Basque CyberSecurity Centre

CMSen babesa Checklist

☐ Automatizatu software-eguneratzeak.

Osagaien eguneratze automatikoa burutzeko aukerak dituzte CMS erabilienek, eta kalteberatasunen zuzenketa azkarra lortzen dute horrela.

☐ Erabili autentifikazioko faktore bikoitz bat.

Sistema babesten laguntzen du, nahi ez diren kredentzial eta sarbideen konpromisoaren aurrean.

☐ Murriztu administratzaileen sarbidea IP helbide jakin batzuetatik.

CMS erabilienek IP, IPen barruti edo eskualde geografiko jakin batzuetatik administratzaileen sarbidea murriztea ahalbidetzen duten sistemak izaten dituzte.

☐ Murriztu administratzaileen sarbidea konfigurazio-aukeren bidez.

Normalean htaccess fitxategiaren bidez, zeinak parametro jakin batzuk autentifikaziorako eta sarbiderako konfiguratzea ahalbidetzen duen.

☐ Babestu webgunea administratzeko baliatzen diren ekipamenduak.

Ekipamendu horien konpromisoak sarbide-kredentzialak konprometitu ditzake, eta, hori horrela, eguneratuta daudela eta babes-neurriak dauzkatela egiaztatzea komeni da.

☐ WAF – Web Application Firewall.

Webgune-aplikazioen firewall bat erabiltzea lagungarria da erasoak blokeatzeko eta sistemak babesteko.

☐ Kalteberatasunen detekzio proaktiboa.

Erasotzaile batek kalteberatasunak aurkitu eta ustiatu baino lehen kalteberatasunak identifikatzea da helburua.

Babesteko moduari buruzko informazio gehiago jakin nahi baduzu, sartu zaitez webgune honetan: **https://www.basquecybersecurity.eus/eu/**

Aholkularitza profesionala behar baduzu, webgunean eskuragarri duzun Euskadiko ziberseguratsun-hornitzaileen katalogoa kontsultatu dezakezu.