[TLP BLANCO]: La información podrá ser compartida libremente de acuerdo con las reglas y procedimientos aplicables para la divulgación pública. Debe regirse a las normas estándar de derechos de autor.

DEFACEMENT / COMPROMISED WEBSITE

1. INTRODUCCIÓN

Una de las actividades cotidianas por parte de los ciber atacantes es la modificación o desfiguración (defacement) no autorizada del contenido de una página web. Las motivaciones para realizar estas acciones son de tipo política, anarquista o simplemente evidenciar las capacidades técnicas de un atacante, con una consecuente pérdida de reputación de la víctima.

2. RIESGO

Un incidente de seguridad de tipo defacement o compromised website que se mantenga activo sin ser gestionado, podría generar los siguientes escenarios de riesgo:

- Impacto negativo a la imagen de la organización, en el sentido de su incapacidad de gestionar infraestructura TICs, debilidad que se podría extender a las capacidades medulares del giro del negocio de la víctima.
- Impacto a la integridad y disponibilidad de la información contenida en una página web ya que el servidor estaría bajo el control del ciber atacante, con el agravante en caso de ser un portal de servicio, o en el caso de que la página también sea utilizada como portal de phishing o como pundo de distribución de malware.

3. DETECCIÓN

Para la víctima, tomar conocimiento de un incidente de seguridad de tipo defacement o compromised website, suele presentarse por la notificación de un tercero como es el caso de las notificaciones de incidentes y vulnerabilidades diarias que emite EcuCERT diariamente. También es posible tomar conocimiento de este tipo de incidente en los casos que las organizaciones cuentan con procesos de monitoreo al servidor web, de tal manera que si existe la violación a una regla predefinida, esto podría ser un indicio de la ocurrencia de un incidente.

4. ACCIONES RECOMENDADAS

<u>Reactivas</u>

- Poner el servidor web en modo mantenimiento a fin de que los elementos modificados (defacement) o creados (compromised website) no estén visibles hacia la Red de Internet.
- Actualizar todas las credenciales de acceso y gestión del servidor web.
- Eliminar el contenido no autorizado.

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana.
Código postal: 170518 / Quito - Ecuador
Teléfono: 593-2 2947-800 - www.arcotel.gob.ec

- En caso de no poder acceder al servidor, implementar un nuevo servidor utilizando los datos generados en los respaldos.

Preventivas

- Eliminar todas las cuentas de usuario y credenciales generadas por defecto en el servidor y las aplicaciones de gestión.
- En relación a los procesos de edición de contenido, mantenimiento, configuración y actualización del servidor, implementar controles de autenticación multifactor.
- Ejecución de auditorías de seguridad y pruebas de penetración de tal manera a fin de encontrar vulnerabilidades o configuración débiles que requieran gestión a fin de evitar su explotación.
- Implementación de controles contra inyecciones de código malicioso tipo SQL.
- Implementación de controles contra ataques de tipo Cross Site Scripting XSS.
- Implementación de procesos de monitoreo de violación de políticas o cambios no autorizados y planificados respecto del contenido del servidor web.
- Generación periódica de respaldos
- Realizar el endurecimiento o hardening del servidor web.

5. Referencias

Cybersecurity and Infrastructure Security Agency. (2018, Noviembre 01). Website Secuirty. Disponible en https://www.us-cert.gov/ncas/tips/ST18-006

Acunetix. (2020, Marzo 13). How to Recover from a Hacked Website Event. Disponible en https://www.us-cert.gov/ncas/tips/ST18-006

Dirección: Av. Diego de Almagro N31-95 entre Whymper y Alpallana.
Código postal: 170518 / Quito - Ecuador
Teléfono: 593-2 2947-800 - www.arcotel.gob.ec