INNOVACIÓN Y TECNOLOGÍA

CIBERSEGURIDAD EN MINERÍA: CONTROLES PREVENTIVOS Y PRUEBAS PROACTIVAS

Con los avances tecnológicos y el aumento del trabajo a distancia, la industria minera es susceptible de sufrir nuevas y avanzadas amenazas y ataques cibernéticos que pueden causar daño tanto interno como a la industria en general.

La transformación digital tiene el potencial de ayudar a las empresas mineras a reducir costos y mejorar sus resultados al agilizar los procesos de trabajo y proporcionar una mayor comprensión del negocio, impulsando la toma de decisiones estratégicas, a partir de los datos obtenidos a partir de diferentes sistemas. La importancia de las tecnologías digitales en la industria minera se reconoce cada vez más a medida que las organizaciones exploran soluciones para reducir la incertidumbre geológica, la volatilidad del mercado y los riesgos operativos. Sin embargo, a medida que la industria minera sigue adoptando estas tecnologías emergentes, el sector se abre a nuevos riesgos potenciales y a la ardua tarea de proteger sus activos, adoptando diferentes mecanismos y controles que permitan disminuir de forma oportuna la superficie de ataque.

LA IMPORTANCIA DE LA CIBERSEGURIDAD EN EL SECTOR

A medida que la industria minera adquiere tecnologías digitales más sofisticadas y eficientes, estas tecnologías también crean nuevos riesgos de posibles ciberamenazas y ataques. Estos riesgos incluyen el acceso no autorizado a sistemas e información confidencial, exposición de datos y ciberespionaje. Los ataques pueden provocar disrupción en la operación y generar pérdidas económicas, daño a la imagen corporativa y uso indebido de información confidencial.

La adopción de controles de seguridad adecuados y la aplicación de un marco de gestión de la ciberseguridad integrado son esenciales para que cualquier organización del sector minero, incluidos sus proveedores, pueda evitar la interrupción del servicio y reaccionar de forma oportuna y efectiva ante las amenazas. Es fundamental construir operaciones fiables y resistentes, para permitir la convergencia segura entre la tecnología operativa y la tecnología de la información (OT/IT), impulsando de este modo la responsabilidad en toda la cadena de valor.

ASEGURANDO LA TRANSFORMACIÓN DIGITAL A TRAVÉS DE UNA ESTRATEGIA DE CIBERSEGURIDAD

Es imprescindible contar con una estrategia de ciberseguridad alineada a diferentes estándares y buenas prácticas internacionales y posibles regulaciones locales, permitiendo incluir a todas las áreas de la compañía para ser partícipes de los procesos de aseguramiento de la información y los activos OT/TI, reconocer la importancia y el rol de los colaboradores en la defensa de dichos activos e implementar controles que permitan asegurar la operación y garantizar su continuidad.

Dicha estrategia debe ser adaptable al panorama actual de amenazas y al contexto empresarial, enmarcada en un proceso de mejora continua que puede estar en constante evolución.

Desarrollo e implementación de una estrategia que equilibre las personas, los procesos y las tecnologías.

Para crear una estrategia de ciberseguridad holística, es necesario gestionar los riesgos de forma continua, educar a los colaboradores, gestionar las expectativas de la junta directiva y asegurarse de cumplir la normativa. Mas importante aún, es necesario que todas las piezas de la estrategia sean cohesivas; las herramientas y los recursos deben estar sincronizados para aumentar la visibilidad de los eventos y atender las necesidades de los usuarios, en un entorno cambiante que requiere de la disponibilidad de los sistemas en todo momento.

Este proceso de implementación de la estrategia requiere del liderazgo de la alta dirección, quienes deben designar los recursos clave para cumplir con los planes a corto, mediano y largo plazo. Esto implica destinar entre el 10% y el 15% del presupuesto anual de OT/TI para temas de ciberseguridad.

¿POR DÓNDE EMPEZAR?

La implementación se debe iniciar con las siguientes actividades:

1. Diseño del Gobierno de la ciberseguridad: Definición de la estructura organizacional del área, objetivos, roles y responsabilidades, procesos, comités asociados e información requerida para hacer seguimiento y control.
2. Selección de personal: encontrar personas con habilidades y experiencias en la materia es tarea complicada; sin embargo, la recomendación es tener una variedad de personas experimentadas en ciberseguridad, en el negocio y hacer alianzas con proveedores estratégicos que conozcan la industria.
3. Elegir un asesor de confianza para el diseño y la implementación de la estrategia y los servicios especializados.
4. Implementar las estructuras internas y las tecnologías necesarias para habilitar una línea base de ciberseguridad, tomando como referencia los 18 controles críticos de ciberseguridad de CIS.

Posteriormente, tomar como referencia un marco internacional como el NIST o la ISO 27032 para aumentar el nivel de madurez de la organización de manera iterativa. El tiempo necesario para implementar una primera versión puede tomar entre seis y dieciocho meses dependiendo del tamaño de la organización.

La estrategia de ciberseguridad siempre tiene que estar alineada con el negocio, el contexto geopolítico, social y financiero y con las amenazas y riesgos relacionados. Por ende, es necesario monitorear estas variables y adaptar la estrategia en consecuencia de los cambios a nivel interno y externo que trae consigo la transformación digital. Durante los últimos años la tendencia fue hacia una digitalización y nivel de exposición digital creciente al igual que el nivel de amenazas en Internet. Los niveles de inversiones en ciberseguridad aumentaron de manera idéntica.

A nivel táctico, la recomendación es partir con la implementación de controles orientados a:

1. Seguridad en redes perimetrales
2. Seguridad en dispositivos, tanto de la red operativa como tecnológica
3. Seguridad en aplicaciones y software de apoyo al negocio
4. Seguridad de datos
5. Identificación, gestión de accesos y privilegios
6. Diseño de una arquitectura basada en el modelo de “cero confianza” (zero trust)

El cambio en la industria minera es una realidad y la digitalización del sector se ha convertido en una prioridad que implica transformar la operación de forma segura, disminuyendo las posibilidades para ser vulnerados, reconociendo la necesidad de implementar controles de ciberseguridad desde la planificación de los proyectos y hacer un seguimiento continuo que facilite la mejora en todos los niveles de la compañía./BM

Fuente: Dreamlab Technologies Chile