



Szkolenie: Reagowanie na incydenty i kryzysy marketingowe.

Numer usługi 2025/08/21/165231/2951883

4 700,00 PLN brutto

4 700,00 PLN netto

293,75 PLN brutto/h

293,75 PLN netto/h

ACTIVE PROFIT
SPÓŁKA Z
OGRANICZONĄ
ODPOWIEDZIALNOŚ
CIĄ

★★★★★ 5,0 / 5

474 oceny

📍 Olsztyn / stacjonarna

🏠 Usługa szkoleniowa

🕒 16 h

📅 18.11.2025 do 19.11.2025

Informacje podstawowe

Kategoria

Biznes / Marketing

Grupa docelowa usługi

Grupą docelową szkolenia są właściciele firm, którzy samodzielnie zarządzają swoją obecnością w internecie lub współpracują z niewielkim zespołem marketingowym. Osoby te prowadzą działania promocyjne w mediach społecznościowych, korzystają z płatnych kampanii reklamowych, lecz nie posiadają formalnego przygotowania w zakresie cyberbezpieczeństwa. Cechuje ich wysoka odpowiedzialność za operacyjne i wizerunkowe aspekty działalności firmy, przy ograniczonym dostępie do specjalistycznego wsparcia IT. Szkolenie jest skierowane do osób, które chcą świadomie reagować na incydenty bezpieczeństwa w obszarze marketingu cyfrowego, zrozumieć mechanizmy zagrożeń oraz budować odporność swojej firmy na przyszłe ataki.

Minimalna liczba uczestników

1

Maksymalna liczba uczestników

1

Forma prowadzenia usługi

stacjonarna

Liczba godzin usługi

16

Podstawa uzyskania wpisu do BUR

Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Celem szkolenia jest przygotowanie właściciela firmy do samodzielnego rozpoznania i skutecznego zarządzania incydem bezpieczeństwa w obszarze marketingu cyfrowego. Uczestnik nauczy się szybko reagować na zagrożenia, minimalizować ich skutki operacyjne i wizerunkowe, właściwie komunikować się z odbiorcami oraz planować działania naprawcze i prewencyjne zwiększające odporność cyfrową firmy.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik identyfikuje symptomy potencjalnego incydentu w kanałach marketingowych.	Wskazuje poprawnie przynajmniej trzy sygnały świadczące o naruszeniu w kontekście social media, stron WWW lub kampanii reklamowych.	Test teoretyczny
Uczestnik określa, które zasoby należy izolować i w jakiej kolejności.	Poprawnie porządkuje działania izolacyjne według priorytetów bezpieczeństwa.	Test teoretyczny
Uczestnik wyjaśnia procedurę zabezpieczenia kont po incydencie.	Opisuje kolejność działań w zakresie przywracania bezpieczeństwa kont (hasła, tokeny, loginy).	Test teoretyczny
Uczestnik planuje sposób komunikacji z zespołem i klientami.	Dobiera właściwe kanały i formy komunikatu do typu odbiorcy.	Test teoretyczny
Uczestnik opisuje zasady dokumentowania incydentu marketingowego.	Wymienia elementy, które należy zarchiwizować jako dowody.	Test teoretyczny
Uczestnik wskazuje kroki do przywrócenia działania stron i kampanii po incydencie.	Porządkuje działania techniczne i komunikacyjne umożliwiające kontynuację kampanii.	Test teoretyczny
Uczestnik analizuje przyczyny incydentu i planuje działania zapobiegawcze.	Wskazuje minimum dwa działania, które należy wdrożyć po incydencie.	Test teoretyczny
Uczestnik rozpoznaje techniki wzmacniania bezpieczeństwa środowiska marketingowego.	Wybiera odpowiednie środki zabezpieczające zgodnie z charakterem kampanii.	Test teoretyczny
Uczestnik formułuje podstawowe założenia edukacji zespołu w kontekście bezpieczeństwa.	Wymienia kluczowe tematy szkoleń dla zespołu marketingowego.	Test teoretyczny
Uczestnik rozpoznaje, kiedy i jak angażować dostawców zewnętrznych.	Określa sytuacje wymagające kontaktu z platformą lub dostawcą usług.	Test teoretyczny
Uczestnik wskazuje podstawowe metryki oceny bezpieczeństwa kanałów marketingowych.	Wymienia i interpretuje przynajmniej dwie metryki bezpieczeństwa.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik konstruuje plan zwiększenia bezpieczeństwa w perspektywie krótkoterminowej.	Dobiera realistyczne i mierzalne cele na okres 30, 60 i 90 dni.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Zajęcia teoretyczne i praktyczne:

Blok I

1. Rozpoznawanie incydentów bezpieczeństwa w kanałach marketingowych (social media, strony WWW, kampanie reklamowe).
2. Priorytetyzacja zasobów i triaż – co izolować i w jakiej kolejności.
3. Procedura resetowania haseł oraz unieważniania tokenów dostępowych.
4. Organizacja komunikacji wewnętrznej w zespole marketingowym w sytuacji kryzysowej.
5. Opracowanie komunikacji zewnętrznej z klientami i odbiorcami.
6. Dokumentowanie przebiegu incydentu i zabezpieczanie materiału dowodowego.
7. Działania umożliwiające szybkie przywrócenie stron internetowych i kampanii reklamowych.
8. Podsumowanie dnia pierwszego i omówienie najważniejszych wniosków operacyjnych.

Blok II

1. Analiza przyczyn incydentu (post-mortem) i planowanie działań korygujących.
2. Wdrażanie zasad hardeningu środowiska marketingowego po ataku.
3. Edukacja i zwiększanie świadomości zespołu w zakresie cyberbezpieczeństwa.
4. Nawiązywanie i utrzymywanie współpracy z dostawcami technologii i platformami zewnętrznymi.
5. Wybór i interpretacja podstawowych metryk bezpieczeństwa oraz przeglądy cykliczne.
6. Opracowanie planu bezpieczeństwa na 30, 60 i 90 dni dla małej firmy.
7. Stworzenie checklisty gotowości na przyszłość i procedur prewencyjnych.
8. Podsumowanie szkolenia i omówienie dobrych praktyk do wdrożenia.
9. Walidacja.

Grupą docelową szkolenia są właściciele firm, którzy samodzielnie zarządzają swoją obecnością w internecie lub współpracują z niewielkim zespołem marketingowym. Osoby te prowadzą działania promocyjne w mediach społecznościowych, korzystają z płatnych kampanii reklamowych, lecz nie posiadają formalnego przygotowania w zakresie cyberbezpieczeństwa. Cechuje ich wysoka odpowiedzialność za operacyjne i wizerunkowe aspekty działalności firmy, przy ograniczonym dostępie do specjalistycznego wsparcia IT. Szkolenie jest skierowane do osób, które chcą świadomie reagować na incydenty bezpieczeństwa w obszarze marketingu cyfrowego, zrozumieć mechanizmy zagrożeń oraz budować odporność swojej firmy na przyszłe ataki.

Warunki organizacyjne:

- Szkolenie będzie miało charakter warsztatowy, łącząc teorię z praktyką w celu skutecznego przyswojenia wiedzy i umiejętności.
- W ramach szkolenia przewidziano ćwiczenia.
- Sala szkoleniowa wyposażona w materiały dydaktyczne oraz narzędzia multimedialne wspomagające proces nauki.
- Organizator zapewnia komplet materiałów szkoleniowych.
- Maksymalna liczba osób w grupie: 1.
- Czas trwania zajęć teoretycznych: około 8 h dydaktycznych - w zależności od umiejętności indywidualnych, reszta zajęć to praktyka - która będzie trwała około 8 h dydaktycznych, podczas której uczestnik zrealizuje pełen zakres praktyczny usługi rozwojowej.
- W celu potwierdzenia nabytych kompetencji uczestnik podda się walidacji w postaci testu teoretycznego, przygotowanego i zweryfikowanego przez walidatora. Test teoretyczny odbędzie się na zakończenie szkolenia. Test będzie trwał 15 minut.
- Walidator nie bierze udziału w części edukacyjnej.
- Szkolenie jest realizowane w godzinach dydaktycznych.
- W trakcie szkolenia nie ma przewidzianych przerw.

Harmonogram

Liczba przedmiotów/zajęć: 17

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 17 Rozpoznanie incydentu (social, WWW, Ads)	Paweł Reczkowski	18-11-2025	07:00	07:45	00:45
2 z 17 Triaż: co izolować i w jakiej kolejności	Paweł Reczkowski	18-11-2025	07:45	08:30	00:45
3 z 17 Resety haseł i unieważnianie tokenów	Paweł Reczkowski	18-11-2025	08:30	09:15	00:45
4 z 17 Komunikacja wewnętrzna w zespole marketingu	Paweł Reczkowski	18-11-2025	09:15	10:00	00:45
5 z 17 Komunikacja z klientami/odbiorcami (zewnętrzna)	Paweł Reczkowski	18-11-2025	10:00	10:45	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 17 Dokumentowanie incydentu i dowodów	Paweł Reczkowski	18-11-2025	10:45	11:30	00:45
7 z 17 Szybkie przywrócenie działań (strony/kampanie)	Paweł Reczkowski	18-11-2025	11:30	12:15	00:45
8 z 17 Podsumowanie dnia pierwszego	Paweł Reczkowski	18-11-2025	12:15	13:00	00:45
9 z 17 Post-mortem i planowanie poprawek	Paweł Reczkowski	19-11-2025	07:30	08:15	00:45
10 z 17 Hardening środowiska kampanii po ataku	Paweł Reczkowski	19-11-2025	08:15	09:00	00:45
11 z 17 Szkolenia i podnoszenie świadomości zespołu	Paweł Reczkowski	19-11-2025	09:00	09:45	00:45
12 z 17 Współpraca z dostawcami i platformami	Paweł Reczkowski	19-11-2025	09:45	10:30	00:45
13 z 17 Metryki bezpieczeństwa i przeglądy cykliczne	Paweł Reczkowski	19-11-2025	10:30	11:15	00:45
14 z 17 Plan 30/60/90 dni dla małej firmy	Paweł Reczkowski	19-11-2025	11:15	12:00	00:45
15 z 17 Checklista gotowości na przyszłość	Paweł Reczkowski	19-11-2025	12:00	12:45	00:45
16 z 17 Podsumowanie szkolenia	Paweł Reczkowski	19-11-2025	12:45	13:15	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 17 Walidacja	-	19-11-2025	13:15	13:30	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 700,00 PLN
Koszt przypadający na 1 uczestnika netto	4 700,00 PLN
Koszt osobogodziny brutto	293,75 PLN
Koszt osobogodziny netto	293,75 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Paweł Reczkowski

Od wielu lat związany z branżą IT, a od 8 lat właściciel firmy specjalizującej się w outsourcingu usług informatycznych. Obecnie koncentruje się na doradztwie w zakresie widoczności marek w internecie oraz wzmacnianiu bezpieczeństwa cyfrowego w firmach produkcyjnych i usługowych.

Jako trener i konsultant dzieli się praktycznym doświadczeniem, pokazując jak nowe technologie – w tym sztuczna inteligencja – mogą wspierać rozwój biznesu i chronić organizacje przed zagrożeniami w sieci.

W ostatnich latach 2020 - 2025 przeprowadził ponad 50 godzin szkoleń z obszaru IT, AI i cyberbezpieczeństwa oraz ponad 80 godzin doradztwa dla przedsiębiorstw, które chcą skuteczniej działać online i zwiększać swoją konkurencyjność.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik otrzyma komplet materiałów edukacyjnych, w tym skrypty i zestawy ćwiczeń.

Warunki uczestnictwa

Grupą docelową szkolenia są właściciele firm, którzy samodzielnie zarządzają swoją obecnością w internecie lub współpracują z niewielkim zespołem marketingowym. Osoby te prowadzą działania promocyjne w mediach społecznościowych, korzystają z płatnych kampanii reklamowych, lecz nie posiadają formalnego przygotowania w zakresie cyberbezpieczeństwa. Cechuje ich wysoka odpowiedzialność za operacyjne i wizerunkowe aspekty działalności firmy, przy ograniczonym dostępie do specjalistycznego wsparcia IT. Szkolenie jest skierowane do osób, które chcą świadomie reagować na incydenty bezpieczeństwa w obszarze marketingu cyfrowego, zrozumieć mechanizmy zagrożeń oraz budować odporność swojej firmy na przyszłe ataki.

Uczestnicy zobowiązani są do 100% obecności na szkoleniu.

Informacje dodatkowe

Cena usługi nie obejmuje kosztów niezwiązanych bezpośrednio z usługą rozwojową, w szczególności kosztów środków trwałych przekazywanych Uczestnikom/- czkom projektu, kosztów dojazdu i zakwaterowania.

Podstawa zwolnienia z VAT: Usługa podlega zwolnieniu z podatku od towarów i usług na podstawie §3 pkt 1,14 rozporządzenia Ministra Finansów z 20 grudnia 2013 roku w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (t. jedn. Dz. U. z 2020 r., po. 1983.).

Uczestnik wymagający specjalnych udogodnień proszony jest o zgłoszenie ich przed szkoleniem do trenera, tak aby ten mógł odpowiednio przygotować salę szkoleniową bądź dostosować materiały do indywidualnych potrzeb uczestnika.

Adres

ul. Franciszka Barcza 54/3
10-611 Olsztyn
woj. warmińsko-mazurskie

Udogodnienia w miejscu realizacji usługi

- Wi-fi

Kontakt



Adrian Sadowski

E-mail activeprofitspzo@gmail.com

Telefon (+48) 572 347 308