THE WHITE HOUSE
WASHINGTON

PARA: Ejecutivos y lideres empresariales

DE: Anne Neuberger, Asistente del Presidente y Asesora Adjunta de Seguridad Nacional para Tecnología Cibernética y Emergente.

ASUNTO: Recomendaciones para protegerse contra las amenazas del *ransomware* o robo de datos.

FECHA: 2 de junio de 2021

La cantidad de incidentes de ransomware o robo de datos, han aumentado significativamente, asimismo el fortalecimiento y protección de nuestra nación frente a los ciberataques, por parte del sector privado como del público, es una de las principales prioridades del Presidente.

El Gobierno Federal, bajo la orden del Presidente Biden, está intensificando sus esfuerzos, trabajando con aliados de todo el mundo para interrumpir y disuadir a los ciberdelicuentes, actores del ransomware. Estos esfuerzos incluyen la desarticulación de las redes de ransomware, mediante la colaboración con socios internacionales para responsabilizar a los países que albergan estos delincuentes de ransomware, así como el desarrollo de políticas cohesivas y coherentes evitando el pago de rescates y contar la posibilidad de rastrear e interceptar rápidamente los ingresos provenientes de pagos por moneda virtual.

El sector privado tiene también una responsabilidad fundamental en la protección contra estas amenazas. Las organizaciones deben reconocer que ninguna empresa está a salvo de ser objetivo del ransomware, independientemente de su tamaño o ubicación. Para ello existen medidas inmediatas que pueden tomar para protegerse así mismas, así como a sus clientes y a la economía en general. Al igual que en los hogares, las casas tienen cerraduras, sistemas de alarma y los edificios de oficinas cuentan guardias y seguridad para protegerlas frente a cualquier amenaza de robo, instamos a que se tomen seriamente el delito de ransomware y asegúrense de contar con ciber protección en sus corporaciones las cuales deben estar a la altura de las amenazas.

Como conclusión de la más reciente oleada de ataques de ransomware a organizaciones estadounidenses, irlandesas, alemanas y en todo el mundo es que, las empresas que priorizan las amenazas del ransomware en sus operaciones comerciales, en lugar considerlo como un simple riesgo de robo de datos, reaccionarán rápidamente y se recuperarán con mayor eficacia. Para comprender mas a fondo del riesgo del que hablamos, los líderes de empresas deben convocar de inmediato a su personal para discutir sobre las amenazas del ransomware y revisar las políticas de seguridad corporativa y los planes de continuidad del negocio con el fin de asegurar que cuentan con la capacidad de continuar o restaurar rápidamente sus operaciones ante un ciberataque.

A continuación encontrarán recomendación del Gobierno de los Estados Unidos sobre las mejores prácticas, seleccionando un número reducido de pasos de que son de gran impacto para ayudar a concentrar los esfuerzos y avanzar rápidamente en la reducción de los riesgos.

Instamos a las siguientes acciones inmediatas:

Implementar las cinco mejores prácticas de la Orden Ejecutiva del Presidente: *La Orden Ejecutiva del Presidente Biden para mejorar la ciberseguridad de la nación* se está aplicando de manera urgente y prioritaria por parte de el Gobierno Federal. Estamos predicando con el ejemplo al ser estas cinco prácticas de alto impacto y por consideradas como la mejor opción: Autenticación de multifactores (las contraseñas por sí solas se ven comprometidas en forma rutinaria), detección y respuesta de puntos finales (para buscar actividad maliciosa en una red y lograr bloquearla), encriptación (en caso que los datos sean robados, sean inutilizables) y un equipo de seguridad capacitado y empoderado (para acatar el problema rápidamente, y así compartir e incorporar información sobre amenazas en sus defensas). Estas prácticas reducirán significativamente con éxito el riesgo de un ciberataque.

Haga copias de seguridad de sus datos, imágenes del sistema y configuraciones, Haga pruebas periódicas y mantenga las copias de seguridad disponibles sin conexión: Asegúrese de que se hagan copias de seguridad periódicamente y sin conexión a la red de la empresa, ya que muchas variantes de ransomware intentan encontrar, cifrar o eliminar las copias de seguridad a las que encuentra accesibles. Mantener las copias de seguridad más recientes sin conexión es fundamental, ya que si los datos de la red se cifran con el ransomware, la organización puede restaurar los sistemas.

Actualice y aplique parches a los sistemas con prontitud: Esto incluye el mantenimiento de la seguridad de los sistemas operativos, las aplicaciones y el firmware, de manera oportuna. Tenga en consideración la posibilidad de utilizar un sistema de gestión de parches centralizado; utilice una estrategia basa en la evaluación del riesgo para dirigir su programa de gestión de parches.

Ponga a prueba su plan de respuesta ante incidentes: No hay nada más revelador cuando hay carencias de los planes que ponerlos a prueba. Analice algunas preguntas básicas y utilícelas para elaborar un plan de respuesta a incidentes: ¿Es capaz de mantener las operaciones comerciales sin acceso a determinados sistemas? ¿Durante cuánto tiempo? ¿Apagaría sus procesos operativos si los sistemas de la empresa tales como la facturación, estuvieran desconectados de red?

Compruebe el trabajo de su equipo de seguridad: Utilice un "pen tester" de terceros para comprobar la seguridad de sus sistemas y su capacidad para defenderse de un ataque sofisticado. Muchos delincuentes de ransomware son agresivos y sofisticados, así que encontrarán el equivalente de lo que puede ser una puerta sin candado.

Segmente sus redes: Se ha producido recientemente un cambio en la forma en que se hacen los ataques mediante ransomware. Estos han pasado de robar datos a interrumpir las operaciones. Es de gran importancia que sus procesos corporativos y las operaciones de fabricación/producción se encuentren separadas, además de que filtre y limite cuidadosamente el acceso a Internet desde las redes operativas. Identifique los enlaces entre estas redes y desarrolle soluciones o controles manuales para garantizar que las redes ICS puedan aislarse y continúen funcionando sin que su red corporativa se vea afectada. Compruebe de manera periódica planes de contingencia, tales como los controles manuales, para que pueda mantenerse la seguridad de las funciones críticas durante un ciberataque.

Los ataques de ransomware han afectado las operaciones de las organizaciones a nivel global, desde hospitales en Irlanda, Alemania y Francia, hasta oleoductos en Los Estados Unidos y bancos en el Reino Unido. Los instamos a tomar estas importantes medidas para la protección de sus organizaciones y a la población. El Gobierno de Los Estados Unidos está trabajando conjuntamente con países de todo el mundo para frenar y castigar a los ciber-delincuentes del ransomware y a los países que los albergan, pero no podemos luchar solos contra la amenaza que esto presenta. El sector privado es clave y tiene una gran responsabilidad en ello. El Gobierno Federal está preparado para ayudarle a aplicar estas mejores prácticas.

Recursos Adicionales:

FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation’s Cybersecurity and Protect Federal Government Networks

CISA - RANSOMWARE GUIDANCE AND RESOURCES