Zał. B

Specyfikacja wymaganego oprogramowania antywirusowego - urządzenia mobilne

Program antywirusowy

A. Wymagania ogólne:

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

B. Zakres funkcjonalny programu:

1. Ochrona antywirusowa:
   1) Ochrona plików w czasie rzeczywistym
   2) Ochrona przed atakami typu „phishing”
   3) Skanowanie rozszerzeń DEX, bibliotek SO plików archiwum oraz innych.
   4) Skanowanie dostępnego w urządzeniu nośnika pamięci SD.
   5) Ochrona proaktywna wykrywająca nieznane zagrożenia.
   6) Aplikacja ma mieć możliwość określenia domyślnej akcji podejmowanej w przypadku wykrycia zagrożenia: przeniesienia do kwarantanny, usunięcia lub zignorowania.
   7) W przypadku wykrycia zagrożenia użytkownik ma otrzymać odpowiednie powiadomienie
   8) Aplikacja musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia

2. Skanowanie na żądanie:
   1) Aplikacja ma mieć możliwość skanowania zainstalowanych aplikacji.
   2) Aplikacja ma wykorzystywać do celu skanowania metody heurystyczne wykrywające nieznane zagrożenia.
   3) Informacje o skanowaniu mają być przechowywane w plikach dziennika.
   4) Użytkownik ma mieć możliwość wskazania akcji jaka ma być podjęta w przypadku wykrycia zagrożenia: poddania kwarantannie, usunięcia lub zignorowania.
   5) Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia, lub wskazania folderu, który ma być przeskanowany.
   6) Aplikacja ma posiadać osobne dzienniki skanowania dla ochrony plików w czasie rzeczywistym, oraz skanowania na żądanie.

3. Filtr SMS/MMS i połączeń (jeśli system zezwala):
   1) Użytkownik ma mieć możliwość tworzenia białej i czarnej listy numerów telefonów.
   2) Użytkownik ma mieć możliwość dodania numeru telefonu, dla którego można określić akcje dla:
      a) Przychodzącej wiadomości SMS
      b) Połączenia wychodzącego
      c) Połączenia przychodzącego.
   3) Aplikacja ma mieć możliwość blokady połączeń telefonicznych oraz wiadomości SMS/MMS dla nieznanych kontaktów (nieznajdujących się w książce telefonicznej urządzenia).
   4) Aplikacja ma mieć możliwość blokowania anonimowych połączeń przychodzących (pochodzących z ukrytych ID).
   5) Aplikacja ma być wyposażona w dziennik modułu antyspamowego zawierający informacje odnośnie filtrowania modułu.

4. Ochrona przed kradzieżą:
   1) Aplikacja ma mieć możliwość wprowadzenia zaufanych odbiorców wiadomości, do których zostanie przesłana informacja w przypadku umieszczenia w urządzeniu innej niż zaufana karty SIM.
   2) Aplikacja ma mieć możliwość włączenia opcji ignorowania niedopasowania kart SIM.
   3) Użytkownik ma mieć możliwość edycji treści wiadomości SMS wysyłanej na zaufane numery telefonów w przypadku nie dopasowania karty SIM.
   4) 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.
   5) Administrator musi mieć możliwość wysyłania powyższych komend bezpośrednio z poziomu konsoli centralnego zarządzania

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

6. Kontrola aplikacji:
1) Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji
2) Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji.
3) 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)

7. Aktualizacje sygnatur:
1) Wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.
2) Aplikacja ma mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje sygnatur co najmniej: raz dziennie, co tydzień.

8. Konfiguracja i zdalne zarządzanie:
Administrator musi mieć możliwość kontrolowania mechanizmu aktualizacji oprogramowania