Detekcja i monitorowanie zagrożeń

Zespół:	Damian Linek Wojciech Minner
Grupa:	1IZ22B

Projekt

Wybrana organizacja: SOR

Opis organizacji

SOR, czyli Szpitalny Oddział Ratunkowy, to kluczowa jednostka w systemie opieki zdrowotnej. Jest to miejsce, gdzie pacjenci w stanie nagłego zagrożenia zdrowia lub życia otrzymują natychmiastową pomoc medyczną. Bezpieczeństwo IT w SOR jest absolutnie kluczowe, gdyż jego naruszenie może skutkować zagrożeniem życia pacjentów czy też wycieku ich wrażliwych danych osobistych. Systemy SOR przechowują wiele wrażliwych danych jak dokumentacja medyczna wykorzystywana do leczenia pacjentów, wrażliwe dane personalne oraz urządzenia zapewniające ciągłe funkcjonowanie systemów ratujących życie. Ataki na SOR mogą stanowić poważne zagrożenie dla danych pacjentów jak i ich życia i zdrowia. Odpowiednie zabezpieczenia infrastruktury krytycznej SOR jest wymagane w celu minimalizacji zagrożeń ataków i ochrony zdrowia i życia pacjentów organizacji.

Zasoby sprzętowe

1. **Stacje robocze:** Komputery używane przez lekarzy, pielęgniarki i personel administracyjny pozwalający na dostęp do dokumentacji medycznej oraz raportowania.
2. **Serwer lokalny:** Serwer przechowujący dane pacjentów, obrazy diagnostyczny oraz system zarządzania hospitalizacją.
3. **Laptopy i tablety:** Mobilne urządzania dla lekarzy i ratowników pozwalających na dostęp do danych w czasie rzeczywistym.
4. **Routery, Switche oraz punkty dostępowe:** Zapewnia dostęp do Internetu dla urządzeń w jednostce SOR.
5. **Telefon IP:** Wykorzystane do komunikacji zewnętrznej i wewnętrznej.
6. **Drukarki i skanery:** Drukarki i skanery IP wykorzystywane do drukowania recept i skanowania dokumentów.
7. **Monitoring i System kontroli dostępu:** Monitorowanie obiektu i zabezpieczanie dostępu do kluczowych pomieszczeń na oddziale.
8. **Urządzenia medyczne:** Takie urządzenia jak pompy infuzyjne, respiratory oraz aparaty diagnostyczne jak tomograf komputerowy.

Zagrożenia

1. **Atak fizyczny:** Uzyskanie dostępu do urządzeń przez osoby nieuprawnione.
2. **Złośliwe oprogramowanie:** Wykorzystanie atakującemu na uzyskanie dostępu do sieci jak i urządzeń znajdujących się w sieci.
3. **Włamanie do sieci:** Wykorzystywanie nieodpowiednio zabezpieczonych urządzeń sieciowych do uzyskania dostępu do sieci.
4. **Manipulacja urządzeniami medycznymi:** Próby przejęcia kontroli nad urządzeniami krytycznymi i zmiany ich ustawień prowadzących do zakłócenia ich pracy.
5. **Ataki na system operacyjny:** Wykorzystanie luk w systemie operacyjnym stacji roboczej bądź serwera do uzyskania nieautoryzowanego dostępu do urządzenia.

Wektory ataków

1. **Atak fizyczny:** Bezpośredni dostęp do urządzenia przez porty komputerowe, zniszczenie bądź uszkodzenie sprzętu, kradzież sprzętu.
2. **Złośliwe oprogramowanie:** Wykorzystanie przez atakujących phishingu, wysyłanie wiadomości email z fałszywymi linkami oraz zainfekowanymi załącznikami. Ataki ransomware czyli szyfrowanie plików, dokumentacji medycznej w celu żądania okupu za odszyfrowanie danych.
3. **Włamanie do sieci:** Eksploatacja słabo zabezpieczonych urządzeń sieciowych, wykorzystujących domyślne hasła oraz posiadające błędy konfiguracyjne. Wykorzystanie przez atakującego znanych luk w oprogramowaniu urządzeń sieciowych.
4. **Manipulacje urządzeniami medycznymi:** Fizyczny dostęp do urządzenia medycznego i zmiana ustawień, próba zdalnego dostępu do urządzenia.
5. **Ataki na system operacyjny:** Eksploatacja znanych luk w systemie operacyjnym które nie są naprawione ze względu na brak aktualizacji. Eskalacja uprawień administratora w systemie. Ataki bruteforce na dane uwierzytelniające użytkownika.

Monitorowanie i wykrywanie

1. **Ataki fizyczne:** Monitoring i rejestracja wejść systemem biometrycznym.
2. **Złośliwe oprogramowanie:** Oprogramowanie antywirusowe.
3. **Włamanie do sieci:** Monitorowanie sieci urządzeniami typu IDS lub IPS, które będą analizować sieć w czasie rzeczywistym i wykrywać ewentualne anomalie.
4. **Manipulacja urządzeń medycznych:** Wdrożenie systemu monitorowania zmian ustawień urządzeń medycznych poprzez osoby nieautoryzowane.
5. **Ataki na system operacyjny:** Wykorzystanie narzędzi SIEM do analizy logów i wykrywania prób włamania.

Środki zaradcze

1. **Ataki fizyczne:** Wprowadzenie systemu kontroli dostępu, który będzie odpowiedzialny za rejestracje wejść do pomieszczeń, jak i wprowadzenie zamków elektronicznych które będą współpracować z systemem kontroli pozwalając na dostęp tylko osobą upoważnionym. Serwery zostaną umieszczone w szczelnie chronionym pomieszczeniu do którego dostęp będzie miał tylko wykwalifikowany personel. Aby zabezpieczyć się przed kradzieżami takich urządzeń jak laptopy i komputery można zastosować szyfrowanie dysków i zabezpieczenia bootowania systemu pinem.
2. **Złośliwe oprogramowanie:** Podstawową ochroną przed takimi atakami jak phishing jest regularna edukacja pracowników z rozpoznawania phishingu i innych prób oszustwa. Zastosowanie oprogramowanie antywirusowego i jego regularne aktualizowanie pozwoli na bezpieczne utrzymanie systemu. Stworzenie polityk dostępu ograniczających instalowanie aplikacji przez użytkowników.
3. **Włamanie do sieci:** Regularne aktualizacje urządzeń sieciowych, poprawne skonfigurowanie urządzeń, wykorzystanie haseł spełniających reguły bezpiecznego hasła , blokowanie dostępu po wielu nieudanych próbach, oraz wyłączenie nieużywanych usług i serwisów urządzeń sieciowych. Monitorowanie sieci i wykorzystanie narzędzi do analizy ruchu sieciowego.
4. **Manipulacje urządzeniami medycznymi:** Oddzielenie urządzeń medycznych od reszty infrastruktury poprzez dedykowaną sieć VLAN. Wymuszanie uwierzytelnienia przy każdej próbie dostępu do urządzenia.
5. **Ataki na system operacyjny:** Regularne aktualizowanie systemu operacyjnego, polityki haseł, blokowanie instalacji nienaturyzowanego oprogramowania, minimalizacja uprawnień. Szkolenia pracowników z bezpiecznych praktyk użytkowania sprzętu.