

**Część 2**

**PARAMETRY MINIMALNE:**

1. **Wdrożenie systemów teleinformatycznych**

Wdrożenie oprogramowania do wykonywania kopii zapasowych:

1: Planowanie i Przygotowanie

* Określenie wymagań dotyczących backupu i replikacji, w tym ilość danych do przechowywania, czas przywracania, dostępność i inne czynniki.
* Weryfikacja posiadania odpowiedniej ilości przestrzeni dyskowej i zasobów sieciowych do przechowywania kopii zapasowych.
* Pobranie niezbędnego oprogramowania do wykonywania kopii zapasowych i przeczytanie jego dokumentacji.

2: Instalacja i Konfiguracja

* Uruchomienie instalatora wybranego oprogramowania do wykonywania kopii zapasowych na wybranym serwerze.
* Postępuj zgodnie z kreatorami instalacji, akceptując licencję, wybierając komponenty do zainstalowania i konfigurując ustawienia.
* Konfiguracja połączenia ze swoim środowiskiem wirtualizacji

3: Konfiguracja Backupu

* Konfiguracja planów backupu, określając harmonogramy, miejsca przechowywania i inne parametry.
* Wybranie, które maszyny wirtualne lub inne zasoby będą chronione za pomocą kopii zapasowych.
* Ustawienie retencji danych i polityki przechowywania, aby dostosować je do wymagań firmy.

4: Konfiguracja Replikacji (opcjonalnie)

* Konfiguracje odpowiedniego zadania replikacji, określając maszyny wirtualne źródłowe i docelowe, harmonogramy i inne parametry.
* Weryfikacja dostępności docelowego środowiska na przyjęcie replikowanych maszyn wirtualnych.

5: Testowanie i Wdrażanie

* Przetestowanie planów backupu i replikacji, aby upewnić się, że są one zgodne z oczekiwaniami i spełniają wymagania czasu przywracania.
* Wdrożenie skonfigurowanych i przetestowanych planów na produkcji, monitorując ich wydajność i skuteczność.

6: Monitorowanie i Administracja

* Regularne monitorowanie wykonywanych kopii zapasowych i replikacji, w celu weryfikacji ich poprawności i zgodności z planem.
* Weryfikacja raportów i dzienników zdarzeń oprogramowania do wykonywania kopii zapasowych, aby szybko reagować na jakiekolwiek problemy.

**Usługi wdrożeniowe realizowane będą hybrydowo, częściowo w siedzibie Zamawiającego, częściowo przy pomocy zdalnego połączenia z systemami Zamawiającego.**

1. **Wdrożenie systemów teleinformatycznych**

**Dostawa oraz wdrożenie oprogramowania typu SIEM**

Zamawiający na potrzeby instalacji i wdrożenia udostępni infrastrukturę na serwerach zwirtualizowanych, wg. specyfikacji uzgodnionych z Wykonawcą. Czynności związane z wdrożeniem systemu będącego przedmiotem umowy będzie wykonywał Wykonawca. Instalacja systemu przez Wykonawcę odbywać się będzie z wykorzystaniem środków komunikacji elektronicznej.

Wykonawca zobowiązuje się do dostarczenia kompleksowego oprogramowania typu Security Information and Event Management (SIEM), które będzie spełniało poniższe wymagania funkcjonalne i techniczne.

1. Funkcjonalności systemu.
2. Monitorowanie występujących zdarzeń (logów) w trybie ciągłym.
3. Zbieranie zdarzeń z serwerów wirtualnych, fizycznych, Active Directory, przełączników oraz innego rodzaju urządzeń, które są oraz zostaną podłączone do infrastruktury zamawiającego.
4. Agregacja oraz korelacja logów.
5. Wykrywanie ataków typu brute force na różne usługi.
6. Wykrywanie i przeciwdziałanie złośliwemu oprogramowaniu.
7. Analiza logów w oparciu o wbudowane reguły bezpieczeństwa.
8. Konfiguracja oprogramowania do przechowywania logów z kluczowych zasobów przez okres 24 miesięcy zgodnie z rozporządzeniem KRI §21 pkt. 4 „Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.”
9. Panel do wyszukiwania zdarzeń.

1. Wdrożenie systemu.
2. Wykonawca będzie odpowiedzialny za instalację i konfigurację oraz optymalizację środowiska systemu w infrastrukturze Zamawiającego oraz opiekę serwisową i wsparcie techniczne przez okres 30 dni.
3. Wykonawca przeprowadzi instruktaż stanowiskowy dla Administratorów (zarządzających systemem), co najmniej w n/w zakresie:
4. Przedstawienie architektury systemu.
5. Omówienie procedur obsługi administracyjnej systemu;
6. omówienie możliwości funkcjonalnych, zakresu dostępnych funkcji oraz ograniczeń systemu;
7. przekazanie informacji na temat konfiguracji i zarządzania systemem;
8. instruktaż stanowiskowy musi obejmować część teoretyczną i praktyczną.
9. **Testy penetracyjne**

Wykonawca posiada potencjał techniczny i osobowy niezbędny do wykonania zamówienia.

Potencjał techniczny przedstawia się poprzez posiadanie narzędzi takich jak automatyczny skaner podatności posiadający funkcje pozwalające na:

* wykonanie skanowań z wykorzystaniem wbudowanych szablonów;
* skanowanie sieciowe (wykrywanie otwartych portów i rozpoznanie uruchomionych na nich usług, wskazywanie listy podatności na wykryte usługi);
* weryfikacje domyślnych haseł według zadanego słownika;
* skanowanie systemów operacyjnych z uwierzytelnieniem (sprawdzenie wersji systemu, zainstalowanych na nim aplikacji, brakujących aktualizacji, wskazywanie listy podatności na wykryte systemy i aplikacje) oraz weryfikację uprawnień zadanego użytkownika;
* ustawienia harmonogramu skanowań;
* możliwość porównania wyników poszczególnych skanowań;
* możliwość konfigurowania zawartości raportu ze skanowania oraz dobieranie różnych formatów wyjściowych raportów (w tym HTML, CVS i XML);
* możliwość wyświetlania wyników na bieżąco oraz możliwość grupowania podobnej klasy podatności i możliwość sortowania po IP i podatnościach.

Aplikacje do testów stron i aplikacji internetowych posiadającej funkcje pozwalające na:

* przechwytywanie wszystkich zapytań i odpowiedzi pomiędzy przeglądarką a aplikacją docelową, nawet gdy używany jest HTTPS;
* przeglądanie, edytowanie oraz upuszczanie pojedynczych wiadomości, w celu manipulacji komponentami aplikacji po stronie serwera lub klienta;
* dodawanie adnotacji do poszczególnych elementów w celu ich oznaczenia do późniejszego sprawdzenia;
* wykonywanie różnych automatycznych modyfikacji odpowiedzi w calu ułatwienia testowania;
* tworzenie reguł dopasowywania i zastępowania do automatycznego stosowania własnych modyfikacji do żądań i odpowiedzi przechodzących przez serwer Proxy;
* precyzyjna konfiguracja reguł przechwytywania wiadomości;
* możliwość wyeliminowania ostrzeżeń bezpieczeństwa przeglądarki, mogących się pojawiać podczas przechwytywania połączeń HTTPS;
* pokazanie całej zawartości odkrytej podczas testowania umieszczana na mapie skanowanej witryny. Treść prezentowana w widoku drzewa, odpowiadającego strukturze stron URL;
* żądania i odpowiedzi dostępne w edytorze http;
* narzędzie do ręcznej edycji i ponownego wstawiania żądań;
* narzędzie do analizy statystycznej tokenów sesji;
* możliwość zapisu pracy na poszczególnych etapach w czasie rzeczywistym oraz  powrót do zapisanego miejsca;
* biblioteka konfiguracji do szybkiego uruchomienia ukierunkowanego skanowania z różnymi ustawieniami;
* możliwość ręcznego umieszczania punktów wstawiania w dowolnych miejscach żądania, w celu poinformowania skanera o niestandardowych formatach danych i wejściach;
* skanowanie na żywo podczas przeglądania, zapewniające pełną kontrolę nad działaniami wykonywanymi dla żądań;
* możliwość analizy docelowej aplikacji internetowych.
* narzędzie do automatycznego przechwytywania szczegółowych wyników o niestandardowych atakach na aplikacje.

Potencjał osobowy przedstawia się poprzez posiadanie przez osoby testujące łącznie takie certyfikaty jak: OSCP (offensice security), CEH (EC-Council), Burp Suite Certified Practitioner (PortSwinger), eWPTX (eLearnSecurity), eCPPT (eLearnSecurity). Skanowania nie mogą być realizowane tylko z wykorzystaniem narzędzi automatycznych, konieczna jest manualna weryfikacja podatności znalezionych w testach automatycznych.  Przeprowadzenie testów nie może wymagać od Zamawiającego zakupu żadnych dodatkowych licencji lub wyposażenia.

W ramach przeprowadzonych testów penetracyjnych infrastruktury, Wykonawca wykona:

1. Rekonesans.
2. Zgromadzenie wszystkich dostępnych publicznie informacji nt. osób reprezentujących instytucję w celu stworzenia potencjalnej bazy loginów i haseł.
3. Zgromadzenie informacji nt. zasobów instytucji dostępnych publicznie (strona internetowa, serwer www, serwer ftp, inne usługi).
4. zgromadzenie informacji nt. potencjalnie niejawnych zasobów dostępnych dla wyszukiwarek internetowych.
5. Sprawdzenie występowania w wyciekach znalezionych loginów.
6. Enumeracja zasobów.
7. Analiza zasobów zidentyfikowanych w pkt. 1 w celu określenia precyzyjnej listy aplikacji (wraz z określeniem ich wersji) działających w ramach usług.
8. Skanowanie publicznej infrastruktury.
9. Skanowanie wewnętrznej infrastruktury z wykorzystaniem automatycznego skanera podatności.
10. Sprawdzenie udostępnionych w sieci wewnętrzej plików i folderów w szczególności pod kątem występowania danych wrażliwych.
11. Analiza dostępnych wewnątrz sieci, usług, protokołów i urządzeń.
12. Eksploitacja.
13. Próba zalogowania do zidentyfikowanych zasobów, m.in. z użyciem list stworzonych w pkt. 1, także logowanie typu brute-force oraz domyślnych haseł.
14. Wykorzystanie podatności ujawnionych na etapie enumeracji (cve dla znanych wersji aplikacji) – po uzgodnieniu z Zamawiającym.
15. Analiza konfiguracji dostępnych środowisk w celu wykorzystania jej błędów (analiza hardeningu, architektury sieci, błędy w konfiguracji serwera www i architektury aplikacji internetowych oraz innych usług).
16. Eskalacja uprawnień.
17. Wykorzystanie zasobów skompromitowanych w pkt. 3 w celu ewentualnego podniesienia uprawnień.
18. Rozpoznanie zasobów wewnętrznych, przechodzenie na inne środowiska dostępne ze skompromitowanych w pkt.3 zasobów (lateral movement).
19. Raport z testu penetracyjnego.

Wykonawca dostarczy raport zawierający:

1. Podsumowanie dla kierownictwa.
2. Opis zakresu wykonanych prac.
3. Wyłączenia z testów jeżeli były.
4. Listę danych zebranych w trakcie rekonesansu (w tym listę zidentyfikowanych adresów IP w sieci wewnętrznej).
5. Listę znalezionych podatności wraz z określoną dla niej waga zgodnie z ze standardem Common Vulnerability Scoring System Version 4.0 oraz modelem STRIDE.
6. Szczegółowy opis znalezionych podatności.
7. Zalecenia naprawy nieprawidłowości bądź mitygacji zagrożeń z nich wynikających.