Sres. PyJ System

Despacho del Gerente de IT.

S/N – 09-01-2024 18:00hs GMT -3

ANALISIS DE EVENTO DE SEGURIDAD.

En la revisión de accesos rutinaria de los sistemas de vuestra empresa, bajo nuestro encargo, hemos detectado una intrusión de seguridad a la carpeta securizada “PyJ Systems”

De la verificación de accesos pudimos detectar que fue **modificado el archivo LOG.TXT** por las pruebas que suministraremos luego, dicho archivo en particular sumado al **acceso no autorizado detectado** nos hace tener certeza que las salvaguardas fueron vulneradas y los contenidos de la carpeta fueron Leídos/copiados por agentes no autorizados.

Acciones Tomadas:

Se han tomado las siguientes medidas:

- bloqueo del acceso a dicha información y otras carpetas de la red, activando el rol de emergencia según el procedimiento de vuestra empresa y blanqueando la contraseña de todo el personal.
- todos los equipos han sido bloqueados de inmediato y sus usuarios referidos al protocolo de ABM de Contraseñas de la compañía
- dichas contraseñas fueron securizadas y normalizadas a 12 caracteres incluyendo Mayúsculas, minúsculas, alfanuméricos y signos especiales según las recomendaciones de la ISO 27001. (A.5.1.1 Políticas de seguridad de la información.)
- bloqueo de acceso remoto completo, para todos los niveles de usuario hasta no hayan modificado su contraseña corporativa.

Análisis ICD (integridad, confiabilidad, disponibilidad)

Los archivos de la carpeta cumplen con Integridad y disponibilidad, pero **ya no son confidenciales**. Cualquier información operativa o de negocios debe darse por publica. Verificar potenciales riesgos a clientes e información clasificada.

Pruebas y Metodología.

Del chequeo del hash MD5 (comparación criptográfica del archivo) podemos detectar que el archivo “log.txt” difiere del backup inmediato anterior al evento. Si bien dicho archivo por si mismo no es prueba suficiente dado que guarda información de accesibilidad normal, detectamos que no existen entradas anteriores a las 12:34hs del 09-01-2024. Dicho archivo

debería contener otras entradas verificadas antes de esa estampa de tiempo. Esta prueba, sumada al acceso remoto desconocido, nos asegura que el archivo fue modificado para borrar evidencia del acceso.

Archivos	Hash Backup	Hash Actual	Check MD5
script.py	66bb9ec43660194bc066bd8b4d35b151	66bb9ec43660194bc066bd8b4d35b151	OK
log.txt	f2b0428b975452afbc641e46a042231b	0b29406e348cd5f17c2fd7b47b1012f9	Error
plan-A.txt	129ea0c67567301df1e1088c9069b946	129ea0c67567301df1e1088c9069b946	OK
plan-B.txt	4e9878b1c28daf4305f17af5537f062a	4e9878b1c28daf4305f17af5537f062a	OK
pass.txt	6d5e43a730490d75968279b6adbd79ec	6d5e43a730490d75968279b6adbd79ec	OK
copia.sh	90965b0eb20e68b7d0b59accd2a3b4fd	90965b0eb20e68b7d0b59accd2a3b4fd	OK

Imagen A.

Recomendaciones:

- Lanzar una campaña de concientización sobre el uso de contraseñas seguras y potenciales riesgos al negocio por divulgación de la información.
- Obtener software de vigilancia de red, dado que la compañía maneja en su mayoría un entorno Microsoft, se recomienda SOLARWINDS.
- Verificar los permisos de los usuarios remotos.
- Auditar las reglas de Firewall.
- No exponer archivos confidenciales sin antes utilizar un método de encriptación segura.

Sin otro particular.

John Locke

Hummingbird Ciberseguridad.