ТЕХНІЧНІ ВИМОГИ

щодо закупівлі
код ЄЗС 021-2015 72410000-7 Послуги провайдерів (72411000-4 Постачальники Інтернет-послуг, код ЄЗС 021-2015 72411000-4)

Предметом закупівлі є послуги з підключення до мережі Інтернет інформаційної системи Замовника, розташованої за адресою **м. Київ, вул. Г.Сковороди, 2.**

Учасник процедури закупівлі для виконання Технічного завдання може запропонувати умови надання послуг, які за своїми технічними та якісними характеристиками будуть не гіршими ніж вимагається Замовником, а саме:

1) Учасник повинен забезпечити підключення інформаційної системи Замовника окремими волоконно-оптичними лініями у синхронному симетричному режимі на гарантованій швидкості:
   - каналу 1 Гбіт/с до захищеного вузла Інтернет-доступу (надалі – ЗВІД) Учасника;
   - каналу 1 Гбіт/с до точки обміну Інтернет-трафіком UA-IX за адресою м. Київ, вул. Леонтовича, 9.
2) На підтвердження наявності ЗВІД Учасник у складі тендерної пропозиції надає копію Атестату відповідності ЗВІД, зареєстрований Державною службою спеціального зв'язку та захисту інформації України, дійсний протягом всього терміну надання послуг.
3) У складі вузла доступу Учасника має бути наявна система захисту від атак класу «розподілені атаки відмови у обслуговуванні» (надалі - DDoS-атак).
4) Система захисту від DDoS-атак Учасника повинна забезпечувати наступні функції протидії кібер-загрозам:

- підсистема очищення повинна підтримувати можливість побудувати дворівневу модель захисту, дозволяючи користувачам самостійно вмикати і вимикати захист через відповідне кінцеве обладнання (CPE);
- підсистема очищення повинна використовувати поведінкові методи аналізу трафіку для блокування атак, включаючи атаки нульового дня;
- підсистема очищення повинна блокувати некоректні пакети (включно з перевіркою коректності заголовків, повноцінності фрагмента, коректності контрольної суми IP, дубліката фрагмента, довжини фрагмента, довжини пакета TCP / UDP / ICMP), коректності контрольної суми TCP / UDP, коректності TCP-прапорів) і забезпечувати статистику для відкинутих пакетів;
- підсистема очищення повинна виявляти і блокувати повільні атаки (Slowloris, Slow read і т.д.);
- підсистема очищення повинна з використовувати поведінкові методи захисту від атак на 3-м, 4-м, 5-м і 7-м рівнях моделі OSI, забезпечуючи пропуск тільки легітимного трафіку і блокування нелегітимного;
- підсистема очищення повинна виявляти і блокувати підозрілий трафік;
- підсистема очищення повинна виявляти і блокувати пульсуючі атаки, які полягають в короткочасному (кілька секунд) сплеску нелегітимного трафіку. Легітимний трафік при цьому повинен пропускатися без втрат;
- підсистема очищення повинна самостійно (без втручання оператора) виявляти і реагувати на зміну вектора атаки з часом реакції до 30 сек;
- підсистема очищення повинна обмежувати кількість одночасних TCP-з'єднань по кожному хосту;
- підсистема очищення повинна мати можливість виявляти і блокувати HTTPS атаки (або мати можливість модернізуватися до такої функціональності без заміни апаратної платформи або залучення додаткових апаратних засобів) і при цьому бути сумісна з вимогами PCI DSS;

- підсистема очищення повинна мати можливість виявляти і блокувати HTTPS page flood атаки з використанням SSL / TLS без дешифрування трафіку, використовуючи поведінкові моделі (або мати можливість модернізуватися до такої функціональності без заміни апаратної платформи або залучення додаткових апаратних засобів);
- при роботі в режимі inline підсистема очищення повинна блокувати атаки перебору піддоменів на DNS сервер, повністю пропускаючи легітимні запити і блокуючи нелегітимні;
- підсистема очищення повинна мати можливість обмежувати кількість DNS, HTTP і SIP-запитів в секунду з кожного джерела відповідно до налаштованим порогом;
- підсистема очищення повинна забезпечувати можливість конфігурувати регулярні вирази в кількості не менше 100 для відкидання певного трафіку як текстових, так і бінарних протоколів;
- підсистема очищення повинна з використовувати поведінкові методи захисту від атак на DNS, що забезпечують пропуск тільки легітимного трафіку;
- підсистема очищення повинна мати можливість здійснювати обмеження (rate limiting) трафіку по його географічним властивостями, тобто на базі країни походження трафіку;
- підсистема очищення повинна виявляти ботів, які не мають можливість розпізнавати і слідувати командам HTTP 302 redirect;
- підсистема очищення повинна виявляти ботів, які не мають можливість розпізнавати і слідувати redirect-командам, закодованим в JavaScript;
- підсистема очищення повинна мати можливість автоматично або у ручному режимі активувати нові захисні техніки за допомогою регулярного оновлення сигнатур атак, що забезпечуються дослідницької командою виробника обладнання, яка здійснює моніторинг Інтернету 24x7, ідентифікуючи найсуттєвішу і недавню активність ботнетів і стратегії нападу. Підсистема аналізу ботнетів і поточних атак повинна здійснювати глобальний моніторинг Інтернет-трафіку з метою виявлення нових методів атаки і вироблення способів протидії їм;
- підсистема очищення повинна дозволяти змінювати параметри захисту під час її роботи. Такі зміни не повинні викликати переривання трафіку;
- підсистема очищення повинна мати вбудований пакетний аналізатор і декодер, який повинен бути здатний захопити не менше 50000 пакетів, відповідно фільтру, який сконфігурований користувачем, забезпечуючи декодування для заголовків протоколів IP, TCP, UDP, ICMP, HTTP, SSL / TLS, SIP та DNS. Користувач повинен мати можливість скачати PCAP файл для його подальшого аналізу;
- при історичному аналізі атак, відображених системою очищення, повинна бути можливість отримання зразка відкинутого трафіку в форматі PCAP;
- підсистема очищення повинна забезпечувати можливість агрегації інтерфейсів Ethernet з використанням стандартних протоколів LAG або навпаки, прозоро пропускати LAG PDU в залежності від налаштувань, зроблених адміністратором;
- підсистема повинна мати можливість в рамках пропозицій при необхідності надати не менше 4x10 Gbps Ethernet інтерфейсів;
- підсистема повинна мати можливість горизонтального розширення. Розширення повинно здійснюватися без заміни використовуваної апаратної платформи або віртуалізації;
- підсистема повинна підтримувати автоматичну дворівневий захист спільно з flowspec або blackhole (при перевищенні певного порогу трафік перестає проходити через систему очищення і включається flowspec або blackhole на маршрутизаторах);
- підсистема очищення повинна мати можливість інтеграції на рівні сигналізації з системами WAF;
- в системі захисту повинна бути реалізована рольова модель управління доступом (RBAC);

- підсистема очищення повинна оновлювати інформацію, що стосується джерел, нещодавніх DDoS-атак, для запобігання атак зловмисників, перш ніж вони націлюються на мережу Замовника;
- рішення, що пропонується, не повинно передавати, обробляти, аналізувати або зберігати трафік Замовника за межами України.

5) Учасник повинен забезпечити резервування системи захисту від DDoS-атак щляхом наявності на вузлі Учасника 2 (двох) незалежних систем захисту від різних виробників на незалежних апаратних платформах.
6) Учасник повинен забезпечити для інформаційної системи Замовника підтримку автономної системи (AS) та блоку з 256 провайдеро-незалежних (PI) IP-адрес v4 без зміни діючої адресації.
7) Система управління інформаційною безпекою Учасника має відповідати міжнародному стандарту ISO 27001, на підтвердження чого Учасник повинен надати у складі пропозиції копію відповідного сертифікату.
8) Учасник повинен бути включений до переліку операторів НСКЗ.
9) Учасник має забезпечити, на період дії Договору надання послуг протягом 24 годин на добу 7 днів на тиждень.
10) Учасник повинен мати цілодобову службу технічної підтримки.
11) Учасник повинен мати можливість надання послуги динамічного розподілу маршрутизації з різноманітним рівнем швидкості до внутрішніх ресурсів Учасника та світових ресурсів.
12) Учасник повинен надавати цілодобовий доступ Замовнику до статистичних даних, щодо завантаження каналів Інтернет у реальному часі та за попередній період з моменту початку надання послуг.
13) Учасник гарантує максимально допустимий час простою відсутності послуг на місяць – не більше 4 годин.
14) Учасник повинен мати можливість підтримки протоколу маршрутизації BGP.
15) Учасник повинен забезпечити підключення у відповідності до всіх означених технічних вимог з 01 березня 2023р.

Термін надання послуг – з березня до 31 грудня 2023р.

Орієнтовна вартість закупівлі 206 100,00 грн

ПІП, підписи робочої групи

Виноград Т.Г.

Ситник К.С.