GUÍA DE SEGURIDAD

Boletín Nro.: 2015-07
Fecha de publicación: 27/07/2015
Tema: Recomendaciones generales de Seguridad

1. Actualizar software (Apache, PHP, MySQL, Wordpress, Joomla, DNS, Zimbra, etc.) a las últimas versiones
2. Actualizar los sistemas operativos y los paquetes de software de los servidores (servidores de correo, web, DNS, de archivos compartidos, etc.)
3. Inspeccionar servidores en busca de archivos extraños.
4. Utilizar alguna herramienta para detectar web shells o backdoors. Algunas herramientas útiles para encontrar backdoors en servidores web son:
    a. http://cbl.abuseat.org/findbot.pl
    b. http://shelldetector.com/

    En ciertas ocasiones, las herramientas pueden no detectar los backdoors, por lo que podría requerir un análisis manual más profundo.

5. Utilizar soluciones antivirus, antispyware y anti rootkit tanto en equipos de usuarios como en servidores. En el caso de servidores, algunas soluciones para detectar rootkit pueden ser:
    a. unhide.rb/unhide
    b. rkhunter
    c. chkrootkit
    d. Malwarebytes
    e. varias: http://www.bleepingcomputer.com/download/windows/anti-rootkit/

    Por lo general, en caso de detectar un rootkit, la mejor solución es la reinstalación del sistema operativo y la restauración de los servicios desde una copia limpia.

6. Revisar políticas de prevención de DoS
7. Comprobar configuraciones de firewall y servidores en general.
8. Implementación de sistemas de detección y prevención de intrusión (IDS/IPS). Existen soluciones open source y gratuitas como Snort, Suricata, Pfsense, etc.
9. Verificar logs en busca de indicios de que el servidor ha sido comprometido por algún acceso indebido

10. Cerrar los puerto de administración de Zimbra (7071) hacia el exterior, así como otros puertos que no deban ser visibles desde el exterior de la red
11. Activación de autenticación de doble factor en las cuentas de redes sociales de la institución
12. Verificación de la robustez de todas las contraseñas (de los servidores, de las aplicaciones web, de cuentas de correo, etc.) y revisión de las políticas de administración de contraseñas y usuarios
13. Implementación de Firewall de aplicación como mod_security, mod_evasive y mod_qos

En caso de detectar un posible incidente o intrusión o en caso de requerir alguna ayuda para el análisis de los mismos, pueden contactar con el CERT-PY a través de nuestros canales de comunicación**:**

Reportar Incidentes: abuse@cert.gov.py

Información General: cert@cert.gov.py

Teléfonos de Contacto:

+595 21 201 014 (lun. a vie. 7:30 - 15:30)

+595 21 3276902 (24 Horas)