Ataques Cibernéticos en el Sector de Manufactura

¿Por qué el sector manufacturero?

Los sistemas informáticos para la manufactura cada vez están más conectados, cuentan con mayor eficiencia brindando control e información en tiempo real. Las redes de Tecnología Operativa (TO) y Tecnología de la Información (TI) están cada vez más conectadas. Con TO proporcionando funcionalidad para dispositivos y procesos de control, y TI ofrece aplicaciones comerciales y de escritorio, la industria ha avanzado de manera drástica.

Dicho esto, la conectividad también tiene sus desventajas. por ejemplo, un problema importante con los sistemas conectados es que las redes de TO a menudo consisten en sistemas más antiguos (heredados) que no tienen parches y están desactualizados. Al conectarse con sistemas de TI más nuevos, este déficit de seguridad puede exponer los puntos débiles de TO. Muchas redes de TO carecen incluso de precauciones simples, como software antivirus, firewalls e inicios de sesión seguros.

Cuanto mayor sea el impulso de la digitalización para satisfacer la creciente demanda de velocidad, eficiencia, control y comodidad, mayores serán las vulnerabilidades.

Las empresas enfocadas al sector de la manufactura se han convertido en un objetivo principal para los delincuentes cibernéticos por distintos motivos como lo son:

- Acelerado avance en la digitalización e innovación, al igual que el almacenamiento de datos sensibles y valiosos en línea.
- Uso creciente de dispositivos de Internet de las Cosas (IoT/Internet of Things) (por ejemplo, para controlar la temperatura, la vibración, la presión, la humedad). Los dispositivos IoT crean sin duda una superficie de ataque más grande.
  - Una característica notable de los dispositivos IoT es que no siempre incorporan “seguridad por diseño”, lo cual garantiza que los dispositivos sean lo más seguros posible desde el inicio. Parchar los agujeros de seguridad y abordar las vulnerabilidades en los dispositivos IoT es responsabilidad del consumidor, un problema que no siempre es plenamente apreciado por quienes los usan.
- Ataques relacionados con el robo de IP.
- El número de dispositivos móviles conectados de forma remota. Esto aumenta el número de puntos vulnerables del perímetro de la red.
- El uso de infraestructura crítica y sistemas de control industrial. El reciente aumento de los ataques de ransomware contra dichas infraestructuras representa un riesgo mayor.
- La creciente amenaza de ataques de phishing contra los empleados.
- Una percepción de que la industria tiene un enfoque en parte reactivo a la seguridad cibernética.
- La creciente sofisticación de los ataques cibernéticos.

¿Estamos realmente en riesgo?

Un ataque cibernético en este sector puede conducir a la interrupción o el bloqueo de los procesos, creando daños significativos y consecuencias financieras considerables.

Incluso si la línea de producción en sí no se ve impactada físicamente, cualquier interrupción en los sistemas que controlan "la entrada de material" y la "salida de bienes" podría paralizar la producción. La complejidad que se refleja en la interfaz entre las distintas partes del proceso (por ejemplo, coordinación de la materia prima, compras, procesamiento, gestión de pedidos, embalaje, entrega y facturación) creando una vulnerabilidad elevada; cualquier ataque cibernético puede tener un efecto significativo en la producción y en los resultados financieros.

Los incidentes cibernéticos también pueden tener implicaciones con terceros. Una interrupción del servicio en una empresa manufacturera puede tener graves consecuencias. Existe el riesgo de que no se cumplan los acuerdos de suministro, lo que puede desencadenar la responsabilidad por incumplimiento de contrato. También existe la posibilidad de que el malware se transmita a otros a través de un punto débil en el sistema, poniendo en peligro la red de clientes y contactos de una empresa, con la posibilidad de nuevas reclamaciones.

Casos de estudio

10 minutos de daños

El administrador de TI de una empresa manufacturera fue despertado a las 3:00 am por una alerta, informándole que el sistema informático estaba presentando comportamiento irregular. Inmediatamente se contrató a un equipo externo de respuesta de incidentes cibernéticos, que reveló ataques al sistema por parte de TrickBot y Ryuk (ransomware). Tras eludir los procedimientos de autenticación, el ataque de ransomware pudo propagarse a 105 sistemas en diez minutos. Se identificó un patrón de ataque donde el análisis forense concluyó que el ataque es atribuible a un sofisticado grupo de atacantes cibernéticos que utiliza Ryuk para atacar a empresas con el objetivo de obtener montos de rescate elevados.

Si bien el ataque se contuvo con bastante rapidez, los retrasos significativos continuaron perjudicando la producción durante los siguientes 67 días. Los costos fueron elevados y abarcaron desde la respuesta a la violación hasta los gastos de restauración del sistema y de los datos. Esto implicó un impacto considerable en los ingresos, mientras que las líneas operativas se vieron obstaculizadas. La compañía contaba con una póliza de Cyber la cual apoyó para resarcir el daño ocasionado por los atacantes.

Líneas de producción infectadas

En 2018 Taiwan Semiconductor Manufacturing Company - TSMC sufrió pérdidas superiores a los 170 millones de dólares tras sufrir un ataque cibernético. El ataque a TSMC fue causado por la variante del ransomware WannaCry, infectando las líneas de producción. La producción de TSMC tuvo que detenerse en tres ubicaciones distintas durante un máximo de tres días, cuyo efecto se entiende que causó un déficit de ingresos del 2% durante ese trimestre.

Seguro de Cyber

No podemos exagerar la importancia de implementar una estrategia integral de seguridad cibernética para su organización. Es vital salvaguardar los sistemas de una empresa para permitirle proteger sus actividades, clientes, reputación e ingresos. Es fundamental reconocer las vulnerabilidades particulares en todo el sector de manufactura.

En Lockton actuamos para un número significativo de empresas de manufactura, lo que nos proporciona una excelente exposición a los hábitos de compra cibernética y a los riesgos que enfrenta el área.

Una póliza de protección de datos está diseñada para responder a los siguientes eventos, que no necesariamente serían cubiertos por pólizas más tradicionales:

- Violación de datos de un ataque cibernético.
- Pérdida financiera e impactos reputacionales tanto a la compañía como a los altos directivos por la falla de un sistema informático debido a un ataque malicioso.
- Defensa regulatoria, multas y sanciones civiles como resultado de una violación de la seguridad (asegurable por ley).
- Costos de respuesta a la violación.
- Solicitud de rescate (ransom) tras un ataque a los sistemas informáticos.

Un ataque cibernético puede tener ramificaciones de gran alcance para el sector de manufactura. Comprender estos riesgos y mitigarlos de manera proactiva es clave. Nuestro equipo de expertos en riesgos cibernéticos trabajará con usted para crear una solución personalizada que proteja y asegure su negocio exactamente donde lo necesita, asegurando que los riesgos cibernéticos se integren en su proceso de gestión de riesgos. Reconstruir la confianza es vital.

Para mayor información:

Ricardo Millán
Head ProFin México
ricardo.millan@lockton.com

Moisés García
ProFin México
moises.garciab@lockton.com