1 PIANO ADEGUAMENTO DEL SITO WEB AL GDPR

Inserire i dati relativi al Sito Web da analizzare:

NOME SITO

WebConsultingSMP | Social Media Press

INDIRIZZO

https://www.webconsultingsmp.it/

Analisi effettuata da:

Nome	Claudio Ancillotti	**Email**	claudio.ancillotti@gmail.com	**Telefono**	348 7289513

DATA	*31.08.2018*	**Tool**	

SEZIONE	ADEGUAMENTO
PRIVACY E COOKIE POLICY	Come richiesto nell' Articolo 12 GDPR, (**Trasparenza e Modalità**) è necessario trasmettere tutte le informazioni relative a come gestisci ed elabori i dati dell'utente con le seguenti modalità: 1. In un linguaggio chiaro e semplice; 2. Facilmente accessibile; 3. Conciso; 4. Trasparente; 5. Intellegibile; 6. Accesso al documento Gratuito
	MODELLO WORDPRESS
	Chi siamo In questa sezione è necessario riportare l'URL del sito, nonché il nome dell'azienda, dell'organizzazione o dell'individuo dietro di esso e alcune informazioni di contatto accurate. La quantità di informazioni che potrebbe essere obbligatoria per la presentazione varierà in base alle normative aziendali locali o nazionali. Ad esempio, potrebbe essere obbligatorio visualizzare un indirizzo fisico, un indirizzo registrato o il numero di registrazione della società. ***Testo suggerito:*** *L'indirizzo del nostro sito web è: https://www.webconsultingsmp.it*.

Quali dati personali raccogliamo e perché li raccogliamo

In questa sezione dovresti annotare quali dati personali raccogli dagli utenti e visitatori del sito. Questo potrebbe includere dati personali, come nome, indirizzo email, preferenze personali sull'account; dati transazionali, come informazioni sugli acquisti; e dati tecnici, come informazioni sui cookies.
Dovresti anche prendere nota della raccolta e della conservazione di dati personali sensibili, come i dati relativi alla salute.
Oltre a elencare i dati personali che raccogli, devi motivare perché li raccogli. Queste spiegazioni devono considerare sia la base legale per la raccolta e la conservazione dei dati sia il consenso attivo che l'utente ha fornito.
I dati personali non vengono creati solo dalle interazioni dell'utente con il tuo sito. I dati personali sono generati anche da processi tecnici come moduli di contatto, commenti, cookie, statistiche e incorporamenti di terze parti.
Di default WordPress non raccoglie dati personali sui visitatori e raccoglie solo i dati mostrati nella schermata Profilo utente dagli utenti registrati. Tuttavia alcuni plugin potrebbero raccogliere dati personali. Dovresti aggiungere le informazioni rilevanti di seguito.

Commenti

In questa sottosezione si dovrebbe riportare quali informazioni vengono prese attraverso i commenti. Abbiamo preso nota dei dati raccolti da WordPress per impostazione predefinita.
Testo suggerito: *Quando i visitatori lasciano commenti sul sito, raccogliamo i dati mostrati nel modulo dei commenti oltre all'indirizzo IP del visitatore e la stringa dello user agent del browser per facilitare il rilevamento dello spam.*
Una stringa anonimizzata creata a partire dal tuo indirizzo email (altrimenti detta hash) può essere fornita al servizio Gravatar per vedere se lo stai usando. La privacy policy del servizio Gravatar è disponibile qui: https://automattic.com/privacy/. Dopo l'approvazione del tuo commento, la tua immagine del profilo è visibile al pubblico nel contesto del tuo commento.

Media

In questa sottosezione dovresti annotare quali informazioni potrebbero essere divulgate dagli utenti che possono caricare media files. Tutti i file caricati sono solitamente pubblicamente accessibili.
Testo suggerito: *Se carichi immagini sul sito web, dovresti evitare di caricare immagini che includono i dati di posizione incorporati (EXIF GPS). I*

visitatori del sito web possono scaricare ed estrarre qualsiasi dato sulla posizione dalle immagini sul sito web.

Modulo di contatto

Per impostazione predefinita, WordPress non include un modulo di contatto. Se si utilizza un plugin per il modulo di contatto, utilizzare questa sottosezione per descrivere quali dati personali vengono acquisiti quando qualcuno invia un modulo di contatto e per quanto tempo lo si conserva. Ad esempio, è possibile riportare che si mantengono gli invii dei moduli di contatto per un certo periodo ai fini del servizio clienti, ma non si utilizzano le informazioni inviate attraverso di loro per scopi di marketing.

Cookie

In questa sottosezione dovresti elencare i cookie utilizzati dal tuo sito web, compresi quelli impostati dai tuoi plugin, social media e statistiche. Abbiamo fornito i cookie che WordPress installa di default.

Testo suggerito: *Se lasci un commento sul nostro sito, puoi scegliere di salvare il tuo nome, indirizzo email e sito web nei cookie. Sono usati per la tua comodità in modo che tu non debba inserire nuovamente i tuoi dati quando lasci un altro commento. Questi cookie dureranno per un anno.*

Se hai un account e accedi a questo sito, verrà impostato un cookie temporaneo per determinare se il tuo browser accetta i cookie. Questo cookie non contiene dati personali e viene eliminato quando chiudi il browser.

Quando effettui l'accesso, verranno impostati diversi cookie per salvare le tue informazioni di accesso e le tue opzioni di visualizzazione dello schermo. I cookie di accesso durano due giorni mentre i cookie per le opzioni dello schermo durano un anno. Se selezioni "Ricordami", il tuo accesso persisterà per due settimane. Se esci dal tuo account, i cookie di accesso verranno rimossi.

Se modifichi o pubblichi un articolo, un cookie aggiuntivo verrà salvato nel tuo browser. Questo cookie non include dati personali, ma indica semplicemente l'ID dell'articolo appena modificato. Scade dopo 1 giorno.

Contenuto incorporato da altri siti web

Testo suggerito: *Gli articoli su questo sito possono includere contenuti incorporati (ad esempio video, immagini, articoli, ecc.). I contenuti incorporati da altri siti web si comportano esattamente allo stesso modo come se il visitatore avesse visitato l'altro sito web.*

Questi siti web possono raccogliere dati su di te, usare cookie, integrare ulteriori tracciamenti di terze parti e monitorare l'interazione con essi, incluso il tracciamento della tua interazione con il contenuto incorporato se

hai un account e sei connesso a quei siti web.

Analytics

In questa sottosezione dovresti annotare quali pacchetti analitici usi, come gli utenti possono uscire dal tracciamento analitico, e un link alla privacy policy dei tuoi provider di analis'i, se presenti.
Di default WordPress non raccoglie dati statistici. Tuttavia, molti account di hosting Web raccolgono dati statistici anonimi. Potresti aver installato anche un plugin per WordPress che fornisce servizi di analisi. In tal caso, aggiungi qui le informazioni da quel plugin.

Con chi condividiamo i tuoi dati

In questa sezione dovresti nominare ed elencare tutti i fornitori di terze parti con cui condividi i dati del sito, inclusi partner, servizi basati su cloud, sistemi di pagamento e fornitori di servizi di terze parti, e riportare quali dati condividi con loro e perché. Aggiungi un collegamento alle loro privacy policies, se possibile.
Per impostazione predefinita, WordPress non condivide alcun dato personale con nessuno.

Per quanto tempo conserviamo i tuoi dati

In questa sezione dovresti spiegare per quanto tempo conservi i dati personali raccolti o elaborati dal sito web. Anche se è tua responsabilità descrivere per quanto tempo mantieni ogni set di dati e perché lo mantieni, queste informazioni devono essere elencate qui. Ad esempio, potresti voler dire che mantieni le voci dei moduli di contatto per sei mesi, i record delle statistiche per un anno e i record di acquisto dei clienti per dieci anni.
Testo suggerito: *Se lasci un commento, il commento e i relativi metadati vengono conservati a tempo indeterminato. È così che possiamo riconoscere e approvare automaticamente eventuali commenti successivi invece di tenerli in una coda di moderazione.*
Per gli utenti che si registrano sul nostro sito web (se presenti), memorizziamo anche le informazioni personali che forniscono nel loro profilo utente. Tutti gli utenti possono vedere, modificare o cancellare le loro informazioni personali in qualsiasi momento (eccetto il loro nome utente che non possono cambiare). Gli amministratori del sito web possono anche vedere e modificare queste informazioni.

Quali diritti hai sui tuoi dati

In questa sezione dovresti indicare quali diritti hanno i tuoi utenti nella gestione dei loro dati e come possono esercitarli
Testo suggerito: *Se hai un account su questo sito, o hai lasciato*

commenti, puoi richiedere di ricevere un file esportato dal sito con i dati personali che abbiamo su di te, compresi i dati che ci hai fornito. Puoi anche richiedere che cancelliamo tutti i dati personali che ti riguardano. Questo non include i dati che siamo obbligati a conservare per scopi amministrativi, legali o di sicurezza.

Dove spediamo i tuoi dati

In questa sezione dovresti elencare tutti i trasferimenti di dati del sito al di fuori dell'Unione Europea e descrivere in che modo i dati sono salvaguardati in base agli standard europei di protezione dei dati. Questo potrebbe includere il tuo web hosting, il cloud storage o altri servizi di terze parti.
La normativa europea sulla protezione dei dati richiede che i dati riguardanti i residenti europei trasferiti al di fuori dell'Unione Europea siano tutelati secondo gli stessi standard come se i dati fossero in Europa. Cosi oltre a elencare dove vengono spostati i dati, dovresti descrivere in che modo vengono assicurati che questi standard siano soddisfatti da parte tua o dai tuoi fornitori di terze parti, sia attraverso un accordo come il Privacy Shield, clausole nei tuoi contratti o regole aziendali vincolanti.
Testo suggerito: *I commenti dei visitatori possono essere controllati attraverso un servizio di rilevamento automatico dello spam.*

Le tue informazioni di contatto

In questa sezione si dovrebbe segnalare un metodo di contatto per problemi riguardanti la privacy. Se è necessario disporre di un Responsabile della Protezione dei Dati (DPO), elencare qui il loro nome e i dettagli completi del contatto.

Informazioni aggiuntive

Se usi il tuo sito per scopi commerciali e ti impegni in una raccolta più complessa o nel trattamento dei dati personali, dovresti prendere nota delle seguenti informazioni nella tua privacy policy oltre alle informazioni di cui abbiamo già discusso.

Come proteggiamo i tuoi dati

In questa sezione dovresti spiegare quali misure hai preso per proteggere i dati dei tuoi utenti'. Questo potrebbe includere misure tecniche come la crittografia; misure di sicurezza come l'autenticazione a due fattori; e misure come la formazione del personale sulla protezione dei dati. Qui puoi anche menzionare se hai effettuato una valutazione dell'impatto sulla privacy.

Quali procedure abbiamo predisposto per prevenire la violazione dei dati

In questa sezione, dovresti spiegare quali procedure attuerai nell'eventualità di una falla dei dati, sia essa potenziale o reale, come ad esempio sistemi di report interni, messa in contatto automatica o cacciatori di bug.

Da quali terze parti riceviamo dati

Se il tuo sito web riceve dati sugli utenti da terze parti, compresi gli inserzionisti, queste informazioni devono essere incluse nella sezione della tua privacy policy che tratta i dati di terze parti.

Quale processo decisionale automatizzato e/o profilazione facciamo con i dati dell'utente

Se il tuo sito web fornisce un servizio che include il processo decisionale automatico, per esempio permettere ai clienti di richiedere credito, o aggregare i loro dati in un profilo pubblicitario - devi notare che questo sta succedendo, e include informazioni riguardo come quell'informazione è usata, quali decisioni sono fatte con quei dati aggregati, e quali diritti hanno gli utenti sulle decisioni prese senza intervento umano.

Requisiti di informativa normativa del settore

Se sei un membro di un'industria regolamentata, o se sei soggetto a ulteriori leggi sulla privacy, potrebbe esserti richiesto di rivelare tale informazione qui.

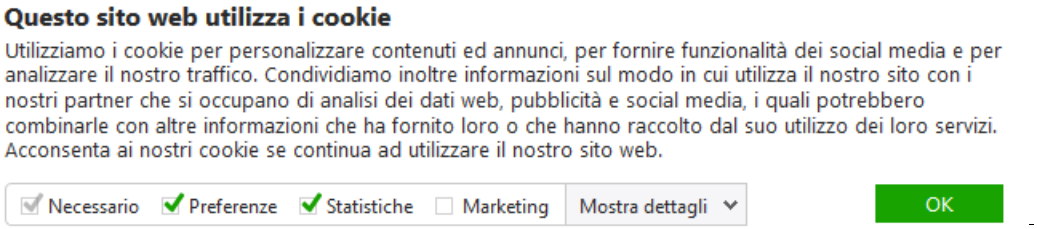
SOLUZIONI

- Il Generatore di Privacy e Cookie Policy di IUBENDA

COOKIE BANNER

Come richiesto nell' Articolo 7 GDPR (**Condizioni per il consenso**)
Non basta che l'utente accetti l'utilizzo dei cookies sul sito web, ma il consenso deve essere:
• **informato e preventivo:** l'utente deve essere informato in anticipo sui cookie utilizzati sul tuo sito web, sulle loro finalità e localizzazione. L'utente deve deve inoltre poter consentire o non consentire a ciascuna tipologia di cookie in ogni momento;
• **esplicito**: il consenso o non consenso dell'utente deve essere una chiara azione affermativa e positiva;
• **registrato**: il consenso deve essere registrato, ovvero devi tenere traccia di tale consenso così da avere la prova che l'utente abbia davvero acconsentito o meno;
• **reversibile**: l'utente deve poter modificare il consenso in qualsiasi momento, anche ritirarlo, pur continuando normalmente la navigazione sul tuo sito web.

MODELLO



SOLUZIONI

- Cookiebot
- Cookie Control
- Iubenda Cookie Solution
- OneTrust

RACCOLTA DEI DATI, ELABORAZIONE CONSERVAZIONE

*Articolo 25 GDPR (***Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita***)*
2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

- **Diritto di accesso:** l'utente può accedere ai propri dati personali
- **Diritto all'oblio:** l'utente può richiedere la cancellazione dei propri dati personali
- **Portabilità:** l'utente può scaricare i propri dati per il trasferimento su altra piattaforma

E' indispensabile adottare un'area riservata nella quale l'utente può visionare, scaricare e cancellare le proprie informazioni.

ACCESSO AI DATI PERSONALI

visibile nella versione PRO

ESPORTAZIONE DEI DATI PERSONALI

CANCELLAZIONE DEI DATI PERSONALI

SOLUZIONI

- GDPR Privacy Center
- GDPR Personal Data Reports
- GDPR Solutions for Wordpress

MODULI INSERIMENTO DATI

CONTATTI

visibile nella versione PRO

COMMENTI

Leave a Reply

visibile nella versione PRO

R E CHATBOT

Trattamento Dati

SOLUZIONI

- WP GDPR Compliance

SICUREZZA

Obbligo, per il titolare del trattamento, di **adottare misure adeguate per la sicurezza dei dati** nell' Articolo 32 GDPR, (**Sicurezza del trattamento**)
L'articolo 32 del Regolamento UE prevede, infatti, che vengano adottate misure di sicurezza idonee a "garantire un livello di sicurezza adeguato al rischio" del trattamento.

Passare a HTTPS

passare da HTTP ad HTTPS significa garantire che le informazioni in transito sulla Rete - dal client dell'utente al nostro sito web - siano criptate e non "in chiaro". Si tratta di una procedura piuttosto semplice: se avete un hosting condiviso sarà sufficiente richiedere al Vs. provider il passaggio ad una soluzione con SSL, se avete un server dedicato dovrete provvedere da soli ad installare un certificato SSL (ce ne sono anche di gratuiti - Let's Encrypt)

Guida Google:

Proteggere il sito con il protocollo HTTPS

Proteggere il proprio sito e i propri utenti

Che cos'è il protocollo HTTPS?

visibile nella versione PRO

HTTPS (Hypertext Transfer Protocol Secure) è un protocollo per la comunicazione che garantisce l'integrità e la riservatezza dei dati scambiati tra gli utenti e il sito. Gli utenti si aspettano che l'utilizzo di un sito web sia sicuro e privato. Ti invitiamo, pertanto, ad adottare HTTPS per proteggere la connessione degli utenti al tuo sito web e i contenuti del sito.
I dati scambiati tramite HTTPS sono protetti tramite il protocollo *Transport Layer Security* (TLS), che fornisce tre livelli di protezione fondamentali:

- **Crittografia**. I dati scambiati vengono criptati per proteggerli dalle intercettazioni. Ciò significa che, mentre l'utente consulta un sito web, nessuno può "ascoltare" le sue conversazioni, tenere traccia delle attività svolte in più pagine o carpire le sue informazioni.
- **Integrità dei dati**. I dati non possono essere modificati o danneggiati durante il trasferimento, intenzionalmente o meno, senza essere rilevati.
- **Autenticazione**. Dimostra che gli utenti comunicano con il sito web previsto. Protegge da attacchi man-in-the-middle e infonde fiducia negli utenti, il che si traduce in altri vantaggi commerciali.

Best practice per l'implementazione del protocollo HTTPS

Utilizzare certificati di sicurezza efficaci
Devi ottenere un certificato di sicurezza nell'attivazione di HTTPS per il sito. Il certificato viene emesso da un'autorità di certificazione (CA), che adotta misure per verificare che il tuo indirizzo web appartenga effettivamente alla tua organizzazione, proteggendo così i tuoi clienti da attacchi man-in-the-middle. Quando configuri il tuo certificato, garantisci un'elevata sicurezza scegliendo una chiave a 2048 bit. Se hai già un certificato con una chiave meno efficace (a 1024 bit), esegui l'upgrade a 2048 bit. Quando scegli il certificato del tuo sito, tieni presente quanto segue:

- Richiedi il certificato a un'autorità di certificazione attendibile che offre assistenza tecnica.
- Stabilisci quale tipo di certificato ti serve:
  - Unico certificato per un'unica origine protetta (ad

esempio www.example.com).
- Certificato multidominio per diverse origini protette note (ad esempio, www.example.com, cdn.example.com, example.co.uk).
- Certificato con caratteri jolly (ad esempio a.example.com, b.example.com).

Utilizzare reindirizzamenti 301 lato server

Reindirizza gli utenti e i motori di ricerca alla pagina HTTPS o alla risorsa con reindirizzamenti HTTP 301 lato server.

Verificare che Google possa eseguire la scansione e l'indicizzazione delle pagine HTTPS

- Non bloccare le pagine HTTPS utilizzando file robots.txt.
- Non includere meta tag nomdex nelle pagine HTTPS.
- Utilizza lo strumento Visualizza come Google per verificare che Googlebot possa accedere alle tue pagine.

Supportare HSTS

È consigliabile il supporto del protocollo HSTS (HTTP Strict Transport Security) per i siti HTTPS. Il protocollo HSTS indica al browser di richiedere automaticamente le pagine HTTPS, anche se l'utente inserisce http nella barra a inoltre a Google di pubblicare URL. protet questo riduce al minimo il rischio di pubbli per i tuoi utenti.
Per su izza un server web che lo supporti e attiva
Anche u complessa la strategia di rollback. Ti consig S nel seguente modo:

- Implementa inizialmente le pagine HTTPS senza HSTS.
- Invia intestazioni HSTS di breve durata massima. Esegui il monitoraggio del traffico di utenti e di altri clienti, così come del rendimento degli elementi che da essi dipendono, quali gli annunci.
- Aumenta lentamente l'età massima HSTS.
- Se HSTS non incide negativamente su utenti e motori di ricerca puoi, se vuoi, richiedere che il tuo sito venga aggiunto all'elenco di precaricamento HSTS usato dalla maggior parte dei browser più noti.

Prendere in considerazione l'utilizzo del precaricamento HSTS

Se attivi HSTS puoi, se vuoi, supportare il precaricamento HSTS per offrire maggiore sicurezza e migliorare il rendimento. Per attivare il precaricamento devi visitare hstspreload.org e rispettare i requisiti per l'invio del tuo sito.

Come evitare errori comuni

Durante la procedura di protezione del tuo sito con TLS, stai attento a non commettere i seguenti errori.

Problema	Azione
Certificati scaduti	Assicurati che il tuo certificato sia sempre aggiornato.
Certificato registrato per il nome sbagliato del sito web	Verifica di avere ottenuto un certificato per tutti i nomi host su cui viene pubblicato il tuo sito. Ad esempio, se il certificato riguarda soltanto www.example.com, un visitatore che carica il tuo sito usando soltanto example.com (senza il prefisso "www.") verrà bloccato per un errore dovuto al nome del certificato che non corrisponde.
Supporto della funzione Indicazione nome server(SNI) mancante	Assicurati che il tuo server web supporti SNI e che il tuo pubblico utilizzi browser supportati. La funzione SNI è supportata da tutti i browser moderni, ma ti servirà un IP dedicato se devi supportare browser meno recenti.
Problemi di scansione	Non impedire la scansione del tuo sito HTTPS utilizzando il file robots.txt.
Problemi di indicizzazione	Se possibile, consenti l'indicizzazione delle [visibile nella versione PRO] parte dei motori di ricerca. Evita di i meta tag noindex.
Versioni protoco	i precedenti del protocollo sono , assicurati di avere le versioni più lle librerie TLS e di implementare le rsioni del protocollo.
Elemen	soltanto contenuti HTTPS nelle pagine HTTPS.
Contenuti diversi su HTTP e HTTPS	Assicurati che i contenuti sul tuo sito HTTP e sul sito HTTPS corrispondano.
Errori di codice di stato HTTPsu HTTPS	Verifica che il tuo sito web restituisca il codice di stato HTTP corretto. Ad esempio, 200 OK per le pagine accessibili, oppure 404 o 410 per le pagine che non esistono.

Ulteriori suggerimenti

Consulta la pagina relativa alle domande frequenti sulla migrazione ad HTTPS per ottenere ulteriori suggerimenti circa l'utilizzo delle pagine HTTPS sul tuo sito.

Migrazione da HTTP a HTTPS

Se esegui la migrazione del sito da HTTP a HTTPS, Google considera l'operazione uno spostamento del sito con modifiche agli URL. Ciò può influire temporaneamente sulle cifre relative al traffico. Per ulteriori informazioni, consulta la pagina recante una panoramica sullo spostamento di un sito.

Aggiungi la proprietà HTTPS a Search Console. Search Console gestisce HTTP e HTTPS separatamente, non condividendo i dati relativi a tali proprietà. Pertanto, se hai pagine che adottano entrambi i protocolli, devi indicare una proprietà Search Console distinta per ciascuno di essi.

Checklist:

- Eseguire il backup
- Reindirizzamento di tutti gli URL per mezzo del redirect 301
- Verificare che nessuna risorsa venga caricata per http
- Sostituire i link interni
- Sostituire i link esterni più importanti
- Aggiornare i reindirizzamenti già esistenti
- Modificare i canonical, gli hreflang e le altre header entries
- Modificare i dati strutturati
- Verificare/adeguare i robot.txt, se necessario
- Modificare/aggiornare la Sitemap
- Sostituire/impostare gli URL all'interno dei tool esterni
- Controllo conclusivo del SSL a verifica del collegamento corretto del certificato e dell'accessibilità delle pagine sia per utenti umani che per i bot
- Conseguente aggiornamento della comunicazione (link all'interno delle newsletter, conferma d'ordine, firma digitale, bigliettini da visita, ecc.)

Aggiornare il Server

una buona prassi è effettuare aggiornamenti periodici del vostro server, aggiornando il sistema operativo ed i vari componenti, come DBMS e linguaggi. Se il vostro sito è in hosting, non dovete fare nulla (al massimo potete chiedere informazioni al Vs. provider circa lo stato di aggiornamento del sistema).

Aggiornare i CMS

se utilizzate dei CMS (come WordPress o Joomla) è determinante effettuare aggior eventuali plugin installati.

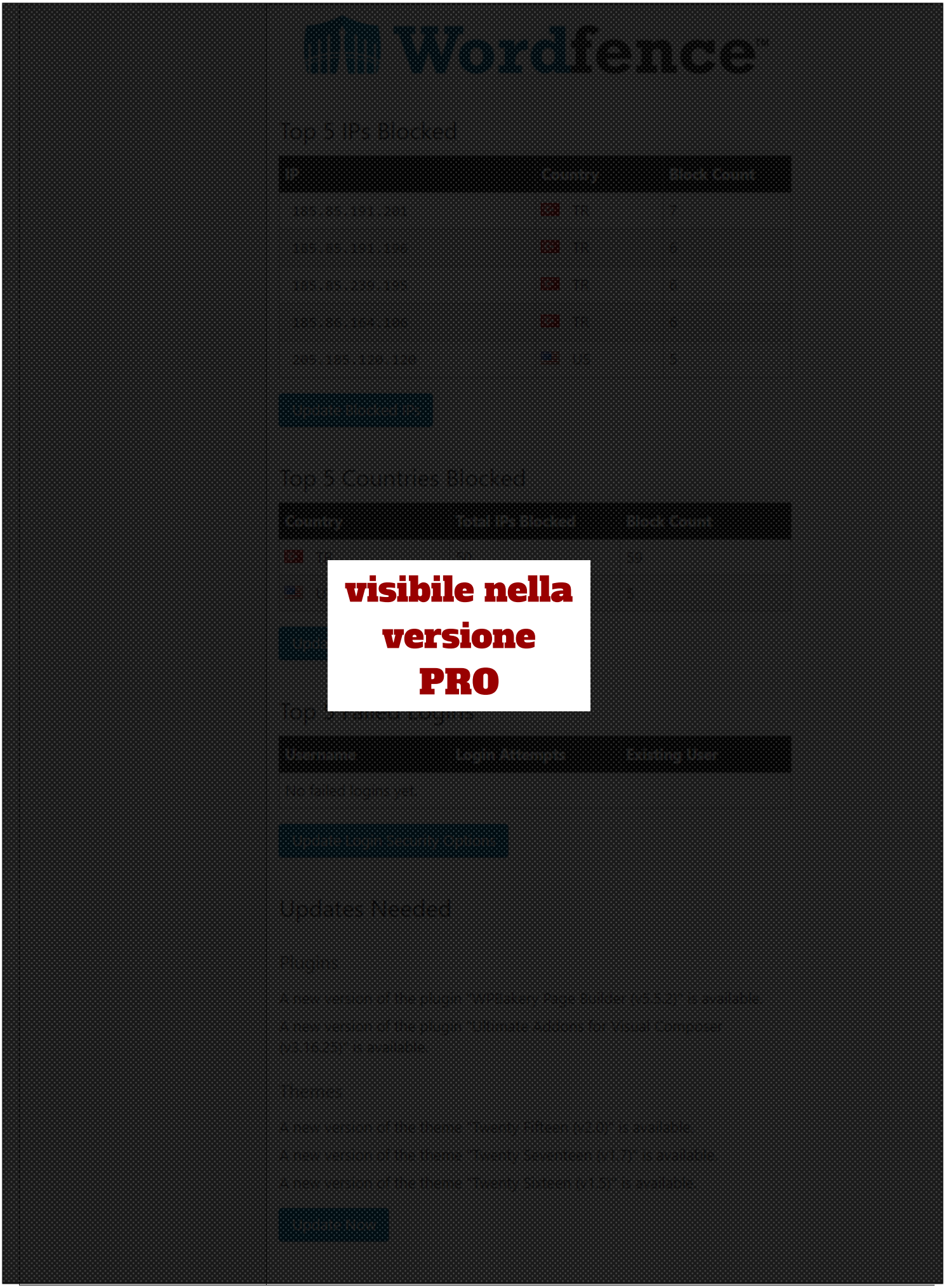
visibile nella versione PRO

zioni per la sicurezza

se util , potete installare qualche plugin come soluzi

- W
- S
- SecuPress

  - Generare e forzare password complesse durante la creazione di profili utente
  - Forzare le password a scadere e ad essere ripristinate regolarmente
  - Log delle azioni degli utenti
  - Aggiornamenti semplificati delle chiavi di sicurezza di WordPress
  - Scansione malware
  - Autenticazione a due fattori
  - reCAPTCHA
  - Firewall di sicurezza WordPress
  - Whitelist degli IP
  - Blacklist degli IP
  - Log delle modifiche dei file
  - Monitoraggio delle modifiche ai DNS
  - Blocco delle reti dannose
  - Visualizzazione delle informazioni WHOIS sui visitatori


Wordfence
Top 5 IPs Blocked
Top 5 Countries Blocked
visibile nella versione PRO
Updates Needed

Tenere traccia delle modifiche del CMS

consentire agli amministratori di vedere tutto ciò che viene modificato, cose come accessi, modifiche della password, modifiche ai temi, modifiche ai widget, nuove creazioni di post, aggiornamenti di WordPress, ecc. Praticamente tutto ciò che accade viene registrato.

- WP Security Audit Log

WP Security Audit Log tiene traccia di ogni singolo cambiamento apportato al vostro sito da voi stessi o da altri utenti. Effettuando il monitoraggio di ciò che stanno facendo i vari account utente, potrete rilevare qualsiasi comportamento sospetto e fermarlo prima che generi problemi.

BACKUP

Revisionare e/o predisporre backup regolari dei dati, dei siti e dei DB. Verificare periodicamente che il ripristino sia sempre possibile.

Se il vostro host non offre backup, ci sono alcuni famosi servizi e plugin per WordPress che potete utilizzare per automatizzare il processo.

- UpdraftPlus

HOSTING

Per gara[illegible]rano sul tuo sito web devi ospitarli su un se[illegible]

Scegli se[illegible]no, oltre allo spazio web anche:

- **[illegible]SL**, ovvero sistema che consenta di avere ur[illegible]o il suo sito web. In questo modo le informaz[illegible]moduli del tuo sito web passeranno dal browser al server web in forma criptata e nessuno sarà in grado di intercettare i tuoi dati.
- **un sistema sicuro di backup giornaliero.**

- Siteground

visibile nella versione PRO