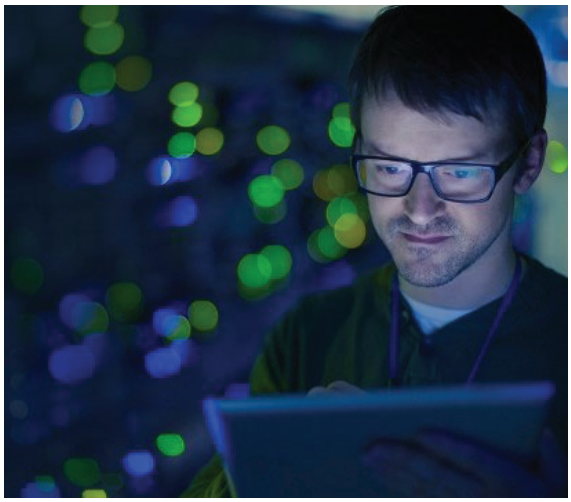
Reacción: El mantenimiento de la vigilancia de la seguridad cibernética durante los constantes desafíos al negocio.

12 de mayo de 2020

Las acciones para mitigar la propagación de COVID-19 están obligando a las organizaciones en la industria de productos químicos y tecnologías a aumentar su dependencia del acceso remoto y del menor personal operativo en el sitio, lo que plantea nuevas preocupaciones vinculadas a la seguridad cibernética. Hablamos con Paul Harnick, Jefe Global de Productos Químicos de KPMG, sobre cómo el sector busca reforzar las ciberdefensas a pesar del impacto que implican los bajos precios del petróleo.



¿Cómo se ven afectadas las operaciones cibernéticas de las compañías químicas estadounidenses por la COVID-19?

Al igual que los líderes empresariales y tecnológicos de todo el mundo, los directores de seguridad de la información (CISO) de los productos químicos están preocupados por mantener saludable su fuerza laboral, al tiempo que deben procurar el mantenimiento de las operaciones cibernéticas que protegen tanto la tecnología de la información como la operativa (TI y OT). El mantra de los intentos de "cuándo, no si" para atacar los sistemas se aplica ahora más que nunca.

Con la COVID-19 provocando interrupciones en toda la cadena de suministro, muchas organizaciones químicas están implementando un nuevo enfoque sobre el efectivo y el capital de trabajo, y están revisando rápidamente sus gastos de capital para el próximo año.

A pesar de la urgente necesidad de mantener la seguridad, los proyectos cibernéticos se encuentran entre los más retrasados o cancelados. Las operaciones internas están buscando ser más ágiles, con reducciones o retrasos en las plantas a medida que se implementan más protocolos de distanciamiento social, lo que resulta en un aumento potencial del riesgo tanto para la seguridad como para el espacio OT.

Finalmente, se considera que las poblaciones de 60 años o más tienen mayor riesgo de complicaciones por el virus. Teniendo esto en cuenta, el impacto potencial de COVID-19 en las operaciones de una planta química aumenta, debido a la elevada experiencia promedio de su fuerza laboral y porque los ingenieros senior solo pudieron adquirir un profundo conocimiento del negocio con décadas de trabajo.

¿Cuáles son las preocupaciones cibernéticas específicas para la industria química en TI y OT?

A medida que algunos actores buscan aprovecharse de esta situación marcada por un período de menor fuerza operativa disponible, se anticipa un número creciente de ataques de phishing. De hecho, la Oficina Federal de Investigaciones de EE. UU. advierte sobre un aumento en los ataques cibernéticos relacionados con la COVID-19, incluidos los CDC falsos y los correos electrónicos de phishing[1]. Los expertos en cibernética en el Reino Unido señalaron que los ataques en línea están aumentando y evolucionando[2]. De hecho, los ciber-adversarios ya se están aprovechando de la situación, y los correos electrónicos de phishing relacionados con la COVID-19 están sucediendo en conjunto a cargas de malware.[3]

[1] Fuente: Oficina Federal de Investigaciones. Alerta número I- 032020-PSA: El FBI ve un aumento en los esquemas de fraude relacionados con la Pandemia por el coronavirus (COVID-19).

[2] Fuente: Centro Nacional de Seguridad Cibernética. Informe de Amenaza semanal del 27 de marzo de 2020.

[3] Fuente: Lectura oscura. "El FBI advierte sobre correos electrónicos falsos de los CDC en Alerta de phishing por la COVID-19 ". 23 de marzo de 2020.

Por lo general, el vector de ataque es a través de la TI corporativa y, luego, baja a la zona industrial, cuando el ciber-adversario ha identificado la cuenta de un empleado involucrado en TI y OT. Mientras tanto, los sistemas de la planta —incluidos los sistemas de control distribuido (distributed control systems, DCS), los sistemas de control de supervisión y adquisición de datos (supervisory control and data acquisition systems, SCADA) y los controladores lógicos programables (programmable logic controllers, PLC)— dependen de sus proveedores propietarios que, tradicionalmente, proporcionan soporte en el sitio o desde las oficinas de los proveedores. Ahora, con las medidas de aislamiento y distanciamiento social, el personal del proveedor está obligado a trabajar de forma remota, lo que añade aún más "saltos" y problemas a la ciberseguridad. Esto ha impactado en una variedad de actividades, desde el mantenimiento normal hasta los proyectos dedicados y, lo que es más importante, a eguridad y los parches del sistema.

¿Cómo está lidiando la industria con un mayor riesgo cibernético, mientras que al mismo tiempo maneja los más grandes desafíos de la COVID-19?

Cada organización se encuentra en niveles diferentes de madurez, capacidades de respuesta operativa y organización en materia de seguridad. Dicho esto, la mayoría de las organizaciones se han refugiado en sus planes de continuidad operativa (BCP) como resultado a las restricciones de viaje y distanciamiento social impuestas por la COVID-19, y están operando con un equipo mínimo en la oficina. Esto funciona para la mayoría de los empleados "corporativos" que pueden operar de forma remota con una computadora portátil y acceso VPN.

Sin embargo, el riesgo aumenta potencialmente a nivel de operaciones de la planta a medida que se reducen los niveles de personal y se incrementa el trabajo remoto, presionando a los equipos de TI y OT que administran esas operaciones. Y como ya se mencionó, los proveedores de servicios críticos como DCS, SCADA y PLC ahora también necesitan operar de forma remota. Donde los contratos en la cadena de suministro ya permitía el acceso remoto para las compañías externas, ahora es más probable que el acceso sea más remoto a través de las redes VPN de los proveedores. La infraestructura de seguridad en los proveedores también estará bajo carga adicional, ya que los trabajadores remotos no tendrán acceso tradicional a las herramientas y recursos de seguridad de TI en las oficinas, lo que eleva el riesgo de compromiso.

Para acomodar la necesidad de trabajo remoto, las organizaciones de productos químicos tienen que aumentar el uso de infraestructura remota. Sin embargo, tal cosa significan más "agujeros" en los cortafuegos de los sistemas corporativos y OT que requieren monitoreo por parte del equipo de seguridad cibernética, y un mayor riesgo de que el malware, si se implementa con éxito, pueda afectar la seguridad, la producción y la integridad operativa. Desafortunadamente, las realidades económicas de la COVID-19 sin duda continuarán teniendo efectos en la entrega operativa de herramientas cibernéticas a medida que los proyectos de seguridad tradicionales estén sujetos a duras revisiones presupuestarias.

Mientras tanto, desde una perspectiva en salud y seguridad, las operaciones en planta buscarán limitar la exposición de los trabajadores, incluyendo la incorporación de turnos que mantengan a los mismos equipos de ingenieros para limitar la exposición generalizada a la COVID-19 y, donde sea posible, se aprovecharán las salas de control múltiple (incluidas las salas de entrenamiento) para reducir la exposición y la carga en el centro neurálgico de las operaciones de la planta. Sin embargo, esto presenta un posible dolor de cabeza en caso de que el virus afecte a uno de los equipos. Si el virus continúa propagándose entre la fuerza laboral, las operaciones actuales de BCP deberán ajustarse aún más, aunque a corto plazo este proceso de igualación de turnos debería proporcionar un alivio táctico. Sin embargo, las presiones económicas (tanto la oferta como la demanda) pueden requerir un replanteamiento de las operaciones en el mediano plazo, junto con una mayor presión en los cambios de planta y mantenimiento (que tradicionalmente tienen hasta tres veces más personal en el piso), los que también suponen parches de seguridad.

Dadas las preocupaciones sobre el grupo demográfico de empleados en mayor riesgo, algunas organizaciones están iniciando una documentación acelerada y extensa de las operaciones en planta y del conocimiento crítico de los ingenieros y otros empleados clave. Este esfuerzo a menudo se combina con una revisión de los procesos de seguridad operacional, que se enfoca en capturar la lógica de administración de alarmas para las operaciones de la planta y la necesidad de que estas estén en su lugar.

¿Qué consideraciones deben tener en cuenta las compañías químicas al proteger sus operaciones y garantizar que sus planes BCP sean lo más sólidos posible?

— En el corto plazo, considerar la necesidad de continuar operando con personal reducido bajo el BCP por más tiempo de lo previsto. Sin embargo, ahora también es el momento de comenzar a actualizar el BCP a la luz de interrupciones que podrían durar por un plazo más largo, y hacer una prueba de resistencia al BCP para escenarios en los que se producen múltiples interrupciones al mismo tiempo.

— Acelere cualquier revisión de seguridad planificada, incluida una revisión de los arreglos y procedimientos de acceso remoto para las organizaciones de OT (buscando ganancias rápidas de seguridad para aquellos que tienen acceso remoto al entorno de la planta desde el exterior) y observe cualquier endurecimiento de OT que se pueda hacer tácticamente.

— Considere si las operaciones de seguridad son robustas y capaces de manejar tanto la capa de TI como la de OT, y, cuando sea posible, aumente la capacidad de la organización para "buscar lo malo" en las redes.

— Revise los riesgos de OT en torno a las implementaciones de parches demorados y las vulnerabilidades potenciales que pueden causar esos retrasos, asegurándose de que tenga controles compensatorios (por ejemplo, asegurándose de que el Sistema instrumentado de seguridad -Safety Instrumented System, SIS- todavía esté aislado del resto de la red).

— Planifique y realice actividades de prueba de penetración remota para verificar y asegurar las instalaciones, especialmente las VPN de la planta. (La preocupación ahora es que esto necesitará un cambio y una expansión continuos, sin recursos para administrar, cambios de políticas y monitoreo continuo)

.

— Revisiones de eficiencia operativa: Realice revisiones de BCP/Disaster Recovery con un enfoque en la documentación crítica para poner "conocimiento en cabeza" en papel y una posible racionalización de los procedimientos de la planta.

— Evalúe formas de ayudar a apuntalar las defensas con ganancias rápidas, como BCP o revisiones de documentación de operaciones, revisiones de procesos y corrección de riesgos de conjuntos de herramientas. Asegúrese de compartir las mejores prácticas en toda la organización y busque proporcionar los recursos adecuados para ayudar a abordar la creciente confluencia de riesgos.

Si se tienen en cuenta estas consideraciones, junto con la realización de exámenes periódicos en ciberseguridad, las organizaciones químicas pueden ayudar a mantener la seguridad de las plantas y, al mismo tiempo, es probable que desarrollen una serie de nuevos y eficaces métodos de trabajo que puedan volver a utilizarse en el futuro.

KPMG Global Energy Institute

El KPMG Global Energy Institute (GEI) es un foro mundial de intercambio de conocimientos sobre temas actuales y emergentes de la industria. Lanzado en 2007, el GEI interactúa con más de 30.000 miembros a través de múltiples canales de medios, incluyendo transmisiones por Internet de audio y video, publicaciones y white papers, podcasts, eventos y boletines trimestrales. Suscríbase hoy para comenzar a recibir información valiosa sobre temas críticos de negocios y asuntos de la industria visitando read.kpmg.us/gei.

Contáctenos

Manuel Fernandes
Socio líder de Energía y Recursos Naturales de KPMG en América Latina
mfernandes@kpmg.com.br
+55 (21) 2207-9412

Leandro Augusto Marco Antonio
Socio líder en Seguridad Cibernética en KPMG en Brasil y Sudamérica
LAntonio@kpmg.com.br
+55 (11) 3940-3740

www.kpmg.com