

mMedica

mModuły - bezpieczeństwo

Spis treści

1. OPIS	3
2. SYSTEM OPERACYJNY.....	3
2.1. AKTUALIZACJE.....	3
2.2. OPROGRAMOWANIE	3
2.3. KONTA DOSTĘPWE.....	3
2.4. LOGI	4
3. SERWERY WWW	4
3.1. PROTOKÓŁ HTTPS	4
3.2. OGRANICZANIE DOSTĘPU	4
3.2.1. IIS	4
3.2.2. Apache	6
3.3. UDOSTĘPNIONE ZASOBY ORAZ APLIKACJE.....	7
3.4. UPRAWNIENIA	7
3.5. HARDENING	8
3.5.1. IIS	8
3.5.2. Apache	8
3.6. LOGI	9
3.6.1. IIS	9
3.6.2. Apache	9
4. USTAWIENIA SIECIOWE ORAZ FIREWALL.....	9
4.1. PROTOKOŁY.....	9
4.2. USTAWIENIA FIREWALL	10
5. APLIKACJE MMODUŁÓW.....	10
5.1. INSTALACJA ORAZ AKTUALIZACJA.....	10
5.2. PUBLIKOWANIE APLIKACJI.....	11
5.3. BAZA DANYCH.....	11
5.4. FILTROWANIE RUCHU	12
5.5. OCHRONA PRZED ATAKAMI BRUTE-FORCE.....	12
5.6. UWIERZYTELNIANIE DWUSKŁADNIKOWE	13

1. Opis

Niniejszy dokument opisuje rekomendacje dotyczące zabezpieczeń aplikacji mModułów pakietu mMedica. Szczegółowe zalecenia dotyczące bezpieczeństwa każdego z mModułów są zapisane w instrukcjach instalacji i konfiguracji każdego z mModułów.

Dokument opisuje podstawowe zasady bezpieczeństwa aplikacji webowych instalowanych na systemach operacyjnych rodziny Windows oraz opartych o jądro Linux.

2. System operacyjny

2.1. Aktualizacje

Aktualizacje systemu operacyjnego zawierają poprawki bezpieczeństwa, które eliminują znane luki umożliwiające zdalne oraz lokalne przejęcie serwera, eskalację uprawnień lub destabilizację środowiska. Należy zwrócić szczególną uwagę na dwa aspekty:

- a) regularność – każda maszyna powinna być objęta harmonogramem aktualizacji,
- b) monitoring źródeł aktualizacji – systemy powinny pobierać aktualizacje wyłącznie z zaufanych repozytoriów lub serwerów producenta.

Wykorzystywany system operacyjny powinien być bezwzględnie na liście systemów wspieranych przez producenta. W innym wypadku nie będzie on otrzymywał krytycznych poprawek bezpieczeństwa i będzie szczególnie narażony na niebezpieczeństwo cyberataku.

Należy podkreślić, że brak aktualizacji systemów operacyjnych jest jedną z najczęstszych przyczyn udanych ataków.

2.2. Oprogramowanie

Podczas instalacji oprogramowania należy zwrócić szczególną uwagę, aby pobierać je wyłącznie z oficjalnych kanałów dystrybucji producenta danego oprogramowania. Należy również pamiętać, że oprogramowanie zainstalowane w systemie operacyjnym powinno być aktualne.

W celu zapewnienia bezpieczeństwa systemowi operacyjnemu, gdzie zainstalowano mModuły należy mieć zainstalowane oprogramowanie antywirusowe oraz oprogramowanie typu firewall.

Należy zwrócić szczególną uwagę, aby oprogramowanie antywirusowe było aktualne i posiadało aktualną definicję zagrożeń. Należy również upewnić się, że oprogramowanie antywirusowe ma aktywną ochronę w trybie rzeczywistym i zdefiniowany harmonogram skanowania zagrożeń.

Ponadto, należy pamiętać o regularnym aktualizowaniu środowiska uruchomieniowego Microsoft .Net. Aktualizację należy wykonać pobierając oprogramowanie ze strony Microsoft lub pobrać z oficjalnego repozytorium pakietów dla systemów operacyjnych opartych o jądro Linuxa.

2.3. Konta dostępne

Dostęp do systemu operacyjnego, gdzie zainstalowane są komponenty mModułów powinien być zabezpieczony hasłem poprzez indywidualne konto dla każdego użytkownika systemu. Należy rozważyć korzystanie z uprawnień administratora / sudo (Linux), wyłącznie do operacji, które tego wymagają.

Hasła dostępu do kont w systemie operacyjnym powinny spełniać [rekomendacje CERT Polska](#). Należy regularnie monitorować logi pod kątem nieudanych prób logowania na konto użytkownika. Proces można zautomatyzować wdrażając rozwiązania typu SIEM. Konta, które nie są używane od dłuższego czasu powinny być blokowane lub

usuwane, aby nie stanowiły potencjalnego punktu wejścia dla atakującego. W przypadku przekroczenia zadeklarowanej liczby nieprawidłowych logowań konto powinno być czasowo blokowane, aby ograniczyć możliwość ataku siłowego (brute force). Dla konfiguracji SSH warto stosować logowanie za pomocą kluczy.

Dostęp przez zdalny dostęp (SSH i RDP) powinien być ograniczony tylko do zaufanych adresów IP (np. przez firewall). Nigdy zdalny dostęp nie powinien być wystawiony bezpośrednio do sieci Internet. Jeśli dostęp ma być spoza intranetu placówki należy rozważyć rozwiązania typu VPN.

2.4. Logi

Ważne z punktu widzenia bezpieczeństwa informacje są zapisywane w logach systemu operacyjnego. Znajdują się tam m.in. informacje o nieprawidłowych próbach logowania na konta użytkowników lub błędach aplikacji.

W systemach operacyjnych rodziny Windows, logi są gromadzone w Podglądzie Zdarzeń. Szczególnie ważne są informacje zapisane w Dzienniku systemu Windows / Zabezpieczenia.

Z kolei w systemach operacyjnych opartych o jądro Linuksa na przykładzie Ubuntu, logi można znaleźć w katalogu /var/logs. Należy szczególnie zwrócić uwagę na następujące zbiory:

- /var/log/auth.log – logi dotyczące autoryzacji, logowania, SSH, sudo,
- /var/log/syslog – ogólne logi systemowe, czasem zawierają informacje o bezpieczeństwie,
- /var/log/faillog – nieudane próby logowania (można wyświetlić poleceniem faillog).

3. Serwery WWW

3.1. Protokół https

Koniecznym jest stosowanie protokołu https dla opublikowanych aplikacji mModułów, który zapewnia szyfrowanie transmitowanych danych. Dzięki temu przesyłane dane, w przypadku przechwycenia, nie zostaną odczytane ani zmodyfikowane. Dla pełnego bezpieczeństwa protokół powinien zostać użyty dla wszystkich mModułów.

Protokół będzie spełniał swoją rolę wyłącznie, gdy wszędzie będą używane adresy internetowe wykorzystujące ten protokół. Z tego powodu nie zaleca się ustawienia podwójnego protokołu dostępu HTTP oraz HTTPS na serwerach WWW.

Należy używać wyłącznie protokołów TLS w wersji 1.2 oraz 1.3, które uznawane są za nowoczesne i bezpieczne. Stosowanie starszych wersji zabezpieczeń w sposób istotny obniża bezpieczeństwo aplikacji.

3.2. Ograniczanie dostępu

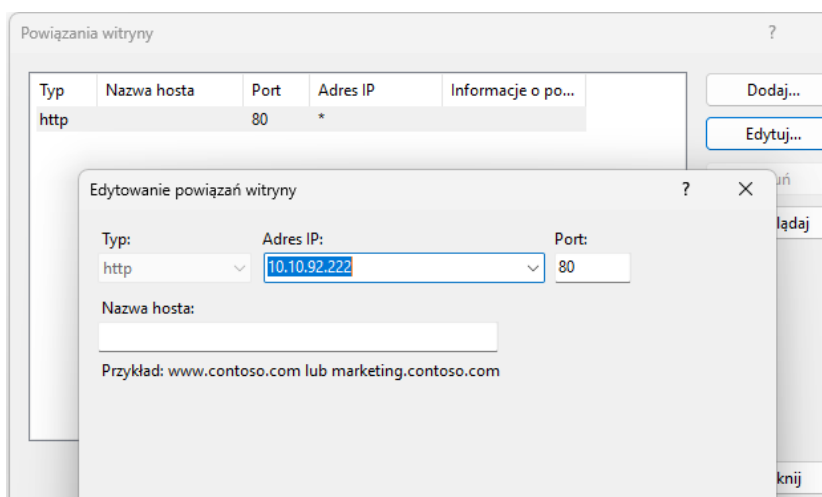
Serwery WWW takie jak IIS oraz Apache umożliwiają ograniczanie dostępu do aplikacji dla konkretnych interfejsów sieciowych, konkretnych adresów IP lub zakresów adresów IP.

3.2.1. IIS

3.2.1.1. Nasłuch interfejsu sieciowego

Zmiana nasłuchu sieciowego, na którym jest dostępna aplikacja w IIS odbywa się na poziomie każdej z witryn IIS. Wybierając opcję edycji powiązania witryny mamy możliwość wyboru zarówno interfejsów sieciowych jak i portu na jakim aplikacja będzie dostępna.

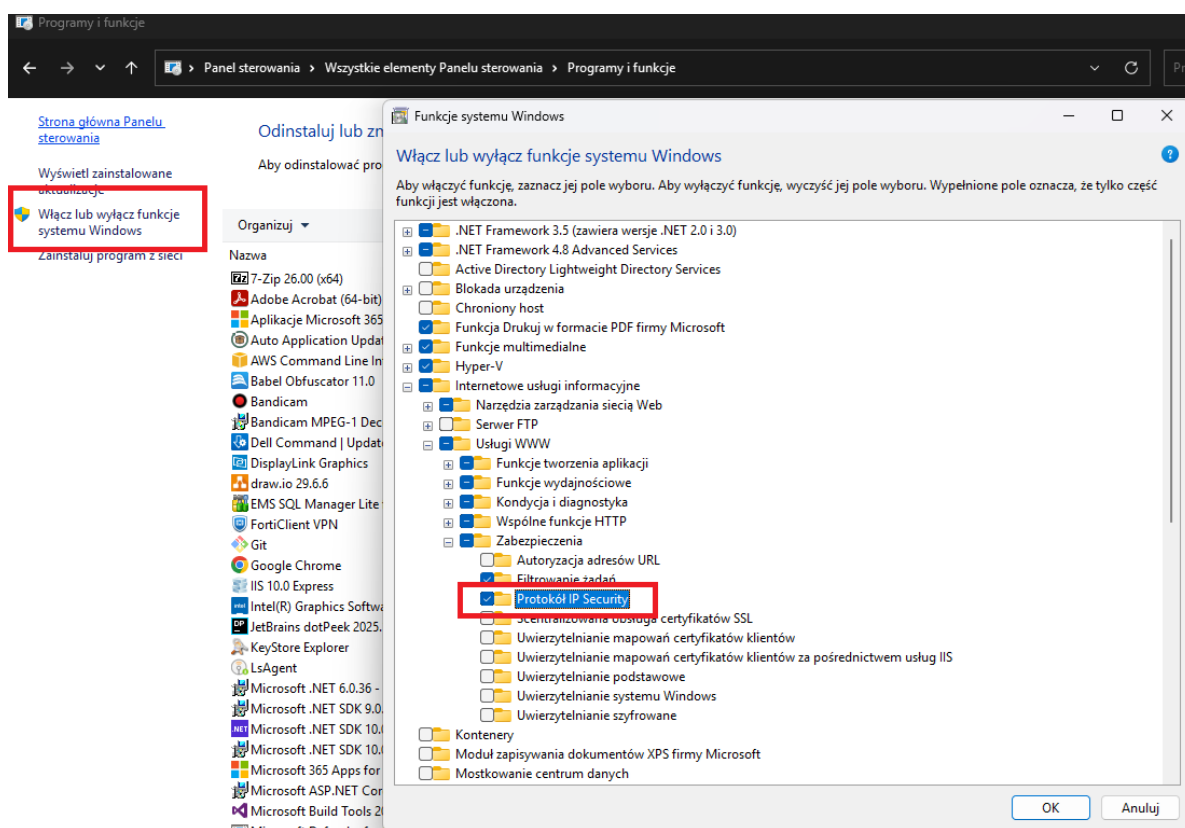
Przykład:



Rysunek 1: Edycja powiązania witryny w IIS

3.2.1.2. Filtrowanie ruchu

Filtrowanie ruchu po adresach IP w IIS jest możliwe po doinstalowaniu komponentu „Protokół IP Security” (ang. „IP and Domain Restrictions”) z poziomu włączania lub wyłączania funkcji systemu Windows. Składnik nie jest domyślnie instalowany.



Rysunek 2: Instalacja składnika do IIS pozwalającego na filtrowanie ruchu po IP

Po zainstalowaniu komponentu w IIS na poziomie:

- globalnego ustawienia serwera (główne okno IIS),
- witryny (po wybraniu witryny),

c) aplikacji w witrynie (po wybraniu aplikacji w witrynie)

dostępna będzie opcja „Ograniczania adresów IP i domen”. Po wybraniu tej pozycji zyskujemy możliwość określania reguł zezwalających lub ograniczających dostęp dla wybranego adresu IP lub zakresu IP.

3.2.2. Apache

3.2.2.1. Nasłuch interfejsu sieciowego

Podstawą do ograniczenia ruchu przychodzącego jest poprawne powiązanie usługi Apache z konkretnym interfejsem sieciowym oraz portem, na którym usługa ma być dostępna. Konfiguracja powiązania znajduje się w pliku `httpd.conf` lub `ports.conf`.

Przykład:

```
Listen 443 # Nasłuchuje na wszystkich interfejsach na porcie 443
Listen 192.168.1.10:443 # Nasłuchuje tylko na interfejsie o IP 192.168.1.10 na porcie 443
Listen 127.0.0.1:8080 # Nasłuchuje tylko na localhost na porcie 8080
```

Dodatkowo na poziomie `VirtualHosta` można wprowadzić ograniczenia nasłuchu do wybranego interfejsu sieciowego oraz portu.

Przykład dopuszczenia wszystkich interfejsów sieciowych (które są dopuszczone przez `Listen`) na porcie 443:

```
<VirtualHost *:443>
```

Ograniczenie do wybranego interfejsu sieciowego na porcie 443:

```
<VirtualHost 192.168.1.10:443>
```

Więcej informacji: <https://httpd.apache.org/docs/2.4/bind.html>

3.2.2.2. Filtrowanie ruchu

W Apache możliwe jest filtrowanie dostępu do zasobów na poziomie pliku `.htaccess` lub na poziomie pojedynczego `VirtualHosta`.

a) Przykład ograniczenia dla pliku `.htaccess`:

```
<Directory "/var/www/html/app">
    Require ip 192.168.1.100 # Pojedynczy adres IP
    Require ip 10.0.0.0/24 # Cała podsieć (np. Intranet)
    Require not ip 203.0.113.0/24 # Odrzuć ruch z tej podsieci
</Directory>
```

b) Przykład dla `VirtualHost`:

```
<VirtualHost *:80>
    ServerName example.com
    DocumentRoot /var/www/example

    <Directory "/var/www/example">
        Require ip 192.168.1.100 # Pojedynczy adres IP
        Require ip 10.0.0.0/24 # Cała podsieć (np. Intranet)
        Require not ip 203.0.113.0/24 # Odrzuć ruch z tej podsieci
    </Directory>
</VirtualHost>
```

Zamiast Directory można stosować również Location. Więcej informacji:

https://httpd.apache.org/docs/2.4/mod/mod_authz_host.html

3.3. Udostępnione zasoby oraz aplikacje

Na bezpieczeństwo serwera, w którym są zainstalowane aplikacje mModułów wpływają również inne udostępnione zasoby lub aplikacje trzecie. Szczególnie należy zwrócić uwagę na zasoby lub aplikacje udostępniane przez serwer WWW, które są dostępne z sieci Internet. Ważne jest, aby regularnie kontrolować, czy udostępnione aplikacje są aktualne oraz nie posiadają znanych podatności.

Należy również zwrócić uwagę, czy serwer WWW nie udostępnia możliwości wyświetlania zawartości folderów. Błędna konfiguracja może spowodować, że zasoby dyskowe maszyny mogą być publicznie dostępne w sieci Internet.

3.4. Uprawnienia

Jednym z najczęściej niedocenianych elementów bezpieczeństwa aplikacji webowych jest sposób zarządzania uprawnieniami do katalogów na serwerze WWW. Aplikacje webowe są w stanie wykonywać operacje na plikach wyłącznie w zakresie przyznanych uprawnień do plików. Odpowiednie uprawnienia nie tylko tworzą warstwę ochrony, ale także minimalizują efekty udanego ataku. Z tego powodu powinno się zawsze stosować zasadę minimalnych uprawnień, czyli aplikacja otrzymuje uprawnienia do tych plików oraz katalogów, które są im niezbędne do prawidłowego działania.

Kluczowym pojęciem w IIS jest pula aplikacji. To ona definiuje, w jakim kontekście bezpieczeństwa uruchamiana jest aplikacja. Każda pula aplikacji działa jako określony tożsamościowy użytkownik systemu Windows (np. ApplicationPoolIdentity lub dedykowane konto domenowe). To właśnie ta tożsamość musi posiadać dostęp do katalogów aplikacji. W przypadku IIS każda aplikacja powinna mieć własną pulę aplikacji co zapewnia oczekiwaną separację.

W Apache dla każdej aplikacji powinno się stosować osobnego użytkownika. Należy również nadać mu stosowane uprawnienia do plików aplikacji. Stanowczo odradza się uruchamiać aplikacje jako root. Konfiguracja użytkownika dla aplikacji jest definiowana w pliku serwisu komponentu. Przykład:

```
[Unit]
Description = mMedica TeleRejestracja
[Service]
ExecStart=/var/www/TeleRejestracja.sh
WorkingDirectory=/var/www/TeleRejestracja
Restart=always
RestartSec=10
SyslogIdentifier=mMedica-TeleRejestracja
User=telerej_user # - wskazanie użytkownika
Environment=ASPNETCORE_ENVIRONMENT=Production

[Install]
WantedBy=Multi-user.target
```

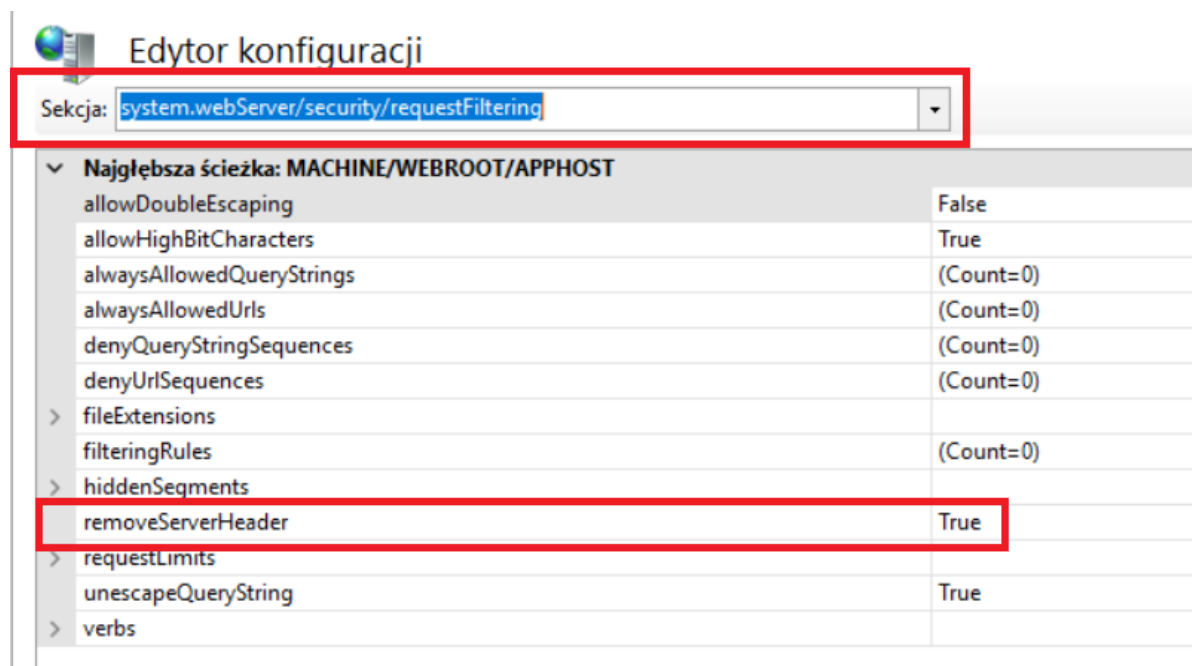
Instalator mModułów nadaje zawsze minimalne oraz konieczne uprawnienia do plików aplikacji mModułów. W przypadku instalacji manualnej należy posilić się instrukcjami instalacji oraz konfiguracji poszczególnych mModułów, gdzie znajdują się informacje o nadawaniu uprawnień do plików.

3.5. Hardening

Hardening to proces wzmacniania bezpieczeństwa serwera www poprzez odpowiednią konfigurację i ograniczenie zbędnych informacji ujawnianych na zewnątrz (np. przez nagłówki http odpowiedzi lub domyślne strony błędów). Jego celem jest zmniejszenie powierzchni ataku oraz utrudnienie potencjalnym napastnikom identyfikacji podatności systemu, co ma kluczowe znaczenie dla ochrony danych i ciągłości działania usług.

3.5.1. IIS

W IIS istnieje możliwość wyłączenia zwracanych informacji o rodzaju serwera www oraz jego wersji. W tym celu należy uruchomić IIS i z poziomu całego serwera lub wybranej witryny wybrać „Edytor konfiguracji”. Następnie w elemencie „Sekcja” wybrać pozycję „system.webServer/security/requestFiltering”, a w kolejnym kroku przełączyć wartość parametru „removeServerHeader” na „True”.



Rysunek 3: Ukrywanie nazwy i wersji serwera www w IIS

Warto również rozważyć konfigurację własnych stron błędów. Opcja jest dostępna z poziomu serwera lub wybranej witryny pod nazwą „Strony błędów”. Funkcjonalność pozwala dla wybranego kodu http zwrócić zdefiniowaną stronę html.

3.5.2. Apache

W apache istnieje dyrektywa `ServerTokens Prod`, która powoduje, że serwer zwraca jedynie ogólną informację „Apache” bez numeru wersji, natomiast dyrektywa `ServerSignature Off` wyłącza podpis serwera na stronach błędów, co dodatkowo ogranicza ujawnianie informacji o środowisku. Obie dyrektywy można wprowadzić w modyfikacji pliku konfiguracyjnego (np. `apache2.conf` lub `httpd.conf`):

```
ServerTokens Prod
ServerSignature Off
```

W apache istnieje również możliwość konfiguracji własnych stron błędów dla wybranych kodów http na poziomie pliku `.htaccess` jak i pojedynczego VirtualHosta.

Przykład konfiguracja dla wybranego VirtualHosta:

```
<VirtualHost *:80>
    ServerName example.com
    DocumentRoot /var/www/html

    ErrorDocument 403 /errors/403.html
    ErrorDocument 404 /errors/404.html
    ErrorDocument 500 /errors/500.html
</VirtualHost>
```

Uwaga: Ścieżki są względne do DocumentRoot, a nie do systemu plików.

3.6. Logi

3.6.1. IIS

Domyślnie logi z dostępu do zasobów IIS istnieją w katalogu C:\inetpub\logs\LogFiles. W tym folderze może znajdować się w wiele katalogów W3SVC[numer], każdy gromadzi logi z pojedynczej witryny. Aby sprawdzić, który folder jest powiązany z witryną można z poziomu IIS wykonać poniższe operacje:

- wybrać interesującą nas witrynę,
- z menu kontekstowego (prawy przycisk myszy) wybrać „Zarządzanie witryną sieci Web” \ ”Ustawienia zaawansowane”,
- wartość w polu „Identyfikator” wskazuje na folder logów, np. identyfikator o wartości 1 wskazuje na folder W3SVC1.

Dodatkowo informacje oraz błędy związane z uruchamianiem aplikacji są zapisywane w Podglądzie Zdarzeń.

3.6.2. Apache

Domyślnie globalne logi w Apache gromadzone są w plikach:

- /var/log/apache2/access.log – logi związane z dostępem do zasobów,
- /var/log/apache2/error.log – logi błędów.

Istnieje możliwość utworzenia własnych plików logów dla wybranego VirtualHosta. Przykład:

```
<VirtualHost *:80>
    ServerName example.com
    DocumentRoot /var/www/example.com
    ErrorLog /var/log/apache2/example.com-error.log # Log z błędami
    CustomLog /var/log/apache2/example.com-access.log combined # Log z dostęпами
</VirtualHost>
```

Po zdefiniowaniu logów w VirtualHost, żądania obsługiwane przez ten VirtualHost będą zapisywane tylko w określonych plikach logów, a nie będą się odkładać w globalnych logach.

4. Ustawienia sieciowe oraz firewall

4.1. Protokoły

Zaleca się wyłącznie na serwerze obsługi protokołów TCP, której nie są używane (np. IPv6). Brak takich działań może skutkować negatywnie m.in. w przypadku, w którym administrator zapomni o odpowiednim skonfigurowaniu zapory ogniowej dla nieużywanego protokołu lub w aplikacji serwera WWW (IIS, Apache).

Instrukcja wyłączenia IPv6 dla Windows:

1. Przejść do „Panelu Sterowania”.
2. Uruchomić „Centrum sieci i udostępniania”.
3. Wybrać „Zmień ustawienia karty sieciowej”.
4. Kliknąć prawym przyciskiem myszy i wybrać z menu kontekstowego „Właściwości” po kolei na każdą z aktywnych kart (fizyczne oraz wirtualne), które komunikują się z siecią.
5. Odznaczyć w oknie „Internet Protocol Version 6 (TCP/IPv6)”.
6. Zapisać zmiany.

Serwery WWW (IIS, Apache) również powinny zostać skonfigurowane tak, aby udostępniać wyłącznie aktywne protokoły komunikacji (np.: http, https, ftp) i to wyłącznie na aktywnych protokołach TCP (IPv4, IPv6).

Instrukcja wyłączania protokołów dla IIS:

1. Uruchomić IIS.
2. W menu „Połączenia” prawym przyciskiem myszy uruchomić menu kontekstowe witryny, której ustawienia należy zmienić (np. Default Web Site).
3. Z menu kontekstowego wybrać opcję „Edytuj powiązania...”.
4. W oknie powiązań zostaną wyświetlone wszystkie uruchomione protokoły komunikacji aplikacji (typy) oraz przypisane adresy IP (symbol * oznacza wszystkie adresy), które wynikają z aktywnych protokołów TCP.
5. Za pomocą opcji „Edytuj...” można zmienić już istniejące w tabeli wpisy. Wpisy można również dodać lub usunąć za pomocą przycisków kolejno „Dodaj...” oraz „Usuń”.
6. Po wprowadzeniu zmian okno „Powiązania witryny” można zamknąć za pomocą przycisku „Zamknij”.

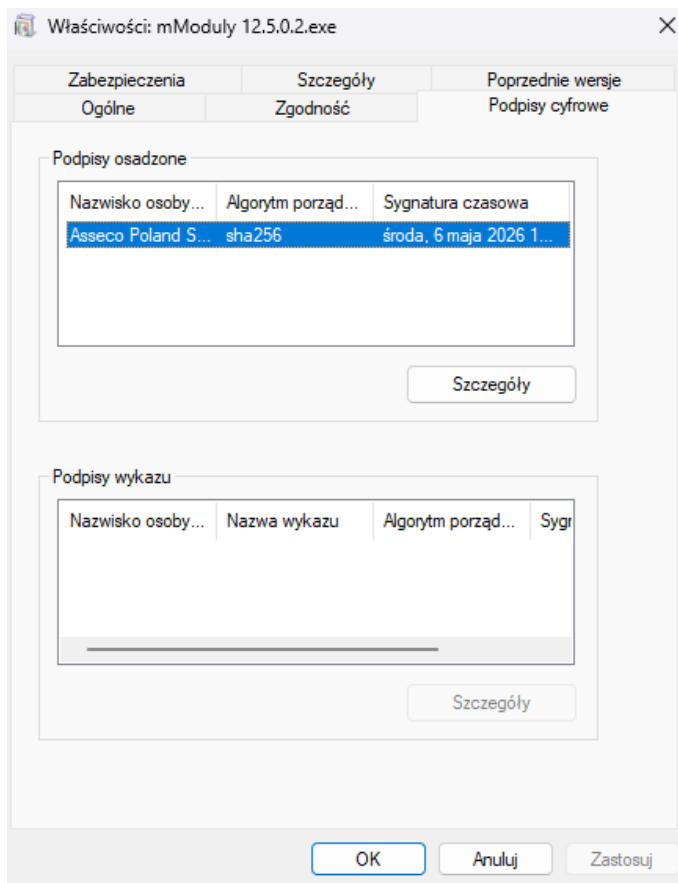
4.2. Ustawienia firewall

Włączone oprogramowanie typu firewall to konieczność w celu zapewnienia bezpieczeństwa. Zapora powinna zezwalać wyłącznie na ruch usług, które są świadomie uruchomione na komputerze. Dotyczy to zarówno ruchu przychodzącego jak i wychodzącego. Przy konfiguracji zapory ogniowej rekomenduje się stosowanie podejścia, w którym punktem wyjścia jest blokada komunikacji, a następnie świadome dodawanie pojedynczych reguł zezwalających dla komunikacji dla usług, aplikacji oraz na numerach portów. Takie podejście jest zalecane wyłącznie osobom posiadającym wiedzę techniczną, gdyż istnieje ryzyko zablokowania komunikacji, która jest wymagana do prawidłowego i bezpiecznego działania systemu operacyjnego oraz zainstalowanych aplikacji czy usług.

5. Aplikacje mModułów

5.1. Instalacja oraz aktualizacja

Bezwzględnie instalacje oraz aktualizacje mModułów należy wykonywać wyłącznie przez Instalator mModułów, Instalator mMedica lub pakiety plikowe, które są dostępne na oficjalnych stronach Asseco mMedica lub dostarczone przez pracowników działu Serwisu Asseco mMedica. Instalator mMedica oraz Instalator mModułów jest również podpisywany przez Asseco Poland S.A celem zapewnienia potwierdzenia pochodzenia pliku.



Rysunek 4: Weryfikacja pochodzenia instalatora mModułów

Należy pamiętać, że oprogramowanie mModułów pochodzące z innych źródeł może być zainfekowane i stanowić realne zagrożenie bezpieczeństwa.

5.2. Publikowanie aplikacji

Do sieci Internet powinny być publikowane tylko te aplikacje mModułów, które tego wymagają. Właściwa izolacja ruchu przychodzącego to jedna z podstaw zabezpieczenia aplikacji.

Przykładem aplikacji, która ze swojej natury powinna być publikowana do sieci Internet jest Portal eRejestracja. Z kolei mMDAB powinien być zawsze ukryty w sieci wewnętrznej placówki. Jeśli Portal eRejestracja łączy się do komponentu mMDAB\mMWS, który jest w innej lokalizacji wtedy rekomenduje się stosowanie VPN.

Aplikacja eArchiwum nie musi być publikowana w sieci Internet o ile nie jest zintegrowana z systemem Informacje Medyczne. Połączenia z: mMedica do eArchiwum, eRejestracja do eArchiwum, eArchiwum do mMDAB\MIAM jeśli nie odbywają się w ramach jednej sieci wewnętrznej powinny być realizowane za pomocą VPN.

W przypadku takich aplikacji jak TeleRejestracja, Konektor eRejestracja, Konektor MON, ruch przychodzący do tych aplikacji może być filtrowany do wybranych adresów IP. Informacje dotyczące IP systemów komunikujących się ze wskazanymi aplikacjami znajdują się w instrukcjach instalacji i konfiguracji tych aplikacji.

5.3. Baza danych

Komunikacja aplikacji mModułów z bazami danych PostgreSQL jest domyślnie zabezpieczona przez dwustronne uwierzytelnianie kluczami publicznymi oraz szyfrowana protokołem TLS. Należy bezwzględnie zapewniać

bezpieczeństwo kluczem serwera PostgreSQL oraz aplikacji mModułów przed działaniem osób trzecich. W przypadku podejrzenia kompromitacji kluczy należy wykonać ponowne przegenerowanie kluczy.

Warto wprowadzić politykę wykonywania i utrzymywania kopii zapasowych bazy danych mModułów. Taka polityka powinna mieć jasno zdefiniowane reguły:

- a) interwał wykonywania kopii zapasowych,
- b) liczba przechowywanych kopii zapasowych (retencje),
- c) w jaki sposób i co ile powinno wykonywać się testowe odtworzenie kopii zapasowej bazy danych celem weryfikacji, czy kopia jest wykonana poprawnie,
- d) miejsce lub miejsca przechowywania kopii wraz z określeniem zabezpieczeń.

Stanowczo nie zaleca się przechowywania kopii baz danych na maszynach, które służą jako serwery WWW. Bez względu na kopie powinny być zabezpieczone przed dostępem osób niepowołanych.

Aplikacja eRejestracja oraz eArchiwum umożliwiają utworzenie zadania dla Harmonogramu zadań Windows, które automatycznie będzie wykonywać kopię bazy danych w zadanym interwale. Dodatkowo w Portalu eRejestracja oraz Portalu eArchiwum jest wyświetlana historia wykonywania kopii bazy danych oraz istnieje możliwość nadania dodatkowego hasła zabezpieczającego kopię bazy danych.

Replikacja bazy danych PostgreSQL umożliwia ciągłe przesyłanie danych z serwera podstawowego na serwer zapasowy w celu zminimalizowania czasu niedostępności systemu w przypadku awarii. Z punktu widzenia bezpieczeństwa replikacja stanowi mechanizm zapewniający ciągłość działania (wysoką dostępność) i minimalizuje ryzyko utraty danych. Szczegóły dotyczące konfiguracji replikacji danych znajdują się w instrukcji modułu „Replikacja” opublikowanej na stronie <https://mmedica.asseco.pl/dokumentacja>.

Serwer zapasowy zawiera pełną kopię bazy danych, w związku z czym powinien być objęty takim samym reżimem bezpieczeństwa jak serwer podstawowy, w szczególności w zakresie aktualizacji systemu, kont dostępowych, oprogramowania antywirusowego oraz monitorowania logów. Po uruchomieniu replikacji należy regularnie weryfikować poprawność jej działania poprzez analizę logów PostgreSQL na serwerze zapasowym. W przypadku awarii serwera podstawowego konieczne jest przeprowadzenie procedury przełączenia ruchu na serwer zapasowy. Po przełączeniu serwer zapasowy przejmuje rolę produkcyjną i wymaga zapewnienia takich samych mechanizmów ochrony, jakie obowiązywały dla serwera podstawowego.

5.4. Filtrowanie ruchu

Aplikacje mModułów posiadają dodatkową możliwość filtrowania dostępów do wybranych obszarów aplikacji za pomocą adresu IP lub zakresu IP do wybranych sekcji aplikacji. Definiowanie polityki filtrowania odbywa się w plikach appsettings.json. Szczegółowe opisy funkcjonalności zostały opisane w instrukcjach instalacji oraz konfiguracji poszczególnych mModułów w rozdziałach „Filtrowanie komunikacji z wybranymi adresami IP”.

5.5. Ochrona przed atakami brute-force

Aplikacje mModułów są zabezpieczone przed atakami siłowymi (brute-force) na poziomie integracji z mMedica (za pomocą hasła usług sieciowych) oraz kont użytkowników na Portalach eRejestracja oraz eArchiwum.

W przypadku przekroczenia dopuszczalnej liczby prób komunikacji w integracji mMedica-mModuły lub mModuły-mModuły następuje blokada adresu IP strony wykonywującej komunikację. W Portalu eRejestracja opcję można włączyć aktywując parametr „Blokowanie adresów IP w usłudze eRWS” i definiując liczbę dopuszczalnych prób w parametrze „Liczba dopuszczalnych błędnych prób logowania w usłudze eRWS” w konfiguracji podstawowej.

Natomiast, analogiczne opcje w eArchiwum są dostępne pod nazwami „Blokowanie adresów IP w API mMedica” oraz „Liczba dopuszczalnych błędnych prób logowania w API mMedica” w konfiguracji podstawowej.

Dla mModułów, które mają bezpośredni dostęp do baz danych mMedica (mMWS, MIAM, TeleRejestracja, Konektor eRejestracja, Konektor MON) konfiguracja maksymalnej liczba błędnych prób logowań do usługi jest dostępna w Konfiguratorze mMedica: „Komunikacja” \ „Inne”.

W przypadku kont użytkowników Portalu eRejestracja oraz eArchiwum może nastąpić blokada konta (poprawna nazwa użytkownika i błędne hasło) lub blokada IP (błędna nazwa użytkownika) na etapie logowania. W Portalu eRejestracja blokada użytkownika lub IP następuje po przekroczeniu wartości "Liczba dopuszczalnych błędnych prób logowania" w konfiguracji podstawowej. Z Kolei, w eArchiwum wartość dopuszczalnych prób błędnego logowania wynosi 5.

Ponadto, w Portalu eRejestracja istnieje możliwość integracji z usługą Google reCAPTCHA, która znacząco zwiększa ochronę przed zautomatyzowanymi atakami.

5.6. Uwierzytelnianie dwuskładnikowe

Aplikacja eRejestracja oraz eArchiwum mają możliwość konfiguracji uwierzytelniania dwuskładnikowego za pomocą przesyłania kodu na adres e-mail lub metodą TOTP. Uwierzytelnianie dwuskładnikowe znacząco zwiększa bezpieczeństwo konta, ponieważ oprócz hasła wymaga dodatkowego potwierdzenia tożsamości. Innymi słowy, jeśli hasło do konta zostanie skompromitowane to bez drugiego składnika nie uda się uzyskać dostępu do systemu. Dzięki temu uwierzytelnienie dwuskładnikowe skutecznie chroni przed phishingiem, wyciekami danych i nieautoryzowanym dostępem. Taką ochronę warto stosować w szczególności w przypadku kont administracyjnych na Portalu eRejestracja oraz eArchiwum.