ОБГРУНТУВАННЯ

(на виконання пункту 4[1] постанови Кабінету Міністрів України від 11 жовтня 2016 р. № 710 «Про ефективне використання бюджетних коштів»)

1. **Предмет закупівлі:** Програмна продукція для захисту служби каталогів Active Directory (AD)

(ДК 021:2015 код 48210000-3 «Пакети мережевого програмного забезпечення»).

2. **Вид процедури:** відкриті торги з особливостями.
3. **Номер оголошення закупівлі:** UA-2024-04-05-011417-a.
4. **Обґрунтування технічних та якісних характеристик предмета закупівлі:**

Відповідно до Положення про Секретаріат Кабінету Міністрів України, затвердженого постановою Кабінету Міністрів України від 12 серпня 2009 р. № 850, основними завданнями Секретаріату є організаційне, експертно-аналітичне, правове, інформаційне, матеріально-технічне забезпечення діяльності Кабінету Міністрів України, урядових комітетів, Прем'єр-міністра України, Першого віце-прем'єр-міністра України, віце-прем'єр-міністрів України.

Служба каталогів Active Directory (AD) є основним засобом авторизації та автентифікації користувачів локальної мережі. Пошкодження служби каталогів внаслідок помилкових дій адміністратора або кібератаки може призвести, як до неможливості підключення користувачів до локальної мережі та інформаційних ресурсів, так і навпаки, до несанкціонованого підвищення рівня прав окремих облікових записів.

Програмна продукція для захисту служби каталогів Active Directory забезпечує:

-можливість безперервного аналізу і пошук помилок в конфігураціях, а також шляхи проведення атак на основі постійного аналізу конфігурацій служби каталогів AD;

-вбудовані сценарії перевірки вразливостей та поведінки роботи служби каталогів AD;

-пріоритезацію «слабких місць» і помилок в конфігураціях служби каталогів AD;

-отримання рекомендацій щодо застосування коректних виправлень для конкретних вразливостей та існуючих шляхів потенційних атак на службу каталогів AD;

-відстежування всіх змін об'єктів та атрибутів служби каталогів AD в реальному часі з вказанням параметру, який змінився, значення параметру до зміни та нового значення параметру;

-можливість виявляти вразливості конфігурації, зокрема:

- Незв'язаний, вимкнений або втрачений об'єкт групової політики.
- Облікові записи з безстроковими паролями.
- Небезпечні довірчі відносини.
- «Сплячі» облікові записи.
- Нативні члени адміністративної групи.
- Остання зміна пароля KDC.
- Комп'ютери зі застарілою ОС.
- Використання слабких криптографічних алгоритмів у Active Directory PKI.
- Відключені облікові записи у привілейованих групах.
- Облікові записи, які використовують систему контролю доступу, сумісну з перед-Windows 2000.
- Права доступу до кореневих об'єктів, що допускають атаки, подібні до DCSync.
- Управління локальним адміністративним обліковим записом.

- Домени мають застарілий функціональний рівень.
- Домен із небезпечною конфігурацією зворотної сумісності.
- Перевірка прав доступу до конфіденційних об'єктів GPO та файлів.
- До користувачів застосовуються політики слабких паролів.
- Контролери домену під керуванням нелегітимних користувачів.
- Перевірка дозволів, пов'язаних з обліковими записами AAD Connect.
- Обліковий запис користувача зі старим паролем.
- Небезпечні права у схемі AD.
- Підтвердження останньої зміни пароля облікового запису AAD SSO.
- Користувачі, яким дозволено приєднувати комп'ютери до домену.
- Обліковий запис, який може мати порожній пароль.
- Група захищених користувачів не використовується.
- Домен без об'єктів групової політики, що підвищують безпеку комп'ютера.
- Зіставлені сертифікати облікових записів користувачів.
- Небезпечні конфіденційні привілеї.
- Можливий пароль у відкритому вигляді.

-зберігання всіх змін об'єктів та атрибутів служби каталогів AD у власній базі даних для запитів та аналізу історичних даних про проведенні розслідування;

-виявлення основних типів і методів, що використовуються при кібератаках на служби каталогів AD;

-виявлення атак в режимі реального часу;

-опис виявлених інцидентів у відповідності з MITRE ATT&CK®;

-виявлення атак на служби каталогів AD без необхідності встановлення агентів на домен контролери.

Відмова від закупівлі підписки, суттєво понизіть рівень захисту та контролю служби каталогів Active Directory (AD), що призведе до зростання вірогідності проходження кібератак цим шляхом.

5. Обґрунтування розміру бюджетного призначення:

Розмір бюджетного призначення на закупівлю програмної продукції для захисту служби каталогів Active Directory (AD) був встановлений на підставі проведених попередніх консультацій з організаціями та установами, відповідно до частини 4 статті 4 Закону України «Про публічні закупівлі», аналізу ринку щодо наявних технологічних рішень та аналізу курсу іноземних валют. Отримана інформація була використана для підготовки технічної специфікації щодо закупівлі програмної продукції.

Всі консультації та надані рекомендації не призводять до порушення статті 5 Закону України «Про публічні закупівлі».

6. Обґрунтування очікуваної вартості закупівлі:

Очікувана вартість закупівлі підтверджена проведенням моніторингу цінових пропозицій.