Podręcznik dla kształcenia i szkolenia zawodowego

Maj 31st, 2024

Co-funded by the European Union

GOOD START

Good Digital Hygiene for Startups

Project No: 2022-1-LV01-KA220-VET-000086725 | Project title: Good Digital Hygiene for Startups

Spis Treści

Moduł 1 - Higiena Cyfrowa dla Profesjonalistów VET

Rozdział 1 - Znaczenie Higieny Cyfrowej w Edukacji VET

Higiena Cyfrowa i Cyberbezpieczeństwo

Higiena cyfrowa odnosi się do praktyk i nawyków, które jednostki stosują, aby utrzymać swoją prywatność online, bezpieczeństwo i ogólne dobre samopoczucie. Obejmuje szeroki zakres proaktywnych zachowań i działań mających na celu ochronę informacji osobistych, zapobieganie zagrożeniom online i minimalizowanie ryzyka związanego z aktywnościami cyfrowymi. Przykłady praktyk higieny cyfrowej obejmują używanie silnych haseł, włączanie dwuskładnikowego uwierzytelniania, regularne aktualizowanie oprogramowania, ostrożność w udostępnianiu informacji osobistych online i zarządzanie swoim śladem cyfrowym. Higiena cyfrowa to pojęcie ściśle związane z innym pojęciem, mianowicie cyberbezpieczeństwem. Często higiena cyfrowa jest uważana za proaktywny element cyberbezpieczeństwa, za który odpowiedzialna jest jednostka.

Cyberbezpieczeństwo to specjalistyczna dziedzina zajmująca się ochroną systemów komputerowych, sieci i danych przed nieautoryzowanym dostępem, cyberatakami i innymi naruszeniami bezpieczeństwa. Obejmuje wdrażanie środków technicznych, protokołów bezpieczeństwa i strategii obronnych w celu ochrony zasobów cyfrowych i minimalizowania potencjalnych ryzyk związanych z różnymi zagrożeniami cybernetycznymi. Osoby odpowiedzialne za cyberbezpieczeństwo często pracują nad identyfikacją luk w systemach, opracowywaniem rozwiązań bezpieczeństwa, monitorowaniem podejrzanych działań i reagowaniem na incydenty związane z bezpieczeństwem w celu zapewnienia integralności, poufności i dostępności informacji oraz zasobów. W konsekwencji działania związane z cyberbezpieczeństwem są często wykonywane przez profesjonalistów, w przeciwieństwie do higieny cyfrowej, która może być odpowiedzialnością każdego.

Higiena Cyfrowa w Organizacjach VET

Różne organizacje oczekują od swoich pracowników przestrzegania pewnych ogólnych zasad, aby zapewnić, że zasady i najlepsze praktyki higieny cyfrowej są przestrzegane. Organizacje kształcenia i szkolenia zawodowego (VET) mają pewne ogólne wytyczne, które są ważne dla wszystkich organizacji pracujących z ludźmi i ich danymi osobowymi oraz z usługami i produktami, które są opracowywane, przechowywane i udostępniane w środowisku cyfrowym. Jednak mają one pewne specyficzne

wyzwania związane z rodzajem świadczonych usług, jak również unikalnym charakterem ich docelowych klientów. Edukatorzy często znajdują się w sytuacji, w której muszą udzielać dodatkowych wskazówek swoim klientom. Może to oznaczać, że muszą być agentami higieny cyfrowej podczas prowadzenia szkoleń, np. świadcząc zamierzone usługi.

Istnieje kilka powodów, dla których higiena cyfrowa jest uważana za bardzo ważną, szczególnie dla organizacji VET:

- **Ochrona wrażliwych informacji**

Podczas wykonywania swojej pracy organizacje VET często mają do czynienia z dużą ilością wrażliwych informacji, w tym zapisami studenckimi, danymi akademickimi i finansowymi. Niektóre z tych informacji mogą być kluczowe dla organizacji podczas wykonywania analiz edukacyjnych lub oceny świadczonych usług. Praktykowanie dobrej higieny cyfrowej pomaga chronić te informacje przed nieautoryzowanym dostępem, naruszeniami danych i zagrożeniami cybernetycznymi, zapewniając poufność i integralność wrażliwych danych.

- **Ochrona reputacji instytucji**

Niewłaściwe zarządzanie danymi powierzonymi organizacji VET może nieumyślnie zmienić sposób, w jaki postrzegają ją jej klienci i partnerzy. Naruszenie danych lub incydent bezpieczeństwa może znacząco zaszkodzić reputacji organizacji VET. Priorytetowe traktowanie praktyk higieny cyfrowej pokazuje instytucji zaangażowanie w bezpieczeństwo, wiarygodność i profesjonalizm, co wzmacnia jej reputację wśród interesariuszy, w tym studentów, rodziców, pracodawców i organów regulacyjnych.

- **Zgodność z przepisami**

W zależności od charakteru swojej pracy i sposobu komunikacji z klientami, organizacje VET podlegają różnym regulacjom i wymogom zgodności związanym z ochroną danych, prywatnością i cyberbezpieczeństwem. Przestrzeganie najlepszych praktyk higieny cyfrowej pomaga zapewnić zgodność z obowiązującymi przepisami prawa, minimalizując ryzyko grzywien, kar i odpowiedzialności prawnej związanej z niezgodnością.

- **Wsparcie dla nauki i nauczania**

Technologie cyfrowe odgrywają kluczową rolę we współczesnej edukacji, ułatwiając naukę online, projekty zespołowe i oceny cyfrowe. Technologie te są wykorzystywane do opracowywania, zarządzania i udostępniania materiałów szkoleniowych, organizowania środowisk szkoleniowych, zarządzania zaangażowaniem uczestników lub analizy danych zebranych podczas procesu szkoleniowego. Utrzymując bezpieczną i niezawodną infrastrukturę cyfrową, organizacje VET mogą

zapewnić bezproblemowe doświadczenia edukacyjne dla studentów i nauczycieli, wspierając innowacyjność, kreatywność i zaangażowanie w procesie nauczania.

- **Minimalizacja ryzyka cyberbezpieczeństwa**

Sektor edukacji może być celem cyberprzestępców, którzy chcą wykorzystać luki w systemach cyfrowych i sieciach lub brak wiedzy i umiejętności studentów i trenerów, którzy nie są przyzwyczajeni do uczestnictwa w szkoleniach w środowisku cyfrowym. Wdrażanie środków higieny cyfrowej pomaga minimalizować ryzyka związane z cyberbezpieczeństwem, w tym infekcje złośliwym oprogramowaniem, ataki phishingowe, zagrożenia związane z ransomware i nieautoryzowany dostęp do zasobów edukacyjnych, chroniąc tym samym ciągłość usług i operacji edukacyjnych.

- **Promocja odpowiedzialnego obywatelstwa cyfrowego**

Dla niektórych uczestników procesu może to być pierwsza okazja do uczestnictwa w szkoleniu prowadzonym w środowisku cyfrowym lub korzystania ze środowiska cyfrowego do tworzenia, zarządzania i udostępniania materiałów szkoleniowych, prowadzenia dzielenia się wiedzą i komunikacji z innymi uczestnikami za pomocą środków cyfrowych lub korzystania z narzędzi cyfrowych do wykonywania zadań administracyjnych podczas szkolenia. Organizacje VET mają obowiązek edukować swoich studentów i pracowników zaangażowanych w szkolenia na temat bezpiecznych i odpowiedzialnych praktyk cyfrowych. Integrując edukację higieny cyfrowej z programem nauczania i szkoleniami, instytucje dają uczniom wiedzę, umiejętności i postawy niezbędne do skutecznego poruszania się w świecie cyfrowym, ochrony tożsamości online i pozytywnego wkładu w społeczeństwo cyfrowe.

- **Przygotowanie do przyszłej kariery**

W dzisiejszym cyfrowym świecie umiejętność posługiwania się technologiami cyfrowymi i świadomość cyberbezpieczeństwa są niezbędnymi umiejętnościami dla osób wchodzących na rynek pracy. Podczas gdy nauka niektórych umiejętności związanych z higieną cyfrową może nie być głównym celem studenta, udział w szkoleniu może dać im możliwości poprawy tych umiejętności, które mogą okazać się przydatne w przyszłości. Trenerzy i organizatorzy szkoleń powinni również być świadomi, że może istnieć potrzeba przeznaczenia czasu i zasobów na ten konkretny cel. Promując praktyki higieny cyfrowej, organizacje VET wyposażą studentów w podstawową wiedzę i umiejętności potrzebne do poruszania się w cyfrowych wyzwaniach w ich przyszłych karierach, niezależnie od tego, czy będą one tradycyjne, czy cyfrowe. To samo dotyczy również trenerów, którzy uczestnicząc w szkoleniu, korzystając z cyfrowych środowisk i narzędzi bezpiecznie i odpowiedzialnie, utrzymują swoje praktyki dydaktyczne na nowoczesnym poziomie i mogą napotkać nowe możliwości rozwoju kariery.

W ogólnym ujęciu higiena cyfrowa jest ważna dla organizacji VET zarówno na poziomie firmowym, jak i na poziomie indywidualnych pracowników i ich klientów, aby chronić wrażliwe informacje, zachować reputację instytucji, przestrzegać przepisów, wspierać naukę i nauczanie, minimalizować ryzyka cyberbezpieczeństwa, promować odpowiedzialne obywatelstwo cyfrowe i przygotować studentów, a także do pewnego stopnia także trenerów i innych pracowników, do sukcesu w cyfrowym świecie. Priorytetowe traktowanie higieny cyfrowej pozwala organizacjom VET na tworzenie bezpiecznego, bezpiecznego i sprzyjającego środowiska edukacyjnego, które umożliwia uczniom odniesienie sukcesu w erze cyfrowej.

Rozdział 2 - Umiejętności i wymagania dla trenerów i edukatorów VET

Role i odpowiedzialności w organizacjach VET

Najpierw zacznijmy od tego, jakie role mogą być zaangażowane w szkolenia VET, które powinny być świadome kwestii higieny cyfrowej i powinny posiadać odpowiednie umiejętności. W zależności od sytuacji podczas prowadzenia i uczestnictwa w szkoleniu, które jest przeprowadzane w środowiskach cyfrowych i z wykorzystaniem narzędzi cyfrowych, trenerzy i edukatorzy VET mogą napotkać różne podziały indywidualnych zadań wykonywanych przez uczestników procesu. Dlatego wdrażanie i zarządzanie higieną cyfrową w organizacji kształcenia i szkolenia zawodowego (VET) może wymagać koordynacji i współpracy różnych interesariuszy z różnymi rolami i odpowiedzialnościami. Trenerzy mogą mieć luksus wsparcia pełnoetatowego personelu IT, który zajmuje się technicznymi aspektami szkolenia, lub mogą musieć polegać na swoich umiejętnościach i wiedzy. Z tego powodu umiejętności i wymagania dla trenerów i edukatorów VET mogą się różnić w zależności od organizacji, do której należą.

Istnieje kilka typowych ról i odpowiedzialności dla osób, które mogą być zaangażowane w proces lub szkolenie w dzisiejszym środowisku cyfrowym, każda z własnymi zadaniami i wymaganiami umiejętności:

- **Dyrektor ds. Informatyki (CIO) lub Dyrektor ds. Technologii (CTO)**

CIO lub CTO głównie zajmuje się opracowywaniem i nadzorowaniem strategii, polityk i procedur higieny cyfrowej w organizacji. Uczestniczą w wyznaczaniu celów dla organizacji z uwzględnieniem higieny cyfrowej i cyberbezpieczeństwa. Ich obowiązki obejmują zapewnienie zgodności działań związanych z higieną cyfrową z ogólnymi celami IT i bezpieczeństwa organizacji, przydzielanie zasobów i budżetu na inicjatywy higieny cyfrowej i środki cyberbezpieczeństwa oraz zapewnianie przywództwa i wsparcia zespołom IT i bezpieczeństwa odpowiedzialnym za wdrażanie praktyk higieny cyfrowej.

- **Menedżer ds. Bezpieczeństwa IT lub Oficer ds. Cyberbezpieczeństwa**

Niektóre organizacje mogą mieć dedykowane stanowisko menedżera ds. bezpieczeństwa IT lub oficera ds. cyberbezpieczeństwa lub kogoś, kto pełni tę rolę jako część swoich obowiązków służbowych. Taka rola projektuje i wdraża środki kontroli cyberbezpieczeństwa, zabezpieczenia i zarządzanie ryzykiem w celu ochrony systemów, sieci i danych VET. Prowadzi również regularne oceny bezpieczeństwa, audyty i skanowanie podatności w celu identyfikacji i łagodzenia potencjalnych zagrożeń i podatności, monitoruje incydenty bezpieczeństwa, reaguje na incydenty cyberbezpieczeństwa i koordynuje działania reagowania na incydenty. Czasami ta rola rozwija i prowadzi szkolenia z zakresu cyberbezpieczeństwa i świadomości dla personelu, co sprawia, że pełni rolę trenera VET. Czasami mogą również zostać zaproszeni do szkolenia studentów w celu promowania dobrych praktyk higieny cyfrowej poza swoją organizacją jako eksperci.

- **Administrator IT lub Administrator Systemów**

Administratorzy IT są odpowiedzialni za zarządzanie infrastrukturą IT w organizacji i mogą wykonywać pewne zadania dla trenerów VET czasami w tle, nie będąc zauważonymi. Ich obowiązki obejmują utrzymanie i administrowanie systemami VET, serwerami i infrastrukturą sieciową zgodnie ze standardami i najlepszymi praktykami higieny cyfrowej; zarządzanie kontami użytkowników, kontrolami dostępu i uprawnieniami w celu zapewnienia bezpiecznego dostępu do zasobów i danych VET; instalowanie, konfigurowanie i aktualizowanie oprogramowania zabezpieczającego, łatki i firmware w celu ochrony przed znanymi podatnościami i eksploatacjami, które mogą być napotkane podczas korzystania z narzędzi cyfrowych i wykonywania działań podczas szkolenia, takich jak udostępnianie materiałów szkoleniowych lub komunikacja między uczestnikami. Są również odpowiedzialni za monitorowanie dzienników systemowych i alertów w poszukiwaniu podejrzanych działań, prób nieautoryzowanego dostępu lub naruszeń bezpieczeństwa.

- **Inspektor Ochrony Danych (DPO) lub Oficer ds. Prywatności**

Inspektorzy ochrony danych odgrywają ważną rolę w VET, ponieważ istnieją przepisy i regulacje na poziomie krajowym i międzynarodowym, które wymagają starannego zarządzania wrażliwymi danymi

uczestników szkolenia. Ta rola zapewnia zgodność z przepisami dotyczącymi ochrony danych i przepisami dotyczącymi prywatności regulującymi gromadzenie, wykorzystywanie i przechowywanie danych osobowych w środowiskach VET; opracowuje i utrzymuje polityki, procedury i dokumentację ochrony danych, w tym oceny wpływu na ochronę danych (DPIA) i powiadomienia o prywatności; zajmuje się żądaniami dostępu do danych, skargami dotyczącymi prywatności i zapytaniami związanymi z praktykami ochrony danych i prywatności, współpracuje z zespołami IT i prawnymi w celu rozwiązywania incydentów bezpieczeństwa danych, naruszeń danych i naruszeń prywatności.

- **Technolog edukacyjny lub projektant instruktażowy**

Podczas gdy poprzednie role mogą być spotykane w każdej organizacji, technolog edukacyjny lub projektant instruktażowy jest bezpośrednio związany ze szkoleniem i edukacją prowadzoną przez organizację. Ich obowiązki obejmują integrację zasad i praktyk higieny cyfrowej z programem nauczania VET, materiałami dydaktycznymi i działaniami edukacyjnymi; zapewnianie szkoleń i wsparcia dla edukatorów i personelu instruktażowego dotyczących włączania edukacji higieny cyfrowej do praktyk dydaktycznych, ocena i rekomendacja narzędzi i zasobów technologii edukacyjnej, które priorytetowo traktują bezpieczeństwo, prywatność i dostępność dla uczniów VET.

- **Użytkownicy końcowi (personel i studenci)**

Ostatnia rola jest często dzielona na dwie grupy, ale obie mają podobne odpowiedzialności w zakresie higieny cyfrowej. Koń Users (personel i studenci) są oczekiwani do przestrzegania polityk, wytycznych i najlepszych praktyk higieny cyfrowej podczas korzystania z systemów, urządzeń i zasobów online VET. Personel szkoleniowy organizacji może być zobowiązany przez firmę do wykonywania działań szkoleniowych lub administracyjnych w określony sposób, określony przez zasady i politykę organizacji. W związku z tym mogą być zobowiązani do uczestnictwa w szkoleniach z zakresu świadomości cyberbezpieczeństwa i inicjatywach edukacyjnych, aby zwiększyć swoje zrozumienie ryzyk cyfrowych i odpowiedzialności oraz zgłaszania incydentów bezpieczeństwa, podejrzanych działań i obaw związanych z cyberbezpieczeństwem odpowiedniemu personelowi IT lub bezpieczeństwa w celu zbadania i rozwiązania. Jednakże trenerzy VET powinni być świadomi swojej roli jako doradców dla uczniów, którzy mogą potrzebować wskazówek przy korzystaniu z środowiska cyfrowego, które może być im obce podczas szkolenia.

Indywidualna osoba w organizacji VET może pełnić kilka ról jednocześnie podczas szkolenia lub może skupić się tylko na kilku odpowiedzialnościach. Niezależnie od tego, definiując jasne role i odpowiedzialności dla osób zaangażowanych we wdrażanie i zarządzanie higieną cyfrową w organizacji VET, instytucje mogą skutecznie współpracować w celu ustanowienia kultury świadomości

cyberbezpieczeństwa, promowania dobrych praktyk higieny cyfrowej i ochrony poufności, integralności i dostępności zasobów i danych VET. Jednakże organizacje będą wymagać od tych osób posiadania określonych umiejętności i wiedzy do wykonywania wyżej wymienionych praktyk.

Ramowe umiejętności cyfrowe

Istnieją istniejące ramy kompetencji ustanowione do opisania zestawu umiejętności, które powinny być posiadane przez osoby zaangażowane w wykonywanie różnych działań w środowisku cyfrowym. Niektóre z nich obejmują ogólne umiejętności cyfrowe, podczas gdy niektóre mogą być bardziej specyficzne dla kwestii związanych z cyberbezpieczeństwem i higieną cyfrową. Następujące ramy są pomocne przy identyfikacji umiejętności higieny cyfrowej dla trenerów i edukatorów VET, a także przy identyfikacji możliwych potrzeb szkoleniowych dla studentów uczestniczących w edukacji w środowisku cyfrowym.

- **Ramowe kompetencje cyfrowe dla obywateli (DigComp) [1]**

Ramy DigComp 2.2, opracowane przez Komisję Europejską, są najnowszą wersją Ram Kompetencji Cyfrowych dla Obywateli. Określają kluczowe elementy kompetencji cyfrowych w pięciu obszarach: umiejętność posługiwania się informacją i danymi, komunikacja i współpraca, tworzenie treści cyfrowych, bezpieczeństwo i rozwiązywanie problemów. Każdy obszar jest dalej podzielony na konkretne kompetencje, które opisują umiejętności i wiedzę potrzebną do biegłości w środowiskach cyfrowych.

Te ramy służą jako przewodnik dla osób indywidualnych do oceny i poprawy swoich umiejętności cyfrowych oraz dla edukatorów i decydentów politycznych do projektowania programów nauczania i polityk wspierających edukację i szkolenia cyfrowe. DigComp 2.2 wprowadza również poziomy biegłości i przykłady zastosowań, co czyni je praktycznymi dla różnych kontekstów edukacyjnych i zawodowych. Ramy podkreślają znaczenie zdolności do efektywnego i krytycznego funkcjonowania w społeczeństwie cyfrowym.

- **Europejskie Ramowe Kompetencje e-Umiejętności (E-CF) [2]**

Europejskie Ramowe Kompetencje e-Umiejętności (e-CF) to znormalizowane ramy opisujące kompetencje, umiejętności i poziomy biegłości zawodowców z zakresu technologii informacyjnych i komunikacyjnych (ICT) opracowane w celu wspierania wzrostu i mobilności zawodowców ICT. Ramy składają się z pięciu obszarów kompetencji związanych z ICT, takich jak Planowanie, Budowanie,

Uruchamianie, Wspieranie i Zarządzanie. Zawierają 41 kompetencji i obejmują poziomy biegłości opisujące wiedzę, umiejętności i autonomię na każdym poziomie, od podstawowego do eksperta. Zawierają również przykłady wiedzy i umiejętności związanych z kompetencjami.

E-CF jest skierowane do pomocy organizacjom, menedżerom HR, trenerom i edukatorom w rozwoju ról zawodowych i ścieżek kariery dla zawodowców ICT, zwiększeniu zarządzania zasobami ludzkimi i wspieraniu rozwoju zawodowego w sektorze ICT. Służy również jako narzędzie do tworzenia polityk, edukacji i dostosowywania szkoleń w europejskim rynku cyfrowym.

- **Europejskie Ramowe Kompetencje Cyberbezpieczeństwa (ECSF) [3]**

Europejskie Ramowe Kompetencje Cyberbezpieczeństwa (ECSF) są zaprojektowane do harmonizacji i standaryzacji umiejętności, ról i kompetencji z zakresu cyberbezpieczeństwa w całej Europie. Służą jako struktura podstawowa do rozwijania i oceny umiejętności z zakresu cyberbezpieczeństwa, mająca na celu wypełnienie luk w umiejętnościach cyberbezpieczeństwa i poprawę postawy organizacji i narodów wobec cyberbezpieczeństwa. ECSF kategoryzuje umiejętności cyberbezpieczeństwa na kilka obszarów, szczegółowo opisując konkretne role i kompetencje wymagane w dziedzinie cyberbezpieczeństwa. Określa główne role cyberbezpieczeństwa, które są zazwyczaj potrzebne przez organizacje, specyficzne umiejętności i zdolności potrzebne do efektywnego wykonywania tych ról, oraz poziomy biegłości lub poziomy ekspertyzy, od początkującego do eksperta, wymagane dla każdej kompetencji.

Te ramy są użyteczne dla różnych interesariuszy, w tym instytucji edukacyjnych, firm i decydentów politycznych, do opracowywania programów nauczania, programów szkoleniowych i ścieżek kariery w dziedzinie cyberbezpieczeństwa. Wspierają tworzenie klarownych struktur kariery w dziedzinie cyberbezpieczeństwa, ułatwiając identyfikację braków w umiejętnościach i skuteczne ich zapełnianie.

- **Ramowe Kompetencje Cyfrowe dla Edukatorów (DigCompEdu) [4]**

Ramy DigCompEdu opisują wymagania dotyczące rozwoju kompetencji cyfrowych edukatorów. Są specjalnie dostosowane do nauczycieli na wszystkich poziomach edukacji, od wczesnego dzieciństwa po edukację wyższą i dorosłych, i skupiają się na doskonaleniu umiejętności cyfrowych niezbędnych do efektywnego nauczania w coraz bardziej cyfrowych środowiskach nauczania. Ramy są zbudowane wokół sześciu obszarów kompetencji: zaangażowanie zawodowe (korzystanie z technologii cyfrowych do komunikacji, współpracy i rozwoju zawodowego), zasoby cyfrowe (tworzenie i modyfikowanie zasobów cyfrowych oraz efektywne nimi zarządzanie), nauczanie i uczenie się (wykorzystanie

technologii cyfrowych do przygotowywania, realizacji i zarządzania procesem nauczania i uczenia się), ocena (wykorzystanie technologii cyfrowych do oceny, uczenia się i jako narzędzie do nauki), wspieranie uczniów (korzystanie z narzędzi cyfrowych w celu zwiększenia włączenia, personalizacji i aktywnego zaangażowania uczniów), wspieranie kompetencji cyfrowych uczniów (strategiczne promowanie umiejętności cyfrowych uczniów oraz bezpieczne i odpowiedzialne korzystanie z narzędzi cyfrowych). Dodatkowo, ramy DigCompEdu identyfikują 22 indywidualne kompetencje i poziomy biegłości, które sięgają od "Nowicjusza" do "Pioniera", zapewniając ścieżkę rozwoju edukatorów w ich praktykach cyfrowych.

Te ramy służą jako przewodnik dla edukatorów do oceny i poprawy ich kompetencji cyfrowych oraz wspierają instytucje edukacyjne w projektowaniu programów szkoleniowych i polityk zgodnych z współczesnymi potrzebami edukacyjnymi.

Ramy wspomniane powyżej, chociaż ogólne w odniesieniu do identyfikacji wymagań dla osób i organizacji uczestniczących w jakiejkolwiek praktyce w środowisku cyfrowym, zapewniają ustrukturyzowany widok zakresu umiejętności wymaganych od trenerów i edukatorów VET.

Umiejętności dla trenerów i edukatorów VET

Do pewnego stopnia, trenerzy i edukatorzy VET nie różnią się od innych uczestników środowiska cyfrowego. Z tego powodu umiejętności, których potrzebują do przestrzegania dobrych praktyk higieny cyfrowej, to umiejętności, które powinny być posiadane przez każdego. Te umiejętności obejmują szeroki zakres umiejętności technicznych, behawioralnych i poznawczych. Są również podzbiorem umiejętności, które można określić jako nowoczesne lub przyszłościowe i w oparciu o ostatni rozwój środowiska cyfrowego, są to te same umiejętności, które zostały podkreślone jako kluczowe dla organizacji lub bliskiej przyszłości, takie jak korzystanie z technologii chmurowych, analiza big data i korzystanie z narzędzi sztucznej inteligencji w celu poprawy produktywności i efektywności pracy.

Jednakże, natura ich pracy wymaga, aby trenerzy i edukatorzy VET zwracali większą uwagę na to, jak zarządzają danymi i wchodzą w interakcje z innymi uczestnikami procesu szkoleniowego. Oto niektóre ważne umiejętności potrzebne dla trenerów i edukatorów VET w odniesieniu do dobrej higieny cyfrowej:

- **Ogólna świadomość cyberbezpieczeństwa**

Umiejętność obejmuje zrozumienie powszechnych zagrożeń online, takich jak malware, phishing i ataki inżynierii społecznej, oraz wiedzę, jak je rozpoznawać i na nie reagować; wiedzę, jak bezpiecznie przeglądać internet, w tym unikanie podejrzanych stron, korzystanie z bezpiecznych połączeń (HTTPS) i ostrożność przy pobieraniu plików lub klikaniu na linki.

- **Ochrona danych i prywatności**

Umiejętność obejmuje umiejętność szyfrowania wrażliwych danych, zarówno w transporcie, jak i w spoczynku, oraz wiedzę, jak bezpiecznie usuwać lub likwidować dane, gdy jest to konieczne; oraz zrozumienie, jak konfigurować ustawienia prywatności na różnych platformach i urządzeniach online w celu kontrolowania udostępniania informacji osobistych.

- **Bezpieczeństwo i zarządzanie urządzeniami**

Ta umiejętność obejmuje praktykę regularnego aktualizowania oprogramowania, systemów operacyjnych i aplikacji w celu łatwego usuwania luk bezpieczeństwa i ochrony przed znanymi eksploatacjami; umiejętność tworzenia silnych, unikalnych haseł dla różnych kont i efektywnego korzystania z narzędzi zarządzania hasłami w celu bezpiecznego przechowywania i zarządzania hasłami; praktykę włączania i zarządzania wieloskładnikowym uwierzytelnianiem tam, gdzie jest to dostępne, w celu dodania dodatkowej warstwy bezpieczeństwa do kont online.

- **Bezpieczna komunikacja cyfrowa**

Ta umiejętność obejmuje praktykowanie bezpiecznych praktyk komunikacyjnych, takich jak korzystanie z zaszyfrowanych usług e-mail lub wybieranie i korzystanie z bezpiecznych aplikacji do przesyłania wiadomości podczas udostępniania poufnych informacji lub komunikowania się ze studentami, kolegami lub partnerami spoza organizacji VET; przestrzeganie wytycznych dotyczących identyfikacji i unikania phishingowych e-maili, oszustw i innych taktyk inżynierii społecznej, które mogłyby narazić systemy VET na zagrożenia lub prowadzić do naruszeń danych.

- **Zarządzanie śladem cyfrowym**

Ta umiejętność obejmuje zrozumienie implikacji własnego śladu cyfrowego i podejmowanie kroków w celu minimalizacji ekspozycji informacji osobistych online; doradzanie uczestnikom szkolenia, aby robili to samo.

- **Krytyczne myślenie**

Ta umiejętność obejmuje rozwijanie i stosowanie umiejętności krytycznego myślenia w celu oceny wiarygodności źródeł online, identyfikacji dezinformacji i oszustw oraz podejmowania świadomych decyzji dotyczących aktywności online podczas prowadzenia lub przygotowywania szkolenia.

- **Ciągłe uczenie się**

Ta umiejętność obejmuje uczestnictwo w ogólnej praktyce doskonalenia swoich umiejętności; naukę nowych narzędzi i podejść do szkolenia w środowisku cyfrowym lub korzystania z nowoczesnych narzędzi cyfrowych; oraz pozostawanie na bieżąco z ewoluującymi zagrożeniami cyberbezpieczeństwa, kwestiami prywatności i najlepszymi praktykami poprzez kontynuację edukacji i szkoleń.

- **Obywatelstwo cyfrowe i etyka**

Ta umiejętność obejmuje praktykowanie odpowiedzialnego obywatelstwa cyfrowego podczas prowadzenia szkoleń VET poprzez przestrzeganie przepisów i szacunek dla praw innych osób i organizacji; promowanie odpowiedzialnego obywatelstwa cyfrowego wśród studentów poprzez nauczanie etycznego zachowania, szacunek komunikacji i etykiety cyfrowej w środowiskach online; wspieranie umiejętności analitycznego myślenia, aby pomóc uczniom ocenić wiarygodność informacji online, rozpoznać zagrożenia cyfrowe i podejmować świadome decyzje dotyczące ich aktywności online; ochrona cyfrowej reputacji osób i organizacji uczestniczących w procesie.

Te umiejętności mogą być odnoszone do ram DigCompEdu opisanych wcześniej, ale mogą nie odpowiadać bezpośrednio indywidualnym kompetencjom zawartym w tych ramach. Raczej istnieją elementy w opisach obszarów kompetencji w ramach, które odpowiadają umiejętnościom korzystnym dla trenerów i edukatorów VET.

Tabela 1. Powiązanie sugerowanych umiejętności trenera VET z obszarami kompetencji DigCompEdu.

Umiejętność trenera VET	Obszar kompetencji DigCompEdu
Ogólna świadomość cyberbezpieczeństwa	• Wspieranie uczniów • Ułatwianie kompetencji cyfrowych uczniów
Ochrona danych i prywatności	• Zasoby cyfrowe • Ułatwianie kompetencji cyfrowych uczniów
Bezpieczeństwo i zarządzanie urządzeniami	• Nauczanie i uczenie się • Ułatwianie kompetencji cyfrowych uczniów
Bezpieczna komunikacja cyfrowa	• Zaangażowanie zawodowe • Ocena
Zarządzanie śladem cyfrowym	• Zasoby cyfrowe • Ułatwianie kompetencji cyfrowych uczniów

Krytyczne myślenie	• Nauczanie i uczenie się • Ułatwianie kompetencji cyfrowych uczniów
Ciągłe uczenie się	• Zaangażowanie zawodowe • Ułatwianie kompetencji cyfrowych uczniów
Obywatelstwo cyfrowe i etyka	• Wspieranie uczniów • Ułatwianie kompetencji cyfrowych uczniów

Umiejętności te zapewniają trenerom i edukatorom VET środki do uczestniczenia w działaniach edukacyjnych, przestrzegając najlepszych praktyk w zakresie higieny cyfrowej. Praktyczny odniesienie do niektórych najlepszych praktyk dostępne jest jako Digital Hygiene Cheat Sheet. Opisuje on 12 zasad bezpiecznego życia cyfrowego, które wszystkie wymagają pewnej wiedzy o świecie cyfrowym, które obejmują:

- utrzymywanie swojego oprogramowania, antywirusa, zapory itp. na bieżąco,
- używanie bezpiecznych haseł, zarządzanie nimi bezpiecznie i korzystanie z wieloskładnikowego uwierzytelniania,
- ostrożność przy pobieraniu oprogramowania,
- świadomość phishingu i innych podejrzanych prób kompromitacji swoich zasobów,
- ograniczanie swojego cyfrowego i społecznego śladu,
- przyjęcie ogólnego podejścia "bezpieczeństwo przede wszystkim" podczas zarządzania informacjami w środowisku cyfrowym.

W szkoleniach i edukacji VET zdobycie i praktykowanie umiejętności higieny cyfrowej jest ważne dla zapewnienia bezpiecznego środowiska wymiany informacji.

Rozdział 3 - Adaptacja higieny cyfrowej do programu nauczania i szkoleń VET

Tematy związane z higieną cyfrową powinny być codzienną częścią szkoleń VET. Trenerzy i edukatorzy VET powinni przestrzegać zasad zdrowej higieny cyfrowej podczas planowania i zarządzania szkoleniami, które obejmują wykorzystanie narzędzi cyfrowych jako część środowiska szkoleniowego; tworzenie i dystrybucję materiałów szkoleniowych; organizowanie komunikacji między uczestnikami oraz analizę wyników szkolenia i wykonywanie procedur administracyjnych oraz planowanie doskonalenia procesu szkoleniowego.

Ponadto trenerzy VET powinni być świadomi, że nawet jeśli temat szkolenia nie dotyczy bezpośrednio zagadnień cyfrowych, niektóre z tych informacji mogą być potrzebne w celu zwiększenia efektywności

prowadzonego szkolenia. Trenerzy powinni być świadomi możliwego zróżnicowania tła swoich studentów i dostosowywać harmonogram szkolenia, rezerwując czas i wysiłek na wyjaśnianie i demonstrację praktyk szkoleniowych, które poprawią higienę cyfrową ich studentów.

Oczywiście, czasami higiena cyfrowa i inne pokrewne tematy mogą być głównym tematem szkolenia. W takich przypadkach trenerzy i edukatorzy VET mogą przystąpić do prowadzenia swoich studentów, podczas gdy zdobywają nową wiedzę i umiejętności związane z higieną cyfrową.

Z perspektywy trenerów VET higiena cyfrowa może być postrzegana jako praktyka utrzymywania i zapewniania bezpiecznych i produktywnych działań cyfrowych podczas prowadzenia szkoleń, niezależnie od tematu szkolenia. Kilka aspektów szkoleń zawodowych i edukacyjnych może wymagać wykorzystania środowiska cyfrowego w celu poprawy wyników szkolenia i zwiększenia satysfakcji studentów uczestniczących w szkoleniu. Trenerzy powinni być świadomi, jak korzystanie z narzędzi cyfrowych wpływa na proces szkoleniowy i starać się włączyć niektóre aspekty związane z higieną cyfrową do samego szkolenia. Oto kilka opcji, jak poprawić proces szkoleniowy:

- **Tematy i moduły kursów dotyczące bezpieczeństwa cyfrowego**

Podczas oferowania treści szkoleniowych, proponując rozpoczęcie określonej aktywności szkoleniowej lub wymagając od studentów wykonania zadania administracyjnego związanego ze szkoleniem, wprowadź pewne porady w formie mniejszych tematów szkoleniowych lub bardziej rozbudowanych modułów, które uczą studentów podstaw cyberbezpieczeństwa, takich jak zarządzanie hasłami, rozpoznawanie prób phishingowych i zabezpieczanie danych osobowych i służbowych. W miarę możliwości dostosuj te tematy do konkretnych branż, linii pracy, ról zawodowych lub działań studentów, związanych z ich rzeczywistą linią pracy lub oczekiwaną przyszłą pozycją zawodową, na którą się przygotowują, czyniąc informacje istotnymi i przydatnymi.

- **Warsztaty praktyczne, prace indywidualne i grupowe**

Podczas prowadzenia praktycznych zadań w trakcie szkolenia, takich jak warsztaty praktyczne lub zadania indywidualne lub grupowe, wprowadź warsztaty, w których studenci mogą praktykować konfigurację bezpiecznych sieci, korzystanie z VPN, instalowanie i zarządzanie oprogramowaniem zabezpieczającym oraz przeprowadzanie regularnych kontroli bezpieczeństwa; lub pozwól im doświadczyć, jak niektóre błędy, których mogą nie być świadomi, wpływają na wykonywane zadania w bezpiecznym środowisku szkoleniowym. Praktyczne podejście i możliwości prób i błędów pomagają ugruntować teoretyczną wiedzę poprzez praktyczne zastosowanie.

- **Etyka i zgodność**

Podczas szkolenia włącz dyskusje i oferuj wskazówki dotyczące etycznego zachowania w sieci oraz prawnych implikacji działań cyfrowych, jeśli teoretyczne tematy szkoleniowe lub zadania praktyczne mają wpływ na niektóre zachowania. Może to obejmować tematy takie jak przepisy dotyczące ochrony danych osobowych, które są istotne dla tematu szkolenia lub ról zawodowych, oraz znaczenie utrzymywania profesjonalnego wizerunku online.

- **Zarządzanie śladem cyfrowym**

Edukacja studentów na temat zarządzania ich śladem cyfrowym, podkreślając długoterminowe skutki działań online na reputację osobistą i zawodową. Szkolenie może obejmować, jak efektywnie korzystać z mediów społecznościowych, zarządzać treściami cyfrowymi i rozumieć konsekwencje publikacji online.

- **Ciągłe uczenie się**

Bądź świadomy, że nowoczesne środowisko cyfrowe stale się zmienia. Na podstawie swojej roli i linii pracy, z której pochodzą lub do której zamierzają dołączyć, studenci mogą wymagać nowej wiedzy na temat tematów związanych z wykorzystaniem nowych narzędzi cyfrowych. Ważne jest, aby być na bieżąco z najnowszymi technologiami i być świadomym najnowszych zagrożeń, które mogą wpływać na studentów uczących się przedmiotu szkolenia. Podnoszenie świadomości na temat nowych możliwości w środowisku cyfrowym i wprowadzanie nowych narzędzi studentom może prowadzić do wyższej postrzeganej jakości szkolenia i poprawy wiedzy i umiejętności studentów. Szukanie możliwości ciągłego uczenia się i certyfikacji w zakresie praktyk bezpieczeństwa cyfrowego może stać się integralną częścią programu nauczania, niezależnie od głównych tematów szkolenia.

- **Ocena i certyfikacja**

Oceny są częścią szkolenia. Na podstawie tematu i celów szkolenia, oceny mogą być mniej lub bardziej formalne i mogą obejmować korzystanie z narzędzi cyfrowych do przeprowadzania oceny oraz gromadzenia i analizy wyników oceny. Dobrą praktyką jest upewnienie się, że studenci są świadomi właściwego korzystania z narzędzi oceny. Zawartość ocen może obejmować testowanie wiedzy i umiejętności zdobytych specjalnie w zakresie higieny cyfrowej, a także wiedzy na tematy ogólne. Oceny i certyfikaty mogą być wykorzystywane do motywowania studentów, a forma, w jakiej prezentowane są wyniki, może wymagać dodatkowego przemyślenia dotyczącego środowiska cyfrowego. Studenci mogą potrzebować pomocy przy zdobywaniu i obsłudze nowych informacji

certyfikacyjnych lub korzystaniu z nowych kwalifikacji w celu zwiększenia swojej atrakcyjności na rynku pracy.

Możesz zauważyć, że niektóre z opcji dotyczących poprawy szkoleń VET w zakresie higieny cyfrowej odpowiadają wcześniej zidentyfikowanym umiejętnościom. Wszystkie te elementy można włączyć do programów VET i spojrzeć na nie z dwóch różnych perspektyw: jakie umiejętności higieny cyfrowej powinny być stosowane jako część szkolenia i wymagają dodatkowej uwagi podczas szkolenia; oraz jakie są dodatkowe możliwości poprawy wiedzy i umiejętności w zakresie higieny cyfrowej podczas szkolenia, oprócz głównych tematów. Rozważenie tych elementów może poprawić jakość szkolenia i zapewnić studentom dodatkowe korzyści w ich środowisku pracy, które w dużej mierze opiera się na opcjach środowiska cyfrowego.

Z praktycznego punktu widzenia oznacza to, że trenerzy i edukatorzy VET powinni: wprowadzać bezpieczne środowiska do nauki i narzędzia specjalnie przypisane do szkoleń, ustanawiać wytyczne dotyczące obsługi materiałów szkoleniowych, korzystać z narzędzi komunikacyjnych i przeprowadzać komunikację z ochroną informacji osobistych i poufnych, zarządzać danymi dotyczącymi procesu szkoleniowego i wyników, które często zawierają informacje wrażliwe, oraz przestrzegać i udzielać ogólnych wskazówek, które ułatwiają przestrzeganie dobrych praktyk higieny cyfrowej.

Rozdział 4 – Przykład dobrej praktyki – Higiena cyfrowa dla VET

Przyjrzyjmy się dobremu przykładowi wprowadzenia higieny cyfrowej w organizacji VET w celu zapewnienia bezpieczeństwa organizacji oraz wykorzystania przez trenerów VET i studentów uczestniczących w szkoleniu.

Opis sytuacji

Firma szkoleniowa z branży edukacji i szkoleń zawodowych chce zapewnić szkolenia online dla swoich studentów, aby uniknąć kosztownego i czasochłonnego podróżowania oraz zapewnić studentom wygodę uczestniczenia w szkoleniu z bezpiecznych środowisk fizycznych. Firma VET ma zespół wewnętrznych i zewnętrznych trenerów, którzy mają różne wcześniejsze doświadczenia z prowadzeniem szkoleń online i mogą mieć różną wiedzę i umiejętności związane z prowadzeniem takich szkoleń. Firma ma również wewnętrznych pracowników, którzy wykonują czynności administracyjne związane ze szkoleniami i zarządzają informacjami, które czasami są wrażliwe i powinny być zgodne z przepisami i wytycznymi dotyczącymi zgodności. Zazwyczaj trenerzy będą korzystać z Microsoft Teams do prowadzenia szkoleń, udostępniania materiałów szkoleniowych i

komunikacji ze studentami, podczas gdy wewnętrzny personel wsparcia będzie korzystać z Microsoft Teams i e-maila do zarządzania studentami przed, w trakcie i po szkoleniu oraz z systemu przechowywania dokumentów do zarządzania i udostępniania materiałów szkoleniowych.

Rzeczy, którymi firma VET się martwi, to:

- nieprawidłowe zarządzanie informacjami osobistymi przez uczestników szkolenia
- ostrożne korzystanie z informacji poufnych firmy i partnerów zewnętrznych
- ograniczenie dostępu do szkolenia wyłącznie dla zamierzonej grupy odbiorców
- zapewnienie bogatego doświadczenia dla studentów
- utrzymanie określonego poziomu reputacji jako dobrego dostawcy usług szkoleniowych na rynku.

Zobaczmy, jak można rozwiązać kwestie higieny cyfrowej w tej sytuacji.

Rozwiązanie

Tego rodzaju sytuacja jest złożona i wymaga uwzględnienia kilku aspektów związanych z higieną cyfrową:

- organizacja konfiguracji środowiska Microsoft Teams i zarządzanie użytkownikami podczas szkolenia
- szkolenie trenerów prowadzących szkolenie
- przeprowadzanie rzeczywistych sesji szkoleniowych z udziałem studentów i trenerów
- zarządzanie materiałami szkoleniowymi używanymi podczas szkolenia
- organizowanie komunikacji między trenerem a studentami oraz między studentami
- przeprowadzanie oceny szkolenia i zbieranie opinii.

Szczegółowy opis dobrej praktyki dla każdego z tych aspektów jest następujący.

Konfiguracja i zarządzanie logowaniem

Teams For Education: Utworzono środowisko Teams oddzielone od środowiska Teams używanego do codziennej komunikacji i dzielenia się wiedzą przez pracowników organizacji VET. Microsoft Teams for Education jest dostępny dla tych organizacji VET, które spełniają wymagania oficjalnych instytucji edukacyjnych i zapewniają dodatkowe funkcje korzystne do prowadzenia szkoleń.

Single Sign-On (SSO): Wdrażanie SSO za pomocą wspólnej platformy uwierzytelniania (takiej jak Active Directory) w celu uproszczenia dostępu do aplikacji Microsoft Teams używanych w środowisku Microsoft Teams oraz innych narzędzi używanych centralnie i za zgodą organizacji VET podczas szkolenia.

Role-Based Access Control: Przydzielono role i uprawnienia w ramach Teams w oparciu o stanowisko użytkownika. Specyficznie przypisano 4 role, każdą z jej uprawnieniami w środowisku Teams: administrator systemu, administrator szkoleniowy (osoba organizująca sesje szkoleniowe przed szkoleniem i analizująca wyniki szkolenia po nim), trener (osoba prowadząca szkolenie i zadania praktyczne oraz zarządzająca materiałami szkoleniowymi podczas szkolenia) i student, zapewniając odpowiedni dostęp do funkcji i informacji.

Praktyki bezpiecznego uwierzytelniania: Tam, gdzie to odpowiednie, użytkownicy, którym przydzielono większe uprawnienia przy dostępie do wrażliwych informacji, zostali przeszkoleni w zakresie korzystania z uwierzytelniania wieloskładnikowego (MFA) i silnych haseł w celu zwiększenia bezpieczeństwa.

Szkolenie trenerów

Warsztaty szkoleniowe z Microsoft Teams: Zaplanowano i przeprowadzono dedykowane warsztaty dla trenerów na temat skutecznego korzystania z Microsoft Teams. Zaproszono trenerów wewnętrznych i zewnętrznych do udziału w szkoleniach, aby otrzymać wytyczne dotyczące bezpiecznego zachowania w środowisku Teams. Szkolenie obejmowało tworzenie i zarządzanie zespołami i kanałami, planowanie spotkań oraz korzystanie z funkcji współpracy, takich jak udostępnianie plików i czat.

Szkolenie z zaawansowanych funkcji: Dodatkowe szkolenie dotyczące zaawansowanych funkcji, takich jak pokoje grupowe, wydarzenia na żywo oraz integracja aplikacji firm trzecich, które mogą poprawić doświadczenie szkoleniowe, zostało zapewnione trenerom. Podczas szkolenia oferowano możliwość praktycznego ćwiczenia tych funkcji jako zadań praktycznych.

Stałe wsparcie: Dla trenerów, którzy potrzebowali pełnej konfiguracji na miejscu, oferowano fizyczne sale szkoleniowe z bezpiecznymi połączeniami internetowymi. Dla trenerów, którzy zamierzali korzystać z własnych pomieszczeń, dostarczano wytyczne dotyczące bezpiecznego prowadzenia szkoleń. Ustalono dane kontaktowe dedykowanego personelu wsparcia IT, aby pomóc trenerom w przypadku problemów technicznych.

Prowadzenie sesji szkoleniowych

Planowanie sesji: Wewnętrzni administratorzy szkoleń i trenerzy zostali przeszkoleni w zakresie korzystania z kalendarza do planowania sesji, ustawiania przypomnień i dostarczania agendy na zaproszeniu do spotkania. Automatyczne zaproszenia były ustawiane dla studentów, aby zminimalizować ryzyko dołączenia do niewłaściwych sesji szkoleniowych.

Funkcje interaktywne: Wszyscy trenerzy zostali poinformowani o możliwości korzystania z dodatkowych funkcji Teams, takich jak ankiety, quizy i tablice, aby angażować studentów i wzmacniać proces uczenia się, kiedy tylko jest to możliwe. Dopuszczono korzystanie z dodatkowych narzędzi i funkcji, ale trenerzy byli proszeni o udzielanie studentom wskazówek dotyczących korzystania z nich w celu uzyskania dodatkowych informacji lub zadań praktycznych.

Nagrywanie sesji: Nagrywanie sesji szkoleniowych było mocno ograniczone ze względu na RODO i odbywało się tylko za wyraźną zgodą wszystkich studentów. Po nagraniu nagrania były bezpiecznie przechowywane i dostępne tylko dla uczestników sesji szkoleniowych, i to tylko przez ograniczony czas. Mimo że nagrania są ogólnie uważane za korzystne dla studentów podczas przeglądania treści szkoleniowych później, organizacja VET powinna być świadoma ryzyk związanych z nimi.

Pokoje grupowe: Pokoje grupowe do działań grupowych lub dyskusji były tworzone przez administratora szkoleń, nadawano odpowiednie prawa dostępu i przeprowadzano odpowiednie szkolenia dla trenerów, umożliwiając im przeskakiwanie między pokojami w celu monitorowania i wspierania postępu szkoleniowego.

Obsługa materiałów szkoleniowych

Udostępnianie plików i zasobów: Wszystkie materiały szkoleniowe używane podczas szkoleń były przechowywane na bezpiecznych serwerach. Elektroniczne klucze do materiałów szkoleniowych lub rzeczywiste kopie materiałów szkoleniowych były zarządzane przez dedykowanego administratora szkoleń. W przypadku mniej wrażliwych materiałów używano środowiska Teams.

Wspólna edycja: Podczas współpracy nad dokumentami lub prezentacjami w czasie rzeczywistym podczas zadań praktycznych, trenerzy i studenci byli proszeni o korzystanie z oficjalnego

oprogramowania, takiego jak integracja z Office 365, i o zachowanie ostrożności w nadmiernym udostępnianiu informacji.

Kontrola wersji: W organizacji VET wprowadzono kontrolę wersji wewnętrznych dokumentów będących częścią materiałów szkoleniowych. Wszyscy trenerzy zostali poproszeni o pełnienie roli ekspertów w zakresie materiałów szkoleniowych zewnętrznych i zachęceni do konsultacji z wewnętrznymi administratorami szkoleń w sprawie wersji materiałów szkoleniowych, podręczników dla studentów i testów praktycznych, gdzie to możliwe, aby zmniejszyć ryzyko dostarczania nieaktualnych wersji materiałów szkoleniowych.

Komunikacja między studentami a trenerami

Regularne aktualizacje: Do ogłoszeń, udostępniania aktualizacji i przekazywania informacji zwrotnych na temat sesji szkoleniowych używano czatu Teams.

Dedykowane kanały: Tworzono kanały dla konkretnych sesji szkoleniowych i indywidualnych grup studentów, co ułatwiało ukierunkowane dyskusje i udostępnianie zasobów.

Prywatne czaty: Dodatkowe prywatne czaty między trenerem a studentami były ograniczone tylko do sytuacji, w których obie strony zgodziły się na dodatkową komunikację, organizując wymianę informacji kontaktowych centralnie.

Ocena i opinie

Formularze opinii: Używanie Microsoft Forms lub dedykowanego oprogramowania opracowanego wewnętrznie przez organizację VET do zbierania opinii na temat sesji szkoleniowych było egzekwowane. Linki do oprogramowania używanego do zbierania opinii były dystrybuowane za pośrednictwem środowiska Teams, zapewniając, że tylko zamierzona grupa odbiorców mogła uczestniczyć w przekazywaniu opinii. Dostęp do informacji zawartych w formularzach opinii był ograniczony do wewnętrznych administratorów szkoleń organizacji VET.

Śledzenie wyników: Funkcje przydzielania zadań w Teams były wykorzystywane do przydzielania zadań, zbierania pracy i przekazywania ocenionych opinii.

Ten setup zarówno środowiska technicznego, jak i procedur oraz ról zaangażowanych w proces zapewnia kompleksowe, bezpieczne i interaktywne środowisko szkoleniowe za pomocą Microsoft

Teams, spełniając potrzeby zarówno trenerów, jak i studentów, jednocześnie utrzymując wysoki standard higieny cyfrowej i efektywności.

Źródła

1. Vuorikari, R., Kluzer, S. and Punie, Y., DigComp 2.2: The Digital Competence Framework for Citizens, EUR 31006 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-48882-8, doi:10.2760/115376, JRC128415.
2. European e-Competence Framework, https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf, [accessed April 15, 2024].
3. European Union Agency for Cybersecurity (ENISA). European Cybersecurity Skills Framework Role Profiles, https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles [accessed April 15, 2024].
4. Punie, Y., editor(s), Redecker, C., European Framework for the Digital Competence of Educators: DigCompEdu, EUR 28775 EN, Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-73718-3 (print),978-92-79-73494-6 (pdf), doi:10.2760/178382 (print),10.2760/159770 (online), JRC107466.
5. World Economic Forum, “Future of Jobs Report 2023”, https://www.weforum.org/publications/the-future-of-jobs-report-2023/
6. Chui, M., Issler, M., Roberts, R., Yee, L. “McKinsey Technology Trends Outlook 2023”, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech#new-and-notable
7. Digital Hygiene Cheat Sheet. https://digitalhygiene.net/ [accessed April 15, 2024].

Moduł 2 - Dostosowany program nauczania higieny cyfrowej dla VET

Wprowadzenie

Higiena cyfrowa przyjęła znacznie większą i bardziej znaczącą rolę w naszym codziennym życiu. Wraz z szybkim rozwojem cyfryzacji i jej ekspansją we wszystkie sfery działalności ludzkiej pojawiła się pilna potrzeba zapewnienia, że nasze środowiska cyfrowe są bezpieczne. Jednym z podstawowych i fundamentalnych środków ochronnych w tym zakresie jest zapewnienie odpowiedniej higieny cyfrowej. Jest to szczególnie prawdziwe w obliczu rosnących zagrożeń cybernetycznych, przed którymi stoją organizacje. Higiena cyfrowa koncentruje się przede wszystkim na utrzymaniu zdrowej i bezpiecznej obecności cyfrowej, a stało się to coraz bardziej istotne, gdy więcej organizacji przenosi swoje działania online. Ten moduł został zaprojektowany, aby zapewnić solidny program nauczania, który może szkolić studentów na poziomie zawodowym w zakresie rozwijania, oceny i utrzymywania dobrych praktyk higieny cyfrowej.

Uczestnictwo w tym programie pozwoli studentowi zdobyć niezbędne podstawowe umiejętności analityczne i praktyczne, aby skutecznie oceniać, utrzymywać i interweniować tam, gdzie jest to konieczne, w celu zapewnienia higieny cyfrowej w środowisku organizacyjnym. Jest to naprawdę istotny program ze względu na wysokie zapotrzebowanie na rynku na profesjonalistów posiadających umiejętności w tej dziedzinie. Ten program rozwojowy został porównany z najlepszymi praktykami w tej dziedzinie. Skupienie się na startupach i małych i średnich przedsiębiorstwach (MŚP) zadecydowało o wyborze modułów i struktury. Celem jest budowanie kompetencji na tym poziomie, co oznacza, że program jest zaprojektowany i zorganizowany tak, aby był dostępny dla osób chcących realizować go w trybie częściowym lub pełnym. Program jest również zaprojektowany w sposób praktyczny i zorientowany na praktykę, z krótkim czasem realizacji. Jednak jest również zaprojektowany tak, aby studenci mogli pracować we własnym tempie.

Rozdział 1 – Przegląd programu nauczania

Niniejszy podręcznik został napisany, aby dostarczyć studentom aktualnie zapisanym lub planującym zapisać się na program Edukacji i Szkolenia Zawodowego (VET) w zakresie higieny cyfrowej oraz instruktorom istotnych informacji dotyczących celu, planowania, struktury i oceny programu. Uznając, że nie wszystkie organizacje są takie same i wymagają tego samego poziomu umiejętności w zakresie

higieny cyfrowej, ten moduł i jego różne części są modułowe w swojej strukturze. Pozwala to osobom, które są biegłe w pewnych obszarach, skupić się lub przejść do innych modułów w miarę rozwoju ich potrzeb. Ostatecznym celem tego programu jest stworzenie solidnych podstaw w zakresie higieny cyfrowej, umożliwiających zarówno studentom, jak i instruktorom skuteczne zarządzanie i minimalizowanie zagrożeń cybernetycznych. Ten program nauczania jest również zaprojektowany tak, aby obejmował znaczne części podstawowych certyfikacji zawodowych w zakresie cyberbezpieczeństwa, takich jak GIAC Security Essentials (GSEC) i CompTIA Security+. W związku z tym dostarcza dodatkowej wartości i zwiększa motywację studentów do udziału w tym programie.

Cel programu i cele modułu

Podstawowe cele modułu higieny cyfrowej są zaprojektowane w celu wzmocnienia postawy bezpieczeństwa cybernetycznego organizacji poprzez umożliwienie uczestnikom:

- Ocenę zagrożeń cybernetycznych, przed którymi stoją organizacje.
- Ocenę i wdrożenie podstawowych zabezpieczeń sieci.
- Poznanie sposobów wdrażania i utrzymania podstawowych protokołów szyfrowania.
- Ocenę i wdrożenie protokołów zarządzania danymi i bezpieczeństwem.
- Ocenę i stosowanie podstawowych protokołów bezpieczeństwa sprzętu i oprogramowania.
- Zarządzanie bezpieczeństwem w środowisku mobilnym.

Metodologia nauczania

Program stosuje mieszankę instrukcji teoretycznych i praktycznego zastosowania. Wykorzystuje studia przypadków, sesje laboratoryjne i warsztaty interaktywne, aby zapewnić, że uczniowie mogą zastosować koncepcje, których się uczą, w rzeczywistych scenariuszach. Takie podejście nie tylko zwiększa zrozumienie, ale także zapewnia, że absolwenci są gotowi do pracy i mogą natychmiast po ukończeniu programu wdrażać kompleksowe praktyki higieny cyfrowej.

Ocena i ciągłe doskonalenie

Ocena w programie higieny cyfrowej jest zarówno rygorystyczna, jak i ciągła, wykorzystując różnorodne metody oceny wiedzy i umiejętności uczestników. Obejmują one quizy, egzaminy praktyczne, oceny projektów i projekt końcowy, który podsumowuje całość nauki uczestników. Mechanizmy przekazywania opinii są integralną częścią programu nauczania, dostarczając uczestnikom terminowych informacji zwrotnych na temat ich postępów i obszarów do poprawy.

Ponadto sam program nauczania jest regularnie aktualizowany, aby dostosować się do najnowszych informacji o zagrożeniach cybernetycznych i postępach technologicznych, zapewniając aktualność i skuteczność w rozwiązywaniu współczesnych wyzwań związanych z cyberbezpieczeństwem.

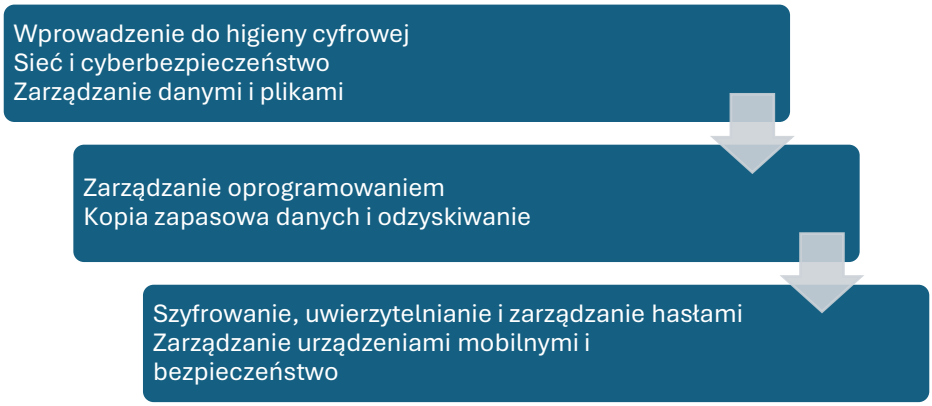
Wnioski

Program higieny cyfrowej w instytucji VET został zaprojektowany nie tylko w celu przekazania niezbędnej wiedzy i umiejętności w zakresie cyberbezpieczeństwa, ale także w celu zaszczepienia proaktywnej i świadomej kultury cyberbezpieczeństwa wśród uczestników. Pod koniec programu uczestnicy nie są tylko absolwentami; są tocybernetyczni obywatele, wyposażeni w narzędzia, aby w znaczący sposób przyczynić się do obrony cybernetycznej swoich organizacji. Ten wszechstronny program stanowi kamień węgielny w przygotowaniu następnej generacji specjalistów ds. cyberbezpieczeństwa, gotowych do stawienia czoła dynamicznym wyzwaniom ery cyfrowej.

Rozdział 2 – Kluczowe obszary nauki

Przegląd programu nauczania

Kod	Obszary nauki / Przedmioty
D21	Wprowadzenie do higieny cyfrowej
D22	Sieci i cyberbezpieczeństwo
D23	Zarządzanie danymi i plikami
D24	Zarządzanie oprogramowaniem
D25	Kopia zapasowa i odzyskiwanie danych
D26	Szyfrowanie, uwierzytelnianie i zarządzanie hasłami
D27	Zarządzanie urządzeniami mobilnymi i bezpieczeństwo



Wprowadzenie do higieny cyfrowej

Ten przedmiot jest zaprojektowany, aby dostarczyć studentom kompleksowego przeglądu higieny cyfrowej. Przegląd ten zapewni zarówno koncepcyjny przegląd treści, jak i niektóre praktyczne

działania, patrząc na program z perspektywy zintegrowanej. Główny nacisk będzie położony na wprowadzenie różnych obszarów higieny cyfrowej i jak różne obszary przedmiotowe są ze sobą powiązane i powiązane. Przedstawi on wstępny przegląd podstawowych zasad i praktyk higieny cyfrowej oraz jak różne komponenty współgrają ze sobą. Ta jednostka dostarcza podstawową wiedzę i zrozumienie, na których można budować inne obszary składowe.

Kluczowe tematy omawiane w tym przedmiocie

- Zrozumienie higieny cyfrowej: Badanie, czym jest higiena cyfrowa i dlaczego jest krytyczna w dzisiejszej epoce cyfrowej.
- Podstawy higieny cyfrowej: Podstawowe praktyki i protokoły zapewniające integralność i bezpieczeństwo danych i systemów.
- Implimkacje bezpieczeństwa higieny cyfrowej: Szczegółowe spojrzenie na to, jak skuteczna higiena cyfrowa może zmniejszyć różne zagrożenia cybernetyczne.
- Podstawy wdrażania higieny cyfrowej: Praktyczne kroki do wdrożenia środków higieny cyfrowej w kontekstach osobistych i organizacyjnych.
- Zgodność z cyberbezpieczeństwem: Przegląd podstawowych krajowych i unijnych polityk, regulacji i wymagań dotyczących zgodności w zakresie cyberbezpieczeństwa.

Wyniki nauczania przedmiotu

Pod koniec tego przedmiotu studenci będą w stanie:

- Zdefiniować higienę cyfrową i zrozumieć jej krytyczne komponenty.
- Zidentyfikować potencjalne zagrożenia cybernetyczne i zrozumieć rolę higieny cyfrowej w ochronie przed tymi zagrożeniami.
- Wdrażać podstawowe praktyki higieny cyfrowej na różnych platformach i urządzeniach.
- Komunikować znaczenie higieny cyfrowej rówieśnikom i przełożonym, promując najlepsze praktyki w swoich organizacjach.
- Zrozumieć podstawowe wymagania dotyczące zgodności z cyberbezpieczeństwem.

Metody nauczania

Mieszanka wykładów, warsztatów interaktywnych i studiów przypadków będzie stosowana, aby zapewnić studentom solidne doświadczenie edukacyjne. Każda sesja ma na celu zrównoważenie

wiedzy teoretycznej z praktycznym zastosowaniem, zapewniając, że studenci mogą przekształcić to, czego się uczą, w strategie działania w swoich miejscach pracy.

Zalecana literatura

- Brooks, C.J., Grow, C., Craig, P., Short, D. (2018). Cybersecurity Essentials.
    - Książka ta stanowi gruntowne wprowadzenie do dziedziny cyberbezpieczeństwa i jest szczególnie przydatna dla osób ubiegających się o certyfikat z zakresu cyberbezpieczeństwa na poziomie podstawowym.
- Paula, D., Cruz, M. (2023). Cybersecurity Essentials Made Easy: A No-Nonsense Guide to Cyber Security for Beginners.
    - Książka ta jest niezbędną lekturą dla zrozumienia wyzwań cyberbezpieczeństwa i sposobów ich łagodzenia. Jest szczególnie istotna dla nowych właścicieli małych i średnich przedsiębiorstw (MŚP) i studentów, którzy chcą zrozumieć bezpieczeństwo online.
- Singer, P. W., Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
    - W niniejszym podręczniku przedstawiono przystępny przegląd najważniejszych pojęć i wyzwań w dziedzinie cyberbezpieczeństwa, co czyni go doskonałym źródłem wiedzy dla studentów rozpoczynających swoją przygodę z poznawaniem zagrożeń cybernetycznych i mechanizmów ochrony.
- Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.
    - Książka Bruce'a Schneiera ma kluczowe znaczenie dla zrozumienia kwestii prywatności i bezpieczeństwa danych, oferując wgląd w sposób gromadzenia i wykorzystywania danych osobowych oraz znaczenie solidnych praktyk zarządzania danymi.

Zasoby te wybrano z myślą o przekazaniu wiedzy teoretycznej i praktycznych umiejętności w zakresie sieci i cyberbezpieczeństwa, wspierając program nauczania i wzbogacając doświadczenia edukacyjne uczniów szkół zawodowych w zakresie higieny cyfrowej.

Sieć & Cyberbezpieczeństwo

Ten przedmiot koncentruje się na dostarczeniu studentom niezbędnych umiejętności potrzebnych do identyfikacji, oceny i neutralizacji zagrożeń sieciowych. Jednym z kluczowych wyzwań, przed którymi stoją organizacje w obecnym środowisku operacyjnym, jest zapewnienie bezpieczeństwa sieci. Ponieważ większość sieci jest połączona z Internetem, często są one narażone na działania złośliwych aktorów, którzy mogą próbować wykorzystać luki w sieci, aby uzyskać do niej nieautoryzowany dostęp. Aby tego dokonać, studenci zostaną poinstruowani w kluczowych koncepcjach sieciowych, wspólnych protokołach, portach, LAN, WAN i systemach chmurowych.

Kluczowe tematy omawiane w tym przedmiocie

- Wprowadzenie do cyberbezpieczeństwa
- Analiza podatności
- Ocena zagrożeń i ryzyka
- Protokoły bezpieczeństwa sieci – Firewalle, antywirusy
- Wspólne ataki cyberbezpieczeństwa
- Narzędzia cyberbezpieczeństwa
- Etyka w cyberbezpieczeństwie

Rezultaty uczenia się

- Zidentyfikowanie kluczowych koncepcji sieciowych: Studenci będą mogli opisać podstawowe aspekty sieci, w tym LAN, WAN i systemy chmurowe, oraz zrozumieć ich role w infrastrukturze organizacyjnej.
- Ocena podatności sieci: Uczestnicy zdobędą umiejętności potrzebne do przeprowadzania analizy podatności na różnych systemach sieciowych w celu identyfikacji potencjalnych słabości bezpieczeństwa.
- Wdrażanie środków bezpieczeństwa: Studenci będą biegli w ustawianiu i zarządzaniu protokołami bezpieczeństwa sieci, takimi jak firewalle i systemy antywirusowe, aby chronić przed zagrożeniami cybernetycznymi.
- Prowadzenie oceny zagrożeń i ryzyka: Wyposażenie studentów w zdolność oceny i priorytetowania ryzyk związanych z zagrożeniami cybernetycznymi dla systemów sieciowych.
- Zrozumienie implikacji etycznych: Studenci będą badać etyczne rozważania w cyberbezpieczeństwie, rozumiejąc odpowiedzialności związane z ochroną danych i systemów przed nieautoryzowanym dostępem.

Metody nauczania

- Wykłady interaktywne: Skoncentrowane na wprowadzeniu podstawowych i zaawansowanych koncepcji sieciowych, protokołów bezpieczeństwa oraz kwestii etycznych w cyberbezpieczeństwie.
- Laboratoria praktyczne: Sesje praktyczne w laboratoriach komputerowych, gdzie studenci mogą używać rzeczywistych i symulowanych środowisk sieciowych do stosowania środków bezpieczeństwa i narzędzi.
- Analiza studiów przypadku: Dyskusje i analizy rzeczywistych incydentów cyberbezpieczeństwa, aby zrozumieć mechanizmy zagrożeń i skuteczne środki zaradcze.
- Projekty grupowe: Zespoły studentów ocenią hipotetyczną konfigurację sieci pod kątem podatności i zaproponują kompleksową strategię bezpieczeństwa.
- Sesje z gośćmi specjalistami: Profesjonaliści z dziedziny cyberbezpieczeństwa są zapraszani, aby dzielić się wglądami i doświadczeniami, podkreślając aktualne wyzwania i nowe technologie.

Zalecana literatura

- Stewart, J. M., Chapple, M., & Gibson, D. (2020). CompTIA Security+ Guide to Network Security Fundamentals (7th ed.). Cengage Learning.
    - Przewodnik obejmuje szeroki zakres podstawowych tematów z zakresu bezpieczeństwa sieci, odpowiedni dla studentów rozpoczynających swoją przygodę z cyberbezpieczeństwem.
- Marsh, N., (2023), Cyberbezpieczeństwo: Przewodnik bez tłuszczu do najlepszych praktyk bezpieczeństwa sieci (Fat-Free Technology Guides). Ta książka zapewnia wszechstronny wgląd w zagrożenia cybernetyczne i kluczowe kwestie bezpieczeństwa sieci.
- Whitman, M. E., & Mattord, H. J. (2018). Zasady bezpieczeństwa informacji (6th ed.). Cengage Learning.
    - Kompleksowe źródło, które zapewnia dogłębny wgląd w zasady bezpieczeństwa informacji, w tym szczegółowe dyskusje na temat analizy podatności, zagrożeń i oceny ryzyka.
- Stallings, W. (2017). Podstawy bezpieczeństwa sieci: Aplikacje i standardy (6th ed.). Pearson. Tekst Stallingsa zapewnia kompleksowe omówienie protokołów i standardów bezpieczeństwa sieci, idealne dla studentów potrzebujących szczegółowego zrozumienia technicznych aspektów zabezpieczania sieci.

- Computer & Internet Security: A Hands-on Approach 3rd ed. Edition by Wenliang Du Te zasoby akademickie wspierają program nauczania, dostarczając zarówno teoretycznych ram, jak i praktycznych wglądów w zarządzanie i zabezpieczanie środowisk sieciowych, zgodnie z przedstawionymi rezultatami uczenia się i strategiami nauczania.

Te zasoby akademickie będą wspierać program nauczania, zapewniając zarówno ramy teoretyczne, jak i praktyczne informacje na temat zarządzania środowiskami sieciowymi i ich zabezpieczania, zgodnie z przedstawionymi rezultatami uczenia się i strategiami nauczania.

Zarządzanie Danymi i Plikami

Dane, jak wspomniano wcześniej, są jednym z najcenniejszych zasobów organizacji. W konsekwencji zarządzanie tym zasobem nabrało coraz bardziej kluczowego znaczenia w organizacji. Jest to szczególnie ważne z powodu wzrostu obaw o bezpieczeństwo w środowisku cybernetycznym. Prawidłowe zarządzanie danymi stało się kluczowe dla efektywnego cyberbezpieczeństwa, zwłaszcza w zakresie przechwytywania, organizowania i rozpowszechniania poufnych informacji. Zarządzanie danymi odnosi się do zasad i praktyk stosowanych w zarządzaniu i ochronie danych. W kontekście cyberbezpieczeństwa zarządzanie danymi dotyczy również ochrony danych przed nieautoryzowanym dostępem, modyfikacją i transmisją. W obecnym środowisku, gdzie gromadzone, analizowane i rozpowszechniane są ogromne ilości danych, aspekty zarządzania bezpieczeństwem zyskały na znaczeniu. Dlatego istnieje zwiększone zapotrzebowanie na profesjonalistów, którzy są biegli w zarządzaniu danymi.

Kluczowe Tematy Zawarte w Tym Przedmiocie

- Zarządzanie danymi
- Klasyfikacja danych
- Szyfrowanie w zarządzaniu danymi
- Monitorowanie i audyt danych
- Kopia zapasowa i odzyskiwanie danych
- Integralność i prywatność danych
- Kontrola dostępu i uwierzytelnianie

Efekty Uczenia się

- Zrozumienie Zarządzania Danymi: Studenci zdobędą podstawowe pojęcia zarządzania danymi i jego roli w kontekście organizacyjnym.
- Klasyfikacja Danych: Uczniowie będą w stanie klasyfikować dane w oparciu o ich wrażliwość i znaczenie, stosując odpowiednie środki bezpieczeństwa do różnych typów danych.
- Implementacja Szyfrowania Danych: Studenci zrozumieją i zastosują techniki szyfrowania w celu ochrony integralności i poufności danych podczas przechowywania i transmisji.
- Przeprowadzanie Audytów Danych: Wyposażyć uczniów w umiejętności do regularnego monitorowania i audytowania danych w celu zapewnienia zgodności z politykami bezpieczeństwa i regulacjami.
- Zarządzanie Odzyskiwaniem Danych: Studenci nauczą się strategii kopii zapasowej i odzyskiwania danych w celu zapewnienia dostępności i ciągłości danych w przypadku ich utraty lub awarii systemu.
- Zapewnienie Integralności i Prywatności Danych: Uczniowie zrozumieją metody utrzymania integralności danych i zarządzania ustawieniami prywatności w celu ochrony danych użytkowników przed nieautoryzowanym dostępem.
- Stosowanie Kontroli Dostępu: Studenci będą w stanie wdrożyć solidne środki kontroli dostępu i uwierzytelniania w celu zabezpieczenia dostępu do danych.

Zalecana Literatura

- Ladley J., (2019)., Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program 2nd Edition. Ta książka zapewnia kompleksowe spojrzenie na zarządzanie danymi i bezpieczeństwo.
- Talabis, M., & Martin, J. (2015). Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis**.** Syngress.
    - Ta książka dostarcza praktycznych narzędzi i technik do oceny ryzyka związanego z bezpieczeństwem informacji, w tym związanego z zarządzaniem danymi.
- Bertino, E., & Sandhu, R. (2017). Data Privacy and Security. Springer.

    - Kompleksowy przegląd technik prywatności i bezpieczeństwa danych, ta książka jest kluczowa dla zrozumienia złożoności ochrony wrażliwych danych w różnych środowiskach.
- Swanson, M., & Guttman, B. (2016). Generally Accepted Principles and Practices for Securing Information Technology Systems. National Institute of Standards and Technology.
    - Ta publikacja rządowa oferuje wytyczne i najlepsze praktyki dotyczące zabezpieczania systemów IT, w tym szczegółowe sekcje dotyczące zarządzania danymi i kontroli bezpieczeństwa.

Te materiały akademickie wzbogacą ramy edukacyjne, dostarczając wiedzy teoretycznej i przykładów praktycznych zastosowań, umożliwiając studentom nabycie umiejętności skutecznego zarządzania danymi organizacyjnymi i ich zabezpieczania.

Zarządzanie Oprogramowaniem

Zarządzanie oprogramowaniem jest kluczowym elementem cyberbezpieczeństwa. Zarządzanie oprogramowaniem obejmuje systematyczny proces planowania, wdrażania, monitorowania i utrzymania oprogramowania przez cały jego cykl życia. Obejmuje zadania takie jak kontrola wersji, zarządzanie poprawkami, licencjonowanie i aktualizacje bezpieczeństwa. Efektywne zarządzanie oprogramowaniem zapewnia optymalną wydajność, bezpieczeństwo i zgodność przy jednoczesnym minimalizowaniu ryzyka i podatności. Współczesne organizacje stają przed różnymi wyzwaniami związanymi z bezpieczeństwem oprogramowania, takimi jak słabe polityki haseł, niebezpieczne API, niezałatane podatności, phishing i naruszenia danych. Dlatego konieczne jest, aby mieli wyszkolonych pracowników, którzy są przeszkoleni do efektywnego zarządzania oprogramowaniem organizacji i zapobiegania naruszeniom bezpieczeństwa oprogramowania. Ten moduł dostarczy studentom podstawowej wiedzy praktycznej na temat efektywnego zarządzania oprogramowaniem organizacji i minimalizowania ryzyka naruszenia bezpieczeństwa.

Kluczowe Tematy Zawarte w Tym Przedmiocie

- Bezpieczeństwo aplikacji
- Testowanie i audytowanie oprogramowania
- Zarządzanie dostępem użytkowników i uprawnieniami
- Implementacja regularnych protokołów aktualizacji

- Środki bezpieczeństwa punktów końcowych

Efekty Uczenia się

- Opanowanie Bezpieczeństwa Aplikacji: Studenci zrozumieją podstawy zabezpieczania aplikacji od projektu po wdrożenie, w tym powszechne podatności i strategie łagodzenia skutków.
- Przeprowadzanie Testów i Audytów Oprogramowania: Uczniowie zdobędą umiejętności w różnych metodach testowania i audytowania oprogramowania w celu identyfikacji i rozwiązywania problemów z bezpieczeństwem.
- Zarządzanie Dostępem Użytkowników: Studenci nauczą się efektywnie zarządzać dostępem użytkowników i uprawnieniami, aby zapewnić, że tylko autoryzowani użytkownicy mają dostęp do krytycznych zasobów oprogramowania.
- Implementacja Protokołów Aktualizacji: Wyposażyć uczniów w wiedzę na temat ustanawiania i utrzymywania regularnych protokołów aktualizacji oprogramowania w celu łagodzenia podatności.
- Zwiększenie Bezpieczeństwa Punktów Końcowych: Studenci zrozumieją środki bezpieczeństwa punktów końcowych w celu ochrony infrastruktury organizacji przed zagrożeniami takimi jak malware i ransomware.

Zalecana Literatura

- Du, W., (2022), Computer Security: A hands-on approach, 3rd edition**.** Ta książka bada zarządzanie oprogramowaniem, podatności i działania łagodzące.
- Allen, J. H., Barnum, S., Ellison, R., McGraw, G., & Viega, J. (2008). Software Security Engineering: A Guide for Project Managers**.** Addison-Wesley Professional.
    - Ta książka oferuje kompleksowy przewodnik po integracji praktyk bezpieczeństwa w rozwój oprogramowania, co jest niezbędne do zrozumienia bezpieczeństwa aplikacji i zarządzania cyklem życia.
- Anton, A. I., & Earp, J. B. (2004). A Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. Academy of Management Review.
    - Dostarcza wglądu w zarządzanie dostępem użytkowników i uprawnieniami poprzez identyfikację kluczowych interesariuszy i ich potrzeb, co jest kluczowe dla efektywnego zarządzania oprogramowaniem.
- Lindqvist, U., & Neumann, P. G. (2017). The Future of Cybersecurity: Challenges and Opportunities**.** IEEE Security & Privacy.

- Ten artykuł omawia przyszłe wyzwania i możliwości w dziedzinie cyberbezpieczeństwa, w tym znaczenie ciągłych aktualizacji oprogramowania i środków bezpieczeństwa punktów końcowych.

Te zasoby będą wspierać program nauczania, dostarczając solidne podstawy teoretyczne i praktyczne wglądy w zarządzanie oprogramowaniem, zapewniając, że studenci są dobrze przygotowani do radzenia sobie z wyzwaniami związanymi z bezpieczeństwem oprogramowania w nowoczesnych środowiskach organizacyjnych.

Kopia zapasowa i odzyskiwanie danych

Ten moduł ma na celu wyposażenie studentów w kompleksowe zrozumienie procesu tworzenia kopii zapasowych i odzyskiwania danych oraz sposobu ich wdrażania. Wszystkie nowoczesne organizacje muszą posiadać odpowiednie polityki, protokoły i systemy tworzenia kopii zapasowych i odzyskiwania danych. Większość współczesnych organizacji jest napędzana danymi, w związku z czym zarządzanie ich danymi i zasobami informacyjnymi ma ogromne znaczenie. W zasadzie większość organizacji, zwłaszcza MŚP, przechowuje swoje dane w scentralizowanej lokalnej lub chmurowej bazie danych. Systemy chmurowe stały się bardziej zaawansowane i bezpieczne dzięki bardzo zaawansowanym kontrolom zarządzania, co sprawia, że są mniej podatne na tradycyjne problemy związane z uszkodzeniem fizycznych systemów przechowywania. Jednak nadal są podatne na błędy ludzkie, błędne konfiguracje i wycieki danych, dlatego ważne jest, aby personel IT nadzorujący takie systemy był zaznajomiony z technologiami, protokołami i procesami z tym związanymi. Moduł ten ma na celu dostarczenie tej wiedzy studentom.

Kluczowe tematy omawiane w tym przedmiocie

- Zarządzanie plikami
- Protokoły tworzenia kopii zapasowych i odzyskiwania danych
- Rodzaje kopii zapasowych
- Usługi i urządzenia do tworzenia kopii zapasowych

Efekty uczenia się

- Zrozumienie zarządzania plikami: Studenci nauczą się zasad efektywnego zarządzania plikami, co jest kluczowe dla organizacji danych do celów tworzenia kopii zapasowych.
- Opanowanie protokołów tworzenia kopii zapasowych i odzyskiwania danych: Uczniowie zrozumieją różne protokoły tworzenia kopii zapasowych i odzyskiwania danych oraz jak stosować je efektywnie w różnych scenariuszach.
- Identyfikacja rodzajów kopii zapasowych: Studenci będą w stanie rozróżnić różne rodzaje kopii zapasowych (pełne, przyrostowe, różnicowe) i zdecydować, które są najbardziej odpowiednie w określonych sytuacjach.
- Wykorzystanie usług i urządzeń do tworzenia kopii zapasowych: Wyposażyć uczniów w wiedzę na temat różnych usług i urządzeń do tworzenia kopii zapasowych, w tym rozwiązań chmurowych i lokalnych, oraz jak wdrażać je bezpiecznie.
- Minimalizowanie ryzyka utraty danych: Studenci zrozumieją, jak planować i realizować strategię odzyskiwania danych, aby minimalizować przestoje i utratę danych w przypadku naruszeń danych lub klęsk żywiołowych.

Zalecana literatura

- Preston, W., (2021), Modern Data Protection: Ensuring Recoverability of All Modern Workloads. Ta książka omawia nowoczesną ochronę danych i sposób jej integracji z ogólnym bezpieczeństwem sprzętu i oprogramowania.
- Data Backup And Recovery: A Complete Guide - 2023 Edition
- Toigo, J. W. (2009). Disaster Recovery Planning: Preparing for the Unthinkable (3rd ed.). Prentice Hall.
    - Oferuje kompleksowe spojrzenie na planowanie odzyskiwania po katastrofie, w tym szczegółowe omówienie strategii tworzenia kopii zapasowych jako kluczowego elementu odzyskiwania po katastrofie.
- Duffy, D. (2014). Cloud Computing: Strategies for Cloud Computing Adoption. Faithful Pen Publishing.
    - Omawia przyjęcie technologii chmurowych, koncentrując się na usługach tworzenia kopii zapasowych w chmurze oraz związanych z nimi zagadnieniach bezpieczeństwa.

Te zasoby akademickie wzmocnią program nauczania, dostarczając studentom zarówno podstawowej wiedzy, jak i praktycznych umiejętności w zarządzaniu i wdrażaniu strategii tworzenia kopii zapasowych i odzyskiwania danych, co jest niezbędne do minimalizowania potencjalnej utraty danych w nowoczesnych środowiskach organizacyjnych.

Kryptografia, uwierzytelnianie i zarządzanie hasłami

Dane i informacje stały się jednym z najważniejszych zasobów organizacyjnych, a w wielu przypadkach są kluczowym czynnikiem determinującym wartość firmy. Istotność takich zasobów sprawia, że muszą być one traktowane z najwyższą starannością. Jednym z kluczowych narzędzi do ochrony danych i zasobów informacyjnych jest kryptografia. Kryptografia jest centralnym elementem cyberbezpieczeństwa, ponieważ jest niezbędna do ochrony wrażliwych danych i informacji oraz bezpiecznej komunikacji. Umożliwia solidne protokoły uwierzytelniania i zarządzania hasłami. Kryptografia umożliwia właściwe wdrożenie systemów uwierzytelniania, które zapewniają poufność, integralność i dostępność danych i informacji organizacyjnych dla odpowiednich pracowników.

Kluczowe tematy omawiane w tym przedmiocie

- Podstawy kryptografii
- Szyfrowanie end-to-end
- Standardy szyfrowania
- Uwierzytelnianie wieloskładnikowe
- Zarządzanie kluczami
- Wybór najlepszych standardów dla Twojej firmy
- Najlepsze praktyki we wdrażaniu technologii szyfrowania

Efekty uczenia się

- Zrozumienie podstaw kryptografii: Studenci poznają podstawowe zasady kryptografii, w tym jej historię, cel i kluczowe mechanizmy.
- Implementacja szyfrowania end-to-end: Uczniowie zdobędą umiejętności w zakresie wdrażania i zarządzania szyfrowaniem end-to-end w celu zabezpieczenia komunikacji.

- Stosowanie standardów szyfrowania: Studenci będą zaznajomieni z różnymi standardami szyfrowania i nauczą się, jak stosować je zgodnie z potrzebami organizacji.
- Wykorzystanie uwierzytelniania wieloskładnikowego: Wyposażyć studentów w umiejętność wdrażania i zarządzania systemami uwierzytelniania wieloskładnikowego w celu zwiększenia bezpieczeństwa.
- Zarządzanie kluczami kryptograficznymi: Studenci zrozumieją procesy zarządzania kluczami oraz najlepsze praktyki w celu zapewnienia bezpieczeństwa i integralności kluczy kryptograficznych.
- Wybór i wdrażanie technologii szyfrowania: Studenci nauczą się, jak wybierać odpowiednie technologie szyfrowania dla swojej firmy oraz najlepsze praktyki we wdrażaniu tych technologii w celu skutecznej ochrony danych.

Zalecana literatura

- Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.)**.** Pearson.
    - Ten podręcznik zapewnia kompleksowe wprowadzenie do dziedziny kryptografii i bezpieczeństwa sieci, w tym szczegółowe omówienie technologii szyfrowania i protokołów uwierzytelniania.
- Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography (2nd ed.)**.** CRC Press.
    - Oferuje dogłębną eksplorację nowoczesnych technik kryptograficznych, koncentrując się na rygorystycznych dowodach bezpieczeństwa i praktycznych zastosowaniach.
- Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications**.** Wiley.
    - Ta książka omawia projektowanie i wdrażanie systemów kryptograficznych, podkreślając znaczenie właściwej implementacji w celu zapobiegania podatnościom.

Te zasoby zostały wybrane, aby dostarczyć teoretyczne podstawy i praktyczne umiejętności z zakresu kryptografii, uwierzytelniania i zarządzania hasłami, wspierając cel programu nauczania, jakim jest wyposażenie studentów w niezbędną wiedzę do skutecznego zabezpieczania danych organizacyjnych.

Zarządzanie i bezpieczeństwo urządzeń mobilnych

Organizacje coraz częściej wdrażają urządzenia mobilne jako główną platformę pracy i środek komunikacji. Jest to szczególnie istotne w przypadku startupów i MŚP, gdzie elastyczność i dostępność w każdym momencie stały się głównym kryterium sukcesu. Chociaż technologia mobilna rozwinęła się tak, że większość zaawansowanych smartfonów jest tak potężna i wszechstronna jak laptopy i komputery stacjonarne, bezprzewodowa natura tych urządzeń sprawia, że są one podatne na działania złośliwych aktorów, którzy chcą uzyskać nieautoryzowany dostęp. Ten moduł ma na celu dostarczenie wglądu w podatności tych urządzeń i ich platform oraz jak można zminimalizować takie ryzyka.

Kluczowe tematy omawiane w tym przedmiocie

- Zrozumienie zagrożeń dla urządzeń mobilnych
- Ocena ryzyk związanych z aplikacjami mobilnymi
- Firewalle dla komunikacji międzyprocesowej
- Technologie bezpieczeństwa mobilnego
- Kontrola dostępu do danych mobilnych i zarządzanie ryzykiem

Efekty uczenia się

- Identyfikacja zagrożeń dla urządzeń mobilnych: Studenci nauczą się rozpoznawać różne zagrożenia skierowane na platformy mobilne i zrozumieją ich potencjalny wpływ.
- Ocena ryzyk dla aplikacji mobilnych: Uczniowie zdobędą umiejętności w ocenie ryzyk związanych z aplikacjami mobilnymi, koncentrując się na podatnościach bezpieczeństwa.
- Wdrażanie technologii bezpieczeństwa mobilnego: Studenci będą w stanie wdrażać i zarządzać technologiami bezpieczeństwa zaprojektowanymi specjalnie dla urządzeń mobilnych.
- Zarządzanie firewallami komunikacji międzyprocesowej: Wyposażyć studentów w wiedzę na temat konfiguracji i zarządzania firewallami kontrolującymi komunikację międzyprocesową na urządzeniach mobilnych.

- Stosowanie kontroli dostępu do danych mobilnych: Studenci nauczą się, jak ustanawiać i egzekwować kontrolę dostępu do danych w celu zabezpieczenia wrażliwych informacji na urządzeniach mobilnych.

Zalecana literatura

- Doherty, J., (2021), Wireless and Mobile Device Security 2nd Edition. Ta książka analizuje implikacje szybkiej integracji urządzeń mobilnych w środowisku komunikacyjnym organizacji, związane z tym obawy dotyczące bezpieczeństwa i sposoby ich łagodzenia.
- Russell, B., Van Duren, Drew., (2018), Practical Internet of Things Security - Second Edition: Design a security framework for Internet-connected Ecosystem
- Zdziarski, J. A. (2015). Hacking and Securing iOS Applications: Stealing Data, Hijacking Software, and How to Prevent It. O'Reilly Media, Inc.
    - Ta książka oferuje dogłębną analizę architektury bezpieczeństwa iOS, omawia wspólne podatności i dostarcza strategie zabezpieczania aplikacji na iOS.
- Fried, S. (2011). Mobile Device Security: A Comprehensive Guide to Securing Your Information in a Moving World. CyberAge Books.
    - Ten przewodnik jest niezbędny dla studentów i praktyków, którzy muszą zrozumieć specyficzne wyzwania bezpieczeństwa prezentowane przez urządzenia mobilne, które są coraz częściej używane zarówno w kontekstach osobistych, jak i zawodowych.

Te zasoby wspierają program nauczania, dostarczając zarówno podstawowej wiedzy, jak i specyficznych umiejętności wymaganych do zarządzania i zabezpieczania urządzeń mobilnych, zapewniając, że studenci są dobrze przygotowani do radzenia sobie z wyzwaniami związanymi z bezpieczeństwem mobilnym we współczesnych kontekstach organizacyjnych.

Rozdział 3 – Ocena higieny cyfrowej i mechanizmy informacji zwrotnej dla VET

Wprowadzenie

Ocena i informacja zwrotna są kluczowymi elementami procesu edukacyjnego, dostarczając zarówno instruktorom, jak i studentom niezbędnych wglądów w skuteczność nauczania i uczenia się. W kontekście programu nauczania Higieny Cyfrowej, solidne mechanizmy oceny i informacji zwrotnej są szczególnie istotne. Zapewniają one, że wiedza i umiejętności przekazywane studentom są nie tylko rozumiane i zapamiętywane, ale również stosowane w rzeczywistych scenariuszach, gdzie ryzyka związane z bezpieczeństwem cyfrowym są powszechne.

Ten rozdział ma na celu przedstawienie strategii i metodologii oceny wyników studentów oraz dostarczania konstruktywnej informacji zwrotnej w ramach programu Higieny Cyfrowej. Obejmuje to połączenie ocen wiedzy teoretycznej i praktycznych, ręcznych ocen.

Strategie Oceny

Oceny Formatywne

- **Quizy i krótkie testy:** Częste quizy i krótkie testy będą przeprowadzane w każdym module, aby ocenić zrozumienie kluczowych pojęć i dostarczyć natychmiastową informację zwrotną. Pomaga to w wzmocnieniu nauki i identyfikacji obszarów, w których studenci mogą potrzebować dodatkowego wsparcia.
- **Zadania praktyczne:** Studenci otrzymają zadania, które będą wymagały zastosowania wiedzy teoretycznej w praktycznych scenariuszach, takich jak konfigurowanie zapory sieciowej, projektowanie planu odzyskiwania danych lub wdrażanie protokołów szyfrowania.
- **Oceny koleżeńskie:** Obejmuje to studentów oceniających zadania lub projekty swoich kolegów. Oceny koleżeńskie mogą pomóc w rozwijaniu umiejętności krytycznego myślenia i analizy, ponieważ studenci uczą się krytykować rozwiązania cyberbezpieczeństwa na podstawie najlepszych praktyk.

Oceny Sumatywne

- **Egzaminy końcowe:** Kompletne egzaminy na końcu każdego modułu sprawdzą studentów z szerszego zakresu tematów omówionych w trakcie kursu. Egzaminy będą zawierały zarówno pytania wielokrotnego wyboru, jak i pytania esejowe, aby ocenić teoretyczne i praktyczne zrozumienie studentów.
- **Projekty końcowe:** Na końcu programu studenci będą realizować projekt końcowy, który obejmuje tworzenie lub zarządzanie kompleksowymi strategiami higieny cyfrowej dla hipotetycznych organizacji. Projekt ten będzie oceniany na podstawie różnych kryteriów, w tym innowacyjności, zastosowalności i zgodności z zasadami cyberbezpieczeństwa.

Ocena Ciągła

- **Przeglądy portfolio:** Studenci będą utrzymywać portfolio swoich prac i osiągnięć przez cały program. Portfolio te będą okresowo przeglądane przez instruktorów, aby ocenić postępy i dostarczyć spersonalizowaną informację zwrotną.
- **Samooceny:** Zachęcanie studentów do angażowania się w samoocenę może sprzyjać większej odpowiedzialności za własne uczenie się. Narzędzia samooceny i listy kontrolne będą dostarczane, aby pomóc studentom w ocenie ich zrozumienia i umiejętności.

Mechanizmy Informacji Zwrotnej

- **Informacja zwrotna od instruktorów:** Informacja zwrotna będzie dostarczana systematycznie dla wszystkich ocen, koncentrując się na mocnych i słabych stronach pracy studentów. Informacja zwrotna będzie terminowa, konkretna i konstruktywna, mająca na celu zachęcenie studentów do refleksji nad swoim uczeniem się i identyfikacji obszarów do poprawy.
- **Informacja zwrotna od kolegów:** W projektach grupowych i ocenach koleżeńskich studenci będą zachęcani do dostarczania informacji zwrotnych swoim kolegom. Informacja zwrotna będzie strukturyzowana, aby była konstruktywna i skoncentrowana na konkretnych kryteriach.
- **Automatyczna informacja zwrotna:** Dla niektórych rodzajów ocen, zwłaszcza quizów i niektórych ćwiczeń praktycznych, będą wykorzystywane systemy automatycznej informacji zwrotnej. Systemy te mogą dostarczyć natychmiastowe wyniki i wglądy, pozwalając na szybkie poprawki.

- **Pętle informacji zwrotnej:** Tworzenie pętli informacji zwrotnej w ramach programu nauczania, gdzie studenci mogą reflektować nad informacją zwrotną, poprawiać swoje prace i ponownie je zgłaszać do dalszej oceny, sprzyja postawie rozwoju i ciągłego doskonalenia.

Wdrażanie Informacji Zwrotnej w Rozwój Programu Nauczania

Informacja zwrotna uzyskana z tych różnych mechanizmów nie jest przeznaczona tylko dla studentów. Odgrywa również kluczową rolę w rozwoju programu nauczania:

- **Dostosowanie programu nauczania:** Regularne przeglądy danych dotyczących wyników studentów i informacji zwrotnej pomogą w identyfikacji obszarów programu nauczania, które mogą wymagać dostosowania lub ulepszeń.
- **Rozwój instruktorów:** Informacja zwrotna od studentów może również wskazywać na potrzeby rozwojowe instruktorów, wskazując obszary, w których mogą potrzebować więcej wsparcia lub szkolenia.

Wniosek

Mechanizmy oceny i informacji zwrotnej zaprojektowane dla programu nauczania Higieny Cyfrowej w instytucjach VET są integralne dla zapewnienia osiągnięcia celów edukacyjnych. Poprzez zastosowanie różnorodnych strategii oceny i wielokanałowych systemów informacji zwrotnej, program nie tylko skutecznie ocenia uczenie się studentów, ale również ciągle doskonali metody nauczania i projektowanie programu nauczania. Dynamiczne podejście zapewnia, że program nauczania pozostaje aktualny i skuteczny w przygotowywaniu studentów do radzenia sobie z rzeczywistymi wyzwaniami higieny cyfrowej.

Rozdział 4 – Dobre Praktyki z VET

Wprowadzenie

W dynamicznej dziedzinie higieny cyfrowej, teoretyczna wiedza połączona z praktycznymi zastosowaniami tworzy najbardziej efektywne środowisko nauki. Ten rozdział zagłębia się w dobre praktyki przyjęte przez instytucje Kształcenia i Szkolenia Zawodowego (VET), które z powodzeniem zintegrowały zasady higieny cyfrowej w swoich programach nauczania. Te studia przypadków służą jako punkty odniesienia do opracowywania i doskonalenia programów higieny cyfrowej, dostarczając

wglądu w skuteczne strategie i metodologie, które mogą być replikowane lub dostosowywane przez inne instytucje.

Studium Przypadku 1: Akademia CyberVET

Przegląd:

Akademia CyberVET jest znana z solidnego programu nauczania higieny cyfrowej, który łączy rygorystyczne akademickie podejście z zastosowaniami w realnym świecie. Ta instytucja stała się modelem, jak bezproblemowo integrować nowe technologie i najlepsze praktyki z zakresu cyberbezpieczeństwa w szkoleniu zawodowym.

Kluczowe Strategie:

- Partnerstwa z przemysłem: CyberVET nawiązał współpracę z wiodącymi firmami technologicznymi, aby zapewnić, że ich program nauczania jest zgodny z aktualnymi standardami i praktykami branżowymi. Te partnerstwa również ułatwiają gościnne wykłady, staże i dostęp do nowoczesnych technologii.
- Symulowane środowiska nauki: Akademia zainwestowała w stworzenie nowoczesnych symulowanych laboratoriów cyberbezpieczeństwa, w których studenci mogą bezpiecznie badać i neutralizować rzeczywiste zagrożenia cybernetyczne. To praktyczne doświadczenie jest bezcenne.

Rezultaty:

- Znaczący wzrost zatrudnialności studentów, z 90% absolwentów zdobywających pracę w dziedzinie cyberbezpieczeństwa w ciągu sześciu miesięcy od ukończenia studiów.
- Zwiększone zaangażowanie i satysfakcja studentów, przypisywane podejściu praktycznemu do nauki i bezpośredniemu zaangażowaniu przemysłu.

Studium Przypadku 2: TechBridge VET

Przegląd:

TechBridge VET wyróżnia się naciskiem na zarządzanie urządzeniami mobilnymi i bezpieczeństwo, obszary o rosnącym znaczeniu w dziedzinie higieny cyfrowej.

Kluczowe Strategie:

- Modułowy projekt programu nauczania: Program nauczania w TechBridge jest wysoce modułowy, pozwalając studentom dostosowywać ścieżki edukacyjne do swoich celów zawodowych i postępów technologicznych.
- Projekty społecznościowe: Studenci uczestniczą w programach zasięgu społecznościowego, gdzie stosują swoją wiedzę, aby pomóc lokalnym małym firmom w poprawie ich środków bezpieczeństwa cyfrowego.

Rezultaty:

- Projekty społecznościowe nie tylko zwiększyły praktyczne umiejętności studentów, ale także podniosły świadomość na temat cyberbezpieczeństwa wśród właścicieli małych firm lokalnych.
- Modułowe podejście doprowadziło do dużej elastyczności w edukacji, dostosowując się do szybkich zmian technologicznych i potrzeb studentów.

Studium Przypadku 3: Instytut SecurePath

Przegląd:

Instytut SecurePath zintegrował higienę cyfrową w swoich programach zawodowych, pokazując, jak cyberbezpieczeństwo jest fundamentalne dla różnych dyscyplin technicznych.

Kluczowe Strategie:

- Podejście interdyscyplinarne: Poprzez integrację lekcji higieny cyfrowej w programach takich jak opieka zdrowotna, technologia motoryzacyjna i zarządzanie biznesem, SecurePath zapewnia, że wszyscy studenci rozumieją znaczenie cyberbezpieczeństwa w swoich dziedzinach.
- Ciągła ocena programu nauczania: Instytut korzysta z systemu analitycznego opartego na sztucznej inteligencji do ciągłego oceniania i aktualizowania swojego programu nauczania w oparciu o najnowsze informacje o zagrożeniach cybernetycznych i trendy branżowe.

Rezultaty:

- Studenci z programów nietechnicznych kończą studia z solidnym zrozumieniem higieny cyfrowej, co czyni ich bardziej wszechstronnymi i atrakcyjnymi dla pracodawców.
- Ciągła ocena programu nauczania utrzymała SecurePath na czołowej pozycji w edukacji dotyczącej higieny cyfrowej, szybko dostosowując się do pojawiających się zagrożeń.

Wnioski dla Najlepszych Praktyk

Sukcesy tych instytucji ilustrują kilka najlepszych praktyk, które mogą być przyjęte lub dostosowane przez innych dostawców VET:

- Współpraca z przemysłem: Silne więzi z przemysłem nie tylko utrzymują aktualność programu nauczania, ale także zwiększają szanse na zatrudnienie studentów po ukończeniu studiów.
- Praktyczne zastosowanie: Praktyczna nauka poprzez laboratoria, symulacje lub projekty społecznościowe jest kluczowa dla skutecznego zrozumienia i zastosowania zasad higieny cyfrowej.
- Elastyczność i interdyscyplinarność: Elastyczne i interdyscyplinarne podejście zapewnia, że edukacja dotycząca higieny cyfrowej może szybko dostosować się do zmian i sprostać szerokiemu zakresowi obszarów zawodowych.
- Informacja zwrotna i ciągłe doskonalenie: Ongoing assessment and revision of the curriculum based on feedback from various stakeholders, including students, faculty, and industry partners, ensure the program's effectiveness and relevance

Studium Przypadku 4: DigitalDefenders College

Przegląd:

DigitalDefenders College jest znane z wyspecjalizowanego podejścia do nauczania cyberbezpieczeństwa, ze szczególnym naciskiem na etyczne hakowanie i techniki cyfrowej kryminalistyki. Ta instytucja VET jest zaangażowana w produkowanie wykwalifikowanych profesjonalistów gotowych do radzenia sobie ze złożonościami zagrożeń cybernetycznych we współczesnym krajobrazie cyfrowym.

Kluczowe Strategie:

- Moduły Etycznego Hakowania: Włączając obszerne moduły dotyczące etycznego hakowania, uczelnia dostarcza studentom umiejętności identyfikowania i wykorzystywania luk w systemach, wszystko w kontrolowanych, etycznych i legalnych ramach.
- Rzeczywista Kryminalistyka Cybernetyczna: Studenci biorą udział w praktycznych ćwiczeniach z zakresu cyfrowej kryminalistyki, które symulują scenariusze naruszenia danych w

rzeczywistych warunkach, pomagając im zrozumieć, jak śledzić, analizować i łagodzić skutki naruszeń.

Rezultaty:

- Absolwenci są znani z proaktywnego podejścia do cyberbezpieczeństwa, wielu z nich zabezpiecza stanowiska w sektorach o wysokich stawkach, takich jak finanse i administracja rządowa.
- Praktyczne doświadczenie w etycznym hakowaniu i cyfrowej kryminalistyce prowadzi do wysokiego zaangażowania wśród studentów, co sprzyja głębokiemu zrozumieniu praktycznych implikacji zagrożeń cybernetycznych.

Studium Przypadku 5: Instytut InnovateTech

Przegląd:

Instytut InnovateTech wyróżnia się integracją zaawansowanych trendów technologicznych, takich jak sztuczna inteligencja (AI) i uczenie maszynowe (ML), w swoim programie higieny cyfrowej. To podejście przygotowuje studentów na coraz bardziej napędzane przez AI środowisko cyberbezpieczeństwa.

Kluczowe Strategie:

- Rozwiązania Bezpieczeństwa Napędzane przez AI: Nauczanie studentów wykorzystania AI i ML w opracowywaniu zaawansowanych środków bezpieczeństwa cybernetycznego, co pozwala wyprzedzać cyberprzestępców również korzystających z zaawansowanych technologii.
- Projekty Współpracy z Firmami Technologicznymi: Studenci pracują nad projektami we współpracy z firmami technologicznymi, tworząc rozwiązania bezpieczeństwa oparte na AI, co daje im wgląd w wyzwania i wymagania branży w czasie rzeczywistym.

Rezultaty:

- Studenci opracowali kilka narzędzi bezpieczeństwa opartych na AI, które zostały przyjęte przez firmy partnerskie, co pokazuje ich bezpośredni wpływ na obecne rozwiązania w zakresie cyberbezpieczeństwa.

- Integracja AI i ML w edukację z zakresu higieny cyfrowej nie tylko wzmocniła program nauczania, ale także znacząco zwiększyła zatrudnialność studentów w branżach napędzanych technologią.

Podsumowanie Dobrych Praktyk

Te dodatkowe studia przypadków z DigitalDefenders College i Instytutu InnovateTech dodatkowo wzmacniają krytyczne aspekty udanego programu nauczania higieny cyfrowej w instytucjach VET:

- Specjalizacja i Zaawansowane Szkolenia: Programy oferujące specjalistyczne szkolenia w obszarach o dużym zapotrzebowaniu, takich jak etyczne hakowanie i AI, mogą znacznie zwiększyć znaczenie i atrakcyjność programu nauczania.
- Zastosowanie w Rzeczywistym Świecie: Praktyczne zastosowanie zdobytych umiejętności, czy to poprzez cyfrową kryminalistykę, czy projekty współpracy z przemysłem, zapewnia, że studenci nie tylko znają teoretyczne koncepcje, ale także są biegli w ich stosowaniu w rzeczywistych sytuacjach.
- Innowacyjny i Przyszłościowy Program Nauczania: Utrzymywanie programu nauczania zgodnego z najnowszymi osiągnięciami technologicznymi przygotowuje studentów na pojawiające się zagrożenia i możliwości, co czyni ich cennymi zasobami w każdej roli w zakresie cyberbezpieczeństwa, którą podejmą po ukończeniu studiów.
- Przykłady te ilustrują różnorodne strategie, które można wdrożyć w celu skutecznego zwiększenia edukacji w zakresie higieny cyfrowej. Każda z nich w unikalny sposób przyczynia się do osiągnięcia nadrzędnego celu, jakim jest kształcenie wykwalifikowanych specjalistów, którzy będą potrafili chronić zasoby cyfrowe w coraz bardziej złożonym środowisku cybernetycznym.

Wnioski

Pięć studiów przypadków zbadanych przez Akademię CyberVET, TechBridge VET, Instytut SecurePath, DigitalDefenders College i Instytut InnovateTech dostarcza bogatej mozaiki udanych strategii i podejść do integracji higieny cyfrowej w programach Kształcenia i Szkolenia Zawodowego (VET). Każda instytucja, ze swoim unikalnym podejściem i metodologią, podkreśla kluczową rolę praktycznej, zorientowanej na przemysł i innowacyjnej edukacji w przygotowywaniu studentów do nawigacji w złożonościach cyberbezpieczeństwa w nowoczesnym cyfrowym świecie.

Kluczowe Wnioski i Najlepsze Praktyki

- Współpraca i Zgodność z Przemysłem: Wspólnym motywem we wszystkich studiach przypadków jest znaczenie utrzymywania silnych więzi z liderami i firmami branżowymi. Te partnerstwa nie tylko utrzymują aktualność programu nauczania z najnowszymi technologiami i praktykami, ale także zwiększają zatrudnialność studentów poprzez staże, projekty w rzeczywistym świecie i ekspozycję na standardy branżowe.
- Praktyczne Doświadczenie: Każda instytucja kładzie nacisk na potrzebę praktycznego zastosowania zdobytych koncepcji. Czy to przez laboratoria cybernetyczne, symulowane środowiska, czy rzeczywiste śledztwa kryminalistyczne, praktyczne doświadczenie jest kluczowe. Nie tylko utrwala teoretyczną wiedzę, ale także przygotowuje studentów na rzeczywiste wyzwania, z którymi będą się spotykać w swoich karierach.
- Specjalistyczne Moduły i Zaawansowane Szkolenia: Instytucje takie jak DigitalDefenders College podkreślają korzyści oferowania specjalistycznych szkoleń w obszarach takich jak etyczne hakowanie i cyfrowa kryminalistyka. Podobnie, nacisk InnovateTech Institute na rozwiązania bezpieczeństwa napędzane przez AI ilustruje przewagę integracji najnowocześniejszych technologii w programie nauczania, przygotowując studentów na przyszłe trendy i innowacje w cyberbezpieczeństwie.
- Interdyscyplinarne i Elastyczne Podejścia do Nauki: Integracja higieny cyfrowej w różnych programach zawodowych w Instytucie SecurePath ukazuje wartość podejścia interdyscyplinarnego, które poszerza zastosowanie i znaczenie edukacji z zakresu cyberbezpieczeństwa. Co więcej, modułowy projekt programu nauczania w TechBridge VET pozwala na większą elastyczność, dostosowując się do szybkich zmian technologicznych i różnorodnych zainteresowań studentów.
- Ciągłe Doskonalenie i Adaptacja: Wykorzystanie analityki opartej na AI przez Instytut SecurePath do ciągłej oceny programu nauczania oraz dynamiczne protokoły aktualizacji w InnovateTech Institute podkreślają znaczenie ciągłej oceny i adaptacji. Utrzymywanie programu nauczania odpowiedzią na ewoluujące zagrożenia cybernetyczne zapewnia, że programy edukacyjne pozostają aktualne i skuteczne.

Synteza wglądów z tych różnorodnych instytucji VET ujawnia, że skuteczność programu nauczania higieny cyfrowej opiera się na zdolności do łączenia wiedzy teoretycznej z umiejętnościami praktycznymi, dostosowywaniu się do postępów technologicznych i pielęgnowaniu silnych więzi z przemysłem. Te elementy są kluczowe w przygotowywaniu studentów nie tylko do spełnienia bieżących wymagań w dziedzinie cyberbezpieczeństwa, ale także do innowacji i przywództwa w

obliczu przyszłych wyzwań. To holistyczne podejście nie tylko wzmacnia doświadczenie edukacyjne, ale także znacznie zwiększa zatrudnialność i gotowość absolwentów do ochrony zasobów cyfrowych w globalnie połączonym świecie. Jak instytucje VET nadal ewoluują i udoskonalają swoje programy, wnioski wyciągnięte z tych studiów przypadków dostarczają cennych wzorców do opracowywania solidnych, kompleksowych programów nauczania higieny cyfrowej, które są przygotowane do sprostania wyzwaniom krajobrazu cyberbezpieczeństwa jutra.

Źródła

1. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson Education.
2. Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security* (6th ed.). Cengage Learning.
3. Katz, J., & Lindell, Y. (2014). *Introduction to Modern Cryptography* (2nd ed.). CRC Press.
4. Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. Wiley.
5. Chapple, M., Seidl, D., & Stewart, J. M. (2018). *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide* (8th ed.). Sybex.
6. Allen, J. H., Barnum, S., Ellison, R., McGraw, G., & Viega, J. (2008). *Software Security Engineering: A Guide for Project Managers*. Addison-Wesley Professional.
7. Conklin, W. A., White, G., Cothren, C., Williams, D., & Davis, R. (2016). *Principles of Computer Security: CompTIA Security+ and Beyond* (5th ed.). McGraw-Hill Education.
8. Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in Computing* (5th ed.). Prentice Hall.
9. Bejtlich, R. (2013). *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*. No Starch Press.
10. Zdziarski, J. A. (2015). *Hacking and Securing iOS Applications: Stealing Data, Hijacking Software, and How to Prevent It*. O'Reilly Media.
11. Tipton, H. F., & Nozaki, M. K. (2013). *Official (ISC)2 Guide to the CISSP CBK* (4th ed.). CRC Press.

12. Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Auerbach Publications.

13. Kim, D., & Solomon, M. G. (2016). *Fundamentals of Information Systems Security* (3rd ed.). Jones & Bartlett Learning.

14. Caloyannides, M. A. (2010). *Privacy Protection and Computer Forensics* (2nd ed.). Artech House.

15. Toigo, J. W. (2009). *Disaster Recovery Planning: Preparing for the Unthinkable* (3rd ed.). Prentice Hall.

16. Ross, R. S. (2013). *Managing Information Security Risks: The OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Approach*. Addison-Wesley.

17. Bodmer, C., Kilger, M., Carpenter, G., & Jones, J. (2012). *Reverse Deception: Organized Cyber Threat Counter-Exploitation*. McGraw-Hill Osborne Media.

18. Enck, W. (2011). *Understanding Android Security*. IEEE Security & Privacy Magazine.

19. Anton, A. I., & Earp, J. B. (2004). *A Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts*. Academy of Management Review.

20. Liska, A., & Gallo, T. (2016). *Rethinking the Security of the Internet of Things*. Elsevier.

21. Clarke, N. L., & Furnell, S. M. (2016). *Cybersecurity Education: Strategies and Best Practices*. Springer.

22. Bishop, M. (2018). *Computer Security: Art and Science*. Addison-Wesley.

23. Eckert, J. W. (2017). *CompTIA Linux+ Guide to Linux Certification*. Cengage Learning.

24. Skoudis, E., & Zeltser, L. (2019). *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Prentice Hall.

25. Easttom, C. (2019). *Modern Cryptography: Applied Mathematics for Encryption and Information Security*. McGraw-Hill Education.

26. Kurose, J. F., & Ross, K. W. (2017). *Computer Networking: A Top-Down Approach* (7th ed.). Pearson.

27. Andress, J., & Winterfeld, S. (2014). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Syngress.

28. Goodrich, M. T., & Tamassia, R. (2019). *Introduction to Computer Security*. Pearson.

29. Dafoulas, G. A., & Maia, C. (2015). *Global Security, Safety, and Sustainability: Tomorrow's Challenges of Cyber Security*. Springer.

Zasoby i strony internetowe:

- Cybersecurity & Infrastructure Security Agency (CISA)
    - Strona internetowa: https://www.cisa.gov/
    - CISA dostarcza bogactwo zasobów na temat najlepszych praktyk i zagrożeń związanych z cyberbezpieczeństwem, oferując wytyczne, narzędzia i alerty, które są kluczowe dla edukacji i świadomości w zakresie cyberbezpieczeństwa.
- National Institute of Standards and Technology (NIST) Cybersecurity Framework
    - Strona internetowa: https://www.nist.gov/cyberframework
    - Ramy NIST są szeroko stosowanym standardem zarządzania ryzykiem cyberbezpieczeństwa i dostarczają uporządkowane wytyczne, które można zintegrować z programami nauczania.
- Open Web Application Security Project (OWASP)
    - Strona internetowa: https://owasp.org/
    - OWASP to internetowa społeczność dostarczająca bezpłatne i otwarte zasoby na temat bezpieczeństwa aplikacji internetowych, w tym narzędzia, standardy i najlepsze praktyki.
- SANS Institute
    - Strona internetowa: https://www.sans.org/
    - Uznany lider w szkoleniu z zakresu cyberbezpieczeństwa, Instytut SANS oferuje różnorodne prace badawcze, materiały szkoleniowe i wytyczne dotyczące bezpieczeństwa.
- Krebs on Security
    - Strona internetowa: https://krebsonsecurity.com/
    - Prowadzony przez dziennikarza Briana Krebsa, ten blog oferuje dogłębne wiadomości i śledztwa dotyczące bezpieczeństwa, koncentrując się na najnowszych zagrożeniach i naruszeniach.

- Infosec Institute
    - Strona internetowa: https://resources.infosecinstitute.com/
    - Instytut Infosec dostarcza zasoby i szkolenia skoncentrowane na bezpieczeństwie informacji, w tym wnikliwe artykuły i aktualizacje branżowe.
- The Hacker News
    - Strona internetowa: https://thehackernews.com/
    - Internetowy magazyn wiadomości o cyberbezpieczeństwie, The Hacker News, oferuje najnowsze informacje na temat aktualnych zagrożeń i innowacji w zakresie cyberbezpieczeństwa.
- Blog Bruce'a Schneiera
    - Strona internetowa: https://www.schneier.com/
    - Bruce Schneier to uznany specjalista ds. bezpieczeństwa, którego blog dostarcza wglądów w kwestie bezpieczeństwa i prywatności w cyfrowym świecie.

Moduł 3: Wdrażanie i utrzymanie

Rozdział 1 - Budowanie kultury higieny cyfrowej w startupach i instytucjach VET

Czym jest kultura higieny cyfrowej?

Jak odkryliśmy w poprzednich modułach, higiena cyfrowa to termin, który pojawił się na początku lat 2000, aby wyjaśnić zasady bezpiecznych, uporządkowanych i etycznych praktyk cyfrowych, które mają na celu skuteczną ochronę danych, prywatności i integralności systemu. W tym module zbadamy systemowe zastosowanie tych zasad na większą skalę, dostosowane do dostawców VET w całej Europie, oraz zaproponujemy sugestie dotyczące budowania lepszej kultury higieny cyfrowej, która zainspiruje innowacje i entuzjazm w organizacjach.

Czym dokładnie jest kultura higieny cyfrowej? Podobnie jak wiele innych kultur sieciowych, które dążą do sukcesu organizacji, czy to skoncentrowanej na strukturze czy eksploracji, kultura higieny cyfrowej skupia się wokół wspólnego myślenia. W tym podejściu każdy członek wierzy w misję organizacji i

formułuje strategie oparte na zbiorowej odpowiedzialności i integracji bezpiecznych praktyk cyfrowych. Przeanalizujmy, jak kultura higieny cyfrowej może być rozszerzona od poziomu przywództwa do grup roboczych i każdego indywidualnie.

Rozwój kultury higieny cyfrowej na poziomie przywództwa

W erze post-Covid, gdzie praca zdalna stała się nową normą, a podatności w świecie cyfrowym mogą być zarówno emocjonalne, jak i techniczne (np. ataki socjotechniczne, które mogą przybrać formę emocjonalnej historii będącej próbą wyłudzenia danych), sytuacja wymaga nie tylko menedżera, ale lidera, który potrafi efektywnie nawigować po złożonościach świata cyfrowego, jednocześnie demonstrując praktyki higieny cyfrowej jako integralną część wartości organizacyjnych. Poniżej przedstawiono kilka ważnych punktów, w których lider może wspierać bezpieczną i wspierającą kulturę higieny cyfrowej:

- **Zachęcanie do elastyczności organizacyjnej [4]:**

Liderzy muszą zapewnić, że ich organizacje są dostosowane do postępów cyfrowych oraz wyzwań, które mogą wynikać z praktyk cyfrowych. Aby kierować swoimi zespołami przez te zmiany, wszyscy liderzy powinni najpierw zrozumieć swoje stanowisko, decyzje i emocje w różnych okolicznościach, zanim zmotywują innych przez wspólny cel.

- **Radzenie sobie z wyzwaniami zarządzania [5]:**

Liderzy w każdej organizacji muszą rozpoznać potencjalne wyzwania zarządzania wynikające z cyfryzacji, takie jak zagrożenia cyberbezpieczeństwa, problemy z prywatnością, luki w umiejętnościach lub kwestie wynikające z pracy zdalnej. Powinni być gotowi ocenić zdolności swoich zespołów do utrzymania higieny cyfrowej. Wymaga to pewnego poziomu wiedzy technicznej; dlatego zaleca się, aby liderzy mogli skutecznie rozumieć i artykułować problemy techniczne ze swoimi zespołami.

- **Tworzenie relacji i procesów współpracy [6]:**

Liderzy w każdej organizacji powinni tworzyć relacje z szerokim zakresem interesariuszy zarówno na poziomie wewnętrznym, jak i zewnętrznym. Wymaga to od nich wysokiej koordynacji i odpowiedzialności, a także zachęcania do silnego poczucia współpracy między pracownikami i innymi interesariuszami.

- **Inwestowanie w edukację i szkolenia [7]:**

Liderzy w każdej organizacji powinni inwestować w ciągłą edukację i szkolenia dla siebie i swoich pracowników, aby być na bieżąco z najnowszymi praktykami higieny cyfrowej i technologiami. Niektóre firmy z branży cyberbezpieczeństwa, jak również niektóre organy rządowe w Europie, takie jak Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA), oferują różnorodne kursy online i stacjonarne na temat świadomości cyberbezpieczeństwa i zarządzania kryzysowego.

Rozwój kultury higieny cyfrowej na poziomie grupowym

Po opracowaniu mapy drogowej strategii higieny cyfrowej, obawy dotyczące cyberbezpieczeństwa każdej organizacji powinny być również omówione na poziomie grupowym. Grupy robocze, w tym działy, programy, studenci lub menedżerowie projektów, mogą znacząco przyczynić się do promowania kultury higieny cyfrowej w swoich instytucjach, przy wsparciu i współpracy odpowiednich Zespołów Reagowania na Incydenty Komputerowe (CERT).

Poniżej przedstawiono kilka ważnych punktów, które każda grupa robocza może wykorzystać, aby stworzyć kulturę higieny cyfrowej:

- **Ustanawianie efektywnej komunikacji w grupach:**

Jedną z efektywnych metod komunikacji w grupach jest rozpoczynanie spotkań lub kursów od dyskusji związanych z cyberbezpieczeństwem. Każda grupa może przeznaczyć pięć minut na początku na pytania członków. Podczas tych spotkań można ustanowić zasady i wytyczne dotyczące sposobu korzystania z urządzeń w działach lub salach lekcyjnych, aby wzmocnić kulturę higieny cyfrowej. Inną pomocną metodą dla grup może być wymóg podpisów elektronicznych lub kodów QR dla udostępnianych dokumentów, które mogą określić, czy e-mail lub transakcja cyfrowa została dokonana przez członka grupy. Innym czynnikiem, na który należy zwrócić uwagę, jest wybór bezpieczniejszych opcji przechowywania, takich jak chmura, zamiast pamięci USB.

- **Ustanawianie efektywnych metod dokumentowania ataków cyfrowych:**

Dokumentowanie ataków cyfrowych jest krytycznym aspektem utrzymania cyberbezpieczeństwa. Wszystkie organizacje powinny jasno wyjaśnić wytyczne dotyczące dokumentacji. Niektóre procedury opracowywania dokumentacji dla ataków cyfrowych mogą być następujące:

Krok 1: Prowadzenie zorganizowanego dziennika: W przypadku incydentu, zachęcaj każdego członka zespołu do wprowadzenia danych, takich jak data, godzina, adres e-mail, odpowiednie linki, nazwy kont i metadane.

Krok 2: Wdrażanie ustrukturyzowanych szablonów: Używaj gotowych szablonów do dokumentowania incydentów naruszenia danych. Na przykład, możesz użyć szablonu dziennika incydentów z Access Now, międzynarodowej NGO, która ma na celu ochronę cyfrowych praw obywatelskich ludzi na całym świecie.

Krok 3: Korzystanie z różnych formatów dokumentacji: Zachęcaj członków swojego zespołu do korzystania z różnych formatów dokumentowania ich problemów. Mogą korzystać z Wayback Machine Internet Archive, aby zapisać stronę internetową lub narzędzi do rejestrowania wideo, aby nagrać wideo jako dowód swoich problemów.

Krok 4: Bezpieczne przechowywanie informacji: Twórz kopie zapasowe na swoich urządzeniach, w zaufanych opcjach przechowywania i chroń swoje pliki za pomocą szyfrowania, jeśli to możliwe.

- **Ustanawianie regularnych ocen higieny cyfrowej:**

Przeprowadzanie regularnych audytów i ocen ryzyka może pomóc zidentyfikować podatności i zapewnić, że praktyki higieny cyfrowej są przestrzegane. Niektóre sposoby ustanawiania regularnych ocen higieny cyfrowej to:

  - Opracowanie rutyny nawyków cyberhigieny, takich jak skanowanie w poszukiwaniu wirusów, zmiana haseł, aktualizacja oprogramowania i czyszczenie dysków twardych.
  - Korzystanie z odpowiednich narzędzi, takich jak zapora sieciowa, oprogramowanie antywirusowe, szyfrowanie lub rozwiązania do tworzenia kopii zapasowych.
  - Szukanie pomocy od niezawodnych usług, które zapewniają skanowanie podatności, skanowanie aplikacji internetowych i oceny phishingu.

Rozwój kultury higieny cyfrowej na poziomie indywidualnym

Czynniki ludzkie są jednym z najsłabszych elementów cyberbezpieczeństwa. Przykłady błędów ludzkich w zakresie praktyk cyfrowych mogą obejmować złe zarządzanie hasłami, przypadkowe usunięcie danych lub padanie ofiarą phishingu lub innych oszustw socjotechnicznych. Jednak zawsze można zredukować ryzyko, zwracając uwagę i przestrzegając praktyk higieny cyfrowej.

Oto kilka kluczowych punktów, w których każda osoba może przyczynić się do stworzenia kultury higieny w organizacji:

- **Uważaj na swój cyfrowy ślad:**

Nawigacja po przestrzeniach online może być skomplikowana, a ludzie powinni być czujni na swój cyfrowy ślad. Mechanizmy śledzenia przeglądarek internetowych, dostawców e-maili, aplikacji mobilnych, wyszukiwarek i platform mediów społecznościowych mogą naruszać prywatność osobistą. Aby zwiększyć bezpieczeństwo w codziennych działaniach w sieci, rozważ te kroki:

- **Krok 1:** Uważaj na informacje udostępniane na platformach społecznościowych i wylogowuj się z kont w mediach społecznościowych, ponieważ te serwisy mogą analizować twoje konta nawet, gdy ich nie używasz.
- **Krok 2:** Korzystaj z przeglądarek dbających o prywatność, takich jak duckduckgo.com i startpage.com, które priorytetowo traktują prywatność i dostarczają użytkownikom wyniki wyszukiwania bez personalizowanego śledzenia.
- **Krok 3:** Zwracaj uwagę na aktywność online swoich kręgów społecznych: Uświadom sobie, że obecność online przyjaciół i rodziny może wpływać na twoje bezpieczeństwo cyfrowe. Doradzaj im w sprawach bezpiecznych praktyk online.
- **Krok 4:** Zwracaj uwagę na ustawienia smartfona: Podobnie jak twoje laptopy, twoje smartfony są również kluczowym aspektem twojej aktywności online. Priorytetowo traktuj bezpieczeństwo, konsekwentnie wylogowując się z aplikacji, które zawierają wrażliwe informacje. Wylogowywanie się będzie również korzystne dla twojej produktywności w pracy. Badanie dotyczące monitorowania użycia smartfonów wykazało, że wylogowywanie się i rezygnowanie z plików cookie śledzących sprawiło, że uczestnicy spędzali mniej czasu w każdej sesji.

- **Zwracaj uwagę na aktualizacje oprogramowania:**

Częste aktualizacje oprogramowania są niezbędne dla dobrej higieny cyfrowej, ponieważ brak aktualizacji oprogramowania lub przeglądarek internetowych może prowadzić do poważnych podatności. Przykład z 2021 roku, kiedy Adobe ogłosiło zakończenie wsparcia dla Flash, z uwagi na luki bezpieczeństwa, które w dużej mierze wpłynęły na ich decyzję. Luki te obejmowały możliwość efektywnego obejścia środków bezpieczeństwa przeglądarek internetowych. Zespoły CERT musiały rozwiązać te problemy. Jak pokazuje ten przykład, zwracanie uwagi na aktualizacje jest ważną częścią ochrony oprogramowania i aplikacji przed podatnościami.

- **Używaj silnych haseł:**

Słabe hasła, które są łatwe do odgadnięcia, mogą narazić osoby i organizacje na ryzyko naruszenia danych. Dlatego nie używaj swojego imienia ani daty urodzenia jako hasła. Najsilniejsze hasła to te,

które będą łatwe do zapamiętania, ale trudne do złamania. Oto kilka wskazówek, jak tworzyć silne hasła i jak je zapamiętać:

  - **Krok 1:** Skonstruuj zdanie z różnymi symbolami, które będzie zawierać duże i małe litery. Na przykład zdanie "Lubię jabłka, ale nie cierpię pomarańczy" można przekształcić w "LJ@bnp0"
  - **Krok 2:** Używaj uwierzytelniania dwuskładnikowego: Oprócz tworzenia solidnych haseł, zwiększ swoje bezpieczeństwo dzięki uwierzytelnianiu dwuskładnikowemu (2FA). Uwierzytelnianie dodaje dodatkową warstwę bezpieczeństwa, wymagając drugiego kroku weryfikacji, takiego jak kod wysłany na twoje urządzenie mobilne, co zmniejsza ryzyko nieautoryzowanego dostępu.
  - **Krok 3:** Zachowaj poufność swoich haseł i przechowuj je bezpiecznie, jeśli to konieczne, za pomocą menedżera haseł lub aplikacji uwierzytelniającej, takich jak Dashlane lub 1Password. (Pamiętaj jednak, że bezpieczeństwo tych menedżerów jest tylko tak mocne, jak ich najsłabsze ogniwo!)
  - **Krok 4:** Zapewnij bezpieczeństwo swoich haseł, regularnie je aktualizując.
- **Ostrożne klikanie: Uważaj na phishing:**

Phishing ma na celu oszukiwanie ludzi, aby przekazywali swoje wrażliwe informacje, udając zaufane źródło. Phishing to poważne przestępstwo. Jeśli oszuści oszukają ludzi, aby przekazali swoje dane osobowe, mogą uzyskać dostęp do ich kont e-mail, bankowych lub mediów społecznościowych. Dlatego jeśli coś wygląda trochę podejrzanie lub może e-mail prosi cię o zweryfikowanie danych osobowych, zwłaszcza z załącznikiem lub linkiem, który zachęca do kliknięcia, najpierw zaufaj swoim instynktom i zastanów się, zanim klikniesz.

Rozdział 2 - Monitorowanie, przegląd i ciągłe doskonalenie praktyk higieny cyfrowej

Myśl o swojej obecności cyfrowej jak o cennym zasobie, takim jak twój dom czy samochód. Tak jak wymagasz regularnych sesji konserwacyjnych, aby twój samochód czy dom były bezpieczne i funkcjonalne, tak samo ważne jest regularne sprawdzanie praktyk higieny cyfrowej, aby stale utrzymywać swoje systemy w bezpieczeństwie i funkcjonalności. W tym rozdziale przyjrzymy się

praktykom, które możesz realizować na poziomie instytucjonalnym i indywidualnym, aby utrzymać swoje kompetencje na bieżąco wraz z rozwojem technologii.

Praktyki na poziomie instytucjonalnym

Oto niektóre narzędzia i metody, które mogą być pomocne w monitorowaniu, ocenianiu i doskonaleniu higieny cyfrowej na poziomie instytucjonalnym.

- **Znajdź najnowsze przepisy UE:**

Zrozumienie i wdrażanie najnowszych przepisów pomaga instytutom zidentyfikować najważniejsze problemy i odpowiednio działać, aby zmniejszyć zagrożenia i wykorzystać korzyści.

Jednym z najpoważniejszych wyzwań, które niepokoiły decydentów, jest sztuczna inteligencja (AI). 9 grudnia 2023 r. Unia Europejska wprowadziła nowe prawo zwane „AI Act", które ma na celu „wykorzystanie potencjalnych korzyści z technologii, przy jednoczesnej ochronie przed możliwymi ryzykami, takimi jak automatyzacja miejsc pracy". Śledzenie najnowszych przepisów Unii Europejskiej dotyczących AI jest kluczowe dla odpowiedzialnych i uprawnionych praktyk cyfrowych. Możesz zapoznać się z aktualizowanymi przepisami, takimi jak AI Act, online na stronie legislacji Unii Europejskiej, aby zapewnić zgodność z wytycznymi i uniknąć potencjalnych implikacji prawnych.

- **Kontrole bezpieczeństwa:**

Przeprowadzanie kompleksowego przeglądu ustawień bezpieczeństwa jest kluczowe w zakresie monitorowania skuteczności wytycznych dotyczących higieny cyfrowej. Możesz korzystać z rutynowych kontroli bezpieczeństwa Google i Facebooka, które prowadzą cię przez środki ochrony prywatności, uprawnienia i kontrolę nad najnowszymi działaniami. Możesz także korzystać z internetowych źródeł, które pozwalają przeszukiwać wiele naruszeń danych, takich jak haveibeenpwnd.com, aby być świadomym ryzyk i częstotliwości naruszeń danych.

- **Analiza SWOT:**

SWOT to akronim od Strengths (Mocne strony), Weaknesses (Słabe strony), Opportunities (Szanse) i Threats (Zagrożenia). Jest to metoda analizy strategicznej, która tworzy mapę drogową do określenia pozycji każdej organizacji i strategii na przyszły rozwój.

Oto kilka wskazówek do zapamiętania podczas przeprowadzania analizy SWOT dla twojej organizacji według badania na temat gotowości firm do cyfryzacji:

1. **Przygotowanie do analizy SWOT:**

   a. Rozpocznij z celem: Rozważ cel i długoterminowe skutki stosowania analizy SWOT.

   b. Określ obszary do analizy: Zidentyfikuj konkretne obszary związane z Kulturą Higieny Cyfrowej, np. świadomość pracowników, przestrzeganie protokołów bezpieczeństwa, infrastruktura itp.

   c. Przydziel zespoły do określonych obszarów: Stwórz zespoły ekspertów w obszarach, które chcesz analizować, i upewnij się, że wszystkie zespoły są zgodne co do metodologii przeprowadzania analizy.

2. **Analiza mocnych i słabych stron:**

   a. Zidentyfikuj swoje mocne i słabe strony: Mocne i słabe strony organizacji to oznaki czynników wewnętrznych, które pokazują skuteczność i nieskuteczność danej organizacji. Ważne jest, aby uwzględnić uzasadnienia dla decyzji dotyczących danego czynnika jako słabości (np. przestarzałe aplikacje mogą być uważane za słabość ze względu na podatność systemu na ataki).

   b. Określ istotność zidentyfikowanych problemów: Określenie, co jest słabością, a co mocną stroną, może być mylące. Badacze sugerują użycie metody „100 punktów” do oceny i priorytetyzacji. Każdy członek zespołu może przydzielić 100 punktów mocnej lub słabej stronie, a im więcej punktów przydzielonych, tym bardziej znacząca jest uważana. Po przydzieleniu punktów przez wszystkich członków zespołu, zespół uśrednia je, aby określić ich ogólną istotność.

3. **Analiza szans i zagrożeń:**

   a. Oceń istotność i prawdopodobieństwo zagrożeń, próbując zorganizować je w kategorie: ekonomiczne, społeczne, polityczne, technologiczne i środowiskowe.

   b. Oblicz szanse związane z każdym rozwojem. Mogą to być zasoby finansowe, zwiększone zainteresowanie społeczne lub międzynarodowe możliwości.

4. **Rozwój macierzy SWOT:** Wybierz mocne strony, słabości, szanse i zagrożenia, i pogrupuj je według największego znaczenia dla Kultury Higieny Cyfrowej twojej organizacji. Opracuj plany działania na podstawie zidentyfikowanych strategii, które mogą: (1) koncentrować się na korygowaniu słabości, korzystając z możliwości, (2) koncentrować się na wykorzystaniu mocnej strony do skorzystania z szansy, (3) koncentrować się na minimalizowaniu słabości, aby uniknąć zagrożenia, lub (4) koncentrować się na wykorzystaniu mocnej strony do zapobieżenia zagrożeniu.
5. **Przegląd wyników:** Regularnie przeglądaj postęp wdrożonych strategii i okresowo powtarzaj analizę SWOT, aby dostosować się do nowych wydarzeń w krajobrazie cyfrowym.

- **Regularne kopie zapasowe:**

  Kopie zapasowe są niezbędne, gdy istnieje potrzeba odzyskania wrażliwych informacji, w przypadku utraty hasła, incydentów technicznych itp. Czasami możliwe jest również monitorowanie przyczyn awarii systemu, przeglądając luki w zabezpieczeniach lub błędy w systemie. Korzystanie z systemu kopii zapasowych typu open-source, takiego jak UrBackUp, który pozwala na przechowywanie kopii dokumentów, może być cennym narzędziem do monitorowania i przeglądu praktyk higieny cyfrowej w przypadku awarii.

Praktyki na poziomie indywidualnym

Każda osoba odgrywa znaczącą rolę w rozwijaniu praktyk higieny cyfrowej, a liczne kroki można podjąć, aby przeglądać, monitorować i rozwijać istniejące praktyki. Oto kilka sposobów na poprawę higieny cyfrowej na poziomie indywidualnym.

- **Świadomość i edukacja:**

Zrozumienie cyfrowej literacji nie polega tylko na znajomości narzędzi i metod, ale także na zrozumieniu ciągle ewoluującego krajobrazu technologicznego. Edukacja na temat zagrożeń online i pozostawanie na bieżąco może być osiągnięte przez udział w ciągłych możliwościach edukacyjnych, takich jak Kursy Cyfrowej Wiedzy Microsoftu, w których uczestnicy mogą nauczyć się podstaw cyfrowej wiedzy, takich jak praca z komputerem, a także zaawansowanych kompetencji, takich jak tworzenie treści online. Podobnie badacze podkreślają znaczenie nauczania o literacji medialnej oraz bezpiecznym i odpowiedzialnym korzystaniu z internetu, które powinno odzwierciedlać realne doświadczenia i zainteresowania jednostek.

- **Odpowiedzialne zachowanie online:**

Nasze zachowanie online ma realne konsekwencje. Jak podkreślono w badaniach akademickich, ważne jest angażowanie się w etyczne działania online, jak również bycie cyfrowo kompetentnym. Odpowiedzialne zachowanie online obejmuje uczestnictwo w dyskusjach online z szacunkiem i wrażliwością. Ponadto, świadomość polityk cyfrowych przyczynia się do bezpieczniejszej i bardziej szanującej społeczności online. Jeśli nie jesteś pewien, czy twoje działania cyfrowe są zgodne z dobrymi praktykami, możesz skorzystać z przewodnika dobrego cyfrowego obywatela Uniwersytetu Michigan.

- **Przegląd i adaptacja:**

Podobnie jak każdy aspekt świata cyfrowego, krajobraz technologiczny jest dynamiczny i wymaga od nas ciągłego dostosowywania naszych praktyk. Dlatego przeglądanie naszych działań cyfrowych, adaptowanie się do oszustw, rozpoznawanie prób wyłudzenia oraz ostrożność w pobieraniu danych są kluczowymi aspektami utrzymania bezpieczeństwa online.

Narzędzie, które może pomóc w przeglądzie praktyk i regularnym aktualizowaniu jest Ramowy Program Kompetencji Cyfrowych lub DigComp. Jest to narzędzie referencyjne dla instytucji, jednostek i edukatorów, które zostało opracowane przez UE i jest stale aktualizowane, z ostatnią wersją 2.2 na dzień publikacji tego podręcznika. DigComp jest dostępny na stronie publikacji UE.

Regularne aktualizacje DigComp zapewniają, że framework pozostaje aktualny i odzwierciedla bieżące środowisko cyfrowe. Podobnie jak DigComp, możesz również przeglądać i aktualizować swoje praktyki higieny cyfrowej, aby upewnić się, że są zgodne z bieżącymi potrzebami twojej organizacji i rozważać włączenie umiejętności związanych z nowymi technologiami.

Rozdział 4 - Przykłady dobrych praktyk kultury higieny cyfrowej

W poprzednich rozdziałach zagłębialiśmy się w istotne aspekty kultywowania solidnej kultury higieny cyfrowej zarówno w start-upach, jak i w instytucjach kształcenia zawodowego (VET). Omówiliśmy

znaczenie monitorowania, przeglądania i ciągłego doskonalenia praktyk higieny cyfrowej w celu zapewnienia bezpiecznego i wydajnego środowiska cyfrowego. Te dyskusje podkreśliły rolę kultywowania dobrej kultury higieny cyfrowej.

Teraz, przechodząc do ostatniej części Modułu 3, w Rozdziale 4, zagłębimy się w praktyczne zastosowania, przedstawiając przykłady, które ukazują praktyczne przypadki użycia zasad higieny cyfrowej.

Przykłady zastosowania higieny cyfrowej na świecie

- **Specjalistyczny zestaw narzędzi do promowania praktyk higieny cyfrowej (Serbia)**

Znaczącym przykładem zastosowania dobrych praktyk higieny cyfrowej jest przewodnik przygotowany przez Share Cert, fundację z siedzibą w Belgradzie, podkreślającą strategiczne środki cyberbezpieczeństwa. Poprzez systematyczną kategoryzację najczęstszych zagrożeń i środków bezpieczeństwa, ten przewodnik jest wspierany przez otwartą platformę, gdzie osoby i organizacje mogą być informowane o najważniejszych tematach w środowisku cyfrowym i otrzymywać ogólne wskazówki dotyczące kultury higieny cyfrowej.

- **Kampanie podnoszące świadomość na temat ochrony praw cyfrowych (Grecja)**

Kolejną ważną inicjatywą w zakresie ochrony praw cyfrowych jest organizacja Homo Digitalis, grecka organizacja pozarządowa (NGO) koncentrująca się na prawie do prywatności, ochronie danych osobowych, zakazie dyskryminacji w przestrzeniach cyfrowych oraz wolności informacji. Dzięki ponad 100 członkom, aktywnie uczestniczą w badaniach i przeprowadzają dochodzenia na rzecz dobra publicznego, co z kolei może pomóc ustawodawcom lepiej zrozumieć kwestie związane z prawami cyfrowymi.

- **Zestaw szybkiego reagowania dla coraz bardziej cyfrowego społeczeństwa obywatelskiego (Globalny)**

Międzynarodowe sieci Zespołów Reagowania na Incydenty Komputerowe (CERT) oraz Sieć Szybkiego Reagowania (RaReNet) współpracowały, aby pomóc szybkim reagującym, trenerom ds. bezpieczeństwa cyfrowego i aktywistom technicznym lepiej chronić się przed najczęstszymi rodzajami zagrożeń cyfrowych za pomocą tzw. Zestawu Pierwszej Pomocy Cyfrowej, który obejmuje różnorodne kwestie. Dostępny w 13 językach i stale rozwijany dzięki zewnętrznym wkładom, Zestaw Pierwszej

Pomocy Cyfrowej jest cennym źródłem promującym odpowiedzialne i bezpieczne korzystanie z Internetu.

- **Budowanie odpornych narzędzi do śledzenia praktyk higieny cyfrowej dla społeczeństwa obywatelskiego (Globalny)**

Centrum Odpornych Systemów Cyfrowych to organizacja non-profit działająca w ponad 20 krajach, której celem jest ustanowienie odpornych systemów cyfrowych w celu zapewnienia bezpieczeństwa społeczeństwa obywatelskiego. Ich projekty obejmują dostarczanie usług i narzędzi, takich jak narzędzie do crowdsourcingu zaprojektowane do identyfikacji i zgłaszania fałszywych informacji, platforma cyfrowa do zgłaszania problemów z bezpieczeństwem, narzędzie do wizualizacji monitorujące zagrożenia i ataki na systemy cyfrowe oraz narzędzie społecznościowe mające na celu stworzenie silnej sieci uczestnictwa w ramach CiviCERT.

- **Sieci ułatwiające wymianę między zespołami reagującymi na incydenty na całym świecie (Globalny)**

CiviCERT to sieć, która łączy CERT, niezależnych dostawców treści internetowych i usług, a także NGO i osoby prywatne. Członkowie sieci wykonują, koordynują i wspierają reakcję na zgłoszone incydenty związane z bezpieczeństwem cyfrowym w mechanizmie współpracy, gdzie potrzebny jest punkt widzenia innych partnerów. CiviCERT utrzymuje dobre praktyki higieny cyfrowej, gdzie członkowie komunikują się za pośrednictwem zaszyfrowanych platform, takich jak zaszyfrowana lista mailingowa i Platforma Wymiany Informacji o Złośliwym Oprogramowaniu, aby dzielić się informacjami na temat nowych zagrożeń dla społeczeństwa obywatelskiego oraz szablonami zapewniającymi wiarygodne i ustandaryzowane procedury obsługi incydentów.

- **Zachęcanie do przestrzegania praw człowieka w środowiskach cyfrowych w krajach rozwijających się (Azja Zachodnia i Afryka Północna)**

SMEX to NGO promująca prawa człowieka w środowiskach cyfrowych w Azji Zachodniej i Afryce Północnej. W zakresie praktyk higieny cyfrowej oferują wsparcie dla użytkowników internetu, aktywistów i organizacji zajmujących się prawami człowieka w ich problemach z cyberbezpieczeństwem oraz tworzą programy informujące ogół społeczeństwa o przepisach i prawie internetowym. SMEX aktywnie współpracuje z lokalnymi i międzynarodowymi partnerami, aby promować świadomość i wdrażanie praktyk higieny cyfrowej, tworząc bezpieczniejsze środowisko

online dla osób i organizacji działających na rzecz praw człowieka w przestrzeni cyfrowej w Azji Zachodniej i Afryce Północnej.

- **Program nauki umiejętności cyfrowych dla uczniów K-12 (Ameryka Północna)**

Koncepcja higieny cyfrowej zyskuje na znaczeniu w systemach edukacyjnych na całym świecie. Jedną z organizacji, która specjalizuje się w przygotowywaniu materiałów dotyczących umiejętności cyfrowych specjalnie dla uczniów K-12, jest Common Sense Media, niezależna organizacja z siedzibą w Ameryce Północnej, której celem jest umożliwienie uczniom, rodzicom i nauczycielom dostępu do danych na temat wpływu mediów i środowisk cyfrowych na potrzeby fizyczne, emocjonalne, społeczne i mentalne dzieci. Ich oparty na badaniach program "Digital Citizenship Curriculum" porusza ważne kwestie związane z mediami i technologiami w szkołach, takie jak: Jak chronić się przed cyberprzemocą? Jak chronić naszą prywatność? Jak radzić sobie z dezinformacją?

- **Materiały edukacyjne na rzecz lepszej umiejętności cyfrowej (Ameryka Północna)**

Center of Digital Literacy to amerykańska organizacja non-profit, której celem jest promowanie badań i tworzenie materiałów open-source, a także narzędzi do projektowania programów nauczania, lekcji, aktywności i ocen, które mogą być wykorzystywane i dostosowywane do różnych kontekstów edukacyjnych. Umiejętność korzystania z mediów jest ważną częścią praktyk higieny cyfrowej, a nacisk na tę umiejętność nie tylko wzmacnia higienę cyfrową, ale także kultywuje bardziej poinformowane i krytycznie myślące społeczeństwo, lepiej przygotowane do radzenia sobie z zawiłościami cyfrowego świata.

- **Europejski Miesiąc Cyberbezpieczeństwa (Europa)**

Każdego roku październik obchodzony jest jako Europejski Miesiąc Cyberbezpieczeństwa (ECSM), ważne coroczne wydarzenie organizowane przez Europejską Agencję ds. Cyberbezpieczeństwa (ENISA) oraz Komisję Europejską. Poświęcony wzmacnianiu świadomości na temat cyberbezpieczeństwa wśród obywateli i organizacji UE, ECSM jest jednym z wielu wielowymiarowych podejść UE do promowania dobrych praktyk higieny cyfrowej. W ciągu października odbywają się konferencje, warsztaty i webinary, tworząc szeroko zakrojoną kampanię, która nie tylko podnosi świadomość na temat cyberbezpieczeństwa, ale także aktywnie dzieli się zaktualizowanymi informacjami i poradami ekspertów. Dążąc do promowania bezpieczniejszego korzystania z internetu, ECSM dostarcza wskazówek dotyczących higieny cyfrowej i staje się wszechstronnym i wspólnym wysiłkiem, podobnym do globalnych sieci takich jak CiviCERT i regionalnych NGO jak SMEX, odgrywając

kluczową rolę w promowaniu i utrzymywaniu dobrych praktyk higieny cyfrowej w całej Unii Europejskiej.

- **Gra dotycząca cyberbezpieczeństwa dla przedszkolaków (Globalny)**

Interland to interaktywna gra stworzona przez Google, będąca częścią programu "Be Internet Awesome", zintegrowanego programu promującego praktyki higieny cyfrowej wśród młodych uczniów. Jako dynamiczna i interaktywna gra, Interland angażuje uczniów poprzez swoją rozgrywkę, oferując praktyczne podejście do nauczania niektórych podstawowych aspektów dobrych praktyk higieny cyfrowej poprzez gamifikację. Złożone kwestie takie jak prywatność, phishing, hacking i cyberprzemoc są tłumaczone młodszym uczniom za pomocą kolorowych animacji, które są odpowiednie dla ich poziomu kompetencji. Ogólnie rzecz biorąc, Interland jest godnym uwagi przykładem wdrażania dobrych praktyk higieny cyfrowej od najmłodszych lat poprzez wykorzystanie technologii.

W tym module omówiliśmy wdrażanie i znaczenie dobrych praktyk higieny cyfrowej. Przeanalizowaliśmy takie tematy jak rozwijanie kultury higieny cyfrowej w organizacji na różnych poziomach zarządzania, eksplorowanie metod ciągłego doskonalenia tych praktyk, bycie poinformowanym o przyszłych możliwościach i wyzwaniach oraz analizę studiów przypadków z całego świata.

Zapoznaj się z innymi modułami tego przewodnika, aby uzyskać dalsze porady i strategie dotyczące dobrych praktyk higieny cyfrowej, i odwiedź stronę internetową Good Digital Hygiene for Startups.

Źródła

Unit 1 - Building a Digital Hygiene Culture in Startups and VET Institutions

[1] Boulet, C. (2006). Digital Hygiene: Clean Living on a Dirty Network. *Interface: The Journal of Education, Community, and Values 6(3).* Retrieved from: Digital Hygiene: Clean Living on a Dirty Network (core.ac.uk) [Access Date 05.12.2023]

[2] Groysberg, B., Lee, J., Price, J., & Cheng, J. Y.-J. (2018, January-February). The leader's guide to corporate culture. *Harvard Business Review.* Retrieved from: The Leader's Guide to Corporate Culture (hbr.org) [Access Date 05.12.2023]

[3] Trevors, M. (2017). Cyber hygiene: 11 essential practices. Software Engineering Institute Blog. Retrieved from https://insights.sei.cmu.edu/blog/cyber-hygiene-11-essential-practices/ [Access Date 05.12.2023]

[4] Ly, B. The Interplay of Digital Transformational Leadership, Organizational Agility, and Digital Transformation. J Knowl Econ (2023). https://doi.org/10.1007/s13132-023-01377-8

[5] Harvard Business School Online. (n.d.). *How to Become a More Effective Leader.* Harvard Business School Publishing. Retrieved from https://info.email.online.hbs.edu/leadership-ebook

[6] Cortellazzo, L., Bruni, E., & Zampieri, R. (2019). The role of leadership in a digitalized world: A review. *Frontiers in Psychology,* 10, 1938. https://doi.org/10.3389/fpsyg.2019.01938

[7] Cisco. (n.d.) Cisco Learning Network Store. Retrieved from https://learningnetworkstore.cisco.com/

[Access Date 06.12.2023]

[8] European Union Agency for Cybersecurity (ENISA). (n.d.). Online training material for cybersecurity specialists: Technical and operational. ENISA. Retrieved from https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#identification_handling [Access Date 06.12.2023]

[9] Sklar, A. (2017). Sound, smart, and safe: A plea for teaching good digital hygiene. *LEARNing Landscapes Journal*, 10(2). https://doi.org/10.36510/learnland.v10i2.799 [Access Date 06.12.2023]

[10] Glazer, K. (2017, March 22). A quick guide to good digital hygiene. *Literacy Now*. Retrieved from https://www.literacyworldwide.org/blog/literacy-now/2017/03/22/a-quick-guide-to-good-digital-hygiene

[Access Date 06.12.2023]

[11] Documenting Digital Attacks (n.d). Digital First Aid. Retrieved from https://digitalfirstaid.org/documentation/

[12] Saraf, A. (2021, May 14). Three steps to healthy digital hygiene. *Forbes*. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2021/05/14/three-steps-to-healthy-digital-hygiene/

[Access Date 11.12.2023]

[13] Kaspersky. (n.d.). Cyber hygiene habits: 11 ways to improve your security. Retrieved from https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

[14] Cybersecurity and Infrastructure Security Agency (CISA). (2022). 4 things you can do to keep yourself cyber safe. Retrieved from https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe [Access Date 11.12.2023]

[15] CHAYN. (2018). *Do it Yourself Online Safety.* Retrieved from https://chayn.gitbook.io/diy-online-safety/english [Access Date 07.12.2023]

[16] Torbet, G. (2019, February 3). Social media sites can predict your behavior even if you don't use them. *Digital Trends.* Retrieved from https://www.digitaltrends.com/social-media/social-media-privacy-friends-prediction/

[17] Toth.R., & Trifonova, T. (2021). Somebody's Watching Me: Smartphone Use Tracking and Reactivity. *Computers in Human Behavior Reports, 4, 100142*, https://doi.org/10.1016/j.chbr.2021.100142

[Access Date 07.12.2023]

[18] Brooks, T. (2021, July 29). Why You Should Update Your Web Browser. *How-To Geek.* Retrieved from https://www.howtogeek.com/725165/why-you-should-update-your-web-browser/ [Access Date 08.12.2023]

[19] Barrons, M. (2016, September 12). How to Create Secure Passwords You Won't Forget. *InfoWare Group Blog.* Retrieved from https://infowaregroup.com/blog/how-to-create-secure-passwords-you-won't-forget [Access Date 08.12.2023]

Unit 2 - Monitoring, Review, and Continuous Improvement of Digital Hygiene Practices

[20] Scott, M. (2023, December 8). Europe's plan to tame Big Tech: A new legal framework. *The New York Times*. Retrieved from E.U. Agrees on AI Act, Landmark Regulation for Artificial Intelligence - The New York Times (nytimes.com)

[21] Rehak, D., & Grasseova, M., (2011). The Ways of Assessing the Security of Organization Information Systems through SWOT Analysis. In M. Alshawi & M. Arif (Eds.), *Cases on E-Readiness and Information Systems Management in Organizations: Tools for Maximizing Strategic Alignment* (1st ed., pp. 162-184). IGI Global. https://doi.org/10.4018/978-1-61350-311-9

[22] Gleason, Benjamin & von Gillern, Sam. (2018). Digital citizenship with social media: Participatory practices of teaching and learning in secondary education. Educational Technology and Society. 21. 200-212. https://www.researchgate.net/publication/322733013_Digital_citizenship_with_social_media_Participatory_practices_of_teaching_and_learning_in_secondary_education [Access Date 20.12.2023]

[23] Lewin, C., Niederhauser, D., Johnson, Q., Saito, T., Sakamoto, A., & Sherman, R. (2021). Safe and Responsible Internet Use in a Connected World: Promoting Cyber-Wellness. *Canadian Journal of Learning and Technology, 47*(4), Special Issue.

Unit 3 - The Future of Digital Hygiene: Challenges and Opportunities

[24] Metz, C. (2023). What's the Future of AI? *The New York Times.* Retrieved from https://www.nytimes.com/2023/03/31/technology/ai-chatbots-benefits-dangers.html?searchResultPosition=1

[25] Gleason, Benjamin & von Gillern, Sam. (2023). Tinkering With ChatGPT, Workers Wonder: Will This Take My Job? *The New York Times.* Retrieved from https://www.nytimes.com/2023/03/28/business/economy/jobs-ai-artificial-intelligence-chatgpt.html

[26] Banholzer, M., Fletcher, B., LaBerge, L., & McClain, J. (2023, August 31). Companies with Innovative Cultures Have a Big Edge with Generative AI. *McKinsey & Company.* Retrieved from https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/companies-with-innovative-cultures-have-a-big-edge-with-generative-ai [Access Date 21.12.2023]

[27] Chng, E., Tan, A.L. & Tan, S.C. Examining the Use of Emerging Technologies in Schools: a Review of Artificial Intelligence and Immersive Technologies in STEM Education. Journal for STEM Educ Res 6, 385–407 (2023). https://doi.org/10.1007/s41979-023-00092-y [Access Date 21.12.2023]

[28] Spatharou, A., Hieronimus, S., & Jenkins, J. (2020, March 10). Transforming healthcare with AI: The impact on the workforce and organizations. *McKinsey & Company.* Retrieved from https://www.mckinsey.com/industries/healthcare/our-insights/transforming-healthcare-with-ai

[29] Kopp, W., & Thomsen, B. S. (2023, May 1). How AI can accelerate students' holistic development and make teaching more fulfilling. *World Economic Forum.* Retrieved from https://www.weforum.org/agenda/2023/05/ai-accelerate-students-holistic-development-teaching-fulfilling/

[30] Pappas, C., (2016, January 7). The Top 8 Benefits Of Using Learning Management Systems. *Elearning Industry.* Retrieved from https://elearningindustry.com/top-8-benefits-of-using-learning-management-systems

[31] Seo, K., Tang, J., Roll, I. *et al.* The impact of artificial intelligence on learner–instructor interaction in online learning. *International Journal of Educational Technology in Higher Education* 18, 54 (2021). https://doi.org/10.1186/s41239-021-00292-9

[32] Yadav, N. R., & Deshmukh, S. S. (2023). Proceedings of the International Conference on Applications of Machine Intelligence and Data Analytics. In *Proceedings of the International Conference on Applications of Machine Intelligence and Data Analytics (ICAMIDA 2022)* Retrieved from https://www.atlantis-press.com/article/125986295.pdf

[33] Duball, J. (2020). Shift to Online Learning Ignites Student Privacy Concerns. *International Association of Privacy Professionals (IAPP).* Retrieved from https://iapp.org/news/a/shift-to-online-learning-ignites-student-privacy-concerns/

[34] United States International Trade Administration. (n.d.). European Union - Data Privacy and Protection. Retrieved from https://www.trade.gov/european-union-data-privacy-and-protection

[35] Gonzalez, G. (2018, October 10). Amazon Abandons AI Recruiting Tool That Showed Bias Against Women. *Inc.* Retrieved from https://www.inc.com/guadalupe-gonzalez/amazon-artificial-intelligence-ai-hiring-tool-hr.html

[36] Gatzemeier, S. (2021, June 18). AI Bias: Where Does It Come From and What Can We Do About It? *UC Berkeley School of Information Blog.* Retrieved from https://blogs.ischool.berkeley.edu/w231/2021/06/18/ai-bias-where-does-it-come-from-and-what-can-we-do-about-it/

[37] Akgun, S., Greenhow, C. Artificial intelligence in education: Addressing ethical challenges in K-12 settings. *AI Ethics* 2, 431–440 (2022). Retrieved from https://doi.org/10.1007/s43681-021-00096-7

[38] Polluveer, K. (2023). Innovation Policy. *European Parliament Fact Sheet.* Retrieved from https://www.europarl.europa.eu/erpl-app-public/factsheets/pdf/en/FTU_2.4.6.pdf

[39] OECD (2021), Teachers and Leaders in Vocational Education and Training, OECD Reviews of Vocational Education and Training, OECD Publishing, Paris, https://doi.org/10.1787/59d4fbb1-en

4. Promoting innovative pedagogical approaches in vocational education and training | Teachers and Leaders in Vocational Education and Training | OECD iLibrary (OECD-ilibrary.org)

[40] eduLAB Pty Ltd. (2020, August 12). eduLAB Introduction Video. *Vimeo.* Retrieved from https://vimeo.com/447337687

[41] N.d. (2022, March 27). 7 Technology Innovations That Will Impact Cybersecurity in 2022 and Beyond. *Cloud Security Alliance Blog.* Retrieved from 7 Technology Innovations That Will Impact Cybersecurity in 2022 | CSA (cloudsecurityalliance.org)

[42] World Economic Forum. (2021, March). Artificial Intelligence for Agricultural Innovation. *Community Paper.* Retrieved from WEF_Artificial_Intelligence_for_Agriculture_Innovation_2021.pdf (weforum.org)

[43] BIS Research. (2021, October 7). The Increasing Adoption of Augmented Reality (AR) in Agriculture. Retrieved from https://blog.marketresearch.com/the-increasing-adoption-of-augmented-reality-ar-in-agriculture

[44] BIS Research. (2021, October 7). The Increasing Adoption of Augmented Reality (AR) in Agriculture. Retrieved from https://eos.com/blog/smart-farming/

[45] Tzachor, A., Devare, M., King, B., et al. (2022). Responsible artificial intelligence in agriculture requires a systemic understanding of risks and externalities. *Nature Machine Intelligence, 4*, 104–109. https://doi.org/10.1038/s42256-022-00440-4

[46] Bettencourt, J. (2023, November 16). How the hospitality industry is using AR, and VR for the guest experience. *Hotel Management.* Retrieved from https://www.hotelmanagement.net/tech/how-hospitality-industry-using-ar-vr-guest-experience

[47] Kover, A. (2020, March 10). A new perspective on hospitality: How Hilton uses VR to teach empathy. *Facebook Reality Labs Tech Blog.* Retrieved from https://tech.facebook.com/reality-labs/2020/3/a-new-perspective-on-hospitality-how-hilton-uses-vr-to-teach-empathy/

[48] Guenther, D. (2021, September 9). Virtual Reality training prepares hospitality workers for the next era of travel. *Medium.* Retrieved from https://medium.com/@DanielGuenther/virtual-reality-training-prepares-hospitality-workers-for-the-next-era-of-travel-7a8d5d3b8be5

[49] Pencarelli, T. The digital revolution in the travel and tourism industry. *Inf Technol Tourism* 22, 455–476 (2020). Retrieved from https://doi.org/10.1007/s40558-019-00160-3

[50] Amon, C., Slaughter, A., & Motyka, M. (2018, September). Global renewable energy trends. *Deloitte.* Retrieved from https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/global-renewable-energy-trends.html

[51] Travelers. (n.d.). Predictive Maintenance at Solar and Wind Installations. Retrieved from https://www.travelers.com/resources/business-industries/energy/predictive-maintenance-at-solar-and-wind-installations

[52] Victor, D. G. (2019, January 10). How artificial intelligence will affect the future of energy and climate. *Brookings Institution.* Retrieved from https://www.brookings.edu/articles/how-artificial-intelligence-will-affect-the-future-of-energy-and-climate/

[9] Sklar, A. (2017). Sound, smart, and safe: A plea for teaching good digital hygiene. *LEARNing Landscapes Journal*, 10(2). https://doi.org/10.36510/learnland.v10i2.799 [Access Date 06.12.2023]

UNIT 4 - Digital Hygiene Culture Good Practice Use Case:

[53] ShareCert Toolkit. (n.d.). Retrieved from Cybersecurity Toolkit

[54] Homo Digitalis. (2022, July 13). A big success for Homo Digitalis: The Hellenic DPA fines CLEARVIEW AI with €20 million. Retrieved from https://homodigitalis.gr/en/posts/12155/

[55] Digital First Aid. (n.d.). Retrieved from Digital First Aid Kit

[56] Digiresilience. (n.d.). Retrieved from Center for Digital Resilience

[57] CivicERT. (n.d.). Retrieved from CiviCERT

[58] SMEX. (n.d.). Retrieved from SMEX

[59] Common Sense Media. (n.d.). Digital Literacy and Citizenship. Retrieved from https://www.commonsensemedia.org/what-we-stand-for/digital-literacy-and-citizenship

[60] Center for Media Literacy. (2005). Five Key Questions of Media Literacy. Retrieved from https://www.medialit.org/sites/default/files/14B_CCKQPoster+5essays.pdf

[61] Center for Media Literacy. (n.d.). Retrieved from https://www.medialit.org/https://www.medialit.org/

[62] European Cyber Security Month. (n.d.). Retrieved from https://cybersecuritymonth.eu/

[63] Google. (2023). Be Internet Awesome: Interland. Retrieved from https://beinternetawesome.withgoogle.com/en_us/interland/

[64] Google. (2023). Be Internet Awesome: Interland. Retrieved from https://beinternetawesome.withgoogle.com/en_us

[65] Bogardus Cortez, M. (2018, April 17). The Digital Citizenship Curriculum: Digital Literacy, Cyber Hygiene and More. *EdTech Magazine.* Retrieved from How to Design Your Digital Citizenship Curriculum - EdTech (edtechmagazine.com)

[66] Bogardus Cortez, M. (2014, July 24). Digital Citizenship Game by Google & ITSE Aims to Educate. *EdTech Magazine.* Retrieved from Digital Citizenship Game by Google & ITSE Aims to Educate | EdTech Magazine

---

[12*] Durbin, S. (2019). The top 3 global cybersecurity threats of 2020. *Dark Reading.* Retrieved from **https://www.darkreading.com/vulnerabilities-threats/crystal-ball-the-top-3-global-cybersecurity-threats-for-2020** [Access Date 06.12.2023]

[13*] Ponemon, L., & Beri, S. (2014). *Data Breach: The Cloud Multiplier Effect.* Retrieved from **https://www.slideshare.net/Netskope/data-breach-the-cloud-multiplier-effect** [Access Date 06.12.2023]

[14*] Hadlington, L. (2017). Human factors in cybersecurity: examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon, 3*. **https://doi.org/10.1016/j.heliyon.2017.e00346**

[15*] Telefonica Tech. (2022, November 10). Human Factors in Cybersecurity: Protect Yourself. *Telefonica Tech Blog.* Retrieved from **https://telefonicatech.com/en/blog/human-factors-in-cybersecurity** [Access Date 11.12.2023]

[XXXXX] Irwin, L. (2020, June). *5 ways to detect a phishing email – with examples*. ITGovernance. https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email [Access Date 08.12.2023]

[XXXXXXX] Federal Trade Commission Consumer Information (2019, May). *How To Recognize and Avoid Phishing Scams.* https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams [Access Date 08.12.2023]

[XX] DCAF (Geneva Centre for Security Sector Governance), Babić, V., & Bratić, A. (2022, October). *Guidebook on Staying Safe Online: Cyber Hygiene for Public Institutions and SMEs.* Retrieved from **https://www.dcaf.ch/sites/default/files/publications/documents/GuidebookStayingSafeOnline_CyberHygiene_EN_web_Jan2023.pdf** [Access Date 06.12.2023]