Planowanie zabezpieczeń aplikacji

Po określeniu struktury danych, następny krok polega na rozważeniu sposobu zabezpieczania danych. Należy rozważyć, jakie dane będą dostępne dla kogo i odwoływać się do zadań, procesów biznesowych i osób, które zostały wymienione w fazie planowania. W tym artykule opisano ogólne pojęcia dotyczące zabezpieczeń dla osób, które nie są z nimi zaznajomione. Więcej informacji na temat technicznych aspektów zabezpieczeń można znaleźć w temacie Role zabezpieczeń i uprawnienia.

Warstwy zabezpieczeń

Konfigurując zabezpieczenia, można skonfigurować cztery różne warstwy zabezpieczeń w aplikacji.

Zabezpieczenia na poziomie aplikacji

Zabezpieczenia na poziomie aplikacji nie chronią lokalizacji przechowywania danych. Sposób zabezpieczania danych będzie różny w zależności od możliwości źródeł danych. W przypadku udostępnienia aplikacji należy upewnić się, że użytkownicy mają również odpowiedni dostęp do danych źródłowych.

Zabezpieczenia na poziomie formularza

W przypadku aplikacji opartych na modelach zabezpieczenia na poziomie formularza pozwalają tylko określonym grupom zabezpieczeń na dostęp do określonych formularzy. Jest to przydatne, jeśli chcesz ograniczyć sposób, w jaki ludzie wprowadzają lub przeglądają dane według ich roli.

Na przykład aplikacja procesu zatwierdzania może mieć jeden formularz dla pracowników do tworzenia i przesyłania wniosku o zatwierdzenie oraz osobny formularz dla osób zatwierdzających do sprawdzenia tego, co zostało przesłane. W tym scenariuszu odpowiednie jest zabezpieczenie na poziomie formularza. Więcej informacji: Kontroluj dostęp do formularzy aplikacji opartej na modelu.

Zabezpieczenia na poziomie rekordu

Zabezpieczenia na poziomie rekordu to typ zabezpieczenia, w którym można przypisać dostęp do określonych rekordów. Załóżmy, że w skoroszycie programu Excel znajduje się już arkusz. Zabezpieczenia na poziomie rekordu umożliwiają konfigurowanie zabezpieczeń poszczególnych wierszy.

Istnieją cztery różne typy dostępu, określane jako CRUD (tworzenie, odczyt, aktualizacja i usuwanie), które można skonfigurować w celu zabezpieczenia na poziomie rekordu:

- **Opcja Utwórz** umożliwia użytkownikowi tworzenie nowych danych (takich jak dodawanie nowego wiersza w programie Excel).
- **Opcja Odczyt** umożliwia użytkownikowi wyświetlanie danych.
- **Aktualizacja** zezwala użytkownikowi na zmianę istniejących już danych. Jest to inna wartość niż w przypadku tworzenia, ponieważ w tworzeniu są dodawane *nowe* dane.
- **Usuwanie** zezwala użytkownikowi na usuwanie danych (takich jak usuwanie wiersza w programie Excel).

Zabezpieczenia na poziomie pola

Zabezpieczenia na poziomie pola są bardziej szczegółowymi zabezpieczeniami w ramach jednego rekordu. To jak konfigurowanie zabezpieczeń dla pojedynczej kolumny w Excelu. Zazwyczaj ma on zbliżony poziom dostępu, jak w przypadku zabezpieczeń na poziomie rekordu, ale na poziomie pola.

Jak różne poziomy zabezpieczeń są powiązane ze sobą?

Wyżej wymienione poziomy zabezpieczeń są podobne do warstw. Projektowanie aplikacji powinno uwzględniać jeden lub kilka z tych poziomów zabezpieczeń, aby odpowiadały Twoim potrzebom. W poniższej tabeli zaprezentowano informacje o poszczególnych poziomach zabezpieczeń w zachowaniu aplikacji.

Poziom zabezpieczeń	**Przykład**
Zabezpieczenia na poziomie aplikacji	Przejdź do „aplikacji Sales”
Zabezpieczenia na poziomie formularza	Dostęp do „karty klienta”
Zabezpieczenia na poziomie rekordu	Dostęp do „Contoso Ltd.”
Zabezpieczenia na poziomie pola	Dostęp do „kwoty przychodu”

Pięć kroków umożliwiających projektowanie zabezpieczeń

Różne poziomy zabezpieczeń mogą pozornie powodować wrażenie złożoności i być przytłaczające, ale można je podzielić na pięć kolejnych kroków:

Krok 1: Określ, kto lub jakie grupy osób (takie jak działy, sekcje lub zespoły) będą miały dostęp do samej aplikacji. Powinien być tym samym zestawem osób, które określił użytkownik w fazie planowania.

Krok 2: wśród użytkowników wskazanych w kroku 1 należy podzielić je na grupy, które będą miały dostęp do ograniczonego typu informacji.

Krok 3: Określ wymagania dotyczące osób, które mogą widzieć rekordy.

Krok 4: Jeśli korzystasz ze źródeł danych innych niż Dataverse— lub usługi, które nie mają uwierzytelniania Office 365 lub Azure Active Directory—, należy rozważyć, jak pozwolić na dostęp do tych systemów. Jeśli użytkownik nie jest odpowiedzialny za te systemy, powinien zasięgnąć opinii administratorów tej usługi.

Krok 5: w zależności od powyższych kroków warto rozważyć sposób zarządzania tymi różnymi grupami. Zalecamy korzystanie z grup zabezpieczeń.

Przykład: zabezpieczenia dotyczące rozwiązania raportu wydatków

W scenariuszu zatwierdzania wydatków wszyscy pracownicy mogą przesyłać raporty z wydatków, więc wszyscy muszą mieć dostęp do aplikacji do tworzenia raportów z wydatków. Ponadto osoby zatwierdzające muszą mieć dostęp do aplikacji zatwierdzania.

Potrzebujemy grupy zabezpieczeń Wszyscy pracownicy, która ma dostęp do aplikacji do raportowania wydatków i wykorzystywanych danych. Potrzebujemy grupy zabezpieczeń Osoby zatwierdzające, która ma dostęp do Aplikacji do zatwierdzania.

Dział księgowy może mieć dostęp do bardziej poufnych danych, takich jak konto bankowe pracowników na potrzeby zwrotu pieniędzy.

Potrzebna jest Grupa zabezpieczeń zespołu księgowości, która jest jedyną grupą zabezpieczeń, która ma dostęp do informacji o banku pracowników.

Najprawdopodobniej nie chcemy, aby pracownicy mogli zobaczyć raporty wydatków, więc musimy skonfigurować zabezpieczenia na poziomie rekordów, aby umożliwić pracownikom dostęp tylko do ich własnych rekordów. Konieczne jest więc również zagwarantowanie, że osoby zatwierdzające będą mogły zobaczyć raporty do zatwierdzenia. Aby widzieć wszystkie raporty o wydatkach (ale nie zmieniać ich), potrzebny jest pracownik działu audytorów.

Potrzebna jest Grupa zabezpieczeń audytorów. Musimy udzielić temu i grupie bezpieczeństwa Zatwierdzających dostępu do wszystkich rekordów, i musimy dać grupie Wszyscy pracownicy dostęp tylko do „rekordów, które tworzę”.