Security

Het beveiligen van je IIS (Internet Information Services) en webserver is essentieel om aanvallen en inbreuken te voorkomen. Hier zijn enkele stappen die je kunt nemen om de beveiligingsproblemen aan te pakken:

1. Updates en Patches

- **Houd je server up-to-date:** Installeer de nieuwste beveiligingsupdates en patches voor je besturingssysteem en IIS. Dit is een van de belangrijkste stappen om bekende kwetsbaarheden te dichten.

2. Server Configuratie

- **Minimale installatie:** Installeer alleen de noodzakelijke onderdelen en services. Minder geïnstalleerde componenten betekenen minder potentiële aanvalsvectoren.
- **Gebruik van IIS lockdown tool:** Overweeg het gebruik van de IIS Lockdown Tool om de aanvalsvectoren te minimaliseren.
- **IIS Hardening:** Volg de Microsoft security best practices voor IIS hardening.

3. Authenticatie en Autorisatie

- **Sterke wachtwoorden:** Zorg ervoor dat alle accounts sterke, complexe wachtwoorden gebruiken.
- **Beperk administratieve toegang:** Geef alleen administratieve toegang aan noodzakelijke gebruikers en gebruik rolgebaseerde toegangscontrole (RBAC).
- **Gebruik SSL/TLS:** Versleutel communicatie met SSL/TLS om afluisteren te voorkomen.

4. Firewall en Netwerkbeveiliging

- **Gebruik een firewall:** Configureer een firewall om alleen noodzakelijke poorten open te stellen (bijv. poort 80 voor HTTP en 443 voor HTTPS).
- **IP-restricties:** Beperk toegang tot de server tot alleen vertrouwde IP-adressen indien mogelijk.

5. Logboekregistratie en Monitoring

- **Actief loggen:** Configureer logging in IIS om alle toegang en fouten bij te houden. Analyseer deze logs regelmatig op verdachte activiteiten.
- **Intrusion Detection System (IDS):** Gebruik een IDS om verdachte activiteiten in je netwerk te detecteren en te melden.

6. Webapplicatie Beveiliging

- **Web Application Firewall (WAF):** Overweeg het gebruik van een WAF om je webapplicaties te beschermen tegen veelvoorkomende aanvallen zoals SQL-injecties en cross-site scripting (XSS).

- **Input Validatie:** Zorg ervoor dat je webapplicaties alle invoer valideren en ontsmetten om te voorkomen dat kwaadwillende gebruikers schadelijke gegevens kunnen injecteren.

7. Beperk Informatie

- **Error Reporting:** Minimaliseer de informatie die wordt weergegeven in foutmeldingen. Configureer IIS om gedetailleerde foutmeldingen alleen weer te geven voor interne verzoeken.
- **Directory Browsing:** Schakel directory browsing uit om te voorkomen dat gebruikers de inhoud van directories kunnen bekijken.

8. Back-ups en Herstel

- **Reguliere back-ups:** Maak regelmatig back-ups van je server en webapplicaties, en test deze back-ups om er zeker van te zijn dat ze werken.
- **Herstelplan:** Heb een herstelplan klaar voor het geval dat je server gecompromitteerd wordt.

9. Security Scans en Audits

- **Regelmatige scans:** Voer regelmatig beveiligingsscans en kwetsbaarheidsbeoordelingen uit op je server en webapplicaties.
- **Penetratietests:** Laat periodieke penetratietests uitvoeren door externe partijen om de effectiviteit van je beveiligingsmaatregelen te beoordelen.

10. Educatie en Bewustzijn

- **Training:** Zorg ervoor dat je team op de hoogte is van de nieuwste beveiligingsdreigingen en best practices door middel van regelmatige training en bewustwordingssessies.

Security WordPress

1. Updates en Patches

- **Core, plugins en thema's up-to-date houden:** Zorg ervoor dat je altijd de nieuwste versies van WordPress, plugins en thema's gebruikt, omdat updates vaak beveiligingspatches bevatten.

2. Sterke Inloggegevens

- **Sterke wachtwoorden:** Gebruik complexe, sterke wachtwoorden voor alle accounts, vooral voor de admin-account.
- **Wijzig de standaard gebruikersnaam "admin":** Gebruik een andere naam dan "admin" voor je beheerdersaccount.

3. Two-Factor Authentication (2FA)

- **Inschakelen van 2FA:** Voeg een extra beveiligingslaag toe door two-factor authentication te implementeren voor alle gebruikers.

4. Beveiliging van de Inlogpagina

- **Inlogpogingen beperken:** Gebruik plugins zoals "Login Lockdown" of "Limit Login Attempts" om het aantal inlogpogingen te beperken.
- **ReCaptcha:** Voeg een reCaptcha toe aan je inlogpagina om bots te blokkeren.

5. Bestands- en Maprechten

- **Correcte bestandsrechten instellen:** Zorg ervoor dat de bestandsrechten correct zijn ingesteld. De meeste WordPress-bestanden moeten 644 rechten hebben, mappen 755, en het wp-config.php bestand 600.
- **Belangrijke bestanden beschermen:** Beveilig belangrijke bestanden zoals wp-config.php en .htaccess door ze te verplaatsen of extra beveiligingsmaatregelen toe te voegen.

6. Gebruik van Beveiligingsplugins

- **Installeer beveiligingsplugins:** Plugins zoals Wordfence, Sucuri Security, en iThemes Security kunnen helpen bij het beschermen van je site door functies zoals firewall, malware-scans en inbraakdetectie.

7. Database Beveiliging

- **Wijzig het standaard tabelvoorvoegsel:** Verander het standaard wp_ tabelvoorvoegsel naar iets unieks om SQL-injectie-aanvallen te helpen voorkomen.
- **Sterke database-wachtwoorden:** Zorg voor een sterk wachtwoord voor je databasegebruiker.

8. SSL/TLS

- **Gebruik SSL/TLS:** Versleutel de communicatie tussen je server en de bezoekers door een SSL-certificaat te gebruiken. Dit kan eenvoudig worden ingesteld met plugins zoals Really Simple SSL.

9. Verberg WordPress Versie

- **Verberg je WordPress versie:** Verwijder de WordPress-versie informatie uit je broncode om het voor aanvallers moeilijker te maken om gerichte aanvallen uit te voeren.

10. Back-ups

- **Regelmatige back-ups:** Maak regelmatig back-ups van je volledige site en database. Gebruik plugins zoals UpdraftPlus of BackWPup om geautomatiseerde back-ups te maken en sla deze op een veilige locatie op.

11. Monitoring en Loggen

- **Actief loggen:** Houd logs bij van alle activiteiten op je site. Plugins zoals WP Security Audit Log kunnen hierbij helpen.
- **Monitoring:** Gebruik een monitoring service om je site te controleren op downtime en beveiligingsproblemen.

12. Firewall en Security Headers

- **Web Application Firewall (WAF):** Gebruik een WAF om je site te beschermen tegen veelvoorkomende aanvallen zoals SQL-injecties en XSS.
- **Security Headers:** Voeg security headers toe zoals Content Security Policy (CSP), X-Content-Type-Options, en X-Frame-Options.

13. Gebruikersbeheer

- **Beperk de toegang van gebruikers:** Geef gebruikers alleen de rechten die ze nodig hebben en verwijder inactieve gebruikersaccounts.
- **Controleren van plugins en thema's:** Verwijder ongebruikte plugins en thema’s en zorg ervoor dat de resterende plugins en thema’s afkomstig zijn van betrouwbare bronnen.

Overige info

Verbeteren van de Beveiliging van WordPress

1. **Regelmatige Updates**:
    - **Core, Plugins en Thema's**: Zorg ervoor dat je altijd de nieuwste versies van WordPress, plugins en thema's gebruikt. Updates bevatten vaak beveiligingspatches die bekende kwetsbaarheden dichten (Kinsta®) (Sucuri).
2. **Sterke Wachtwoorden en Unieke Gebruikersnamen**:
    - **Sterke Wachtwoorden**: Gebruik complexe wachtwoorden voor alle accounts en vermijd het gebruik van de standaard "admin" gebruikersnaam. Hulpmiddelen zoals KeePass of online wachtwoordmanagers kunnen helpen bij het genereren en opslaan van sterke wachtwoorden (Kinsta®).
3. **Tweefactorauthenticatie (2FA)**:
    - **Extra Beveiligingslaag**: Voeg een extra beveiligingslaag toe door tweefactorauthenticatie in te schakelen met plugins zoals Google Authenticator (Codeless).
4. **Beperk Inlogpogingen**:
    - **Bescherming tegen Brute Force-aanvallen**: Gebruik plugins zoals Login LockDown of Jetpack om het aantal inlogpogingen te beperken en brute force-aanvallen te voorkomen (Codeless).
5. **SSL Certificaten en HTTPS**:
    - **Versleutelde Communicatie**: Zorg ervoor dat je website HTTPS gebruikt om de communicatie tussen je site en gebruikers te versleutelen. Veel hosts bieden gratis SSL-certificaten via Let's Encrypt (Learn WordPress with WPLift) (Codeless).
6. **Web Application Firewall (WAF)**:
    - **Bescherming tegen Aanvallen**: Gebruik een WAF om kwaadwillende verkeer te filteren en blokkeren. Diensten zoals Cloudflare of Sucuri kunnen deze bescherming bieden (Codeless).
7. **Bestandsbewerking Uitschakelen**:
    - **Voorkomen van Ongeautoriseerde Wijzigingen**: Voeg **define('DISALLOW_FILE_EDIT', true);** toe aan je wp-config.php bestand om de bestandseditor in WordPress uit te schakelen (Codeless).
8. **Regelmatige Back-ups**:
    - **Veiligstellen van Gegevens**: Plan regelmatige back-ups met plugins zoals UpdraftPlus of Jetpack en bewaar deze op externe servers (Codeless).

9. **Veilige Hosting**:
    - **Kies een Betrouwbare Webhost**: Kies een webhost met sterke beveiligingspraktijken, inclusief regelmatige updates, firewalls, en beveiligingsmonitoring (Codeless).
10. **Beveiligingsplugins**:
    - **Gebruik van Plugins**: Maak gebruik van beveiligingsplugins zoals WordFence, SolidWP (voorheen iThemes Security), All-In-One WP Security, of WPScan om kwetsbaarheden te scannen en extra beveiligingsfuncties toe te voegen (WPBeginner).

Beveiliging van IIS (Internet Information Services)

1. **Regelmatige Updates**:
    - **Houd de Server Bijgewerkt**: Zorg ervoor dat je IIS-server en alle geïnstalleerde componenten up-to-date zijn met de laatste beveiligingspatches van Microsoft (Jetpack).
2. **SSL Certificaten en HTTPS**:
    - **Gebruik HTTPS**: Versleutel alle communicatie naar je IIS-server door HTTPS te gebruiken. Verkrijg en configureer SSL-certificaten op de juiste manier (Jetpack).
3. **Web Application Firewall (WAF)**:
    - **Bescherming tegen Aanvallen**: Implementeer een WAF om te beschermen tegen veelvoorkomende webaanvallen zoals SQL-injectie en cross-site scripting (XSS) (Jetpack).
4. **Applicatie-isolatie**:
    - **Gebruik van Applicatiepools**: Isoleer verschillende applicaties door gebruik te maken van applicatiepools. Dit helpt voorkomen dat een gecompromitteerde applicatie invloed heeft op andere applicaties op dezelfde server (Jetpack).
5. **Schakel Onnodige Functies uit**:
    - **Verminder het Aanvalsoppervlak**: Schakel ongebruikte functies en modules in IIS uit (Jetpack).
6. **Veilige Configuraties**:
    - **Beveilig IIS Configuratie**: Zorg ervoor dat IIS correct is geconfigureerd door best practices te volgen, zoals het uitschakelen van directory browsing en het instellen van de juiste bestandsrechten (Jetpack).
7. **Log Monitoring**:
    - **Controleer Logs Regelmatig**: Houd logs bij voor verdachte activiteiten en gebruik tools zoals Microsoft's Advanced Threat Analytics om potentiële dreigingen te detecteren en erop te reageren (Jetpack).
8. **Beperk Toegang**:
    - **Principe van de Minst Noodzakelijke Toegang**: Implementeer het principe van de minst noodzakelijke toegang voor alle gebruikers en diensten (Jetpack).

Door deze stappen te volgen, kun je de beveiliging van zowel je WordPress-website als je IIS-webserver aanzienlijk verbeteren en de risico's op aanvallen en inbreuken verkleinen.

Handleiding

WordPress Beveiliging

1. Updates en Patches

- **WordPress Kern, Plugins en Thema's Bijwerken**
    1. Log in op je WordPress-dashboard.
    2. Ga naar **Dashboard > Updates**.
    3. Werk de WordPress-kern, plugins, en thema's bij naar de nieuwste versies.

2. Sterke Wachtwoorden en Unieke Gebruikersnamen

- **Gebruikersnaam en Wachtwoord Wijzigen**
    1. Ga naar **Gebruikers > Alle Gebruikers**.
    2. Klik op de gebruiker die je wilt bewerken.
    3. Verander de gebruikersnaam (als dit een nieuwe gebruiker is) en gebruik een sterk wachtwoord. Gebruik bijvoorbeeld een wachtwoordgenerator.

3. Tweefactorauthenticatie (2FA)

- **2FA Instellen met Google Authenticator**
    1. Installeer en activeer een plugin zoals "Google Authenticator".
    2. Ga naar de plugin-instellingen en volg de configuratiestappen om 2FA in te schakelen.

4. Inlogpogingen Beperken

- **Beperk Inlogpogingen met Login LockDown**
    1. Installeer en activeer de "Login LockDown" plugin.
    2. Ga naar **Instellingen > Login LockDown** en configureer de plugin om inlogpogingen te beperken.

5. SSL Certificaten en HTTPS

- **SSL Certificaat Instellen**
    1. Verkrijg een SSL-certificaat via je hostingprovider (bijvoorbeeld Let's Encrypt).
    2. Installeer en activeer de "Really Simple SSL" plugin.
    3. Volg de stappen in de plugin om HTTPS op je site in te schakelen.

6. Web Application Firewall (WAF)

- **WAF Gebruiken met Cloudflare**
    1. Maak een account aan op Cloudflare en voeg je website toe.
    2. Volg de instructies om je DNS-instellingen bij te werken en Cloudflare als je WAF te gebruiken.

7. Bestandsbewerking Uitschakelen

- **Bestandsbewerking Uitschakelen in wp-config.php**
    1. Open je **wp-config.php** bestand in een teksteditor.
    2. Voeg de volgende regel toe: **define('DISALLOW_FILE_EDIT', true);**.
    3. Sla het bestand op en upload het terug naar je server.

8. Regelmatige Back-ups

- **Back-ups Maken met UpdraftPlus**
    1. Installeer en activeer de "UpdraftPlus" plugin.
    2. Ga naar **Instellingen > UpdraftPlus Backups** en configureer de back-upinstellingen.
    3. Plan regelmatige back-ups en kies een externe opslaglocatie zoals Google Drive of Dropbox.

9. Beveiligingsplugins

- **Beveiligingsplugin Installeren**
    1. Installeer en activeer een beveiligingsplugin zoals "WordFence" of "All-In-One WP Security".
    2. Ga naar de instellingen van de plugin en volg de configuratiestappen om je site te beveiligen.

IIS Beveiliging

1. Updates en Patches

- **Windows Update Configureren**
    1. Open de Windows Server Update Services (WSUS) console.
    2. Configureer automatische updates om ervoor te zorgen dat IIS en het besturingssysteem up-to-date blijven.

2. SSL Certificaten en HTTPS

- **SSL Certificaat Configureren**
    1. Verkrijg een SSL-certificaat via een Certificate Authority (CA).
    2. Open de IIS Manager.
    3. Ga naar **Sites > je site > Bindings**.

4. Klik op **Add** en selecteer **https** als type.
5. Kies je SSL-certificaat en klik op **OK**.

3. Web Application Firewall (WAF)

- **WAF Instellen**
    1. Implementeer een WAF zoals ModSecurity met IIS.
    2. Volg de installatie- en configuratiehandleiding van de WAF-provider.

4. Applicatie-isolatie

- **Applicatiepools Configureren**
    1. Open de IIS Manager.
    2. Ga naar **Application Pools**.
    3. Maak afzonderlijke applicatiepools voor verschillende applicaties om isolatie te garanderen.

5. Onnodige Functies Uitschakelen

- **Functies en Modules Uitschakelen**
    1. Open de IIS Manager.
    2. Ga naar **Server Roles** en schakel onnodige rollen en functies uit.

6. Veilige Configuraties

- **IIS Configureren**
    1. Schakel directory browsing uit: **IIS Manager > Directory Browsing > Disable**.
    2. Stel juiste bestandsrechten in: Zorg ervoor dat alleen noodzakelijke gebruikers toegang hebben tot specifieke mappen.

7. Log Monitoring

- **Logboeken Controleren**
    1. Open de Event Viewer om logs te bekijken.
    2. Controleer regelmatig op verdachte activiteiten en configureer alerts indien nodig.

8. Toegangsbeheer

- **Principe van de Minst Noodzakelijke Toegang**
    1. Beperk de toegangsrechten van gebruikers tot wat strikt noodzakelijk is.
    2. Gebruik groep- en gebruikersbeleid om toegangsrechten te beheren.

Yasha Noteringen:

CHECKLIST

Advies schrijven en verbeteringen toepassen bij de volgende stukken.

Website:

- Kijk naar de versie van de website.
- Kijk naar de plugins die gebruikt worden op de website.

I.I.S. :

- Kijk naar de versie van de I.I.S.

App:

- Kijk naar de versie van de app.
- Kijk of er updates mogelijk zijn voor de app.

Server zelf:

- Kijk naar de OS versie zoals windows 10 of server 2019 en vertel waarom dit geupgrade moet worden.
- Kijk naar de drivers.
- Kijk of er backups gemaakt worden.
- Kijk naar server data.

Netwerk:

- Kijk naar of firewall aan staat.
- Kijk naar poorten die open staan.

Om te kijken welke poorten er open staan gebruik command:
#Netstat of #Netstat -S

Kijk naar welke poorten open staan:

Adviseer over welke poorten dicht moeten en pas dit aan. Vertel ook hoe bepaalde poorten die verplicht open moeten staan gecontroleerd open kunnen blijven of poorten die niet nodig zijn gesloten kunnen worden.

Timo Noteringen:

Elke appilicatie moet geupdate worden naar de nieuwste versie.

Netstat.

Poorten staan open, port 80 staat open. Die moet open blijven maar wel gecontroleerd d.m.v. een firewall. Port 443 is https en ook open.

Je heb lagen en daar moet je over praten, geef advies zo specifiek mogelijk.

Staat de firewall aan? Staat anti virus aan?

Porten die voor applicaties zijn gereserveerd is.

Kwaadwillige verstoppen zich in de laatste twee lagen.

Maakt niet uit welke applicatie, je kan de blueprint blueprint in elke laag zetten.

Geef duidelijk advies, porten, back-ups, alles moet geüpdate worden.

Geen domein omgeving, je kan naar een domein gaan om het veiliger te maken, iedereen op het netwerk kan toegang krijgen. Zodra je naar een domein gaat kan dit niet.

Wachtwoord beleid.

Netwerk, server, applicaties