**PKP INTERCITY S.A.**
Biuro Teleinformatyki
02-305 Warszawa
Aleje Jerozolimskie 142A

**BST-P6/076/10/2022**

## Z A P Y T A N I E  O  I N F O R M A C J Ę

**Zwracamy się do Państwa z prośbą o udzielenie informacji cenowej w poniższym zakresie.**

| Funkcjonalność | Metoda realizacji |
|---|---|
| Opis ogólny rozwiązania | Proponowane rozwiązanie powinno być przeznaczone do zaawansowanej ochrony serwisów www w wersji desktopowej oraz mobilnej w szczególności do ochrony API oraz do zarządzania i ochrony przed ruchem botów.<br><br>Rozwiązanie powinno być kompatybilne z ekosystemem działającym obecnie na serwisach należących do PKP Intercity, który to ekosystem zawiera funkcjonalności:<br>• ochrony strony www przy użyciu Web Application Firewalla<br>• dostarczenia i przyspieszenia aplikacji za pośrednictwem rozproszonej platformy serwerów CDN (Edge)<br>• rozłożenia ruchu pomiędzy różne data center warstwie aplikacyjnej (load balancing),<br>• DNS autorytatywny<br>• pełnego polskojęzycznego wsparcia w zakresie wdrożenia powyższych produktów i obsługi powdrożeniowej (support 24/7)<br>• bieżącej ekspertyzy dotyczącej działających rozwiązań<br>• zapewnienia odpowiednich poziomów SLA dla dostępności platformy oraz mitygacji ataków<br><br>Z ww. ekosystemem rozwiązanie powinno posiadać wspólny i ogólnodostępny interfejs. |
| Platforma CDN (Edge) | Platforma, na której musi być oparte rozwiązanie, powinna posiadać serwery w Polsce (minimum 10 lokalizacji), Europie Środkowo-Wschodniej (minimum 40 lokalizacji) oraz na terenie całej Europy (ponad 300 lokalizacji).<br><br>Dostępność platformy CDN objęta 99,99% SLA.<br><br>Musi istnieć możliwość limitowania obsługi aplikacji jedynie do serwerów CDN znajdujących się na terenie Unii Europejskiej.<br><br>CDN musi posiada własny protokół, umożliwiający dostarczenie contentu alternatywną ścieżką w stosunku do tej, proponowanej przez protokół BGP, co przekłada się na dodatkowe przyspieszanie działania aplikacji. |

| | |
|---|---|
| Monitoring | Platforma powinna udostępniać funkcjonalność monitorowania traffic-u, użytkowników oraz warstwy bezpieczeństwa, pod kątem:<br>• Ruchu webowego na naszej aplikacji, (w podziale na Edge hits, wolumen – GB, URL, odpowiedzi z origina, pochodzenie użytkowników – typy systemów operacyjnych, przeglądarek, pochodzenia geograficznego)<br>• poziomu offload-u (redukcja obciążenia infrastruktury – ilość traffic-u przejętego przez platformę vs tego, który dotarł do origina)<br>• typów ataków w podziale na ich pochodzenie (IP, region), składnię (możliwość sprawdzenia jakie zapytanie zostało wykorzystane w trakcie ataku), typ ataku (m.in. SQL Injection, Local File Inclusion, Cross Site Scripting, Web Protocol Attack oraz inne)<br>• sprawdzenia która warstwa ochrony została wykorzystana DDoS/Rate Controls/WAF/IP<br>• możliwość sprawdzenia powyższych danych na 90 dni wstecz<br>• monitoring ruchu na API<br>• zaawansowany monitoring ruchu botów |
| Funkcjonalności dla ochrony API | • Automatyczne wykrywanie i profilowanie nieznanych i zmieniających się API<br>• Ochrona backendu (infrastruktury) należącego do API od ataków typu low and slow<br>• Ochrona API przy użyciu rate controls dla punktów końcowych, bazujących na API key/endpoint/HTTP<br>• Zdefiniowanie dozwolonych requestów API wg klucza, pozwalające na pełną kontrolę zużycia (każdy klucz powinien być definiowalny niezależnie)<br>• Możliwość cache-owania calli API<br>• Zarządzanie cyklem życia (lifecycle) API wraz z możliwością wersjonowania<br>• Bezpieczna autentykacja i autoryzacja poprzez walidację JSON Web Token (JWT)<br>• Możliwość manualnej definicji, rejestracji oraz uploadu standardowych definicji API (Swagger/OAS oraz RAML)<br>• Możliwość ustawienia pozytywnego modelu bezpieczeństwa, bazując na definicjach. Tylko te API calle, które korespondują z definicjami nie będą blokowane.<br><br>Rozwiązanie powinno być kompatybilne z firewallem aplikacyjnym wraz z możliwością ustawienia oddzielnych konfiguracji dla poszczególnych hostname-ów, manualnego doboru reguł i dostępu do security operations center). |

| | |
|---|---|
| Funkcjonalności dla ochrony przed ruchem botów oraz do zarządzania ruchem botów | Zarządzanie botami partnerskimi (poprzez whitelistowanie lub wdrożenie oddzielnej akcji - spowolnienia lub wydzielenia API)<br><br>Zarządzanie ruchem botów, bazujące na pasywnych modelach detekcji. Możliwości wykrycia:<br>• impersonatorów (botów podszywających się pod wiarygodne requesty),<br>• niepożądanych user agentów,<br>• anomalii requestów,<br>• złej reputacji danego botnetu,<br>• naruszenia polityki rate controli<br><br>Zarządzanie ruchem botów, bazujące na aktywnych metodach detekcji, w tym:<br>• naruszona integralności cookie,<br>• walidacja sesji (session validation),<br>• walidacja przeglądarki,<br>• walidacja cyklu (workflow)<br><br>Klasyfikacja botów przez producenta. Pokazanie wiarygodnych danych, dotyczących zachowania danego botnetu w internecie. Możliwość podglądu w jaki sposób atakowane strony podejmują akcje wobec danego botnetu.<br><br>Rozwiązanie powinno dawać możliwość rozbudowy o kolejne moduły, w tym moduły zbierające dane telemetryczne z requestu użytkownika końcowego, oraz moduły pozwalające na rating użytkowników końcowych i weryfikację, czy nie dochodzi do ewentualnego impersonowania (podszywania) pod innego usera na poziomie strony z loginem. |
| SLA na dostępność | Wymagane SLA na dostępność platformy - 99,99%. |
| Brak limitu ataku | Wielkość ataku nie jest w żaden sposób limitowana. |
| Dodatkowe opłaty za ataki | Dodatkowe opłaty za obsługę ataków nie mogą być naliczane |
| Przekroczenie szacowanego progu ruchu | Dodatkowe opłaty za przekroczenie miesięcznej estymowanej wartości traffic-u nie mogą być naliczane (Fixed price) |
| Support i obecność w Polsce | Gwarancja dostępu do polskojęzycznego wsparcia.<br>Support musi być dostępny w trybie 24/7 z możliwością zgłoszeń elektronicznych oraz telefonicznych. |
| Services Management Package | Dedykowany ekspert odpowiedzialny za bieżącą asystę w konfiguracji i tuningu rozwiązania do aktualnych potrzeb. |

**Wymagane warunki supportu oraz SLA na mitygację ataków**

PKP INTERCITY S.A.
Biuro Teleinformatyki
02-305 Warszawa
Aleje Jerozolimskie 142A

**1) SLA na mitygację**

Producent powinien oferować SLA, określające maksymalny czas, potrzebny na mitygację określonego typu ataku. Mitygacja ataku oznacza, że akcje podjęte proaktywnie na platformie w stosunku do ruchu, dotyczącego Zamawiającego, zagrażającego serwisowi webowemu Zamawiającego, który jest dostarczany przez platformę, podjęte zgodnie z konfiguracją konta klienta, okazały się skuteczne i atak został zatrzymany w czasie określonym w poniższej tabeli.

| Attack Type | TTM - Time to Mitigate (typical) | TTM – Time to Mitigate - Guaranteed (Service Level) |
|---|---|---|
| * UDP/ICMP Floods | 0 seconds | 0 seconds |
| * SYN Floods | 0 seconds | 0 seconds |
| * TCP Flag Abuses | 0 seconds | 0 seconds |
| * DNS Reflection | 0 seconds | 0 seconds |
| * DNS Attack | 0 seconds | 0 seconds |

**2) SLA na dostępność platformy:**

99,99% Dostępności: Platforma będzie dostarczała content Zamawiającego przez 99,99% czasu. W przypadku przerw w dostępności platformy i braku możliwości dostarczania contentu z uwagi na niedziałającą platformę, okres w którym platforma była niedostępna może zostać skredytowany po wcześniejszym zgłoszeniu tego przypadku do producenta. Przez skredytowanie rozumie się proporcjonalny zwrot opłaty, jedynie za okres, w którym platforma nie była dostępna, na podstawie wzoru:
- [czas niedostępności (minuty) / 43800 (minut) ] * opłata miesięczna za całość usługi = wysokość ewentualnego zwrotu
Wysokość ewentualnego zwrotu nie może przekroczyć miesięcznej opłaty za usługę.

**3) Support:**

Zgłoszenia supportowe mogą być dokonywane 24/7/365:
- bezpośrednio u producenta bądź jego oficjalnego partnera (dane kontaktowe…….)
- w portalu producenta
- telefonicznie w jednym z kilkudziesięciu miejsc na świecie (w tym Kraków, Polska)
- mailowo

Zgłoszenia supportowe:

| | | |
|---|---|---|
| Czas odpowiedzi na zgłoszenie | Zgłoszenie krytyczne (P1) | < 2 godziny |
| | Zgłoszenie poważne (P2) | < 4 godziny |
| | Zgłoszenie niskiego priorytetu (P3) | < 2 dni robocze |

| | | |
|---|---|---|
| Dostępność Live Support | Zgłoszenie krytyczne (P1) | 24/7 |
| | Zgłoszenie poważne (P2) | Godziny Biznesowe |
| | Zgłoszenie niskiego priorytetu (P3) | Godziny Biznesowe |

Godziny biznesowe, zgodnie z położeniem geograficznym – od poniedziałku do piątku, z wyłączeniem lokalnych dni wolnych od pracy:
• Ameryki ET (GMT – 05:00) 9:00 AM to 9:00 PM
• Europa (CET) 9:00 AM to 6:00 PM
• Azja-Indie (GMT + 05:30) 9:00 AM to 6:00 PM
• Azja-Oceania (GMT + 9:00) 9:30 AM to 6:30 PM

Poziom zgłoszeń:
Zgłoszenie krytyczne (P1) – Platforma lub krytyczna aplikacja Zamawiającego nie działa lub problem ma istotny wpływ na działanie tej aplikacji, a jednocześnie rozsądne obejście problemu nie jest możliwe

Zgłoszenie poważne (P2) - Incydent ma częściowy lub umiarkowany wpływ na system lub aplikację dostarczaną przez producenta, lub zgłaszany jest pojedynczy incydent, dla którego nie ma obejścia lub jego obejście jest uciążliwe

Zgłoszenie niskiego priorytetu (P3) – P3 - niewielki wpływ: rutynowa konserwacja, żądania zmiany konfiguracji, pytania dotyczące konta lub umowy, pomoc w zarządzaniu usługami online, prośby o informacje i ogólne informacje, dotyczące serwisów producenta

PKP INTERCITY S.A.
Biuro Teleinformatyki
02-305 Warszawa
Aleje Jerozolimskie 142A

**Terminy składania pytań oraz udzielenie informacji:**

W odpowiedzi na niniejsze zapytanie prosimy przesłać:

1. Zakres wsparcia dla oferowanych urządzeń, systemu oraz klienta
2. uzupełniony formularz cenowy według wzoru w poniższej tabeli.

Termin składania informacji cenowych upływa **w dniu 10.03.2022 r. o godz. 15.00**
(ewentualne pytania prosimy kierować do dnia **07.03.2022 r. do godziny 15:00**).
Odpowiedź proszę przesłać w formie e-mail na adres: it@intercity.pl

**Formularz cenowy**

Poniższe pozycje wypełnia Oferent:

| L.P. | Przedmiot | Wartość jednostkowa za 1 mc (PLN) | Integracja Opłata jednorazowa |
|---|---|---|---|
| 1. | Kona Site Defender | | |
| 2. | Bot Manager Standard | | |
| 3. | API Gateway | | |
| **SUMA** | | | |

***„PKP INTERCITY" S.A. zastrzega, że niniejsze zapytanie nie stanowi elementu jakiegokolwiek postępowania o udzielenie zamówienia, wobec czego PKP INTERCITY S.A. nie jest zobligowane do wyboru którejkolwiek oferty. Niniejsze pismo nie stanowi również oferty w rozumieniu Kodeksu Cywilnego."***