OWASP - Architektura bezpieczeństwa aplikacji

Wprowadzenie

Ta ściągawka zawiera porady dotyczące wstępnego projektowania i przeglądu architektury bezpieczeństwa projektu.

Wymagania biznesowe

Model biznesowy

- Jaki jest główny cel biznesowy aplikacji?
- W jaki sposób aplikacja będzie zarabiać pieniądze?
- Jakie są planowane etapy rozwoju lub ulepszenia aplikacji?
- W jaki sposób aplikacja jest sprzedawana?
- Jakie kluczowe korzyści oferuje aplikacja dla użytkowników?
- Jakie przepisy dotyczące ciągłości działania zostały określone dla aplikacji?
- Jakie obszary geograficzne obsługuje aplikacja?

Podstawy dotyczące danych

- Jakie dane otrzymuje, tworzy i przetwarza aplikacja?
- Jak te dane mogą być klasyfikowane w kategorie wg ich wrażliwości?
- Jak atakujący może odnieść zyski poprzez przechwycenie lub modyfikację danych?
- Jakie wymagania dotyczące tworzenia i przechowywania danych zostały zdefiniowane dla aplikacji?

Użytkownicy końcowi

- Kim są użytkownicy końcowi aplikacji?

- Jak użytkownicy końcowi korzystają z aplikacji?
- Jakie oczekiwania wobec bezpieczeństwa mają użytkownicy końcowi?

Partnerzy

- Jakie podmioty zewnętrzne dostarczają dane do aplikacji?
- Jakie podmioty zewnętrzne otrzymują dane z aplikacji?
- Jakie podmioty zewnętrzne przetwarzają dane aplikacji?
- Jakie mechanizmy są używane do udostępniania danych podmiotom zewnętrznym poza samą aplikacją (transmisje EDI, przetwarzanie plików FTP, udostępniane przez producenta API itd.)?
- Jakich wymagań bezpieczeństwa wymagają partnerzy?

Administratorzy

- Kto ma możliwości administracyjne w aplikacji?
- Jakie możliwości administracyjne oferuje aplikacja?

Przepisy

- W jakich branżach działa aplikacja?
- Jakie przepisy dotyczące bezpieczeństwa obowiązują?
- Jakie przepisy dotyczące audytu i zgodności obowiązują?
- W jaki sposób zmiany przepisów będą komunikowane, zarządzane i wdrażane w czasie?

Wymagania Infrastruktury

Sieć

- Jakie szczegóły dotyczące routingu, przełączania, firewalla i równoważenia obciążenia (routing, switching, firewalling, load balancing) zostały zdefiniowane?
- Jaki projekt sieci wspiera tę aplikację?
- Jakie podstawowe urządzenia sieciowe wspierają aplikację?

- Jakie są wymagania dotyczące wydajności sieci?
- Jakie prywatne i publiczne łącza sieciowe obsługują aplikację?

Systemy

- Jakie systemy operacyjne obsługują aplikację?
- Jakie wymagania sprzętowe zostały zdefiniowane?
- Jakie szczegółowe informacje dotyczące wymaganych komponentów systemu operacyjnego i potrzeb w zakresie blokowania zostały zdefiniowane?

Monitorowanie infrastruktury

- Jakie wymagania dotyczące monitorowania wydajności sieci i systemu zostały zdefiniowane?
- Jakie są mechanizmy wykrywania złośliwego kodu lub zaatakowanych komponentów aplikacji?
- Jakie wymagania dotyczące monitorowania bezpieczeństwa sieci i systemu zostały zdefiniowane?

Wirtualizacja i eksternalizacja

- Jakie aspekty aplikacji nadają się do wirtualizacji?
- Jakie wymagania wirtualizacji zostały określone dla aplikacji?
- Jakie aspekty produktu mogą być hostowane w modelu chmury obliczeniowej?
- Jeśli ma to zastosowanie, jakie będzie podejście do przetwarzania w chmurze obliczeniowej (zarządzany hosting czy "czysta" chmura, podejście "całkowicie maszynowe" takie jak AWS-EC2, czy podejście oparte na "hostowanej bazie danych" jak AWS-RDS i Azure itp.)?
- W jaki sposób zalety i ograniczenia każdego podejścia będą rozważane i ustalane?

Wymagania Aplikacji

Środowisko

- Jakie frameworki i języki programowania zostały użyte do stworzenia aplikacji?
- Jakie zależności procesu, kodu, lub infrastruktury zostały zdefiniowane dla aplikacji?
- Jakie bazy danych i serwery aplikacji wspierają aplikację?
- W jaki sposób ciągi połączeń, klucze szyfrowania i inne poufne komponenty będą przechowywane, dostępne i chronione przed nieuprawnionym dostępem?

Przetwarzanie danych

- Jakie ścieżki wprowadzania danych obsługuje aplikacja?
- Jakie ścieżki wyjściowe danych obsługuje aplikacja?
- W jaki sposób dane przepływają przez wewnętrzne komponenty aplikacji?
- Jakie wymagania walidacji danych wejściowych zostały zdefiniowane?
- Jakie dane przechowuje aplikacja i w jaki sposób?
- Jakie dane są zaszyfrowane lub mogą wymagać zaszyfrowania i jakie kluczowe wymagania dotyczące zarządzania zostały zdefiniowane?
- Jakie istnieją możliwości wykrywania wycieku wrażliwych danych?
- Jakie wymagania dotyczące szyfrowania zostały określone dla przesyłanych danych - w tym transmisji przez sieć WAN, LAN, SecureFTP lub publicznie dostępne protokoły, takie jak http: i https :?

Dostęp

- Jakie poziomy uprawnień użytkownika obsługuje aplikacja?
- Jakie wymagania dotyczące identyfikacji użytkownika i uwierzytelniania zostały zdefiniowane?
- Jakie wymagania dotyczące autoryzacji użytkowników zostały zdefiniowane?

- Jakie wymagania dotyczące zarządzania sesją zostały zdefiniowane?
- Jakie wymagania dostępu zostały zdefiniowane dla URI i zgłoszeń serwisowych?
- Jakie ograniczenia dostępu użytkownika zostały zdefiniowane?
- W jaki sposób zarządzane są tożsamości użytkowników podczas transakcji?

Monitorowanie Aplikacji

- Jakie wymagania dotyczące audytu aplikacji zostały zdefiniowane?
- Jakie wymagania dotyczące monitorowania wydajności aplikacji zostały zdefiniowane?
- Jakie wymagania dotyczące monitorowania bezpieczeństwa aplikacji zostały zdefiniowane?
- Jakie zostały zdefiniowane wymagania dotyczące obsługi i rejestrowania błędów aplikacji? Jakie procesy zostały zastosowane by pokazać użytkownikowi końcowemu tylko minimalne wymagane informacje o błędzie, a nie ujawniać aspektów projektowania aplikacji, bezpieczeństwa i implementacji?
- W jaki sposób uzyskuje się dostęp do logów audytu i debugowania, i jak są one przechowywane i zabezpieczane?

Projekt Aplikacji

- Jakie praktyki przeglądu projektu aplikacji zostały zdefiniowane i wykonane?
- W jaki sposób dane pośrednie lub wewnątrzprocesowe są przechowywane w pamięci komponentów aplikacji i w cache?
- Ile poziomów logicznych grupuje komponenty aplikacji?
- Jakie wymagania dotyczące wystawiania, testowania i zapewniania jakości zostały zdefiniowane?

Wymagania programu bezpieczeństwa

Operacje

- Jaki jest proces identyfikowania i usuwania luk bezpieczeństwa w aplikacji?
- Jaki jest proces identyfikowania i usuwania luk bezpieczeństwa w sieci i komponentach systemu?
- Jaki dostęp administratorzy systemów i sieci mają do wrażliwych danych aplikacji?
- Jakie wymagania dotyczące incydentu bezpieczeństwa zostały określone?
- W jaki sposób administratorzy uzyskują dostęp do infrastruktury produkcyjnej by nią zarządzać?
- Jakie kontrole fizyczne ograniczają dostęp do komponentów i danych aplikacji?
- Jaki jest proces przyznawania dostępu do środowiska hostingującego aplikację?

Zarządzanie zmianami

- Jak kontrolowane są zmiany w kodzie?
- Jak kontrolowane są zmiany w infrastrukturze?
- Jak kod jest wdrażany do produkcji?
- Jakie mechanizmy istnieją do wykrywania naruszeń praktyki zarządzania zmianami?

Rozwój oprogramowania

- Jakie dane są dostępne dla developerów do testowania?
- Jak developerzy pomagają przy rozwiązywaniu problemów i debugowaniu aplikacji?
- Jakie wymagania zostały zdefiniowane w zakresie kontroli dostępu do kodu źródłowego aplikacji?
- Jakie procesy bezpiecznego kodowania zostały ustalone?

Korporacyjne

- Jakie wymagania programu bezpieczeństwa korporacyjnego zostały zdefiniowane?
- Jakie szkolenia bezpieczeństwa przechodzą programiści i administratorzy?
- Jaki personel nadzoruje procesy bezpieczeństwa i wymagania związane z aplikacją?
- Jakie procedury wprowadzania i zwalniania pracowników zostały zdefiniowane?
- Jakie wymagania aplikacji wymuszają konieczność egzekwowania zasady rozdziału obowiązków?
- Jakie mechanizmy kontrolne chronią zagrożoną (aplikację? - opuścili tu jedno słowo, z kontekstu domyślam się że chodzi o “aplikację”) w środowisku korporacyjnym przed wpływem na produkcję?
- Jakie wymagania w zakresie zarządzania bezpieczeństwem zostały zdefiniowane?