LITORALPRESS

Fecha: 24-12-2024
Medio: El Mercurio
Supl. : El Mercurio - Minería y Comunidad
Tipo: Noticia general
Título: Cuando los peligros de la ciberseguridad traspasan las barreras digitales

Pág. : 3
Cm2: 612,0

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

SABOTAJE INDUSTRIAL EN MINERÍA:

Cuando los peligros de la ciberseguridad traspasan las barreras digitales

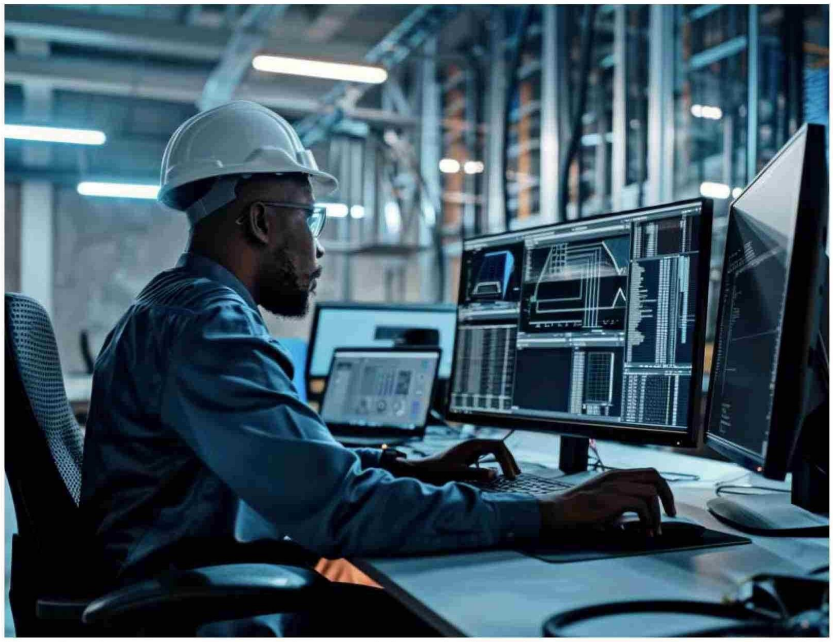
La integración de los sistemas operativos y tecnológicos es una amenaza, en la medida en que un ataque informático puede provocar el mal funcionamiento de maquinarias e, incluso, poner en riesgo la vida de las personas.

CATERINNA GIOVANNINI

En agosto de este año, el grupo minero Industrias Peñoles de México fue atacado por un *ransomware*, un código capaz de impedir el funcionamiento de los ordenadores que infecta. Ese mismo mes, Evolution Mining, en Australia, también detectó un incidente de este tipo. Casi un año antes, en noviembre de 2023, un ciberataque afectó por tres días la actividad de algunos camiones autónomos de Codelco en Antofagasta.

Este último incidente demuestra la gravedad que suponen los ataques a la ciberseguridad en la industria minera, especialmente por su potencial impacto en la seguridad de las personas y de la infraestructura crítica. Para la directora ejecutiva de la Corporación de Ciberseguridad Minera, Katherina Canales, "no es lo mismo que un atacante ingrese a la base de datos de una organización a que entre al control industrial de maquinarias, porque ahí ya está en riesgo la vida de las personas".

Ese tipo de ataques, que podrían comprometer la seguridad de las operaciones mineras, causar lesiones a los trabajadores, daños a equipos e incluso daños ambientales, son los que Marcos Riveros, gerente del área Negocios Estratégicos en ITQ Latam, define como sabotaje industrial.



No es lo mismo que un atacante ingrese a la base de datos de una organización a que entre al control industrial de maquinarias, porque ello afecta la seguridad de los trabajadores.

EL MAYOR RIESGO

Este podría ser un riesgo cada vez más frecuente en sectores industriales que, en busca de mayor interoperabilidad y eficiencia operativa, integran tecnologías que digitalizan la realidad. Así, los elementos físicos y tangibles de la vida cotidiana pasan a estar a merced de ciberamenazas que antes se limitaban a lo virtual, explica el Equipo de Respuesta ante Incidentes de Seguridad Informática del Ministerio del Interior en su página web.

En estos casos, "los dispositivos de tecnología operativa (OT) son particularmente vulnerables, ya que suelen carecer de las actualizaciones regulares y los estándares de seguridad robustos que caracterizan a los sistemas de tecnologías de la información (TI)", explica Erich Zschaeck, gerente sénior de Ciberseguridad de EY.

Canales coincide y agrega que con el paso de los años, esos equipamientos tecnológicos son más vulnerables a los ataques porque pierden la garantía de soporte técnico de los fabricantes, algo que pasa porque "las mineras proyectan su inversión a largo plazo", explica, y los equipos se vuelven antiguos.

Por esto es que "la innovación tecnológica en la minería debe venir aparejada de las soluciones que la protejan. El punto ya no es saber si serán o no atacadas, sino que cuándo", explica Riveros.

Para protegerse y prevenir incidentes, "cada vez que levantamos un sitio web, desarrollamos una aplicación, etc., todo tiene que hacerse en base a prácticas de desarrollo seguro que nos permitan blindar nuestros equipos tecnológicos, nuestras infraestructuras", explica Canales.

Para lograrlo, las empresas deben empezar por identificar los activos críticos y comprender en detalle su tecnología, tanto de TI como de OT, explica Zschaeck. Una vez identificados estos activos, se pueden evaluar las posibles amenazas y vulnerabilidades asociadas a ellos para, a continuación, implementar "estándares de configuración segura con sistemas de monitoreo que detecten comportamientos anómalos", afirma el experto.

También se debe tener en consideración a los trabajadores de la minería. "En ciberseguridad se dice que las personas son el eslabón más débil, porque basta un clic en un correo malicioso para que infectes a tu organización", dice Canales, quien agrega que para estar realmente preparados es necesario poner en marcha planes de educación, capacitaciones y realizar ejercicios de crisis con equipos de profesionales de ciberseguridad que puedan desarrollar planes de respuesta ante incidentes.

"En ciberseguridad se dice que las personas son el eslabón más débil, porque basta un clic en un correo malicioso para que infectes a tu organización".

KATHERINA CANALES, directora ejecutiva de la Corporación de Ciberseguridad Minera.