CYBERSEC
EDUCHECK

LESSON 3 – Incidenty

Reakce na incidenty: Efektivní reakce na kybernetické incidenty

Spolufinancováno Evropskou unií

VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe

PARTNEŘI: KREATYWNI DLA BIZNESU STOWARZYSZENIE; EUROPEAN CENTRE FOR CAREER EDUCATION

LEKCE 3 – Incidenty

Plán výuky pro střední školy

Scénář vytvořený v rámci projektu „CyberSec EduCheck“ – projekt č. 2023-2-PL01-KA210-VET-000176822

Autoři scénáře: Weronika Kędzierska, Mateusz Pękala - Coventry University Wrocław

Věcná redaktorka: Pavla Vybíhalová - European Centre for Career Education

Grafická úprava: Karolína Kornecka-Kupiec, Jadwiga Maj - KREA Association

Wroclaw 2024

Spolufinancováno Evropskou unií

VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe

PARTNEŘI: KREA Stowarzyszenie Kreatywni dla Biznesu; European Centre for Career Education

Vážení,

představujeme vám plán lekce na téma digitální bezpečnostní incidenty, což je klíčový prvek při řízení rizik spojených s ochranou osobních údajů a IT systémů. Naše 45minutová lekce je navržena tak, aby studenty naučila, jak efektivně reagovat na bezpečnostní incidenty, včetně změny hesel, přezkoumání bezpečnostních opatření a hlášení porušení. Zaměříme se také na důležitost pravidelných záloh a nejlepší postupy pro jejich vytváření. Studenti se seznámí s nástroji jako Have I Been Pwned pro monitorování bezpečnosti dat a rozvinou analytické dovednosti a kritické myšlení, aby lépe hodnotili hrozby a účinně na ně reagovali v budoucnosti.

Během lekcí poskytujeme praktická cvičení a diskuze, které posílí získané znalosti. Jsme si vědomi, že 45 minut je omezený čas, proto doporučujeme rozdělit toto téma do několika hodin, pokud to bude potřeba, což studentům umožní podrobněji prozkoumat a lépe pochopit dané problémy.

Scénář a výukové materiály, včetně prezentace, lze přizpůsobit a modifikovat podle vašich potřeb a schopností skupiny.

S pozdravem,

Tým projektu CyberSec

Spolufinancováno Evropskou unií

VEDOUCÍ PROJEKTU:
Coventry University
Research Institute
Europe

PARTNEŘI:
KEA
STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

Obsah

Spolufinancováno Evropskou unií

VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe

PARTNEŘI: KREA Stowarzyszenie Kreatywni dla Biznesu; European Centre for Career Education

Cíle lekce

- **Explicitní cíle**
    - Reakce na incidenty: Studenti se naučí, jaké kroky podniknout při zjištění bezpečnostního narušení, jako je změna hesel a přezkoumání bezpečnosti.
    - Důležitost záloh: Studenti pochopí důležitost pravidelných záloh a jak je provádět.
    - Nástroje a služby: Studenti se naučí, jak používat nástroje, jako je https://haveibeenpwned.com/, k ověření, zda jejich data byla kompromitována.
    - Rozvoj analytických a kritických dovedností.
- **Skryté cíle:**
    - Posílení spolupráce ve skupině.
    - Podpora samostatného myšlení a řešení problémů.

Kontext - klíčová slova

bezpečnostní incidenty, reakce na incidenty, zálohy, bezpečnost dat, nástroje pro monitorování, kyberbezpečnost

- **Odůvodnění výběru tématu:**

V éře široce dostupných technologií a internetu roste riziko bezpečnostních incidentů, zejména když uživatelé nejsou obeznámeni s tím, jak správně reagovat na narušení bezpečnosti. Mladí lidé často využívají různé online služby, což zvyšuje šance na ztrátu soukromých údajů nebo hacknutí účtů.

Vědět, jak efektivně reagovat na takové incidenty, včetně změny hesel a přezkoumání bezpečnosti, je klíčové pro ochranu osobních údajů.

Pochopení důležitosti pravidelných záloh a vědění, jak používat nástroje pro monitorování, jako je Have I Been Pwned, pomáhá minimalizovat dopad bezpečnostních incidentů.

Vzdělávání v oblasti správy incidentů a rozvoj analytických a kritických dovedností v kontextu kyberbezpečnosti jsou důležité pro budování povědomí o hrozbách a odpovědný přístup k ochraně dat v digitálním světě.

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KEA STOWARZYSZENIE KREATYWNI DLA BIZNESU; EUROPEAN CENTRE FOR CAREER EDUCATION

LESSON 3 – Incidenty

Příprava na lekci

- **Materiály**:
  - Multimediální prezentace [Digitální bezpečnostní incidenty].
  - Pracovní listy s cvičeními.
  - Tabule (tradiční nebo interaktivní).
  - Počítače/tablety s připojením k internetu (pokud je potřeba).
- **Učebna**:
  - Místnost vybavená projektorem.
  - Uspořádání lavic tak, aby umožňovalo práci ve skupinách nebo individuálně.

Struktura lekce

Účel	Aktivita	Čas	Materiály
Úvod	Představení tématu. Učitel se ptá studentů: Co znamená slovo incident? Jaké příklady bezpečnostních incidentů znáte? Něco z vaší zkušenosti? Učitel prezentuje některé příklady bezpečnostních incidentů.	5 min	Prezentace, tabule
Mini kvíz – Kontrola zranitelnosti	Učitel se studenty klade 7 otázek „Ověřte svou zranitelnost vůči hackerským útokům“ Chce vás někdo napadnout? a) Ne, protože nemám žádná důležitá data, která by se dala prodat b) Ano, protože někdo může použít můj účet na sociálních médiích k podvádění ostatních c) Ano, protože někdo může zašifrovat má data a požadovat výkupné	10 min	Prezentace

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KEA STOWARZYSZENIE KREATYWNI DLA BIZNESU; EUROPEAN CENTRE FOR CAREER EDUCATION

	Používáte stejné heslo pro několik různých účtů? a) Ano, protože se lépe pamatují b) Ne, mám jedinečné heslo pro každý účet c) Používám jedno hlavní heslo a menší úpravy na dalších účtech Ověřujete zdroje odkazů, které obdržíte v e-mailech nebo zprávách? a) Ne vždy, obvykle kliknu, pokud odesílatel vypadá známý b) Vždy zkontroluji, zda je odkaz bezpečný, než na něj kliknu c) Pouze pokud zpráva vypadá podezřele Co děláte, když obdržíte podezřelý e-mail, který žádá o vaše údaje? a) Ignoruji ho nebo ho smažu b) Zkontroluji detaily odesílatele a odkazy, než se rozhodnu c) Otevřu, ale nezadávám žádné údaje Jaké kroky podnikáte k ochraně svých zařízení? a) Nepoužívám žádné další bezpečnostní funkce b) Mám nainstalovaný antivirový program a pravidelně jej aktualizuji c) Používám antivirový program, aktualizuji svůj software a používám správce hesel Myslíte si, že vaše osobní údaje jsou cenné pro ostatní? a) Ne, nikdo nebude mít zájem o mé údaje b) Ano, mohou být použity pro krádež identity nebo podvod c) Pouze mé bankovní údaje nebo hesla jsou cenné Co děláte, když zaznamenáte podezřelou aktivitu na svém účtu? a) Nic, možná je to chyba b) Okamžitě změním heslo a zkontroluji své další účty c) Čekám a sleduji, jestli se situace opakuje		

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KEA STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

	Většina odpovědí „a“: Máte co zlepšovat, hackeři mohou využít vaší slabé bezpečnosti. Zvýšte povědomí o hrozbách a zaveďte lepší návyky. **Většina odpovědí „b“:** Jste dobře připraveni a vědomi si rizik, ale vždy je dobré prohloubit své znalosti o online bezpečnosti. **Většina odpovědí „c“:** Máte základní znalosti, ale stále je prostor pro zlepšení. Pracujte na posílení bezpečnosti svých účtů a zařízení. - Učitel klade jednu nebo více otázek k povzbuzení diskuse: - Co činí naše online účty zranitelnými vůči útoku? - Jaké jsou nejběžnější problémy s online bezpečností, se kterými se můžeme setkat? - Jaké mohou být důsledky, pokud bude náš účet napaden nebo ukraden? - Co můžeme udělat, abychom se vyhnuli problémům s bezpečností na internetu? - Známé případy, kdy někdo měl problém s online bezpečností? - Jak často slyšíme o problémech s online bezpečností? Je to vzácné nebo běžné? - Co dělat, pokud nám někdo ukradne účet nebo přístup k němu? - Jaké jsou rozdíly mezi různými online bezpečnostními problémy, jako je krádež účtu a viry?		

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KEA STOWARZYSZENIE KREATYWNI DLA BIZNESU, EUROPEAN CENTRE FOR CAREER EDUCATION

	- Jaké aplikace nebo programy nám mohou pomoci chránit naše účty na internetu? - Které instituce nebo organizace jsou zodpovědné za ochranu našich údajů na internetu?		
Předání znalostí - Ransomware	Kdo je hacker? Očekávání vs. realita Cinematický obraz: Často si hackery představujeme jako osoby v kapucích, které dokážou prolomit každý počítačový systém. Superhrdinové: Vypadají velmi inteligentně a pracují ve tmě, aby získali tajné informace. Realita: Různé typy hackerů: Existují různé typy hackerů, včetně těch, kteří pomáhají zlepšit bezpečnost (nazýváni „bílé klobouky“) a těch, kteří dělají něco nelegálního (nazýváni „černé klobouky“). Dovednosti a nástroje: Hackeři používají speciální nástroje a techniky, ale jejich činy jsou často technické a ne tak dramatické jako ve filmech. Ne vždy pracují v tajnosti. Často používají sociální inženýrství. Sledování úniků Učitel prezentuje webovou stránku Have I Been Pwned https://haveibeenpwned.com/website Oblíbený nástroj pro kontrolu, zda vaše e-mailová adresa nebo heslo nebyly součástí úniků dat. Učitel povzbudí studenty, aby zkontrolovali, zda jejich e-maily nejsou v seznamu. Volitelně použít – Pracovní list č. 1. Co dělat v případě úniku hesla? Co dělat v případě úniku hesla?	10 min	Presentation, multimedia examples

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KEA Stowarzyszenie Kreatywni dla Biznesu, European Centre for Career Education

	Okamžitě změňte své heslo Čím dříve změníte heslo, tím menší je šance, že někdo využije váš účet. Jak: Přejděte na webovou stránku nebo do aplikace, přihlaste se, přejděte do nastavení a změňte své heslo na nové, silné heslo. Ověřte aktivní přihlášení Kontrola, kde jste přihlášeni, vám umožní odhlásit potenciálně nebezpečné relace. Jak: V nastavení účtu najděte sekci „Aktivní relace“ nebo „Zařízení“ a podívejte se, z jakých míst a zařízení jste přihlášeni. Odhlaste podezřelé relace. Změňte všechna podobná hesla Pokud používáte podobná hesla na jiných účtech, změňte je, abyste předešli kompromitaci dalších účtů, pokud někdo získá jedno z vašich hesel. Jak: Ujistěte se, že každý účet má jedinečné heslo, které není podobné žádnému jinému. Zadejte dvoufaktorovou autentifikaci (2FA) Dvoufaktorové přihlášení poskytuje další vrstvu bezpečnosti, i když někdo zná vaše heslo. Jak: Povolit 2FA v nastavení účtu výběrem možnosti přidat druhý faktor, např. SMS kód, autentifikační aplikaci (např. Google Authenticator) nebo dongle. Začněte používat správce hesel Správce hesel vám pomůže generovat a uchovávat silná, jedinečná hesla pro každý účet. Jak: Nainstalujte správce hesel (např. KeePassXC, LastPass) a přeneste do něj všechna svá hesla. Používejte ho k automatickému vyplňování hesel při přihlašování. **Prezentace klíčových informací o Ransomware.** Ochrana proti ransomware – nástroj ve Windows		

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KEA STOWARZYSZENIE KREATYWNI DLA BIZNESU; EUROPEAN CENTRE FOR CAREER EDUCATION

LESSON 3 – Incidenty

Praktická cvičení – zálohování dat	Pracujte individuálně nebo ve skupinách na kontrole, zda je antivirový program zapnutý. Ransomware – Vysvětlení, co to je a jak se chránit Je to typ malwaru, který zablokuje přístup k vašim souborům na počítači a požaduje výkupné, aby je odemkl. Vypadá to, jako by vás někdo zamknul v místnosti a požadoval peníze, aby vás pustil ven. Pravidelné zálohy: Uchovávejte důležité soubory na externím disku nebo v cloudu. Pokud váš počítač bude infikován, můžete své soubory obnovit ze zálohy. Aktualizace softwaru: Ujistěte se, že váš operační systém a všechny programy jsou vždy aktuální. Nové aktualizace často opravují bezpečnostní zranitelnosti. Antivirus: Nainstalujte a používejte antivirový program, který dokáže detekovat a blokovat hrozby. Bezpečné surfování: Neklikejte na podezřelé odkazy a nestahujte soubory z neznámých zdrojů. Vzdělávání: Naučte se rozpoznávat podezřelé e-maily a zprávy, které mohou obsahovat malware. Zkontrolujte v nastavení počítače, zda je povolena ochrana proti ransomware. Pravidlo 3-2-1 3 kopie vašich dat: Mějte alespoň tři kopie svých dat. Jedna kopie je originál a další jsou zálohy.	15 min	Počítače

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KEA STOWARZYSZENIE KREATYWNI DLA BIZNESU
EUROPEAN CENTRE FOR CAREER EDUCATION

	2 různé média: Uchovávejte tyto kopie na dvou různých typech médií. Například jednu kopii na počítači a druhou na externím pevném disku. 1 offline záloha: Mějte alespoň jednu zálohu, která není připojena k internetu, aby byla bezpečná i v případě, že váš počítač bude infikován virem. Příklad pro 13letého: Představte si, že máte důležité fotografie a projekty na svém počítači. Chcete se ujistit, že o tato data nepřijdete, i když se něco stane. Tady je, jak můžete aplikovat pravidlo 3-2-1: 3 kopie vašich dat: Udělejte tři kopie svých fotografií. Jedna kopie je ta na vašem počítači, druhá je na externím pevném disku (např. flash disk) a třetí můžete dát do cloudu (např. Google Drive). 2 různé média: Uchovávejte tyto kopie na různých médiích. Například jednu kopii na počítači, druhou na USB disku a třetí v cloudu. Flash disk a cloudový disk jsou různá média. 1 offline kopie: Uchovávejte flash disk (se druhou kopií) na bezpečném místě, které není trvale připojeno k internetu. To zabezpečí vaše data, i když váš počítač havaruje nebo bude napaden virem.		
Diskuze o výsledcích	Prezentace výsledků práce, diskuze, vysvětlení obtížnějších problémů.	10 min	Tabule, poznámky
Shrnutí a zamyšlení	Shrnutí klíčových problémů. Podnět k zamyšlení nad tématem.	5 min	Prezentace

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KEA Stowarzyszenie Kreatywni dla Biznesu
EUROPEAN CENTRE FOR CAREER EDUCATION

LESSON 3 – Incidenty

Pracovní list pro studenty 1 – Komentář pro učitele

Cíl: Pomoci studentům pochopit, jak reagovat na únik hesla a jaké kroky podniknout k minimalizaci jeho dopadu.

Doba trvání: 15-30 minut

Popis aktivity:

1. Úvod do situace: Studenti jsou informováni, že jejich heslo bylo uniknuto (může jít o fiktivní situaci, např. „Obdržíte e-mail, že váš účet byl hacknut“).

   Úvod do situace: Studenti jsou informováni, že jejich heslo bylo uniknuto (může jít o fiktivní situaci, např. „Obdržíte e-mail, že váš účet byl hacknut“).
   Otázka pro studenty: Co si myslíte, cítíte a děláte, když se dozvíte o úniku hesla? (Pracovní list č. 1)

   Příprava na vyprávění příběhu: V rámci skupiny studenti připraví příběh, který začíná „nešťastnou událostí“ – dozvědění se o úniku hesla. Měli by sdílet své myšlenky, emoce a kroky, které v této situaci podnikli. K dispozici mají tři otázky, které je povedou:

   Co si myslíte? – Jaké myšlenky vám přijdou na mysl, když zjistíte, že vaše heslo bylo ukradeno? Přemýšlíte o tom, co by se mohlo stát s vašimi daty?
   Co cítíte? – Jaké emoce v této chvíli prožíváte? Cítíte paniku, úzkost, hněv, možná stud? Jak na tuto situaci reagujete?
   Co děláte? – Jaké kroky podnikáte k nápravě situace? Měníte heslo, kontaktujete administrátora, kontrolujete svůj účet? Co konkrétně děláte pro zajištění svých dat?

   Události: Jaké mohou být důsledky této události? Co se může stát? (např. hacknutí e-mailu/oblíbené webové stránky, kde bylo stejné heslo).
2. Práce na příběhu: Studenti používají pracovní list jako základ pro vytvoření svého příběhu. Měli by vyzdvihnout klíčové události (např. zjištění o úniku hesla) a přemýšlet, jak přivést příběh k pozitivnímu závěru (tzv. šťastný konec).
3. Skupinová prezentace: Každá skupina představí svůj příběh, popisující emoce a kroky, které podnikly po úniku hesla.
   - Společná diskuse o aktivitách: Na základě představených příběhů učitel diskutuje o vhodných krocích, které je třeba podniknout po úniku hesla, např.:
     - Změna hesla na všech webech, kde bylo použito stejné heslo
     - Kontrola historie přihlášení (pokud je k dispozici)
     - Kontaktování administrátora webu nebo technické podpory
     - Používání správce hesel a povolení dvoufaktorové autentifikace
     - Monitorování účtu pro podezřelou aktivitu

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KEA Stowarzyszenie Kreatywni dla Biznesu
EUROPEAN CENTRE FOR CAREER EDUCATION

LESSON 3 – Incidenty

Pracovní list pro studenty 1

Událost	Co si myslím?	Co cítím?	Co to dělám?	Co dělat v případě úniku hesla?
OH NO				

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KREATYWNI DLA BIZNESU, EUROPEAN CENTRE FOR CAREER EDUCATION

Volitelný domácí úkol

- **Zkontrolujte své e-mailové adresy:**

Použijte službu Have I Been Pwned a zkontrolujte, zda vaše e-mailové adresy byly součástí úniků dat.

Vytvořte seznam e-mailových adres, které byly uniknuty.

- **Zůstaňte informováni o nových únicích:**

Použijte upozornění Have I Been Pwned na nové úniky. Zadejte své e-mailové adresy, abyste byli informováni o budoucích únicích souvisejících s těmito adresami.

- **Změňte hesla:**

Změňte hesla účtů, které byly součástí úniků. Používejte silná, náhodná hesla. Můžete použít správce hesel, jako je KeePassXC, pro generování a uchovávání nových hesel.

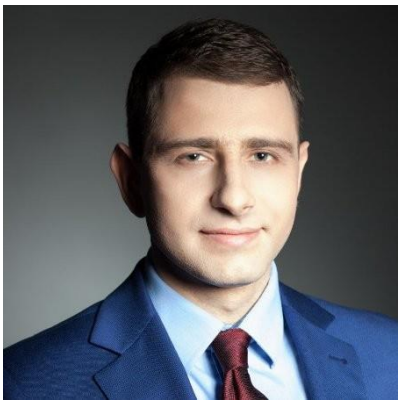
- **Vytvořte zálohy:**

Vyberte důležité soubory, jako jsou dokumenty, fotografie a další data, která chcete chránit před ztrátou. Použijte externí úložiště (např. externí disk) nebo cloud (např. Google Drive, OneDrive) pro zálohování těchto souborů. Ujistěte se, že přístup k vašim zálohám je chráněn silným heslem a pravidelně je aktualizujte.

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KEA Stowarzyszenie Kreatywni dla Biznesu
EUROPEAN CENTRE FOR CAREER EDUCATION

Autoři a odborníci

Weronika Kędzierska – expertka v oblasti měkkých aspektů kyberbezpečnosti, zaměřující se na vytváření bezpečné základny kyberbezpečnosti pro mladé organizace. Specializuje se na rozvoj efektivních týmů, organizační změny a implementaci inovačních strategií. Jako nezávislá konzultantka a koučka pomáhá lídrům a týmům budovat zapojení a spolupráci. Je oceňována za kreativní a hodnotné workshopy, které efektivně inspirují týmy k dosahování jejich cílů.



Mateusz Pękala – specialista na zvyšování povědomí o bezpečnosti informací, security compliance, audity informační bezpečnosti a řízení rizik. Má dlouholeté zkušenosti jako auditor, školitel a konzultant v oblasti informační bezpečnosti. Je členem profesionálních organizací, jako jsou ISSA Poland a ISACA. Vlastní certifikace Certified in Risk and Information Systems Control™ (CRISC), Certified Information Security Professional (CISSP), Certified Data Privacy Solutions Engineer™ (CDPSE)® a Certified Information Systems Auditor® (CISA), a je také certifikovaným auditorem v oblasti ISO 27001.

Spolufinancováno Evropskou unií
VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe
PARTNEŘI: KERA Stowarzyszenie Kreatywni dla Biznesu; European Centre for Career Education

Více informací o projektu

Financováno Evropskou unií. Vyjádřené názory a názory jsou však výhradně názory autora (autorů) a nemusí nutně odrážet názory Evropské unie nebo Evropské výkonné agentury pro vzdělávání a kulturu (EACEA). Evropská unie ani EACEA za ně nemohou nést odpovědnost.

PROJEKT Č. 2023-2-PL01-KA210-VET-000176822

- https://www.coventry.ac.uk/wroclaw/
- https://kreatywnidlabiznesu.pl/cyber-sec-edu-check/
- https://eccedu.net/

CYBERSEC
EDUCHECK

Spolufinancováno Evropskou unií

VEDOUCÍ PROJEKTU: Coventry University Research Institute Europe

PARTNEŘI: KREA Stowarzyszenie Kreatywni dla Biznesu; European Centre for Career Education