Sistemi e moduli sicurezza server Webita

I server di keliweb gestiti da Webita sfruttano la potenza del software Direct Admin su una soluzione di hosting condiviso per gestire, organizzare e mettere in sicurezza i dati dei propri clienti. Tali informazioni sulle tecnologie adottate e moduli di sicurezza attivi si intendono informazioni ad uso interno. Webita mette a conoscenza i suoi clienti dell'utilizzo di determinate tecnologie a scopo informativo, ma non si ritiene responsabile dell'uso eventuale di queste informazioni da parte di malintenzionati esterni per poter carpire indicazioni utili ad eventuali atti di hacking sul server stesso.

Per questo motivo le seguenti informazioni cercheranno di essere complete, soddisfacenti, ma per quanto possibile prive di dettagli che potrebbero aiutare qualsiasi hacker a reperire info utili per eventuali manomissioni di sorta.

I server sono monitorati e protetti costantemente con sistemi all'avanguardia che offrono protezione contro accessi non autorizzati.

Offriamo a tutti i clienti il massimo livello di sicurezza grazie alla tecnologia Condor Guard Smart Firewall Protection (sistema di monitoraggio continuo del traffico web per individuare e bloccare qualunque tipo di attacco informatico dislocato con sonde di intercettazione in tutto il mondo) e tramite due diverse protezioni anti-DDoS che operano con due tecnologie di scrubbing center diverse, proteggiamo i server da attacchi distribuiti fino a 1.5TB di intensità. Questo tipo di protezione rappresenta uno dei punti di forza che permette la classificazione Tier-4.

Inoltre, utilizziamo per tutte le soluzioni hosting vari livelli di protezione e analisi costante dei dati, in particolare contro gli attacchi brute force dei CMS più utilizzati, impedendo qualunque intrusione non autorizzata.

Di seguito vedremo quali azioni Webita adotta più nel dettaglio per la messa in sicurezza dei propri server:

1- Utilizzo di password sicure per l'accesso amministrativo (maggiore di 8 caratteri, alfanumerica, maiuscole e minuscole, caratteri speciali) ed autenticazione a due fattori per l'accesso a Direct Admin.
2- Criptazione via connessione SSL (Secure socket layer) dei dati trasmessi tra browser (visita e immissione dei dati) e server.
3- Un sistema di firewall per controllare le connessioni e che riguarda la sicurezza lato network
4- SiteLock uno strumento di sicurezza Cloud-based che esegue l'analisi di malware e vulnerabilità sul server e siti web.
5- Clam AntiVirus un software libero di tipo antivirus multipiattaformaparticolarmente diffuso come antivirus su server di posta elettronica per il controllo dei messaggi in transito.

Webita di Giorgio Sanna
P.IVA: 08180880729

5° Trav. Tratturo Spagnuolo, 14 - 70013 Castellana Grotte (BA)
Tel: +393398937151 Mail: info@webita.eu PEC: webita@pec.net webita.eu