rolí bude nevyhnutnou podmienkou pre splnenie zákonných požiadaviek.

Výsledky tejto otázky tak poukazujú na potrebu jasne definovať zodpovednosti za KIB, a to buď formou interných pozícií, alebo kombináciou internej koordinácie a externej odbornej podpory.

3.2 Otázka 6: Počet pracovníkov venujúcich sa KIB

Počet pracovníkov	Podiel respondentov
0	31 %
1	49 %
2	15 %
3 a viac	5 %

Až **31 % organizácií** nemá ani jedného pracovníka venujúceho sa KIB. Z nich **96 % zároveň odpovedalo „nie“** na otázku 5, teda nemajú ani formálne určenú zodpovednosť. Organizácie s nulovou alebo minimálnou kapacitou zároveň vykazujú absenciu smerníc, incidentných procesov a školení.

4 Úroveň zabezpečenia KIB (otázka 7)

4.1 Otázka 7: Sebahodnotenie úrovne kybernetickej bezpečnosti

Úroveň	Počet	Podiel
Systematicky riešená	10	12 %
Základné opatrenia	31	37 %
Neucelený prístup	21	25 %

Minimálna / reaktívna	16	19 %
Bez riešenia	5	6 %

Len 12 % organizácií hodnotí svoju bezpečnosť ako systematicky riešenú. Väčšina respondentov (62 %) sa pohybuje v pásme základných alebo neucelených opatrení. To znamená, že bezpečnosť je síce čiastočne riešená, no **bez pravidelného hodnotenia, auditu a strategického plánovania**.

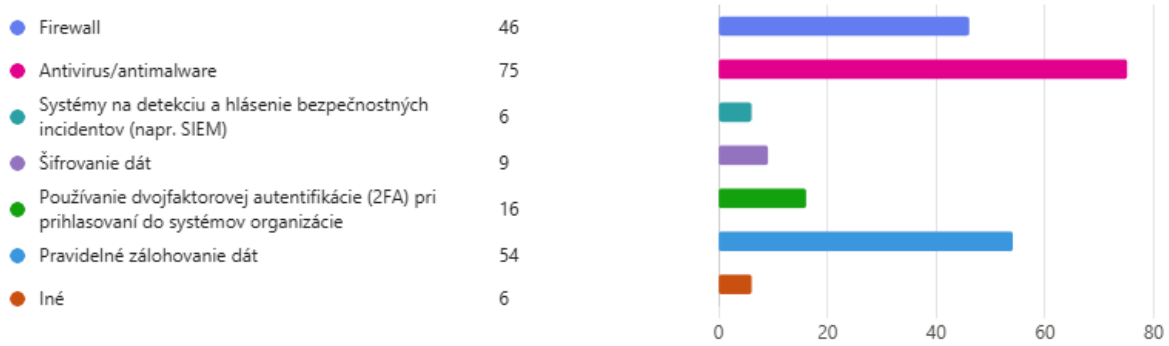
Takmer štvrtina organizácií rieši bezpečnosť minimálne alebo vôbec, čo predstavuje vysoké riziko z pohľadu ochrany osobných údajov, kontinuity služieb a súladu s legislatívou. Viac ako **50 % organizácií** sa nachádza v pásme **nízkej až veľmi nízkej úrovne bezpečnosti**. Len **12 %** organizácií deklaruje systematický prístup s pravidelným vyhodnocovaním a zlepšovaním opatrení.

5 TECHNICKÉ OPATRENIA (OTÁZKA 8)

5.1 OTÁZKA 8: POUŽÍVANÉ TECHNOLÓGIE A NÁSTROJE

Vysoké zastúpenie antivírusových riešení (90 %) naznačuje, že organizácie sa sústreďujú na **základnú ochranu koncových zariadení**. Naopak, nízke využívanie šifrovania, viacfaktorovej autentifikácie a monitorovacích systémov poukazuje na absenciu preventívneho a proaktívneho prístupu.

Takýto stav znamená, že organizácie sú schopné reagovať len na známe a jednoduché hrozby, pričom sofistikovanejšie útoky môžu zostať nepovšimnuté.

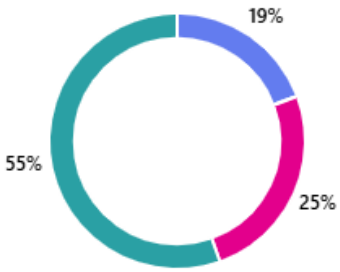


Technická bezpečnosť je orientovaná najmä na **základné ochranné prvky**. Pokročilé nástroje, ako monitoring incidentov, šifrovanie či viacfaktorová autentifikácia, sú využívané len okrajovo.

6 Bezpečnostné politiky a incident manažment (otázky 9–10)

6.1 Otázka 9: Bezpečnostné smernice

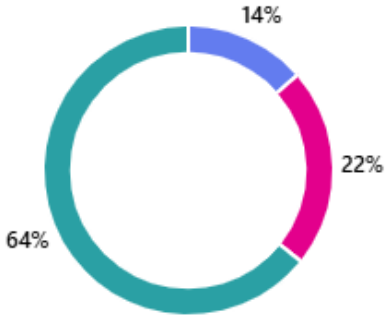
Stav	Počet	Podiel
Plne vypracované	16	19 %
Čiastočne	21	25 %
Neexistujú	46	55 %



Viac ako polovica organizácií nemá žiadne bezpečnostné smernice. To znamená, že zamestnanci nemajú jasne definované pravidlá správania, zodpovednosti ani postupy pri práci s informačnými systémami.

6.2 Otázka 10: Procesy riešenia incidentov

Stav	Počet	Podiel
Plne zdokumentované	11	14 %
Čiastočne	18	22 %
Neexistujú	52	64 %

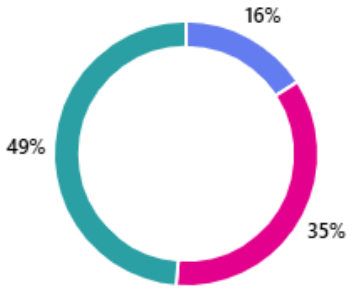


Viac ako **60 % organizácií** nemá definované procesy na riešenie kybernetických bezpečnostných incidentov, čo predstavuje významné prevádzkové aj legislatívne riziko.

7 Používatelia a zariadenia (otázky 11–13)

7.1 Otázka 11: Používanie súkromných zariadení (BYOD)

Odpoveď	Počet	Podiel
Áno, s pravidlami	13	16 %
Áno, bez pravidiel	29	35 %
Nie	40	49 %

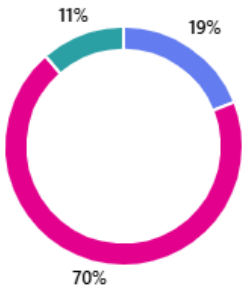


Takmer **tretina organizácií** umožňuje používanie súkromných zariadení **bez akýchkoľvek bezpečnostných pravidiel**.

7.2 OTÁZKA 12: KVALIFIKÁCIA ZAMESTNANCOV

Prevažujú skúsenosti získané praxou, pričom špecializované vzdelanie má len menšia časť respondentov. To poukazuje na potrebu systematického vzdelávania a certifikácie.

Špecializované vzdelanie v oblasti KIB (napr. certifikáty CISSP, CEH...)	15
Skúsenosti získané praxou	55
Iné	9



7.3 Otázka 13: Dostatočnosť odborných kapacít

Odpoveď	Počet	Podiel
Áno	27	31 %
Nie	47	53 %
Iné	14	16 %

Výsledky tejto otázky ukazujú, že **53 % organizácií nepovažuje svoje odborné kapacity v oblasti kybernetickej a informačnej bezpečnosti za dostatočné**, zatiaľ čo len **31 % respondentov** uviedlo, že kapacity považuje za postačujúce. Zvyšná časť odpovedí spadá do kategórie „iné“, čo často naznačuje neistotu alebo nejednoznačné vnímanie tejto problematiky.

Tieto výsledky je potrebné interpretovať v kontexte predchádzajúcich otázok, najmä otázok 5 a 6. Organizácie, ktoré nemajú určenú zodpovednú osobu za KIB alebo disponujú maximálne jedným pracovníkom, prirodzene vnímajú svoje kapacity ako nedostatočné. Subjektívne hodnotenie respondentov tak **potvrdzuje objektívne zistenia o personálnej poddimenzovanosti** vo verejnom sektore.

Nedostatočné odborné kapacity sa neprejavujú len v absencii špecialistov, ale aj v obmedzených možnostiach sledovať aktuálne hrozby, legislatívne zmeny (napr. požiadavky NIS2) a nové technologické trendy. Zamestnanci poverení KIB často vykonávajú túto činnosť popri iných pracovných úlohách, čo vedie k reaktívnemu a fragmentovanému prístupu k bezpečnosti.

Dôležitým aspektom je aj kvalitatívna stránka odbornosti. Ako vyplynulo z otázky 12, prevažujú skúsenosti získané praxou, zatiaľ čo formálne vzdelanie alebo certifikácie v oblasti KIB sú zastúpené len okrajovo. To zvyšuje závislosť organizácií od externých dodávateľov a zároveň znižuje ich schopnosť kvalifikovane kontrolovať a riadiť dodávané bezpečnostné služby.

Z dlhodobého hľadiska predstavuje nedostatok odborných kapacít jedno z **najvýznamnejších systémových rizík**. Bez jeho riešenia nie je možné efektívne zavádzať bezpečnostné politiky, incidentné procesy ani realizovať pravidelné školenia. Výsledky tejto otázky preto jasne poukazujú na potrebu budovania interných kapacít, regionálnej spolupráce alebo využívania centralizovanej metodickej podpory zo strany kompetenčných centier.

8 Vzdelávanie a povedomie o bezpečnosti (otázky 14–15)

8.1 Otázka 14: Pravidelné školenia

Stav	Počet	Podiel

Pravidelné	26	32 %
Jednorazové	21	26 %
Žiadne	35	43 %

Len tretina organizácií realizuje pravidelné školenia. Absencia systematického vzdelávania výrazne znižuje schopnosť zamestnancov rozpoznať hrozby a správne reagovať na incidenty.

8.2 Otázka 15: Školenia pre zamestnancov komunikujúcich s externým prostredím

Typ	Počet	Podiel
Cielené (phishing a pod.)	16	20 %
Všeobecné	42	51 %
Žiadne	24	29 %

Väčšina organizácií sa spolieha len na všeobecné poučenie. Cielené školenia na phishing a sociálne inžinierstvo sú pritom kľúčové, keďže práve tieto útoky patria medzi najčastejšie.

9 Incidenty a hlavné výzvy (otázky 16–19)

9.1 Otázka 16: Zaznamenané incidenty

Odpoveď	Počet	Podiel
Áno	8	10 %
Nie	75	90 %

Nízky počet hlásených incidentov (10 %) pravdepodobne neznamená ich reálnu absenciu, ale skôr **nedostatočné monitorovanie a evidenciu**.

9.2 Otázka 17: Najväčšie výzvy

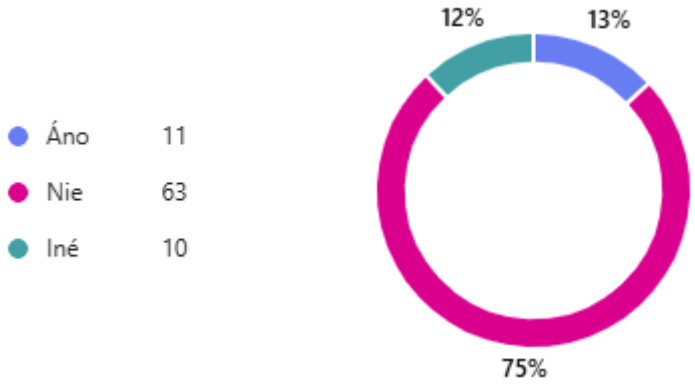
Výzva	Počet
Slabé financovanie	28
Nedostatok personálu	20
Nízke povedomie	16
Technologické nedostatky	12

Najvýraznejšími bariérami sú financovanie a personálne kapacity. Až **76 % organizácií** nemá prístup k externému financovaniu na zlepšenie KIB (otázka 19).

9.3 Otázka 18: Najprínosnejšie riešenia

Respondenti najčastejšie uvádzali potrebu jednoduchých a praktických školení, metodických materiálov a dostupného poradenstva.

9.4 Otázka 19: Financovanie



Až 75 % organizácií nemá prístup k externému financovaniu, čo výrazne obmedzuje ich schopnosť realizovať systematické zlepšenia.

10 Záujem o podporu a spoluprácu (otázky 20–22)

Otázka	Áno	Nie

20 – Odborné poradenstvo	49	32
21 – Ďalšia spolupráca	52	31
22 – Workshop	9	7

Výsledky poukazujú na **výrazný dopyt po metodickej a odbornej podpore**.

11 SWOT ANALÝZA KYBERNETICKEJ BEZPEČNOSTI VO VEREJNOM SEKTORE

Silné stránky	**Slabé stránky**
Základné technické opatrenia	Nedostatok personálu
Záujem o spoluprácu	Absencia procesov
Externá odborná podpora	Nízke povedomie
Príležitosti	**Hrozby**
Vzdelávacie programy KCKB	Rast kybernetických útokov
Financovanie z EÚ	Sankcie a výpadky služieb
Implementácia Zákona o KB	Závislosť od dodávateľov

ZÁVER

Analýza potvrdzuje, že úroveň kybernetickej a informačnej bezpečnosti vo verejnom sektore je prevažne **nízka až stredná**. Najväčšie rezervy sú v personálnych kapacitách, systematickom riadení, incidentnom manažmente a vzdelávaní. Výsledky predstavujú pevný analytický základ pre strategické rozhodovanie, projektové aktivity a cielenú podporu zo strany KCKB UPJŠ.