Zakup subskrypcji na oprogramowanie do monitorowania i blokowania przepływu danych osobowych na komputerach

1. Liczba komputerów do ochrony w ramach niniejszego oprogramowania: 55 szt.
2. W ramach zakupu zalicza się wdrożenie produktu u Zamawiającego z 8-godzinnym przeszkoleniem trzech osób wyznaczonych przez Zamawiającego.
3. Oprogramowanie musi być typu DLP (Data Loss Prevention).
4. Oprogramowanie musi umożliwiać ochronę przed wyciekiem informacji z systemów informatycznych Zamawiającego.
5. Oprogramowanie musi realizować swoje funkcje zarówno na poziomie sieci (Network DLP) oraz stacji końcowej jak komputer, czy laptop (Endpoint DLP).
6. Zarządzanie, obsługa incydentów, oraz raportowanie musi być spójne dla ochrony na poziomie sieci i stacji końcowych i odbywać się z pojedynczej webowej konsoli zarządzającej.
7. Dostęp do konsoli zarządzającej powinien odbywać się w bezpiecznym połączeniu https.
8. Ochrona informacji powinna odbywać się w oparciu o reguły bezpieczeństwa informacji odzwierciedlające procesy biznesowe.
9. Oprogramowanie musi umożliwiać monitorowanie i ochronę wielu typowych kanałów komunikacyjnych, w szczególności:
    a. http oraz https (patrz punkt 23)
    b. email
    c. komunikatory internetowe
    d. ActiveSync (dla synchronizacji poczty z urządzeń mobilnych)
10. Oprogramowanie musi umożliwiać definiowanie własnych kanałów transmisji, które mają być monitorowane.
11. Oprogramowanie w zakresie stacji końcowej musi umożliwiać monitorowanie takich czynności jak kopiowanie informacji na zewnętrzne nośniki danych, nagrywanie płyt, lokalne drukowanie, wklejanie informacji w okna aplikacji.
12. Oprogramowanie musi umożliwiać tworzenie polityk uwzględniających takie akcje jak:
    a. wysyłanie powiadomień w ramach odnotowanych incydentów, przy czym powiadamiane powinny być następujące osoby:
        - nadawca, czyli osoba, która wysyłała informacje,
        - zwierzchnik nadawcy,
        - właściciel informacji zdefiniowany w polityce,
        - właściciel polityki.
    b. blokowanie transmisji naruszających zdefiniowaną politykę,
    c. kwarantannę informacji,
    d. szyfrowanie informacji,
    e. umożliwienie użytkownikowi kontynuowania operacji po zatwierdzeniu komunikatu wyświetlonego przez agenta ochrony informacji na stacji końcowej.
13. Oprogramowanie musi umożliwiać łączenie polityk w grupy.
14. Oprogramowanie musi umożliwiać budowanie polityk ochrony informacji uwzględniając kontekst w jakim informacja jest używana, czyli musi uwzględniać okoliczności jak:
    a. Kto wysyła informacje,
    b. Gdzie informacje są wysyłane,

    c. W jaki sposób informacje są wysyłane (patrz punkt 7),
    d. Co jest wysyłane, czyli właściwa identyfikacja treści (patrz punkt 15).
15. Oprogramowanie musi wykorzystywać szeroką gamę mechanizmów identyfikowania treści, m.in.:
    a. słowa kluczowe,
    b. wyrażenia regularne,
    c. tworzenie odcisku palca – fingerprint,
    d. Algorytmy Machine Learning
16. Algorytm tworzenia odcisku palca powinien tworzyć wiele odcisków palca dla pojedynczego pliku, tak aby chronić informacje zawarte w pliku a nie wyłącznie dokument w całości.
17. Oprogramowanie powinno również umożliwić tworzenie odcisków palca z zasobów zawartych w bazach danych. Tworzenie takich odcisków powinno odbywać się bez uprzedniego kopiowania informacji do pliku (np. za pomocą ODBC).
18. Oprogramowanie musi zawierać predefiniowane reguły ochrony informacji, dotyczące np. numerów krat kredytowych, IBAN, oraz takich identyfikatorów jak PESEL, REGON, NIP, nr Dowodu Osobistego.
19. System musi umożliwiać integrację z usługami katalogowymi umożliwiająca m.in.:
    a. przypisywanie użytkowników i grup jako autoryzowanych nadawców i odbiorców monitorowanych informacji,
    b. przypisanie użytkowników do ról zarządzających takich jak administrator, audytor, manager incydentów,
    c. wyświetlanie szczegółów dotyczących użytkownika w ramach incydentu związanego z jego aktywnością, np. powinno być możliwe wyświetlenie informacji o zwierzchniku użytkownika.
20. Producent systemu DLP powinien w swoim portfolio produktów oferować system Web Security oraz filtrowania URL, który w integracji z systemem DLP będzie udostępniał dodatkowe informacje widoczne w szczegółach incydentu, np. kategoria strony internetowej do której miejsce miał transfer informacji.
21. Oprogramowanie musi umożliwiać zautomatyzowane wykrywanie informacji objętych politykami ochrony na serwerach i stacjach końcowych w sieci Zamawiającego (funkcjonalność Discovery). Funkcjonalność ta powinna być również oferowana dla folderów Exchange, serwera SharePoint oraz baz danych.
22. Konsola zarządzająca powinna zawierać ekran przedstawiający podstawowe statystki aktywności z ostatnich 24 godzin jak ilość incydentów względem ważności, najczęściej naruszane kategorie polityk, stacje końcowe, na których wykryto najwięcej naruszeń, etc.
23. Konsola zarządzająca powinna umożliwiać zarządzanie incydentami, m.in. zmianę ich statusu, przekazywanie do innego administratora.
24. Oprogramowanie musi umożliwić ziarnistą delegację uprawnień do konfiguracji systemu, polityk, raportów oraz incydentów w oparciu o wbudowane jak również własne role, takie jak administrator, audytor, manager incydentów.
25. Oprogramowanie w ramach odnotowanych incydentów musi udostępniać informacje dotyczące reguły, która została naruszona, jak również kopię informacji, która była

przesyłana. Wgląd w tak szczegółowe informacje powinien być kontrolowany zgodnie z pkt. 22.

26. Oprogramowanie powinno umożliwiać rozpoznawanie tekstu zawartego w plikach graficznych i jego analizie pod względem wrażliwości informacji (OCR). Ta funkcjonalność powinna być oferowana dla dokumentów graficznych wysyłanych poprzez styk z Internetem (smtp, http, https)
27. Oprogramowanie klienckie (Endpoint) powinno być oferowane w polskiej wersji językowej.
28. Oprogramowanie powinno być zaopatrzone we własny moduł analityczny, który umożliwi wskazanie z listy incydentów tych najbardziej istotnych poprze ich korelacje i grupowanie. System musi zwrócić alert w przypadku zwiększonej ilości zdarzeń mających wspólne źródło np. w jednym konkretnym użytkowniku.
29. Producent oprogramowania DLP powinien w swoim portfolio produktów oferować system CASB, który w integracji z systemem DLP będzie udostępniał dodatkowe informacje widoczne w szczegółach incydentu i skupiał się na ochronie danych wysyłanych i składowanych w chmurze za pomocą aplikacji chmurowych.
30. Oprogramowanie powinno mieć możliwość rozbudowy do systemu umożliwiającego dynamiczną ocenę ryzyka użytkownika (na podstawie incydentów DLP) i w zależności od tego ryzyka powinien mieć możliwość modyfikowania akcji przeprowadzonych przez system. Wyższe ryzyko skutkuje bardziej restrykcyjną polityką dla konkretnego użytkownika, w zależności od poziomu ryzyka.
31. Oprogramowanie powinno mieć możliwość integracji z rozwiązaniami klasyfikacji danych. W szczególności, dla wybranych systemów, powinien być w stanie przypisać politykę DLP na podstawie klasyfikatora. W przypadku wykrycia pliku posiadającego dane wrażliwe, a nie sklasyfikowanego, powinien być w stanie nadać taki klasyfikator lub zwrócić informację do systemu.
32. Zamawiający wymaga aby czas reakcji serwisu Wykonawcy na zgłoszenie błędu, awarii lub nieprawidłowego funkcjonowania oprogramowania, był nie krótszy niż 3 godziny robocze.
33. Zamawiający wymaga aby czas usunięcia lub naprawienia zgłoszonych błędów, awarii lub nieprawidłowego funkcjonowania oprogramowania był nie dłuższy niż 8 godzin roboczych.