Załącznik nr 2 do OPZ

Strategia bezpieczeństwa informatycznego w zakresie aplikacji mobilnych i portali internetowych

Dokument obejmuje następujące produkty projektu:

Etap 1 - Strategia bezpieczeństwa informatycznego w zakresie aplikacji mobilnych i portali internetowych

NINIEJSZY DOKUMENT STANOWI ROZSZERZENIE STOSOWANEJ W NIZP-PZH STRATEGII BEZPIECZENSTWA SYSTEMÓW INFORMATYCZNYCH NIZP-PZH

Podpisany certyfikatem wystawionym dla Monika Wiktorska (Certyfikat kwalifikowany). Utworzony w dniu: 2023-03-20 16:45:13 +0100

SPIS TREŚCI

Projekt pn. „E-ATESTY uruchomienie e-usług za pośrednictwem dedykowanej aplikacji mobilnej wspieranej interoperacyjną platformą informatyczną” współfinansowanego ze środków EFRR w ramach POPC nr POPC.02.04.00-00-0089/20-00

Definicje

SKRÓT/OKREŚLENIE	WYJAŚNIENIE
Administrator systemu	Osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień.
Autoryzacja	Nadanie uprawnienia na dostęp do konkretnych informacji lub zasobów.
ATiK	Asysta Techniczna i Konserwacja – umowa zapewniająca utrzymanie wybranego systemu informatycznego na uzgodnionym poziomie SLA.
Baza danych	Zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych itp. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze rekordów lub obiektów, w których są zapisane dane jednostkowych obiektów.
BPMN	Business Process Model and Notation, BPMN – graficzna notacja służąca do opisywania procesów biznesowych.
Certyfikat klucza	Sekwencja danych opatrzona przez Ośrodek Certyfikacji podpisami cyfrowymi, która zawiera co najmniej: nazwę Ośrodka Certyfikacji, identyfikator użytkownika, klucz publiczny użytkownika, określenie okresu ważności oraz numer seryjny.
Dane krytyczne	Dane wymagające szczególnej ochrony ze względu na interes Instytutu oraz objęte tajemnicą na podstawie odrębnych przepisów.
Dane osobowe	Dane osobowe oznaczające informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizyczne, wymagające szczególnej ochrony. Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
ESB (Enterprise Service Bus)	Integracyjna szyna danych – warstwa pośrednia w wielowarstwowej architekturze systemów informatycznych umożliwiająca zastosowanie koncepcji SOA (architektura zorientowana na usługi) w środowisku korporacyjnym. Umożliwia dynamiczne przyłączanie i odłączanie usług wchodzących w skład korporacyjnego systemu informatycznego.
Firewall	Urządzenie (lub grupa urządzeń), którego głównym zadaniem jest zabezpieczenie sieci wewnętrznej przed nieuprawnionym dostępem z zewnątrz.
Hasło	Słowo złożone z liter, cyfr lub innych znaków, które musi podać użytkownik, aby mógł korzystać z dostępu do zastrzeżonych zasobów itp. sieci komputerowej, bazy danych, komputera. Hasło jest jednym ze sposobów ochrony danych przed osobami nieupoważnionymi.

Incydent	Nieplanowana przerwa w usłudze informatycznej lub obniżenie jakości usługi informatycznej.
Incydent bezpieczeństwa	Zdarzenie bezpośrednio naruszające bezpieczeństwo systemu lub sieci w systemie informatycznym, bądź mogące spowodować takie naruszenie.
Inspektor Ochrony Danych Osobowych (IODO)	Pracownik wyznaczony przez Instytut odpowiedzialny za organizację ochrony danych osobowych.
Instytut	Narodowy Instytut Zdrowia Publicznego – Państwowy Zakład Higieny.
Jednostki organizacyjne	Funkcjonujące w Instytucie komórki organizacyjne.
Kierownik	Kierownik, dyrektor albo inna osoba pełniąca funkcje kierownicze jednostki organizacyjnej Instytutu.
Klucz publiczny	Parametr przekształcenia matematycznego, który może zostać podany do publicznej wiadomości używany do weryfikacji podpisów cyfrowych utworzonych z użyciem odpowiadającego mu klucza prywatnego. Klucze publiczne są również używane do szyfrowania wiadomości lub plików, które mogą zostać później odszyfrowane z udziałem odpowiadających im kluczy prywatnych.
Koń trojański	Program, który udaje pracę innego legalnego programu, a w międzyczasie wykonuje szereg niepożądanych działań mogących zagrozić bezpieczeństwu systemu
Kopie archiwalne	Kopie plików danych lub plików oprogramowania tworzone na nośniku wymiennym lub dysku twardym komputera, przeznaczone do ich trwałego przechowywania, jak również do odtworzenia danych w przypadku ich utraty lub uszkodzenia.
Kopie bezpieczeństwa	Kopie plików danych lub plików programowania tworzone na nośniku wymiennym lub dysku twardym komputera w celu ich odtworzenia w przypadku utraty lub uszkodzenia danych.
Nośnik komputerowy (wymienny)	Nośnik służący do zapisu informacji, np. płyta CD, wymienny dysk twardy, pendrive.
Plik	Ciąg bajtów posiadający swoją nazwę odróżniającą ją od innych plików i parametry: rozmiar, datę powstania lub datę ostatniej modyfikacji itp.
Pliki logów	Pliki tekstowe (dzienniki) zawierające informacje o czasie i rodzajach zdarzeń występujących w systemie informatycznym.

Podatność	Słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenia.
Proces	Proces biznesowy – seria powiązanych ze sobą działań lub zadań, które prowadzą do osiągnięcia określonego efektu.
Program komputerowy	Zbiór instrukcji, które po umieszczeniu na rozpoznawalnym przez urządzenie nośniku i automatycznym przetłumaczeniu na język zrozumiały dla tego urządzenia powoduje, że osiąga on zdolność do wykonywania danej czynności lub też wykonuje daną czynność.
Przetwarzanie	Operacje lub zestaw operacji wykonywanych na danych lub zestawach danych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
RDBMS (Relational Database Management System)	System pozwalający na zarządzanie relacyjnymi bazami danych stanowiący zestaw programów służących do korzystania z bazy danych opartej na modelu relacyjnym przy wykorzystaniu języka SQL.
Serwer	Wyróżniony specjalistyczny komputer świadczący usługi na rzecz mających z nim łączność innych komputerów itp. przechowujący pliki, pośredniczący w przekazywaniu poczty itp.
Sieć komputerowa	Połączenie komputerów umożliwiające im dzielenie się swoimi zasobami takimi jak: pamięć dyskowa, programy, urządzenia peryferyjne.
Sieć publiczna	Sieć komputerowa zewnętrzna w stosunku do sieci wewnętrznej (lokalnej) Instytutu służąca do świadczenia publicznie dostępnych usług telekomunikacyjnych w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U.2017.1907 t.j.).
Sieć wewnętrzna (lokalna)	Sieć komputerowa będąca własnością Instytutu i zarządzana przez służby informatyczne Instytutu.
Służby informatyczne	Pracownicy Działu Informatycznego oraz wskazani pracownicy jednostek organizacyjnych Instytutu odpowiedzialni za należyte funkcjonowanie systemów informatycznych.
SOA (Service-Oriented Architecture)	Architektura zorientowana na usługi – architektura systemów informatycznych oparta o model usługowy, polegający na udostępnianiu usług sieciowych wspierających procesy biznesowe. Wykorzystuje szynę danych (ESB) jako magistralę integrująca usługi.
SLA (Service Level Agreement)	Poziom świadczenia usługi teleinformatycznej.
Strategia	Opisana w niniejszym dokumencie Strategia Bezpieczeństwa Systemów Informatycznych NIZP-PZH

System autentyfikacji użytkownika	Proces weryfikacji dostępu użytkownika do systemu informatycznego opierający się na identyfikatorach lub hasłach.
System informatyczny (System)	Zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
Teletransmisja danych	Przesyłanie danych przy pomocy dostępnych łączy.
Usługa	Usługa świadczona przez dostawcę usług informatycznych składająca się z połączenia technologii informatycznych, ludzi i procesów.
Uwierzytelnianie	Proces potwierdzenia tożsamości osoby, urządzenia lub integracji danych.
Użytkownik	Osoba użytkująca system informatyczny
Użytkownik wewnętrzny	Pracownik Instytutu lub osoba upoważniona posiadająca uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych, użytkownik z uprawnieniami na poziomie administratora staje się administratorem systemu.
Użytkownik zewnętrzny	Osoba nie będąca pracownikiem Instytutu posiadająca dostęp do usług udostępnianych w sieci zewnętrznej.
Wewnętrzna sieć komputerowa	Własna lub dzierżawiona sieć komputerowa wraz z wszelkimi zasobami informatycznymi będącymi własnością Instytutu.
Wirus	Program, który uaktywniony w pamięci operacyjnej, powoduje wadliwe działanie, zniszczenie lub modyfikację systemu operacyjnego, programu komputerowego lub danych.
Właściciel procesu	Rola w procesie. Osoba zarządzająca, której cele dany proces realizuje. W ramach tej analizy stosowane są dwa pojęcia właściciela procesu: • Właściciel personalny: konkretna osoba, która jest odpowiedzialna za to, że proces przebiega optymalnie w ramach jednostki, za którą odpowiada • Właściciel organizacyjny - jednostka, do której proces przynależy, jednostka z której pochodzi właściciel personalny
Właściciel systemu	Pracownik merytoryczny Instytutu określający wymagania funkcjonalne systemu w stosunku do wspieranych przez niego procesów.
WS (Web Service)	Usługa sieciowa - element systemu informatycznego polegająca na powtarzalnym wykonywaniu przez ten system z góry określonych funkcji po otrzymaniu, za pomocą sieci komputerowej, danych uporządkowanych w określonej strukturze. Zgodnie z zaleceniami W3C, dane do WS oraz odpowiedzi przekazywane są za pomocą protokołu HTTP i z wykorzystaniem XML.
Zaplecze	Wydzielona część portalu internetowego lub aplikacji mobilnej pozwalająca na zarządzanie treścią, danymi i funkcjami portalu lub aplikacji mobilnej

Projekt pn. „E-ATESTY uruchomienie e-usług za pośrednictwem dedykowanej aplikacji mobilnej wspieranej interoperacyjną platformą informatyczną” współfinansowanego ze środków EFRR w ramach POPC nr POPC.02.04.00-00-0089/20-00

Projekt pn. „E-ATESTY uruchomienie e-usług za pośrednictwem dedykowanej aplikacji mobilnej wspieranej interoperacyjną platformą informatyczną” współfinansowanego ze środków EFRR w ramach POPC nr POPC.02.04.00-00-0089/20-00

1. Wprowadzenie

1.1. Cele i zakres Strategii

Niniejsza Strategia bezpieczeństwa informatycznego w zakresie aplikacji mobilnych i portali internetowych stanowi rozszerzenie Strategii Bezpieczeństwa Systemów Informatycznych NIZP-PZH. Jest zbiorem zasad mających na celu właściwe zarządzanie portalami internetowymi i aplikacjami mobilnymi udostępniającymi dane i usługi z Systemów Informatycznych NIZP-PZH.

1.2. Wyłączenia i punkty styku

Zapisy niniejszej Strategii pozostają w zgodzie z przyjętą przez Instytut Polityką Bezpieczeństwa Ochrony Danych Osobowych zgodnie § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Strategia realizuje Politykę Bezpieczeństwa Ochrony Danych Osobowych wskazując standardy oraz wytyczne dla procedur służące zapewnieniu bezpieczeństwu informacji i danych przetwarzanych w systemach informatycznych Instytutu.

Strategia w zakresie oceny ryzyka bezpieczeństwa systemów informatycznych Instytutu jest zgodna z Polityką Zarządzania Ryzykiem.

Niniejsza Strategia jest zgodna z Załącznikiem nr 2 do Zarządzenia Dyrektora Instytutu z dnia 4 czerwca 2020 „Instrukcja zarządzania system informatycznym służącym do przetwarzania danych osobowych w Narodowym Instytucie Zdrowia Publicznego – Państwowym Zakładzie Higieny" określającym szczegółowe instrukcje dotyczące bezpieczeństwa systemów służących do przetwarzania danych osobowych.

1.3. Obszar stosowania

Za obszar stosowania Strategii traktuje się pomieszczenia budynków będących własnością Instytutu lub zarządzanych przez Instytut, w których zachodzi przetwarzanie danych, w tym danych osobowych. Udostępnianie usług w ramach systemów informatycznych oraz dostęp do systemów informatycznych Instytutu poprzez stanowiska robocze jak również poprzez usługi udostępniane poprzez chmurę prywatną lub publiczną NIZP PZH w zakresie usług i danych udostępnianych z Systemów Informatycznych NIZP PZH.

1.4. Odpowiedzialność za bezpieczeństwo systemów informatycznych

Strategia obowiązuje wszystkie osoby będące administratorami oraz użytkownikami systemów informatycznych Instytutu oraz sprawujące nadzór nad stosowaniem Strategii w podległych sobie jednostkach.

Projekt pn. „E-ATESTY uruchomienie e-usług za pośrednictwem dedykowanej aplikacji mobilnej wspieranej interoperacyjną platformą informatyczną" współfinansowanego ze środków EFRR w ramach POPC nr POPC.02.04.00-00-0089/20-00

Szczegółowy zakres odpowiedzialności w zakresie stosowania i utrzymania Strategii określono w nadrzędnej Strategii Bezpieczeństwa Systemów Informatycznych NIZP-PZH

2. Standardy bezpieczeństwa portali internetowych i aplikacji mobilnych

2.1. Architektura i udostępnianie danych i usług

Dane i usługi mogą być udostępniane poprzez portale internetowe i aplikacje mobilne w sposób wyizolowany od wewnętrznej sieci NIZP-PZH poprzez umieszczenie systemów zaplecza portali i aplikacji mobilnych w strefie DMZ infrastruktury NIZP PZH.

Autentykacja aplikacji i portali z serwerami danych i usług zaplecza powinna odbywać się w sposób zapewniający bezpieczny delegowany dostęp zgodnie ze standardem OAuth w wersji 2.0 lub równoważnym dla wybranej technologii.

2.2. Wymagania funkcjonalne i pozafunkcjonalne

W poniższej tabeli zestawiono listę standardów bezpieczeństwa oraz zestaw wymagań funkcjonalnych i pozafunkcjonalnych dla portali internetowych i aplikacji mobilnych udostępniających dane i usługi NIZP PZH użytkownikom zewnętrznym i wewnętrznym stosowanym w celu zapewnienia wymaganego poziomu bezpieczeństwa dostępu do danych i usług.

Wymagania te powinny zostać zaadaptowane podczas określania wymagań funkcjonalnych i pozafunkcjonanych dla wdrażanych przez NIZP-PZH portali internetowych i aplikacji mobilnych.

1. Autentykacja użytkowników i dostęp do danych i usług- określa zasady dostępu użytkowników do danych i usług
1.1. Poziomy uwierzytelnienia użytkowników zewnętrznych: • Poziom 0 – użytkownik nieuwierzytelniony • Poziom 1 (uwierzytelnienie słabe) – użytkownik uwierzytelniony kontem lokalnym • Poziom 2 (uwierzytelnienie silne) – użytkownik uwierzytelniony poświadczeniami globalnymi (LDAP lub Active Directory dla użytkowników wewnętrznych, Węzeł Krajowy dla użytkowników zewnętrznych)
1.2. Określenie poziomu dostępności danych i usług dla poszczególnych poziomów uwierzytelnienia
2. Raporty bezpieczeństwa – określa funkcjonalności związane z definiowaniem i generowaniem raportów bezpieczeństwa dla zapleczy (back-office) portali internetowych i aplikacji mobilnych.

Projekt pn. „E-ATESTY uruchomienie e-usług za pośrednictwem dedykowanej aplikacji mobilnej wspieranej interoperacyjną platformą informatyczną” współfinansowanego ze środków EFRR w ramach POPC nr POPC.02.04.00-00-0089/20-00

2.1	Definiowanie i generowanie raportów bezpieczeństwa w zakresie określonym dla danego systemu
2.2	Eksport raportów bezpieczeństwa
2.3	Powiadomienia e-mail
3	**Rejestry audytowe** – określa funkcjonalności zawiązane z przeglądaniem rejestrów audytowych z poziomu zapleczy (back-office) portali internetowych i aplikacji mobilnych.
3.1	Historia zmian uprawnień Użytkowników (z dokładnością do roli): login, nazwisko, imię, jednostka, komórka organizacyjna, grupa ról, rola, data nadania roli/grupy ról, data odebrania roli/grupy.
3.2	Lista sesji Użytkowników zawierająca listę wszystkich sesji Użytkowników, wraz z informacjami: login, nazwisko, imię, jednostka, komórka organizacyjna, data i godzina początku sesji, data i godzina zakończenia sesji (jeżeli sesja już została zakończona), adres IP komputera, na którym powstała sesja
3.3	Lista otwartych sesji: login, nazwisko, imię, jednostka, komórka organizacyjna, data /godzina początku sesji wraz możliwością wylogowania wszystkich zalogowanych użytkowników.
3.4	Lista kont Użytkowników w Systemie: login, nazwisko, imię, jednostka, komórka organizacyjna, data założenia konta, data dezaktywacji konta, informacja czy konto aktywne, do kiedy ważne, data zmiany hasła, data ostatniego logowania
3.5	Historia logowań: login, nazwisko, imię, jednostka, komórka organizacyjna, data i godzina zalogowania, data i godzina wylogowania, czas logowania.
3.6	Historia zmian dotyczących kont Użytkowników: zawierająca wszystkie atrybuty konta Użytkownika (login, nazwisko, imię, adres e-mail, data założenia konta, data zablokowania konta, czy aktywne, do kiedy ważne, data zmiany hasła) oraz powiązań konta Użytkownika z innymi obiektami (np. uprawnienia, sesje), wraz z datą i godziną zmiany oraz informacją o tym kto zmianę wykonał.