PARAMETRY USŁUGI
OCHRONA DDOS

T-Mobile oferuje nieprzerwaną ochronę witryn internetowych firm i centrów danych przed atakami DDoS. Monitorujemy sieć IP pod kątem aktywności wykraczającej poza zdefiniowane normy, blokując wszelki wykryty ruch złośliwy i przepuszczając ruch pożądany.

ELEMENTY USŁUGI:

- Monitorowanie

T-Mobile aktywnie monitoruje i analizuje ruch przychodzący, analizując w nim wszelkie anomalie i niedozwolone sygnatury, profile ruchu i najnowsze identyfikujące go wzorce.

- Przeciwdziałanie

T-Mobile oferuje indywidualnie dostosowany plan ochrony, oparty na światowej klasy technologiach czyszczenia ruchu oraz procedury operacyjne, umożliwiające odfiltrowywanie złośliwego ruchu, stosowane przez naszych ekspertów do ochrony przed atakami DDoS.
Wykrycie ataku powoduje aktywację planu ochrony. Pierwszym jego etapem jest przekierowanie ruchu do centrum czyszczenia. Dbamy o jakość naszych usług, więc przed podjęciem działań kontaktujemy się z Klientem, upewniając się, czy wykryta anomalia nie jest przypadkiem fałszywym alarmem. T-Mobile nie tylko wdraża kluczowe technologie sieciowe. Zapewniamy także bieżącą ochronę, dostosowując ją do zmiennej dynamiki danego ataku DDoS.
Abonent usługi Ochrona DDoS otrzymuje dostęp do portalu (Network Intelligence Portal), umożliwiającego wgląd w czasie rzeczywistym w raporty i analizy dotyczące ruchu sieciowego.

FUNKCJA / USŁUGA	MONITOROWANIE	OCHRONA	MONITOROWANIE I OCHRONA
Wsparcie 24/7	+	+	+
Nieograniczona liczba działań ochronnych		+	+
Rozliczenia niezależne od liczby ataków		+	+
Brak opłat za przekierowywanie ruchu złośliwego		+	+

Dostęp do raportów bieżących w portalu Network Intelligence Portal	+		
Wykrywanie zdarzeń, wysyłanie alertów i raportowanie niemal w czasie rzeczywistym	+		+
Powiadamianie autoryzowanych kontaktów przez e-mail /SMS / telefon	+		+
Raporty	Miesięczny raport podsumowujący		
Gwarantowany poziom świadczenia usług	+	+	+
Czas do rozpoczęcia ochrony		30 minut	15 minut
Czas do powiadomiania			15 minut
Dostępność usługi	99,99%		

Według najnowszych danych, liczba ataków DDoS wzrosła w ciągu ostatniego roku o 20%, a ich przeciętna skala sięga nawet 40-50Gbps. Ich intensywność i zaawansowanie sprawia, że tradycyjne metody ochrony – np. miejscowe stosowanie urządzeń brzegowych lub podnoszenie przepustowości łącz – przestały już być wystarczające. Jedynym sposobem zapewnienia najwyższego poziomu ciągłości biznesowej są obecnie operatorskie rozwiązania sieciowe.

Proces ochrony zachowania ciągłości biznesowej działa sprawnie i szybko:
1. Planowanie. Opracowanie i wdrożenie planu ochrony dostosowanego do potrzeb Klienta.
2. Ciągły monitoring. Dane przychodzące i wychodzące przepływają zwykłą, niezmienioną trasą. System monitorowania ataków DDoS na bieżąco i nieprzerwanie analizuje otrzymywany ruch, porównując jego parametry z ustalonymi wartościami progowymi.
3. Próba ataku DDoS. Gdy system monitorowania T-Mobile wykryje zagrożenie, rejestruje je i natychmiast powiadamia o nim personel T-Mobile i Klienta za pomocą SMS i e-mail. Ekspert T-Mobile niezwłocznie sprawdza i klasyfikuje zdarzenie, po czym kontaktuje się z klientem w celu poinformowania go o sytuacji.
4. Mitygacja ataku DDoS. Klasyfikacja zdarzenia jako ataku DDoS powoduje uruchomienie przez eksperta T-Mobile procedury eliminacji zagrożenia. W ciągu mniej niż sekundy ruch przychodzący zostaje przekierowany do centrum czyszczenia ruchu T-Mobile (gdzie odbywa się jego tzw. scrubbing) i aplikacja internetowa Klienta odzyskuje pełną dostępność. Aby osiągnąć najwyższy standard ochrony, personel techniczny T-Mobile będzie monitorować zdarzenie dopóki, dopóty wykrywany będzie strumień złośliwego ruchu kierowanego w stronę sieci Klienta.
5. Koniec ataku DDoS. Gdy odpowiednie wskaźniki czasowe pozwolą stwierdzić powrót ruchu do normy, ekspert T-Mobile zakończy procedurę zapobiegawczą i przekieruje ruch na normalną ścieżkę.