Załącznik 2

Szczegółowy opis przedmiotu zamówienia Systemu Antyspamowego dla NCBR

1. Opis przedmiotu zamówienia

   1.1. Przedmiotem zamówienia jest System Antyspamowy
   1.2. W zakres przedmiotu zamówienia wchodzi:
   a) konfiguracja i uruchomienie systemu
   b) dostarczenie licencji systemu antyspamowego

2. Wymagania dotyczące systemu Antyspamowego:

   2.1. Rozwiązanie musi oferować ochronę « Predictive Defense » opierającą się o nowoczesne mechanizmy analizy. Rozwiązania opierające się jedynie o technologie fingerprint/sygnature oraz reputację nie zostaną wzięte pod uwagę.
   2.2. Rozwiązanie jest w stanie filtrować przychodzący i wychodzący ruch pocztowy
   2.3. Rozwiązanie musi identyfikować i blokować szczegółowe kategorie zagrożeń:
   a) spam : 3 poziomy High, Medium, Low
   b) malware'y m.i ransomware'y
   c) phishing
   d) business email compromises (spear phishing)

   2.4. Rozwiązanie musi wykrywać złośliwe skrypty i macro ukryte w najczęściej udostępnianych typach plików, np. Pliki PDF i Office
   2.5. Rozwiązanie musi blokować wiadomości e-mail na podstawie formatu załącznika;
   Lista zabronionych formatów może być skonfigurowana dobrowolnie przez klienta.
   2.6. Rozwiązanie musi wykrywać ataki opierające się o mechanizmy :
   a) Domain spoofing
   b) Alias spoofing
   c) Similar address

   2.7. Rozwiązanie musi posiadać zaawansowane technologie do wykrywania ataków typu Spear Phishing, nie tylko oparte o technologie SPF.

2.8. Rozwiązanie musi posiadać zrozumiały i prosty w obsłudze dla administratora Webowy interfejs graficzny do konfiguracji i administracji, nie wymagający wielodniowego szkolenia oraz codziennej kompleksowej administracji
2.9. Rozwiązanie musi zapewniać przestrzeń kwarantanny dla każdego konta użytkownika
2.10. Rozwiązanie powinno obsługiwać white-listing i black-listing zarówno na poziomie administratora, jak i użytkownika
2.11. Rozwiązanie musi być dostępne na głównych platformach wirtualizacyjnych, tj: VMWare, Hyper-V
2.12. Rozwiązanie musi współdziałać z LDAP i Active Directory w celu zarządzania kontami użytkowników
2.13. Rozwiązanie musi rejestrować logi, związane zarówno z analizą poczty e-mail, jak i zdarzeniami systemowymi
2.14. Rozwiązanie powinno mieć możliwość udostępniania raportów statystycznych
2.15. Rozwiązanie musi obsługiwać protokół Syslog, w celu przekazywania logów do zewnętrznych systemów
2.16. Rozwiązanie musi posiadać funkcjonalność szyfrowania TLS.
2.17. Rozwiązanie obsługuje SPF oraz DKIM
2.18. Rozwiązanie musi obsługiwać protokół SNMP
2.19. Rozwiązanie może zapobiec problemom Single Point Of Failure
2.20. Rozwiązanie może działać w środowisku load-balanced