Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Implementácia NIS2SK v Slovenskej republike

Report on community consultations

V 0.1

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

Deliverable Summary

Deliverable Number	D2.1
Deliverable Name	Report on community consultations
Work Package Number	WP 2
Type of document	R-Document, report, PU
Public Due Month/Date	M5 (31/12/2023)

Verzia	Dátum	SCHVÁLIL
V 0.1	28.2.2024	Schválený Riadiacim výborom

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

Obsah

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

Zoznam skratiek

Skratka	Výklad skratky
AMKB	Asistent manažéra kybernetickej bezpečnosti
CSIRT	Computer Security Incident Response Team
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
IS	Informačný systém
KCCKB	Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
MKB	Manažér kybernetickej bezpečnosti
NBÚ	Národný bezpečnostný úrad
NIS2	Smernica o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii
PZS	Poskytovateľ základnej služby
SK-CERT	Slovak Computer Emergency Response Team

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

Manažérske zhrnutie

Každodenný život aj hospodárstvo sú stále závislejšie od digitálnych technológií. Občania sú preto častejšie vystavení vážnym kybernetickým incidentom. Budúca bezpečnosť závisí od posilnenia schopnosti chrániť Úniu pred kybernetickými hrozbami, pretože civilná infraštruktúra aj vojenské kapacity sa spoliehajú na bezpečné digitálne systémy.

Národný bezpečnostný úrad vyvíja snahy, aby sa čo najviac sa priblížil k regulovaným subjektom a aktívne ich zapojil do činností, ktoré súvisia so zvyšovaním úrovne stavu kybernetickej bezpečnosti na Slovensku – realizuje projekt NIS2 Implementation in the Slovak Republic.

Súčasťou projektu č. 101127928 – NIS2SK – projekt EÚ na základe výzvy: „NIS2 Implementation in the Slovak Republic“ je **Pracovný balík (Aktivita) 2 Národná legislatíva a stratégia.**

Hlavným cieľom tohto pracovného balíka je vytvoriť a zaviesť nový národný rámec kybernetickej bezpečnosti. Tento cieľ sa dosiahne v niekoľkých etapách. Každá z nich bude mať vymedzený rozsah a ciele, ktoré budú slúžiť ako základ pre ďalší vývoj. Jednou z hlavných etáp sú konzultácie s komunitou. Táto etapa má dva hlavné doplňujúce sa ciele:

1. zhromažďovanie podnetov od rôznych skupín zainteresovaných strán pre implementáciu nových právnych predpisov a prijímanie následných opatrení. Prechod z NIS na NIS2 sa vníma ako príležitosť na revíziu súčasného rámca, jeho silných stránok a nedostatkov. Kľúčové orgány tvoriace politiku majú záujem zhromaždiť čo najviac relevantných vstupov, vyvolať diskusiu o zmenách, ktoré treba vykonať, a o spôsobe ich efektívneho zavedenia,

2. táto komunikácia s komunitou bude zároveň slúžiť ako prípravná fáza zvyšovania povedomia a vzdelávania. Aktívna účasť očakávaných aktérov zmeny je kľúčom k ich motivácii sledovať ďalší vývoj.

Preto NBÚ oslovil kontaktné osoby prevádzkovateľa základnej služby a požiadal o účasť na prieskume, ktorý má za cieľ zozbierať a zanalyzovať ich praktické poznatky v tejto oblasti. Odpovede od regulovaných subjektov napomôžu pri aplikovaní nástrojov kybernetickej bezpečnosti do reálneho sveta. Rovnako tým jednotlivé subjekty dostali možnosť aktívne sa zapojiť do procesu prípravy novely zákona o kybernetickej bezpečnosti.

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

1. Cieľ

Transpozícia smernice poskytuje členským štátom priestor na prispôsobenie sa ich aktuálnej situácii, organizačnému nastaveniu a prípadne vzájomne prepojeným stratégiám, činnostiam a iniciatívam.

NBÚ chce túto možnosť v plnej miere využiť na vytvorenie modernizácie a rozšírenie v súčasnosti fungujúcich mechanizmov. Proces transpozície smernice bude prebiehať participatívnym spôsobom.

Participácia bola v úvodnej fáze realizovaná organizovaným a metodickým procesom, do ktorého sa zapojili všetky zainteresované strany s cieľom iniciovať diskusiu a kooperatívny konzultačný proces zameraný na prijímanie kolektívne záväzných rozhodnutí.

Debata predstavovala interaktívny proces medzi zainteresovanými partnermi z kybernetickej komunity zastúpenej súkromným sektorom, akademickou obcou, organizáciami a verejnými činiteľmi s cieľom významne prispieť k politickým rozhodnutiam transparentným a zodpovedným spôsobom.

V úvodnej fáze projektu sa iniciovala štruktúrovaná diskusia s hlavnými skupinami zainteresovaných strán – orgánmi verejnej správy, reprezentatívnymi organizáciami kritických sektorov, odborníkmi na kybernetickú bezpečnosť, akademickou obcou, súkromnými poskytovateľmi riešení a služieb.

Komunikačné formáty sa realizovali s týmito cieľmi:

- predchádzať konfliktom záujmov,
- budovať dôveru medzi verejnosťou (spoločnosťou) a verejnou štátnou správou,
- zlepšiť kvalitu právnych predpisov,
- zvýšiť legitimitu právnych predpisov,
- zvýšiť úroveň identifikácie (porozumenia) verejnosti s legislatívou,
- získať podporu verejnosti pri presadzovaní právnych predpisov,
- zjednodušiť vykonávanie právnych predpisov,
- zvýšiť povedomie verejnosti o právnych predpisoch.

Ukončenie konzultácií s komunitou predstavuje dôležitý krok v legislatívnom procese a dokazuje záväzok k transparentnosti, inkluzívnosti a zodpovednosti. Aktívnym zapojením verejnosti a zohľadnením jej názorov NBÚ ako zákonodarca prijíma informované rozhodnutia, ktoré lepšie odrážajú potreby jeho klientov a vedú k efektívnejšej a inkluzívnejšej legislatíve.

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

2. Použitá metodológia

Workshopy a panely sú jedným z hlavných nástrojov pre získanie spätnej väzby od širokej kyberbezpečnostnej komunity. V projekte bolo realizované veľké množstvo workshopov a panelov, v ktorých si komunita navzájom odovzdávala skúsenosti so súčasnou legislatívou a prezentovala očakávania v súvislosti s novou legislatívou.

Zástupcovia NBÚ aj KCCKB prezentovali požiadavky novej legislatívy, približovali legislatívny proces, a to s cieľom získať spätnú väzbu a pripraviť komunitu na prichádzajúce zmeny súvisiace s aplikáciou NIS2 do praxe.

One2One stretnutia

Individuálne stretnutia sú jedným z nástrojov, pri ktorých je možné získať spätnú väzbu a informácie, ktoré pri workshopoch s viacerými účastníkmi nie je možné získať z časového hľadiska.

Stretnutia boli organizované so zástupcami subjektov verejnej správy, ktorí poskytli spätnú väzbu k aktuálne platnej legislatíve a návrhy na jej úpravu s ohľadom na aplikáciu NIS2 v praxi.

Dotazníkový prieskum

Počet účastníkov workshopov a odborných panelov má limity. NBÚ preto využil ako ďalší nástroj konzultácií dotazníkový prieskum, ktorý mal za cieľ identifikovať úroveň zrozumiteľnosti zákona č. 69/2018 o kybernetickej bezpečnosti či aktívne zapojiť prevádzkovateľov základnej služby do procesu prípravy novely tohto zákona.

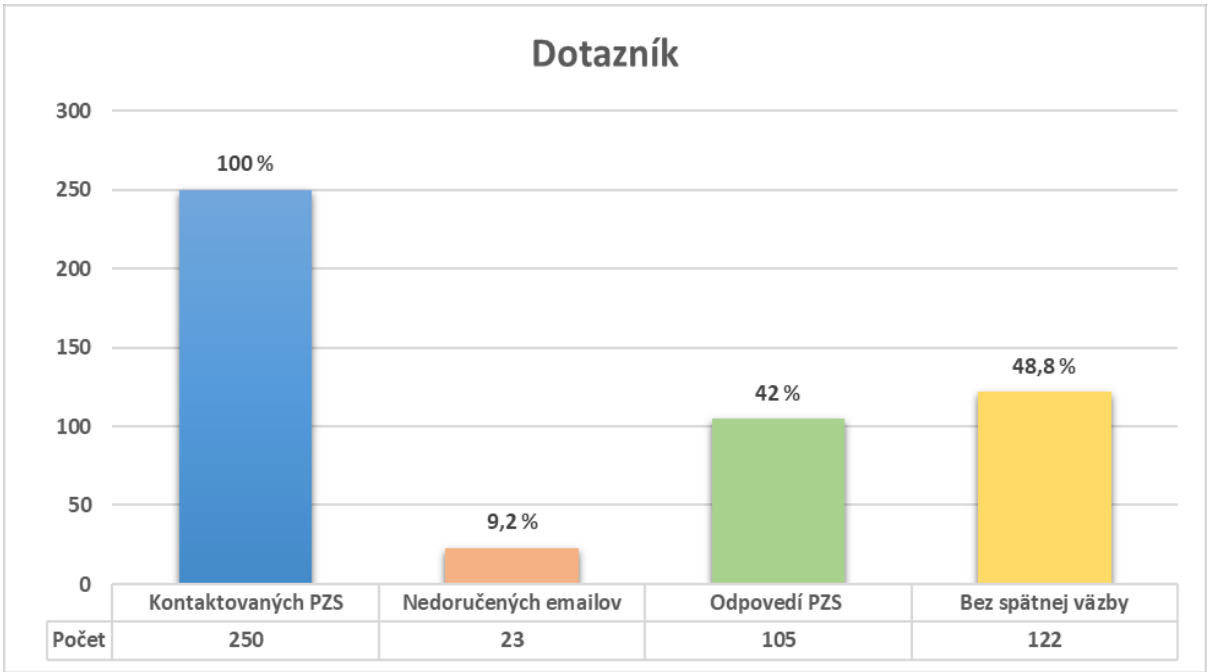
Tento dotazník bol navrhnutý s cieľom získať hlbší pohľad na pochopenie zákona, jeho aplikáciu a prípadné požiadavky na jeho zmenu zo strany širokej komunity. Odpovede respondentov pomôžu lepšie pochopiť povedomie osôb konajúcich v mene prevádzkovateľov základných služieb v spomínanej oblasti.

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

3. Výstupy z konzultácií

3.1. Výstupy z dotazníkového prieskumu

Dotazník bol distribuovaný elektronicky e-mailom 250 najvýznamnejším prevádzkovateľom základnej služby. Viac ako 3 týždne bol zverejnený na webovom sídle www.nbu.gov.sk. Celkovo bolo doručených 105 odpovedí, ktoré sú zhrnuté v tejto kapitole.



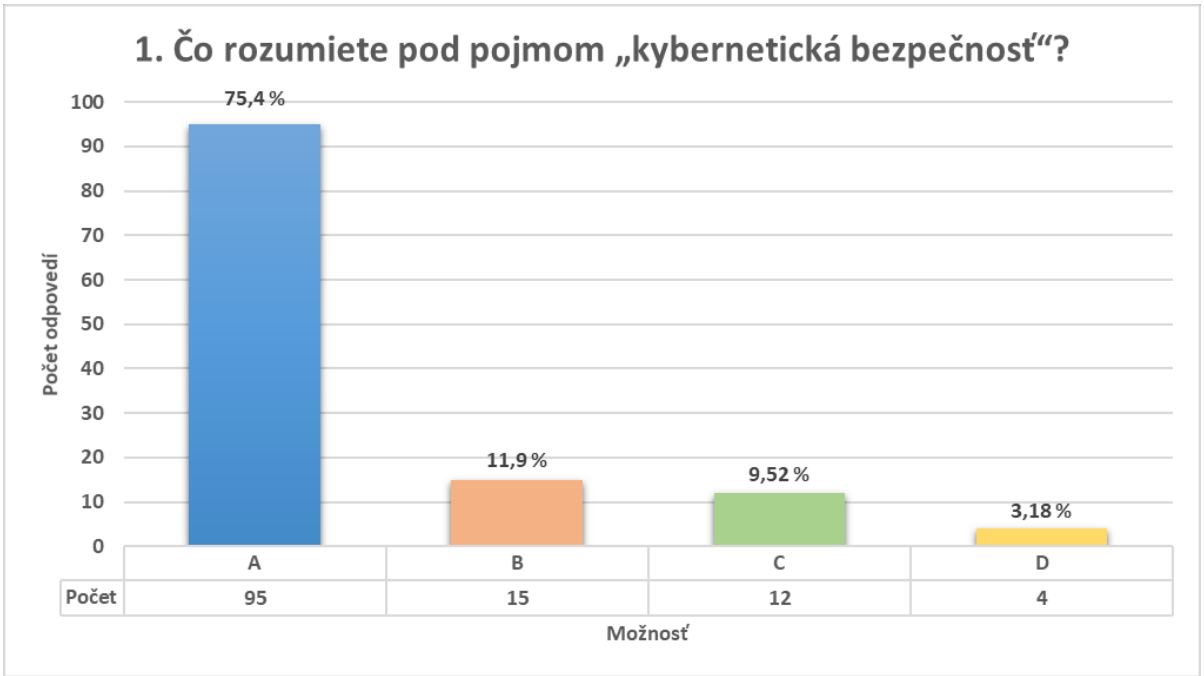
3.1.1. Čo rozumiete pod pojmom „kybernetická bezpečnosť“?

Ako je možné vidieť z grafu nižšie, 75 % subjektov pod pojmom kybernetická bezpečnosť rozumie „stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov“.

Približne 11,9 % pod týmto pojmom rozumie „postup ochrany digitálnych informácií, zariadení a aktív, ku ktorým patria vaše osobné informácie, kontá, súbory, fotografie a dokonca aj peniaze“; 9,52 % pojem chápe ako činnosti potrebné na ochranu sietí a informačných systémov, užívateľov takýchto systémov a iných osôb dotknutých kybernetickými hrozbami“ (napr. zneužitie za účelom získania finančných prostriedkov

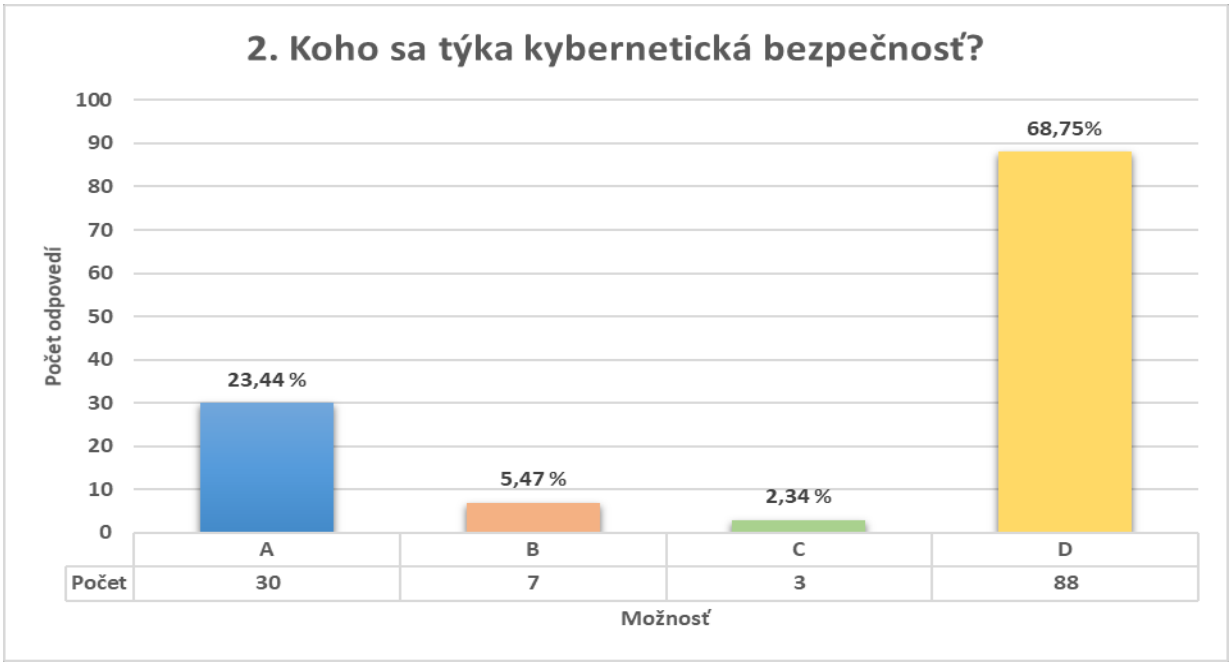
Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

formou vydierania). Len 3% pod týmto pojmom rozumejú „ochranu štátu a štátnych orgánov pred napadnutím treťou mocou v kyberpriestore“.



3.1.2. Koho sa týka kybernetická bezpečnosť?

68,75 % respondentov správne uviedlo, že kybernetická bezpečnosť sa týka nás všetkých; 23,44 % uviedlo verejné a súkromné subjekty, ktoré reguluje zákon; 5,47 % subjekty kritickej infraštruktúry a 2,34 % respondentov uviedlo, že kybernetická bezpečnosť sa týka subjektov zasiahnutých kybernetickým incidentom, ktoré nie sú regulované zákonom.



Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

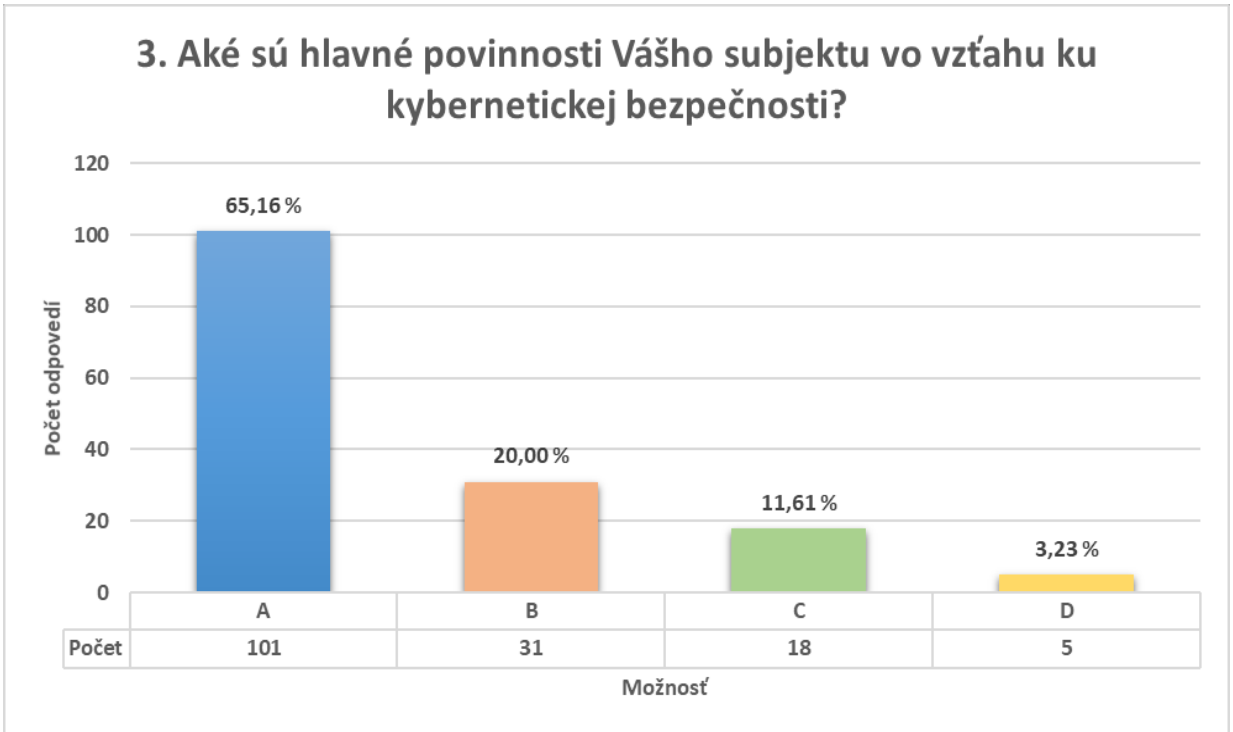
3.1.3. Aké sú hlavné povinnosti Vášho subjektu vo vzťahu ku kybernetickej bezpečnosti?

65,16 % respondentov plní opatrenia, ktoré sa viažu na prevádzkovateľa základnej služby alebo poskytovateľa digitálnej služby podľa zákona č. 69/2018.

Pätina respondentov realizuje aj aktivity, ktoré prispievajú k zvyšovaniu úrovne kybernetickej bezpečnosti ako informovanosť a vzdelávanie o dodržiavaní kybernetickej bezpečnosti, kybernetická hygiena, segmentácie siete, konfigurácia zariadení, penetračné testy a podobne.

11,61 % využíva externé konzultačné služby a aktívne zapája špecializované firmy pri nastavovaní bezpečnosti systémov a sietí za účelom zvýšenia úrovne kybernetickej bezpečnosti.

Odpoveď iné uviedlo 3,23 % respondentov, pričom sa jednalo najmä o respondentov, ktorí nie sú prevádzkovatelia základnej služby alebo poskytovatelia digitálnej služby.



3.1.4. Čo je to kybernetický bezpečnostný incident?

Takmer tri štvrtiny respondentov za kybernetický bezpečnostný incident považujú „akúkoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému, obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby, vysoká pravdepodobnosť

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

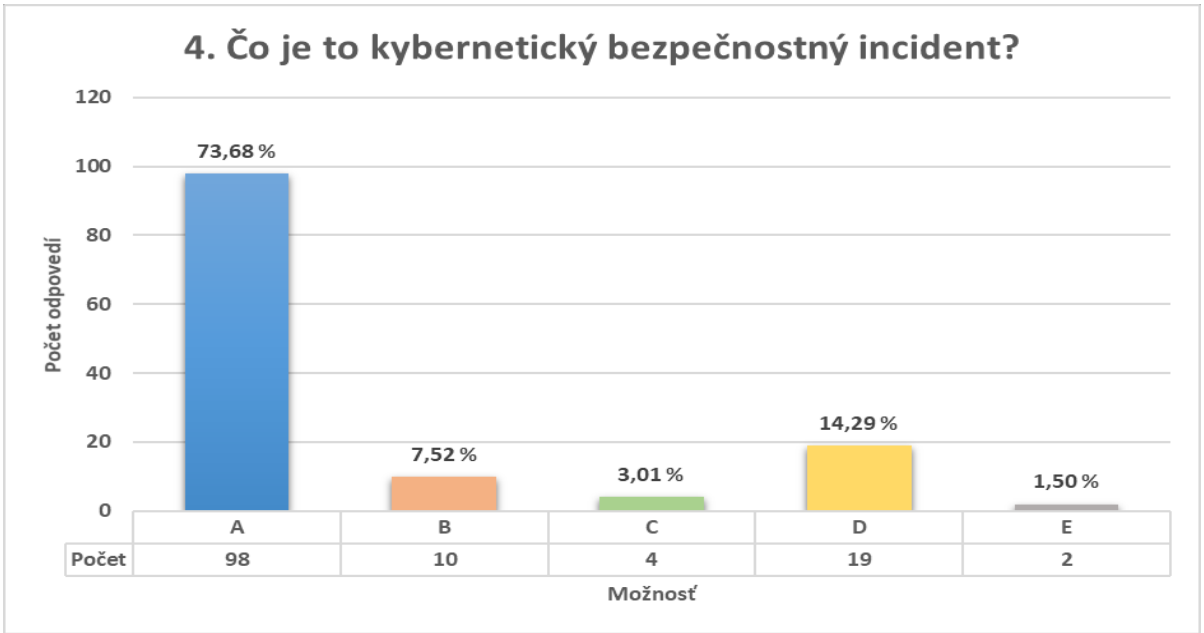
kompromitácie činností základnej služby alebo digitálnej služby alebo ohrozenie bezpečnosti informácií“.

7,52 % respondentov definuje kybernetický bezpečnostný incident ako „narušenie bezpečnosti informácií v informačných systémoch, alebo narušenie bezpečnosti služieb, alebo bezpečnosti a integrity sietí elektronických komunikácií v dôsledku kybernetickej bezpečnostnej udalosti“.

3,01 % respondentov označilo za kybernetický bezpečnostný incident „narušenie informačných činností, ktoré slúžia na získavanie, zhromažďovanie, spracúvanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archiváciu a likvidáciu údajov takým spôsobom, že dôvernosť a integrita týchto informačných činností nemôže byť zaručená“.

14,29 % respondentov za kybernetický bezpečnostný incident považuje „udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov“.

Len 1,50 % uviedlo odpoveď iné (napr. kybernetický incident je tiež realizácia bezpečnostného rizika, čiže realizácia hrozby s následným dopadom na dostupnosť, dôvernosť, integritu alebo nepopierateľnosť informácií v kybernetickom priestore, takže napríklad nie únik alebo rekonštrukcia tlačených písomností alebo hovoreného slova), alebo iný príklad: kybernetický incident je nežiaduci alebo neoprávnený prípad alebo udalosť, ktorá sa týka bezpečnosti informačných technológií, počítačových systémov, sietí alebo elektronických údajov. Tieto incidenty môžu byť spôsobené rôznymi hrozbami, útokmi alebo nežiaducimi udalosťami, ktoré majú za následok poškodenie, stratu alebo neoprávnený prístup k informáciám).



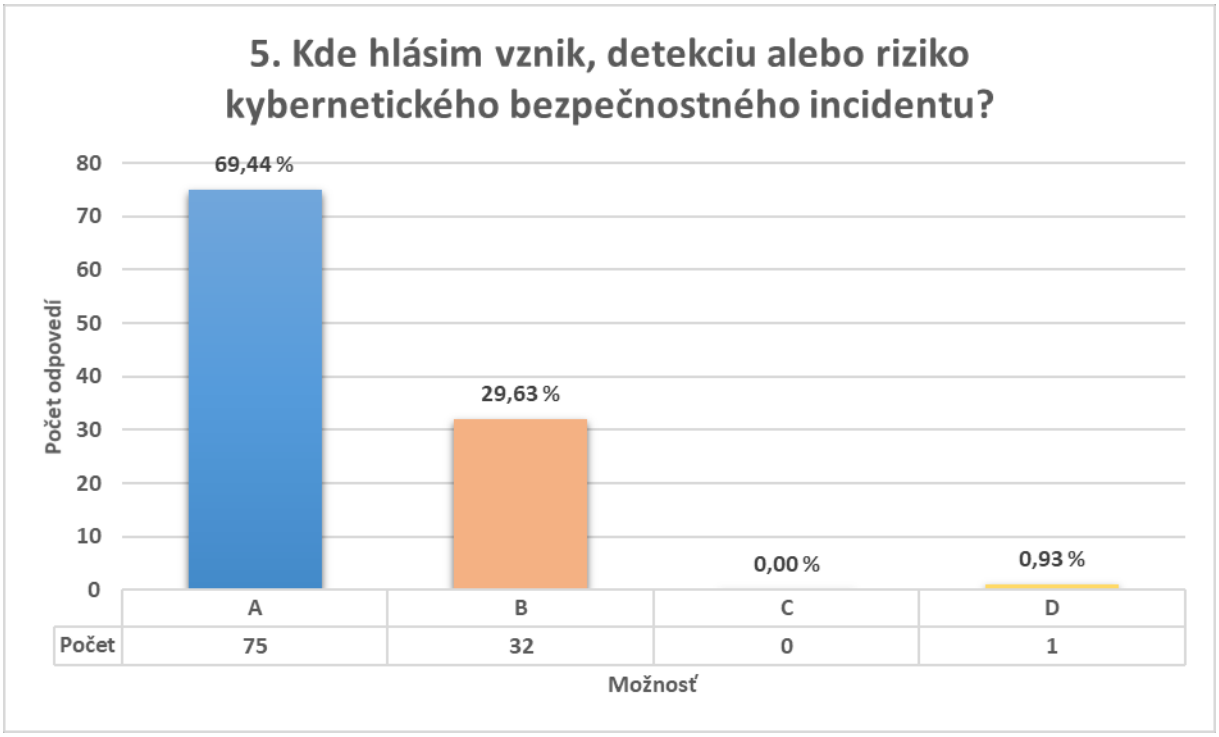
Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

3.1.5. Kde hlásim vznik, detekciu alebo riziko kybernetického bezpečnostného incidentu?

Z pohľadu odpovedí na otázku, ktorej účelom bolo zistiť povedomie o tom, kde subjekty majú hlásiť kybernetický bezpečnostný incident, 69,44 % respondentov odpovedalo, že hlási každý závažný kybernetický bezpečnostný incident, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov.

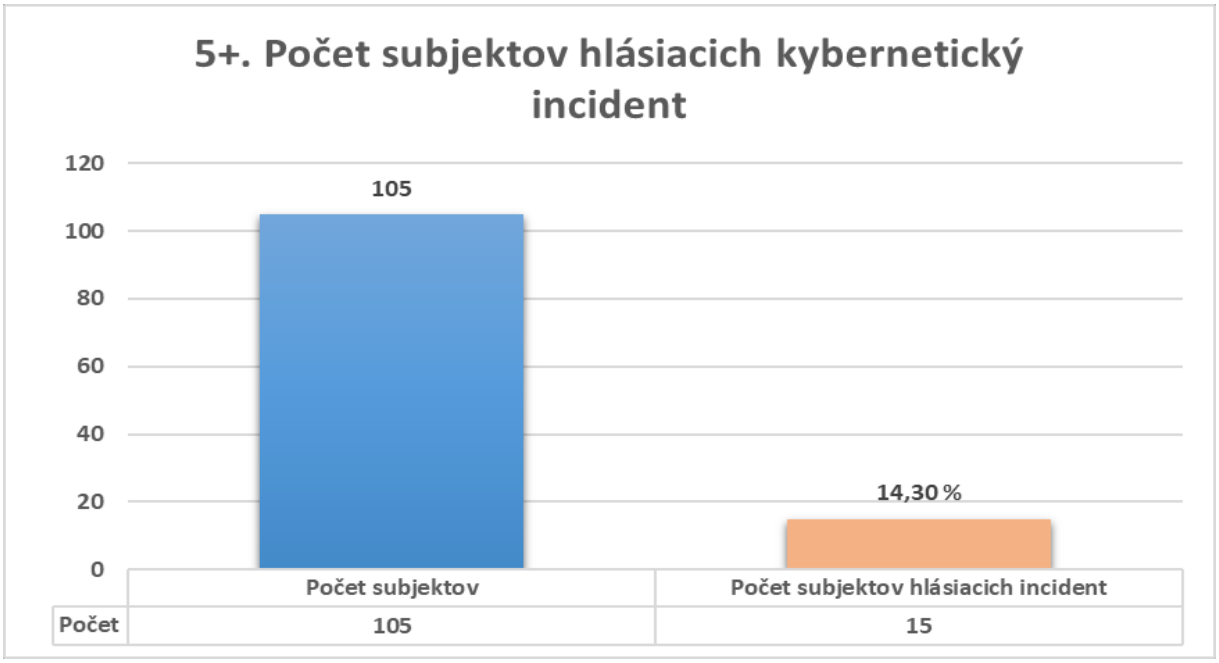
Hlásenie kybernetických bezpečnostných incidentov vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti príslušnému orgánu. 29,63 % respondentov odpovedalo, že hlási každý závažný kybernetický bezpečnostný incident, pričom hlásenie kybernetických bezpečnostných incidentov vykonáva prostredníctvom manažéra kybernetickej bezpečnosti/štatutára.

Iba 0,93 % respondentov odpovedalo, že hlásenie kybernetických bezpečnostných incidentov vykonáva prostredníctvom orgánov presadzovania práva (resp. orgánov činných v trestnom konaní). Ani jeden respondent neuviedol, že hlásenie kybernetických bezpečnostných incidentov vykonáva hlásením medzinárodným orgánom na to určeným (ENISA).



Z celkového počtu 105 respondentov, len 14,30 % respondentov uviedlo, že hlásili kybernetický incident. Inštitúcie tieto incidenty nahlasovali prioritne SK-CERT, menší počet aj CSIRT, Úradu na ochranu osobných údajov a dodávateľom IS.

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť



3.1.6. Čo znamená audit kybernetickej bezpečnosti?

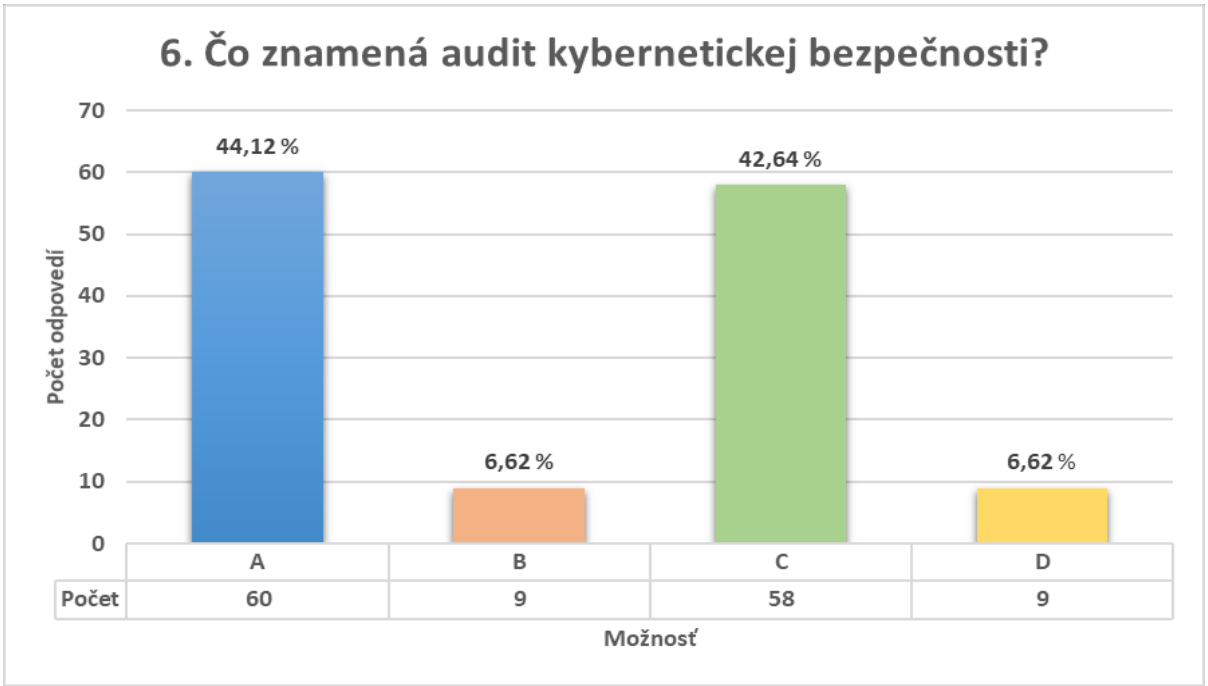
Na otázku čo znamená audit kybernetickej bezpečnosti 44,12 % respondentov uviedlo, ako odpoveď „splnenie si zákonných povinností, ktoré mi ukladá zákon č. 69/2018 o kybernetickej bezpečnosti“.

Približne rovnaký podiel respondentov 42,64 % uviedlo, že „audit, je nástrojom na zisťovanie nedostatkov úrovne kybernetickej bezpečnosti a zraniteľnosti regulovaného subjektu, spoločnosti (firma), orgánu verejnej moci, samosprávy alebo obce“.

6,62 % respondentov uviedlo že audit znamená zvyšovanie úrovne kybernetickej bezpečnosti regulovaného subjektu, spoločnosti (firmy), orgánu verejnej moci, samosprávy alebo obce.

Rovnaký počet respondentov uviedol inú odpoveď.

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť



Z odpovedí jednotlivých respondentov, uvádzame niektoré stanoviská, ktoré preukazujú vnímanie definície auditu jednotlivými PZS:

- odpoveď 6A je len čiastočne platná v zmysle, že vykonanie auditu je síce zákonnou povinnosťou pre určité subjekty, audit však automaticky neznamená splnenie všetkých zákonných povinností, ale je to nástroj, ktorý umožňuje zistiť mieru a vyspelosť plnenia v jednotlivých oblastiach a prispieva k zvyšovaniu úrovne KB daného subjektu. Audit slúži vedeniu spoločnosti aj ako nezávislé porovnanie deklarovaného stavu so skutočným. V zmysle ISO 19011 je audit systematický, nezávislý a dokumentovaný proces pre získanie objektívneho dôkazu a pre jeho objektívne hodnotenie s cieľom stanoviť, v akom rozsahu sú splnené kritériá auditu. Kritériami kybernetického auditu je potom napríklad plnenie legislatívnych požiadaviek,
- nástroj na zisťovanie súladu skutkového stavu s požadovaným stavom,
- overenie plnenia povinností, ktoré PZS ukladá zákon č. 69/2018 a posúdenie zhody prijatých bezpečnostných opatrení s požiadavkami podľa vyššie uvedeného zákona,
- iné:
  - posúdenie zhody prijatých bezpečnostných opatrení s požiadavkami podľa zákona a súvisiacich osobitných predpisov,
  - cieľom auditu je proaktívne identifikovať nedostatky v kybernetickej bezpečnosti – najmä neodhalené hrozby a riziká,
  - audit vykonáva výhradne certifikovaný audítor kybernetickej bezpečnosti.
- overenie plnenia povinností podľa zákona 69/2018, posúdenie zhody prijatých bezpečnostných opatrení s požiadavkami zákona 69/2018,

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

- overenie plnenia povinností a prijatých opatrení pre jednotlivé oblasti podľa (najmä) §20 ods. 3 zákona o kybernetickej bezpečnosti,
- auditom kybernetickej bezpečnosti sa rozumie overenie plnenia povinností podľa zákona. 69/2018, posúdenie zhody prijatých bezpečnostných opatrení s požiadavkami podľa tohto zákona, ktoré sa vzťahujú na bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby pre jednotlivé siete a informačné systémy základnej služby a pre prostriedky, ktoré podporujú základné služby,
- auditom kybernetickej bezpečnosti sa overuje plnenie povinností podľa zákona a posudzuje sa zhoda prijatých bezpečnostných opatrení s požiadavkami podľa zákona a súvisiacich osobitných predpisov. Cieľom auditu kybernetickej bezpečnosti je zabezpečiť požadovanú úroveň kybernetickej bezpečnosti a predchádzať kybernetickým bezpečnostným incidentom,
- auditom sa overuje plnenie povinností podľa zákona 69/2018 a posudzuje sa zhoda prijatých bezpečnostných opatrení s požiadavkami podľa tohto zákona a súvisiacich osobitných predpisov vzťahujúcich sa na bezpečnosť sietí a IS prevádzkovateľa základnej služby pre jednotlivé siete a IS základnej služby.

3.1.7. Vykonali ste už audit kybernetickej bezpečnosti?

Siedma otázka sa zaoberala vykonaním auditu kybernetickej bezpečnosti.

Takmer 90 % respondentov vykonalo audit kybernetickej bezpečnosti, pričom 43,26 % z nich neidentifikovalo žiadne problémy, 23,40 % identifikovalo problém v podobe nedostatočných personálnych zdrojov, 11,70 % identifikovalo ako problém finančnú náročnosť. Pre 4,26 % respondentov bola problematická nejasná formulácia v zákone. 2,13 % označilo za problematickú nepostačujúcu dobu na vykonanie auditu.

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

V odpovediach jednotlivých respondentov sú nižšie uvedené vybrané exempláre, ktoré preukazujú vnímanie náročnosti auditu jednotlivými PZS:

- audit KB a príprava naň je náročný proces a určite sa objavujú všetky uvedené problémy, je zrejmé že subjekty od určitej úrovne musia aplikovať systém riadenia informačnej bezpečnosti vrátane kybernetickej bezpečnosti, ale samotné požiadavky a procesy auditov by mali byť dlhodobo harmonizované s najlepšou praxou existujúcich štandardov informačnej bezpečnosti, zrozumiteľné a zjednodušené, vrátane dostupnosti vysvetlení a praktických návodov. Možno ešte dôležitejším nástrojom pre zvyšovanie úrovne kybernetickej bezpečnosti by malo byť organizované vzdelávanie a nastavovanie spolupráce prevádzkovateľov základných (esenciálnych) služieb, formou konferencií, stretnutí, workshopov a cvičení ktoré by organizovali príslušné inštitúcie a prevádzkovatelia by mali stanovenú povinnú mieru účasti na týchto aktivitách.

  Z hľadiska auditu – dôležité je hodnotenie vyspelosti (maturity) organizácie v jednotlivých oblastiach, aby výstupom auditu bola realistická indikácia stavu a vývoja zavedeného systému, čo v prípade binárneho hodnotenia kritérií popísaných legislatívnym jazykom neprináša realistické výsledky blízke skutočnému stavu. Otázka je nejednoznačne položená. Nie je jasné, či je potrebné odpovedať z pozície audítora alebo auditovaného. Na otázku „podstúpili ste audit kybernetickej bezpečnosti?“ odpovedáme „Áno“,

- niektoré položky auditného checklistu sú ťažko uchopiteľné a nie je hmatateľné, aké opatrenia sa očakávajú pre ich naplnenie,

- technický problém – neaplikovateľnosť niekoľkých požiadaviek v OT prostredí, ktoré potom môžu svietiť ako čiastočný nesúlad v správe,

- odlišný pohľad audítora na rozsah a spôsob plnenia niektorých povinností vyplývajúcich zo zákona,

- existujú len nároky na prevádzkovateľa, čo má mať splnené, ale je veľmi málo šablón, metodík, workshopov alebo príkladov, ako opatrenia (technické, dokumentácia, atď.) správne a efektívne do organizácie zaviesť. Poukázať na chyby je dobré, ale zbytočné, ak v organizácii nevedia, ako ich vyriešiť. Tiež by som privítal, keby boli PZS upozorňovaní NBÚ a notifikovaní o povinnosti vykonať audit do určitého dátumu.

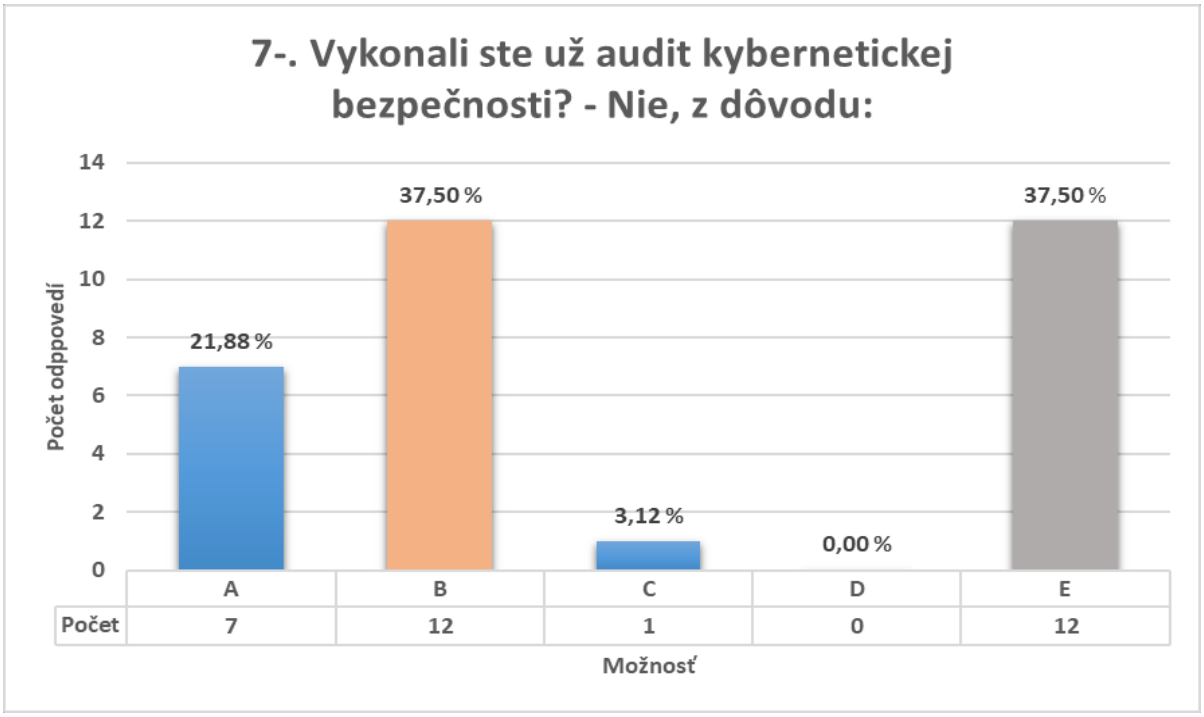
Približne 10 % respondentov audit kybernetickej bezpečnosti ešte nevykonalo.

37,50 % respondentov označili ako dôvod nevykonania auditu kybernetickej bezpečnosti nedostatok finančných prostriedkov, rovnako 37,50 % respondentov uviedlo odpoveď „Iné“ kam patria predovšetkým samosprávy, ktoré vykonalo

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

samohodnotenie kybernetickej bezpečnosti ktoré im umožňovala legislatíva do 31. 12. 2023.

U ostatných respondentov audit práve prebieha, alebo ho plánujú, alebo audit vykonala nadradená organizácia. 21,88 % respondentov uviedlo, že audit nevykonali z dôvodu nedostatku personálnych zdrojov, 3,12 % uviedlo ako dôvod nedostatočnú znalosť zákona.



3.1.8. Čo Vám chýba v zákone č. 69/2018 Z. z. a čo by ste chceli upraviť (doplniť)?

Posledná otázka bola otvorenou otázkou a predstavuje významný zdroj informácií o očakávaniach komunity vo vzťahu k novej legislatíve. Odpovede zaslané respondentmi sú zosumarizované v kapitole č. 4.

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

3.2. Konzultácie s odbornou a laickou verejnosťou

Podujatie	Konferencia Kybernetická bezpečnosť 2023
Dátum	02. – 03.10. 2023
Popis	Mesiac október bol Európskym mesiacom kybernetickej bezpečnosti. Uskutočnila sa v ňom prestížna EPI konferencia Kybernetická bezpečnosť 2023. Piaty ročník sa venoval širokému spektru tém – od zdôraznenia reálneho presahu notácie informačnej architektúry a kybernetickej bezpečnosti, resp. riadenia kybernetických rizík, cez odolnosť v kyberpriestore založenú na každodennej realite, bilancii auditu a posudzovania kyberbezpečnosti až po ľudské zdroje v kyberbezpečnosti a ochrane údajov. Predmetom bolo aj predstavenie a konzultácie k pripravovanej novele zákona č. 69/2018 o kybernetickej bezpečnosti, ktorou sa implementuje Smernica o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (smernica NIS2).
Cieľová skupina	samospráva, súkromný sektor
Link	https://konferencie.profivzdelavanie.sk/2023/kyberneticka-bezpecnost/

Podujatie	Webinár zvyšovanie kybernetickej bezpečnosti slovenských firiem z pohľadu aktuálnej legislatívy a financií
Dátum	05.10.2023
Popis	Slovenská agentúra pre rozvoj investícií a obchodu (SARIO) pre slovenských podnikateľov zorganizovala webinár s názvom Zvyšovanie kybernetickej bezpečnosti slovenských firiem z pohľadu aktuálnej legislatívy a financií. Počas webináru boli prezentované najnovšie novinky z oblasti legislatívy kybernetickej bezpečnosti; možnosti, ako získať finančnú podporu na kyberbezpečnostné projekty a ako zvýšiť kybernetickú bezpečnosť slovenských firiem. Keďže na sektory ako digitálna infraštruktúra, energetika, fintech, priemysel, obehové hospodárstvo, zdravotníctvo a bankovníctvo sa vzťahujú povinnosti zo zákona o kybernetickej bezpečnosti, boli predstavené informácie o tom, ako ich naplniť, novinky v legislatíve NIS2 aj informácie o novom znalostnom štandarde pre roly v KB.
Cieľová skupina	súkromný sektor
Link	https://www.sario.sk/sk/projekty-podujatia/zvysovanie-kybernetickej-bezpecnosti-slovenskych-firiem-z-pohladu-aktualnej

Podujatie	Peer Learning Session on Cybersecurity Skills in the context of National Cybersecurity Strategies
Dátum	17.10.2023
Popis	Agentúra Európskej únie pre kybernetickú bezpečnosť ENISA realizovala na Slovensku sériu neverejných seminárov

	zameraných na kyberbezpečnostné vzdelávanie. Ich cieľom bolo vytvoriť priestor, v ktorom môžu členské štáty zdieľať skúsenosti a dohodnúť sa, ako budú postupovať v nasledujúcom období. Na prvom seminári v Bratislave sa zúčastnili zástupcovia agentúry ENISA a národných koordinačných centier kybernetickej bezpečnosti zo Španielska, Talianska, Českej republiky a Slovenska. Slovensko svoj prístup k vzdelávaniu prezentovalo na seminári ostatným zúčastneným členským štátom. Predmetom seminára bola aj diskusia k legislatíve NIS2.
Cieľová skupina	verejná správa
Link	https://www.nbu.gov.sk/2023/10/19/v-kybernetickej-bezpecnosti-mame-nedostatok-ludi-problem-nam-pomaha-riesit-europska-unia/index.html

Podujatie	Stretnutie certifikovaných audítorov
Dátum	21.11.2023
Popis	Národný bezpečnostný úrad, Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (KCCKB) v spolupráci so spoločnosťou Tüv Süd Slovakia zorganizovali podujatie pre desiatky audítorov z oblasti kybernetickej bezpečnosti. Zástupcovia spomínaných organizácií si s nimi vymenili aktuálne poznatky a skúsenosti v oblasti regulácie. Hlavnou témou podujatia bola nová smernica NIS2 a jej dôsledky na prevádzkovateľov základnej služby (PSZ). Cieľom bola diskusia k smernici NIS 2, ktorá je zameraná na celoeurópske zlepšenie úrovne kybernetickej bezpečnosti.
Cieľová skupina	Verejná správa, súkromný sektor
Link	https://www.nbu.gov.sk/2023/11/23/slovensku-chybaju-auditori-kybernetickej-bezpecnosti/index.html

Podujatie	Medzinárodná konferencia ITAPA
Dátum	20.11 – 23.11. 2023
Popis	Prednáška NBÚ a diskusia v rámci viacerých panelov sa zamerala na legislatívnu aktivitu EK a SR. Od predstavenia prvej horizontálnej kyberbezpečnostnej legislatívy, ktorou bola smernica NIS, prešla takmer dekáda. Jej cieľom bolo dosiahnutie vysokej úrovni kybernetickej bezpečnosti v celej EÚ, čo sa podarilo. Dokonca štandard NIS úspešne EÚ exportuje aj do tretích krajín podobne ako pri GDPR. Nedávne obdobie bolo pomerne bohaté na viaceré dôležité spisy. Spomeňme napríklad finalizáciu aktualizovanej Smernice o bezpečnosti sietí a informácií (NIS2). Panelisti diskutovali o tom, či je náš súčasný legislatívny rámec naďalej vhodný na účinnú reakciu voči kyberbezpečnostným incidentom, hrozbám a trendom. Diskusia mala poukázať na to, kde sa vlastne nachádzame s úrovňou kybernetickej bezpečnosti a súvisiacou digitálnou legislatívou s kyberbezpečnostnými prvkami.
Cieľová skupina	Verejná správa, súkromný sektor, akademická sféra
Link	https://www.itapa.sk/14721-sk/program-jarna-itapa-2023/

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

Podujatie	Workshop KCCKB pre komunitu
Dátum	17.01.2024
Popis	Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (KCCKB) v spolupráci s Národným bezpečnostným úradom, privítali v Bratislave na neformálnom podujatí desiatky členov kyberbezpečnostnej komunity. Hlavnou témou podujatia bola nová smernica NIS2 a jej dôsledky na prevádzkovateľov základnej služby (PSZ). Zástupcovia komunity si s NBÚ a KCCKB vymenili aktuálne poznatky a skúsenosti v oblasti regulácie NIS2 a prezentovali návrhy týkajúce sa jej implementácie do praxe.
Cieľová skupina	Verejná správa, súkromný sektor, akademická sféra
Link	N/A

Podujatie	Výročná schôdza PPP
Dátum	18.01.2024
Popis	Zástupcovia NBÚ prezentovali na výročnej schôdzke združenia Partnerstvá pre prosperitu legislatívnu aktivitu EK a SR. Prezentácia bola zameraná na novú smernicu NIS2 a jej dôsledky na prevádzkovateľov základnej služby (PSZ). Zástupcovia komunity si s NBÚ vymenili aktuálne poznatky a skúsenosti v oblasti regulácie NIS2 a prezentovali návrhy týkajúce sa jej implementácie do praxe.
Cieľová skupina	Verejná správa, súkromný sektor, akademická sféra
Link	N/A

Podujatie	Webinár pre rakúske spoločnosti pôsobiace v rámci SR
Dátum	30.01.2024
Popis	Európska smernica NIS2 zavádza prísnejšie predpisy o kybernetickej bezpečnosti pre mnohé odvetvia a spoločnosti – vrátane tých, ktorých sa predchádzajúce predpisy netýkali. Cieľom je obmedziť útoky na IT systémy v EÚ, ktoré poškodzujú hospodárstvo a spoločnosti. Rakúskym spoločnostiam bol na webinári poskytnutý prehľad o situácii v Českej republike a na Slovensku so štyrmi špičkovými odborníkmi z Bratislavy, Prahy, Brna a Viedne. Cieľom bolo umožniť rakúskym spoločnostiam, ktoré dodávajú na Slovensko a do Českej republiky, a ich miestnym pobočkám, pripraviť sa čo najlepšie na nové požiadavky, ktoré budú platiť od októbra 2024.
Cieľová skupina	Súkromný sektor
Link	N/A

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

4. Zhrnutie návrhov v rámci konzultácií

Poznatky a odporúčania získané cez vyššie uvedené komunikačné nástroje je možné zhrnúť do nasledujúcich bodov:

- zosúladiť vyhlášku 162/2018, ktorou sa určujú identifikačné kritériá prevádzkovateľa služby so smernicou EP 2022/2555 kde v našej vyhláške chýbajú niektoré body.

- smernica NIS 2 v prílohe č. 1 obsahuje v odvetví 8. Digitálna infraštruktúra tieto typy subjektov:

    - poskytovatelia internetových prepojovacích uzlov:
        - poskytovatelia služieb DNS, s výnimkou prevádzkovateľov koreňových názvových serverov,
        - správcovia názvov TLD,
        - poskytovatelia služieb cloud computingu,
        - poskytovatelia služieb dátového centra,
        - poskytovatelia sietí na sprístupňovanie obsahu,
        - poskytovatelia dôveryhodných služieb,
        - poskytovatelia verejných elektronických komunikačných sietí,
        - poskytovatelia verejne dostupných elektronických komunikačných služieb.

    V slovenskej vyhláške 164/2018 Národného bezpečnostného úradu z 1. júna 2018 (ktorá bola doplnená od 1.9.2023), ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby) v prílohe č. 1 je však v odvetví 8. Digitálna infraštruktúra iný počet subjektov:

    - poskytovateľ služby výmenného uzla internetu na prepájanie sietí, ktoré sú z technického a organizačného pohľadu oddelené,
    - poskytovateľ služieb systému doménových mien na internete,
    - subjekt spravujúci alebo prevádzkujúci register internetových domén najvyššej úrovne.

- legislatíva by mala byť zjednodušená na podstatné oblasti, viac klásť dôraz na zdieľanie zdrojov o najlepšej praxi, vzdelávanie/zvyšovanie povedomia aj organizované zo strany štátnych inštitúcií, ale aj zabezpečenie vzájomného informovania medzi prevádzkovateľmi. Napríklad v súčasnosti prevádzkovatelia nedisponujú kontaktnými údajmi iných prevádzkovateľov v oblasti kybernetickej bezpečnosti, teda rýchla reakcia je oslabená, rovnako ani nie je deklarovaný rozsah a možnosti pomoci zo strany centier kybernetickej bezpečnosti štátu v prípade zistenia možnej udalosti/incidentu. Tiež je dôležité aby podobná sieť vzájomnej komunikácie a požiadaviek bola nastavená vo vzťahu k subdodávateľom, teda zvýšený dôraz na odolnosť/riadenie dodávateľského

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

reťazca – vhodná inšpirácia Digital Operations Resilience Act, NIST Updates Cybersecurity Guidance for Supply Chain Risk Management a pod. Radi sa zúčastníme na procese prípravy novelizácie/zmien zákona o kybernetickej bezpečnosti a poskytneme ďalšie informácie a skúsenosti z doterajšej implementácie kybernetickej bezpečnosti, aj vzhľadom na to, že podniky poskytujúce elektronické komunikačné služby často slúžia aj na notifikáciu možných narušení v sieťach/zariadeniach svojich účastníkov a poskytujú základnú osvetu svojim zákazníkom,

- definícia a jednoznačné rozdelenie požiadaviek na IT a priemyselné systémy je potrebné, keďže nie všetky sú aplikovateľné v oblasti OT,

- základným stavebným prvkom pri plnení bezpečnostných opatrení podľa zákona č. 69/2018 je analýza rizík. Bolo by vhodné vykonávacím predpisom upraviť podrobnosti, najmä jednotnú a záväznú metodiku analýzy rizík. Hoci NBÚ má na svojom portáli zverejnenú odporúčanú metodiku pre analýzu rizík, tá však nie je právne záväzná pre všetkých prevádzkovateľov základných služieb.

  V nadväznosti na nadchádzajúcu transpozíciu Smernice NIS 2 do slovenského právneho poriadku zároveň budeme veľmi pozitívne vnímať, ak nedôjde k transpozícii nad rámec povinností v nej stanovených (tzv. goldplating). Vzhľadom na predmet úpravy NIS 2 by povinnosti zavedené nad rámec smernice mali za následok významný finančný dopad pre prevádzkovateľov základných služieb pri implementácii nevyhnutných technických a organizačných nástrojov za účelom splnenia takýchto prípadne stanovených extenzívnych povinností.

- Väčší dôraz na realizáciu analýzy rizík a následná väčšia autonómia pri stanovení bezpečnostných opatrení, ktoré budú aplikované. Aktuálne sú bezpečnostné opatrenia taxatívne vymenované a ich splnenie nemusí vždy znamenať optimálnu (miera rizika / účinnosť opatrenia/ náklady) ochranu. Príkladom takéhoto zákonom vyžadovaného technického riešenia je napr. vulnerability scanner.

- Kybernetické hrozby sú na svete rovnaké, avšak subjekty a možné dopady v prípade útokov nie sú dostatočné diverzifikované. Klasifikácia a kategorizácia samotných informačných systémov a zároveň samotná definícia dôvernosti, dostupnosti a integrity dát by mohla mať hlbší charakter a sprievodné vysvetlenie pre samotnú identifikáciu.

- Návrhy týkajúce sa dokumentov nadväzujúcich na legislatívu:
  - Bližšia identifikácia, zároveň definícia manažéra kybernetickej bezpečnosti
  - Chýbajúce metodické usmernenia, bezplatné školenia a webináre – celkovo pre kybernetickú bezpečnosť a zároveň rolu MKB.
  - Uznávanie certifikácii aj iných krajín, nie len SK

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

- Platforma/fórum na výmenu „best practise“, poznatkov, prístupov – mimo spoplatnené semináre, s možnosťou otvorene komunikovať obdobné problémy a prístupy, nové technológie, riešenia. Skrz finančnú náročnosť by sa tak podporila a hlavne zefektívnila samotná kybernetická bezpečnosť (vyšší záujem a reálny prístup k zákonu). Obdobne ako etický hackeri, aj v kybernetickej bezpečnosti máme excelentných ľudí, ktorých skúsenosti nie sú vždy predávané ako spoplatnená služba na báze predplatného.

- Vzhľadom na rýchly vývoj technológií a kybernetických hrozieb je dôležité pravidelne aktualizovať definície v zákone tak, aby zodpovedali súčasným trendom a technologickým výzvam (napr. AI). Zabezpečenie, aby zákon bol navrhnutý tak, aby bol flexibilný a schopný sa prispôsobiť rýchlemu vývoju kybernetických hrozieb. Zabezpečenie, že zákon podporuje a uľahčuje spoluprácu medzi verejným a súkromným sektorom pri riešení kybernetických hrozieb.

- Možnosť vykonať samohodnotenie aj v ďalších rokoch, ktorým sa nahradí povinnosť vykonať certifikovaný audit v zmysle zákona, nakoľko samospráva nemá dostatok finančných prostriedkov na zabezpečenie certifikovaného auditu. Rovnako v zákone chýbajú jasné špecifikácie povinností jednotlivých subjektov, t.j. v zákone sú vymedzené široko, resp. všeobecne. Zároveň by sme uvítali možnosť získania nenávratných fin. prostriedkov, ktoré by boli určené na zvyšovanie úrovne kybernetickej bezpečnosti v samospráve.

- Samosprávy by privítali aktívnejšiu pomoc štátu, napríklad vybudovaním centier kybernetickej bezpečnosti, napr. v každom kraji, ktoré by pre mestá túto agendu za určitú úhradu realizovali, namiesto toho, aby sme prostriedky investovali do súkromných firiem. Vychádzajú z toho, že infraštruktúra na mestách je dosť podobná a používa sa obmedzená množina softvéru, tak správa a dohľad by boli jednoduchšie.

- Zapracovanie možnosti Samohodnotenia kontroly plnenia povinností v zmysle zákona o kybernetickej bezpečnosti vo frekvencii raz za 12 mesiacov a zároveň frekvenciu vykonávania auditu prostredníctvom certifikovaného audítora kybernetickej bezpečnosti v zmysle ustanovení §29 ods. 3 zákona o kybernetickej bezpečnosti predĺžiť na obdobie raz za 5 rokov. Vzhľadom na fakt, že v zmysle § 29 ods. 7 zákona o kybernetickej bezpečnosti si náklady na audit kybernetickej bezpečnosti audítorom kybernetickej bezpečnosti uhrádzajú prevádzkovatelia základnej služby, prišlo by tak k zníženiu finančnej záťaže subjektov, ktoré by výkon kontroly plnenia povinností v zmysle zákona o kybernetickej bezpečnosti realizovali formou Samohodnotenia v zmysle zákona o kybernetickej bezpečnosti raz za 12 mesiacov

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

- Jasnejšia definícia čo je to základná služba a ktoré informačné systémy PZS pod ňu spadajú a ktoré už nie (súčasná definícia „Základnou službou je služba, ktorá je zaradená v zozname základných služieb....“ je niekedy mätúca a nejasná)

- Zosúladenie zákonov: Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a Zákona č. 95/2019 o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

- Pre subjekt zaradený NBÚ (ako poskytovateľ základnej služby) do povinnosti aplikovať zákon o KB č. 69/2018, zabezpečiť nenávratné finančné zdroje na zabezpečenie potrebných školení, personálu a technického vybavenia

- Vedľa pozície MKB by bolo vhodné doplniť v zákone napr. pozíciu asistenta MKB (AMKB). Pracovné zaťaženie MKB narastá a AMKB by bol súčinný pri riešení pracovných úloh pod vedením MKB. Počet AMKB by bol napr. závislý od veľkosti organizácie/počtu zamestnancov. Ďalej by bol priamo AMKB zastupujúcim v prípade neprítomnosti MKB (PN, dovolenka ap.).

- Zákon alebo jeho vyhláška o bezpečnostných opatreniach by mohla obsahovať exaktnejšie požiadavky v oblasti bezpečnostných testov.

- V zákone lepšie definovať BCM a BIA a v novele zákona sa zaoberať aj utajovanými skutočnosťami.

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

5. Prílohy

Príloha 1 Znenie dotazníka

1. Čo rozumiete pod pojmom „kybernetická bezpečnosť“?

A Stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov.
B Postup ochrany digitálnych informácií, zariadení a aktív, ku ktorým patria vaše osobné informácie, kontá, súbory, fotografie a dokonca aj peniaze.
C Činnosti potrebné na ochranu sietí a informačných systémov, užívateľov takýchto systémov a iných osôb dotknutých kybernetickými hrozbami (napr. zneužitie za účelom získania finančných prostriedkov formou vydierania).
D Ochrana štátu a štátnych orgánov pred napadnutím treťou mocou v kyber priestore.

2. Koho sa týka kybernetická bezpečnosť?

A Verejných a súkromných subjektov, ktoré reguluje zákon.
B Subjektov kritickej infraštruktúry.
C Subjektov zasiahnutých kybernetickým incidentom, ktoré nie sú regulované zákonom.
D Nás všetkých.

3. Aké sú hlavné povinnosti Vášho subjektu vo vzťahu ku kybernetickej bezpečnosti?

A Plníme opatrenia, ktoré sa viažu na prevádzkovateľa základnej služby alebo poskytovateľa digitálnej služby podľa zákona č. 69/2018 Z. z.[1]
B Realizujeme aktivity, ktoré prispievajú k zvyšovaniu úrovne kybernetickej bezpečnosti ako informovanosť a vzdelávanie o dodržiavaní kybernetickej bezpečnosti, kybernetická hygiena, segmentácie siete, konfigurácia zariadení, penetračné testy a podobne.
C Využívame externé konzultačné služby a aktívne zapájame špecializované firmy pri nastavovaní bezpečnosti systémov a sietí za účelom zvýšenia úrovne kybernetickej bezpečnosti.
D Iné (prosím uviesť)
.....

[1] zákon č. 69/2018 o kybernetickej bezpečnosti

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

4. Čo je to kybernetický bezpečnostný incident?

A Akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je:

1. strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,
2. obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,
3. vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo
4. ohrozenie bezpečnosti informácií.

B Narušenie bezpečnosti informácií v informačných systémoch, alebo narušenie bezpečnosti služieb, alebo bezpečnosti a integrity sietí elektronických komunikácií v dôsledku kybernetickej bezpečnostnej udalosti.
C Narušenie informačných činností, ktoré slúžia na získavanie, zhromažďovanie, spracúvanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archiváciu a likvidáciu údajov takým spôsobom, že dôvernosť a integrita týchto informačných činností nemôže byť zaručená.
D Udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov.
E Iné (prosím uviesť)
.....

5. Kde hlásim vznik, detekciu alebo riziko kybernetického bezpečnostného incidentu?

A Riadim sa povinnosťou hlásiť každý závažný kybernetický bezpečnostný incident, ktorý identifikujem na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov. Hlásenie kybernetických bezpečnostných incidentov vykonávam prostredníctvom jednotného informačného systému kybernetickej bezpečnosti príslušnému orgánu.
B Hlásim každý závažný kybernetický bezpečnostný incident, ktorý identifikujem na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov. Hlásenie kybernetických bezpečnostných incidentov vykonávam prostredníctvom manažéra kybernetickej bezpečnosti/štatutára.
C Hlásim každý závažný kybernetický bezpečnostný incident, ktorý identifikujem na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov. Hlásenie kybernetických bezpečnostných incidentov vykonávam prostredníctvom hlásenia medzinárodným orgánom na to určeným (ENISA).
D Hlásim každý závažný kybernetický bezpečnostný incident, ktorý identifikujem na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov. Hlásenie kybernetických bezpečnostných incidentov vykonávam prostredníctvom orgánov presadzovania práva (resp. orgánov činných v trestnom konaní).

5+ V prípade, ak ste hlásili kybernetický bezpečnostný incident
A Uveďte počet incidentov, ktoré ste nahlásili ..... a komu ..... .

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť

6. Čo znamená audit kybernetickej bezpečnosti?

A Splnenie si zákonných povinností, ktoré mi ukladá zákon č. 69/2018 Z. z.[1]
B Zvyšovanie úrovne kybernetickej bezpečnosti regulovaného subjektu, spoločnosti (firmy), orgánu verejnej moci, samosprávy alebo obce.
C Nástroj na zisťovanie nedostatkov úrovne kybernetickej bezpečnosti a zraniteľnosti regulovaného subjektu, spoločnosti (firma), orgánu verejnej moci, samosprávy alebo obce.
D Iné (prosím uviesť)
.....

7. Vykonali ste už audit kybernetickej bezpečnosti?

ÁNO
7+
Áno a stretli sme sa s nasledujúcimi problémami:
A Žiadne problémy
B Časový rámec (*nepostačujúca doba na vykonanie auditu*)
C Personálne zdroje (*bolo to náročné na vykonanie zo strany zamestnanca/ov*)
D Finančné zdroje (*bolo to finančne nákladné*)
E Nejasná formulácia v zákone (*nie úplne sme rozumeli tejto povinnosti*)
F Iné (prosím uviesť)
.....

NIE
7-
Nie, z dôvodu:
A Nedostatok personálnych zdrojov (chýba nám odborný pracovník)
B Nedostatok finančných prostriedkov (chýbajú nám peniaze na vykonanie auditu)
C Nedostatočná znalosť zákona (neoboznámili sme sa s danou povinnosťou)
D Nejasná formulácia v zákone (nerozumieme tejto povinnosti, keďže zákon to neupravuje jasne)
E Iné (prosím uviesť)
.....

8. Čo Vám chýba v zákone č. 69/2018 Z. z.[1] a čo by ste chceli upraviť (doplniť)?

.....
.....
.....
.....
.....

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť