Basque CyberSecurity Centre

Protección de CMS Checklist

☐ Automatizar las actualizaciones de software.

Los CMS más utilizados disponen de opciones para la actualización automática de componentes, consiguiendo de esta forma una rápida corrección de vulnerabilidades.

☐ Utilizar un doble factor de autenticación.

Ayuda a proteger los sistemas frente al compromiso de credenciales y accesos no deseados.

☐ Restringir el acceso de los administradores desde determinadas direcciones IP.

Los CMS más utilizados suelen disponer de sistemas que permiten restringir el acceso de los administradores desde determinadas IP, rangos de IP o regiones geográficas.

☐ Restringir el acceso de los administradores mediante las opciones de configuración.

Habitualmente a través del fichero .htaccess, que permite configurar determinados parámetros para la autenticación y el acceso.

☐ Securizar los equipos desde los que se administra la web.

El compromiso de estos equipos puede comprometer las credenciales de acceso, por lo que conviene comprobar que se encuentran actualizados y que disponen de medidas de protección.

☐ WAF – Web Application Firewall.

La utilización de un firewall de aplicaciones web ayuda a bloquear los ataques y proteger los sistemas.

☐ Detección proactiva de vulnerabilidades.

El objetivo es tratar de identificar las vulnerabilidades antes de que las encuentre y explote un atacante.

Para conocer más información sobre cómo protegerte puedes visitar **https://www.basquecybersecurity.eus/es/**

Si necesitas asesoramiento profesional, puedes consultar el catálogo de proveedores de ciberseguridad de Euskadi disponible en la web.