DIARIO FINANCIERO®

Fecha: 03/10/2024 Audiencia: 48.450 Sección: ACTUALIDAD
Vpe: $2.800.078 Tirada: 16.150 Frecuencia: OTRAS
Vpe pág: $7.443.240 Difusión: 16.150
Vpe portada: $7.443.240 Ocupación: 37,62%

CIBERSEGURIDAD: ¿CÓMO SE PROTEGEN LAS EMPRESAS MINERAS?

Con el avance tecnológico y la automatización de procesos, los riesgos de ciberataques son cada vez mayores. Aquí, varios expertos analizan las mejores estrategias para proteger la infraestructura crítica de las empresas del rubro.

POR MACARENA PACULL M.

El sector minero se ha visto beneficiado ante la irrupción de nuevas herramientas tecnológicas que se traducen en mayor eficiencia y productividad, pero estos avances abrieron la puerta a fuertes amenazas.

Los expertos advierten que proteger la infraestructura crítica es clave, porque la exposición de datos para una industria tan importante para el país podría provocar pérdidas y daños irreparables.

El fundador de Wingsoft, Danilo Naranjo, comenta que dentro del rubro se están implementando diversas estrategias de ciberseguridad para la protección de sus redes, y resalta que entre las principales acciones está la adopción de soluciones avanzadas como firewalls, sistemas de detección de intrusiones y monitoreo en tiempo real. Cuenta, además, que las empresas están invirtiendo en capacitaciones para sus equipos, en la segmentación de redes y en la actualización constante de los sistemas operativos para evitar vulnerabilidades. "Muchas compañías han integrado tecnologías como la inteligencia artificial para identificar amenazas emergentes y mejorar la respuesta ante posibles incidentes", enfatiza Naranjo.

El director de análisis e investigación de Kaspersky para América Latina, Fabio Assolini, advierte que en la industria no se conoce en

DIARIO FINANCIERO®

Fecha: 03/10/2024 Audiencia: 48.450 Sección: ACTUALIDAD
Vpe: $2.817.951 Tirada: 16.150 Frecuencia: OTRAS
Vpe pág: $7.443.240 Difusión: 16.150
Vpe portada: $7.443.240 Ocupación: 37,86%

detalle cuál es la estrategia adoptada por cada empresa minera para proteger sus redes y sistemas de control, pero sí se han analizado las que deberían tener en cuenta para estar protegidas. Entre las buenas prácticas a considerar destaca el aislamiento de la red, algo que a raíz de la pandemia cambió bastante. "En la pandemia, muchas empresas adoptaron accesos remotos a los sistemas industriales, y así se han quedado hasta el día de hoy. De ahí vienen los peligros y riesgos de ataque e invasión, al poder acceder de forma remota", dice, mientras advierte que se debe cuidar la autenticación en caso de mantener esta modalidad.

"El uso de tecnologías de seguridad como la autenticación multifactor y la encriptación de datos está ganando relevancia, sobre todo para proteger la comunicación entre los equipos en terreno y los centros de control remoto", añade el CEO de Unitti, Cristián López. El ejecutivo cuenta que, además, muchas compañías deberían optar por servicios de monitoreo externo 24/7 para detectar y mitigar ataques de manera temprana. Añade que la capacitación continua en temas de ciberseguridad también es clave, ya que los errores humanos

son frecuentes y un paso en falso o un descuido pueden vulnerar a una empresa entera.

El director del magíster en ciberseguridad de la Facultad de Ingeniería y Ciencias de la Universidad Adolfo Ibáñez, Ricardo Seguel, ha observado que, actualmente, las empresas están fortaleciendo en capas el control de acceso y cifrado en la infraestructura crítica, como redes wi-fi, celulares 4G/LTE y 5G privadas, enlaces de internet para operaciones remotas de las faenas, conexiones entre máquinas y el monitoreo en tiempo real de cada artefacto conectado a la red.

"La capacitación continua del personal en ciberseguridad también es clave, ya que el error humano es uno de los puntos más vulnerables en este tipo de infraestructuras críticas", enfatiza el CEO de Unitti, Cristián López.

Para enfrentar las amenazas cibernéticas, el director de agilidad & innovación en Nisum Chile, Fernando Benavides, resalta estrategias robustas como separar las redes tecnológicas de las operativas para evitar que una vulnerabilidad en una afecte a la otra. Para que no ocurran interrupciones en sus operaciones, cuenta que las compañías están implementando planes de recuperación ante desastres, que definen "cómo deben responder ante un ataque, garantizando que las operaciones sigan funcionando o se restablezcan rápidamente".

Seguel indica que, además, se están agregando controles de monitoreo preventivo para responder ante una amenaza, con herramientas de ciberinteligencia y con el aislamiento y virtualización de parches en sistemas industriales legados u obsoletos que, señala, son difíciles de reemplazar por otros modernos por el costo que esto significa. Además, asegura que se está fortaleciendo la seguridad de la cadena de suministro tecnológica, exigiendo a los proveedores de la industria certificaciones como la ISO 27001 y SOC2.