Zerbitzariak bastioitzea

Aurrekontua: 7.300 €

Deskribapena:

Bastioia sistema baten kalteberatasunak murrizteko beharrezko neurri teknikoak eta antolakuntzakoak ezartzeko prozesua da, helburu hauekin:

• Makinaren balizko eraso fisikoetatik edo hardware-erasoetatik babesteko beharrezko konfigurazioak aplikatzea (periferikoak, USB gailuak desgaituz, BIOSetan abiaraztea mugatuz, pasahitzarekin babestuz, etab.).
• Sistema eragilea modu seguruan instalatzea.
• Eguneratze automatikoen zerbitzuak aktibatu eta/edo behar bezala konfiguratu.
• Segurtasun-programak instalatzea, konfiguratzea eta mantentzea, eta segurtasun-adabakiak behar bezala aplikatzea.
• Sistemaren tokiko politika konfiguratzea, pasahitzen politika sendoa, pribilegioen kudeaketa, software-murrizketak, sistema-auditoretzaren aktibazioa, sare-protokoloen murrizketa eta konfigurazio egokia, urruneko sarbideen konfigurazio segurua, erabiltzaile-kontuak, zifratzea, etab.

Horretarako, fabrikatzaileen gidak erabiliko dira, eta patroi orokor gisa, CCN-CERTek hainbat ingurune babesteko argitaratutako STIC gidak.

Bastionado de servidores

Presupuesto: 7.300 €

Descripción:

El bastionado es el proceso mediante el cual se implantan las medidas técnicas y organizativas necesarias para reducir las vulnerabilidades de un sistema con el objetivo de:

• Aplicar las configuraciones necesarias para protegerse de posibles ataques físicos o de hardware de la máquina (deshabilitando periféricos, dispositivos USB, restringiendo arranque en BIOS, protección con contraseña, etc.).
• Instalar de manera segura el sistema operativo.
• Activar y/o configurar adecuadamente los servicios de actualizaciones automáticas.
• Instalar, configurar y mantener los programas de seguridad y correcta aplicación de parches de seguridad.
• Configurar la política local del sistema, política robusta de contraseñas, gestión de privilegios, restricciones de software, activación de auditoría de sistema, restricción y configuración adecuada de protocolos de red, configuración segura de los accesos remotos, cuentas de usuario, cifrado, etc.

Para ello, se emplearán las guías de los distintos fabricantes, y como patrón general las guías STIC publicadas por CCN-CERT para la protección de distintos entornos.