Załącznik nr 1 do ogłoszenia – Opis Przedmiotu Zamówienia

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

2. **Sprzęt komputerowy - laptop – (18 sztuk)o następujących parametrach technicznych:**

1. Ekran: 14 cali o rozdzielczości min. Full HD (1920x1080 pikseli)
2. Powłoka matrycy: matowa
3. Procesor (4 rdzeniowy/min. 8 wątki) min. 6458 punktów w teście Passmark CPU - http://www.cpubenchmark.net/
4. Bazowe taktowanie rdzeni procesora w przedziale od 1,6 GHz do 4,2 GHz
5. Min. 8GB DDR4 pamięci RAM, możliwość rozbudowy do min 32GB, 2 słoty na pamięci w tym min. jeden wolny
6. Dysk twardy min: 256 GB NVME SSD oraz możliwość montażu drugiego dyska 2,5 cali
7. Tryby pracy: tryb notebooka
8. Klawiatura mechanicznie połączona z komputerem, wyklucza się możliwość wykorzystania technologii bluetooth w komunikacji pomiędzy klawiaturą a komputerem, z wbudowanym w klawiaturze podświetleniem, (układ US z dolarem), min 80 klawiszy. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12.
9. Multimedia: Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo o mocy 2x 2W. Cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy. Kamera internetowa z diodą informującą o aktywności, min 0.9 Mpix, trwale zainstalowana w obudowie matrycy.
10. Łączność: certyfikowany modul WiFi 6 (802,11ax), 2,4Ghz, 5Ghz, maksymalna prędkość 2,4Gbps. Bluetooth min.5.0, Karta sieciowa ETH zgodna ze standardem 10/100/1000 Ethernet
11. Wbudowane porty i złącza:

- Min. 1 x HDMI
- min. 4xUSB (co najmniej: 2x USB 3.2 Gen 1 oraz 1x USB Type C 3.2 Gen 1)

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

- Wbudowane porty i złącza: 1x HDMI 1.4, 1x RJ-45, 2x USB 3.2, 1x USB TYP-C z obsługą DP 1.2, 1x USB 2.0, port zasilania, złącze linki zabezpieczającą
- 1 port audio typu combo (słuchawki i mikrofon)
- Port Ethernet 1x RJ-45

12. Zasilanie: zasilacz dedykowany do danego modelu;
13. Waga: max 1,7kg z baterią
14. Obudowa: Szkielet obudowy i zawiasy notebooka wzmacniane, dookoła matrycy uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią. Kąt rozwarcia matrycy 180 stopni. Laptop powinien spełniać normy MIL-STD-810G.
15. Bezpieczeństwo: zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.
16. System operacyjny: Preinstalowany system operacyjny Windows 10 Professional, klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.
17. Gwarancja: Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, 3-letnia gwarancja producenta świadczona na miejscu u klienta, Czas reakcji serwisu - do końca następnego dnia roboczego.
18. Zakupiony i dostarczony sprzęt komputerowy powinien być nowy i nieużywany.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

3. Sprzęt informatyczny - zakup macierzy dyskowej NAS - 1 sztuka o następnych parametrach technicznych:

1. Wnęka dysków:4 dyski 3,5-calowe SATA 6 Gb/s, 3 Gb/s
2. Kompatybilność dysków 3,5-calowe wnęki:
   a. 3,5-calowe dyski twarde SATA
   b. 2,5-calowe dyski twarde SATA
   c. 2,5-calowe dyski SSD SATA
3. Opcja Hot-PLUG HDD: Wymieniany podczas pracy
4. Obsługa dysków do min. 10TB
5. Obsługa przyspieszenia pamięci podręcznej SSD
6. Port Gigabit Ethernet (RJ45)x2
7. Port 10 Gigabit Ethernet 1 x 10GbE SFP+
8. min. 2x USB 3.2 Gen 1
9. KształtTower
10. Wskaźniki: LED, Zasilanie, stan, LAN, USB, HDD1–4
11. Przyciski: Zasilanie, reset, automatyczne kopiowanie USB
12. Złącze bezpieczeństwa Kensington
13. Maks. liczba jednoczesnych połączeń (CIFS) 1500, Obsługa ramek Jumbo
14. Zarządzanie prawami dostępu: Zbiorcze tworzenie użytkowników, Import/ eksport użytkowników, zarządzanie limitami użytkowników, kontrola dostępu użytkowników lokalnych dla CIFS, AFP, FTP i WebDAV, obsługa uprawnień do podfolderów dla zarządzania CIFS / SMB, AFP, FTP
15. Administracja WWW: Zarządzanie systemem w wielu oknach i wielozadaniowości,
16. Obsługiwany system operacyjny klienta: Windows 7-10, Apple Mac OS 10.7 lub nowszy, Microsoft Windows Server 2003, 2008 R2, 2012, 2012 R2 i 2016, Linux i UNIX
17. Bezpieczeństwo: Ochrona dostępu do sieci z automatycznym blokowaniem: SSH, Telnet, HTTP (S), FTP, CIFS / SMB, AFP, 256-bitowe szyfrowanie dysków zewnętrznych AES, Natychmiastowe powiadomienie przez e-mail, SMS, sygnał dźwiękowy, Weryfikacja dwuetapowa
18. Zarządzanie pamięcią masową: Monitorowanie wykorzystania przestrzeni dyskowej, Elastyczne woluminy i

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

jednostki LUN z elastycznym alokowaniem i odzyskiwaniem miejsca

19. Typy woluminów dyskowych: pojedynczy dysk, RAID 0, 1, 5, 6, 10, zapasowy i globalny zapasowy

20. Obsługa migawek: Menedżer migawek, Klon migawki, Przechowalnia migawek, Replika migawki, Agent migawki dla Microsoft Windows i VMware vSphere

21. Przyspieszenie SSD: pamięć podręczna SSD tylko do odczytu lub do odczytu i zapisu.

22. Integracja uwierzytelniania domeny:

23. Obsługa Microsoft Active Directory (AD) i kontrolera domeny, Serwer LDAP, klient LDAP, użytkownicy domeny logują się za pośrednictwem CIFS / SMB, AFP, FTP

24. Systemy plików: Wewnętrzny dysk twardy: EXT4, zewnętrzny dysk twardy: EXT3, EXT4, NTFS, FAT32, HFS +

25. Sieć: TCP / IP (IPv4 i IPv6), Klient DHCP, serwer DHCP, Protokoły: CIFS / SMB, AFP (v3.3), NFS (v3), FTP, FTPS, SFTP, TFTP, HTTP (S), Telnet, SSH, iSCSI, SNMP, SMTP i SMSC, Wykrywanie UPnP i Bonjour

26. Obsługa adaptera USB Wi-Fi

27. Serwer plików: Udostępnianie plików w systemach Windows, Mac i Linux / UNIX, Windows ACL, Zaawansowane uprawnienia do folderów dla CIFS / SMB, AFP, FTP, Monitorowanie i zarządzanie agregacją folderów współdzielonych (CIFS / SMB), Tworzenie i łączenie się z iSCSI target / LUN

28. Usługi sieciowy: Bezpłatna rejestracja nazwy hosta (DDNS), Obsługuje certyfikaty SSL (DDNS), Internetowy menedżer plików z szyfrowaniem min. HTTPS 2048-bitowym,

29. Backup: Backup z możliwością synchronizacji ze zdalnymi serwerami przez RTRR, Rsync, FTP i CIFS / SMB, Obsługa Amazon S3, Amazon Glacier, Microsoft Azure, Google Cloud Storage, Openstack Swift i WebDAV, Synchronizacja z Microsoft OneDrive,
Google Drive, Dropbox, Amazon Drive, Yandex Disk, Box i hubiC,
Tworzenie kopii zapasowych danych na wielu zewnętrznych urządzeniach magazynujących, Obsługa iSCSI, USB, DVD i zdalnego serwera NAS jako urządzeń archiwizujących, FTP przez SSL / TLS

30. Usługi VPN: Zintegrowany serwer VPN, klient VPN i usługi L2TP / IPSec VPN, Serwer VPN PPTP, L2TP / IPSec i OpenVPN, do 300 klientów, obsługuje użytkowników domeny jako

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

użytkowników VPN, Możliwość importowanie plików .ovpn w celu utworzenia połączenia OpenVPN

31. Wsparcie wielojęzyczne: min. Polski, angielski, możliwość zgłoszenia pomocy technicznej producenta, w celu rozwiązywania problemów (za zgodą użytkownika)

4. **Sprzęt informatyczny -zakup dysków HDD - 4 sztuki o następnych parametrach technicznych:**

1. Dyski twarde dedykowane do ciągłej pracy 24/7/365
2. Format szerokości: 3,5" (LFF)
3. Typ napędu: Wewnętrzny
4. Pojemność dysku :4 TB
5. Interfejs dysku: SATA III - 6 Gb/s
6. Prędkość obrotowa: 7200 obr/min
7. Bufor: min. 256 MB
8. Gwarancja producenta min. 5 lat

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

1. System operacyjny Windows 10 Professional licencja wieczysta - 18 szt. lub równoważne.
2. Pakiet oprogramowania biurowego MS Office 2019 Standard licencja wieczysta - 20 szt. lub równoważne.
3. **Zakup oprogramowania ochrony stacji roboczych i serwerów -** ESET Endpoint Protection Advanced pierwszy zakup – 25 szt. na okres dwunastu miesięcy lub równoważne.
4. Zakupione i dostarczone ww. oprogramowanie powinno być nowe i nieużywane**.** W przypadku, gdy wykonawca oferuje licencje na oprogramowanie inne niż wskazane wyżej, oprogramowanie powinno spełniać określone w pkt .6 wymogi równoważności.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

6. **Wymogi równoważności**

a. **Wymogi równoważności odnośnie systemu operacyjnego**

System powinien spełniać następujące warunki:

1. licencji:

- licencja uprawniająca do użytkowania wieczystego;

2. funkcjonalności:

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

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

b. **Wymogi równoważności odnośnie oprogramowania biurowego**

Wymogi równoważności w zakresie:
1) licencji:
a) licencja uprawniająca do wieczystego użytkowania;

b) wszystkie komponenty oferowanego pakietu biurowego muszą być integralną częścią tego samego pakietu, współpracować ze sobą (osadzanie i wymiana danych), posiadać jednolity interfejs oraz ten sam jednolity sposób obsługi, wykonywanie i edycja makr oraz kodu zapisanego w języku Visual Basic w plikach xls, xlsx oraz formuł w plikach wytworzonych w MS Office 2003, MS Office 2007,MS Office 2010, MSOffice 2013 oraz MS Office 2016 bez utraty danych oraz bez konieczności przerabiania dokumentów
2) funkcjonalności:
a) pakiet musi składać się z programów:
- do edycji tekstu;
- arkusza kalkulacyjnego;
- do tworzenia prezentacji;
- program do obsługi kontaktów;
b) edytor tekstu powinien umożliwiać:
- zapis i odczyt dokumentów w formatach: rtf, doc, docx oraz odt (dopuszczalne jest wykorzystanie w tym celu wtyczki);
- pełną współpracę z opcjami Recenzji pakietu Microsoft Office 2007 i wyższe, w szczególności tryb „Śledź zmiany" oraz obsługę komentarzy;
- obsługę trybu korespondencji seryjnej z użyciem źródeł danych ze skoroszytów generowanych za pomocą Microsoft Excel (oraz, w razie zaoferowania innego pakietu niż Microsoft Office, także arkusza kalkulacyjnego będącego częścią oferty);
c) arkusz kalkulacyjny powinien umożliwiać zapis i odczyt dokumentów w formatach: xls, xlsx, ods (dopuszczalne jest wykorzystanie w tym celu wtyczki), możliwość jednoczesnej pracy wielu użytkowników na udostępnionym dokumencie arkusza kalkulacyjnego;
d) program do tworzenia prezentacji powinien umożliwiać zapis i odczyt dokumentów w formatach:

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

ppt, pptx, odp (dopuszczalne jest wykorzystanie w tym celu wtyczki);
e) wszystkie programy pakietu powinny umożliwiać eksport do formatu pdf, (dopuszczalne jest wykorzystanie w tym celu wtyczki);
f) program do obsługi kontaktów powinien realizować funkcje:
- klienta e-mail;
- kalendarza z terminarzem;
- menadżera kontaktów.
g) możliwość aktualizacji z serwerów producenta
h) umożliwienie aktualizacji poprawek bezpieczeństwa
h) umożliwienie synchronizacji oraz integracji z Microsoft 365

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

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

Ochrona antywirusowa i antyspyware
7. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
8. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing,
narzędzi hakerskich, backdoor.
9. Wbudowana technologia do ochrony przed rootkitami.
10. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

11. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
12. Możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.
13. System ma posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.
14. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
15. Skanowanie „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
16. Możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
17. Możliwość skanowania dysków sieciowych i dysków przenośnych.
18. Skanowanie plików spakowanych i skompresowanych.
19. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
20. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
21. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
22. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
23. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
24. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
25. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
26. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ”
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
27. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
28. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
29. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
30. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
31. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
32. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
33. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
34. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
35. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
36. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
37. Program ma zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
38. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
39. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
40. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

41. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
42. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
43. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.
44. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
45. Możliwość automatycznego wysyłania nowych do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
46. Do wysłania próbki zagrożenia do laboratorium producenta, aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
47. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
48. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
49. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
50. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
51. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
52. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

53. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
54. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
55. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
56. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
57. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
58. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
59. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
60. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
61. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
62. W momencie podłączenia zewnętrznego nośnika, aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
63. Administrator ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

64. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
65. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

- tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
- tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
- tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
- tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

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

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ”
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

74. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
75. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
76. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
77. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
78. Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback). Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
79. Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
80. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
81. W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji.
82. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
83. Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron internetowych i kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
84. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.
85. Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
86. Program musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

87. Możliwość podejrzenia informacji o licencji, która znajduje się w programie.
88. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM.
89. W programie musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.
90. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.
91. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.
92. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.
93. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
94. Program musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.
95. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
96. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
97. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
98. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
99. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
100. Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ”
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

101. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.
102. Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”.
103. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
104. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
105. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
106. Administrator musi posiadać możliwość zastosowania reguł dla kontroli dostępu do stron w zależności od zdefiniowanego przedziału czasowego.
107. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
108. Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.
109. Program ma posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.

Ochrona przed spamem

110. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
111. Program ma umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
112. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
113. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
114. Możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
115. Możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
116. Możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
117. Program ma domyślnie współpracować z folderem „Wiadomości-śmieci”, dostępnym w programie Microsoft Outlook.
118. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana”

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ”
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

119. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana”.
120. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

Zapora osobista (personal firewall)
121. Zapora osobista ma pracować w jednym z czterech trybów: • tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
- tryb interaktywny – program pyta się o każde nowo nawiązywane połączenie,
- tryb oparty na regułach – program blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
- tryb uczenia się – program automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

122. Program musi oceniać reguły zapory systemu Windows.
123. Możliwość tworzenia list sieci zaufanych.
124. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
125. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego.
126. Możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
127. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
128. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet.
129. Wykrywanie modyfikacji w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu.
130. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
131. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ”
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

132. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
133. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie.
134. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6.
135. Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci.
136. Program musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów:
• z aplikacją lokalną, którą administrator wskazuje z listy,
• z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP.

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

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

Ochrona serwera Windows

1. Wsparcie dla systemów: Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012, Microsoft Windows Server 2008 R2 SP1, Microsoft Windows Server 2008 SP2 (oparty na procesorze x86 i x64), Server Core (Microsoft Windows Server 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016).
2. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
3. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
5. Wbudowana technologia do ochrony przed rootkitami i exploitami.
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
11. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
12. Możliwość skanowania dysków sieciowych i dysków przenośnych.
13. Skanowanie plików spakowanych i skompresowanych.
14. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
15. Aplikacja powinna wspierać mechanizm klastrowania.
16. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
17. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ”
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
b. tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
d. tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
e. tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.
18. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
19. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
20. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
21. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
22. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
23. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na serwerze.
24. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
25. Funkcja blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
26. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
27. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
28. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
29. Program musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
30. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
31. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
32. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
33. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
34. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
35. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
36. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
37. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
38. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
39. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ”
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
40. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
41. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
42. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
43. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
44. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
45. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.
46. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.
47. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
48. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i wyświetlić listę niezainstalowanych aktualizacji.
49. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
50. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
51. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
52. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
53. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
54. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.
55. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
56. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
57. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
58. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
59. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
60. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
61. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
62. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
63. Aplikacja musi wspierać skanowanie magazynu Hyper-V.
64. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

65. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji modułów i samego oprogramowania.
66. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
67. Program musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść".
68. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
69. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.
70. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
71. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
72. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.
73. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
74. Program musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów.
75. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
76. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
77. Program musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

Ochrona serwera - Linux

Architektura rozwiązania

1. Skaner antywirusowy i antyspyware.
2. Skanowanie plików, plików spakowanych i archiwów samorozpakowujących.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

3. Oprogramowanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów oprogramowania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
4. Oprogramowanie musi posiadać wbudowany mechanizm typu ,,watchdog". Monitoruje on tzw. stan zdrowia poszczególnych mikro-serwisów i automatycznie przeładowuje je w przypadku wykrycia zakłóceń w pracy mikro-serwisu.
5. Architektura rozwiązania musi pozwalać na uruchamianie poszczególnych mikro-serwisów, tylko na czas realizacji funkcjonalności przez nie realizowanych, co pozwala w znaczącym stopniu ograniczyć wykorzystanie zasobów systemu operacyjnego.
6. Oprogramowanie antywirusowe musi wspierać wieloprocesorową i wielordzeniową architekturę, w celu zapewnienia maksymalnego zwiększenia wydajności.
7. Oprogramowanie antywirusowe musi być wyposażone w moduł ochrony systemu plików w czasie rzeczywistym. Moduł nie może wymagać instalowania jakichkolwiek dodatkowych komponentów w systemie operacyjnym. Wszystkie komponenty muszą być instalowane w systemie, podczas instalacji z dostarczonego instalatora binarnego.
8. Silnik ochrony systemu plików w czasie rzeczywistym musi stanowić dodatkowy moduł jądra systemu Linux i musi być dodawany do jądra, podczas procesu instalacji oprogramowania antywirusowego.
9. Ochrona systemu plików w czasie rzeczywistym musi być zapewniona nieprzerwanie od uruchomienia produktu i obejmuje skanowanie zarówno dysków lokalnych jak i zmapowanych dysków sieciowych.
10. Silnik skanujący musi działać wyłącznie z wykorzystaniem 64-bitowej architektury.
11. Oprogramowanie musi być w pełni zgodne z modułem SELinux, pracującym zarówno w trybie ,,Permissive" jak i ,,Enforcing".
12. Oprogramowanie podczas procesu instalacji, musi dodawać i konfigurować własne polityki modułu SELinux, które są kompatybilne z następującymi dystrybucjami systemów Linux: Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Centos 6, Centos 7.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

13. Wszystkie mechanizmy bezpieczeństwa oprogramowania muszą wspierać system informowania o zagrożeniach w czasie rzeczywistym. System ten pozwala na weryfikowanie reputacji plików oraz procesów i identyfikację nowych i nieznanych zagrożeń.
14. Skaner systemu plików w czasie rzeczywistym musi działać dla operacji obsługi plików, dla co najmniej takich operacji jak: dostęp do pliku, utworzenie (zapisanie) pliku.
15. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
16. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
17. Oprogramowanie musi być wyposażone we własny wiersz polecenia (CLI). Polecenia muszą być odpowiedzialne co najmniej za: skanowanie na żądanie, konfigurację mechanizmów bezpieczeństwa, uruchamianie aktualizacji, przeglądanie logów aplikacji, konfigurację graficznego interfejsu użytkownika, obsługę kwarantanny plików.
18. Rozwiązanie musi wspierać system plików zamontowany z flagą ,,noexec".
19. Oprogramowanie musi pozwalać na uruchamianie zadań skanowania działających ,,w tle", z możliwością ustawienia dla nich niskiego priorytetu.
20. Zadania skanowania nie mogą zmieniać znacznika dostępu do plików.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

Skanowanie sieciowych systemów plików

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

Instalacja

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

Licencjonowanie

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

Interfejs graficzny

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

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349

2. Lokalna konsola administracyjna musi działać w oparciu o dynamicznie generowaną zawartość tworzoną z wykorzystaniem następujących technologii: React/Node.js, HTML5.
3. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
4. Lokalna konsola administracyjna musi zapewniać bezpieczne połączenie działające w oparciu o protokół HTTPS.
5. Lokalna konsola administracyjna musi umożliwiać uruchomienie jej, na wskazanym porcie TCP.
6. Logowanie do lokalnej konsoli administracyjnej musi być realizowane, poprzez podanie danych w postaci nazwy użytkownika i zdefiniowanego dla niego hasła.
7. Administrator systemu musi mieć możliwość zdefiniowania dodatkowych kont użytkowników, w lokalnej konsoli administracyjnej.
8. Lokalna konsola administracyjna musi zapewniać funkcjonalność zweryfikowania stanu licencji i informacji na jej temat.
9. Z poziomu lokalnej konsoli administracyjnej musi być możliwość zarządzania, wbudowanym modułem menadżera kwarantanny.
10. Lokalna konsola administracyjna musi zapewniać możliwość przełączenia wersji językowej konsoli, na etapie logowania. Lokalna konsola administracyjna musi posiadać interfejs, co najmniej w języku: polskim, angielskim.

Dodatkowe wymogi:

1. Wykonawca gwarantuje najwyższą jakość przedmiotu zamówienia.
2. Wykonawca udzieli gwarancji na sprzęt na okres 24 miesięcy (typ gwarancji door to door, chyba że OPZ stanowi inaczej), liczony od dnia podpisania protokołu odbioru przedmiotu zamówienia z nieodpłatnym (wliczonym w cenę oferty) serwisem wynikającym z warunków gwarancji i naprawą w okresie gwarancyjnym. Szczegółowe warunki gwarancji określa umowa
3. Wykonawca gwarantuje dostarczenie sprzętu w terminie do 14 dni liczonym od dnia podpisania umowy.

Sieć Badawcza Łukasiewicz – Instytut Organizacji i Zarządzania w Przemyśle ,,ORGMASZ"
08-879 Warszawa, ul. Żelazna 87, Tel: +48 601 579 728,
E-mail: instytut@orgmasz.pl | NIP: 525 00 08 293, REGON: 000040347
Sąd Rejonowy dla m.st. Warszawy XVI Wydział Gospodarczy KRS nr 0000098349