SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

W POSTĘPOWANIU PROWADZONYM W TRYBIE PRZETARGU NIEOGRANICZONEGO ZGODNIE Z ZAPISAMI USTAWY Z DNIA 29 STYCZNIA 2004 ROKU PRAWO ZAMÓWIEŃ PUBLICZNYCH (TEKST JEDNOLITY DZ. U. Z 2019 R. POZ. 1843) (dalej zwana ustawą)

PT.
DOSTAWA OPROGRAMOWANIA ANTYWIRUSOWEGO ZAMAWIANEGO NA POTRZEBY PAŃSTWOWEJ SZKOŁY WYŻSZEJ IM. PAPIEŻA JANA PAWŁA II W BIAŁEJ PODLASKIEJ

Zatwierdzam

prof. dr hab. Jerzy Nitychoruk
Rektor PSW im. Papieża Jana Pawła II
w Białej Podlaskiej

Biała Podlaska styczeń 2020 r.

1. Nazwę (firmę) oraz adres Zamawiającego;

1.1. Zamawiający:	Państwowa Szkoła Wyższa im. Papieża Jana Pawła II w Białej Podlaskiej
1.2. Adres:	ul. Sidorska 95/97, 21 – 500 Biała Podlaska
1.3. REGON:	030310705
1.4. NIP:	537-21-31-853
1.5. Telefony:	
1.5.1. Rektorat	83 344 99 00
1.5.2. Magda Kalinowska	83 344 99 86
1.6. Adres e-mail:	
1.6.1. Rektorat	psw@pswbp.pl
1.6.2. Magda Kalinowska	m.kalinowska@pswbp.pl
1.6.3. Strona www	www.pswbp.pl

2. Tryb udzielenia zamówienia;

2.1. Postępowanie jest prowadzone w trybie przetargu nieograniczonego o wartości nie przekraczającej równowartość kwoty 214 000 euro zgodnie z art. 39 ustawy Prawo zamówień publicznych oraz przepisy wykonawcze wydane na jej podstawie.
2.2. Postępowanie nie jest prowadzone w celu zawarcia umowy ramowej.
2.3. Zamawiający nie przewiduje wyboru ofert z zastosowaniem aukcji elektronicznej.
2.4. Zamawiający informuje, iż nie przewiduje możliwości udzielenia zamówień, o których mowa w art. 67 ust. 1 pkt. 7) ustawy.
2.5. Zamawiający nie przewiduje określenia w opisie przedmiotu zamówienia wymagań związanych z realizacją zamówienia wskazanych w art. 29 ust. 4 ustawy.
2.6. Zaleca się, aby wszystkie pisma związanie z niniejszym postępowaniem, w tym ewentualne zapytania itp. były opatrzone numerem sprawy tj. SZP.272.1.2020.
2.7. Zamawiający informuje, iż przed wszczęciem przedmiotowego postępowania nie przeprowadził dialogu technicznego.
2.8. Zamawiający nie żąda przedstawienia informacji zawartych w ofercie w postaci katalogu elektronicznego lub dołączenia katalogu elektronicznego do oferty.
2.9. Zamawiający informuje, iż w Opisie przedmiotu zamówienia stanowiący załącznik nr 6 do niniejszej Specyfikacji Istotnych Warunków Zamówienia, dalej zwana SIWZ, określił standardy jakościowe odnoszące się do wszystkich istotnych cech przedmiotu zamówienia.

3. Opis przedmiotu zamówienia;

3.1. Przedmiotem zamówienia jest dostawa oprogramowania antywirusowego zamawianego na potrzeby Państwowej Szkoły Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej, szczegółowo opisane w Opisie przedmiotu zamówienia stanowiącym załącznik 6 do Specyfikacji Istotnych Warunków Zamówienia, dalej zwanej SIWZ.
3.2. Zamawiający nie dopuszcza możliwości złożenia ofert częściowych.
3.3. Nie dopuszcza się oferty wariantowej przewidującej odmienny niż określony w SIWZ sposób wykonania zamówienia.
3.4. Kod CPV: 48761000-0 Pakiety oprogramowania antywirusowego.

4. Termin wykonania zamówienia, termin płatności faktury/ rachunku, termin gwarancji.

4.1. Przedmiot zamówienia należy zrealizować w terminie do 2 dni kalendarzowych od dnia podpisania umowy.

4.2. Zapłata wynagrodzenia dokonana będzie na podstawie faktury / rachunku wystawionego po podpisaniu protokołu odbioru zrealizowanej bez usterek i wad całego przedmiotu zamówienia, płatnego w formie przelewu na rachunek bankowy Wykonawcy tam wskazany w terminie do 30 dni od dnia jej doręczenia Zamawiającemu.

5. Warunki udziału w postępowaniu oraz opis sposobu dokonywania oceny spełniania tych warunków.

5.1. O udzielenie Zamówienia mogą ubiegać się Wykonawcy, którzy:

5.1.1. Nie podlegają wykluczeniu.

5.1.2. Spełniają warunki:

5.1.2.1. Kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów. Zamawiający odstępuje od opisu warunku w tym zakresie.

5.1.2.2. Sytuacji ekonomicznej lub finansowej. Zamawiający odstępuje od opisu warunku w tym zakresie.

5.1.2.3. Zdolności technicznej lub zawodowej. Zamawiający odstępuje od opisu warunku w tym zakresie.

5.2. Spełnienie powyższych warunków podlegać będzie ocenie Zamawiającego dokonywanej metodą 0 – 1, tj. spełnia – nie spełnia, w oparciu o dokumenty, oświadczenia określone w SIWZ.

6. Podstawy wykluczenia;

6.1. Zamawiający wykluczy z postępowania Wykonawcę w przypadku zaistnienia którejkolwiek przesłanki określonej w art. 24 ust. 1 pkt 12 – 23 ustawy.

6.2. Zamawiający w niniejszym postępowaniu nie ustanawia żadnej przesłanki wykluczenia, o których mowa w art. 24 ust. 5 ustawy.

7. Wykaz oświadczeń lub dokumentów, potwierdzających spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia;

7.1. W celu potwierdzenia spełniania warunków udziału w postępowaniu Wykonawca złoży oświadczenie, którego wzór stanowi załącznik nr 2 do niniejszej SIWZ.

7.2. W celu potwierdzenia nie podlegania wykluczeniu na podstawie art. 24 ust. 1 pkt. 12-23 ustawy, Wykonawca złoży oświadczenie, którego wzór stanowi załącznik nr 3 do niniejszej SIWZ.

7.3. Zamawiający informuje, iż nie zastrzega osobistego wykonania przez Wykonawcę kluczowych części przedmiotu zamówienia objętego niniejszym postępowaniem.

7.4. Wykonawca zobowiązany jest w ofercie wskazać część zamówienia, którą zamierza powierzyć podwykonawcom.

7.5. Wykonawca, który zamierza powierzyć wykonanie części zamówienia podwykonawcom, w celu wykazania braku istnienia wobec nich podstaw wykluczenia, jest zobowiązany do złożenia oświadczenia, o którym mowa w punkcie 7.2. SIWZ w części dotyczącej podwykonawców.

7.6. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia.

7.6.1. W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego, a pełnomocnictwo do pełnienia takiej funkcji wystawione zgodnie z wymogami prawa, podpisane przez prawnie upoważnionych przedstawicieli każdego z partnerów winno być dołączone do wniosku.

7.6.2. Oferta winna być podpisana przez każdego partnera lub ustanowionego pełnomocnika.
7.6.3. Przepisy i wymagania dotyczące niepodlegania wykluczeniu z udziału w postępowaniu stosuje się odpowiednio do każdego Wykonawcy.
7.6.4. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia kopie dokumentów dotyczące każdego z tych Wykonawców są poświadczane za zgodność z oryginałem przez Wykonawcę lub pełnomocnika.
7.6.5. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia, których oferta zostanie uznana za najkorzystniejszą, przed podpisaniem umowy o realizację niniejszego zamówienia zobowiązani będą do zawarcia między sobą umowy cywilno-prawnej. Umowa musi być zawarta na czas trwania umowy. Niezwłocznie, po zawiadomieniu o wyborze oferty, jednakże nie później niż 3 dni od wysłania w/w zawiadomienia przez Zamawiającego, Wykonawcy muszą przedstawić Zamawiającemu umowę, opisującą przyjętą formę prawną oraz określającą zakres obowiązków każdego z Wykonawców przy realizacji umowy, w oryginale.
7.6.6. Umowa, o której mowa wyżej musi być podpisana przez upełnomocnionych przedstawicieli wszystkich Wykonawców składających ofertę wspólną. W umowie tej Wykonawcy wyznaczą spośród siebie Pełnomocnika upoważnionego do zaciągania zobowiązań w imieniu wszystkich Wykonawców realizujących wspólnie umowę. Pełnomocnik upoważniony będzie także do wystawiania faktur, przyjmowania płatności od Zamawiającego i do przyjmowania poleceń na rzecz i w imieniu wszystkich Wykonawców wspólnie realizujących umowę.

8. Oświadczenie składane obligatoryjnie przez wszystkich Wykonawców w terminie do 3 dni od dnia upublicznienia na stronie internetowej Zamawiającego wykazu złożonych ofert.

8.1. Oświadczenie o przynależności albo braku przynależności do tej samej grupy kapitałowej według wzoru stanowiącego załącznik nr 4 do SIWZ. Oświadczenie należy złożyć w oparciu o zamieszczony na stronie internetowej Zamawiającego wykaz ofert złożonych w danym postępowaniu.

9. Prócz dokumentów wskazanych w pkt. 7 do oferty należy załączyć:

9.1. Wypełniony formularz ofertowy, którego wzór stanowi załącznik nr 1 do SIWZ.
9.2. O ile nie wynika to z 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 (tekst jednolity Dz.U. z 2019 r. poz. 700 z późn. zm.) do oferty należy załączyć pełnomocnictwo lub inny dokument potwierdzający umocowanie osoby lub osób podpisujących ofertę do reprezentowania Wykonawcy.

10. Jeżeli Wykonawca nie złożyły oświadczeń lub dokumentów niezbędnych do przeprowadzenia postępowania, złożone oświadczenia lub dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez Zamawiającego wątpliwości, Zamawiający wezwie do ich złożenia, uzupełnienia lub poprawienia lub do udzielania wyjaśnień w terminie przez siebie wskazanym, chyba że mimo ich złożenia, uzupełnienia lub poprawienia lub udzielenia wyjaśnień oferta Wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.

11. Informacje o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń lub dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z wykonawcami.

11.1. Osoby upoważnione przez Zamawiającego do kontaktowania się z Wykonawcami:
- 11.1.1. w zakresie przedmiotu zamówienia: inż. Marcin Stefanowicz, tel. 83 344 99 55, m.kalinowska@pswbp.pl, pok. 333 ul. Sidorska 95/97, Biała Podlaska.
- 11.1.2. w zakresie proceduralnym: mgr Magda Kalinowska, tel. 83 344 99 86, m.kalinowska@pswbp.pl, pok. 338, ul. Sidorska 95/97, Biała Podlaska.

11.2. Korespondencja związana z niniejszym postępowaniem wedle uznania strony może być przekazywana za pomocą listu poleconego lub drogą elektroniczną.

11.3. Jeżeli Zamawiający lub Wykonawca przekazują oświadczenia, wnioski, zawiadomienia oraz informacje drogą elektroniczną, każda ze Stron na żądanie drugiej potwierdza fakt ich otrzymania.

11.4. W przypadku braku potwierdzenia otrzymania wiadomości przez Wykonawcę, Zamawiający domniema, iż pismo wysłane przez Zamawiającego na adres mailowy podany przez Wykonawcę zostało doręczone w sposób umożliwiający się zapoznanie Wykonawcy z treścią pisma.

11.5. Zamawiający uzna za ważne wszystkie oświadczenia, wnioski, zawiadomienia oraz informacje przekazane za pomocą poczty elektronicznej na adres r.olczuk@pswbp.pl.

11.6. Oferta wraz z wymaganymi SIWZ dokumentami i oświadczeniami musi zostać złożona w formie pisemnej przed upływem terminu składania ofert.

12. Adres poczty elektronicznej lub strony internetowej Zamawiającego, jeżeli zamawiający dopuszcza porozumiewanie się drogą elektroniczną;

12.1. http://bip.pswbp.pl, m.kalinowska@pswbp.pl

13. Wymagania dotyczące wadium;

13.1. Zamawiający nie żąda wniesienia wadium.

14. Termin związania ofertą;

14.1. Wykonawca będzie związany ofertą przez 30 dni.

14.2. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

14.3. Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą, z tym, że Zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni.

15. Opis sposobu przygotowywania ofert;

15.1. Wykonawca powinien zapoznać się ze wszystkimi rozdziałami składającymi się na SIWZ.

15.2. Wykonawca może złożyć tylko jedną ofertę, w której musi być zaoferowana tylko jedna ostateczna cena.

15.3. Oferta musi być przygotowana zgodnie z ustawą Prawo zamówień publicznych, aktami wykonawczymi wydanymi na podstawie ustawy oraz wymogami SIWZ.

15.4. Oferta powinna zostać przygotowana na / lub w formie formularzy, które stanowią załączniki do SIWZ.

15.5. Załączniki powinny być wypełnione przez Wykonawcę bez wyjątku, ściśle według warunków i postanowień zawartych w SIWZ.

15.6. Oferta musi być sporządzona w języku polskim, pisemnie na papierze przy użyciu nośnika pisma nieulegającego usunięciu bez pozostawiania śladów oraz podpisana przez upoważnionego przedstawiciela Wykonawcy.
15.7. Naniesione poprawki muszą być dokonane w sposób czytelny i parafowane przez osobę podpisującą ofertę.
15.8. Wszystkie dokumenty muszą być przedstawione w formie oryginału, kopii poświadczonej za zgodność z oryginałem przez osobę upoważnioną do reprezentowania Wykonawcy lub notarialnie potwierdzonej kopii, z zastrzeżeniem, że pełnomocnictwo musi być złożone w formie oryginału lub notarialnie potwierdzonej kopii.
15.9. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia oraz w przypadku podmiotów, o których mowa w pkt. 7.5. SIWZ, kopie dokumentów dotyczących odpowiednio wykonawcy lub tych podmiotów są poświadczane za zgodność z oryginałem przez Wykonawcę lub te podmioty.
15.10. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
15.11. Oferta musi być złożona w nieprzejrzystym, zamkniętym (zaklejonym), nienaruszonym opakowaniu, oznaczonym napisem:

„Oferta oprogramowanie antywirusowe SZP.272.1.2020”.
Nie otwierać do dnia 17.01.2020 r. godz. 10^{00}”
oraz nazwa i dokładny adres Wykonawcy.

15.12. Wszystkie koszty związane z przygotowaniem i złożeniem oferty ponosi Wykonawca.
15.13. Część oferty, która zawiera informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, a wykonawca zastrzega ich poufność, należy umieścić w odrębnej kopercie z opisem „Zastrzeżona część oferty”. Zamawiający nie odpowiada za ujawnienie informacji stanowiących tajemnicę przedsiębiorstwa przekazanych mu przez Wykonawcę wbrew postanowieniom niniejszego podpunktu. Wykonawca nie może zastrzec informacji, o których mowa w art. 86 ust. 4 ustawy.
15.14. W przypadku zastrzeżenia części oferty Wykonawca musi wykazać, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Przez tajemnicę przedsiębiorstwa rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co, do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności, zgodnie z ustawą z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tekst jednolity Dz. U. z 2019 r. poz. 1010).
15.15. Wykonawca może wprowadzić zmiany lub wycofać złożoną przez siebie ofertę pod warunkiem, że Zamawiający otrzyma powiadomienie o wprowadzeniu zmian lub wycofaniu przed terminem składania ofert. Powiadomienie musi być złożone według takich samych zasad jak składana oferta z dopiskiem ZMIANA lub WYCOFANIE.
15.16. Przy przesłaniu oferty drogą kurierską lub pocztową ryzyko uszkodzenia, zniszczenia, nie dotarcia oferty na czas i w miejsce wskazane do składania ofert ponosi Wykonawca.
15.17. W toku oceniania ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień dotyczących treści złożonych ofert.
15.18. Zamawiający nie planuje zwołania zebrania Wykonawców.

16. Miejsce oraz termin składania i otwarcia ofert;

16.1. Ofertę należy złożyć do dnia 17.01.2020 r. do godz. 9^{00} w Kancelarii Państwowej Szkoły Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej przy ul. Sidorskiej 95/97, 21 –500 Biała Podlaska.

16.2. Oferta złożona po terminie składania ofert, bez względu na przyczynę, zostanie niezwłocznie zwrócona Wykonawcy.

16.3. Otwarcie ofert nastąpi w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej ul. Sidorska 95/97 w pokoju nr 338 w dniu 17.01.2020 r. o godz. 10^{00}.

16.4. Otwarcie ofert jest jawne.

16.5. Bezpośrednio przed otwarciem ofert Zamawiający podaje kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia.

16.6. Podczas otwarcia ofert Zamawiający poda nazwy (firmy) oraz adresy Wykonawców, a także informacje dotyczące ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.

16.7. Wykonawcom, którzy nie byli na otwarciu ofert, informacje ogłoszone podczas otwarcia ofert zostaną doręczone na ich pisemny wniosek.

17. Opis sposobu obliczenia ceny;

17.1. Wykonawca musi przedstawić cenę oferty w formie indywidualnej kalkulacji, przy uwzględnieniu wymagań i zapisów ujętych SIWZ oraz doświadczenia zawodowego Wykonawcy.

17.2. W zaoferowanej cenie należy uwzględnić wszystkie koszty związane z dostawą oraz uruchomieniem przedmiotu zamówienia w tym koszty bezpośrednie i pośrednie, jakie Wykonawca uważa za niezbędne do poniesienia dla terminowego i prawidłowego wykonania przedmiotu zamówienia, zysk Wykonawcy oraz wszystkie wymagane przepisami podatki i opłaty oraz ewentualne upusty cenowe.

17.3. Wykonawca w formularzu Oferta poda łączną wartość brutto za zrealizowanie całości przedmiotu zamówienia.

17.4. Cena musi być wyrażona w złotych polskich niezależnie od wchodzących w jej skład elementów.

17.5. Oferowana cena jest ceną ostateczną i nie podlega waloryzacji w okresie realizacji umowy.

17.6. Wszystkie rozliczenia związane z przedmiotem zamówienia będą się odbywały w polskich złotych.

17.7. Zamawiający poprawi w tekście oferty oczywiste omyłki pisarskie, oczywiste omyłki rachunkowe z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek, inne omyłki polegające na niezgodności oferty ze specyfikacją istotnych warunków zamówienia, niepowodujące istotnych zmian w treści oferty - niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.

17.8. W przypadku rozbieżności pomiędzy wskazaną w ofercie ceną pisaną liczbową i słownie, Zamawiający uzna za prawidłowa cenę podaną słownie.

17.9. Nie przewiduje się zwrotu kosztów udziału w postępowaniu.

17.10. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami.

17.11. Wykonawca, składając ofertę, zobowiązany jest do poinformowania Zamawiającego, czy wybór oferty będzie prowadzić do powstania obowiązku

podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.

17.12. W przypadku Wykonawców, którzy posiadają siedzibę, stałe miejsce prowadzenia działalności lub stałe miejsce zamieszkiwania poza terytorium Rzeczypospolitej Polskiej to Zamawiający będzie zobowiązany do rozliczenia podatku od towarów i usług, Zamawiający, wyłącznie dla celów porównania ofert, doliczy do podanej ceny podatek VAT, zgodnie z obowiązującymi polskimi przepisami podatkowymi.

18. Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem znaczenia tych kryteriów i sposobu oceny ofert;

18.1. Do oceny oferty będzie brana oferowana cena brutto za cały zakres zamówienia.

18.2. W przypadku Wykonawców, którzy posiadają siedzibę, stałe miejsce prowadzenia działalności lub stałe miejsce zamieszkiwania poza terytorium Rzeczypospolitej Polskiej, jeśli to Zamawiający będzie zobowiązany do rozliczenia podatku od towarów i usług, Zamawiający, wyłącznie dla celów porównania ofert, doliczy do podanej ceny podatek VAT, zgodnie z obowiązującymi polskimi przepisami podatkowymi.

18.3. Zamówienie zostanie udzielone Wykonawcy nie podlegającemu wykluczeniu, którego oferta nie będzie podlegała odrzuceniu i otrzyma największą ilość punków zgodnie z przyjętym kryterium: Cena brutto oferty – 100 pkt.

18.4. Oferty zostaną ocenione wg wzoru:

Xc = (Cmin : Cof) x 100 pkt.
gdzie:

Xc	wartość punktowa ceny
Cmin	najniższa cena brutto wśród złożonych ofert
Cof	cena brutto oferty ocenianej

18.5. Jeżeli Wykonawca, którego oferta została wybrana, uchyla się od zawarcia umowy w sprawie zamówienia publicznego, Zamawiający wybierze ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzania ich ponownego badania i oceny, chyba, że zajdzie którakolwiek z przesłanek skutkująca koniecznością unieważnienia postępowania.

18.6. Za uchylanie się od zwarcia umowy Zamawiający uzna m.in.:

18.6.1. Wykonawca nie dostarczy przez podpisaniem umowy dokumentów wymaganych w SIWZ,

18.6.2. Dostarczone dokumenty nie będą potwierdzać wymagań określonych w SIWZ,

18.6.3. Nie stawienie się Wykonawcy w terminie lub miejscu wskazanym przez Zamawiającego w celu podpisania umowy,

18.6.4. Osoba reprezentująca Wykonawcę, która przybędzie w celu podpisania umowy, nie będzie posiadała stosownego umocowania do reprezentowania Wykonawcy.

18.7. O wyborze najkorzystniejszej oferty Zamawiający zawiadomi niezwłocznie wszystkich Wykonawców podając nazwę albo imię i nazwisko, siedzibę albo miejsce zamieszkania i adres, jeżeli jest miejscem wykonywania działalności Wykonawcy, którego ofertę wybrano, oraz nazwy albo imiona i nazwiska, siedziby albo miejsca zamieszkania i adresy, jeżeli są miejscami wykonywania działalności Wykonawców, którzy złożyli oferty, a także punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację.

18.8. O wykluczeniu Wykonawcy z postępowania lub odrzuceniu oferty lub unieważnieniu postępowania Zamawiający zawiadomi równocześnie wszystkich Wykonawców podając uzasadnienie faktyczne i prawne.
18.9. Informacje, o których mowa w pkt. 18.7. i 18.8. SIWZ, zostaną zamieszczone na stronie internetowej Zamawiającego oraz na tablicy ogłoszeń zlokalizowanej przy pokoju nr 338 w budynku Zamawiającego przy ul. Sidorskiej 95/97 w Białej Podlaskiej.

19. Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego;
19.1. Umowa zostanie zawarta niezwłocznie w terminie związania z ofertą jednak nie krótszym niż:
19.1.1. 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej.
19.1.2. 10 dni – jeżeli zostało przesłane w inny sposób niż przy użyciu środków komunikacji elektronicznej.
19.2. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminów, o których mowa w pkt. 19.1., jeżeli złożono tylko jedną ofertę.
19.3. W przypadku nie załączenia do oferty zaświadczenia z ewidencji działalności gospodarczej lub wypisu z krajowego rejestru sądowego do oferty Wykonawca zobowiązany jest do ich dostarczenia, na żądanie Zamawiającego, (w formie oryginału lub kopii potwierdzonej za zgodność z oryginałem) przed podpisaniem umowy.
19.4. W przypadku posłużenia się podwykonawcą Wykonawca złoży w formie załącznika do umowy zakres przedmiotu zamówienia, jego wartość oraz dane podwykonawcy odpowiedzialnego za powierzony zakres umowy.

20. Wymagania dotyczące zabezpieczenia należytego wykonania umowy;
20.1. Zamawiający nie żąda wniesienia zabezpieczenia należytego wykonania umowy.

21. Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia publicznego, ogólne warunki umowy albo wzór umowy, jeżeli Zamawiający wymaga od Wykonawcy, aby zawarł z nim umowę w sprawie zamówienia publicznego na takich warunkach;
21.1. Projekt umowy zawieranej w sprawie realizacji przedmiotu zamówienia objętego niniejszym postępowaniem stanowi załącznik nr 4 do SIWZ.
21.2. Zamawiający dopuszcza zmiany postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy w sytuacji wystąpienia zjawisk związanych z działaniem siły wyższej (jak np. klęska żywiołowa, niepokoje społeczne, działania militarne itp.). Zmiana postanowień umowy będzie dotyczyć zmiany zakresu przedmiotu umowy oraz sposobu jego realizacji, wynagrodzenia, terminu realizacji itp.
21.3. Zamawiający dopuszcza zmiany w sytuacji wystąpienia problemów finansowych po stronie Zamawiającego z przyczyn od niego niezależnych. Zmiana postanowień umowy może dotyczyć m.in. zmiany zakresu przedmiotu umowy, wynagrodzenia, terminu realizacji itp.
21.4. Zamawiający dopuszcza zmiany postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy w przypadku zaprzestania produkcji asortymentu oferowanego przez Wykonawcę, jeśli Wykonawca pomimo

dołożenia należytej staranności nie mógł uzyskać takiej informacji do chwili złożenia oferty. Wykonawca zobowiązany jest do uzyskania od producenta danego asortymentu informacji dotyczącej daty zaprzestania produkcji i zaoferować w zamian inny urządzenie o identycznych lub wyższych parametrach technicznych i funkcjonalności w zakresie wskazanym w SIWZ oraz przedstawić na piśmie propozycje zmian w zakresie specyfikacji technicznej i funkcjonalnej w stosunku do specyfikacji technicznej i funkcjonalnej określonej w opisie przedmiotu zamówienia. Zmiana postanowień umowy może dotyczyć m.in. zmiany zakresu przedmiotu umowy, wynagrodzenia (jedynie obniżenia), terminu realizacji itp.

21.5. Zmiany osób odpowiedzialnych za realizację zamówienia, zarówno ze strony Zamawiającego, jak i Wykonawcy, zmiana danych teleadresowych, zmiany osób reprezentujących strony itp. podobne zmiany nie stanowią istotnej zmiany umowy w rozumieniu art. 144 ust. 1e ustawy.

22. Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy w toku postępowania o udzielenie zamówienia.

22.1. Środki ochrony prawnej przysługują Wykonawcy a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy przysługują środki ochrony prawnej określone w Dziale VI ustawy.

22.2. Środki ochrony prawnej określone w Dziale VI ustawy wobec ogłoszenia o zamówieniu oraz SIWZ przysługują również organizacjom wpisanym na listę, o której mowa w art. 154 pkt. 5 ustawy.

23. Obowiązek informacyjny wynikający z art. 13 RODO w przypadku zbierania danych osobowych bezpośrednio od osoby fizycznej, której dane dotyczą, w celu związanym z postępowaniem o udzielenie zamówienia publicznego.

23.1. Zgodnie z art. 13 ust. 1 i 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, str. 1), dalej „RODO", informuję, że:

23.1.1. administratorem Pani/Pana danych osobowych jest Państwowa Szkoła Wyższa im. Papieża Jana Pawła II w Białej Podlaskiej ul. Sidorska 95/97, 21 - 500 Biała Podlaska

23.1.2. inspektorem ochrony danych osobowych w Państwowa Szkoła Wyższa im. Papieża Jana Pawła II w Białej Podlaskiej jest Jan Sroka tel. 83 344 99 82 e-mail iod@pswbp.pl;

23.1.3. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego nr SZP.272.1.2020.

23.1.4. odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy Prawo zamówień publicznych;

23.1.5. Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Prawo zamówień publicznych, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;

23.1.6. obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach

ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;

23.1.7. w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;

23.1.8. posiada Pani/Pan:

23.1.8.1. na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;

23.1.8.2. na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych;

23.1.8.3. na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;

23.1.8.4. prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

23.1.8.5. nie przysługuje Pani/Panu:

23.1.8.5.1. w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;

23.1.8.5.2. prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;

23.1.8.5.3. na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

24. Wykaz załączników

24.1.	Załącznik nr 1	Formularz oferty.
24.2.	Załącznik nr 2	Oświadczenie o spełnianiu warunków.
24.3.	Załącznik nr 3	Oświadczenie o niepodleganiu wykluczeniu.
24.4.	Załącznik nr 4	Oświadczenie grupa kapitałowa.
24.5.	Załącznik nr 5	Projekt umowy.
24.6.	Załącznik nr 6	Opis przedmiotu zamówienia.

Nazwa Wykonawcy Załącznik nr 1

……

……

Adres siedziby

……

……

Adres do korespondencji

……

……

tel. - ……

E-mail: ……

NIP - ……

O F E R T A

Nawiązując do ogłoszenia o postępowaniu o udzielenie zamówienia publicznego prowadzonego zgodnie z art. 39 ustawy z dnia 29 stycznia 2004 roku Prawo Zamówień Publicznych (tekst jednolity Dz. U. z 2019 r. poz. 1843) w trybie przetargu nieograniczonego pt. *„Dostawa oprogramowania antywirusowego zamawianego na potrzeby Państwowej Szkoły Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej”* składam niniejszą ofertę i oferuję wykonanie przedmiotu zamówienia objętego niniejszym postępowaniem, zgodnie z wymogami zawartymi w SIWZ za cenę brutto …… zł (słownie: ……..…… zł)

1. Oświadczam, iż przedmiot zamówienia zrealizuję w terminie do 2 dni kalendarzowych od dnia podpisania umowy.
2. Akceptuję termin zapłaty wynagrodzenia wskazany w SIWZ i zagwarantuję wykonanie całości przedmiotu zamówienia przy założeniu, że zapłata wynagrodzenia dokonana będzie na podstawie faktury / rachunku wystawionego po podpisaniu protokołu odbioru zrealizowanego bez usterek, niedoróbek, całego przedmiotu zamówienia, płatnego przelewem na rachunek bankowy w nich wskazany, w terminie do 30 dni od dnia doręczenia Zamawiającemu prawidłowo wystawionych faktury / rachunku.

……

podpis osoby upoważnionej

3. Akceptuję wskazany w SIWZ termin związania ofertą, tj. 30 dni.
4. Oświadczam, że wybór oferty będzie / nie będzie* prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług.
5. Akceptuję projekt umowy i w sytuacji wybrania oferty zobowiązuje się do podpisania umowy na warunkach zawartych w SIWZ, w miejscu i terminie wskazanym przez Zamawiającego.
6. Oświadczam, iż oferowany przedmiot zamówienia jest zgodny z wymogami Zamawiającego określonymi w niniejszej SIWZ.
7. Oświadczam, że:
   1) Realizację przedmiotu zamówienia zamierzam wykonać sam*
   2) Realizację przedmiotu zamówienia zamierzam wykonać sam oraz przy użyciu podwykonawców. Zakres przedmiotu zamówienia jaki planuje powierzyć podwykonawcom (podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG oraz precyzyjne określić powierzaną część zamówienia):
      ……
      ……*
      W sytuacji nie wykreślenia / zaznaczenia żadnej z powyższych opcji, Zamawiający uzna, że Wykonawca wykonuje przedmiot bez udziału podwykonawców.
8. Oświadczam, że załączone do oferty dokumenty opisują stan prawny i faktyczny, aktualny na dzień otwarcia ofert.
9. Informacje stanowiące tajemnicę Wykonawcy znajdują się na następujących stronach oferty: ……do, których tylko Zamawiający ma możliwość wglądu.
10. Wykonawca oświadcza, że jest:
    1) mikroprzedsiębiorstwem (przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów EUR);**

……
podpis osoby upoważnionej

2) małym przedsiębiorstwem (przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EUR);**
3) średnim przedsiębiorstwem (przedsiębiorstwo, które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwami i które zatrudniają mniej niż 250 osób i których roczny obrót nie przekracza 50 milionów EUR lub roczna suma bilansowa nie przekracza 43 milionów EUR);**
4) innym niż ww.**

11. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu****.
12. Załącznikami do niniejszego formularza stanowiącymi integralną część oferty są:

1) …… 3) ……

2) …… 4) ……

Oferta wraz z załącznikami składa się z …… kolejno ponumerowanych stron/kartek**.

…… ……
miejscowość data podpis osoby upoważnionej

* niepotrzebne skreślić (w sytuacji nie wykreślenia / zaznaczenia żadnej z powyższych opcji, Zamawiający uzna, że wybór oferty nie będzie prowadził do powstania u Zamawiającego obowiązku podatkowego lub/oraz Wykonawca wykonuje przedmiot bez udziału podwykonawców).
** niepotrzebne skreślić.
*** W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).

Załącznik nr 2

Nazwa Wykonawcy

……

……

……

O Ś W I A D C Z E N I E

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez Zamawiającego w postępowaniu nr SZP.272.1.2020 określone w Specyfikacji Istotnych Warunków Zamówienia.

…… ……

miejscowość data podpis osoby upoważnionej

Załącznik nr 3

Nazwa Wykonawcy

……

……

……

O Ś W I A D C Z E N I E
nie podleganiu wykluczeniu z udziału w postępowaniu

1. Oświadczam, iż nie podlegam wykluczeniu z udziału w postępowaniu nr SZP.272.1.2020 na podstawie art. 24 ust. 1 pkt. 12-23 ustawy Prawo zamówień publicznych (tekst jednolity Dz. U. z 2019 r. poz. 1843).
2. Oświadczam, że podlegam wykluczeniu wykluczenia z postępowania na podstawie art. ……. ustawy (Wykonawca zobowiązany jest określić mającą zastosowanie podstawę wykluczenia wymienioną w art. 24 ust. 1 pkt 13-14 oraz 16-20 ustawy). Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 24 ust. 8 ustawy Pzp podjąłem następujące środki naprawcze: ……

   ……

   ……

   ……*

…… ……

miejscowość data podpis osoby upoważnionej

OŚWIADCZENIE
dotyczące podanych informacji:

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

…… ……

miejscowość data podpis osoby upoważnionej

* Wykonawca, który podlega wykluczeniu na podstawie art. 24 ust. 1 pkt 13 i 14 oraz 16–20 ustawy, 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. Wykonawca nie podlega wykluczeniu, jeżeli Zamawiający, uwzględniając wagę i szczególne okoliczności czynu Wykonawcy, uzna za wystarczające w/w dowody.

OŚWIADCZENIE
DOTYCZĄCE PODWYKONAWCY NIEBĘDĄCEGO PODMIOTEM, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA

Oświadczam, że w stosunku do następującego/ych podmiotu/tów, na którego/ych, będącego podwykonawcą: ……

……..…

……

……

(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG), nie zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia.

……
podpis osoby upoważnionej

OŚWIADCZENIE
DOTYCZĄCE PODMIOTU, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA:

Oświadczam, że w stosunku do następującego/ych podmiotu/tów, na którego/ych zasoby powołuję się w niniejszym postępowaniu, tj.: ……..……

……

……

……

(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG) nie zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia.

…… ……
miejscowość data podpis osoby upoważnionej

* Wykonawca, który podlega wykluczeniu na podstawie art. 24 ust. 1 pkt 13 i 14 oraz 16–20 ustawy, 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. Wykonawca nie podlega wykluczeniu, jeżeli Zamawiający, uwzględniając wagę i szczególne okoliczności czynu Wykonawcy, uzna za wystarczające w/w dowody.

Załącznik nr 4

Nazwa Wykonawcy

……

……

……

O Ś W I A D C Z E N I E *

1. Zgodnie z zamieszczoną w dniu w składania i otwarcia ofert na stronie internetowej www.bip.pswbp.pl informacji, o której mowa w art. 86 ust. 5 ustawy, dotyczącą postępowania nr SZP.272.1.2020, postępując zgodnie z art. 24 ust. 11 ustawy Prawo zamówień publicznych oświadczam, że:
   1) Nie należę do grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt. 23) ustawy Prawo zamówień publicznych (tekst jednolity Dz. U. z 2019 r. poz. 1843).*
   2) Należę do grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt. 23) ustawy Prawo zamówień publicznych (tekst jednolity Dz. U. z 2019 r. poz. 1843) i jako załącznik składam listę podmiotów należących do tej samej grupy kapitałowej, którzy złożyli oferty w przedmiotowym postępowaniu*/** ……
   ……
   ……
   ……
   ……
   ……

…… ……
miejscowość data podpis osoby upoważnionej

* Oświadczenie należy złożyć w oryginale w terminie 3 dni od dnia, o którym mowa pkt. 1.
** W przypadku przynależności do tej samej grupy kapitałowej Wykonawca wraz z oświadczeniem może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w przedmiotowym postępowaniu.

Załącznik nr 5

UMOWA NR SZP…2020

zawarta zgodnie z art. 39 ustawy Prawo zamówień publicznych w trybie przetargu nieograniczonego o wartości poniżej 221 tys. euro (tekst jednolity Dz. U. z 2019 r. poz. 1843)

w dniu …… roku w Białej Podlaskiej, pomiędzy:
Państwową Szkołą Wyższą im. Papieża Jana Pawła II w Białej Podlaskiej z siedzibą przy ul. Sidorskiej 95/97 w Białej Podlaskiej, NIP …… zwaną w treści umowy „Zamawiającym", reprezentowaną przez:
……..
przy kontrasygnacie:
……
a …… z siedzibą w …… przy ul. ……, wpisanym do …… za nr …… NIP ……, REGON …… zwanym w treści umowy „Wykonawcą", reprezentowanym przez:
……
łącznie dalej zwanych Stronami.
Na podstawie dokonanego przez Zamawiającego wyboru oferty Wykonawcy w przetargu nieograniczonym opublikowanym w dniu …… pod nr …… w Biuletynie Zamówień Publicznych została zawarta umowa o następującej treści:

Przedmiot umowy
§ 1

1. Przedmiotem zamówienia jest dostawa oprogramowania antywirusowego – licencji na 500 stanowisk na okres 3 lat na potrzeby Państwowej Szkoły Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej, szczegółowo opisanej co do rodzaju w niniejszej umowie i Opisie przedmiotu zamówienia, której kopia stanowi załącznik nr 1 do niniejszej umowy, oraz zgodnie z ofertą Wykonawcy, której kopia stanowi załącznik nr 2 do niniejszej umowy (przedmiot umowy). W/w i n/w załączniki stanowią integralną część niniejszej umowy.
2. Wykonawca zapoznał się z warunkami realizacji niniejszej umowy, dokonał szczegółowej ich analizy oraz zapoznał się z warunkami dostawy i w związku z tym oświadczył, iż posiada uprawnienia, niezbędną wiedzę, umiejętności oraz potencjał do wykonania czynności określonych w ust. 1 niniejszego paragrafu i zobowiązuje się do wykonywania czynności objętych niniejszą umową z należytą starannością oraz, że nie zachodzą żadne okoliczności, które mogłyby mieć wpływ na należyte wykonanie przez niego niniejszej umowy.
3. Wykonawca będzie realizował przedmiot umowy, o którym mowa w ust. 1 niniejszej umowy, siłami własnymi lub przy udziale wybranych przez siebie podwykonawców. Zakres powierzonych podwykonawcom części przedmiotu umowy oraz ich wartość została określona w załączniku nr 3 do niniejszej umowy. Wykonawca za działania bądź zaniechania podwykonawcy, odpowiada tak jak za działania bądź zaniechania własne.

Warunki realizacji
§ 2

Wykonawca w ramach realizacji przedmiotu umowy, o którym mowa w § 1 ust. 1 niniejszej umowy, zobowiązany jest do:

1) dostawy oprogramowania antywirusowego – licencja na 500 stanowisk,
2) licencja 3-letnia na użytkowanie i aktualizacje,

3) dostarczenia wszelkich wymaganych dokumentów takich jak licencje, certyfikaty itp. w wersji zarówno papierowej jak i elektronicznej o ile stanowią one nieodłączną część w/w pakietu oprogramowania.

Termin realizacji

§ 3

Przedmiot umowy, o którym mowa w § 1 ust. 1 niniejszej umowy, należy zrealizować w terminie do …. dni kalendarzowych od daty zawarcia niniejszej umowy.

§ 4

1. Zamawiający dokona odbioru przedmiotu umowy, o którym mowa w § 1 ust. 1 niniejszej umowy, niezwłocznie po osiągnięciu gotowości do odbioru tj. jego dostawie do Zamawiającego.
2. Z czynności odbioru zostanie sporządzony protokół odbioru zawierający wszelkie istotne okoliczności i oświadczenia Stron, a w tym oświadczenie Zamawiającego o odbiorze prawidłowo wykonanego przedmiotu umowy, o którym mowa w § 1 ust. 1 niniejszej umowy bądź odmowie odbioru, wskazaniu przyczyn odmowy oraz ewentualnie wyznaczeniu nowego terminu odbioru.
3. Zamawiający ma prawo odmówić odbioru, jeżeli:
   1) przedmiot umowy, o którym mowa w § 1 ust. 1 niniejszej umowy, nie będzie zgodny z Opisem przedmiotu zamówienia stanowiącym załącznik nr 1 do niniejszej umowy oraz ofertą stanowiącą załącznik nr 2 do umowy, albo
   2) stwierdzone zostaną wady przedmiotu umowy, o którym mowa w § 1 ust. 1 niniejszej umowy, albo
   3) Wykonawca naruszy inne postanowienia niniejszej umowy.

Cena i warunki płatności

§ 5

1. Za terminowe i prawidłowe pod względem jakościowym i ilościowym wykonanie przedmiotu umowy, o którym mowa w § 1 ust. 1 niniejszej umowy, Zamawiający zapłaci Wykonawcy łączne wynagrodzenie w kwocie brutto ……..… zł (słownie: …… zł i 00/100) wskazanej w ofercie Wykonawcy, której kopia stanowi załącznik nr 2 do niniejszej umowy.
2. Zapłata wynagrodzenia, o którym mowa w ust. 1 niniejszego paragrafu, dokonana będzie na podstawie faktury / rachunku, wystawionego po podpisaniu protokołu odbioru bez uwag zrealizowanego bez usterek, niedoróbek, wad całego przedmiotu umowy, o którym mowa w § 1 ust. 1 niniejszej umowyy, płatnego przelewem na rachunek bankowy wskazany w fakturze / rachunku w terminie do … dni od dnia doręczenia Zamawiającemu faktury / rachunku.
3. Kwota określona w ust. 1 niniejszego paragrafu jest kwotą ostateczną obejmującą cały zakres umowy przedstawiony w § 1 ust. 1 niniejszej umowy, i jako wynagrodzenie ryczałtowe nie będzie podlegać jakiejkolwiek waloryzacji ani jakiemukolwiek zwiększeniu, w tym w szczególności w przypadku ustawowej zmiany stawki podatku VAT.
4. Zamawiający oświadcza, że jest płatnikiem podatku VAT i posiada nr NIP 537-21-31-853.
5. Wykonawca oświadcza, że jest płatnikiem podatku VAT i posiada nr NIP ……...

Odstąpienie od umowy i kary umowne

§ 6

1. Poza wypadkami wymienionymi w Kodeksie cywilnym, ustawie Prawo zamówień publicznych oraz Specyfikacji Istotnych Warunków Zamówienia Zamawiający może

odstąpić od umowy w całości z przyczyn leżących po stronie Wykonawcy, również w szczególności gdy:
1) Wykonawca w terminie, o którym mowa w § 3 niniejszej umowy, nie przystąpi do realizacji przedmiotu umowy lub nie dostarczy całego przedmiotu umowy, o którym mowa w § 1 ust. 1 niniejszej umowy;
2) Zamawiający odmówi dokonania odbioru całego przedmiotu umowy, o którym mowa w § 1 ust. 1 niniejszej umowy, z przyczyn wskazanych w umowie;
3) Wykonawca wykona usługę bez należytej staranności co skutkować będzie niewłaściwym funkcjonowaniem oprogramowania;
4) Wykonawca naruszy inne istotne warunki niniejszej umowy.

2. W przypadku odstąpienia od niniejszej umowy w całości Wykonawcy nie przysługuje jakiekolwiek wynagrodzenie z tytułu wykonana przedmiotu umowy, o którym mowa w § 1 ust. 1 niniejszej umowy.
3. Prawo odstąpienia od niniejszej umowy Zamawiający może wykonać w terminie 3 dni kalendarzowych od uzyskania informacji o okoliczności wskazanej w ust. 1 niniejszego paragrafu, stanowiącej przyczynę odstąpienia.
4. Odstąpienie od niniejszej umowy powinno nastąpić w formie pisemnej pod rygorem nieważności i powinno zawierać uzasadnienie.

§ 7

5. Wykonawca zobowiązuje się do zapłaty kary umownej w wysokości:
   1) 20% ceny brutto wskazanej w § 5 ust. 1 umowy jeżeli odstąpi od umowy lub też jeżeli od umowy odstąpi Zamawiający z przyczyn za które odpowiedzialność ponosi Wykonawca i to niezależnie od ewentualnego odbioru częściowego, tj. fakt dokonania odbioru częściowego nie ma wpływu na obowiązek zapłaty kary umownej, która również w takim przypadku obliczona zostanie od wartości całego zamówienia;
   2) 0,5% ceny brutto wskazanej w § 5 ust. 1 umowy za każdy dzień opóźnienia w wykonaniu przedmiotu zamówienia w stosunku to terminu wskazanego w § 3 umowy i to niezależnie od ewentualnego odbioru częściowego, tj. fakt dokonania odbioru częściowego nie ma wpływu na obowiązek zapłaty kary umownej, która również w takim przypadku obliczona zostanie od wartości całego zamówienia.
6. Zastrzeżenie kar umownych, o których mowa w ust. 1 niniejszego paragrafu, nie wyłącza możliwości dochodzenia przez Zamawiającego odszkodowania na zasadach ogólnych, w wysokości przenoszącej zastrzeżone kary umowne. Wykonawca zobowiązuje się w szczególności do pokrycia wszelkich kosztów poniesionych przez Zamawiającego na skutek niewykonania lub nienależytego wykonania umowy, w terminie 7 dni od doręczenia Wykonawcy zestawienia tych kosztów.
7. Naliczone kary umowne, jak również koszty wskazane w ust. 2 niniejszego paragrafu, Zamawiający może również potrącić z przysługującej Wykonawcy wierzytelności z tytułu wynagrodzenia.
8. Skorzystanie przez Zamawiającego z prawa odstąpienia, nie wyłącza uprawnienia Zamawiającego do naliczenia kar umownych wynikających z niniejszej umowy, a następnie dochodzenia zapłaty tychże kar umownych, jak również odszkodowania na zasadach ogólnych, w wysokości przenoszącej zastrzeżone kary umowne.

Postanowienia końcowe

§ 8

1. Zmiana postanowień niniejszej umowy wymaga formy pisemnej pod rygorem nieważności.
2. Niedopuszczalna jest zmiana postanowień zawartej umowy oraz wprowadzenie nowych postanowień do umowy niekorzystnych dla Zamawiającego, jeżeli przy ich uwzględnieniu

należałoby zmienić treść oferty, na podstawie której dokonano wyboru Wykonawcy, chyba że konieczność wprowadzenia takich zmian została przewidziana w Specyfikacji Istotnych Warunków Zamówienia lub ogłoszeniu.

§ 9

Ewentualne spory wynikłe przy wykonywaniu niniejszej umowy Strony poddają rozstrzygnięciu sądowi powszechnemu właściwemu dla siedziby Zamawiającego.

§ 10

W sprawach nieunormowanych niniejszą umową mają zastosowanie przepisy Kodeksu cywilnego i ustawy Prawo zamówień publicznych.

§ 11

1. Osoba po stronie Wykonawcy podpisująca niniejszą umowę oświadcza, że jest w pełnym zakresie umocowana do podpisywania i składania oświadczeń woli w imieniu Wykonawcy, którego reprezentuje i że umocowanie to nie wygasło w dniu zawarcia niniejszej umowy.
2. Osoby po stronie Zamawiającego podpisujące niniejszą umowę oświadczają, że są umocowane do podpisywania i składania oświadczeń woli w imieniu Zamawiającego, którego reprezentują i że umocowanie to nie wygasło w dniu zawarcia niniejszej umowy.
3. Zawiadomienia wskazane w niniejszej umowie mogą być dokonywane na piśmie, pocztą elektroniczną za potwierdzeniem odbioru lub drogą telefaksową na numery telefoniczne i adresy stron:
   1) Wykonawcy: ……
   2) Zamawiającego: Państwowa Wyższa Szkoła im. Papieża Jana Pawła II w Białej Podlaskiej ul. Sidorska 95/97, 21-500 Biała Podlaska e-mail: psw@pswbp.pl, tel. 83 344 99 00,
4. Strony są zobowiązane informować się niezwłocznie nawzajem na piśmie o każdej zmianie siedziby, bądź adresu do doręczeń, pod rygorem uznania doręczenia korespondencji na ostatnio wskazany adres za skuteczne, tj. wywołujące skutki prawne.
5. Osobą odpowiedzialną za realizację i odbiór przedmiotu niniejszej umowy ze strony Zamawiającego jest ……
6. Osoba wskazana w ust. 5 niniejszego paragrafu nie jest upoważniona do składania oświadczeń woli w imieniu Zamawiającego, które zmierzałyby do zmiany bądź uzupełnienia niniejszej umowy.

§ 12

Umowę sporządzono w trzech jednobrzmiących egzemplarzach - dwa dla Zamawiającego, jeden dla Wykonawcy.

Załączniki:

1. Opis przedmiotu zamówienia,
2. Kopia oferty Wykonawcy.

Załącznik nr 6

Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest dostawa oprogramowania antywirusowego zamawianego na potrzeby Państwowej Szkoły Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej, szczegółowo opisane
2. Ochrona stacji roboczych - Windows
   2.1. Pełne wsparcie dla systemu Windows 7/Windows 8/Windows 8.1/Windows 10.
   2.2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
   2.3. Wersja programu dostępna co najmniej w języku polskim oraz angielskim.
   2.4. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
   2.5. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim oraz angielskim.
   2.6. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives
3. Ochrona antywirusowa i antyspyware
   3.1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
   3.2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
   3.3. Wbudowana technologia do ochrony przed rootkitami.
   3.4. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
   3.5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
   3.6. Możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików "na żądanie" lub według harmonogramu.
   3.7. 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.
   3.8. 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).
   3.9. Skanowanie „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
   3.10. Możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania "na żądanie" i według harmonogramu.
   3.11. Możliwość skanowania dysków sieciowych i dysków przenośnych.
   3.12. Skanowanie plików spakowanych i skompresowanych.
   3.13. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
   3.14. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
   3.15. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
   3.16. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
   3.17. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputer.

3.18. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
3.19. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
3.20. 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.
3.21. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
3.22. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
3.23. 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).
3.24. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
3.25. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
3.26. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
3.27. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
3.28. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
3.29. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
3.30. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
3.31. Program ma zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
3.32. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
3.33. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
3.34. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
3.35. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
3.36. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
3.37. 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.
3.38. 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.

3.39. 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.

3.40. Do wysłania próbki zagrożenia do laboratorium producenta, aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.

3.41. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

3.42. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.

3.43. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.

3.44. 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.

3.45. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.

3.46. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.

3.47. 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.

3.48. 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.

3.49. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.

3.50. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.

3.51. 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.

3.52. 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.

3.53. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.

3.54. 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.

3.55. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla

podłączanych urządzeń w zależności od zalogowanego użytkownika.

3.56. W momencie podłączenia zewnętrznego nośnika, aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.

3.57. Administrator ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.

3.58. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).

3.59. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

3.59.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

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

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

3.59.4. 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,

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

3.60. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.

3.61. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.

3.62. Oprogramowanie musi posiadać zaawansowany skaner pamięci.

3.63. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.

3.64. 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.

3.65. 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.

3.66. 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.

3.67. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.

3.68. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.

3.69. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.

3.70. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium

aktualizacji modułów.

3.71. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.

3.72. Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).

3.73. Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

3.74. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.

3.75. W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji.

3.76. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.

3.77. Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń.

3.78. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.

3.79. Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.

3.80. 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.

3.81. Możliwość podejrzenia informacji o licencji, która znajduje się w programie.

3.82. W programie musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.

3.83. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.

3.84. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.

3.85. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.

3.86. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.

3.87. Program musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.

3.88. 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.

3.89. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.

3.90. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.

3.91. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

3.92. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia

zagrożenia.

3.93. Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.

3.94. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.

3.95. Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść".

3.96. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

3.97. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.

3.98. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.

3.99. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.

3.100. Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.

3.101. Program ma posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.

4. Ochrona stacji roboczych - Mac OSX

4.1. Procesor 32-bit (x86) / 64-bit (x64), Intel®.

4.2. Pełne wsparcie dla systemów Mac OS X 10.9 lub nowszy.

4.3. Wersja programu dostępna co najmniej w języku polskim oraz angielskim.

4.4. Pomoc w programie (help) w języku polskim oraz angielskim.

4.5. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

4.6. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.

4.7. W momencie wykrycia trybu pełnoekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.

4.8. Skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

4.9. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.

4.10. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności).

4.11. Możliwość skanowania dysków sieciowych i dysków przenośnych.

4.12. Skanowanie plików spakowanych i skompresowanych.

4.13. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

4.14. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.

4.15. 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.

4.16. 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.

4.17. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.

4.18. Możliwość wykonania skanowania i wysłania pliku do analizy z poziomu menu kontekstowego.

4.19. Aktualizacje modułów analizy heurystycznej.

4.20. 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 mają być wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.

4.21. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.

4.22. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

4.23. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.

4.24. Ochrona przed atakami typu „phishing".

4.25. Funkcja blokowania nośników wymiennych ma umożliwiać wyłączenie dostępu do nośników: Płyta CD/DVD, Pamięć masowa, karty sieciowe, Drukarka USB, Urządzenie do tworzenia obrazów, Port szeregowy, Urządzenie przenośne.

4.26. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.

4.27. Aktualizacja modułów programu antywirusowego ma być dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy serwera HTTP.

4.28. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.

4.29. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po wystąpieniu zdarzenia).

4.30. Program umożliwia automatyczne sprawdzanie plików wykonywanych podczas uruchamiania systemu operacyjnego.

4.31. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

4.32. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania oraz dokonanym skanowaniem komputera.

4.33. Program ma umożliwiać importowanie oraz eksportowanie ustawień. Z poziomu interfejsu graficznego użytkownik ma mieć możliwość przywrócenia wartości domyślnych wszystkich ustawień.

4.34. Program musi posiadać mechanizm Ochrony dostępu do stron internetowych monitoruje komunikację w ramach protokołu HTTP.

4.35. Program musi pozwalać na konfigurację portów, dla których ma się odbywać skanowanie protokołu HTTP.

4.36. Program ma umożliwiać w ramach zdefiniowanej grupy „Uprzywilejowani użytkownicy" na modyfikację konfiguracji programu.

4.37. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

4.38. Możliwość zdalnego zarządzania programem z poziomu Administracji zdalnej.
4.39. Ochrona poczty mail:
4.39.1. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej niezależnie od programu pocztowego.
4.39.2. 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).
4.39.3. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
4.39.4. Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.
4.39.5. Możliwość opcjonalnego dołączenia informacji w temacie zainfekowanej wiadomości o jej przeskanowaniu.
4.39.6. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.

5. Ochrona urządzeń mobilnych opartych o system Android
5.1. Wspierany system co najmniej Android 5.0.
5.2. Rozdzielczość wyświetlacza urządzenia 480x800px lub wyższa.
5.3. Procesor: ARM z obsługą ARMv7 lub x86 Intel Atom.
6. Ochrona antywirusowa:
6.1. Ochrona plików w czasie rzeczywistym.
6.2. Ochrona przed atakami typu „phishing”.
6.3. Skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
6.4. Aplikacja musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
6.5. Ochrona proaktywna wykrywająca nieznane zagrożenia.
6.6. W przypadku wykrycia zagrożenia użytkownik ma otrzymać odpowiednie powiadomienie.
6.7. Aplikacja musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia.
6.8. Aplikacja musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
7. Skanowanie na żądanie:
7.1. Aplikacja ma mieć możliwość skanowania zainstalowanych aplikacji.
7.2. Informacje o skanowaniu mają być przechowywane w plikach dziennika.
7.3. Użytkownik ma mieć możliwość wyboru akcji jaka ma być podjęta w przypadku wykrycia zagrożenia, co najmniej: poddania kwarantannie, usunięcia oraz zignorowania.
7.4. Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia.
8. Ochrona przed kradzieżą:
8.1. Administrator ma mieć możliwość skonfigurowania zaufanej karty SIM.
8.2. Dodanie zaufanej karty SIM ma się odbyć w oparciu o kartę wprowadzoną w danym urządzeniu lub w oparciu o wprowadzony ręcznie numer IMSI karty SIM.
8.3. W przypadku kradzieży urządzenia, Administrator ma mieć możliwość wysłania na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
8.3.1. usunięcie zawartości urządzenia,
8.3.2. przywrócenie urządzenie do ustawień fabrycznych,
8.3.3. zablokowania urządzenia,
8.3.4. uruchomienie sygnału dźwiękowego,

8.3.5. lokalizację GPS.

9. Polityka ustawień:
   9.1. Administrator musi mieć wgląd w podstawowe ustawienia urządzenia, w tym co najmniej:
      9.1.1. połączenie Wi-Fi,
      9.1.2. GPS,
      9.1.3. usługi lokalizacyjne,
      9.1.4. pamięć,
      9.1.5. roaming danych,
      9.1.6. roaming połączeń,
      9.1.7. nieznane źródła,
      9.1.8. tryb debugowania,
      9.1.9. komunikacja NFC,
      9.1.10. szyfrowanie pamięci masowej,
      9.1.11. urządzenie zrootowane.
10. Kontrola aplikacji:
   10.1. Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji.
   10.2. Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji.
   10.3. Blokowanie aplikacji musi być możliwe w oparciu o:
      10.3.1. nazwę aplikacji,
      10.3.2. nazwę pakietu,
      10.3.3. kategorię sklepu Google Play,
      10.3.4. uprawnienia aplikacji,
      10.3.5. pochodzenie aplikacji z nieznanego źródła.
11. Zabezpieczenia urządzenia:
   11.1. W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej:
      11.1.1. minimalny poziom zabezpieczeń i złożoność blokady ekranu,
      11.1.2. maksymalną dopuszczaną liczbę błędnych prób odblokowania,
      11.1.3. odstęp czasu, po którym użytkownik musi zmienić kod odblokowujący urządzenie,
      11.1.4. czas, po którym automatycznie nastąpi blokada ekranu,
      11.1.5. ograniczenie dostępu do kamery wbudowanej w urządzenie.
12. Aktualizacje sygnatur:
   12.1. Wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.
   12.2. Aplikacja ma mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje sygnatur co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin.
   12.3. Aplikacja ma posiadać możliwość zabezpieczenia hasłem konkretnych modułów, w tym co najmniej: dostępu do ustawień ochrony antywirusowej, ochrony przed kradzieżą, deinstalacją.
13. Konfiguracja i zdalne zarządzanie:
   13.1. Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne.
   13.2. Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją.
   13.3. Administrator musi mieć możliwość zdalnego wysyłania komunikatów

z poziomu konsoli centralnego zarządzania do użytkowników urządzeń mobilnych.
13.4. Przesłana wiadomość musi wyświetlać się w formie wyskakującego okna.
13.5. Wdrożenie urządzenia mobilnego z poziomu konsoli zarządzającej musi się odbyć co najmniej na jeden z trzech możliwych sposobów:
13.5.1. za pomocą kodu QR,
13.5.2. za pomocą unikatowego łącza,
13.5.3. za pomocą wiadomości e-mail,
14. W ramach aktywacji za pomocą kodu QR musi istnieć możliwość aktywacji w trybie właściciela urządzenia (Android Enterprise Device Owner).
15. Stacje robocze Linux
15.1. Wymagania sprzętowe:
15.1.1. Procesor 32-bit / 64-bit AMD®, Intel®,
15.1.2. RAM 512MB wolnej pamięci RAM,
15.1.3. HDD 100MB wolnej przestrzeni.
16. Pełne wsparcie dla dystrybucji opartych na systemach Debian i RedHat (Ubuntu, OpenSuse, Fedora, Mandriva itp). Dodatkowe wymagania systemowe :
16.1. Kernel 2.6.x,
16.2. Biblioteki GNU C w wersji 2.3 lub nowszej,
16.3. GTK+ 2.6 lub nowszej,
16.4. Zalecana kompatybilność z LSB 3.1.
17. Wsparcie dla dystrybucji 32- i 64-bitowych.
18. Wersja programu dostępna zarówno w języku polskim jak i angielskim.
19. Pomoc w programie (help) w języku polskim.
20. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
21. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
22. Wbudowana technologia do ochrony przed rootkitami.
23. Skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
24. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
25. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności).
26. Skanowanie plików spakowanych i skompresowanych.
27. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
28. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
29. 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.
30. 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.
31. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
32. Możliwość wykonania skanowania z poziomu menu kontekstowego.
33. Aktualizacje modułów analizy heurystycznej.
34. 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 mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
35. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
36. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
37. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
38. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: stacji dyskietek, napędów CD/DVD oraz portów USB.
39. Funkcja blokowania nośników wymiennych ma umożliwiać wyłączenie dostępu do nośników : Napęd CD-Rom, Dyskietka, Firewire, USB, HotPlug, Inne.
40. Automatyczna, inkrementacyjna aktualizacja baz sygnatur wirusów i innych zagrożeń.
41. Aktualizacja systemu antywirusowego ma być dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
42. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
43. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po wystąpieniu zdarzenia).
44. Program umożliwia automatyczne sprawdzanie plików wykonywanych podczas uruchamiania systemu operacyjnego.
45. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
46. Program ma umożliwiać importowanie oraz eksportowanie ustawień. Z poziomu interfejsu graficznego użytkownik ma mieć możliwość przywrócenia wartości domyślnych wszystkich ustawień.
47. Program ma posiadać dwie wersje interfejsu (standardowy – z ukrytą częścią ustawień oraz zaawansowany – z widocznymi wszystkimi opcjami).
48. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz sygnatur wirusów i samego oprogramowania oraz dokonanym skanowaniem komputera.
49. Program ma umożliwiać w ramach zdefiniowanej grupy „Uprzywilejowani użytkownicy" na modyfikację konfiguracji programu.
50. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
51. Ochrona serwera - Linux
52. Architektura rozwiązania
    - 52.1. Skaner antywirusowy i antyspyware.
    - 52.2. Skanowanie plików, plików spakowanych i archiwów samorozpakowujących.
    - 52.3. 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.
    - 52.4. 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.

52.5. 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.

52.6. Oprogramowanie antywirusowe musi wspierać wieloprocesorową i wielordzeniową architekturę, w celu zapewnienia maksymalnego zwiększenia wydajności.

52.7. 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.

52.8. 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.

52.9. Ochrona systemu plików w czasie rzeczywistym musi być zapewniona nieprzerwanie od uruchomienia produktu i obejmuje skanowanie zarówno dysków lokalnych jak i zmapowanych dysków sieciowych.

52.10. Silnik skanujący musi działać wyłącznie z wykorzystaniem 64-bitowej architektury.

52.11. Oprogramowanie musi być w pełni zgodne z modułem SELinux, pracującym zarówno w trybie „Permissive" jak i „Enforcing".

52.12. 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.

52.13. 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.

52.14. Skaner systemu plików w czasie rzeczywistym musi działać dla operacji obsługi plików, dla co najmniej takich operacji jak: dostęp do pliku, utworzenie (zapisanie) pliku.

52.15. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

52.16. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.

52.17. 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.

52.18. Rozwiązanie musi wspierać system plików zamontowany z flagą „noexec".

52.19. Oprogramowanie musi pozwalać na uruchamianie zadań skanowania działających „w tle", z możliwością ustawienia dla nich niskiego priorytetu.

52.20. Zadania skanowania nie mogą zmieniać znacznika dostępu do plików.

53. Interfejs graficzny

53.1. Produkt musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.

53.2. Lokalna konsola administracyjna musi działać w oparciu o dynamicznie

generowaną zawartość tworzoną z wykorzystaniem następujących technologii: React/Node.js, HTML5.

53.3. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.

53.4. Lokalna konsola administracyjna musi zapewniać bezpieczne połączenie działające w oparciu o protokół HTTPS.

53.5. Lokalna konsola administracyjna musi umożliwiać uruchomienie jej, na wskazanym porcie TCP.

53.6. Logowanie do lokalnej konsoli administracyjnej musi być realizowane, poprzez podanie danych w postaci nazwy użytkownika i zdefiniowanego dla niego hasła.

53.7. Administrator systemu musi mieć możliwość zdefiniowania dodatkowych kont użytkowników, w lokalnej konsoli administracyjnej.

53.8. Lokalna konsola administracyjna musi zapewniać funkcjonalność zweryfikowania stanu licencji i informacji na jej temat.

53.9. Z poziomu lokalnej konsoli administracyjnej musi być możliwość zarządzania, wbudowanym modułem menadżera kwarantanny.

53.10. Lokalna konsola administracyjna musi zapewniać możliwość przełączenia wersji językowej konsoli, na etapie logowania. Lokalna konsola administracyjna musi posiadać interfejs, co najmniej języku: polskim, angielskim, niemieckim, francuskim, hiszpańskim, japońskim.

54. Skanowanie sieciowych systemów plików

54.1. Oprogramowanie antywirusowe musi pozwalać na skanowanie plików składowanych i obsługiwanych przez zewnętrzne rozwiązania obsługi danych typu NAS / SAN.

54.2. 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.

54.3. Rozwiązanie musi umożliwiać zmianę domyślnego portu protokołu ICAP.

54.4. Oprogramowanie antywirusowe, do celów skanowania plików na rozwiązaniach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.

55. Instalacja

55.1. Oprogramowanie musi wspierać mechanizm instalacji zdalnej, realizowanej przez narzędzia do orkiestracji systemami operacyjnymi. Wspieranymi narzędziami muszą być co najmniej: Puppet, Chef, Ansible.

55.2. Oprogramowanie antywirusowe musi być wyposażone w mechanizm automatycznej aktualizacji komponentów programu.

55.3. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.

55.4. 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

56. Licencjonowanie

56.1. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

56.2. 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.

57. Ochrona serwera Windows

57.1. 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).

57.2. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.

57.3. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

57.4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

57.5. Wbudowana technologia do ochrony przed rootkitami i exploitami.

57.6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

57.7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.

57.8. 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).

57.9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.

57.10. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.

57.11. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.

57.12. Możliwość skanowania dysków sieciowych i dysków przenośnych.

57.13. Skanowanie plików spakowanych i skompresowanych.

57.14. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

57.15. Aplikacja powinna wspierać mechanizm klastrowania.

57.16. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).

57.17. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

57.17.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

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

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

57.17.4. 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,

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

57.18. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.

57.19. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.

57.20. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
57.21. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
57.22. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
57.23. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na serwerze.
57.24. 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.
57.25. 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.
57.26. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
57.27. 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.
57.28. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
57.29. Program musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
57.30. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
57.31. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
57.32. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
57.33. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
57.34. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
57.35. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
57.36. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
57.37. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
57.38. 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.
57.39. 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.

57.40. 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.

57.41. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu email użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.

57.42. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.

57.43. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.

57.44. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.

57.45. 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.

57.46. 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.

57.47. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.

57.48. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i wyświetlić listę niezainstalowanych aktualizacji.

57.49. 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.

57.50. 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.

57.51. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.

57.52. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.

57.53. 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.

57.54. 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.

57.55. 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.

57.56. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.

57.57. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
57.58. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
57.59. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
57.60. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
57.61. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
57.62. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
57.63. Aplikacja musi wspierać skanowanie magazynu Hyper-V.
57.64. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów.
57.65. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji modułów i samego oprogramowania.
57.66. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
57.67. Program musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”.
57.68. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
57.69. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.
57.70. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
57.71. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
57.72. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.
57.73. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
57.74. 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.
57.75. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
57.76. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
57.77. Program musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

58. Ochrona bezagentowa maszyn wirtualnych

58.1. Rozwiązanie zapewnia bezagentową ochronę maszyn wirtualnych w wersjach systemu gościa: Windows XP SP3 x32, Windows Server 2003 SP2 x32, Windows Vista x32, Windows 7 x32/x64, Windows Server 2008 x32/x64, Windows Server 2008 R2 x32/x64, Windows Server 2012, Windows Server 2012 R2, Windows 8 x32/x64, Windows 8.1 x32/x64, Windows 10 x32/x64.
58.2. Rozwiązanie umożliwia ochronę nieograniczonej liczby fizycznych serwerów ESXi w roli hypervisora.
58.3. Ochrona środowiska wirtualnego zarządzana z jednej, centralnej konsoli administracyjnej, niezależnie od ilości chronionych hostów wirtualnych i serwerów w roli hypervisora.
58.4. W ramach całego chronionego środowiska wirtualnego wymagane jest uruchomienie tylko jednej maszyny wirtualnej.
58.5. Wyłączenie serwera z centralną konsolą administracyjną, nie wpływa na działanie mechanizmów ochrony maszyn wirtualnych (silniki antywirusowe pozostają aktywne).
58.6. Wdrożenie rozwiązania do ochrony środowiska wirtualnego jest przeprowadzane w sposób zautomatyzowany z wykorzystaniem dedykowanego narzędzia, niezależnie od liczby systemów wirtualnych.
58.7. Wdrożenie rozwiązania nie wymaga instalowania jakichkolwiek zewnętrznych składników czy plug-inów na natywnym systemie operacyjnym nadzorcy wirtualnego (hypervisora).
58.8. Rozwiązanie funkcjonuje bez konieczności instalowania jakiegokolwiek własnego agenta na systemach operacyjnych wirtualnych hostów.
58.9. Rozwiązanie wspiera środowisko VMware vSphere 5.5 U2 lub nowsze wraz z VMware NSX 6.2.4
58.10. Ochrona środowiska wirtualnego realizowana jest z wykorzystaniem VMWare EPSec Library.
58.11. Ochrona środowiska wirtualnego sprzedawana wraz z dwoma możliwymi do wyboru modelami licencjonowania: liczba chronionych hypervisorów lub liczba procesorów serwera hypervisora.
58.12. Ochrona środowiska wirtualnego dostarczana jest wyłącznie w postaci obrazów maszyn wirtualnych (OVA- Open Virtual Appliance).
58.13. Rozwiązanie wspiera technologię Vmware vMotion Migration - host wirtualny jest chroniony w trybie ciągłym niezależnie od tego na jakim serwerze fizycznym znajduje się w ramach jednego środowiska vSphere.
58.14. System ochrony maszyny wirtualnej działa w trybie aktywnym (ochrona systemu w czasie rzeczywistym) jak i pasywnym (realizowanie skanowania na żądanie).
58.15. Mechanizmy ochrony wirtualnych serwerów i desktopów realizowane są bezagentowo przez silnik producenta uruchomiony na dedykowanym wirtualnym appliance.
58.16. Aktualizacje baz sygnatur antywirusowych pobierane są wyłączenie przez silnik producenta uruchomiony na dedykowanym wirtualnym appliance.
58.17. Silnik antywirusowy wykorzystuje mechanizmy weryfikowania w chmurze producenta plików i procesów w czasie rzeczywistym - musi istnieć możliwość zdecydowania, czy funkcja ta ma być włączona, czy też nie.
58.18. Do mechanizmów ochrony maszyn wirtualnych rozwiązanie wykorzystuje wyłączenie sieć zdefiniowaną programowo (SDN).
58.19. Wyłączenie adaptera sieci TCP/IP na maszynie wirtualnej w żaden sposób nie wpływa na jej ochronę przez silnik antywirusowy.

58.20. Administrator ma możliwość zdefiniowania aktywacji ochrony bezagentowej tylko na wybranych maszynach wirtualnych.

59. Administracja zdalna

59.1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2008 R2, 2012, 2016, 2019 oraz systemach Linux.

59.2. Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD.

59.3. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL

59.4. Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik.

59.5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.

59.6. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.

59.7. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.

59.8. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy.

59.9. Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6.

59.10. Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs.

59.11. Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji.

59.12. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.

59.13. Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.

59.14. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.

59.15. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.

59.16. Serwer administracyjny musi posiadać wsparcie dla „VDI" oraz „Golden Master Image".

59.17. Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów.

59.18. Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy.

59.19. Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.

59.20. Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.

59.21. Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS.

59.22. Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP.

59.23. Serwer administracyjny musi posiadać możliwość konfiguracji polityk zabezpieczeń takich jak: ograniczenia funkcji urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11.

59.24. Serwer administracyjny musi posiadać możliwość lokalizacji urządzeń

mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap.

59.25. Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych.

59.26. Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów.

59.27. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.

59.28. Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi, host agenta wirtualnego.

59.29. Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android.

59.30. Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS.

59.31. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.

59.32. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.

59.33. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.

59.34. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania.

59.35. Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.

59.36. Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny.

59.37. W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play.

59.38. Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.

59.39. Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS.

59.40. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.

59.41. Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi.
59.42. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
59.43. Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
59.44. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
59.45. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej.
59.46. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany.
59.47. Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
59.48. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
59.49. Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych.
59.50. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
59.51. Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.
59.52. Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
59.53. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
59.54. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
59.55. Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.
59.56. Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.
59.57. Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta.
59.58. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej.

59.59. Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.
59.60. Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce.
59.61. Serwer administracyjny musi posiadać minimum 170 szablonów raportów, przygotowanych przez producenta.
59.62. Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.
59.63. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.
59.64. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.
59.65. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.
59.66. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
59.67. Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny.
59.68. Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF, CSV oraz PS.
59.69. Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
59.70. Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów.
59.71. Powiadomienia mailowe mają być wysyłane w formacie HTML.
59.72. Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń.
59.73. Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
59.74. Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
59.75. Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji.
59.76. Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami.
59.77. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych.
59.78. W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu.
59.79. Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji

produktu, na który jest licencja oraz jej właściciela.

59.80. Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan.

59.81. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

59.82. Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli.

59.83. W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych.

59.84. Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta.

59.85. Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli.

59.86. Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania.

59.87. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie.

59.88. Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.

59.89. Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, grupy, zadania, komputery oraz szablony grupy dynamicznych.

59.90. Konsola administracyjna musi mieć możliwość zarządzania rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta.

59.91. Konsola administracyjna musi pozwalać na utworzenie wykluczeni globalnych, bez konieczności przypisywania ich do konkretnych polityk.