Łukasiewicz
Instytut
Organizacji
i Zarządzania
w Przemyśle
ORGMASZ

SPECYFIKACJA
ISTOTNYCH WARUNKÓW ZAMÓWIENIA

Sieć Badawcza Łukasiewicz - Instytut Organizacji i Zarządzania w Przemyśle "ORGMASZ", ul. Żelazna 87, 00-879 Warszawa, zwany dalej „Zamawiającym", zaprasza do złożenia oferty w postępowaniu o udzielenie zamówienia publicznego pn. „dostawa sprzętu informatycznego, komputerowego i oprogramowania", w trybie przetargu nieograniczonego (art. 39 ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych, Dz. U. z 2019 r. poz. 1843, z późn. zm.).

Niniejsza specyfikacja istotnych warunków zamówienia, zwana dalej „SIWZ", składa się z następujących rozdziałów:

Rozdział I	Instrukcja dla Wykonawców
Rozdział II	Opis przedmiotu zamówienia
Rozdział III	Formularz oferty wraz z załącznikami
Rozdział IV	Wzór umowy

Kody CPV: 30200000-1; 30213100-6; 33195100-4; 38652100-1; 48760000-3

Termin realizacji przedmiotu zamówienia:
Do 30 dni od daty zawarcia umowy.
Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.
Zamawiający nie dopuszcza możliwości składania oferty wariantowej.
Zamawiający nie dopuszcza składania ofert częściowych.
Zamawiający nie przewiduje zamówień, o których mowa w art. 67 ust. 1 pkt 7 ustawy Prawo zamówień publicznych.
Wartość zamówienia nie przekracza kwoty określonej w przepisach wydanych na podstawie art. 11 ust. 8 ustawy Prawo zamówień publicznych.

Rozdział I
Instrukcja dla Wykonawców

1. Opis warunków udziału w postępowaniu i podstawy wykluczenia

O zamówienie mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na podstawie przesłanek określonych w art. 24 ust. 1 pkt 12 – 23 ustawy Prawo zamówień publicznych oraz w art. 24 ust. 5 pkt 1 tej ustawy jeżeli zaistniały one

Jednostka
Notyfikowana
Unii Europejskiej
nr 1454.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

w okresach określonych w art. 24 ust. 7 ustawy Prawo zamówień publicznych oraz spełniają warunki udziału w postępowaniu określone w SIWZ (pkt 2).

2. Warunki udziału w postępowaniu

Wykonawcy ubiegający się o przedmiotowe zamówienie powinni spełniać warunki zgodnie z art. 22 ust. 1b ustawy Prawo zamówień publicznych, dotyczące:

a. <u>kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej:</u>

Zamawiający nie określa warunku w tym zakresie.

b. <u>sytuacji ekonomicznej lub finansowej:</u>

Wykonawca powinien wykazać, że jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności gospodarczej na terytorium Rzeczypospolitej Polskiej związanej z przedmiotem zamówienia na sumę gwarancyjną w wysokości nie niższej niż 100 000,-zł.

W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, powyższy warunek może zostać spełniony przez jednego Wykonawcę lub łącznie przez wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia.

c. <u>zdolności technicznej lub zawodowej:</u>

(w zakresie doświadczenia)

Do udziału w postępowaniu może przystąpić Wykonawca, który posiada poniższe doświadczenie:

a)w okresie ostatnich 3 (trzech) lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy -w tym okresie wykonał lub wykonuje co najmniej 2 dostawy (rozumianą jako dwie umowy) laptopów lub komputerów o wartości co najmniej 70 000,00 zł (słownie złotych: siedemdziesiąt tysięcy 00/100) brutto każda. W przypadku dostaw, które są w trakcie realizacji, Wykonawca musi wykazać, że do chwili składania ofert, wartość każdej z wykonanych częściowo dostaw wynosi co najmniej 70 000,00 zł (słownie złotych: siedemdziesiąt tysięcy 00/100) brutto. Na potwierdzenie powyższych warunków Wykonawca wypełnia wykaz dostaw stanowiący załącznik nr do SIWZ.

W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, powyższy warunek mogą spełniać Wykonawcy łącznie.

3. Poleganie na zasobach innych podmiotów

a. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

b. Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów, musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia. Dokument ten (np. zobowiązanie) należy dołączyć do oferty.

c. Z dokumentu np. zobowiązania, o którym mowa w pkt 3.2. lub innych dokumentów musi wynikać w szczególności:
   1. zakres dostępnych Wykonawcy zasobów innego podmiotu,
   2. sposób wykorzystania zasobów innego podmiotu, przez Wykonawcę, przy wykonywaniu zamówienia publicznego,
   3. zakres i okres udziału innego podmiotu przy wykonywaniu zamówienia publicznego,
   4. czy podmiot, na zdolnościach którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje prace, których wskazane zdolności dotyczą.

d. Zamawiający oceni, czy udostępniane Wykonawcy przez inne podmioty zdolności techniczne lub zawodowe lub sytuacja ekonomiczna lub finansowa, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu oraz zbada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, o których mowa w art. 24 ust. 1 pkt 12–23 i ust. 5 pkt 1 ustawy Prawo zamówień publicznych.

e. Jeżeli zdolności techniczne lub zawodowe lub sytuacja ekonomiczna lub finansowa, podmiotu, o którym mowa powyżej, nie potwierdzają spełnienia przez Wykonawcę warunków udziału w postępowaniu lub zachodzą wobec tych podmiotów podstawy wykluczenia, Zamawiający zażąda, aby Wykonawca w terminie określonym przez Zamawiającego:
   1) zastąpił ten podmiot innym podmiotem lub podmiotami lub
   2) zobowiązał się do osobistego wykonania odpowiedniej części zamówienia, jeżeli wykaże zdolności techniczne lub zawodowe wymagane przez Zamawiającego dla Wykonawcy.

4. Podstawy wykluczenia Wykonawcy

4.1. Zamawiający wykluczy z udziału w postępowaniu Wykonawcę w przypadku wystąpienia okoliczności, o których mowa w art. 24 ust. 1 ustawy Prawo zamówień publicznych. Zamawiający przewiduje fakultatywne przesłanki wykluczenia Wykonawcy w przypadku wystąpienia okoliczności, o których mowa w art. 24 ust. 5

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

pkt 1 ustawy Prawo zamówień publicznych. Wykluczenie Wykonawcy następuje, gdy okoliczności stanowiące podstawę wykluczenia zaistniały w okresach określonych w art. 24 ust. 7 ustawy Prawo zamówień publicznych.

4.2. Wykonawca, który podlega wykluczeniu na podstawie art. 24 ust. 1 pkt 13 i 14 oraz 16-20 oraz ust. 5 pkt 1 ustawy Prawo zamówień publicznych, może przedstawić dowody na to, że podjęte przez niego środki są wystarczające do wykazania jego rzetelności, w szczególności udowodnić naprawienie szkody wyrządzonej przestępstwem lub przestępstwem skarbowym, zadośćuczynienie pieniężne za doznaną krzywdę lub naprawienie szkody, wyczerpujące wyjaśnienie stanu faktycznego oraz współpracę z organami ścigania oraz podjęcie konkretnych środków technicznych, organizacyjnych i kadrowych, które są odpowiednie dla zapobiegania dalszym przestępstwom lub przestępstwom skarbowym lub nieprawidłowemu postępowaniu Wykonawcy. Ww. przepisu nie stosuje się, jeżeli wobec Wykonawcy, będącego podmiotem zbiorowym, orzeczono prawomocnym wyrokiem sądu zakaz ubiegania się o udzielenie zamówienia oraz nie upłynął określony w tym wyroku okres obowiązywania tego zakazu, art. 24 ust. 9 i 10 ustawy Prawo zamówień publicznych stosuje się.

4.3. W przypadkach, o których mowa w art. 24 ust. 1 pkt 19 ustawy Prawo zamówień publicznych, przed wykluczeniem Wykonawcy, Zamawiający zapewnia temu Wykonawcy możliwość udowodnienia, że jego udział w przygotowaniu postępowania o udzielenie zamówienia nie zakłóci konkurencji.

4.4. Wykonawca, w terminie 3 dni od zamieszczenia na stronie internetowej informacji z otwarcia ofert, o której mowa w art. 86 ust. 5 ustawy Prawo zamówień publicznych, przekazuje Zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy Prawo zamówień publicznych, zgodnie ze wzorem zamieszczonym w Załączniku nr 1 do Rozdziału III SIWZ. Wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.

4.5. Zamawiający, zgodnie z art. 24aa PZP, najpierw dokona oceny ofert, a następnie zbada, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu. Zamawiający przed udzieleniem zamówienia wezwie Wykonawcę, którego oferta została oceniona najwyżej, do złożenia w wyznaczonym terminie, lecz nie krótszym niż 5 dni, aktualnych na dzień złożenia oświadczeń i dokumentów potwierdzających

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

spełnienie warunków udziału w postępowaniu oraz braku podstaw wykluczenia z postępowania.

5. Wykaz oświadczeń i dokumentów składanych w celu potwierdzenia okoliczności, o których mowa w art. 25 ust. 1 ustawy Prawo zamówień publicznych

5.1. **W celu potwierdzenia spełniania przez Wykonawcę warunków udziału w postępowaniu:**

1) wykaz dostaw wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy, w tym okresie, wraz z podaniem przedmiotu, dat wykonania i podmiotów na rzecz których usługi zostały wykonane (lub są nadal wykonywane) oraz załączeniem dowodów określających czy te dostawy zostały wykonane należycie lub są wykonywane należycie. Dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi były wykonane (lub są nadal wykonywane), a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy, w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert – na potwierdzenie warunku, o którym mowa w pkt 2.c. Rozdziału I SIWZ (Załącznik nr 4 do Rozdziału III SIWZ),
2) dokument potwierdzający, że Wykonawca jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności na terytorium Rzeczypospolitej Polskiej związanej z przedmiotem zamówienia na sumę gwarancyjną w wysokości nie niższej niż 100 000,-zł – na potwierdzenie warunku określonego w pkt 2.b. Rozdziału I SIWZ.

5.2. **W celu potwierdzenia braku podstaw wykluczenia Wykonawcy z udziału w postępowaniu, Zamawiający będzie żądał dokumentów:**

odpisu z właściwego rejestru lub centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 24 ust. 5 pkt 1 ustawy Prawo zamówień publicznych.

5.3. **Dokumenty podmiotów zagranicznych:**

Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentu, o którym mowa w pkt 5.2 składa

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

dokument zgodny z rozporządzeniem Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia (Dz. U. z 2020 r. poz. 1282).

6. Opis sposobu przygotowania oferty

6.1. Oferta składana przez Wykonawcę powinna być sporządzona zgodnie z Formularzem oferty zamieszczonym w Rozdziale III SIWZ.

6.2. Do oferty należy załączyć:

1) oświadczenia aktualne na dzień składania ofert:
   a) o braku podstaw do wykluczenia z postępowania (Załącznik nr 3 do Rozdziału III SIWZ),
   b) potwierdzające spełnienie warunków udziału w postępowaniu (Załącznik nr 4 do Rozdziału III SIWZ);
2) pełnomocnictwa w przypadku podpisywania oferty przez osoby, których uprawnienie do występowania w imieniu Wykonawcy nie wynika z dokumentu rejestrowego Wykonawcy, który Zamawiający może pobrać za pomocą bezpłatnej, ogólnodostępnej bazy danych wskazanej przez Wykonawcę (pełnomocnictwo Wykonawca składa w oryginale lub kopii potwierdzonej za zgodność z oryginałem);
3) w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia – informacje o ustanowieniu pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia publicznego albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego – w formie pisemnej;
4) zobowiązanie podmiotu, na którym polega Wykonawca na zasadach określonych w art. 22a ustawy Prawo zamówień publicznych - w formie pisemnej;
5) w przypadku, gdy Wykonawca zamierza powierzyć wykonanie części zamówienia podwykonawcom - wskazanie przez Wykonawcę tych części zamówienia - w formie pisemnej. Nazwy firm podwykonawców Wykonawca podaje odpowiednio w Załącznikach 2 i 3 do Formularza oferty;
6) specyfikacje oferowanego sprzętu, zgodne z Opisem przedmiotu zamówienia stanowiącym Rozdział II SIWZ.

6.3. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia Zamawiający wymaga przedstawienia dokumentu ustanowienia pełnomocnika do reprezentowania Wykonawców w postępowaniu o udzielenie zamówienia publicznego albo do reprezentowania ich w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

Dokument pełnomocnictwa powinien:

1) zawierać w szczególności wskazanie:
   a) postępowania o zamówienie publiczne, którego dotyczy,
   b) Wykonawców ubiegających się wspólnie o udzielenie zamówienia,
   c) ustanowionego pełnomocnika oraz zakres jego umocowania, obejmujący przede wszystkim: reprezentowanie Wykonawców w postępowaniu o udzielenie zamówienia publicznego, zaciąganie w imieniu Wykonawców zobowiązań, złożenie oferty wspólnie, prowadzenie korespondencji i podejmowanie zobowiązań związanych z postępowaniem o udzielenie zamówienia publicznego;
2) być podpisany przez wszystkich Wykonawców ubiegających się wspólnie o udzielenie zamówienia, w tym Wykonawcę ustanowionego jako pełnomocnika i przez osoby uprawnione do składania oświadczeń woli i zaciągania zobowiązań w imieniu Wykonawców w wysokości odpowiadającej cenie oferty.

6.4. Oferty oraz wszelkie inne oświadczenia i zaświadczenia składane w trakcie postępowania są jawne, z wyjątkiem – odrębnie i jednoznacznie wskazanych przez Wykonawcę – informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913). Zgodnie z art. 8 ust. 3 ustawy Prawo zamówień publicznych: nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli wykonawca, nie później niż w terminie składania ofert, zastrzegł, że nie mogą być one udostępniane oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, o których mowa w art. 86 ust. 4 ustawy Prawo zamówień publicznych.

6.5. Dokumenty sporządzone w języku obcym powinny być składane wraz z tłumaczeniem na język polski.

6.6. Oferta powinna być sporządzona w języku polskim, na komputerze lub inną trwałą i czytelną techniką. Oferty nieczytelne nie będą rozpatrywane.

6.7. Wszystkie strony oferty powinny być podpisane przez osobę (osoby) uprawnioną (uprawnione) do występowania w imieniu Wykonawcy. Wszystkie strony oferty powinny być kolejno ponumerowane. Niespełnienie tego wymagania nie będzie skutkowało odrzuceniem oferty, jednak wszelkie negatywne konsekwencje mogące wyniknąć z niezachowania tego wymagania będą obciążały Wykonawcę.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

6.8. Poprawki powinny być naniesione czytelnie przez skreślenie oraz opatrzenie podpisem osoby uprawnionej do reprezentowania Wykonawcy.

6.9. Ofertę należy umieścić w kopercie zaadresowanej następująco: „Instytut Organizacji i Zarządzania w Przemyśle „ORGMASZ"" i oznaczonej:
„Oferta w postępowaniu pn.**„** dostawa sprzętu informatycznego, komputerowego i oprogramowania". **Nie otwierać do dnia 28.12.2020 r. do godz. 13[15]"**.

6.10. Koperta poza ww. oznaczeniami powinna być opatrzona nazwą i siedzibą Wykonawcy.

7. Informacje o dokumentach

7.1. Oświadczenia i dokumenty, o których mowa w pkt 5 Rozdziału I SIWZ składane są w formie przewidzianej w rozporządzeniu Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia (Dz. U. z 2020 r. poz. 1282).

7.2. Wykonawca nie jest obowiązany do złożenia oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 pkt 1 i 3 ustawy Prawo zamówień publicznych, jeżeli Zamawiający posiada oświadczenia lub dokumenty dotyczące tego Wykonawcy lub może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r. poz. 346, z późn. zm.). W przypadku wskazania przez Wykonawcę oświadczeń lub dokumentów, o których mowa w zdaniu pierwszym, które znajdują się w posiadaniu Zamawiającego, w szczególności oświadczeń lub dokumentów przechowywanych przez Zamawiającego zgodnie z art. 97 ust. 1 ustawy Prawo zamówień publicznych, Zamawiający w celu potwierdzenia okoliczności, o których mowa w art. 25 ust. 1 pkt 1 i 3 ustawy Prawo zamówień publicznych, korzysta z posiadanych oświadczeń lub dokumentów, o ile są one aktualne. Podobnie, w przypadku wskazania przez Wykonawcę dostępności tych oświadczeń lub dokumentów w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych.

7.3. Oświadczenia i dokumenty wymienione odpowiednio w pkt 5 Rozdziału I SIWZ, Wykonawca składa za siebie, każdego z Wykonawców składających ofertę wspólną i podmioty udostępniające zasoby, jeżeli taka sytuacja zachodzi.

7.4. Zamawiający informuje, iż zgodnie z art. 26 ust. 2f ustawy Prawo zamówień publicznych, jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, Zamawiający może na każdym etapie

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

postępowania wezwać Wykonawców do złożenia wszystkich lub niektórych oświadczeń lub dokumentów potwierdzających, że nie podlegają wykluczeniu, spełniają warunki udziału w postępowaniu, a jeżeli zachodzą uzasadnione podstawy do uznania, że złożone uprzednio oświadczenia lub dokumenty nie są już aktualne, do złożenia aktualnych oświadczeń lub dokumentów.

7.5. Jeżeli Wykonawca nie złoży wraz z ofertą oświadczeń, o których mowa w art. 25a ust. 1 ustawy Prawo zamówień publicznych, oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 tej ustawy, lub innych dokumentów niezbędnych do przeprowadzenia postępowania, oświadczenia lub dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez Zamawiającego wątpliwości, Zamawiający wezwie do ich złożenia, uzupełnienia lub poprawienia lub do udzielenia wyjaśnień w wyznaczonym terminie, chyba, że mimo ich uzupełnienia lub poprawienia oferta Wykonawcy podlegałaby odrzuceniu lub konieczne byłoby unieważnienie postępowania.

8. Opis kryteriów i sposobu oceny ofert.

8.1. Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującymi kryteriami:

1) **Cena (C)**: 70% (70 pkt) - sposób obliczenia wartości punktowej za cenę jest opisany w pkt 8.2.;
2) **Termin dostawy (T):** 30% (30pkt) - sposób obliczenia wartości punktowej za termin dostawy jest opisany w pkt 8.3.

8.2. Sposób obliczenia wartości punktowej w kryterium „Cena".

Liczba punktów przyznanych w tym kryterium zostanie wyliczona wg wzoru:

$C = (C_{min} / C_{bad}) \times 70$ pkt

gdzie:

$C_{min.}$ – najniższa cena brutto wśród ważnych ofert

$C_{bad.}$ – cena brutto badanej oferty.

8.3. Sposób obliczenia wartości punktowej w kryterium „Termin dostawy".

Ocena za termin dostawy (T) będzie liczona następująco:

Zaoferowany termin dostawy musi być podany w pełnych dniach. W przypadku zaoferowania przez Wykonawcę terminu realizacji w niepełnych dniach, Zamawiający do oceny przyjmie pełne dni, zaokrąglone do dołu.

Punkty za kryterium „termin dostawy , zostaną przyznane ofertom, gdzie Wykonawcy zadeklarują okres dostawy, krótszy niż 30 dni kalendarzowych w wysokości jak niżej:

do 14 dni – 30 pkt.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

do 20 dni - 20 pkt.

do 26 dni - 10 pkt.

Powyżej 26 dni - 0 pkt.

Maksymalny czas dostawy – 30 dni.

8.4. Sposób obliczenia wartości punktowej oferty.

Liczba punktów przyznanych ofercie (P) zostanie wyliczona wg wzoru:

P = C + T

gdzie:

C liczba punktów przyznanych za cenę oferty

T liczba punktów przyznanych za termin dostawy

Oferta, która uzyska największą liczbę punktów (P) zostanie wybrana przez Zamawiającego jako najkorzystniejsza.

9. Opis sposobu obliczenia ceny.

9.1. Wybór najkorzystniejszej oferty będzie dokonany w oparciu o najniższą cenę zaproponowaną dla łącznej liczby zamówienia oraz skróconego terminu dostawy, z zastrzeżeniem, iż termin dostawy nie może być dłuższy niż 30 dni od daty zawarcie umowy. Oferty zwierające dłuższy czas dostawy niż 30 dni zostaną odrzucone, jako niespełniające wymagań SIWZ.

9.2. Cena winna uwzględniać wszystkie koszty związane z realizacją zamówienia, zgodnie z wymogami zawartymi w Rozdziale II SIWZ „Opis przedmiotu zamówienia", w tym również koszty dostawy do Zamawiającego, wszelkich należnych opłat i podatków.

9.3. Rozliczenia pomiędzy Zamawiającym a Wykonawcą będą prowadzone w walucie PLN.

9.4. Cena w Formularzu oferty muszą być wyrażone w złotych polskich niezależnie od wchodzących w jej skład elementów i powinny być podane z dokładnością do dwóch miejsc po przecinku. Tak obliczone ceny będą brane pod uwagę przez Zamawiającego w trakcie wyboru oferty najkorzystniejszej.

9.5. Jeżeli nie będzie można dokonać wyboru oferty najkorzystniejszej ze względu na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i innych kryteriów oceny ofert, Zamawiający spośród tych ofert wybierze ofertę z niższą ceną , a jeżeli zostały złożone oferty o takiej samej cenie, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych (art. 91 ust. 4 ustawy Prawo zamówień publicznych).

10. Termin wykonania zamówienia: do 30 dni od daty zawarcia umowy.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

11. Miejsce i termin składania ofert

1) Oferty powinny być złożone w terminie do dnia **28.12.2020 r. do godz. 13^{00}** w siedzibie Instytutu Organizacji i Zarządzania w Przemyśle „ORGMASZ" w pok. nr 504 , w godz. 8.00 – 16.00, z wyłączeniem dni ustawowo wolnych od pracy.
2) Oferta powinna być umieszczona w kopercie oznaczonej zgodnie z pkt 6.9. i 6.10. Rozdziału I SIWZ.

12. Miejsce i termin otwarcia ofert

12.1. Otwarcie ofert nastąpi **w dniu 28.12.2020 r. o godz. 13^{15}** w siedzibie Instytutu Organizacji i Zarządzania w Przemyśle „ORGMASZ" w pok. Nr 306.

12.2. Niezwłocznie po otwarciu ofert, Zamawiający zamieści na swojej stronie internetowej: (www.orgmasz.pl), informację zgodnie z art. 86 ust. 5 ustawy Prawo zamówień publicznych.

12.3. Oferta otrzymana przez Zamawiającego po terminie składania ofert zostanie niezwłocznie zwrócona Wykonawcy.

12.4. O wyborze najkorzystniejszej oferty Zamawiający zawiadomi Wykonawców, a także przekaże informacje zgodnie z art. 92 ustawy Prawo zamówień publicznych.

13. Termin związania ofertą

Wykonawca pozostaje związany ofertą przez okres 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

14. Wymagania dotyczące wadium

14.1. Zamawiający wymaga wniesienia wadium w wysokości: 3 000,- zł (trzy tysiące złotych).

14.2. Wadium może być wnoszone w pieniądzu, gwarancjach lub poręczeniach bankowych, poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym, że poręczenie kasy jest zawsze poręczeniem pieniężnym, gwarancjach ubezpieczeniowych, poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2020 r. poz. 299).

14.3. Wadium wnoszone w pieniądzu należy wpłacić przelewem na rachunek bankowy Zamawiającego: 34 1020 4900 0000 8102 3326 4041, do terminu składania ofert. Skuteczne wniesienie wadium w pieniądzu następuje z chwilą uznania na rachunku bankowym Zamawiającego.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

14.4. Pozostałe formy wadium, jak poręczenia lub gwarancje bankowe, gwarancje ubezpieczeniowe, poręczenia udzielane przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości, powinny być złożone razem z ofertą, w sposób umożliwiający zwrot wadium, zgodnie z ustawą Prawo zamówień publicznych.

14.5. Wadium wniesione w formie poręczeń lub gwarancji musi zawierać zobowiązanie gwaranta lub poręczyciela do bezwarunkowej zapłaty Zamawiającemu pełnej kwoty wadium, na każde pisemne żądanie Zamawiającego w terminie związania ofertą, w okolicznościach określonych w art. 46 ust. 4a i 5 ustawy Prawo zamówień publicznych.

14.6. Zamawiający zatrzymuje wadium wraz z odsetkami, jeżeli Wykonawca w odpowiedzi na wezwanie, o którym mowa w art. 26 ust. 3 i 3a ustawy Prawo zamówień publicznych, z przyczyn leżących po jego stronie, nie złożył oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1, oświadczenia, o którym mowa w art. 25a ust. 1 tej ustawy, pełnomocnictw lub nie wyraził zgody na poprawienie omyłki, o której mowa w art. 87 ust. 2 pkt 3 tej ustawy, co spowodowało brak możliwości wybrania oferty złożonej przez wykonawcę jako najkorzystniejszej.

14.7. Zamawiający zatrzymuje wadium wraz z odsetkami, jeżeli Wykonawca, którego oferta została wybrana:

1) odmówił podpisania umowy w sprawie zamówienia publicznego na warunkach określonych w ofercie;
3) zawarcie umowy w sprawie zamówienia publicznego stało się niemożliwe z przyczyn leżących po stronie Wykonawcy.

14.8. Na podstawie art. 89 ust. 1 pkt 7b ustawy Prawo zamówień publicznych, Zamawiający odrzuci ofertę, jeżeli Wykonawca nie wniesie wadium lub wadium zostanie wniesione w sposób nieprawidłowy.

15. Wyjaśnienia treści SIWZ

15.1. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SIWZ.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

15.2. Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert.

16. Formalności, jakie powinny zostać dopełnione po zakończeniu postępowania w celu zawarcia umowy.

16.1. Zamawiający przekaże wybranemu Wykonawcy projekt umowy zgodny ze wzorem umowy stanowiącym Rozdział IV SIWZ.

16.2. Jeżeli w przedmiotowym postępowaniu zostanie wybrana oferta Wykonawców wspólnie ubiegających się o zamówienie, Zamawiający będzie wymagał przed zawarciem umowy przedłożenia umowy regulującej współpracę tych Wykonawców.

17. Sposób porozumiewania się Zamawiającego z Wykonawcami

17.1. Oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują drugiej stronie pisemnie.

17.2. Komunikacja między Zamawiającym a Wykonawcami odbywa się:

1) za pośrednictwem operatora pocztowego w rozumieniu ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe (Dz. U. z 2020 r. poz. 1041);
2) przy użyciu środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344) – na adres e-mail Zamawiającego: pawel.prusik@orgmasz.lukasiewicz.gov.pl, każda ze Stron na żądanie drugiej niezwłocznie potwierdza fakt otrzymania korespondencji. W przypadku braku potwierdzenia otrzymania korespondencji Zamawiający uznaje, że korespondencja wysłana na numer faksu lub adres poczty e-mail, podany przez Wykonawcę, została doręczona w sposób umożliwiający zapoznanie się z jej treścią.

17.3. Korespondencję związaną z niniejszym postępowaniem należy kierować na adres: Sieć Badawcza Łukasiewicz - Instytut Organizacji i Zarządzania w Przemyśle "ORGMASZ", ul. Żelazna 87, 00-879 Warszawa.

17.4. Miejsce składania dokumentów: Sieć Badawcza Łukasiewicz - Instytut Organizacji i Zarządzania w Przemyśle "ORGMASZ", ul. Żelazna 87, 00-879 Warszawa, w godz. 8.00 – 16.00, z wyłączeniem dni ustawowo wolnych od pracy.

17.5. Osobą uprawnioną do porozumiewania się z Wykonawcami jest p. Paweł Prusik, pawel.prusik@orgmasz.lukasiewicz.gov.pl,

17.6. Adres strony internetowej Zamawiającego: www.orgmasz.pl

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

18. Inne informacje

18.1. W sprawach nieuregulowanych w SIWZ mają zastosowanie przepisy ustawy Prawo zamówień publicznych.

18.2. Wykonawcom, których interes prawny doznał uszczerbku w wyniku naruszenia przez Zamawiającego zasad określonych w ustawie Prawo zamówień publicznych przysługują środki ochrony prawnej przewidziane w Dziale VI tej ustawy.

18.3. Zgodnie z art. 13 ust. 1 i ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, z 04.05.2016 r., s. 1, z późn. zm.), zwanego dalej „RODO", Zamawiający informuje:

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1, z późn. zm.) – dalej RODO, Zamawiający informuje:

1) Administratorem Danych Osobowych zawartych w ofertach przetargowych jest Instytut Organizacji i Zarządzania w Przemyśle „ORGMASZ" , ul. Żelazna 87, Warszawa;

2) z Administratorem danych można się skontaktować poprzez tel. 22 10 01 463 lub przekazując korespondencję na adres siedziby Administratora.

3) przetwarzanie danych osobowych będzie odbywać się na podstawie art. 6 ust. 1 lit. b i c RODO w celu przeprowadzenia postępowania przetargowego oraz realizacji zawartej umowy, zgodnie z ustawą z dnia 29 stycznia 2004 r. Prawo zamówień publicznych.

4) podanie danych osobowych jest dobrowolne, lecz niezbędne do wzięcia udziału w przedmiotowym postępowaniu i zawarcia umowy;

5) dane osobowe z postępowania będą przechowywane zgodnie z art. 97 ust. 1 Prawo zamówień publicznych przez okres 4 lat od dnia zakończenia postępowania, a jeżeli czas trwania umowy będzie przekraczał 4 lata przez cały czas trwania umowy.

Dane osobowe wynikające z zawartej umowy będą przechowywane przez okres, w którym mogą ujawnić się roszczenia związane z zawartą umową;

6) każdej osobie, której dane są przetwarzane przysługuje:

a) prawo dostępu do treści swoich danych osobowych,

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

b) prawo do sprostowania swoich danych osobowych,

c) w zakresie wynikającym z przepisów - prawo do usunięcia swoich danych osobowych, jak również prawo do ograniczenia przetwarzania,

Skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Prawo zamówień publicznych oraz nie może naruszać integralności protokołu oraz jego załączników. Prawo do ograniczenia przetwarzania danych nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego;

7) każdej osobie, której dane są przetwarzane przysługuje prawo wniesienia skargi do Prezesa UODO, jeśli jej zdaniem, przetwarzanie danych osobowych - narusza przepisy prawa;

8) Wykonawca ubiegając się o przedmiotowe zamówienie publiczne jest zobowiązany do wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO i złożenia oświadczenia, którego treść zamieszczona jest w Formularzu oferty.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

Rozdział II

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa sprzętu informatycznego, komputerowego i oprogramowania spełniającego parametry techniczne określone poniżej:

1. **Sprzęt komputerowy - laptop – (15 sztuk) o następujących parametrach technicznych:**

W ofercie należy podać model, symbol oraz producenta.

1. Ekran: 14 cali o rozdzielczości min. Full HD (1920x1080 pikseli)
2. Powłoka matrycy: matowa
3. Procesor (4 rdzeniowy/min. 8 wątki) min. 6458 punktów w teście Passmark CPU - http://www.cpubenchmark.net/
4. Bazowe taktowanie rdzeni procesora w przedziale od 1,6 GHz do 4,2 GHz
5. Min. 8GB DDR4 pamięci RAM, możliwość rozbudowy do min 32GB, 2 słoty na pamięci w tym min. jeden wolny
6. Dysk twardy min: 256 GB NVME SSD oraz możliwość montażu drugiego dyska 2,5 cali
7. Tryby pracy: tryb notebooka
8. Klawiatura mechanicznie połączona z komputerem, wyklucza się możliwość wykorzystania technologii bluetooth w komunikacji pomiędzy klawiaturą a komputerem, z wbudowanym w klawiaturze podświetleniem, (układ US z dolarem), min 80 klawiszy. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12.
9. Multimedia: Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo o mocy 2x 2W. Cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy. Kamera internetowa z diodą informującą o aktywności, min 0.9 Mpix, trwale zainstalowana w obudowie matrycy.
10. Łączność: certyfikowany moduł WiFi 6 (802,11ax), 2,4Ghz, 5Ghz, maksymalna prędkość 2,4Gbps. Bluetooth min.5.0, Karta sieciowa ETH zgodna ze standardem 10/100/1000 Ethernet
11. Wbudowane porty i złącza:
    - Min. 1 x HDMI
    - min. 4xUSB (co najmniej: 2x USB 3.2 Gen 1 oraz 1x USB Type C 3.2 Gen 1)
    - Wbudowane porty i złącza: 1x HDMI 1.4, 1x RJ-45, 2x USB 3.2, 1x USB TYP-C z obsługą DP 1.2, 1x USB 2.0, port zasilania, złącze linki zabezpieczającą
    - 1 port audio typu combo (słuchawki i mikrofon)
    - Port Ethernet 1x RJ-45
12. Zasilanie: zasilacz dedykowany do danego modelu;
13. Waga: max 1,7kg z baterią
14. Obudowa: Szkielet obudowy i zawiasy notebooka wzmacniane, dookoła matrycy uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią. Kąt rozwarcia matrycy 180 stopni. Laptop powinien spełniać normy MIL-STD-810G.
15. Bezpieczeństwo: zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.

16. System operacyjny: Preinstalowany system operacyjny Windows 10 Professional, klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.
17. Gwarancja: Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, 3-letnia gwarancja producenta świadczona na miejscu u klienta, Czas reakcji serwisu - do końca następnego dnia roboczego.
18. Zakupiony i dostarczony sprzęt komputerowy powinien być nowy i nieużywany**.**

Do każdego laptopa należy dostarczyć :
Oprogramowanie (fabrycznie nowe, nieużywane):

1. System operacyjny Windows 10 Professional licencja wieczysta lub równoważne.
2. Pakiet oprogramowania biurowego MS Office 2019 Standard licencja wieczysta lub równoważne.

2. Zakup monitorów (32 sztuki)

W ofercie należy podać model, symbol oraz producenta.

1. Rodzaj urządzenia: monitor musi posiadać trwałe oznaczenie logo producenta.
2. Przekątna ekranu: min. 24” z regulacją wysokości i pochylenia
3. Rozdzielczość: min. 1920 x 1080
4. Rodzaj matrycy: antyodblaskowa; IPS; podświetlanie LED; matowa
5. Jasność: min. 250 cd/m ,
6. Kontrast: min. 1000:1,
7. Proporcje ekranu: 16:9
8. Kąt widzenia min. 178° (w pionie) min. 178° (w poziomie)
9. Porty: HDMI, DVI, DP min. 1 x USB
10. Napięcie wejściowe: 220-240V
11. Długość kabla zasilającego: min. 1,5m
12. Certyfikaty: aktualny certyfikat CE
13. Dokumentacja: Dołączone instrukcje użytkownika w języku polskim w wersji papierowej lub elektronicznej.
14. Gwarancja: 24 miesięcy; gwarancja zero martwych pikseli.

3. Zakup urządzeń wskazujących (30 zestawów)

Urządzenie wskazujące klawiatura pełnowymiarowa + mysz komputerowa
W ofercie należy podać model, symbol oraz producenta.

1. Typ łączności: Bezprzewodowa, szyfrowanie AES
2. Układ klawiatury: QWERTY (PL) z klawiaturą numeryczną po prawej stronie
3. Mysz komputerowa: Sensor optyczny, profil myszy uniwersalny
4. Kolor: dominujący kolor czarny.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

5. Żywotność baterii: deklarowany przywidziany czas pracy na jednym zestawie baterii – 12 miesięcy.
6. Baterie w zestawie
7. Zasięg: Deklarowany zasięg min. 10m
8. Przełączniki dodatkowe: Przełącznik on/off na górnej części klawiatury i dolnej części myszy komputerowej.

4. Zakup projektora – 1 sztuka

W ofercie należy podać model, symbol oraz producenta.
1. Technologia wyświetlania: Laserowa
2. Rozdzielczość natywna: 3840 x 2160, HDR.
3. Format obrazu: 4:3, 16:9
4. Jasność min.: 5000 lm
5. Kontrast min.: 2 000 000:1
6. Minimalna odległość projekcji: max. 1.5 metra
7. Maksymalna odległość projekcji: min. 6 metrów
8. Żywotność lampy min.: 20000 h
9. Przekątna projekcji: od 40” do 300”
10. Funkcje korekcji obrazu: min. 1,6-krotny zoom, 12-punktowy Warping
11. Złącza: Wejście audio - 1 szt.; Wyjście audio - 1 szt.; HDMI (std. min. 2.0) - 1 szt.; VGA in (D-sub) - 1 szt.; RJ-45 (LAN) - 1 szt.; USB 2.0 - 1 szt (do odtwarzania formatów DivX, MP3, JPEG i JPEG4, dodatkowe odtwarzanie plików Powerpoint lub Excel przez USB bez komputera);
12. Łączność bezprzewodowa: WI-FI, Bluetooth
13. Głośniki wbudowane: min. 10w sumarycznie
14. Zdalne sterownie: Aplikacja/Miracast umożliwiające wyświetlenie zawartości ekranu, używając połączenia sieci lokalnej, bez konieczności podłączenia się kablem sygnałowym, dla systemów min Windows 7,10 oraz Android od wersji 9 wzwyż.
Pilot do zdalnego sterownia rzutnikiem min. funkcje ON/OFF, wybór wejścia, konfiguracja obrazu, regulacja głośności.
15. Zasilanie: Zasilacz wbudowany (220V – 240V @ 50~60 Hz), kabel zasilający min. 3m
16. Umiejscowienie: Projektor powinien być zbudowany w sposób umożliwiający jego eksploatację w dwóch płaszczyznach: pozioma standardowa i pozioma odwrócona (tj. w położeniu na górnej części obudowy projektora, posiadać otwór do montażu pod sufitem (na uchwyt)).
17. Hałas: Niska emisja hałasu max 30 dBA.
18. Gwarancja producenta: min. 24 miesięcy, Door-to-Door lub wyższa.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

5. Oprogramowanie - Zamawiający oczekuje, że oprogramowanie będzie oferowane w wariancie licencjonowania najtańszym dla danej wersji programu (wariant Edu/gov/org itp.) o ile zgodnie z polityką prowadzoną przez producenta oprogramowania, Zamawiający jest uprawniony do takiej licencji.

1. **Zakup oprogramowania ochrony stacji roboczych i serwerów -**
   ESET Endpoint Protection Advanced pierwszy zakup – 15 szt. na okres dwunastu miesięcy lub równoważne. Zakupione i dostarczone ww. oprogramowanie powinno być nowe i nieużywane**.** W przypadku, gdy wykonawca oferuje licencje na oprogramowanie inne niż wskazane wyżej, oprogramowanie powinno spełniać określone w pkt .6 wymogi równoważności.

6. Wymogi równoważności

a. **Wymogi równoważności odnośnie systemu operacyjnego**

System powinien spełniać następujące warunki:

1. licencji:

- licencja uprawniająca do użytkowania wieczystego;

2. funkcjonalności:

- możliwość natywnego (bez korzystania z emulatorów) uruchomienia pakietu biurowego będącego przedmiotem tego zamówienia;
- obsługa szyfrowania wybranych katalogów dysku twardego;
- polska wersja językowa;
- natywne wsparcie pracy w domenie w systemie Active Directory w zakresie obsługi udziałów, korzystania z zasobów sieciowych udostępnianych przez system Windows Server;
- pełna obsługa wszystkich podzespołów (kamera, karta sieci bezprzewodowej, itd.) laptopów będących przedmiotem zakupu; możliwość aktualizacji z serwerów producenta;
- możliwość dostępu przez zdalny pulpit;
- obsługa bibliotek DirectX12;
- możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne, umożliwienie aktualizacji poprawek bezpieczeństwa
- system operacyjny ma pozwalać na uruchomienie i pracę z aplikacjami użytkowanymi przez Zamawiającego, w szczególności: MS Office 2010, 2013, 2016;MS Visio 2007, 2010, 2016;MS Project 2007, 2010, 2016;EMID, AutoCAD
- możliwość zarządzania stacją roboczą poprzez polityki grupowe –przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji
- możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

b. **Wymogi równoważności odnośnie oprogramowania biurowego**

Wymogi równoważności w zakresie:
1) licencji:
a) licencja uprawniająca do wieczystego użytkowania;
b) wszystkie komponenty oferowanego pakietu biurowego muszą być integralną częścią tego samego pakietu, współpracować ze sobą (osadzanie i wymiana danych), posiadać jednolity interfejs oraz ten sam jednolity sposób obsługi, wykonywanie i edycja makr oraz kodu zapisanego w języku Visual Basic w plikach xls, xlsx oraz formuł w plikach wytworzonych w MS Office 2003, MS Office 2007,MS Office 2010, MSOffice 2013 oraz MS Office 2016 bez utraty danych oraz bez konieczności przerabiania dokumentów
2) funkcjonalności:
a) pakiet musi składać się z programów:
- do edycji tekstu;
- arkusza kalkulacyjnego;
- do tworzenia prezentacji;
- program do obsługi kontaktów;
b) edytor tekstu powinien umożliwiać:
- zapis i odczyt dokumentów w formatach: rtf, doc, docx oraz odt (dopuszczalne jest wykorzystanie w tym celu wtyczki);
- pełną współpracę z opcjami Recenzji pakietu Microsoft Office 2007 i wyższe, w szczególności tryb „Śledź zmiany" oraz obsługę komentarzy;
- obsługę trybu korespondencji seryjnej z użyciem źródeł danych ze skoroszytów generowanych za pomocą Microsoft Excel (oraz, w razie zaoferowania innego pakietu niż Microsoft Office, także arkusza kalkulacyjnego będącego częścią oferty);
c) arkusz kalkulacyjny powinien umożliwiać zapis i odczyt dokumentów w formatach: xls, xlsx, ods (dopuszczalne jest wykorzystanie w tym celu wtyczki), możliwość jednoczesnej pracy wielu użytkowników na udostępnionym doku mencie arkusza kalkulacyjnego;
d) program do tworzenia prezentacji powinien umożliwiać zapis i odczyt dokumentów w formatach: ppt, pptx, odp (dopuszczalne jest wykorzystanie w tym celu wtyczki);
e) wszystkie programy pakietu powinny umożliwiać eksport do formatu pdf, (dopuszczalne jest wykorzystanie w tym celu wtyczki);
f) program do obsługi kontaktów powinien realizować funkcje:
- klienta e-mail;
- kalendarza z terminarzem;
- menadżera kontaktów.
g) możliwość aktualizacji z serwerów producenta
h) umożliwienie aktualizacji poprawek bezpieczeństwa
h) umożliwienie synchronizacji oraz integracji z Microsoft 365

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

c. **Wymogi równoważności odnośnie oprogramowania ochrony stacji roboczych i serwerów**

Ochrona stacji roboczych

1. Pełne wsparcie dla systemu Windows 7/Windows 8/Windows 8.1/Windows 10
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja programu dostępna co najmniej w języku polskim oraz angielskim.
4. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
5. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim oraz angielskim.
6. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives

Ochrona antywirusowa i antyspyware

7. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
8. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
9. Wbudowana technologia do ochrony przed rootkitami.
10. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
11. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
12. Możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie" lub według harmonogramu.
13. System ma posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.
14. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
15. Skanowanie „na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
16. Możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu.
17. Możliwość skanowania dysków sieciowych i dysków przenośnych.
18. Skanowanie plików spakowanych i skompresowanych.
19. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
20. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
21. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
22. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
23. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

24. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
25. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
26. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
27. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
28. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
29. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
30. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
31. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
32. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
33. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
34. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
35. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
36. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
37. Program ma zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
38. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
39. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
40. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
41. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
42. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

43. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.
44. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
45. Możliwość automatycznego wysyłania nowych do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
46. Do wysłania próbki zagrożenia do laboratorium producenta, aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
47. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
48. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
49. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
50. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
51. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
52. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
53. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
54. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
55. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
56. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
57. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
58. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
59. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

60. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
61. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
62. W momencie podłączenia zewnętrznego nośnika, aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
63. Administrator ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
64. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
65. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

• tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

• tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

• tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

• tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

66. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
67. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
68. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
69. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
70. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
71. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.
72. Program ma posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
73. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
74. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
75. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

76. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
77. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
78. Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback). Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
79. Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
80. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
81. W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji.
82. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
83. Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron internetowych i kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
84. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.
85. Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
86. Program musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.
87. Możliwość podejrzenia informacji o licencji, która znajduje się w programie.
88. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM.
89. W programie musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.
90. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.
91. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.
92. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.
93. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
94. Program musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

95. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
96. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
97. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
98. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
99. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
100. Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
101. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.
102. Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść".
103. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
104. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
105. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
106. Administrator musi posiadać możliwość zastosowania reguł dla kontroli dostępu do stron w zależności od zdefiniowanego przedziału czasowego.
107. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
108. Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.
109. Program ma posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.

Ochrona przed spamem

110. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
111. Program ma umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
112. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
113. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
114. Możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
115. Możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

116. Możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
117. Program ma domyślnie współpracować z folderem „Wiadomości-śmieci", dostępnym w programie Microsoft Outlook.
118. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana"
119. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana".
120. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

Zapora osobista (personal firewall)
121. Zapora osobista ma pracować w jednym z czterech trybów: • tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
• tryb interaktywny – program pyta się o każde nowo nawiązywane połączenie,
• tryb oparty na regułach – program blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
• tryb uczenia się – program automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
122. Program musi oceniać reguły zapory systemu Windows.
123. Możliwość tworzenia list sieci zaufanych.
124. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
125. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego.
126. Możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
127. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
128. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet.
129. Wykrywanie modyfikacji w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu.
130. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
131. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
132. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
133. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie.
134. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

135. Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci.
136. Program musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów:
• z aplikacją lokalną, którą administrator wskazuje z listy,
• z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP.

Kontrola dostępu do stron internetowych
137. Aplikacja musi być wyposażona w zintegrowany moduł kontroli dostępu do stron internetowych.
138. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory.
139. Aplikacja musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
140. Podstawowe kategorie, w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy

Ochrona serwera Windows
1. Wsparcie dla systemów: Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012, Microsoft Windows Server 2008 R2 SP1, Microsoft Windows Server 2008 SP2 (oparty na procesorze x86 i x64), Server Core (Microsoft Windows Server 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016).
2. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
3. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
5. Wbudowana technologia do ochrony przed rootkitami i exploitami.
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
11. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

12. Możliwość skanowania dysków sieciowych i dysków przenośnych.
13. Skanowanie plików spakowanych i skompresowanych.
14. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
15. Aplikacja powinna wspierać mechanizm klastrowania.
16. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
17. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
b. tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
d. tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
e. tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.
18. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
19. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
20. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
21. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
22. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
23. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na serwerze.
24. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
25. Funkcja blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
26. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
27. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
28. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
29. Program musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

30. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
31. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
32. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
33. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
34. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
35. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
36. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
37. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
38. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
39. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
40. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
41. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
42. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
43. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
44. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
45. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.
46. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.
47. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
48. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i wyświetlić listę niezainstalowanych aktualizacji.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

49. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
50. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
51. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
52. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
53. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
54. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.
55. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
56. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
57. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
58. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
59. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
60. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
61. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
62. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
63. Aplikacja musi wspierać skanowanie magazynu Hyper-V.
64. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów.
65. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji modułów i samego oprogramowania.
66. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
67. Program musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”.
68. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

69. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.
70. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
71. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
72. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.
73. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
74. Program musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów.
75. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
76. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
77. Program musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

Ochrona serwera - Linux
Architektura rozwiązania
1. Skaner antywirusowy i antyspyware.
2. Skanowanie plików, plików spakowanych i archiwów samorozpakowujących.
3. Oprogramowanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów oprogramowania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
4. Oprogramowanie musi posiadać wbudowany mechanizm typu ,,watchdog". Monitoruje on tzw. stan zdrowia poszczególnych mikro-serwisów i automatycznie przeładowuje je w przypadku wykrycia zakłóceń w pracy mikro-serwisu.
5. Architektura rozwiązania musi pozwalać na uruchamianie poszczególnych mikro-serwisów, tylko na czas realizacji funkcjonalności przez nie realizowanych, co pozwala w znaczącym stopniu ograniczyć wykorzystanie zasobów systemu operacyjnego.
6. Oprogramowanie antywirusowe musi wspierać wieloprocesorową i wielordzeniową architekturę, w celu zapewnienia maksymalnego zwiększenia wydajności.
7. Oprogramowanie antywirusowe musi być wyposażone w moduł ochrony systemu plików w czasie rzeczywistym. Moduł nie może wymagać instalowania jakichkolwiek dodatkowych komponentów w systemie operacyjnym. Wszystkie komponenty muszą być instalowane w systemie, podczas instalacji z dostarczonego instalatora binarnego.
8. Silnik ochrony systemu plików w czasie rzeczywistym musi stanowić dodatkowy moduł jądra systemu Linux i musi być dodawany do jądra, podczas procesu instalacji oprogramowania antywirusowego.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

9. Ochrona systemu plików w czasie rzeczywistym musi być zapewniona nieprzerwanie od uruchomienia produktu i obejmuje skanowanie zarówno dysków lokalnych jak i zmapowanych dysków sieciowych.
10. Silnik skanujący musi działać wyłącznie z wykorzystaniem 64-bitowej architektury.
11. Oprogramowanie musi być w pełni zgodne z modułem SELinux, pracującym zarówno w trybie ,,Permissive" jak i ,,Enforcing".
12. Oprogramowanie podczas procesu instalacji, musi dodawać i konfigurować własne polityki modułu SELinux, które są kompatybilne z następującymi dystrybucjami systemów Linux: Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Centos 6, Centos 7.
13. Wszystkie mechanizmy bezpieczeństwa oprogramowania muszą wspierać system informowania o zagrożeniach w czasie rzeczywistym. System ten pozwala na weryfikowanie reputacji plików oraz procesów i identyfikację nowych i nieznanych zagrożeń.
14. Skaner systemu plików w czasie rzeczywistym musi działać dla operacji obsługi plików, dla co najmniej takich operacji jak: dostęp do pliku, utworzenie (zapisanie) pliku.
15. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
16. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
17. Oprogramowanie musi być wyposażone we własny wiersz polecenia (CLI). Polecenia muszą być odpowiedzialne co najmniej za: skanowanie na żądanie, konfigurację mechanizmów bezpieczeństwa, uruchamianie aktualizacji, przeglądanie logów aplikacji, konfigurację graficznego interfejsu użytkownika, obsługę kwarantanny plików.
18. Rozwiązanie musi wspierać system plików zamontowany z flagą ,,noexec".
19. Oprogramowanie musi pozwalać na uruchamianie zadań skanowania działających ,,w tle", z możliwością ustawienia dla nich niskiego priorytetu.
20. Zadania skanowania nie mogą zmieniać znacznika dostępu do plików.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

Skanowanie sieciowych systemów plików

1. Oprogramowanie antywirusowe musi pozwalać na skanowanie plików składowanych i obsługiwanych przez zewnętrzne rozwiązania obsługi danych typu NAS / SAN.
2. Oprogramowanie antywirusowe nie może wymagać instalacji jakichkolwiek dodatkowych modułów na rozwiązaniach typu NAS / SAN, a skanowanie plików musi się odbywać wyłącznie w oparciu o protokół ICAP.
3. Rozwiązanie musi umożliwiać zmianę domyślnego portu protokołu ICAP.
4. Oprogramowanie antywirusowe, do celów skanowania plików na rozwiązaniach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.

Instalacja

1. Oprogramowanie musi wspierać mechanizm instalacji zdalnej, realizowanej przez narzędzia do orkiestracji systemami operacyjnymi. Wspieranymi narzędziami muszą być co najmniej: Puppet, Chef, Ansible.
2. Oprogramowanie antywirusowe musi być wyposażone w mechanizm automatycznej aktualizacji komponentów programu.
3. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
4. Oprogramowanie musi wspierać następujące systemy operacyjne: RedHat Enterprise Linux (RHEL) 6 64-bit, RedHat Enterprise Linux (RHEL) 7 64-bit, CentOS 6 64-bit, CentOS 7 64-bit, Ubuntu Server 16.04 LTS 64-bit, Ubuntu Server 18.04 LTS 64-bit, Debian 9 64-bit, SUSE Linux Enterprise Server (SLES) 12 64-bit, SUSE Linux Enterprise Server (SLES) 15 64-bit

Licencjonowanie

1. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
2. Program musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.

Interfejs graficzny

1. Produkt musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna musi działać w oparciu o dynamicznie generowaną zawartość tworzoną z wykorzystaniem następujących technologii: React/Node.js, HTML5.
3. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
4. Lokalna konsola administracyjna musi zapewniać bezpieczne połączenie działające w oparciu o protokół HTTPS.
5. Lokalna konsola administracyjna musi umożliwiać uruchomienie jej, na wskazanym porcie TCP.
6. Logowanie do lokalnej konsoli administracyjnej musi być realizowane, poprzez podanie danych w postaci nazwy użytkownika i zdefiniowanego dla niego hasła.
7. Administrator systemu musi mieć możliwość zdefiniowania dodatkowych kont użytkowników, w lokalnej konsoli administracyjnej.
8. Lokalna konsola administracyjna musi zapewniać funkcjonalność zweryfikowania stanu licencji i informacji na jej temat.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814

9. Z poziomu lokalnej konsoli administracyjnej musi być możliwość zarządzania, wbudowanym modułem menadżera kwarantanny.
10. Lokalna konsola administracyjna musi zapewniać możliwość przełączenia wersji językowej konsoli, na etapie logowania. Lokalna konsola administracyjna musi posiadać interfejs, co najmniej w języku: polskim, angielskim.

Dodatkowe wymogi:

1. Wykonawca gwarantuje najwyższą jakość przedmiotu zamówienia.
2. Wykonawca udzieli gwarancji na sprzęt na okres 24 miesięcy (typ gwarancji door to door, chyba że OPZ stanowi inaczej), liczony od dnia podpisania protokołu odbioru przedmiotu zamówienia z nieodpłatnym (wliczonym w cenę oferty) serwisem wynikającym z warunków gwarancji i naprawą w okresie gwarancyjnym. Szczegółowe warunki gwarancji określa umowa.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle Orgmasz
00-879 Warszawa, ul. Żelazna 87, Tel: +48 (22) 100 14 63,
E-mail: instytut@orgmasz.pl | NIP: 525-000-82-93, REGON: 387143432
Sąd Rejonowym.st. Warszawy, XIII Wydz. Gospodarczy KRS nr 0000860814