Aktualizacja – 03.09.2021 r.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi wspierać system co najmniej Android 5.0.
2. Rozwiązanie musi wspierać rozdzielczość wyświetlacza urządzenia 480x800px lub wyższa.
3. Rozwiązanie musi wspierać procesory: ARM z obsługą ARMv7 lub x86 Intel Atom.
4. Rozwiązanie musi posiadać ochronę plików w czasie rzeczywistym.
5. Rozwiązanie musi posiadać ochronę przed atakami typu „phishing".
6. Rozwiązanie musi skanować wszystkie typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
7. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
8. Rozwiązanie musi posiadać ochronę proaktywną wykrywającą nieznane zagrożenia.
9. W przypadku wykrycia zagrożenia użytkownik musi otrzymać odpowiednie powiadomienie.
10. Rozwiązanie musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia.
11. Rozwiązanie musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).

Skanowanie na żądanie:

12. Rozwiązanie musi mieć możliwość skanowania zainstalowanych aplikacji.
13. Informacje o skanowaniu mają być przechowywane w plikach dziennika.
14. Użytkownik ma mieć możliwość wyboru akcji jaka ma być podjęta w przypadku wykrycia zagrożenia, co najmniej: poddania kwarantannie, usunięcia oraz zignorowania.
15. Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia.

Ochrona przed kradzieżą:

16. Administrator ma mieć możliwość skonfigurowania zaufanej karty SIM.
17. W przypadku kradzieży urządzenia, Administrator ma mieć możliwość wysłania na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
    a. usunięcie zawartości urządzenia,
    b. przywrócenie urządzenie do ustawień fabrycznych,
    c. zablokowania urządzenia,
    d. uruchomienie sygnału dźwiękowego,
    e. lokalizację GPS.

Polityka ustawień:

18. Administrator musi mieć wgląd w podstawowe ustawienia urządzenia, w tym co najmniej:
    a. połączenie Wi-Fi,
    b. 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,
k. urządzenie zrootowane.

Kontrola aplikacji:

19. Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji.
20. Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji.
21. Blokowanie aplikacji musi być możliwe w oparciu o:
    a. nazwę aplikacji,
    b. nazwę pakietu,
    c. kategorię sklepu Google Play,
    d. uprawnienia aplikacji,
    e. pochodzenie aplikacji z nieznanego źródła.

Zabezpieczenia urządzenia:

22. 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, po którym automatycznie nastąpi blokada ekranu,
    e. ograniczenie dostępu do kamery wbudowanej w urządzenie.

Aktualizacje modułów:

23. Rozwiązanie musi umożliwiać wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.
24. Rozwiązanie musi mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje modułów co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin.
25. Rozwiązanie musi posiadać możliwość zabezpieczenia hasłem konkretnych modułów, w tym co najmniej: dostępu do ustawień ochrony antywirusowej, ochrony przed kradzieżą, deinstalacją.

Konfiguracja i zdalne zarządzanie:

26. Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne.

27. Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją.
28. Administrator musi mieć możliwość zdalnego wysyłania komunikatów z poziomu konsoli centralnego zarządzania do użytkowników urządzeń mobilnych.
29. Przesłana wiadomość musi wyświetlać się w formie wyskakującego okna.
30. Wdrożenie urządzenia mobilnego z poziomu konsoli zarządzającej musi się odbyć co najmniej na jeden z trzech możliwych sposobów:
    a. za pomocą kodu QR,
    b. za pomocą unikatowego łącza,
    c. za pomocą wiadomości e-mail,

W ramach aktywacji za pomocą kodu QR musi istnieć możliwość aktywacji w trybie właściciela urządzenia (Android Enterprise Device Owner).