

Wykonanie audytu bezpieczeństwa informacyjnego i podatności sieci w kontekście UKSC, KRI oraz RODO/UODO w ramach projektu: „eCareMed – rozwój cyfrowych usług medycznych w Wojewódzkim Szpitalu Specjalistycznym Nr 2 w Jastrzębiu - Zdroju”

Szczegółowy opis przedmiotu zamówienia

I. Podstawowe informacje:

Przedmiotem zamówienia jest **Wykonanie audytu bezpieczeństwa informacyjnego i podatności sieci w kontekście UKSC, KRI oraz RODO/UODO w ramach projektu: „eCareMed – rozwój cyfrowych usług medycznych w Wojewódzkim Szpitalu Specjalistycznym Nr 2 w Jastrzębiu - Zdroju”.**

II. Opis przedmiotu zamówienia:

W ramach audytu Wykonawca zrealizuje następujące zadania:

- Analiza topologii siec+i,
- Weryfikacja podziału LAN na strefy sieciowe (w tym wykorzystanie firewallei oraz VLAN/PVLAN),
- Określenie usług działających w sieci LAN,
- Poszukiwanie podatności w kilku wybranych podsieciach (przykładowo: detekcja),
- Weryfikacja dostępnych mechanizmów uwierzytelniania dostępnych w sieci,
- Weryfikacja mechanizmów ochronnych w warstwie 2 i 3 modelu OSI,
- Weryfikacja kilku podstawowych zasad bezpieczeństwa na wybranych kilku stacjach roboczych,
- Weryfikacja dostępu do Internetu z LAN,
- Szczegółowa analiza wybranej komunikacji sieciowej,
- Weryfikacja zasad utrzymania sieci,
- Weryfikacja podatności sieci na zagrożenia typu Denial of Service,
- Weryfikacja podatności sieci na zagrożenia związane z umyślnymi zakłóceniami,
- Weryfikacja podatności sieci na zagrożenia związane z podszywaniem się pod elementy infrastruktury i rozsyłaniem do klientów sieci fałszywych ramek kontrolnych,
- Weryfikacja odporności sieci na ataki związane z przeciążaniem zasobów sieciowych, takich jak punkty dostępowe i kontroler sieci bezprzewodowej,
- Weryfikacja podatności bezpieczeństwa zmierzająca do pozyskania haseł dostępu do sieci poprzez podstawienie elementów infrastruktury punktu dostępowe,
- Skanowaniu sieci w poszukiwaniu wszystkich podłączonych hostów, wykryciu czy jest dostęp do innych podsieci z danej podsieci, wykryciu usług działających na hostach podłączonych do sieci, wykryciu podatności na wybranych hostach w sieci,
- Wykonanie zewnętrznych i wewnętrznych testów penetracyjnych infrastruktury oraz aplikacji sieciowych,
- Wykonanie zewnętrznych i wewnętrznych testów penetracyjnych i analiza bezpieczeństwa interakcyjnych aplikacji Webowej,
- Analiza bezpieczeństwa w obszarze utrzymania ciągłości działania ważnych procesów sieci.
- Analiza poprawności projektu i konfiguracji zabezpieczeń sieciowych (firewall, WAF, DLP, itp.) w zakresie zgodności z zasadami projektowania zabezpieczeń, normami bezpieczeństwa oraz dobrymi praktykami,
- Wskazanie potencjalnych, dodatkowych metod ochrony sieci,

Audyt wykonywany będzie w sposób manualny oraz automatyczny za pomocą specjalistycznych narzędzi oraz własnych skryptów przygotowanych na podstawie wiedzy i doświadczeń.

- Analiza i badanie dokumentacji,

- Procedur zarządzania systemami teleinformatycznymi,
- Procedur planowania aktualizacji systemów teleinformatycznych,
- Zasad ochrony przed oprogramowaniem szkodliwym, w tym weryfikacja zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania,
- Procedur zarządzania historią zmian,
- Procedur zarządzania kopiami zapasowymi,
- Procedur zabezpieczania nośników,
- Polityk kontroli dostępu do systemów,
- Zasad odpowiedzialności użytkowników,
- Procedur dostępu do systemów operacyjnych,
- Procedur dostępu i kontroli do usług internetowych,
- Zasad zarządzania hasłami,
- Zasad stosowania zabezpieczeń kryptograficznych,
- Zasad kontroli eksploatowanego oprogramowania,
- Procedur kontroli zabezpieczeń komputerów przenośnych,
- Bezpieczeństwa sieci LAN, WAN, WiFi,
- Zasad użytkownika Internetu,
- Zasad użytkownika systemów monitorujących,
- Procedur rejestracji błędów,
- Zasad funkcjonowania metod autoryzacji na stacjach roboczych,
- Analiz stopnia zabezpieczenia stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe,
- Weryfikacji zasad postępowania z urządzeniami przenośnymi w szczególności tymi, na których przetwarzane są dane osobowe,
- Zasad wytycznych związanych z użytkowaniem sprzętu poza siedzibą,
- Zasad funkcjonowania procedur bezpiecznego przekazywania sprzętu,
- Niszczanie niepotrzebnych nośników,
- Zasad funkcjonowania poprawności składowania danych elektronicznych,
- Analiz procedur backupu (sposób wykonywania kopii bezpieczeństwa, zakres kopiowanych danych, przechowywanie kopii bezpieczeństwa) oraz procesu ich administracji,
- Analiz planów ciągłości działania,
- Weryfikacja zapisów umów ze stronami trzecimi (SLA),
- Organizacji i zakresu działania archiwów zakładowych,
- Dokumentacji systemu zarządzania ciągłością działania usługi kluczowej wytworzona zgodnie z wymaganiami normy PN-EN ISO 22301,
- Dokumentacji technicznej systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej,
- Dokumentacji wynikająca ze specyfikacji świadczonej usługi kluczowej w danym sektorze lub podsektorze tym zasady bezpieczeństwa obsługi.

Wynikiem przeprowadzonych audytów i testów będzie raport po-audytowy w standardzie ENISA zawierający:

- Opis wszystkich elementów, które zostały poddane audytowi,
- Podział podatności ze względu na ryzyko,
- Wskazanie zaleceń, rekomendacji, najlepszych praktyk – dla każdej znalezionej podatności,
- Wylistowanie wszystkich podatności ze względu na ryzyko,
- Określenie bezpieczeństwa informatycznego w Szpitalu poprzez wskazanie ilości i rodzaju znalezionych podatności,
- Rekomendacje poaudytowe.