Załącznik nr 1 do SWZ

FU.271.5.2022
„Zakup sprzętu komputerowego i oprogramowania w ramach grantu PPGR i Cyfrowa Gmina”

OPIS PRZEDMIOTU ZAMÓWIENIA

Cześć 1 – serwer sieciowy wraz z oprogramowaniem

a) Opis serwera sieciowego

Parametry techniczne	Wymagane minimum
Obudowa	-obudowa typu Rack; -wysokość nie więcej niż 1U; -dostarczona wraz z szynami montażowymi do szafy rack umożliwiającymi pełne wysunięcie z szafy;
Procesor	-zainstalowany procesor 4-rdzeniowy taktowany podstawowym zegarem o częstotliwości 4 GHz, osiągający w testach wydajności CPU Benchmarks (https://www.cpubenchmark.net/cpu_list.php) minimum 9655 pkt.
Płyta główna	-dedykowana serwerowa, wyprodukowana i zaprojektowana przez producenta serwera; -minimum 3 sloty PCI Express generacji 3 w tym minimum 2 sloty o prędkości x8; -minimum 4 gniazda pamięci RAM DDR4 obsługujące pamięci o taktowaniu 2666Mhz; -2 gniazda dla dysków M.2 nie zajmujące wnęk hotplug dla dysków twardych (możliwość instalacji dysku M.2 np. na potrzeby bootowania);
Pamięć RAM	-nie mniej niż 16GB RAM DDR4-2666MHz ; -zabezpieczenie pamięci mechanizmem ECC; -możliwość rozbudowy do minimum 128 GB RAM;
HDD	-dyski hotplug; -możliwość instalacji 4 dysków 2,5” hotplug SATA/SAS/SSD; -fabrycznie zainstalowane trzy dyski typu hotplug 2,5” 960GB SATA SSD, DWPD min. 3; -możliwość rozbudowy obudowy serwera do 8 zatok na dyski 2,5”;
Kontroler dysków	-zainstalowany kontroler SAS 3.0 RAID 0,1,5,6,10,50,60, 2GB pamięci podręcznej cache;
Napęd optyczny	możliwość instalacji wewnętrznego napędu DVD +/- RW;
Karta graficzna	zintegrowana z płytą główną , minimum 32MB pamięci RAM, wsparcie dla rozdzielczości minimum 1280x1024;
Karty sieciowe	-2x LAN 1Gbit/s ze wsparciem iSCSI, RJ-45 ze wsparciem akceleracji TCP/IP, iSCSI, PXE-Boot i Wake-on-LAN; -zintegrowana, dedykowana karta LAN 1Gbit/s do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym serwera
Zasilanie i chłodzenie	-dwa, nadmiarowe zasilacze hotplug o mocy maksymalnej nie więcej niż 460W, o maksymalnej sprawności minimum 94% (potwierdzenie na podstawie dokumentacji technicznej producenta serwera) -nadmiarowy układ chłodzenia typu hot plug (redundancja minimum typu N+1)
Zarządzanie zdalne, inwentaryzacja	1. -umieszczona z przodu chowana karta identyfikacyjna serwera zawierająca nazwę serwera, numer handlowy, numer seryjny, adresy MAC kart sieciowych

Parametry techniczne	Wymagane minimum
	2. -zintegrowany trwale z płytą główną kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający: 3. zdalne uruchomienie, wyłączenie i restart serwera, pełne zarządzanie sprzętowe: monitorowanie pracy kluczowych układów, wentylatorów, zasilaczy, napędów, temperatur, itp., logowanie błędów w zakresie ustalonym przez administratora 4. dostęp do interfejsu karty zarządzającej za pomocą przeglądarki MS Internet Explorer lub Mozilla Firefox bez konieczności instalowania jakiegokolwiek software specyficznego dla producenta sprzętu 5. przekierowanie konsoli graficznej na poziomie sprzętowym oraz montowanie zdalnych napędów (CD, DVD, klucz USB) i ich obrazów na poziomie sprzętowym (cyfrowy KVM) 6. monitorowanie zużycia energii serwera w trybie rzeczywistym i wizualizacja raportów w postaci wykresów graficznych, 7. dedykowana karta LAN 1 Gb/s do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym serwera. 8. możliwość konfiguracji 16 niezależnych kont administracyjnych (dostępowych) do karty zarządzającej, logowanie aktywności użytkowników, wsparcie dla integracji z Active Directory i LDAP 9. wsparcie dla aktualizacji firmware karty zarządzającej online, bez konieczności restartu serwera
Porty	-minimum 6 portów USB w tym minimum 2 porty USB 3.1 z przodu obudowy oraz minimum 2 porty USB 3.1 z tyłu obudowy; -minimum trzy porty RJ45; -nie dopuszcza się stosowania przejściówek, adapterów oraz rozgałęziaczy i przedłużaczy;
Oprogramowanie	oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).
Wsparcie dla systemów operacyjnych	wymagana kompatybilność i wsparcie serwera dla następujących systemów operacyjnych: Microsoft Windows Server 2019;
Inne	2 kable zasilające C13-C14 o dł. 4m;
Gwarancja	5 lat gwarancji producenta, z czasem reakcji w miejscu instalacji sprzętu najpóźniej w następnym dniu roboczym od zgłoszenia usterki; -dostępność części zamiennych co najmniej 5 lat po zakończeniu produkcji serwera (potwierdzone przez producenta)
Inne	-Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane (wymagane oświadczenie producenta dołączone do oferty) oraz muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne; -Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce - Wymagane oświadczenie producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg; -Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu; -Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca

Parametry techniczne	Wymagane minimum
	po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; -Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

b) Opis oprogramowania sieciowego

Oprogramowanie musi zostać dostarczone do serwera fizycznego wyposażonego w jeden procesor 4-rdzeniowy. Dodatkowo wymaga się dostarczenia sumarycznie 20 licencji dostępowych na użytkownika współpracujących z dostarczanym systemem operacyjnym.

Licencja na serwerowy system operacyjny musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego.
Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.
1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
   a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
   b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
   c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
   d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
   a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc,

komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
a. Login i hasło,
b. Karty z certyfikatami (smartcard),
c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
a. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
b. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika na przykład typu certyfikatu użytego do logowania,
c. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
d. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
c) Zdalna dystrybucja oprogramowania na stacje robocze.
d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
a. Dystrybucję certyfikatów poprzez http
b. Konsolidację CA dla wielu lasów domeny,
c. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
d. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
e. Szyfrowanie plików i folderów.
f. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
e) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
f) Serwis udostępniania stron WWW.
g) Wsparcie dla protokołu IP w wersji 6 (IPv6),
h) Wsparcie dla algorytmów Suite B (RFC 4869),
i) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
j) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:

a. - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
b. - Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
c. - Obsługi 4-KB sektorów dysków
d. - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
e. - Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
f. - Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

c) Dodatkowe oprogramowanie

1. Microsoft SQL Server 2019 Standard Edition
2. Microsoft SQL Server 2019 18 User CAL

Cześć 2 – Diagnoza cyberbezpieczeństwa

1. Diagnoza cyberbezpieczeństwa w ramach projektu „Cyfrowa Gmina" zgodnie z zakresem oraz formularzem stanowiącym obowiązujący na dzień wykonywania audytu załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina zakończonego raportem, opublikowanego na stronie Centrum Projektów Polska Cyfrowa pod adresem https://www.gov.pl/web/cppc/cyfrowa-gmina.

Cześć 3 – Rozbudowa zabezpieczeń logicznych (firewall, systemy IDS, IPS)

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
System musi wspierać IPv4 oraz IPv6 w zakresie:

1. Firewall.
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie

1. System realizujący funkcję Firewall musi dysponować minimum:
   a) 10 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

Funkcje Systemu Bezpieczeństwa

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    a) Translację jeden do jeden oraz jeden do wielu.
    b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
    a) Amazon Web Services (AWS).
    b) Microsoft Azure
    c) Google Cloud Platform (GCP).
    d) OpenStack.
    e) VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
    a) Wsparcie dla IKE v1 oraz v2.
    b) Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
    c) Obsługa protokołu Diffie-Hellman grup 19 i 20.
    d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
    e) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
    f) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
    g) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
    h) Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
    i) Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
    a) Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
    b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
    c) Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
    a) Routingu statycznego.
    b) Policy Based Routingu.

c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   c) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.
3. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
4. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
5. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

1. ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

1. Kontrola Aplikacji, IPS, Antywirus, Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Rozszerzone wsparcie serwisowe AHB/SOS

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7

Oferent winien przedłożyć dokumenty:

a) Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
b) Certyfikat ISO 9001 podmiotu serwisującego.

Cześć 4 – Licencja programu antywirusowego – 30 szt. na 36 miesięcy

Ochrona stacji roboczych - Windows

1. Rozwiązanie musi wspierać systemy operacyjne Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11.
2. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.
3. Rozwiązanie musi wspierać architekturę ARM64.
4. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
5. Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
6. Pomoc w rozwiązaniu (help) i dokumentacja rozwiązania dostępna co najmniej w języku polskim oraz angielskim.
7. Skuteczność rozwiązania potwierdzona nagrodami VB100 i AV-comparatives.

Ochrona przed spamem

1. Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
2. Rozwiązanie musi umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
3. Rozwiązanie musi umożliwiać automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
4. Rozwiązanie musi posiadać możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
5. Rozwiązanie musi posiadać możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
6. Rozwiązanie musi posiadać możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
7. Rozwiązanie musi możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
8. Rozwiązanie musi domyślnie współpracować z folderem „Wiadomości-śmieci”, dostępnym w programie Microsoft Outlook.
9. Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana”
10. Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana”.
11. Rozwiązanie musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

Zapora osobista (personal firewall)

1. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
   a) tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
   b) tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
   c) tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na

połączenia skonfigurowane przez administratora,

d) tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

2. Rozwiązanie musi oceniać reguły zapory systemu Windows.
3. Rozwiązanie musi posiadać możliwość tworzenia list sieci zaufanych.
4. Rozwiązanie musi posiadać możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
5. Rozwiązanie musi posiadać możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego.
6. Rozwiązanie musi posiadać możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
7. Rozwiązanie musi posiadać możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
8. Rozwiązanie musi posiadać możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet.
9. Rozwiązanie musi wykrywać modyfikację w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu.
10. Rozwiązanie musi posiadać możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
11. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
12. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
13. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie.
14. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6.
15. Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci.
16. Rozwiązanie musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów:
    a) z aplikacją lokalną, którą administrator wskazuje z listy,
    b) z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP.

Kontrola dostępu do stron internetowych

1. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
2. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory.
3. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
4. Podstawowe kategorie, w jakie rozwiązanie musi być wyposażone to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
5. Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych.
6. Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być automatycznie aktualizowana przez producenta.

7. Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.
8. Rozwiązanie musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj.
9. Rozwiązanie musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej.

Bezpieczna przeglądarka

1. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
2. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
3. Użytkownik w momencie wejścia na stronę, która znajduje się na liście chronionych witryn, musi automatycznie zostać przekierowany do okna bezpiecznej przeglądarki.
4. Administrator musi mieć możliwość konfiguracji listy chronionych witryn, przez bezpieczną przeglądarkę.
5. Administrator musi mieć możliwość konfiguracji, aby użytkownik przy próbie dostępu do strony bankowości elektronicznej, automatycznie został przekierowany do okna bezpiecznej przeglądarki.
6. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

Ochrona antywirusowa i antyspyware

1. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
3. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
4. Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje.
5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
6. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.
7. Rozwiązanie musi 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.
8. Rozwiązanie musi posiadać 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).
9. Rozwiązanie musi posiadać opcję skanowania „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
11. Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych.
12. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.
13. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

14. Administrator musi mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
15. Rozwiązanie musi posiadać możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
16. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.
17. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
18. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
19. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
20. Rozwiązanie musi posiadać 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.
21. Rozwiązanie musi posiadać wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
22. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
23. Rozwiązanie musi umożliwiać 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).
24. Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
25. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
26. Rozwiązanie musi umożliwiać skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
27. Rozwiązanie musi posiadać możliwość blokowania możliwości przeglądania wybranych stron internetowych. Rozwiązanie musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
28. Rozwiązanie musi posiadać możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
29. Rozwiązanie musi automatycznie integrować się z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
30. Rozwiązanie musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
31. Rozwiązanie musi zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
32. Rozwiązanie musi posiadać możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
33. Administrator ma mieć możliwość zdefiniowania portów TCP, na których rozwiązanie będzie realizowało proces skanowania ruchu szyfrowanego.
34. Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
35. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
36. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego

reputacji bezpośrednio z poziomu menu kontekstowego.

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.
38. Rozwiązanie musi posiadać dwa wbudowane 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.
39. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
40. Do wysłania próbki zagrożenia do laboratorium producenta, rozwiązanie nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
41. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
42. Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
43. Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
44. Rozwiązanie musi posiadać możliwość zabezpieczenia przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji rozwiązanie musi pytać o hasło.
45. Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo.
46. Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
47. Rozwiązanie musi 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.
48. Po instalacji rozwiązania, 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.
49. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
50. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
51. Rozwiązanie musi posiadać 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.
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.
53. Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
54. Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
55. Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
56. W momencie podłączenia zewnętrznego nośnika, rozwiązanie musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
57. Administrator ma posiadać możliwość takiej konfiguracji rozwiązania, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.

58. Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS).
59. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    a) tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    b) tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    c) tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    d) tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    e) tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
60. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
61. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
62. Rozwiązanie musi posiadać zaawansowany skaner pamięci.
63. Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
64. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, 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.
65. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
66. Rozwiązanie musi posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
67. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
68. Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
69. Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego rozwiązanie zgłosi posiadanie nieaktualnego silnika detekcji.
70. Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
71. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
72. Rozwiązanie musi być wyposażone w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
73. Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
74. Rozwiązanie musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
75. W momencie wykrycia trybu pełnoekranowego, rozwiązanie ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań rozwiązania.
76. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
77. Rozwiązanie musi być wyposażone w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń.

78. Rozwiązanie musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
79. Rozwiązanie 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.
80. Rozwiązanie musi mieć możliwość podejrzenia informacji o licencji, która znajduje się w programie.
81. W trakcie instalacji rozwiązanie ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM.
82. W rozwiązaniu musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.
83. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień rozwiązania na stacji końcowej.
84. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.
85. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.
86. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
87. Rozwiązanie musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.
88. Rozwiązanie musi posiadać 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.
89. Rozwiązanie musi posiadać możliwość definiowana stanów rozwiązania, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
90. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
91. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
92. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
93. Rozwiązanie musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
94. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.
95. Rozwiązanie musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”.
96. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
97. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
98. Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
99. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
100. Rozwiązanie musi posiadać ochronę przed dołączeniem komputera do sieci botnet.
101. Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego dostania się do stacji roboczej za pomocą protokołu RDP i SMB.
102. Rozwiązanie musi posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
103. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego

przez producenta programu.

Cześć 5 – Oprogramowanie do sporządzania backupu i kopii zapasowych

Ogólne:

1. Oprogramowanie może być instalowane w dwóch scenariuszach:
    a) Cloud(Software as Service),
    b) On-premise.
2. Istnieje możliwość migracji w obie strony pomiędzy środowiskiem on-premise oraz cloud.
3. Interfejs systemu dostępny jest co najmniej w języku polskim,
4. Oprogramowanie nie preferuje platformy sprzętowej, nie jest profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych,
5. Oprogramowanie może być uruchomione w kontenerze docker,
6. Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:
    a) Debian: 9+
    b) Ubuntu: 16.04+
    c) Fedora: 29+
    d) centOS: 7+
    e) RHEL: 6+
    f) openSUSE: 15+
    g) SUSE Enterprise Linux (SLES): 12 SP2+
    h) Windows Client: 7, 8.1, 10 (1607+)
    i) Windows Server: 2008 R2+,
7. System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji,
8. Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii(awaria jednego z komponentów nie spowoduje przestoju),

Zarządzanie:

1. Zarządzanie całością działania systemu (backup, przywracanie)z poziomu jednej konsoli webowej,
2. Zarządzanie całym systemem poprzez dashboardy,
3. Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego,
4. System posiada wbudowane predefiniowane zadania backupowe,
5. System umożliwia tworzenie zadań backupowych w oparciu o kalendarz.
6. Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem,
7. Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem,
8. Monitorowanie postępu działania zadania,
9. Posiada system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach:
    a) Zadanie zostało zakończone pomyślnie,
    b) Zadanie zostało zakończone z ostrzeżeniami,
    c) Zadanie zostało zakończone z błędem,
    d) Zadanie zostało anulowane,

e) Zadanie nie zostało uruchomione.

10. System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego.
11. Możliwość zdefiniowania okna backupowego dla każdego z zadań,
12. Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów,
13. System pozwala na klonowanie planów kopii zapasowych,
14. System umożliwia reset hasła administratora w przypadku jego utraty,
15. Oprogramowanie umożliwia definiowanie retencji według schematów:
    a) GFS(Grandfather-Father-Son),
    b) FIFO(First-In, First-Out).
16. Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami,
17. Konta użytkowników mogą być tworzone poprzez import pliku CSV,
18. Oprogramowanie umożliwia tworzenie grup urządzeń,
19. Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
20. System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.:
    a. System Administrator,
    b. Backup operator,
    c. Restore operator,
    d. Viewer.

Składowanie danych:

1. Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie,
2. System umożliwia składowanie danych:
    a) Lokalnie:
        i. Zasób SMB,
        ii. Zasób NFS,
        iii. Zasób ISCSI,
        iv. Zasób S3,
        v. Katalog zabezpieczonego urządzenia.
    b) W chmurze:
        i. Amazon Web Service,
        ii. Magazyn zgodny z S3,
        iii. Dostarczanej przez producenta.
3. System pozwala na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji,
4. System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.

Odtwarzanie:

1. Odtwarzanie granularne:
    a) Pojedynczych plików z kopii obrazu dysku,

   b) Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365,
2. Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów:
   a) Windows: 7+,
   b) Windows Server: 2008 R2+,
3. Odtwarzanie Bare metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
4. Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive'a,
5. Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V.
6. Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(VHD, VHDX, VMDK),
7. Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL),
8. Odtwarzanie zasobów plikowych z prawami dostępu,
9. Przywracanie plików pomiędzy systemami operacyjnymi(np. odtwarzanie danych plikowych Linux na systemie Windows),
10. Odtwarzanie danych według harmonogramu,
11. Przywracanie danych z określonego urządzenia/użytkownika,
12. Przywracanie kopii z wybranego magazynu.
13. Przywracanie danych Microsoft 365:
    a) do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku:
       i. pst,
       ii. mbox.
    b) do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji),
14. System posiada możliwość nieodwracalnego kasowania danych,Backup:
15. Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla:
    a) Systemów operacyjnych:
       i. Alpine 3.10+,
       ii. Debian: 9+,
       iii. Ubuntu: 16.04+,
       iv. Fedora: 29+,
       v. centOS: 7+,
       vi. RHEL: 6+,
       vii. openSUSE: 15+,
       viii. SUSE Enterprise Linux(SLES): 12 SP2+,
       ix. macOS: 10.13+,
       x. Windows: 7, 8.1, 10(1607+),
       xi. Windows Server: 2008 R2+,
    b) Środowisk wirtualnych:
       i. Hyper-V,
       ii. VMware: 6.7+.

16. Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla:
    a) Baz danych**:**
       i. Microsoft SQL,
       ii. MySQL,
       iii. PostgreSQL,

iv. Firebird,
v. Dowolnych innych przez podpięcie skryptów pre/post.

17. Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości:
    a) 128 bit,
    b) 192 bit,
    c) 256 bit.
18. Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów:
    a) ZStandard,
    b) LZ4.
19. Oprogramowanie umożliwia zarządzanie poziomem kompresji,
20. Wykonywanie kopii zapasowej otwartych plików(VSS),
21. System umożliwia uruchamianie skryptów przed i po backupie,
22. System umożliwia uruchamianie skryptów po wykonaniu migawki VSS,
23. System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów,
24. Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT,
25. Backup plikowy,
26. Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe,
27. Oprogramowanie umożliwia konsolidację wersji kopii zapasowych,
28. Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia,
29. Oprogramowanie pozwala na automatyczne uruchomienie kopii zapasowej podczas zamykania systemu operacyjnego.
30. Oprogramowanie pozwala na backup zaszyfrowanych partycji.

Licencjonowanie:

1. Sposób licencjonowania opiera się na:
    a) Ilości serwerów/endpointów- dla fizycznych urządzeń,
    b) Ilości fizycznych hostów - dla środowisk wirtualnych,
    c) Ilości repozytoriów - dla GIT.
2. Wsparcie techniczne:
3. Świadczone jest w języku polskim, bezpośrednio przez producenta,
4. Zapewnia dostęp do aktualizacji oprogramowania,
5. Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego
6. Licencja “wieczysta” na 1 maszynę fizyczną Microsoft Server z 12 miesięcznym supportem i 200GB przestrzeni w chmurze producenta oprogramowania

Cześć 6 – Laptop

Przedmiotem zamówienia jest dostawa komputerów przenośnych typu laptop w ilości 140 szt. w ramach Programu Cyfrowa Polska - Wsparcie dzieci z rodzin pegeerowskich w rozwoju cyfrowym – Granty PPGR, spełniających poniższe minimalne parametry i wymagania:

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputera przenośnego typu laptop
1.	Przeznaczenie	Komputer przenośny, który będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty
2.	Ekran	Ekran o przekątnej 15,6" o rozdzielczości FHD WLED (1920x1080) i jasności co najmniej 250 cd/m2, matryca matowa AG. Metalowe, wzmacniane zawiasy, kąt
3.	Procesor	Procesor klasy x86 ze zintegrowaną grafiką, zapewniający równoważną wydajność całego oferowanego laptopa (Rating) min 5000 pkt w teście Passmark CPU Mark wg wyników dostępnych na stronie: https://www.cpubenchmark.net/high_end_cpus.html
4.	Pamięć operacyjna RAM	Pamięć operacyjna: 8 GB z możliwością rozbudowy do min 32 GB, możliwość łatwej wymiany pamięci po odkręceniu pojedynczej śruby – bez konieczności demontowania laptopa. Przynajmniej jeden slot do rozbudowy pamięci RAM wolny.
5.	Pamięć masowa	Parametry pamięci masowej: dysk SSD M.2 NVMe o pojemności min. 256GB, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników.
6.	Karta graficzna	Wydajność grafiki: Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia do 1,5 GB pamięci. Obsługująca funkcje: DirectX 12, OpenGL 4.4, OpenCL 2.0, HLSL shader model 5.1
7.	Multimedia	Wydajność grafiki: Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia do 1,5 GB pamięci. Obsługująca funkcje: DirectX 12, OpenGL 4.4, OpenCL 2.0, HLSL shader model 5.1
8.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji
9.	Bateria i zasilanie	Min. 3-cell, 45 Wh, 4200 mAh Li-Ion. Czas pracy na baterii minimum 9 godzin według dokumentacji producenta laptopa. Możliwość łatwej wymiany baterii po odkręceniu jeden śruby. Zasilacz o mocy min. 65 W
10.	Klawiatura	Klawiatura wyspowa układ US –QWERTY odporna na zachlapanie, minimum 104 klawisze z wydzielonym blokiem klawiatury numerycznej. Touchpad wyposażony w dwa niezależne klawisze funkcyjne.
11.	System operacyjny	Licencja na system operacyjny Microsoft Windows 10 Professional 64-bit PL lub równoważny, zainstalowany niewymagający ręcznej aktywacji za pomocą telefonu lub Internetu. Opis równoważności znajduje się w załączniku nr 2 do Opisu przedmiotu zamówienia

12.	Porty i złącza	RJ-45 (nie dopuszcza się stosowania adapterów) Min. 1x UB 3.2 Gen2 typu USB-C z możliwością ładowania baterii laptopa oraz wyprowadzenia sygnału Display Port Min. 3x USB 3.2 Gen1 (1 z możliwością ładowania zewnętrznych urządzeń bezpośrednio z portu USB komputera nawet przy wyłączonym laptopie). HDMI w wersji co najmniej 1.4 Czytnik kart multimedialnych (SD, SDHC i SDXC) Audio: line-in/mikrofon (combo z Audio line-out) Audio: line-out/słuchawki (combo z Audio line-in) Karta sieciowa LAN 10/100/1000 Ethernet RJ 45 zintegrowana z płytą główną. Zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN obsługująca łącznie standardy IEEE 802.11ac z dwiema antenami. Zintegrowana karta WLAN musi zapewniać możliwość bezprzewodowego bezpośredniego (t.j. bez pośrednictwa punktu dostępowego lub sieci LAN) podłączenia do komputera dodatkowego monitora lub projektora wyposażonego w odpowiedni adapter (lub natywną obsługę takiej funkcji) z wykorzystaniem standardów IEEE 802.11n w pasmie 2,4 GHz lub 5GHz, w trybie ekranu systemowego – z obsługą wyświetlania w trybie klonowania ekranów, rozszerzonego desktopu oraz wyświetlania ekranu systemu jedynie na dodatkowym monitorze lub projektorze (Clone, Extended Desktop, Remote Only). Wymagana jest obsługa przesyłania dowolnej treści ekranu oraz dźwięku systemu operacyjnego z parametrami nie gorszymi niż: rozdzielczość 1920x1080 - 30 fps–kompresja H.264 dźwięk with AC3 5.1 Surround Audio obsługa szyfrowania WPS/WPA2/WEP Bluetooth co najmniej w standardzie v5.0,
13.	Bezpieczeństwo	Sprzętowe wsparcie technologii weryfikacji poprawności podpisu cyfrowego wykonywanego kodu oprogramowania, oraz sprzętowa izolacja segmentów pamięci dla kodu wykonywanego w trybie zaufanym wbudowane w procesor, kontroler pamięci, chipset I/O. Złącze typu Kensington Lock lub równoważne. Zintegrowany z płytą główną układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Co najmniej zgodne z TPM 2.0.
14.	Waga i wymiary	Waga nie więcej niż 2kg. Grubość laptopa po złożeniu powinna być mniejsza niż 24 mm.
15.	Obudowa	Szkielet i zawiasy notebooka wykonane z wzmacnianego metalu. Możliwość wymiany pamięci RAM, dysku i baterii przez użytkownika – bez konieczności wizyty serwisie i bez konieczności rozbierania laptopa – dostępna klapa serwisowa wymagająca odkręcenia jedynie pojedynczej śruby.

16.	Certyfikaty	Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 10 Pro 64-bit (załączyć wydruk ze strony Microsoft WHCL). Deklaracja zgodności CE lub równoważne (załączyć do oferty) Norma EnergyStar 8.0 - komputer musi znajdować się na liście zgodności dostępnej na stronie www.energystar.gov oraz http://www.eu-energystar.org lub inny dokument od producenta sprzętu potwierdzający spełnianie przez oferowany sprzęt wymaganej normy. Oferowane laptopy muszą być wykonane/wyprodukowane w systemie zapewnienia jakości ISO 9001 i ISO 14001 – certyfikat należy załączyć do oferty. Zamawiający wymaga dodatkowo: - dla potwierdzenia, że oferowany sprzęt odpowiada postawionym wymaganiom i był wykonany przez Wykonawcę (a jeżeli Wykonawca nie jest producentem to przez producenta) w systemie zapewnienia jakości wg normy ISO 9001 aby Wykonawca posiadał :Certyfikat ISO 9001 lub inne zaświadczenie/dokument wydane przez niezależny podmiot zajmujący się poświadczaniem zgodności działań wykonawcy z normami jakościowymi -odpowiadającej normie ISO 9001- (załączyć dokument potwierdzający spełnianie wymogu). - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia wykonawcy wystawionego na podstawie dokumentacji producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram
17.	BIOS	Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: Modelu komputera. Nr seryjnego komputera. Wersji BIOS (z datą). Modelu procesora wraz z informacjami o prędkości taktowania. Informacji o ilości i typie i obsadzeniu pamięci RAM. Informacji o dysku twardym: producent i model oraz pojemność Informacja o napędzie optycznym: producent i model MAC adresie zintegrowanej karty sieciowej Numerze matrycy Możliwość wyłączenia/włączenia bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych min.: - karty sieciowej RJ45, karty sieciowej WLAN z Bluetooth, kamery, portów USB, czytnika kart multimedialnych, kontrolera audio, głośników, mikrofonu, zintegrowanej, funkcjonalności TPM, portów USB Funkcja blokowania/odblokowania BOOT-owania z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z USB Możliwość włączenia/wyłączenia hasła dla dysku twardego, Możliwość - bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych - ustawienia hasła na poziomie użytkownika, administratora i dysku twardego

18.	Dodatkowe oprogramowanie	Oprogramowanie umożliwiające w pełni automatyczną instalację sterowników urządzeń opartą o automatyczną detekcję posiadanego sprzętu
19.	Gwarancja	Gwarancji jakości producenta: Na okres co najmniej 36 miesięcy - świadczonej w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta ,lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca. Czas reakcji na zgłoszoną reklamację gwarancyjną - do końca następnego dnia roboczego W przypadku naprawy trwającej dłużej niż 48 godzin, zamawiającemu musi zostać dostarczony komputer zastępczy Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta, Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela

Oprogramowanie równoważne musi spełniać poniższe warunki:

1. System operacyjny dla komputerów z graficznym interfejsem użytkownika,
2. System operacyjny ma pozwalać na uruchomienie i pracę z MS Office 20XX, Microsoft Teams
3. System ma udostępniać dwa rodzaje graficznego interfejsu użytkownika:
   a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy
   b) Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,
4. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim,
5. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
6. Wbudowany system pomocy w języku polskim,
7. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
9. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
10. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
11. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
12. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
13. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
14. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
15. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
16. Obsługa standardu NFC (near field communication),
17. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
18. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
19. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
20. Oprogramowanie dla tworzenia kopii zapasowych; automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,

22. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
23. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.