

Dodatek nr 8- Funkcjonalności dodatkowe

Za każde spełnione wymaganie Wykonawca dostanie 3 pkt. Maksymalnie można uzyskać 30 pkt.

|  |  |  |
| --- | --- | --- |
| **FUNKCJONALNOŚCI DODATKOWE** | **PARAMETRY OFEROWANE: Potwierdzenie Wykonawcy TAK lub NIE** | |
| **TAK** | **NIE** |
| 1. System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji:    1. Sygnatur ochronnych (np. IPS);    2. Sygnatur aplikacyjnych (nowych definicji aplikacji);   (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa – funkcja ta musi być wbudowana w firewall i nie może wymagać korzystania z rozwiązań trzecich. |  |  |
| 1. System zabezpieczeń firewall pozwala na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach, przy czym w przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji. |  |  |
| 1. System zabezpieczeń firewall posiada moduł inspekcji antywirusowej, który za pomocą lokalnych sygnatur i definicji wirusów umożliwia inspekcje plików archiwalnych pod kątem zawartości złośliwego oprogramowania, min: archiwa typu zip, gzip, bz2, rar, tar, 7zip. System musi mieć możliwość zablokowania w locie w/w typów archiwów jeśli w środku znajduje się plik, który poprzez sygnatury AV jest zaklasyfikowany jako niebezpieczny. |  |  |
| 1. System zabezpieczeń firewall musi posiadać moduł filtrowania poczty elektronicznej pod kątem spamu. Filtrowanie musi obejmować ruch przychodzący i wychodzący. |  |  |
| 1. System zabezpieczeń firewall musi zapewniać wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie sprzętowym. Logowanie zdarzeń w urządzeniu nie może powodować degradacji wydajności tego urządzenia i obciążenie procesora przekazującego ruch nie może degradować wydajności zarządzania urządzeniem. |  |  |
| 1. System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności zakupu jakichkolwiek dodatkowych komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |  |  |
| 1. System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |  |  |
| 1. System zabezpieczeń firewall musi realizować w ramach oferowanych subskrypcji przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box”, minimum następujących typy plików (exe, dll, pdf, msoffice, java, jpg, swf, apk, js, vbs, ps1, eml), które będą mogły zostać poddane pełnej analizie behawioralnej. |  |  |
| 1. System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |  |  |
| 1. System zabezpieczeń firewall musi umożliwiać zdefiniowanie stron WWW i serwisów do których użytkownicy mogą wysyłać swoje poświadczenia. W przypadku próby wysłania poświadczeń do niezaufanej strony lub serwisu ruch musi zostać zablokowany. |  |  |

|  |
| --- |
|  |