Załącznik Nr 1 do zarządzenia Nr 8/2023/BBIICD

Prezesa Narodowego Funduszu Zdrowia

z dnia 16 stycznia 2023 r.

Warunki akceptacji

1) Podstawowym systemem, który może być objęty finansowaniem jest system kopii zapasowych wszystkich systemów służących udzielaniu świadczeń opieki zdrowotnej u świadczeniodawcy. System kopii zapasowych musi umożliwiać realizację kopii zapasowej za pomocą streamera lub biblioteki taśmowej. Kopie te muszą być przechowywane w innej lokalizacji niż środowisko produkcyjne, np. inny budynek, a w przypadku braku takiej możliwości, w pomieszczeniu oddalonym od serwerowni. System ten powinien umożliwiać odtworzenie kopii zapasowej i testowe odtworzenie systemów w środowisku testowym. Cały proces musi być opisany procedurą stanowiącą element dokumentacji bezpieczeństwa. Możliwe jest również wdrożenie innego systemu wykonywania kopii zapasowych, który nie będzie oparty na taśmach magnetycznych, jednak musi on być skonfigurowany przez osobę posiadającą kompetencje z zakresu realizacji systemów kopii zapasowych, gwarantującą wykonanie skutecznych kopii zapasowych oraz konfigurację separacji sieciowej.

Kryterium akceptacji:

Efektem realizacji musi być przeprowadzenie audytu systemu kopii zapasowej, którego wynik potwierdzi utworzenie odmiejscowionej kopii zapasowej i odtworzenie z niej kompletnego systemu oraz wykonanej dokumentacji bezpieczeństwa.

2) Jeśli świadczeniodawca posiada powyższy system, o którym mowa w pkt 1, może w ramach finansowania zrealizować zakup lub rozwój systemów Firewall pozwalający analizować przesyłane pakiety pod względem ich treści wraz z wdrożeniem w infrastrukturze teleinformatycznej świadczeniodawcy przez osobę posiadającą kompetencje z zakresu bezpieczeństwa sieci.

Kryterium akceptacji:

Efektem wdrożenia musi być wykonanie zewnętrznych skanów podatności, które wykażą brak podatności krytycznych oraz które mogą doprowadzić do incydentu poważnego w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863, z późn. zm.).

Wnioskodawca jest zobowiązany do utwardzania konfiguracji do momentu uzyskania wskazanego efektu. Wyeliminowanie podatności musi być potwierdzone przez audyt bezpieczeństwa.

3) Jeśli świadczeniodawca posiada już systemy, o których mowa w pkt 1 i 2, może w ramach finansowania zakupić system lub rozwój systemu poczty elektronicznej wraz z systemem bezpieczeństwa, który będzie obejmował mechanizmy SPF, DMARC, DKIM, antyspam oraz ochronę antywirusową.

Kryterium akceptacji:

Efektem realizacji musi być przeprowadzenie audytu systemu poczty elektronicznej, którego wynik potwierdzi skuteczność wdrożenia SPF, DMARC, DKIM, antyspam oraz ochronę antywirusową.

4) Jeśli świadczeniodawca posiada już systemy, o których mowa w pkt 1-3, może w ramach finansowania zrealizować zakup lub rozwój systemów opartych na rozwiązaniach co najmniej klasy Endpoint Detection and Response w architekturze serwera - klient na wszystkich stacjach roboczych oraz serwerach świadczeniodawcy wraz z wdrożeniem w infrastrukturze teleinformatycznej świadczeniodawcy przez osobę posiadającą kompetencje z zakresu realizacji systemów antywirusowych.

Kryterium akceptacji:

Efektem realizacji musi być przeprowadzenie audytu systemu Endpoint Detection and Response, na wszystkich stacjach roboczych oraz serwerach świadczeniodawcy, który potwierdzi prawidłowość wdrożenia systemu.

Słownik skrótów:

SPF: Sender Policy Framework - niekomercyjny projekt mający na celu wprowadzenie zabezpieczenia serwerów SMTP przed przyjmowaniem poczty z niedozwolonych źródeł. Ma to pozytywnie wpłynąć na ograniczenie liczby wiadomości mailowych będących spamem,

DMARC: (Domain-based Message Authentication Reporting and Conformance) - możliwość ochrony domeny przed nieautoryzowanym użyciem, powszechnie znanym jako fałszowanie wiadomości e-mail,

DKIM: (DomainKeys Identified Mail) - metoda łączenia domeny internetowej z wiadomością e-mail, która pozwala organizacji brać odpowiedzialność za treść e-maila. Sygnatura DKIM zabezpiecza przed podszywaniem się pod nadawcę z innych domen.