Krótki opis tematu

Tematem naszego projektu jest stworzenie strony internetowej obsługującej ,,Ogólnopolski Rejestr Ciągłych metod Nerkozastępczych u Dzieci" dla placówek medycznych w całej Polsce (placówek biorących udział w projekcie ma być niewiele – około 10). Technologie końcowe, w jakich zdecydowaliśmy się realizować projekt to ASP MVC .NET (z HTTPS) oraz PostrgeSQL. Użytkownikami tego systemu będą lekarze (wprowadzające dane medyczne) oraz administratorzy (akceptują nowe osoby, zarządzają statystykami).

Odniesienie do pierwszego spotkania

Po pierwszym spotkaniu otrzymaliśmy kilka istotnych wskazówek i poleceń, które wykonaliśmy w tym etapie projektu. Na rozmowie z klientką podjęliśmy temat odnośnie specjalistycznych danych medycznych i danych osobowych. Otrzymaliśmy informację, że w ciągu miesiąca nie ma możliwości otrzymania pisemnego potwierdzenia od prawnika odnośnie danych poufnych oraz konieczności ich specjalnego zabezpieczenia. Dowiedzieliśmy się jednak, że wszystko będzie konsultowane w odpowiednim czasie, ponieważ musi dojść tutaj również do spotkań pomiędzy uczelniami oraz zatwierdzenia tego w wielu płaszczyznach, jednak to wykracza już po za ramy czasowe i zakres naszego projektu. Na sam czas projektowy nie otrzymamy żadnych danych od osób fizycznych, będą to tylko dane testowe służące do sprawdzenia poprawności działania systemu – sam system jednak staramy się przygotować na posiadanie takich danych, dlatego dane będą szyfrowane.

Zdecydowaliśmy się również na postawienie bazy danych w kontenerze, jednak tak jak nam Pan przekazał na poprzednim spotkaniu pamięć do tego kontenera będzie zewnętrzną pamięcią, aby mieć możliwość przebudowania kontenera (np. na łatkach bezpieczeństwa).

Model zagrożeń

W ramach projektu oprócz zastanowienia się nad architekturą i funkcjonalnością, konieczne jest również przemyślenie bezpieczeństwa systemu końcowego.

Zabezpieczenie dostępu do systemu dla osób nie powiązanych z dziedziną projektu – aby móc otrzymać dostęp do systemu istnieją tylko dwie możliwości: założenie konta i konieczność akceptacji przez administratora, który sprawdza daną osobę w rejestrze lekarzy oraz dodanie osoby przez administratora (wynika to z tego, że z systemu mogą korzystać osoby, które nie są dobrze obyte z systemami informatycznymi).

Dostęp do wszystkich danych zgromadzonych w systemie posiadają tylko administratorzy systemu – administratorzy będą zawsze zaufanymi i sprawdzonymi osobami. Będzie to też bardzo nieliczna grupa, która wykorzysta informację do poprawienia jakości leczenia.

Wykradnięcie danych z bazy danych – aby zapobiec niebezpiecznym wyciekom poufnych danych wykorzystamy szyfrowanie bazy danych, które w jak największym stopniu ma przeszkodzić w dostępie do danych

Zabezpieczenie hasła – jak wiemy w obecnym czasie złamanie krótkich i słabych haseł jest dość proste, dlatego nałożymy obostrzenia na hasło, aby zawierało przynajmniej 8 znaków, w tym przynajmniej po jednej małej i dużej literze, liczbie i znaku specjalnym. Samo hasło będzie przechowywane również jako hash, aby zmaksymalizować jego bezpieczeństwo.

Komunikacja między klientem a serwerem – wykorzystamy protokół HTTPS, który szyfruje komunikację przy pomocy szyfrowania protokołu TLS. Zapobiegnie to przechwyceniu bądź modyfikacji przesyłanych danych.

Ataki DDoS – niestety żaden system nie jest w stanie się w pełni przed nimi zabezpieczyć. W naszym systemie ciężko zastosować jakąkolwiek metodę, umożliwiającą ograniczenie takich ataków, jednak zakładamy, że możliwość takiego ataku na nasz system nie jest bardzo duża. W razie takiego przypadku administrator mógłby odciąć ruch sieciowy, gdy ilość zapytań przekroczy np. 100 na minutę.

Phishing – w naszym przypadku może być zastosowany do ataku na administratorów systemu, mające na celu otrzymanie ich uprawnień na stronie i dostęp do danych pacjentów. Metodą zapobiegania jest tutaj jedynie edukacja, dokładne sprawdzanie adresata oraz tekstu wiadomości.

Atak na sieć wewnętrzną klienta – w razie takiego ataku nie jesteśmy w stanie nic zrobić, bezpieczeństwo pod tym względem stoi po stronie klienta.

Zaopatrzenie strony w certyfikat SSL – zarekomendujemy klientce, aby w raz z wdrożeniem zaopatrzyć stronę internetową w certyfikat SSL, który zabezpiecza transmisję poufnych danych.

Tworzenie kopii zapasowych danych – aby móc odtworzyć stan sytemu ważne jest tworzenie kopii zapasowych danych, również zarekomendujemy podane rozwiązanie naszej klientce.

Wdrożenie oraz serwis

Nasz zespół nie będzie zajmował się wdrożeniem całego projektu, z racji na to, że wykracza to za zakres projektu oraz jego czas. Wdrożeniem oraz utrzymaniem systemu, jeśli taki będzie finalny efekt projektu, zajmie się mgr inż. Kamil Deja z Instytutu Informatyki na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej. Jest on również opiekunem naszego projektu i taką informację uzyskaliśmy od niego. Obsługą incydentów i reagowaniem na awarie zajmie się Pan Deja lub ewentualnie osoby wskazane przez niego (nasz zespół nie będzie brał w tym udziału).

Od klientki uzyskaliśmy informację, że w przyszłości nasz system będzie prawdopodobnie rozwijany i personalizowany dla konkretnych placówek.

Administrowanie systemem będzie polegało na dbaniu o ciągłość działania systemu i reagowanie na błędy zgłaszane przez jego użytkowników oraz wprowadzanie poprawek i nowych funkcjonalności.

Utworzony będzie również plik Dockerfile, który będzie budował obraz nowej wersji i montował do niego dane. Wystarczy wtedy uruchomić podany plik, aby zaktualizować obraz to najnowszej wersji.