Plán hodiny

2023-1-SK01-KA220-SCH-00015112

Téma	**Bezpečnostní a digitální nástroje**	
Název bloku	**Kybernetičtí strážci: Zkoumání bezpečnosti prostřednictvím digitálních nástrojů**	
Věková kategorie 9–16	**Trvání (min)** 100 minut	**Počet vyučovacích hodin** 3

Vzdělávací cíle zaměřené na studenta (obsahové a výkonnostní standardy)

Hlavní cíl: Pochopení důležitosti kybernetické bezpečnosti. Studenti se seznámí s různými typy digitálních bezpečnostních hrozeb as tím, jak lze technologie využít k ochraně informací a údajů. 3D svět bude použit pro simulaci scénářů kybernetické bezpečnosti a studenti by měli být schopni je řešit, nejlépe prací v týmech, podporou týmové práce a inovativního řešení problémů.

Didaktické materiály a didaktické techniky

- Počítače s přístupem na internet nebo lokální síť, na které bude umístěno prostředí 3D světa.

Zdroje/reference (videa, metodiky)

Motivační fáze

Trvání (min): 10 minut

Cílem je vytvořit úvod do digitální bezpečnosti a přimět studenty zamyslet se nad důležitostí ochrany informací online. Toho lze dosáhnout aktivitou ve virtuálním světě, která připomíná bludiště.

Studenti dorazí do velkého bludiště, na jehož začátku bude označení „Kybernetické bludiště“. Uvnitř bludiště najdou různé překážky představující běžné bezpečnostní hrozby, jako jsou phishingové e-maily, malware nebo hackování hesel. Při každé překážce se setkají s výzvami, jako jsou hádanky a kvízy, které od nich budou vyžadovat, aby identifikovaly způsoby, jak se těmto digitálním hrozbám vyhnout nebo je zmírnit. Řešení těchto výzev umožní studentům najít východ z bludiště.

Průzkumná fáze

Trvání (min): 20 min

Cílem je povzbudit studenty, aby prozkoumali fungování nástrojů kybernetické bezpečnosti a prostřednictvím interaktivního učení se seznámili s klíčovými principy digitální bezpečnosti. Navrhovaná aktivita v této fázi má název „Vytvoření virtuálního bezpečnostního systému“. Studenti by měli pracovat v týmech na návrhu virtuálního bezpečnostního systému pro fiktivní společnost nebo organizaci, řešit potenciální bezpečnostní hrozby a navrhovat řešení.

Studenti prozkoumají různé typy kybernetických hrozeb, jako jsou viry, phishingové útoky a úniky údajů. Také prozkoumají základní bezpečnostní nástroje, jako jsou firewally, šifrování a vícefaktorové ověřování. Pomocí platformy virtuálního světa studenti vytvoří digitální reprezentaci zabezpečeného kancelářského prostředí nebo datového centra. Začlení prvky, jako je přístup chráněn heslem, šifrované datové trezory a firewally. Týmy budou simulovat potenciální narušení bezpečnosti ve svém virtuálním světě (např. hackeři se pokoušejí ukrást data) a demonstrují, jak jejich bezpečnostní systém chrání organizaci. Po dokončení návrhu každý tým prodiskutuje bezpečnostní funkce, které se rozhodly zahrnout, a jak řeší konkrétní hrozby.

Následují některé klíčové prvky, které by měly být zahrnuty v plánované aktivitě:

- Pochopení fungování virů, malwaru a jiných kybernetických hrozeb na technické úrovni.
- Aplikace bezpečnostních nástrojů, jako jsou šifrování, firewally a ochrana heslem.
- Návrh funkčního virtuálního bezpečnostního systému pro řešení problémů reálného světa.
- Výpočet šifrovacích klíčů, rychlosti přenosu dat nebo určení bezpečnosti hesla.
- Vytvoření poutavého a uživatelsky přívětivého rozhraní pro bezpečnostní systém.

Fáze fixace (konsolidace a prohloubení)

Trvání (min): 30 min

Navrhovaná aktivita má název „Výzva kybernetické bezpečnosti: Ochrana budoucnosti“

Cílem je, aby se studenti setkali s reálným problémem kybernetické bezpečnosti a aby měli za úkol navrhnout digitální řešení na ochranu fiktivní organizace nebo skupiny před kybernetickým útokem.

K dispozici budou tři alternativní scénáře:

Navrhněte bezpečnostní systém pro ochranu inteligentní domácnosti se zařízeními připojenými k internetu (IoT), jako jsou inteligentní reproduktory, kamery a spotřebiče. Řešení musí řešit hrozby, jako je neoprávněný přístup a úniky údajů.

Vypracovat plán kybernetické bezpečnosti pro školní síť se zaměřením na ochranu údajů studentů, předcházení hackerským útokům a zajištění bezpečné komunikace mezi učiteli, studenty a rodiči.

Vytvořte řešení kybernetické bezpečnosti pro zdravotnickou organizaci, která zpracovává citlivé údaje o pacientech. Systém by měl chránit před hackerskými útoky, neoprávněným přístupem a úniky údajů a zároveň zajišťovat soukromí.

Kroky pro studenty jsou následující:

- Studenti si vyberou scénář a identifikují konkrétní rizika kybernetické bezpečnosti (např. hackerské útoky, krádež údajů, ransomware).
- Týmy brainstormují řešení a zvažují, které nástroje kybernetické bezpečnosti (např. šifrování, firewally, autentifikační systémy) lze použít. Navrhnou prototyp na platformě virtuálního světa.
- Pomocí virtuálního světa budou studenti simulovat scénář kybernetického útoku (např. hacker se pokouší proniknout do systému). Týmy předvedou, jak jejich bezpečnostní řešení chrání organizaci před útokem.
- Týmy představí třídě svůj prototyp digitální bezpečnosti a vysvětlí, jak funguje a jak řeší hrozby, které představuje daný scénář. Zpětná vazba od učitele a kolegů jim může pomoci upřesnit jejich řešení.

Hodnocení studentů

- Účast ve virtuálním bludišti a hledání cesty z něj.
- Kreativita a funkčnost digitálního bezpečnostního systému navrženého ve virtuálním světě.
- Prezentace a schopnost vysvětlit, jak jejich bezpečnostní řešení řeší konkrétní hrozby pomocí digitálních nástrojů.

Přílohy:

Tento projekt byl realizován s podporou Evropské komise. Podpora Evropské komise na vypracování této publikace nepředstavuje schválení obsahu, který odráží pouze názory autorů, a Agentura ani Národní komise nenesou odpovědnost za žádné použití informací v ní obsažených.