Správa o činnosti pedagogického klubu

1. Prioritná os	Vzdelávanie
2. Špecifický cieľ	1.2.1 Zvýšiť kvalitu odborného vzdelávania a prípravy reflektujúc potreby trhu práce
3. Prijímateľ	Obchodná akadémia Liptovský Mikuláš
4. Názov projektu	Zvýšenie kvality odborného vzdelávania a prípravy na Obchodnej akadémii Liptovský Mikuláš
5. Kód projektu ITMS2014+	312011AGY1
6. Názov pedagogického klubu	Klub IKT
7. Dátum stretnutia pedagogického klubu	21.06.2022
8. Miesto stretnutia pedagogického klubu	Obchodná akadémia Liptovský Mikuláš, miestnosť 103
9. Meno koordinátora pedagogického klubu	Ing. Stanislav Peniaško
10. Odkaz na webové sídlo zverejnenej správy	www.oalm.edupage.org

11. **Manažérske zhrnutie:**

Posledné stretnutie členov klubu v tomto školskom roku bolo zamerané na dve kľúčové téma:

- Kybernetické hrozby – zapracovanie tejto témy do výuky v predmetoch (najmä z pohľadu momentálne platných dokumentov a smerníc EÚ),
- Kyberšikanovanie – momentálny stav na škole, riešenie tejto problematiky na škole a prevencia pred kyberšikanovaním.

V priebehu klubu boli použité a prediskutovávané materiály zverejnené najmä na internetových stránkach:

- https://www.consilium.europa.eu/sk/policies/cybersecurity/
- https://www.minedu.sk/kyberneticke-sikanovanie-medialna-gramotnost-bezpecnost-a-ochrana-sukromia-potreba-kritickeho-myslenia-a-schopnosti-posobit-v-digitalnom-prostredi-pozitivne-a-spravat-sa-zodpovedne/
- https://bezpecnenanete.eset.com/sk/pre-ucitelov/
- https://mpc-edu.sk materiál: 16_oso_titkova_jarmila_-_program_prevecie_sikanovania.pdf

Kľúčové pojmy:

Kybernetické hrozby, dokumenty EÚ, kyberšikanovanie, aktivity so žiakmi - ukážky

12. **Hlavné body, témy stretnutia, zhrnutie priebehu stretnutia:**

1. Kybernetické hrozby
2. Kyberšikanovanie
3. Práca na vlastnými materiálmi k téme

K bodu 1:

EÚ v poslednej dobe intenzívne rieši problematiku kybernetických hrozieb. V rámci diskusie si členovia klubu prezreli a prediskutovali materiály, ktoré sú zverejnené na stránke https://www.consilium.europa.eu/sk/policies/cybersecurity. Najviac času sa venovalo materiálom:

- Infografika – Najväčšie kybernetické hrozby v EÚ
- Boj proti zneužívaniu detí online
- Sankcie proti kybernetickým útokom
- Program Digitálna Európa

Najbežnejšie kybernetické útoky na školách o ktorých bola diskusia sú:

- neoprávnené používanie WiFi sietí a internetového pripojenia – hranie hier a nelegálne sťahovanie súborov, nebezpečného a škodlivého obsahu, strata súkromia a nenávistné prejavy na internete,
  z uvedeného sa na našej škole vyskytli strata súkromia z dôvodu obnovenia a vytvorenia konta na zariadení spolužiaka,
- prezradenie hesiel a útoky na mailové služby –skôr je u nás problém s častou stratou a zabudnutím hesla ku školskému emailu, rieši sa administráciou školských emailov v prostredí GoogleApps,
- ransomvérové útoky – šifrovacie a výpalnícke víry sa zatiaľ na škole nezistili,
- phishingové útoky vedúce k odhaleniu osobných a dôverných údajov – zneužívanie prvkov sociálneho inžinierstva, rieši sa individuálne so žiakmi, ktorí nahlasujú veľký počet nevyžiadaným emailov,
- útoky odmietnutia služby – DDoS útoky a preťaženie školskej infraštruktúry sa rieši prenajímaním priestoru na web servery externým dodávateľom, takýto útok bol v poslednom roku jeden a spôsobil výpadok stránky školy na 2 dni,
- iné počítačové incidenty, ktoré majú za následok narušenie plynulého chodu školy a neoprávnené zneužitie citlivých a dôverných dát, rieši sa pravidelnou zálohou citlivých údajov na servery edupage.

Kvôli širokému dosahu kontextov, pre ktoré môžete použiť kybernetickú bezpečnosť, má kybernetická bezpečnosť tieto kategórie:

- Zabezpečenie siete, ktoré zahŕňa zabezpečenie vašich počítačov pred útočníkmi a škodlivým softvérom; rieši sa na škole len čiastočne vyblokovaním niektorých komunikačných portov na školskom servery,
- Zabezpečenie aplikácií, ktoré sa zameriava na ochranu softvéru a zariadení pred počítačovými hrozbami; je vyriešené školskou licenciou na antivírový programom od spoločnosti Eset zabezpečovanou ministerstvom školstva,
- Informačná bezpečnosť, ktorá zahŕňa ochranu integrity vašich údajov a súkromia počas ich ukladania alebo prenosu; tieto údaje sú zhromažďované jedine cez ASC agendu a ich

bezpečnosť je zaručená cez prístupové heslá k edupage, konkrétne bolo na klube vysvetlené ako a kde sú uložené prístupové heslá na zariadení s Windows, odstraňovanie profilov s uloženými heslami,

- Obnova po hardvérovom zlyhaní ,nehody v kybernetickom zabezpečení, ktoré vedú k strate údajov sa zatiaľ na škole nevyskytli;
- Vzdelávanie koncových používateľov, ktoré sa zameriava na to, ako jednotlivci chránia svoje zariadenia pred škodlivými útokmi sa rieši na škole len individuálnymi konzultáciami, spoločné školenie zatiaľ neuskutočnilo.

K bodu 2:

Problematika kyberšikanovania je na škole aktuálna a v určitej forme sa na škole objavilo v minulom mesiaci. Problém bol s odcudzením súkromného účtu v sociálnej sieti a následne k zneužitiu citlivých osobných fotiek. Príčina sa zistila v neuváženom používaní cudzích zariadení pri vytvorení a aktualizácii prihlasovacích údajov vlastného konta. Na takéto a podobné prejavy kyberšikany by mala škola reagovať zahrnutím do vyučovania aj oblasť prevencie proti kyberšikane formou pútavých aktivít so žiakmi. Príklady takýchto aktivít sa prediskutovali v ďalšej časti klubu. Najmä sa čerpalo s web stránok, ktoré sú uvedené v treťom a štvrtom bode v manažérskom zhrnutí.

Diskutovalo sa o vhodnosti jednotlivých príkladov pre potreby našej školy. Diskutujúci sa vyjadrili k použiteľnosti vo svojom predmete.

K bodu 3:

V poslednej časti klubu pracovali jeho členovia nad vlastných materiáloch k aktivitám podporujúcim prevenciu proti kyberšikane. Svoje otázky k tematike si hneď v diskusii objasnili s ostatnými členmi klubu.

13. **Závery a odporúčania:**

1. Z prediskutovávaných materiálov použiť čo najviac inšpiráciu pre vlastné aktivity so žiakmi v oblasti prevencie proti kybernetickým hrozbám a kyberšikane.
2. Zapracovať odporúčania z prediskutovávaných materiálov do školského poriadku. Pripraviť návrhy na ich zapracovanie do školského poriadku pre ďalší školský rok.
3. Pracovať so žiakmi a rodičmi na škole v oblasti prevencie proti kyberšikane podľa prediskutovaných odporúčaní uvedených na začiatku v manažérskom zhrnutí. Zamerať sa najmä na prácu so žiakmi, ktorí boli účastní na riešenej kyberšikane v šk.r. 2021/2022 v I. A..

14. Vypracoval (meno, priezvisko)	Ing. Stanislav Peniaško
15. Dátum	21.06.2022
16. Podpis	
17. Schválil (meno, priezvisko)	Mgr. Anna Dvorščáková
18. Dátum	21.06.2022
19. Podpis	