PROGRAM SZKOLENIA

Temat szkolenia: Cyberbezpieczeństwo

CELE SZKOLENIA

Poziom wiedzy

1. Uczestnicy będą w stanie opisać podstawowe pojęcia związane z cyberbezpieczeństwem, w tym definicje, znaczenie ochrony danych oraz zagrożenia związane z kradzieżą danych osobowych, oszustwami internetowymi oraz atakami na infrastrukturę krytyczną.
2. Uczestnicy nauczą się identyfikować różne techniki wyłudzania danych, takie jak phishing, vishing i smishing oraz będą w stanie omówić sposoby ich wykrywania i przeciwdziałania.
3. Uczestnicy zdobędą wiedzę na temat podstawowych zasad ochrony przed zagrożeniami w internecie, w tym stosowania wielowarstwowej ochrony przed złośliwym oprogramowaniem i metodami ochrony danych osobowych zgodnie z wymogami RODO.

Poziom umiejętności

1. Uczestnicy nauczą się stosować narzędzia ochrony przed phishingiem, takie jak uwierzytelnianie wieloetapowe (MFA), oprogramowanie antyphishingowe, a także będą potrafili rozpoznawać elementy wskazujące na złośliwe wiadomości e-mail.
2. Uczestnicy będą potrafili analizować przykłady rzeczywistych ataków, takie jak ransomware, DDoS oraz spoofing, a także proponować odpowiednie metody ochrony.
3. Uczestnicy zdobędą umiejętność korzystania z menedżerów haseł oraz technik tworzenia silnych haseł, a także stosowania zasad bezpiecznych płatności online, w tym korzystania z certyfikatów SSL oraz metod dwuskładnikowego uwierzytelniania.

Poziom kompetencji społecznych (postaw)

1. Uczestnicy będą umieli promować kulturę cyberhigieny w swoim otoczeniu zawodowym, podnosząc świadomość współpracowników na temat zagrożeń związanych z cyberbezpieczeństwem.
2. Uczestnicy rozwiną kompetencje związane ze wspieraniem współpracowników/rodziny/znajomych w rozpoznawaniu zagrożeń i promowaniem dobrych praktyk bezpieczeństwa, minimalizując ryzyko wynikające z ludzkich błędów

Poziom narzędzi

1. Uczestnicy zdobędą umiejętności stosowania narzędzi do monitorowania zagrożeń oraz do reagowania na cyberataki.
2. Uczestnicy będą w stanie korzystać z narzędzi umożliwiających efektywną komunikację zagrożeń i rozwiązań związanych z cyberbezpieczeństwem, tak aby zwiększyć świadomość wśród współpracowników/rodziny/znajomych.

Akademia WIT w Warszawie Newelska 6, 01-447 Warszawa 22 3486 570 skills@wit.edu.pl
Certes Sp. z o.o. Hafciarska 11, 04-704 Warszawa
Polska Izba Opakowań ul. Konstancińska 11, 02-942 Warszawa

SCENARIUSZ SZKOLENIA Z HARMONOGRAMEM				
DZIEŃ 1				
Czas	**Zakres merytoryczny**	**Cele z modułu/ ćwiczenia/ wnioski**	**Nazwa i Opis ćwiczenia**	**Metody/ Narzędzia**
09:00-10:30	1. **Wprowadzenie do Cyberbezpieczeństwa** **Definicja i znaczenie:** • Omówienie podstawowych pojęć związanych z cyberbezpieczeństwem. • Znaczenie ochrony danych w codziennym życiu i pracy zawodowej. • Zagrożenia związane z kradzieżą danych osobowych, oszustwami internetowymi, atakami na infrastrukturę krytyczną oraz ich konsekwencje. • Wpływ cyberbezpieczeństwa na użytkowników indywidualnych, firmy oraz instytucje. **Główne źródła wiedzy o cyberbezpieczeństwie:** • Wiarygodne źródła informacji o cyberzagrożeniach, takie jak publikacje naukowe, raporty branżowe oraz czasopisma akademickie. • Platformy e-learningowe, takie jak Coursera, Udemy, edX oraz certyfikacje branżowe jako sposób na rozwój umiejętności w zakresie cyberbezpieczeństwa. • Organizacje zajmujące się cyberbezpieczeństwem oraz fora dyskusyjnie.	*Celem modułu jest zapoznanie uczestników z podstawowymi pojęciami cyberbezpieczeństwa oraz wskazanie im źródeł wiedzy, dzięki którym będą mogli rozwijać swoje kompetencje w tej dziedzinie.*	*Ćwiczenie 1 „Mapa zagrożeń” - ćwiczenie grupowe polegające na tworzeniu wizualnej mapy cyberzagrożeń i ich wzajemnych powiązań, zakończone wspólną dyskusją.*	*Wykład interaktywny połączony z prezentacją multimedialną i dyskusją grupową*
10:30-10:45	*Przerwa kawowa*			

10:45-12:15	2. **Techniki wyłudzania/przechwytywania danych oraz rodzaje cyberataków** **Phishing, Vishing, Smishing:** • Definicje i omówienie technik wyłudzania danych, takich jak phishing (e-mail), vishing (telefon) oraz smishing (SMS). • Personalizacja ataków phishingowych, spear phishing, whaling – jak przestępcy wykorzystują informacje o ofiarach, aby zwiększyć skuteczność swoich ataków. • Przykłady rzeczywistych ataków oraz analiza mechanizmów psychologicznych, które wpływają na podatność użytkowników na takie ataki, w tym wykorzystanie presji czasowej, zaufania i lęku. **Przechwytywanie Danych:** • Keyloggery, Man-in-the-Middle (MitM), skimming online, podsłuch sieciowy – analiza każdej techniki, sposobów jej wykrycia oraz możliwego przeciwdziałania. • Przykłady ataków MitM z użyciem rogue access points oraz ich skutki. • Techniki ochrony przed przechwytywaniem danych: stosowanie TLS, VPN, HTTPS. • Zagrożenia związane z używaniem niezabezpieczonych sieci Wi-Fi. • Wykorzystanie kryptografii asymetrycznej do ochrony danych. **Rodzaje cyberataków:** • Ransomware: charakterystyka, przykłady ataków oraz analiza wpływu na przedsiębiorstwa, infrastruktury krytyczne oraz organizacje rządowe. • DDoS: cel ataków, metody przeprowadzania, jakie są ich skutki oraz jak można się przed nimi zabezpieczyć. • Business Email Compromise (BEC): jak przestępcy podszywają się pod kadrę kierowniczą. • Spoofing: techniki podszywania się pod osoby, urządzenia, w tym spoofing adresów IP, DNS oraz ARP.	*Głównym celem modułu jest zapoznanie uczestników z różnymi technikami wyłudzania i przechwytywania danych, poprzez szczegółowe omówienie mechanizmów działania konkretnych rodzajów cyberataków, takich jak phishing, ransomware czy ataki Man-in-the-Middle. Dodatkowo, moduł ma na celu nauczenie uczestników rozpoznawania symptomów tych ataków oraz przedstawienie skutecznych metod obrony przed nimi.*	*Ćwiczenie 2 „Symulacja ataku": ćwiczenie symulacyjne, w którym jedna grupa tworzy wiadomości phishingowe, a druga grupa analizuje je i wykrywa elementy oszustwa, co pozwala zrozumieć techniki ataku i metody obrony.*	*Analiza przypadków i narzędzia analityczne. Materiały wideo i studia przypadku. Praca w grupach.*

Akademia WIT w Warszawie Newelska 6, 01-447 Warszawa 22 3486 570 skills@wit.edu.pl
Certes Sp. z o.o. Hafciarska 11, 04-704 Warszawa
Polska Izba Opakowań ul. Konstancińska 11, 02-942 Warszawa

12:15-12:45	*Przerwa obiadowa*			
12:45-14:15	3. **Phishing i socjotechnika - techniki cyberprzestępców** **Zjawisko phishingu i socjotechniki:** • Mechanizmy phishingu i socjotechniki – jak cyberprzestępcy manipulują użytkownikami. • Techniki manipulacji, takie jak wywoływanie zaufania, presji czasowej, manipulacja emocjonalna, a także tworzenie fałszywego poczucia bezpieczeństwa. • Wpływ heurystyk poznawczych i błędów poznawczych na podatność na ataki phishingowe i socjotechniczne. • AI – wykorzystanie sztucznej inteligencji do ataków. **Rozpoznawanie wiadomości phishingowych:** • Elementy wskazujące na złośliwe wiadomości e-mail: fałszywe adresy e-mail, błędy językowe, nietypowe prośby. • Znaczenie edukacji w zakresie cyberhigieny i podnoszenia świadomości. • Metody weryfikacji wiadomości. • Przykłady narzędzi, które pomagają w analizie bezpieczeństwa e-maili. **Techniki manipulacji:** • Spoofing, CEO fraud, fałszywe nagrody – jak cyberprzestępcy manipulują ofiarami, aby uzyskać dostęp do danych firmowych lub zasobów finansowych. • Wykorzystanie elementów zaskoczenia, presji czasowej oraz wzbudzania poczucia pilności jako kluczowych narzędzi manipulacji. • Przykłady rzeczywistych incydentów. **Ochrona przed phishingiem:** • Uwierzytelnianie wieloetapowe (MFA) jako standard zabezpieczeń. • Stosowanie rozwiązań antyphishingowych oraz szkolenia z zakresu rozpoznawania ataków i odpowiednich reakcji.	*Głównym celem modułu jest nauczenie uczestników rozpoznawania technik manipulacji stosowanych w atakach phishingowych i socjotechnicznych, ze szczególnym uwzględnieniem mechanizmów psychologicznych wykorzystywanych przez cyberprzestępców. Dodatkowo, moduł ma na celu przekazanie praktycznej wiedzy o metodach ochrony przed takimi atakami, w tym wykorzystania narzędzi technicznych i rozwoju umiejętności krytycznej analizy otrzymywanych wiadomości.*	*Ćwiczenie 3 „Analiza manipulacji" polega na analizie przez uczestników autentycznych kampanii phishingowych, gdzie w małych grupach identyfikują oni zastosowane techniki manipulacji psychologicznej i proponują skuteczne metody obrony.*	*Analiza przypadków. Studia przypadku i analiza scenariuszy. Wykład interaktywny i praca w grupach.*

Akademia WIT w Warszawie Newelska 6, 01-447 Warszawa 22 3486 570 skills@wit.edu.pl
Certes Sp. z o.o. Hafciarska 11, 04-704 Warszawa
Polska Izba Opakowań ul. Konstancińska 11, 02-942 Warszawa

14:15-14:30	*Przerwa kawowa*			
14:30-16:00	4. **Złośliwe oprogramowanie** **Czym jest malware:** • Definicja i rodzaje złośliwego oprogramowania. • Cele działania malware – kradzież, szpiegowanie, nieautoryzowany dostęp. • Przykłady wykorzystania malware do ataków APT. • Ewolucja złośliwego oprogramowania – jak zmieniają się metody ataków oraz typy zagrożeń. **Rodzaje złośliwego oprogramowania:** • Wirusy, robaki, trojany, spyware, adware, ransomware, keyloggery – omówienie. • Przykłady znanych ataków z wykorzystaniem złośliwego oprogramowania oraz analiza ich wpływu na poziomie krajowym i międzynarodowym. **Metody ochrony:** • Wielowarstwowa ochrona przed malware. • Monitorowanie aktywności sieci, wykrywanie anomalii. • Zasady najmniejszych uprawnień (least privilege) oraz segmentacja sieci. • Regularne aktualizacje, backupy oraz testy penetracyjne – omówienie, jak proaktywne działania mogą pomóc w zmniejszeniu ryzyka związanego z atakami.	*Celem modułu jest przekazanie uczestnikom kompleksowej wiedzy o różnych rodzajach złośliwego oprogramowania, ich mechanizmach działania i potencjalnych skutkach ataków. Dodatkowo, moduł ma na celu nauczenie uczestników skutecznych metod ochrony przed malware poprzez zrozumienie zasad wielowarstwowej ochrony i proaktywnych działań zabezpieczających.*	------	*Wykład interaktywny połączony z prezentacją multimedialną. Analiza scenariuszy i materiały wideo. Narzędzia analityczne i burza mózgów.*
DZIEŃ 2				
Czas	**Zakres merytoryczny**	**Cele z modułu/ ćwiczenia/ wnioski**	**Nazwa i Opis ćwiczenia**	**Metody/ Narzędzia**

Akademia WIT w Warszawie Newelska 6, 01-447 Warszawa 22 3486 570 skills@wit.edu.pl
Certes Sp. z o.o. Hafciarska 11, 04-704 Warszawa
Polska Izba Opakowań ul. Konstancińska 11, 02-942 Warszawa

09:00-10:30	1. **Programy antywirusowe oraz ich znaczenie w codziennej pracy** **Rodzaje oprogramowania antywirusowego:** • Omówienie płatnych i darmowych rozwiązań antywirusowych. • Różnice między nimi: zakres ochrony, aktualizacje, dodatkowe funkcje. • Przykłady popularnych programów antywirusowych i analiza ich skuteczności w kontekście wykrywania zagrożeń, takich jak ransomware, phishing oraz rootkity. **Dobre praktyki:** • Regularne aktualizacje oprogramowania antywirusowego oraz systemów operacyjnych. • Tworzenie kopii zapasowych danych jako zabezpieczenie – zasada 3-2-1. • Bezpieczne korzystanie z internetu i poczty elektronicznej. • Regularne skanowanie systemów oraz segmentacja danych w tym wdrażanie zasad najmniejszych uprawnień.	*Głównym celem modułu jest zapoznanie uczestników z różnymi rodzajami programów antywirusowych oraz nauczenie ich świadomego wyboru i efektywnego korzystania z tego typu oprogramowania. Dodatkowo, moduł ma na celu przekazanie wiedzy o dobrych praktykach związanych z codziennym wykorzystaniem programów antywirusowych, w tym zasadach tworzenia kopii zapasowych i regularnych aktualizacji.*	------	*Analiza scenariuszy i materiały wideo. Narzędzia analityczne i burza mózgów. Prezentacja narzędzi.*
10:30-10:45	*Przerwa kawowa*			

Akademia WIT w Warszawie Newelska 6, 01-447 Warszawa 22 3486 570 skills@wit.edu.pl
Certes Sp. z o.o. Hafciarska 11, 04-704 Warszawa
Polska Izba Opakowań ul. Konstancińska 11, 02-942 Warszawa

10:45-12:15	2. **Bezpieczne hasła i uwierzytelnianie wieloetapowe** **Jak tworzyć silne hasła:** • Długość i złożoność haseł jako kluczowe elementy ich bezpieczeństwa. • Przykłady dobrych i złych haseł – dlaczego niektóre hasła są bardziej podatne na ataki. • Ryzyko związane z używaniem powtarzających się haseł – tzw. efekt domina. • Przykłady narzędzi do analizy siły haseł – omówienie. • Menedżery haseł jako narzędzia do bezpiecznego tworzenia, przechowywania i zarządzania silnymi hasłami. **Uwierzytelnianie wieloetapowe (MFA):** • Skuteczność MFA jako metody zabezpieczania dostępu. • Różne metody MFA: SMS, aplikacje uwierzytelniające, tokeny sprzętowe. • Przykłady udaremnionych ataków dzięki MFA – jak MFA znacząco zmniejsza ryzyko przejęcia kont przez atakujących.	*Głównym celem modułu jest nauczenie uczestników tworzenia i zarządzania bezpiecznymi hasłami oraz zrozumienia znaczenia uwierzytelniania wieloetapowego w ochronie danych. Dodatkowo, moduł ma na celu zapoznanie uczestników z praktycznymi narzędziami i technikami zwiększającymi bezpieczeństwo procesu uwierzytelniania.*	*Ćwiczenie "Warsztat bezpiecznych haseł" polega na zespołowej analizie przykładowych haseł przy użyciu specjalistycznych narzędzi oraz tworzeniu własnych technik generowania silnych, ale praktycznych haseł, co pozwala uczestnikom zrozumieć kluczowe aspekty bezpiecznego uwierzytelniania.*	*Wykład interaktywny połączony z prezentacją multimedialną. Analiza narzędzi. Burza mózgów.*
12:15-12:45	*Przerwa obiadowa*			

Akademia WIT w Warszawie Newelska 6, 01-447 Warszawa 22 3486 570 skills@wit.edu.pl
Certes Sp. z o.o. Hafciarska 11, 04-704 Warszawa
Polska Izba Opakowań ul. Konstancińska 11, 02-942 Warszawa

12:45-14:15	3. **Bezpieczne płatności w internecie** **Zagrożenia związane z płatnościami online:** • Phishing i skimming: wyłudzanie danych oraz przechwytywanie danych kart płatniczych. • Ataki MitM, czyli przechwytywanie komunikacji. • Fałszywe sklepy internetowe: tworzenie nieautentycznych sklepów w celu wyłudzeń. **Bezpieczne metody płatności:** • Korzystanie z zabezpieczonych stron: sprawdzanie certyfikatu SSL, unikanie publicznych sieci Wi-Fi. • Dwuskładnikowe uwierzytelnianie (2FA): stosowanie dodatkowego poziomu zabezpieczeń przy płatnościach. • Zaufane bramki płatności: BLIK, PayPal czy Przelewy24. **Weryfikacja sklepów i aplikacje bankowe:** • Weryfikacja sklepów online: analiza opinii klientów, sprawdzanie certyfikatów SSL, Trustpilot. • Bezpieczeństwo aplikacji bankowych: aktualizacje, logowanie biometryczne bądź dwuskładnikowe. • Monitorowanie konta: limity transakcji, powiadomienia SMS. 4. **Ciasteczka (Cookies)** **Czym są ciasteczka:** • Działanie ciasteczek jako mechanizmu przechowywania małych fragmentów danych w przeglądarce użytkownika. • Rodzaje ciasteczek: sesyjne, stałe, podmiotów zewnętrznych. • Personalizacja treści a zagrożenia dla prywatności – jak ciasteczka są wykorzystywane do analizowania zaachowań użytkowników. **Zarządzanie ciasteczkami:** • Ustawienia przeglądarki do blokowania lub usuwania ciasteczek – instrukcje dla różnych przeglądarek. • Korzyści i wady akceptowania ciasteczek – omówienie • Wtyczki do przeglądarek umożliwiające kontrolę nad ciasteczkami.	*Głównym celem modułu jest nauczenie uczestników rozpoznawania zagrożeń związanych z płatnościami internetowymi oraz przekazanie praktycznej wiedzy o metodach bezpiecznego dokonywania transakcji online. Moduł koncentruje się również na rozwoju umiejętności weryfikacji wiarygodności sklepów internetowych i bezpiecznym korzystaniu z aplikacji bankowych.* *Głównym celem modułu jest zrozumienie przez uczestników mechanizmu działania ciasteczek oraz ich wpływu na prywatność i bezpieczeństwo w sieci. Dodatkowo,*	------ ------	Wykład interaktywny połączony z prezentacją multimedialną i dyskusją grupową i studia przypadku. Analiza narzędzi. *Wykład interaktywny połączony z prezentacją multimedialną i dyskusją grupową*

Akademia WIT w Warszawie Newelska 6, 01-447 Warszawa 22 3486 570 skills@wit.edu.pl
Certes Sp. z o.o. Hafciarska 11, 04-704 Warszawa
Polska Izba Opakowań ul. Konstancińska 11, 02-942 Warszawa

	• Tryb prywatny (incognito) jako narzędzie ochrony prywatności, jego zalety i ograniczenia.	*moduł ma nauczyć uczestników praktycznego zarządzania ciasteczkami w różnych przeglądarkach oraz świadomego podejmowania decyzji o ich akceptacji lub odrzuceniu*		
14:15-14:30	*Przerwa kawowa*			

Akademia WIT w Warszawie Newelska 6, 01-447 Warszawa 22 3486 570 skills@wit.edu.pl
Certes Sp. z o.o. Hafciarska 11, 04-704 Warszawa
Polska Izba Opakowań ul. Konstancińska 11, 02-942 Warszawa

14:30-16:00	5. **RODO** **Podstawowe zasady RODO:** • Dane chronione przez RODO i podmioty zobowiązane do przestrzegania regulacji. • Prawa osób fizycznych dotyczące dostępu, poprawiania i usuwania danych - jak użytkownicy mogą korzystać ze swoich praw. • Obowiązki administratorów oraz możliwe sankcje za nieprzestrzeganie przepisów RODO. **Bezpieczeństwo danych osobowych:** • Wymagania dotyczące bezpieczeństwa danych osobowych - omówienie. • Przykłady dobrych praktyk w zakresie ochrony danych - omówienie. 6. **Bezpieczeństwo nośników danych i zasobów dostępnych w chmurze** **Zewnętrzne nośniki danych:** • Wady i zalety korzystania z zewnętrznych nośników danych – ułatwienia vs. ryzyka. • Szyfrowanie danych na zewnętrznych nośnikach jako podstawowa metoda zabezpieczania danych. **Bezpieczna praca w chmurze:** • Wybieranie zaufanych dostawców chmur – na co zwrócić uwagę przy wyborze dostawcy usług chmurowych. • Bezpieczne przechowywanie oraz udostępnianie plików – jakie są najlepsze praktyki podczas przechowywania oraz udostępniania plików.	*Głównym celem modułu jest przekazanie uczestnikom praktycznej wiedzy o zasadach RODO i ich zastosowaniu w codziennej pracy, ze szczególnym uwzględnieniem praw osób, których dane są przetwarzane.* *Głównym celem modułu jest nauczenie uczestników bezpiecznego korzystania z zewnętrznych nośników danych oraz usług chmurowych, ze szczególnym uwzględnieniem metod szyfrowania i zabezpieczania informacji. Moduł ma również na celu wykształcenie umiejętności świadomego wyboru dostawców usług chmurowych oraz stosowania dobrych*	------ *Ćwiczenie „Bezpieczna migracja do chmury" polega na zespołowym opracowaniu planu bezpiecznej migracji danych do chmury dla fikcyjnej organizacji, gdzie uczestnicy muszą przeanalizować potrzeby firmy, wybrać odpowiednie rozwiązania i zaplanować proces z uwzględnieniem wszystkich aspektów bezpieczeństwa.*	*Wykład interaktywny połączony z prezentacją multimedialną i dyskusją grupową* *Wykład interaktywny połączony z prezentacją multimedialną i dyskusją grupową i studia przypadku. Analiza narzędzi.*

Akademia WIT w Warszawie Newelska 6, 01-447 Warszawa 22 3486 570 skills@wit.edu.pl
Certes Sp. z o.o. Hafciarska 11, 04-704 Warszawa
Polska Izba Opakowań ul. Konstancińska 11, 02-942 Warszawa

		praktyk w zakresie przechowywania i udostępniania plików.		

Efekty uczenia się na poziomie wiedzy, umiejętności i kompetencji społecznych (postaw)

- **Zrozumienie zagrożeń cybernetycznych**: zdobędą wiedzę na temat różnorodnych zagrożeń cybernetycznych, w tym typów ataków, wirusów i malware. Będą w stanie rozpoznać potencjalne ryzyka związane z cyberbezpieczeństwem.
- **Umiejętność identyfikacji i zarządzania ryzykiem**: będą potrafili identyfikować i oceniać ryzyko w kontekście cyberbezpieczeństwa oraz podejmować działania w celu jego zarządzania i ograniczenia.
- **Zdolność do stosowania narzędzi i technik ochrony**: zdobędą umiejętności w zakresie konfiguracji i zarządzania narzędziami zabezpieczającymi, takimi jak firewall, antywirusy, IPS, IDS, oraz wdrażania technik szyfrowania danych i komunikacji.
- **Umiejętność tworzenia planów bezpieczeństwa**: będą w stanie opracować plany bezpieczeństwa zarówno na poziomie infrastruktury, jak i aplikacji, uwzględniając zabezpieczenia sieciowe i bazy danych.
- **Zwiększona świadomość i edukacja w zakresie cyberbezpieczeństwa**: będą świadomi znaczenia bezpieczeństwa w środowisku pracy oraz zdolni do rozpowszechniania wiedzy na temat cyberbezpieczeństwa w swojej organizacji i zachęcania do praktyk bezpiecznego korzystania z technologii.

Informacje dodatkowe – metody szkoleniowe:
Szkolenie realizowane metodami interaktywnymi i aktywizującymi tj. symulacje, case study, scenki treningowe, ćwiczenia grupowe i indywidualne, gry i filmy szkoleniowe, dyskusje, analizy doświadczeń uczestników, dzięki czemu zdobędą wiedzę oraz rozwiną umiejętności, postawy i zachowania.

Informacje dodatkowe – szkolenia zdalne:

W przypadku szkoleń online będą one realizowane przy pomocy platformy Microsoft Teams, która zapewni wszystkie niezbędne narzędzia do efektywnego prowadzenia zajęć, takie jak możliwość podziału uczestników na mniejsze grupy w osobnych pokojach, współdzielenie ekranu, czat czy wirtualną tablicę. Wykorzystanie Microsoft Teams pozwoli na płynną realizację wszystkich zaplanowanych ćwiczeń i aktywności, przy jednoczesnym zachowaniu wysokiego poziomu interakcji między uczestnikami oraz trenerem. Dodatkowo, dzięki zintegrowanym funkcjom platformy Microsoft Teams możliwe będzie sprawne udostępnianie materiałów szkoleniowych, przeprowadzanie ankiet czy quizów.

Akademia WIT w Warszawie Newelska 6, 01-447 Warszawa 22 3486 570 skills@wit.edu.pl
Certes Sp. z o.o. Hafciarska 11, 04-704 Warszawa
Polska Izba Opakowań ul. Konstancińska 11, 02-942 Warszawa