Toruń, dn. 19.08.2024

Urząd Miasta Torunia
Biuro Projektów Informatycznych
ul. Wały gen. Sikorskiego 10
e-mail: zp_bpi@um.torun.pl

syg. BPI.271.42.2024

--- Wg. rozdzielnika ---

W ramach badania rynku

nr BPI/C/53/2024

Biuro Projektów Informatycznych
87-100 Toruń
ul. Wały gen. Sikorskiego 10

zwraca się z uprzejmą prośbą o przesłanie w trybie badania rynku propozycji cenowej na:

zakup, dostawa, instalacja oraz konfiguracja systemu zarządzania dostępem uprzywilejowanym (Privileged Access Management - PAM) wraz z niezbędnym oprogramowaniem i licencjami zgodnie z załączoną specyfikacją

1. Proszę podać ryczałtową cenę **netto i brutto w złotych dla każdej licencji z osobna**
2. Miejsce składania ofert: Ofertę proszę dostarczyć do Biura Projektów Informatycznych UMT ul. Wały gen. Sikorskiego 10, pok.23 osobiście, lub na adres e-mail (np. w formacie PDF): zp_bpi@um.torun.pl
3. Termin składania ofert: do **26.08.2024r. do godz. 12:00 (decyduje godzina otrzymania oferty przez Zamawiającego)**
4. Wymagania i warunki Zamawiającego:
   a) W celu zapewnienia porównywalności wszystkich ofert, Zamawiający zastrzega sobie prawo do skontaktowania się z Oferentami w celu uzupełnienia lub doprecyzowania ofert.
   b) Oferent może wprowadzić zmiany w złożonej ofercie lub ją wycofać, pod warunkiem, że uczyni to przed upływem terminu składania ofert. Zarówno zmiana jak i wycofanie oferty wymagają zachowania formy pisemnej.
   c) Oferty złożone po terminie nie zostaną rozpatrzone.
5. Niniejsza oferta nie stanowi oferty w myśl art. 66 Kodeksu Cywilnego, jak również nie jest ogłoszeniem w rozumieniu ustawy Prawo zamówień publicznych.
6. Zaproszenie nie jest postępowaniem o udzielenie zamówienia publicznego w rozumieniu przepisów Prawa zamówień publicznych oraz nie kształtuje zobowiązania Zamawiającego do przyjęcia którejkolwiek z ofert.
7. **Zaproszenie ma na celu dokonanie oszacowania wartości zamówienia publicznego zgodnie z Zarządzeniem nr 247 PMT z dnia 22.09.2021r.**

Główny Specjalista
Grzegorz Hrynek

Załącznik 1

PRZEDMIOT ZAMÓWIENIA	PAM .....
ZAMAWIAJĄCY	Gmina Miasta Toruń - wydział prowadzący – Biuro Projektów Informatycznych UMT .....
WYKONAWCA **Adres** **Numer telefonu / fax** **Internet http: //** **e-mail**	
Kryterium 1. CENA OFERTY NETTO / BRUTTO (z obowiązującym podatkiem VAT)	Cyfrowo netto: ..... Cyfrowo brutto: ..... Słownie brutto: .....
Data **Podpis**	

Specyfikacja Istotnych Warunków Zamówienia (SIWZ)

1. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest zakup, dostawa, instalacja oraz konfiguracja systemu zarządzania dostępem uprzywilejowanym (Privileged Access Management - PAM) wraz z niezbędnym oprogramowaniem i licencjami.

Zakres usługi

a. Dostarczenie systemu
b. Instalacja i konfiguracja
c. Dostarczenie dokumentacji powykonawczej
d. Szkolenie dla 6 administratorów systemu

2. Wymagania funkcjonalne

Opis ogólny

Dostępne narzędzia typu PAM (*ang: Privileged Access Management*) to rozwiązanie zapewniające zarządzanie uprzywilejowanym dostępem do zasobów sieciowych. Wymagania funkcjonalne dla tego typu rozwiązania dla poprawy rozliczalności i bezpieczeństwa budowanej infrastruktury muszą obejmować przede wszystkim:

1. **Zarządzanie kontami uprzywilejowanymi**: centralne zarządzanie kontami uprzywilejowanymi, takimi jak konta administratorów, konta z dostępem root czy konta serwisowe. Powinno być możliwe tworzenie, usuwanie i modyfikowanie kont, zarządzanie hasłami, a także kontrola dostępu i uprawnień.
2. **Bezpieczne przechowywanie danych uwierzytelniających**: System powinien zapewniać bezpieczne przechowywanie danych uwierzytelniających, takich jak hasła, certyfikaty czy klucze prywatne. Dane te powinny być zaszyfrowane i chronione przed nieuprawnionym dostępem.
3. **Kontrola dostępu**: musi być możliwa kontrola dostępu do zasobów sieciowych na podstawie zasad i polityk. Powinno być możliwe definiowanie reguł i ograniczeń dostępu dla poszczególnych kont uprzywilejowanych, a także monitorowanie i rejestrowanie działań użytkowników.
4. **Audyt i monitorowanie aktywności**: System musi umożliwiać audyt i monitorowanie aktywności użytkowników posiadających uprzywilejowany dostęp. Powinno być możliwe rejestrowanie i analiza logów związanych z operacjami wykonywanymi przez konta uprzywilejowane, w celu identyfikacji potencjalnych zagrożeń i śledzenia działań.
5. **Uwierzytelnianie wieloskładnikowe**: narzędzie powinno wspierać uwierzytelnianie wieloskładnikowe (MFA), takie jak tokeny OTP, certyfikaty czy biometria. Wprowadzenie MFA zwiększa bezpieczeństwo procesu uwierzytelniania i utrudnia atakującym przejęcie kont uprzywilejowanych.
6. **Zarządzanie sesjami uprzywilejowanymi**: System powinien umożliwiać zarządzanie sesjami uprzywilejowanymi, takie jak monitorowanie i kontrola aktywnych sesji, automatyczne wylogowywanie nieaktywnych sesji czy możliwość zdalnego przerwania sesji w przypadku podejrzenia nadużyć.
7. **Integracja z innymi narzędziami i rozwiązaniami**: PAM powinien umożliwiać integrację z innymi narzędziami i rozwiązaniami, takimi jak systemy zarządzania tożsamościami (IAM), narzędzia do zarządzania incydentami czy SIEM (Security Information and Event Management). Integracja ta pozwala na lepszą koordynację działań i wykorzystanie przygotowywanej infrastruktury bezpieczeństwa.

Wymagania dla systemu PAM

1. Zapewnienie wysokiego poziomu bezpieczeństwa danych i poufności informacji
2. Wsparcie dla szyfrowania danych w transmisji i przechowywaniu haseł i kluczy
3. Elastyczność w zakresie skalowania infrastruktury w celu obsługi zwiększonego obciążenia
4. System musi posiadać Mechanizmy failover i redundancji, aby zapewnić ciągłość działania w przypadku awarii serwera lub innego komponentu
5. System PAM musi posiadać przyjazny interfejs graficzny (GUI) umożliwiający łatwe zarządzanie kontami uprzywilejowanymi i monitorowanie działań użytkowników.
6. Integracja z technologią ZTNA (Zero Trust Network Access) oraz możliwość działania jako punkt wymuszania dla ZTNA
7. Musi istnieć możliwość sprawdzania silnikiem antywirusowym przesyłanych podczas sesji plików. Kontrola musi być realizowana co najmniej dla transferu plików poprzez web (Web SFTP, Web SAMBA) oraz SCP.
8. Automatyczne blokowanie niebezpiecznych poleceń za pomocą profilu filtrowania SSH. System musi monitorować komendy wydawane przez operatora sesji.
9. System PAM powinien być dostarczony jako urządzenie na utwardzonym przez jednego producenta systemie operacyjnym w formie gotowego i pełnego rozwiązania
10. Rozwiązanie musi być dostępne w formie zarówno urządzeń wirtualnych (*virtual appliance*), jak i sprzętowych. Dla wirtualizacji musi być wspierany co najmniej hypervisor VMWare oraz KVM.
11. Działanie PAM musi pozwalać na obsługę połączeń bezpośrednich jak i proxy.
12. Możliwość obsługi niestandardowych protokołów chociażby poprzez dedykowane wyzwalacze (*custom application launcher*)
13. Możliwość ostrzegania użytkowników o nagrywaniu w celu zapewnienia zgodności z wymaganiami RODO.
14. System PAM w wersji wirtualnej musi obsługiwać moduł vTPM (*Virtual Trusted Platform Module*) dla przechowywania kluczy prywatnych użytkowników.
15. PAM musi obsługiwać mechanizm awaryjnego dostępu do zaszyfrowanych haseł przechowywanych w systemie na zasadzie procedury „glass breaking". Wszystkie działania w tym trybie muszą być logowane celem możliwości przeprowadzenia audytu.
16. System musi automatycznie nagrywać obraz podczas uruchomienia procedury awaryjnej (glass breaking)
17. Automatyczna zmiana hasła konta po poprawnym zalogowaniu
18. Wsparcie dla zaplanowanej zmiany haseł według harmonogramu
19. Możliwość tworzenia procedury żądania dostępu do haseł i zatwierdzania takich żądań poprzez konfigurowalną ilość administratorów
20. Ustawienie dedykowanego dostępu do skonfigurowanego hasła dla jednego administratora. W tym stanie dostęp jest ograniczony tylko dla jednego użytkownika uprzywilejowanego.
21. Wymagane jest wsparcie dla algorytmów szyfrowania SSH o wysokiej sile
22. Zaawansowany protokół uwierzytelniania RDP, w tym CredSSP i TLS
23. Kontrola dostępu oparta na rolach (RBAC)
24. Kontrola uprawnień oparta na użytkownikach oraz grupach użytkowników
25. Kontrola profili dostępowych w formie polityk
26. Wsparcie dla Disaster Recovery
27. Użytkownik uprzywilejowany musi mieć możliwość pracy co najmniej w następujących trybach:
    a. Agentowy – dostępne wszystkie funkcjonalności. Agent musi być dostępny bezpłatnie

b. Bezagentowo, za pomocą przeglądarki internetowej wraz z dedykowanym rozszerzeniem. Metoda ta musi umożliwiać uzupełnianie haseł przez PAM oraz nagrywanie sesji
c. Bezagentowo, za pomocą przeglądarki internetowej bez dodatkowych rozszerzeń

Uwierzytelnianie

1. Obsługa uwierzytelniania użytkowników za pomocą certyfikatów
2. Możliwość korzystania z lokalnej bazy danych użytkowników
3. Obsługa uwierzytelniania wieloskładnikowego opartego na SAML
4. Obsługa OIDC (openID Connect), SAML
5. Obsługa wielu połączeń SAML SP
6. Możliwość integracji z istniejącymi usługami uwierzytelniania, w nie mniejszym zakresie niż Active Directory, LDAP, radius.
7. Wsparcie dla integracji z istniejącymi systemami zarządzania tożsamościami
8. Możliwość obsługi większej liczby kont uprzywilejowanych w miarę rozwoju organizacji
9. Dostęp do zasobów użytkowników uprzywilejowanych musi również obejmować możliwości blokady w oparciu o dodatkowe parametry:
    a. Kontrola dostępu oparta na adresie źródłowym IP użytkownika
    b. Ograniczanie dostępu oparte na harmonogramie użytkownika
    c. Kontrola dostępu do docelowego serwera oparta o przypisane tagi ZTNA (stan stacji, z której następuje połączenie jest badany przez mechanizmy ZTNA)

Licencjonowanie

1. Oprogramowanie musi być objęte kompletną licencją producenta na całe rozwiązanie. Nie dopuszcza się dodatkowych wymagań licencyjnych dla systemu operacyjnego, bazy danych, oprogramowania serwera WWW lub podobnych.
2. Nie dopuszcza się licencjonowania ilości zasobów, do których realizowany jest nadzorowany dostęp.
3. Nie dopuszcza się licencjonowania ilości zajętego miejsca na dysku przez nagrania sesji.
4. Licencja systemu musi pozwalać na podłączenie się co najmniej 25 użytkowników do monitorowanych zasobów.

Monitorowanie i raportowanie

1. Możliwość monitorowania aktywności użytkowników z kontami uprzywilejowanymi.
2. Generowanie szczegółowych raportów audytowych w celu analizy i śledzenia działań użytkowników

Wsparcie techniczne i aktualizacje

1. Gwarancja wsparcia technicznego i dostępności aktualizacji oprogramowania w celu utrzymania systemu w aktualnym i bezpiecznym stanie musi być zapewniona na okres 36 miesięcy .
2. Dostawca rozwiązania musi zapewnić pojedynczy punkt kontaktu z pomocą techniczną dla wszystkich zainstalowanych komponentów w urządzeniu wirtualnym lub sprzętowym.