



AFFINITY

Partnerski program po partnersku

Ubezpieczenia affinity to produkty skierowane do specyficznych grup klientów, zdefiniowanych na podstawie wspólnych cech, takich jak zawód, zainteresowania czy przynależność do określonej organizacji lub stowarzyszenia.

powane samodzielnie. Czasem wręcz niedostępne indywidualnie.

Dzięki affinity klienci zyskują prosty w zakupie dostęp do ubezpieczeń bez konieczności samodzielnego wyszukiwania oferty na rynku.

Przykłady zastosowań to:

Ubezpieczenia sprzętu elektronicznego oferowane przez sklepy elektroniczne, np. dodatkowa ochrona telefonów komórkowych.

Ubezpieczenia kosztu zakupu biletu/karnetu na wydarzenia, czyli ubezpieczenie rezygnacji z udziału w koncercie, festiwalu, rozgrywce sportowej lub innym przedpłaconym abonamencie, oferowane przez aplikacje dystrybucyjne.

Polisy zdrowotne i na życie oferowane przez organizacje zawodowe, takie jak izby lekarskie czy prawnicze.

Ubezpieczenia turystyczne sprzedawane przez linie lotnicze lub biura podróży.

Powyższe przykłady mają trzy główne cele:

1. **Zwiększenie dostępności ubezpieczeń** – klienci mogą łatwiej skorzystać

z produktów ubezpieczeniowych, które są oferowane bezpośrednio przez ich zaufanych partnerów.

2. **Zwiększenie lojalności klientów** – oferowanie ubezpieczeń dopasowanych do potrzeb danej grupy może zwiększyć lojalność wobec marki, która te produkty dystrybuuje. Np. użytkownicy aplikacji zakupowej (biletów na wydarzenia) będą częściej i lojalnie z niej korzystać, wiedząc, że odpowiednio stworzony produkt ubezpieczeniowy niesie dla nich realne korzyści w postaci zwrotu wydatków za bilet w sytuacji, kiedy nie będą mogli z niego skorzystać.

3. **Rozszerzenie oferty i możliwości zarobku dla partnerów** – partnerzy, jak np. sklepy e-commerce czy banki, mogą dzięki temu wprowadzać nowe produkty do swojej oferty, generując dodatkowe przychody bez konieczności inwestowania w skomplikowane struktury sprzedaży ubezpieczeń.

Partnerstwo

Kluczowe jest jednak partnerstwo wszystkich zaangażowanych stron.

Zaczynając od stworzenia takiego programu, jego wdrożenia, a następnie weryfikacji jego użyteczności w czasie.

Z naszego doświadczenia dla programu Going Pro Ticket oferowanego przez Unię wszystkie te elementy zadziałały i działają. Usługa jest łatwo dostępna na stronach dystrybutora, spełniając wszystkie wymagania prawne. Klienci kupują ubezpieczenia na bieżąco i korzystają z nich w razie potrzeby.

Z analiz prowadzonych przez ubezpieczyciela wynika, że świadczenia są wypłacane sprawnie. Co więcej, skala rezygnacji jest bardzo niska. A klienci z biegiem czasu wykształcili nawyk korzystania z opcji zakupu ubezpieczenia. Zatem po prawie dwóch latach wiemy, że był to projekt potrzebny i jest cały czas używany. To oczywiście skłania wszystkich partnerów do realizacji nowych projektów, na które czeka rynek.

Grzegorz Waszkiewicz
BezpierzenstwBiznesie.pl

Ubezpieczenia mogą być oferowane przez partnerów, takich jak stowarzyszenia zawodowe, banki, kluby sportowe, sieci handlowe, a także platformy e-commerce. Dzięki współpracy z tymi podmiotami ubezpieczyciele mają dostęp do szerokiej bazy klientów, co pozwala im na skuteczne dotarcie do grupy docelowej.

Do czego służą i po co istnieją ubezpieczenia affinity?

Podstawową funkcją ubezpieczeń affinity jest dostarczenie rozwiązań, które odpowiadają konkretnym potrzebom danej grupy klientów. Produkty te są często personalizowane, co oznacza, że mogą być bardziej atrakcyjne pod względem warunków lub ceny niż standardowe polisy ku-



DYREKTYWA UE W SPRAWIE BEZPIECZEŃSTWA SIECI I SYSTEMÓW INFORMACYJNYCH

NIS2 a ubezpieczenia cybernetyczne

W 2023 r. weszła w życie Dyrektywa NIS2 ustanawiająca standardy bezpieczeństwa informatycznego. Nowe przepisy powinny być stosowane we wszystkich krajach Unii Europejskiej od 18 października 2024 r.

poszerzenie katalogu sektorów objętych działaniem dyrektywy poprzez podział na sektory kluczowe i ważne.

Za **podmioty kluczowe** uznaje się podmioty z sektorów, takich jak: energetyka, transport, bankowość, infrastruktura rynków finansowych, opieka zdrowotna, woda pitna, ścieki, infrastruktura cyfrowa, zarządzanie usługami ICT, administracja publiczna, przestrzeń kosmiczna.

Z kolei **podmioty ważne** to firmy działające w sektorze usług pocztowych i kurierskich, gospodarowania odpadami, produkcji, wytwarzania i dystrybucji chemikaliów oraz żywności, badań naukowych oraz dostawy usług cyfrowych.

W kontekście ubezpieczeń od ryzyka cybernetycznych dyrektywa NIS2 może mieć kilka istotnych powiązań:

1. **Obowiązki raportowania:** Przedsiębiorstwa objęte dyrektywą NIS2 będą zobowiązane do zgłaszania incydentów związanych z bezpieczeństwem cyfrowym. Ubezpieczenie od ryzyka cybernetycznych może obejmować pokrycie kosztów związanych z takim raportowaniem oraz działań naprawczych.

2. **Zarządzanie ryzykiem:** Dyrektywa NIS2 nakłada obowiązek na organizacje, by wdrażały odpowiednie środki bezpieczeństwa oraz zarządzania ryzykiem cybernetycznym. Polisa może pomóc w całościowym zabezpieczeniu organizacji przed skutkami finansowymi incydentów cybernetycznych, na wypadek gdyby posiadane systemy i procedury zawiodły.

3. **Odpowiedzialność prawna:** W przypadku incydentów bezpieczeństwa organizacje mogą ponosić odpowiedzialność cywilną. Polisy

ubezpieczeniowe mogą obejmować ochronę przed roszczeniami wynikającymi z tych incydentów.

4. **Podnoszenie świadomości:** Z perspektywy ubezpieczycieli dyrektywa NIS2 może skłonić przedsiębiorstwa do większej dbałości o bezpieczeństwo cyfrowe, co w rezultacie może wpłynąć na warunki ubezpieczenia i stawki.

W praktyce organizacje, które chcą zabezpieczyć się przed ryzykiem cybernetycznym, powinny rozważyć zarówno zgodność z dyrektywą NIS2, jak i odpowiednią polisę ubezpieczeniową, która może stanowić istotne wsparcie w przypadku incydentów związanych z bezpieczeństwem cybernetycznym.

Maciej Strużek
prawnik, broker ubezpieczeniowy
Equinum Broker

Dyrektwa NIS2 (Dyrektwa Unii Europejskiej w sprawie bezpieczeństwa sieci i systemów informacyjnych) to regulacja, która ma na celu zwiększenie bezpieczeństwa cybernetycznego w Europie. Jest ona rozszerzeniem wcześniejszej dyrektywy NIS (Network and Information Security) i dotyczy zwiększenia obowiązków w zakresie ochrony systemów informacyjnych oraz zarządzania ryzykiem cybernetycznym.

Jedną z istotnych zmian w porównaniu z dotychczasową regulacją jest