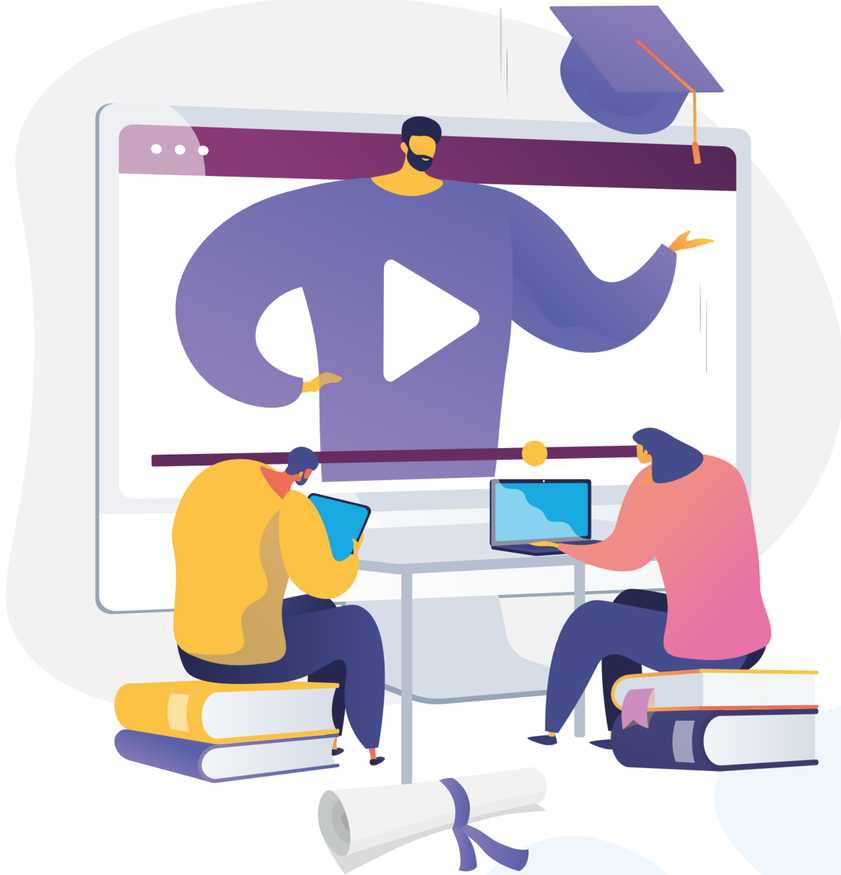
DIGITAL academy

by register.it



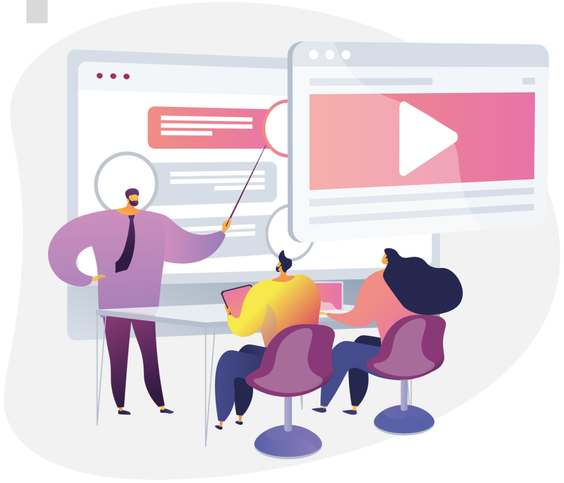
Sicurezza su WordPress

Scenari di rischio, sicurezza Hosting e configurazioni

Register.it e la Digital Academy

La mission di **Register.it** è quella di accompagnare persone e aziende nella **creazione della propria presenza online** con un **percorso di miglioramento continuo.**

1 Webinar



2 Certificazioni

3 Network

Web Agency Network

La “**Web Agency Network**" è una **rete di rivenditori accreditati** garantita da Register.it

Lo scopo è quello di **mettere in contatto i clienti finali di Register.it** che cercano rivenditori garantiti su tutto il territorio nazionale **con i Business Partner accreditati e certificati**.

Entrano a far parte della "**Web Agency Network**" i clienti Business Partner che **hanno ottenuto almeno una certificazione della Digital Academy** di Register.it.

Programma Business Partner

Il **programma Business Partner di Register.it** si rivolge ad agenzie e professionisti del web e del digitale in tutta Italia come consulenti IT, web agency, web developer e web designer.

I clienti che hanno aderito al programma hanno numerosi vantaggi come **sconti riservati** su tutta la vasta gamma di prodotti di Register.it, **consulenza personalizzata** e dedicata, **servizio di assistenza tecnica prioritaria** e molto altro.

.I nostri speakers

Alessio Rossi - Security & Compliance manager
Sviluppo, implementazione e mantenimento di politiche e programmi di gestione della compliance e della sicurezza aziendale in Register.it.

Daniele Melosi - Service Management Manager
Amministrazione, gestione e supporto all'infrastruttura IT e ai servizi di rete di Register.it. Verifica del corretto funzionamento dei sistemi hardware e software aziendali.

WordPress. La libertà che ha conquistato il web e il prezzo di tutte le libertà

WordPress è il CMS più scelto e usato a livello mondiale:

- Alimenta più del **43%** di tutti i siti web in Internet.
- Alimenta più del **23%** dei 10 milioni di siti internet più visitati al mondo.
- Detiene una quota superiore al **65%** nel mercato dei siti web realizzati mediante CMS.
- Ha superato gli altri CMS anche in segmenti specifici come l'e-commerce, grazie ai suoi plugin.

La “Carta dei diritti” di WordPress

1. La libertà di eseguirlo per qualsiasi finalità.
2. La libertà di studiare come funziona e di modificarlo a piacere.
3. La libertà di ridistribuirlo.
4. La libertà di distribuire ad altri le proprie versioni modificate.

La sicurezza come valore dei servizi offerti

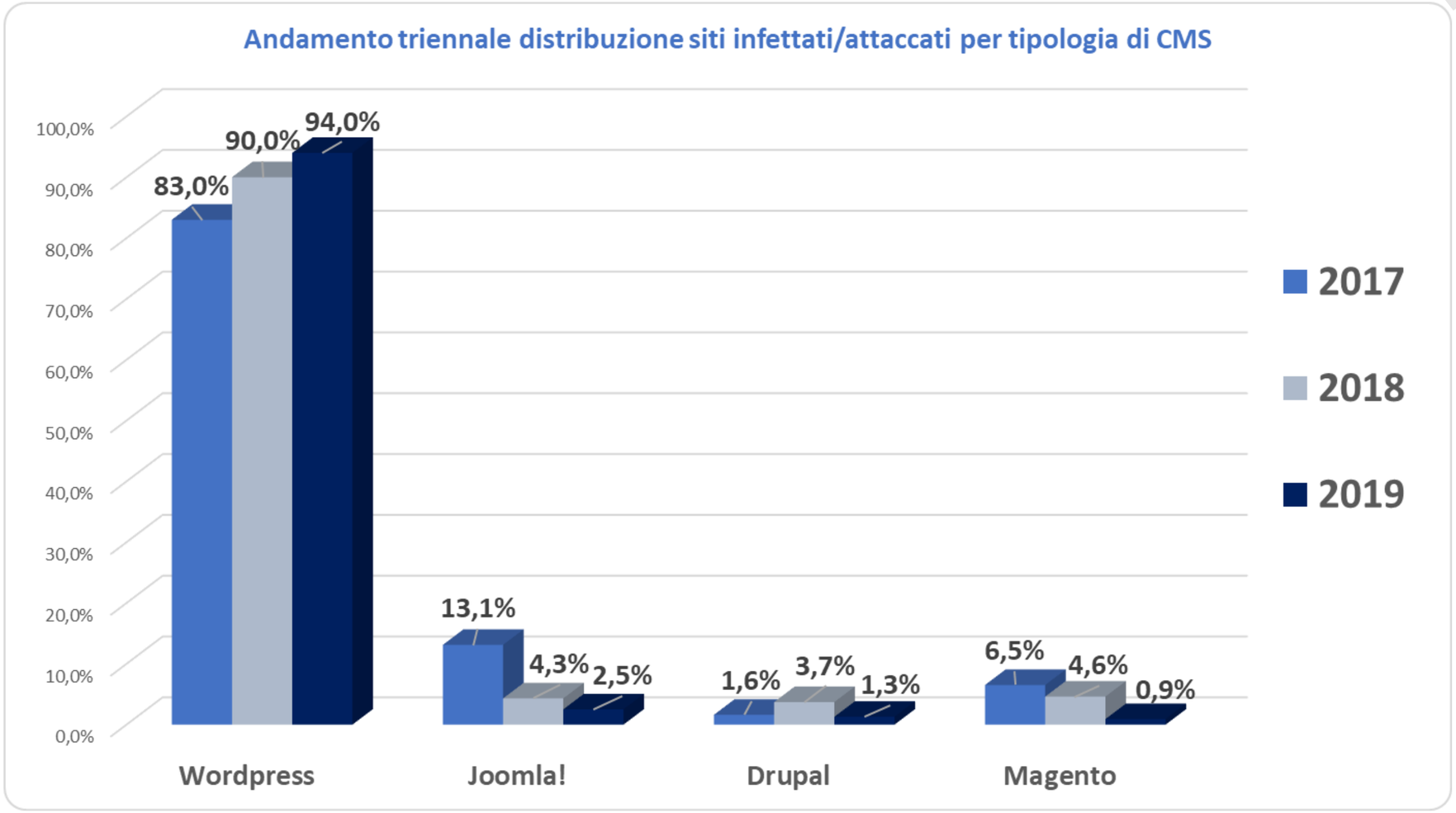
Maggiore libertà significa anche maggiori rischi e responsabilità

La gestione attenta delle tematiche di sicurezza in WordPress rappresenta lo strumento indispensabile tramite cui **tutelare il proprio sito**, il **valore** dei servizi che fornisce, le informazioni e in esso contenute e non **l'affidabilità percepita** dagli utenti finali dalle molteplici **minacce**, molto spesso **ignote** da chi ha la comprensibile priorità di gestire il proprio business prima delle tematiche di sicurezza e **invisibili** finché non manifestano i loro effetti deleteri.

Argomenti di questo webinar

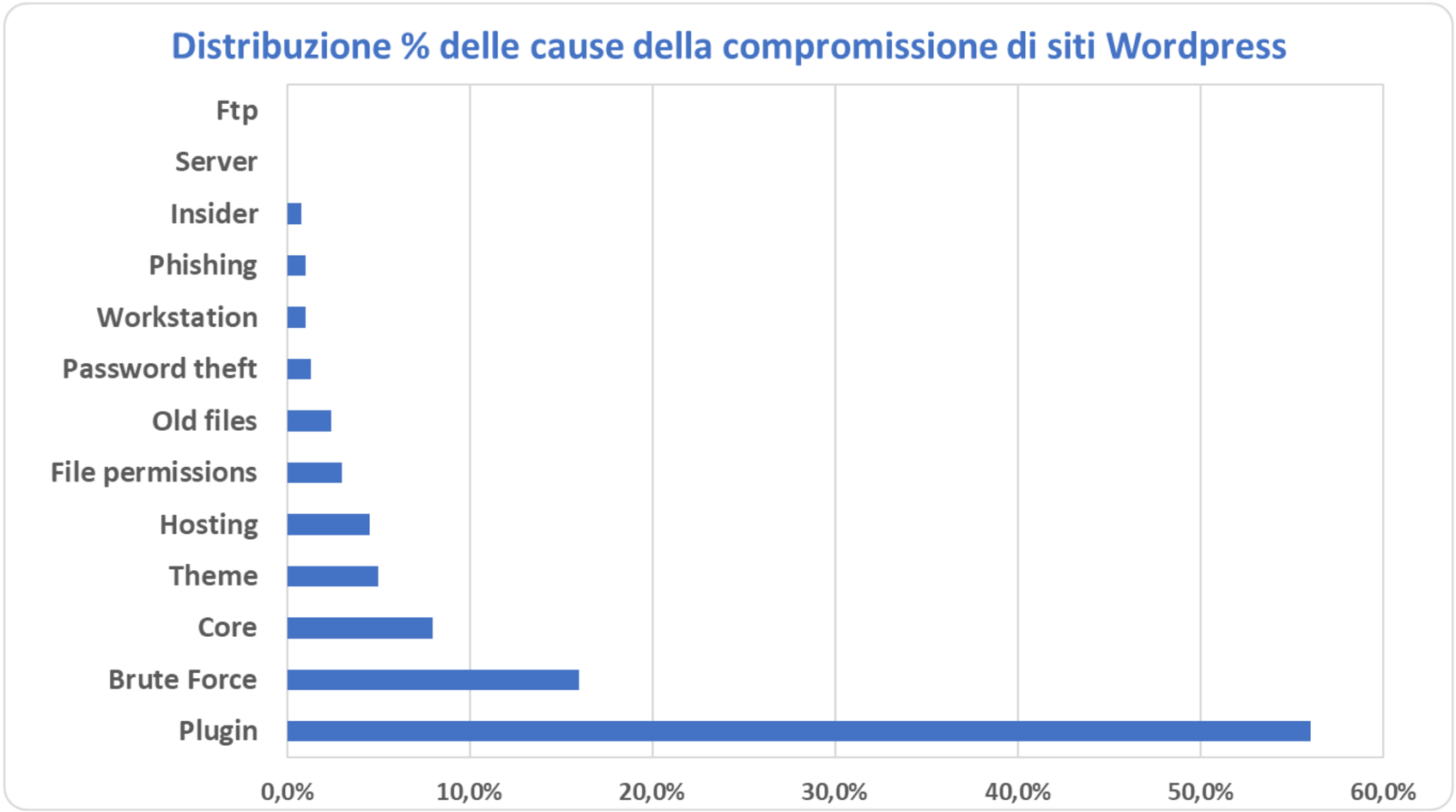
- Quali sono i **rischi** e gli scenari di possibili **attività malevole** cui WordPress è esposto e a quali conseguenze possono portare?
- Quali sono gli **aspetti** da considerare e gli **ambiti** in cui intervenire per **aumentare la sicurezza in WordPress** in modo da prevenire le minacce di attacchi o mitigarne gli effetti?
- Sicurezza delle piattaforme di Hosting.
- **Aggiornamento** sistematico **di WordPress** e delle componenti installate.
- Sicurezza della **configurazione** e dei **dati** esposti.
- Affidabilità e sicurezza delle **componenti esterne** installate.

Quali sono i rischi e gli scenari di possibili attività malevole cui WordPress è esposto e a quali conseguenze possono portare ?



Quali sono i rischi e gli scenari di possibili attività malevole cui WordPress è esposto e a quali conseguenze possono portare?

2

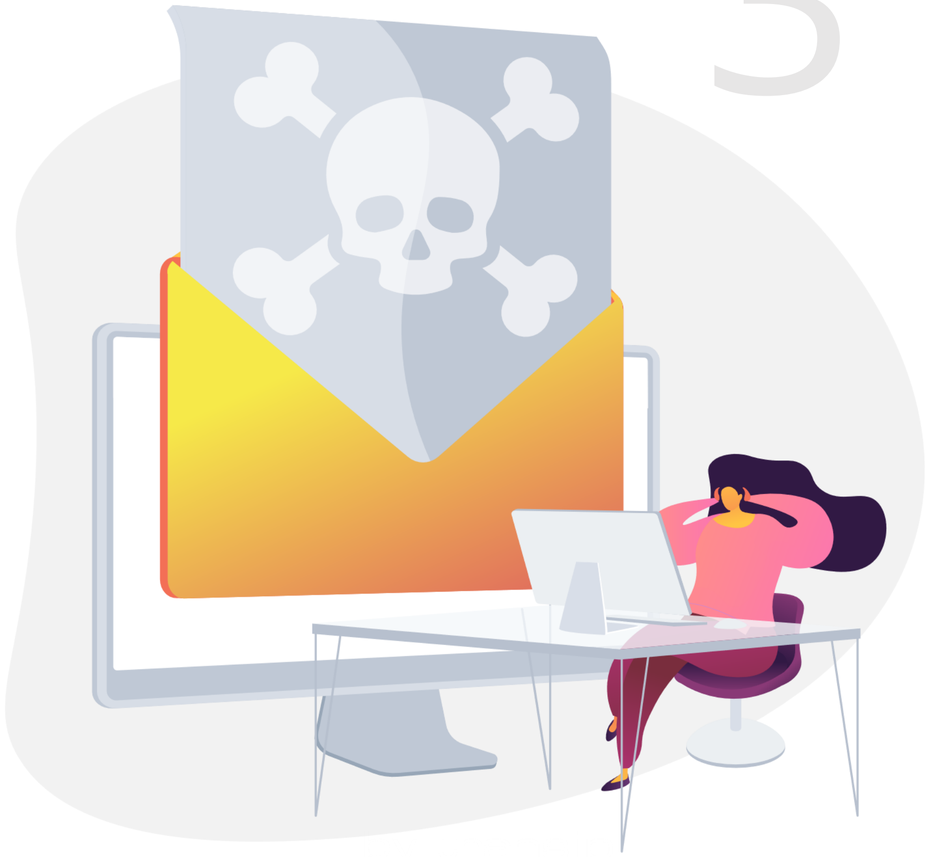


Quali sono i rischi e gli scenari di possibili attività malevole cui WordPress è esposto e a quali conseguenze possono portare?

3

Tipologie di attacco più frequenti con le conseguenze più dannose:

- **DDoS**
- **Malware / Backdoor**
- **Brute Force attack**
- **SQL Injection**
- **Cross Site Scripting**
- **Pharma Hack**
- **Clickjacking**



Quali sono gli aspetti da considerare e gli ambiti in cui intervenire per aumentare la sicurezza in WordPress in modo da prevenire le minacce di attacchi o mitigarne gli effetti?

1° webinar

- Sicurezza delle piattaforme di Hosting
- Aggiornamento sistematico di WordPress e delle componenti installate
- Sicurezza della configurazione e dei dati esposti
- Affidabilità e sicurezza delle componenti esterne installate

2° webinar

- Gestione degli account amministrativi
- Sicurezza degli accessi
- Sicurezza dei dispositivi client
- Utilizzo di certificati SSL
- Backup

Sicurezza delle piattaforme di Hosting

Caratteristiche da valutare in un servizio di hosting:

1. Controlli logici e fisici su tutti i livelli e componenti dell'architettura della piattaforma che ospita il sito WordPress ma anche sull'organizzazione e sulla sicurezza e qualità dei processi adottati del personale che la gestisce.

2. Disponibilità da parte del provider di servizi o pacchetti che permettano di aggiungere features di sicurezza.

3. Pacchetti di hosting chiari e dimensionabili rispetto a diverse esigenze di capacità.

Come valutare la presenza delle features necessarie a garanzia della sicurezza:

1. **CERTIFICATI**
    1. ISO/IEC 27001 - Sistema di gestione della sicurezza delle informazioni
    2. ISO/IEC 27017 (estensione ISO 27001) - Codice di condotta per controlli avanzati di sicurezza informativa specifici per servizi cloud
    3. ISO/IEC 27018 (estensione ISO 27017) - Codice di condotta per la protezione dei dati personali information nei servizi di public cloud per i cloud provider
    4. ISO/IEC 9001 - Sistema di gestione per la qualità per il servizio di hosting
2. **Disponibilità di :**
    - Soluzioni di backup personalizzabili rispetto alle esigenze del sito e dei suoi contenuti.
    - Servizi o soluzioni anti DDoS.
    - Servizi o soluzioni antimalware.
    - Assistenza tecnica specialistica.
3. **Descrizione chiara di:**
    - Caratteristiche tecniche e capacità elaborativa.
    - Capacità di storage della piattaforma di hosting per i vari pacchetti/livelli.


ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO
DOCUMENTI
BANCHE DATI
HOME
CHI SIAMO
ACCREDITAMENTO
SERVIZI ACCREDITATI
ALTRE ATTIVITÀ
COMUNICAZIONE
CONTATTI
ACCREDITAMENTI
CERTIFICAZIONI
Organizzazioni/aziende con sistema di gestione certificato
Legenda dei settori di certificazione IAF
Prodotti e servizi certificati
Figure professionali certificate
STATISTICHE
Organizzazioni/aziende con sistema di gestione certificato
Selezionare i criteri desiderati e cliccare sul pulsante Cerca. Verranno visualizzati i certificati trovati, con l'elenco dei siti (sedi, filiali, stabilimenti, ecc.) coperti da certificazione.
NOTA: Se la parola da ricercare contiene dei punti di separazione, es. A.B.C., questi non devono essere omessi o sostituiti con uno spazio
Legenda:
Per il campo organismo accreditato/riconosciuto:
A - Organismo accreditato
R - Organismo riconosciuto per il settore IAF 28 schema SGQ
Ricerca organizzazioni/aziende
N. di certificato
Data di rilascio
dal
(gg/mm/aaaa)
al
(gg/mm/aaaa)
Azienda
Partita IVA / Codice Fiscale
Scopo

N.Certificato: 207253-2016-AIS-ITA-ACCREDIA

Emesso il 28-10-2016
in corso di validita'

dall'organismo Accreditato:

DNV Business Assurance Italy S.r.l.
www.dnv.com

REGISTER S.p.A. - Sede Legale e Operativa
SEDE LEGALE o principale - SEDE - Viale Della Giovine Italia, 17 - 50122 - Firenze (FI) - Toscana

Scopo: Progettazione, sviluppo e conduzione di servizi di Posta elettronica certificata (PEC), identificazione e autenticazione digitale(SPID), di Conservazione a Norma e validazione temporale (TSA) in qualità di fornitore di servizi digitali fiduciari (TSP) e di servizi cloud di tipo IaaS, PaaS, SaaS, di gestione dell'infrastruttura informatica su server dedicati e di email. In accordo con la Dichiarazione di Applicabilità, estesa ai controlli della ISO/IEC 27017:2015 e ISO/IEC 27018:2019, versione del 9 settembre 2019

Norma: UNI CEI ISO/IEC 27001:2014
Schema di Accreditamento: SSI

Dati aggiornati dall'Organismo il 18/01/2022

Partita IVA: 04628270482

N.Certificato: 139296-2013-AQ-ITA-ACCREDIA

Emesso il 26-07-2013
in corso di validita'

dall'organismo Accreditato:

DNV Business Assurance Italy S.r.l.
www.dnv.com

REGISTER S.p.A. - Sede Legale e Operativa
SEDE LEGALE o principale - SEDE - Viale Della Giovine Italia, 17 - 50122 - Firenze (FI) - Toscana

Scopo: Progettazione, sviluppo e conduzione di servizi di Posta elettronica certificata (PEC), identificazione e autenticazione digitale(SPID), di Conservazione a Norma e validazione temporale (TSA) in qualità di fornitore di servizi digitali fiduciari (TSP) e di servizi cloud di tipo IaaS, PaaS, SaaS, di gestione dell'infrastruttura informatica su server dedicati e di email (IAF 33)

Norma: UNI EN ISO 9001:2015
Schema di Accreditamento: SGQ
Settori: **33**

Dati aggiornati dall'Organismo il 18/01/2022

Partita IVA: 04628270482

N.Certificato: 207253-2016-AIS-ITA-ACCREDIA

Emesso il 28-10-2016
in corso di validita'

dall'organismo Accreditato:

DNV Business Assurance Italy S.r.l.
www.dnv.com

REGISTER S.p.A. - Sede Operativa Call Center
UNITA' SECONDARIA - SITO - Via Zanchi, 22 - 24126 - Bergamo (BG) - Lombardia

Scopo: Progettazione, sviluppo e conduzione di servizi di Posta elettronica certificata (PEC), identificazione e autenticazione digitale(SPID), di Conservazione a Norma e validazione temporale (TSA) in qualità di fornitore di servizi digitali fiduciari (TSP) e di servizi cloud di tipo IaaS, PaaS, SaaS, di gestione dell'infrastruttura informatica su server dedicati e di email. In accordo con la Dichiarazione di Applicabilità, estesa ai controlli della ISO/IEC 27017:2015 e ISO/IEC 27018:2019, versione del 9 settembre 2019

Norma: UNI CEI ISO/IEC 27001:2014
Schema di Accreditamento: SSI

Dati aggiornati dall'Organismo il 18/01/2022

Partita IVA: 04628270482

N.Certificato: 139296-2013-AQ-ITA-ACCREDIA

Emesso il 26-07-2013
in corso di validita'

dall'organismo Accreditato:

DNV Business Assurance Italy S.r.l.
www.dnv.com

REGISTER S.p.A. - Sede Operativa Call Center
UNITA' SECONDARIA - SITO - Via Zanchi, 22 - 24126 - Bergamo (BG) - Lombardia

Scopo: Progettazione, sviluppo e conduzione di servizi di Posta elettronica certificata (PEC), identificazione e autenticazione digitale(SPID), di Conservazione a Norma e validazione temporale (TSA) in qualità di fornitore di servizi digitali fiduciari (TSP) e di servizi cloud di tipo IaaS, PaaS, SaaS, di gestione dell'infrastruttura informatica su server dedicati e di email (IAF 33)

Norma: UNI EN ISO 9001:2015
Schema di Accreditamento: SGQ
Settori: **33**

Dati aggiornati dall'Organismo il 18/01/2022

Partita IVA: 04628270482

Aggiornamento sistematico di WordPress e delle componenti installate

Il codice Il codice sorgente dei **file core** di WordPress, dei **temi** e dei **plugin** è pubblico e liberamente consultabile.
Il **mancato aggiornamento** di queste 3 componenti espone ad un **rischio enorme** perché chiunque può avere accesso a informazioni sui bugs appena vengono risolti.

Tali **bugs** possono essere **sfruttati,** su installazioni non prontamente aggiornate, **da potenziali attaccanti** che riescono ad avere accesso alle versioni di WordPress o dei plugin utilizzati molto spesso rivelate nei vari **readme.html.**

È quindi importante:

- **Aggiornare la versione di WordPress** appena sono disponibili nuove release o abilitando l'aggiornamento automatico.
- Controllare sempre la disponibilità di nuovi aggiornamenti, specie se motivati da patch di sicurezza.
- Provvedere all'**aggiornamento** anche di tutti i **plugin e temi** installati.

Sicurezza della configurazione e dei dati esposti

- **Evitare di cambiare le estensioni** dei files in modo che non vengano più interpretati dal server web come php.
- **Impostare headers di sicurezza**
  - CONTENT-SECURITY-POLICY (CSP)
  - X-XSS-Protection
  - STRICT TRANSPORT SECURITY
  - X-FRAME-OPTIONS
  - EXPECT-CT
  - X-CONTENT-TYPE
- **Disabilitare la modifica dei file** dal pannello di amministrazione
- Prevenire l'esecuzione di file PHP
- **Disabilitare la navigazione** nelle directory
- Disabilitare XMLPRC e Pingback

Affidabilità e sicurezza delle componenti esterne installate

Quando si è alla ricerca di un plugin/tema è fondamentale:

- **Valutare l'affidabilità del repository** da cui li si scarica considerando:
  - La notorietà del sito e la sua popolarità su canali tematici.
  - Il numero degli utenti che lo hanno scaricato e i loro commenti.
  - Eventuali segnalazioni di vulnerabilità note per il plugin/tema di interesse.

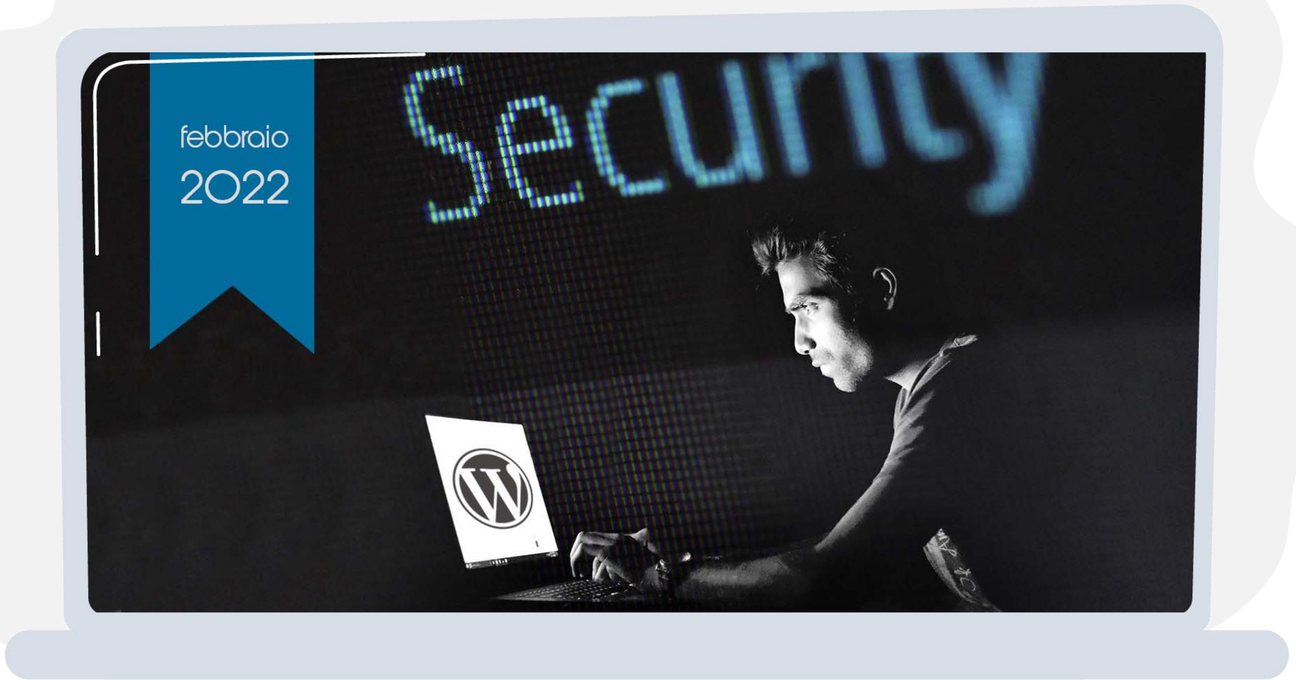
- **Optare per versioni premium** verificando innanzitutto la sicurezza della pagina di pagamento, la presenza delle funzionalità di aggiornamento sistematico del plugin/tema e i servizi di assistenza collegati.

- **Testare il plug-in/tema in un ambiente di sviluppo separato** che non contenga i dati presenti nel server produzione verificando non soltanto che il plugin realizzai le funzioni pubblicizzate ma anche che il sito e tutta l'infrastruttura non presenti comportamenti anomali o inattesi.

Questions and Answers

.Thanks

Il prossimo webinar



register.it

part of team.blue