Ciberseguridad enfocada al sector químico

James R. Slaby
Director of Cyber Protection, Acronis

Estos son tiempos difíciles para la industria química, los hackers y los gobiernos están atacando cada vez más a los ciberataques. Se unen a las filas otros sectores para los cuales los datos robados o perdidos y el tiempo de inactividad son amenazas graves para el negocio, como la atención médica (donde el tiempo de inactividad en la sala de emergencias es una cuestión de vida o muerte), la fabricación (donde los costes de inactividad de la fábrica pueden alcanzar cientos de miles de euros por hora), y los sistemas escolares (donde los servicios comprometidos pueden costarles el trabajo a políticos y administradores).

Las empresas químicas presentan un objetivo atractivo porque también sufren enormes costes de tiempo de inactividad, son los custodios de la propiedad intelectual sensible y pueden perder la confianza de los clientes, socios e inversores si sufren un grave ataque de malware. El ataque de ransomware del año pasado al productor noruego de aluminio Norsk Hydro redujo su producción en más del 50 % durante varias semanas y le costó al menos 58M de dólares, minando sus ganancias trimestrales en un 82 %. Las compañías químicas estadounidenses Hexion y Momentive también sufrieron ataques de ransomware el año pasado que destruyeron los datos en cientos de sus ordenadores, lo que obligó a su costoso reemplazo.

AMENAZAS DE NIVEL SUPERIOR: APAGANDO LOS ATAQUES DEL "DÍA CERO"

El ransomware, el malware utilizado para atacar a Norsk y objetivos similares, es ahora la amenaza cibernética de mayor crecimiento y penetración del mundo. Un ataque exitoso de ransomware bloquea los datos de los sistemas objetivo con un cifrado irrompible, luego exige una tarifa de extorsión considerable en bitcoin para que las claves lo desbloqueen. Desde su aparición inicial a gran escala hace unos años con las notorias pandemias mundiales WannaCry y NotPetya, ha crecido de manera constante y se proyecta que inflija 20 mil millones de dólares en daños a las empresas en todo el mundo en 2020.

» Las empresas químicas presentan un objetivo atractivo porque también sufren enormes costes de tiempo de inactividad

La defensa de los sistemas del sector químico de los ataques de ransomware requiere una estrategia de defensa en profundidad. Eso comienza con el seguimiento de las vulnerabilidades conocidas en los sistemas operativos y las aplicaciones, y la instalación de actualizaciones de software y parches de seguridad para cerrarlos lo antes posible. El software antivirus basado en firmas puede ayudar a detener las amenazas de malware conocidas, pero los ciberdelincuentes ahora generan nuevas iteraciones de malware

con tanta rapidez que a menudo evaden estas defensas. La detención de las llamadas amenazas de "día cero" requiere soluciones antimalware de comportamiento que empleen inteligencia artificial para identificar procesos maliciosos, incluso desconocidos anteriormente, por sus acciones y luego terminarlos.

CAPAS ADICIONALES DE DEFENSA

La capacitación en conciencia de seguridad también es un elemento esencial de la ciberseguridad. Las empresas deben llevar a cabo una educación periódica sobre las técnicas de infección más comunes como el phishing: correos electrónicos de aspecto inocente que importan malware si un usuario hace clic en sus enlaces o archivos adjuntos incrustados.

Hacer cumplir una fuerte disciplina de autenticación, al insistir en el uso de la autenticación multifactor, alentar contraseñas más largas y desalentar la reutilización de credenciales en varias cuentas, puede ayudar a frustrar los ataques que aprovechan las numerosas violaciones de datos en los últimos años. Estos llamados ataques de "relleno de credenciales" explotan el hecho de que las personas reutilizan las mismas contraseñas para todas sus cuentas. Los delincuentes tomarán contraseñas robadas en una violación de datos y las probarán en todas partes. Cuando encuentran una coincidencia, pueden robar datos valiosos y propagar ransomware u otro malware.

La protección de datos clásica en forma de respaldo y recuperación ante desastres también es una red de seguridad esencial contra los ciberataques. En el caso de una pérdida masiva de datos infligida por malware, las empresas con regímenes de copia de seguridad diligentes pueden simplemente retroceder el reloj a su estado previo al ataque. Otras herramientas que pueden ser útiles para agregar capas de defensas incluyen el escaneo de vulnerabilidades de aplicaciones, prácticas de desarrollo seguras y firewalls de aplicaciones.

RESPUESTA DE INCIDENCIA DE SEGURIDAD

Es aconsejable suponer que en algún momento un ataque atravesará las defensas más rigurosas. Todo lo que se necesita es que un empleado desprevenido haga clic en el archivo adjunto de un correo electrónico incorrecto, momento en el cual la capacidad de una empresa para recuperarse del daño de manera efectiva y rápida será su mejor salvavidas. Esa inevitabilidad hace que sea crítico construir un plan de respuesta a incidentes de seguridad. El proceso comienza con la identificación de las personas clave que deben actuar primero después de un incidente: personal de TI con credenciales administrativas y conocimiento del diseño de la infraestructura. Los líderes de otros departamentos, desde altos ejecutivos hasta personal legal, de gestión de riesgos, cumplimiento y comunicaciones externas, también deben ser identificados por los aspectos no técnicos de la respuesta.

» Se debe definir qué amenazas requieren una escalada inmediata, por ejemplo, interrupciones de la aplicación, destrucción de datos, violaciones de la privacidad, daños a la reputación de la empresa, etc.

El plan también debe nombrar delegados para cubrir los días festivos u otras ausencias y publicar su información de contacto y la de los principales proveedores de tecnología y proveedores de servicios. Al menos a una persona se le debe otorgar la autoridad para hacer llamadas en caso de emergencia, por ejemplo, si se debe cerrar la red para evitar la propagación de un ataque de ransomware. Se debe definir qué amenazas requieren una escalada inmediata, por ejemplo, interrupciones de la aplicación, destrucción de datos, violaciones de la privacidad, daños a la reputación de la empresa, etc. Y debe establecer puntos de escalada que identifiquen hacia dónde pasar de la detección de incidentes, al análisis y contención de problemas activos, a los esfuerzos de recuperación, a los análisis forenses posteriores al incidente.

Un gran plan que simplemente se encuentra en el estante esperando que ocurra un incidente seguramente presentará fallos cuando sea demasiado tarde para solucionarlos. Por lo tanto, todas las empresas deben ensayar su plan de manera rutinaria para que cada empleado sepa instintivamente su rol y responsabilidades en caso de riesgo. El análisis forense también es una pieza crucial de la respuesta posterior al incidente: encontrar las brechas en las políticas, la tecnología y el personal que permitieron que ocurriera el incidente para que puedan repararse antes de futuros ataques.

En un mundo de delincuentes cibernéticos cada vez más sofisticados, la industria química presenta un objetivo maduro y rentable. Los líderes de tecnología inteligente construirán estrategias de protección cibernética que combinen la seguridad cibernética con una rigurosa disciplina de respaldo, antimalware conductual habilitado para IA para combatir las amenazas de día cero, capacitación continua sobre conciencia de seguridad y planificación de respuesta a incidentes para reducir su exposición al riesgo y alentar a los ciberdelincuentes a encontrar víctimas más débiles.