Załącznik nr 2

Wymagania dot. zaoferowania oprogramowania innego niż ESET Endpoint Security for Android.

W ramach dostawy oprogramowania innego niż ww. wskazane Wykonawca musi dostarczyć 100 licencji na oprogramowanie antywirusowe spełniające poniższe wymagania. Ponadto musi odinstalować obecnie posiadane przez PUW oprogramowanie antywirusowe i zainstalować nowe oprogramowanie na wszystkich urządzeniach mobilnych w Urzędzie (kilka lokalizacji w Rzeszowie, Krośnie. Przemyślu i Tarnobrzegu). W ramach wymiany na inne oprogramowanie należy wykonać asystę przy instalacji konsoli administracyjnej.
Ponadto należy przeszkolić 5 administratorów z administrowania zaoferowanym systemem antywirusowym – szkolenie min. 16 godzin lekcyjnych. Szkolenie musi się odbyć w siedzibie Zamawiającego – Rzeszów ul .Grunwaldzka 15.
Całość prac musi się zakończyć do dnia 5.10.2021 r.

Ochrona urządzeń mobilnych opartych o system Android

1. Wspierany system co najmniej Android 4.0 (Ice Cream Sandwich)
2. Rozdzielczość wyświetlacza urządzenia 480x800px lub wyższa.
3. Procesor: ARM (minimum ARMv7)
4. Pamięć wewnętrzna: 20 MB.
5. Połączenie z siecią Internet dla celów aktualizacji sygnatur i aktywacji licencji

Ochrona antywirusowa:

6. Ochrona plików w czasie rzeczywistym
7. Ochrona przed atakami typu „phishing”
8. Skanowanie rozszerzeń DEX, bibliotek SO plików archiwum oraz innych.
9. Skanowanie dostępnego w urządzeniu nośnika pamięci SD.
10. Aplikacja musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne
11. Ochrona proaktywna wykrywająca nieznane zagrożenia.
12. Aplikacja ma mieć możliwość określenia poziomu głębokości skanowania plików archiwum.
13. Aplikacja ma mieć możliwość określenia domyślnej akcji podejmowanej w przypadku wykrycia zagrożenia: przeniesienia do kwarantanny, usunięcia lub zignorowania.
14. W przypadku wykrycia zagrożenia użytkownik ma otrzymać odpowiednie powiadomienie
15. Aplikacja musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia
16. Aplikacja musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności, w pełni naładowane i podłączone do ładowarki

Skanowanie na żądanie:

17. Aplikacja ma mieć możliwość skanowania zainstalowanych aplikacji.
18. Aplikacja ma wykorzystywać do celu skanowania metody heurystyczne wykrywające nieznane zagrożenia.
19. Informacje o skanowaniu mają być przechowywane w plikach dziennika.

20. Użytkownik ma mieć możliwość wskazania akcji jaka ma być podjęta w przypadku wykrycia zagrożenia: poddania kwarantannie, usunięcia lub zignorowania.
21. Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia, lub wskazania folderu, który ma być przeskanowany.
22. Aplikacja ma posiadać osobne dzienniki skanowania dla ochrony plików w czasie rzeczywistym, oraz skanowania na żądanie.

Filtr SMS/MMS i połączeń (jeśli system zezwala):
Użytkownik musi mieć możliwość definiowania własnych reguł dotyczących połączeń oraz wiadomości SMS/MMS bez konieczności podawania hasła administratora

23. Reguły zdefiniowane przez administratora (w trybie administratora) muszą mieć wyższy priorytet niż reguły zdefiniowane przez użytkownika.
24. Użytkownik i administrator ma mieć możliwość tworzenia białej i czarnej listy numerów telefonów.
25. Użytkownik i administrator ma mieć możliwość dodania numeru telefonu, dla którego można określić akcje dla:
    a. Przychodzącej wiadomości SMS
    b. Przychodzącej wiadomości MMS
    c. Połączenia wychodzącego
    d. Połączenia przychodzącego.
26. Aplikacja ma mieć możliwość aktywacji blokady dla wszystkich połączeń oraz wiadomości SMS/MMS dla znanych kontaktów znajdujących się w książce telefonicznej urządzenia.
27. Aplikacja ma mieć możliwość blokady połączeń telefonicznych oraz wiadomości SMS/MMS dla nieznanych kontaktów (nieznajdujących się w książce telefonicznej urządzenia).
28. Aplikacja ma mieć możliwość blokowania anonimowych połączeń przychodzących (pochodzących z ukrytych ID).
29. Aplikacja ma być wyposażona w dziennik modułu antyspamowego zawierający informacje odnośnie filtrowania modułu.

Ochrona przed kradzieżą:

30. Użytkownik ma mieć możliwość wprowadzenia zaufanej karty SIM.
31. Dodanie zaufanej karty SIM ma się odbyć się w oparciu o kartę wprowadzoną w danym urządzeniu lub w oparciu o dane wprowadzone ręcznie.
32. Wprowadzenie danych ręcznie dotyczących zaufanej karty SIM ma się odbywać w oparciu o numer IMSI karty SIM.
33. Aplikacja ma mieć możliwość wprowadzenia zaufanych odbiorców wiadomości, do których zostanie przesłana informacja w przypadku umieszczenia w urządzeniu innej niż zaufana karty SIM.
34. Aplikacja ma mieć możliwość włączenia opcji ignorowania niedopasowania kart SIM.
35. Użytkownik ma mieć możliwość edycji treści wiadomości SMS wysyłanej na zaufane numery telefonów w przypadku nie dopasowania karty SIM.
36. W przypadku kradzieży urządzenia, prawowity użytkownik ma mieć możliwość wysłania na urządzenie komendy która umożliwi:
    a. usunięcie zawartości urządzenia
    b. zablokowania urządzenia
    c. przesłania na zaufany numer telefonu lokalizacji GPS w której skradzione urządzenie się znajduje.

37. Administrator musi mieć możliwość wysyłania powyższych komend bezpośrednio z poziomu konsoli centralnego zarządzania
38. Możliwość zdalnego zresetowania hasła ma być możliwa tylko w przypadku wysłania odpowiedniego polecenia z zaufanego urządzenia

Polityka ustawień:
Aplikacja musi posiadać funkcjonalność pozwalającą administratorowi na monitorowanie ustawień urządzenia w celu weryfikacji czy są one zgodne z polityką.

39. Administrator musi mieć wgląd w podstawowe ustawienia urządzenia:
    a. Połączenie Wi-Fi
    b. Satelity GPS
    c. Usługi lokalizacyjne
    d. Pamięć
    e. Roaming danych
    f. Roaming połączeń
    g. Nieznane źródła
    h. Tryb debugowania
    i. Komunikacja NFC
    j. Szyfrowanie pamięci masowej
40. Administrator ma mieć możliwość wyboru powyższych elementów

Kontrola aplikacji:

41. Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji
42. Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji
43. Blokowanie aplikacji musi być umożliwione co najmniej za pomocą polityk:
    a. manualnego zdefiniowania listy blokowanych aplikacji na podstawie nazwy
    b. blokowanie na podstawie kategorii (np. kategorii Gry lub Społecznościowe)
    c. blokowanie na podstawie uprawnień aplikacji (np. aplikacji, które korzystają z modułu GPS do odczytania lokalizacji)
    d. blokowanie na podstawie źródła (np. aplikacje instalowane z innych źródeł niż sklep Google Play)
44. Administrator musi mieć możliwość monitorowania czasu, jaki użytkownik spędza na korzystaniu z poszczególnych aplikacji i sprawdzenia z jakich aplikacji użytkownik korzystał w ciągu ostatnich 30 dni, 7 dni oraz 24 godzin.

Zabezpieczenia urządzenia:

45. W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej:
    a. minimalny poziom zabezpieczeń i złożoność blokady ekranu
    b. maksymalną dopuszczaną liczbę błędnych prób odblokowania
    c. odstęp czasu po którym użytkownik musi zmienić kod odblokowujący urządzenie
    d. czas przeznaczony na odblokowanie urządzenia
    e. ograniczyć dostęp do kamery wbudowanej w urządzenie

Aktualizacje sygnatur:

46. Wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.

47. Aplikacja ma mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje sygnatur co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin.
48. Aplikacja ma mieć funkcjonalność ochrony hasłem wybranych modułów ochrony, w tym co najmniej dostępu do ustawień ochrony antywirusowej, ustawień modułu antyspamowego, ochrony przed kradzieżą, uruchamiania zadań audytu zabezpieczeń oraz przed deinstalacją.
49. Aplikacja ma mieć możliwość ukrycia ikony powiadomień.

Konfiguracja i zdalne zarządzanie:

50. Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne
51. Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją
52. Administrator musi mieć możliwość zdalnego wysyłania komunikatów z poziomu konsoli centralnego zarządzania do użytkowników urządzeń mobilnych
53. Przesłana wiadomość musi wyświetlać się w formie wyskakującego okna, aby użytkownik ich nie przeoczył
54. Administrator musi mieć możliwość kontrolowania mechanizmu aktualizacji oprogramowania