Zasób	Zagrożenie i źródło	Identyfikacja zagrożenia	Ocena zagrożeń			Zabezpieczenia	Audyt
			C	I	A		
Router	**Nieuprawniony dostęp do panelu administracyjnego poprzez ataki brute force lub domyślne dane logowania.** Atak zewnętrzny - zagrożenie techniczne **Atak typu Denial of Service (DoS) blokujący dostęp do sieci.** Atak zewnętrzny - zagrożenie techniczne. **Podszywanie się pod router (ARP spoofing) w celu przechwycenia danych.** Atak wewnętrzny - zagrożenie techniczne. **Złośliwe oprogramowanie (np. botnet) instalowane na routerze w celu ataków na inne sieci lub urządzenia.** Atak zewnętrzny i wewnętrzny – zagrożenie techniczne. **Nieautoryzowany dostęp do konfiguracji sieci bezprzewodowej poprzez słabe hasło Wi-Fi.** Atak zewnętrzny - zagrożenie techniczne.	1.1 Złamanie hasła: metodą brute force, metodą słownikową 1.2 Atak DoS: przeciążenie serwera 1.3 Atak ARP spoofing: podszywanie się pod urządzenia sieciowe 1.4 Infekcja malware: instalacja złośliwego oprogramowania 1.5 Łamanie hasła Wi-Fi: przechwycenie hasła Wi-Fi Skutek: Utrata kontroli nad routerem, potencjalne przechwycenie danych przesyłanych przez sieć.	4	4	3	1.1 Zmiana domyślnych danych logowania. Włączenie uwierzytelniania dwuskładnikowego. Regularna aktualizacja firmware'u. 1.2 Implementacja filtrów i limitów połączeń. Korzystanie z usług dostawców oferujących ochronę przed DoS. Monitorowanie ruchu sieciowego. 1.3 Włączenie zabezpieczeń ARP. Segmentacja sieci. Monitorowanie i filtrowanie ruchu ARP. 1.4 Regularne aktualizacje firmware'u. Włączenie systemów wykrywania i zapobiegania włamaniom (IDS/IPS). 1.5 Używanie silnych haseł do Wi-Fi. Regularna zmiana hasła. Włączenie szyfrowania WPA3. Segmentacja sieci dla gości.	1.1 Regularny audyt ustawień routera. Weryfikacja logów pod kątem nieautoryzowanych prób logowania. Testy penetracyjne. 1.2 Monitorowanie ruchu sieciowego. Regularne testy odporności na ataki DoS. Weryfikacja logów połączeń. 1.3 Regularny audyt sieci pod kątem ataków ARP. Testy bezpieczeństwa sieci. Weryfikacja logów ARP. 1.4 Regularne skanowanie pod kątem złośliwego oprogramowania. Weryfikacja aktualności firmware'u. Monitorowanie ruchu sieciowego. 1.5 Audyt ustawień sieci bezprzewodowej. Weryfikacja siły hasła Wi-Fi. Testy penetracyjne sieci bezprzewodowej.

System studencki USOS	**Nieautoryzowany dostęp do kont studentów lub pracowników poprzez ataki phishingowe lub brute force.** Atak zewnętrzny - zagrożenie techniczne i organizacyjne. **Ataki typu Denial of Service (DoS) uniemożliwiające korzystanie z systemu w okresach wzmożonego ruchu.** Atak zewnętrzny - zagrożenie techniczne. **Nieautoryzowana modyfikacja danych akademickich (ocen, zapisów kursów) przez użytkowników z uprawnieniami administracyjnymi.** Atak wewnętrzny - zagrożenie techniczne i organizacyjne. **Przechwycenie danych osobowych studentów i pracowników przez nieautoryzowane osoby (np. ataki SQL injection).** Atak zewnętrzny - zagrożenie techniczne. **Utrata danych w wyniku awarii sprzętu lub oprogramowania.** Zagrożenie techniczne.	2.1 Złamanie hasła: phishing, brute force 2.2 Atak DoS: przeciążenie serwera 2.3 Modyfikacja danych: fałszowanie rekordów akademickich 2.4 Atak SQL injection: wstrzyknięcie złośliwego kodu SQL 2.5 Awaria sprzętu: utrata krytycznych danych akademickich Skutek: Możliwość modyfikacji ocen, przechwycenie danych osobowych studentów i pracowników.	5	4	4	2.1. Uwierzytelnianie dwuskładnikowe. Edukacja użytkowników na temat phishingu. Regularne audyty bezpieczeństwa. 2.2. Ochrona DDoS od dostawców usług. Redundancja serwerów. Monitorowanie ruchu sieciowego. 2.3 Ścisła kontrola dostępu. Audyty działań administracyjnych. Szyfrowanie danych w bazie danych. 2.4 Regularne testy penetracyjne. Wdrożenie WAF (Web Application Firewall). Edukacja użytkowników. 2.5 Regularne tworzenie kopii zapasowych. Redundancja danych. Testowanie planów odzyskiwania danych po awarii.	2.1. Monitorowanie logów dostępu. Regularne testy penetracyjne. Weryfikacja i analiza incydentów bezpieczeństwa. 2.2 Regularne testy obciążeniowe. Monitorowanie wydajności systemu. Analiza i optymalizacja zasobów serwerowych. 2.3 Regularna weryfikacja logów działań administracyjnych. Audyty bezpieczeństwa. Szkolenia dla administratorów. 2.4 Regularne audyty bezpieczeństwa aplikacji. Monitorowanie i analiza logów aplikacyjnych. Testy penetracyjne. 2.5 Regularne testy odzyskiwania danych. Monitorowanie stanu sprzętu i oprogramowania. Audyty kopii zapasowych.

Baza danych chorych NFZ	**Nieautoryzowany dostęp do danych medycznych poprzez ataki phishingowe lub brute force.** Atak zewnętrzny - zagrożenie techniczne i organizacyjne. **Ataki typu Denial of Service (DoS) uniemożliwiające dostęp do bazy danych.** Atak zewnętrzny - zagrożenie techniczne. **Nieautoryzowana modyfikacja danych medycznych przez użytkowników z uprawnieniami administracyjnymi.** Atak wewnętrzny - zagrożenie techniczne i organizacyjne. **Przechwycenie danych medycznych przez nieautoryzowane osoby (np. ataki SQL injection).** Atak zewnętrzny - zagrożenie techniczne. **Utrata danych w wyniku awarii sprzętu lub oprogramowania.** Zagrożenie techniczne.	3.1. Złamanie hasła: phishing, brute force 3.2 Atak DoS: przeciążenie serwera 3.3 Modyfikacja danych: fałszowanie danych medycznych 3.4 Atak SQL injection: wstrzyknięcie złośliwego kodu SQL 3.5 Awaria sprzętu: utrata krytycznych danych medycznych Skutek: Naruszenie poufności danych medycznych pacjentów, możliwość wykorzystania danych do szantażu lub kradzieży tożsamości.	5	5	4	3.1. Uwierzytelnianie dwuskładnikowe. Szyfrowanie danych w spoczynku i w tranzycie. Edukacja użytkowników. 3.2 Ochrona DDoS od dostawców usług. Redundancja serwerów. Monitorowanie ruchu sieciowego. 3.3 Ścisła kontrola dostępu. Audyty działań administracyjnych. Szyfrowanie danych w bazie danych. 3.4 Regularne testy penetracyjne. Wdrożenie WAF (Web Application Firewall). Edukacja użytkowników. 3.5 Regularne tworzenie kopii zapasowych. Redundancja danych. Testowanie planów odzyskiwania danych po awarii.	3.1. Monitorowanie logów dostępu. Regularne testy penetracyjne. Audyty bezpieczeństwa. 3.2 Regularne testy obciążeniowe. Monitorowanie wydajności systemu. Analiza i optymalizacja zasobów serwerowych. 3.3 Regularna weryfikacja logów działań administracyjnych. Audyty bezpieczeństwa. Szkolenia dla administratorów. 3.4 Regularne audyty bezpieczeństwa aplikacji. Monitorowanie i analiza logów aplikacyjnych. Testy penetracyjne. 3.5 Regularne testy odzyskiwania danych. Monitorowanie stanu sprzętu i oprogramowania. Audyty kopii zapasowych.

Kamerka komputerowa	**Nieautoryzowany dostęp do kamerki internetowej przez złośliwe oprogramowanie (malware).** Atak zewnętrzny - zagrożenie techniczne. **Podszywanie się pod urządzenie i przechwycenie obrazu (np. ataki typu Man-in-the-Middle).** Atak wewnętrzny – zagrożenie techniczne. **Nieautoryzowana modyfikacja ustawień kamerki przez atakującego.** Atak wewnętrzny – zagrożenie techniczne. **Utrata dostępu do kamerki w wyniku awarii sprzętu lub oprogramowania.** Zagrożenie techniczne.	4.1 Infekcja malware: zdalne przejęcie kontroli nad kamerką 4.2 Atak MITM: przechwycenie obrazu 4.3 Modyfikacja ustawień: zmiana konfiguracji urządzenia 4.4 Awaria sprzętu: niemożność korzystania z urządzenia Skutek: Naruszenie prywatności użytkownika, możliwość szantażu, przechwycenie poufnych informacji.	4	3	2	4.1 Używanie oprogramowania antywirusowego. Regularne aktualizacje systemu i sterowników. Uwierzytelnianie dwuskładnikowe. 4.2 Włączenie szyfrowania komunikacji. Używanie bezpiecznych sieci. Regularne aktualizacje oprogramowania. 4.3 Uwierzytelnianie dwuskładnikowe. Szyfrowanie ustawień urządzenia. Regularne aktualizacje firmware'u. 4.4 Regularne testy funkcjonalności. Aktualizacje oprogramowania. Kopie zapasowe ustawień.	4.1 Regularne skanowanie systemu pod kątem malware. Monitorowanie logów dostępu do kamerki. Testy penetracyjne. 4.2 Regularne audyty bezpieczeństwa. Testy bezpieczeństwa komunikacji. Monitorowanie logów. 4.3 Regularne audyty ustawień urządzenia. Monitorowanie logów zmian ustawień. Testy penetracyjne. 4.4 Regularne testy urządzenia. Monitorowanie stanu sprzętu. Audyty aktualności oprogramowania.

Baza danych odcisków palców	**Nieautoryzowany dostęp do danych biometrycznych przez ataki phishingowe lub brute force.** Atak zewnętrzny - zagrożenie techniczne i organizacyjne. **Ataki typu Denial of Service (DoS) uniemożliwiające dostęp do bazy danych.** Atak zewnętrzny - zagrożenie techniczne. **Nieautoryzowana modyfikacja danych biometrycznych przez użytkowników z uprawnieniami administracyjnymi.** Atak wewnętrzny - zagrożenie techniczne i organizacyjne. **Przechwycenie danych biometrycznych przez nieautoryzowane osoby (np. ataki SQL injection).** Atak zewnętrzny - zagrożenie techniczne. **Utrata danych w wyniku awarii sprzętu lub oprogramowania.** Zagrożenie techniczne.	5.1. Złamanie hasła: phishing, brute force 5.2 Atak DoS: przeciążenie serwera 5.3 Modyfikacja danych: fałszowanie danych biometrycznych 5.4 Atak SQL injection: wstrzyknięcie złośliwego kodu SQL 5.5 Awaria sprzętu: utrata krytycznych danych biometrycznych Skutek: Naruszenie poufności danych biometrycznych, możliwość wykorzystania danych do kradzieży tożsamości.	5	5	3	5.1. Uwierzytelnianie dwuskładnikowe. Szyfrowanie danych w spoczynku i w tranzycie. Edukacja użytkowników. 5.2 Ochrona DDoS od dostawców usług. Redundancja serwerów. Monitorowanie ruchu sieciowego. 5.3 Ścisła kontrola dostępu. Audyty działań administracyjnych. Szyfrowanie danych w bazie danych. 5.4 Regularne testy penetracyjne. Wdrożenie WAF (Web Application Firewall). Edukacja użytkowników. 5.5 Regularne tworzenie kopii zapasowych. Redundancja danych. Testowanie planów odzyskiwania danych po awarii.	5.1. Monitorowanie logów dostępu. Regularne testy penetracyjne. Audyty bezpieczeństwa. 5.2 Regularne testy obciążeniowe. Monitorowanie wydajności systemu. Analiza i optymalizacja zasobów serwerowych. 5.3 Regularna weryfikacja logów działań administracyjnych. Audyty bezpieczeństwa. Szkolenia dla administratorów. 5.4 Regularne audyty bezpieczeństwa aplikacji. Monitorowanie i analiza logów aplikacyjnych. Testy penetracyjne. 5.5 Regularne testy odzyskiwania danych. Monitorowanie stanu sprzętu i oprogramowania. Audyty kopii zapasowych.