CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Incidente de ciberseguridad

Fecha: 16/04/2024

Problemática: **Ataque a proveedor de cadena de suministros del gobierno de Sevilla, España**

Correlativo: **AC-0014**

Institución / Sector: **Público y Privado**

SITUACIÓN

Empresa proveedora de cadena de suministross de Medios de Prevención Externos SUR S.L. con sede en Sevilla España ha confirmado que se encuentra experimentando un ciberataque de tipo «ramsomware» que afecto al Estado de Guardia Civil de España el pasado 22 de marzo de 2024. El actor de amenazas «lockbit3» se atribuyó el ataque a través de sus canales oficiales.

RIESGOS

- Cifrado de Información
- Daños críticos a la infraestructura tecnológica
- Suplantación de identidad
- Campañas de censura y desprestigio

RECOMENDACIONES

- Implementar y/o reforzar la seguridad perimetral
- Emplear contraseñas seguras
- Cambiar contraseñas periódicamente
- Utilizar la autenticación de dos factores
- Nunca haga clic en enlaces o descargue archivos adjuntos de fuentes desconocidas.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
No Urgente	Preventiva

Matriz de evaluación

Riesgo Alto/Medio/Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	Alto	Alto	Alto

ANEXO

GUARDIA CIVIL

Estimados guardias civiles, personal de Fuerzas Armadas y personal civil con destino en la Dirección General de la Guardia Civil.

Desde MEDIOS DE PREVENCION EXTERNOS SUR SL, empresa encargada en la realización de los reconocimientos médicos en el marco de la vigilancia de la salud, queremos comunicar que el pasado día 22 de marzo de 2024, nuestros sistemas de información han sufrido un ciberataque de tipo Ransonware Lockbit 3.0.

Inmediatamente se interpuso denuncia en Guardia Civil y se está trabajando conjuntamente con Telefónica para tratar de revertir, solucionar e investigar los hechos mencionados.

De acuerdo con lo establecido en el artículo 34 del Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos, se informa que los autores podrían haber tenido acceso a los siguientes datos confidenciales del personal de la Guardia Civil y de las Fuerzas Armadas y personal civil con destino en el ámbito de la Dirección General de la Guardia Civil:

- Número de la tarjeta de identificación profesional (TIP).
- Número de teléfono móvil.
- Correo electrónico.
- Fecha de nacimiento.
- Sexo.
- Puesto de trabajo.
- Resultado del reconocimiento médico.
- Certificado de aptitud.

Hasta el momento no hay evidencia de que se haya producido una fuga de dicha información y se han adoptado las siguientes acciones correctoras:

- Medidas técnicas e informáticas para detener la afectación del ciberataque y erradicar su capacidad.
- Análisis forense del impacto y alcance del ciberataque.
- Proceso de restauración de la información.
- Cambio masivo de contraseñas. Para ello, el usuario debe cliquear en "he olvidado contraseña" cuando acceda a la página web o la app. Esto hará que le llegue un correo electrónico donde podrá restablecerla. Dicha contraseña deberá cumplir unos requisitos de seguridad. Tendrá varios intentos para introducir la contraseña, tras los cuales, de no conseguirlo, el usuario se bloqueará durante unos minutos.

En todo caso, la empresa cuenta con copias de seguridad que ha permitido que podamos seguir prestando el servicio a todo el personal objeto de los reconocimientos médicos.

Para cualquier aclaración, duda o consulta al respecto, se adjunta la siguiente dirección de correo electrónico del delegado de protección de datos de nuestra empresa: dpo@ingadeconnect.es

EL DIRECTOR GENERAL
Gilberto Conde Rosado

GRUPO MPE
Avenida de la innovación 11, 41020, Sevilla
Teléfono: 910 888 127
Email: vigilanciasalud@guardiacivil@grupompe.es

REFERENCIAS

Fuente: https://twitter.com/ASESGC/status/1780178254512505148/photo/1