Centro de Periodismo Investigativo | (http://periodismoinvestigativo.com/2017/03/ataque-cibernetico-pone-en-evidencia-el-precario-sistema-de-seguridad-en-el-gobierno/)

ACTUALIDAD

Ataque cibernético pone en evidencia el precario sistema de seguridad en el gobierno

Dos semanas después del incidente que le costó al gobierno al menos $200,000, todavía no se han identificado los responsables.

por **Damaris Suárez** | 17 de Marzo 2017

Foto por andrewfhart via Visual Hunt / CC BY-SA

El gobierno no podrá ofrecer servicios en línea de forma eficiente mientras carezca de una política pública integral de tecnología, y el ataque cibernético que afectó la pasada semana al sistema electrónico del Departamento de Hacienda es prueba de ello, según tres expertos en tecnología consultados por el Centro de Periodismo Investigativo.

La falta de controles de seguridad y el uso de sistemas operativos obsoletos en esa agencia podrían parte de la razón por la que intrusos lograron acceso al sistema en el ataque que dejó inoperante su página web.

El gobierno ya tiene un informe preliminar sobre lo ocurrido el lunes, 6 de marzo y recomendaciones sobre la implementación de un sistema de seguridad específico para Microsoft, preparado por los mismos especialistas de esta compañía. Ese informe no entra en el aspecto forense del ataque pirata, explicó Luis Arocho González, Principal Oficial de Información del gobierno (conocido por sus siglas en inglés, CIO), quien además indicó que espera un segundo informe por especialistas en tecnología cibernética de la empresa CompSec Direct, con los detalles del origen y los posibles responsables del ataque pirata, el cual será entregado al FBI.

De acuerdo al funcionario, la falla del sistema surgió por la falta de una política de seguridad cibernética adecuada en la agencia, la principal responsable de recaudar las contribuciones de los ciudadanos.

“Los especialistas en tecnología cibernética nos han solicitado más tiempo para entregar la parte investigativa de la posible procedencia del ataque y la evidencia que se sometería a las

autoridades federales que esperamos esté saliendo durante el fin de semana o para inicios de la próxima", confirmó. No se ha cuantificado el costo del ataque pirata, pero la inversión preliminar del gobierno para normalizar el sistema según Arocho ronda los $200,000. Para mitigar el ataque, el gobierno contrató CompSec Direct, con base en Washington, que ha ofrecido servicios al Departamento de la Defensa de EE.UU.. Se integraron también a la investigación funcionarios de Hacienda, la Unidad de Crímenes Cibernéticos del FBI, y la Enterprise Incident Response, unidad élite de respuestas cibernéticas de Microsoft.

El sistema se restableció el pasado sábado -cinco días después del ataque-, pero el gobierno dejó de ingresar en recaudos unos $25 a $30 millones diarios durante una semana debido a que no se pudieron radicar planillas, confirmó el secretario de Hacienda, Raúl Maldonado, quien añadió que espera recuperar los recaudos esta semana.

"La seguridad en Hacienda estaba deficiente. Logran entrar porque había una contraseña básicamente como viene del manufacturero. No hay una política de seguridad ni controles establecidos. La operación en general no estaba a acorde con las mejores prácticas de seguridad", dijo Arocho.

El funcionario admitió al Centro de Periodismo Investigativo que las configuraciones utilizadas por la agencia no se ajustan a las que son sugeridas por los parámetros de óptima seguridad del National Institute of Standards and Technology (NIST) (https://www.nist.gov/topics/cybersecurity) del gobierno de Estados Unidos, y el Center for Internet Security, entre otras entidades. Mencionó que existen sobre 500 máquinas en la agencia con sistemas operativos que se consideran obsoletos por el manufacturero, y que por esta razón se han sacado del mercado, como Windows XP, Windows 2000 y servidores con Windows 2003.

En el caso del Departamento de Hacienda son varios los suplidores responsables de ofrecer la seguridad de los sistemas pero, Arocho aclaró que no han tomado la decisión de responsabilizarlos por el ataque cibernético. "No hemos llegado a eso", dijo.

Todo apunta a un trabajo interno: federales investigan

Arocho mencionó que originalmente se creyó que se trataba de un 'ransomware', que es un virus que encripta o toma de rehén los archivos para solicitar una recompensa. No obstante, los especialistas se percataron de que se habían borrado datos de los servidores que tienen los discos que hacen resguardo a los sistemas Windows de la agencia, lo que no ocurre con el virus *ransomware*. De acuerdo al funcionario, en ese momento se tomó la determinación de iniciar una pesquisa criminal forense para precisar la identidad y el motivo de los autores del ataque, pues no se descarta que los piratas hayan tenido la intención criminal de borrar datos del Departamento de Hacienda.

"El objetivo pudo ser hacer daño en tiempos de planillas. Puedo pensar que lo hacen para evitar que pudiéramos recuperar el sistema. Quizá el 'ransomware' fue una distracción y el objetivo final fuese borrar data (sic)", sostuvo. Los piratas solicitaban 22 criptomonedas por cada una de las 682 computadoras infectadas, lo que llevaba a $16.8 millones la cifra, según Hacienda.

Por su parte, Carlos Osorio, portavoz del FBI señaló que la intervención de la Unidad de Crímenes Cibernéticos se encamina a levantar evidencia sobre los responsables del ataque, que podría terminar en un pliego acusatorio, independientemente de la investigación que realiza el gobierno. Se negó a precisar cuándo podrían culminar la pesquisa federal. "Cuando entramos en una investigación entramos para radicar cargos si entendemos necesario", puntualizó.

De acuerdo a Arocho, el responsable de proteger los datos y mantener una seguridad óptima del sistema es el dueño de la información, en este caso el Departamento de Hacienda.

Los sistemas de informática de esa agencia son monitoreados por el área de Tecnología de Información, que tiene una División de seguridad interna, y consultores externos. La empresa Microsoft ofrece servicios de monitoreo y seguimiento a sus propios sistemas; mientras que

la empresa Evertec ofrece servicios de monitoreo y seguridad a otros sistemas de la agencia, explicó en una escueta declaración escrita la Oficial de Comunicaciones de Hacienda, Kiara Hernández González.

La pasada semana el secretario Maldonado confirmó que fueron suspendidos varios empleados que no siguieron los protocolos de seguridad. Maldonado admitió que la agencia fue laxa en el manejo de las contraseñas de los sistemas de información.

Relacionó el ataque pirata con un proceso de revisión de los sistemas en el que, como parte de la colaboración de la agencia con una investigación del FBI sobre presunto fraude en el área de licencias, dos empleados de área de Rentas Internas fueron arrestados la pasada semana (http://elvocero.com/identifican-a-empleados-de-hacienda-arrestados-por-el-fbi/) .

“Se le quitó el acceso al sistema a un grupo de empleados debido a una investigación interna. Me levantó bandera por una cuestión operacional en la que los accesos al sistema en años anteriores (los tenía) personal de poca experiencia”, admitió Maldonado al CPI.

Por su parte, el CIO del gobierno anticipó que referirá el informe final al secretario de Hacienda y al gobernador Ricardo Rosselló, que incluirá medidas de seguridad y un plan de acción correctivo para mitigar los daños y corregir la fragilidad de los sistemas.

Manga por hombro la seguridad en los sistemas del gobierno

Las redes que tienen equipos que cumplen con las normativas para gobierno cuentan con la capacidad de habilitar servicios óptimos de seguridad pero, es imprescindible la educación de los usuarios, en este caso, los empleados públicos, y la responsabilidad de la administración del sistema, explicó Carlos Bouche, CIO de Mantis Corporation, empresa dedicada a la informática, automatización y mantenimiento de sistemas y seguridad.

“Al instalar un servidor tú le puedes decir que obligue al usuario a un cambio de la contraseña inicialmente y cada cierto tiempo. Una vez está configurado, lo puede hacer automáticamente. Hay que forzar las políticas de seguridad y reforzarlas para que se utilicen”, sostuvo.

Bouche criticó que no haya un sistema centralizado para minimizar los riesgos en distintos niveles de seguridad, ya que solo una parte que esté insegura pone en riesgo todo el sistema.

De acuerdo a las estadísticas recopiladas por la empresa global de investigaciones y expertos en seguridad cibernética Kroll Advisory Solutions (http://www.kroll.com/en-us/cyber-security/data-breach-prevention/cyber-risk-assessments/data-security-statistics) , el 31% de los ataques cibernéticos son producto de la negligencia de los empleados, mientras que el 25% de las organizaciones identifican como la causa errores o fallas en los sistemas.

“El proyecto de seguridad para prevenir ataques desde la Red Interagencial del gobierno quedó paralizado y en el 2016 lo que se entregó en transición fue una red muy vulnerable”, confirmó el pasado Principal Oficial de Información del gobierno, Giancarlo González, quien opinó además que del 2013 al 2016 el deterioro en la visión y soporte a nivel central ha sido notable.

En el 2013, bajo el mandato de la oficina del CIO, Giancarlo González, existía un sub-director cuyo rol incluía velar por la seguridad de la red. Se había creado además, un comité de seguridad de informática compuesto por los jefes de tecnología de diversas agencias, entre ellas Hacienda, BGF, DTOP y un designado de Homeland Security. Estos esfuerzos se detuvieron al ser desmantelada la oficina en el 2015, aseguró el exfuncionario.

Para Arocho, el gobierno históricamente ha fallado al minimizar la posición del Principal Oficial de Información, que es el responsable de establecer y asegurar que se cumpla con una política pública adecuada sobre los sistemas de información.

“Olvídate de innovación; necesitamos una arquitectura de manejo de la información en los

sistemas del gobierno holística. El gobierno carece de una política integral de tecnología. El CIO debería tener más poderes de 'enforcement' y de establecer políticas y procedimientos que sean seguidos en todas las agencias y corporaciones", opinó Gabriel Pagán, consultor independiente de infraestructura de tecnologías de información.

Arocho mencionó que no fue hasta que se dio este ataque cibernético que se determinó crear el Oficial de Seguridad Cibernética, posición que existe en todas las jurisdicciones de los Estados Unidos para asegurarse que se cumple con los estándares de seguridad necesarios para los servicios públicos que se ofrecen en línea.

Indicó que existe un proyecto de ley para crear una nueva agencia que estará a cargo de implementar las políticas de seguridad con un modelo tomado de la experiencia del US Digital Service y otros establecidos en Reino Unido.

También aclaró que la red de Hacienda está compuesta por muchos sistemas y aplicaciones, y que los datos de contribuyentes están en un sistema independiente por lo que no se comprometieron con el ataque. "La data (sic) de los contribuyentes no se vio afectada. Eso tiene su propio sistema de seguridad que de detectar una anomalía, puede protegerse", aseguró Arocho. Si hubiese ocurrido, la reglamentación federal obliga que se notifique al usuario de cualquier instancia en la que sus datos se hubieran expuesto tras un ataque cibernético, explicó la Lcda. Julizzette Colón de la firma de consultoría de inteligencia social Monitor SN.

La abogada indicó que aunque cada jurisdicción maneja sus políticas de seguridad, y que existen unos requisitos básicos utilizados por el gobierno federal (https://www.digitalgov.gov/resources/checklist-of-requirements-for-federal-digital-services/) para las páginas web y servicios en línea.

Ataques cibernéticos de Hacienda y CRIM no están relacionados

El llamado 'ransomware' sí mantuvo fuera de operaciones el portal del Centro para la Recaudación de Ingresos Municipales (CRIM). Ambos ataques, aunque simultáneos, alegadamente no están relacionados, indicó Arocho, quien también destacó que en el CRIM había un mejor nivel de seguridad de los sistemas y un método de resguardo más eficiente que Hacienda, lo que minimizó el impacto del ataque.

El alcalde de Cidra y presidente del CRIM, Javier Carrasquillo, señaló que el ataque en esa agencia se considera externo, que se normalizó el sistema más rápido que en Hacienda y que no estuvo en riesgo la información de los usuarios.

"Debemos concluir que fue una casualidad. No están relacionados porque es muy diferente a lo ocurrido en Hacienda. Sí se presume que es intencional, pero no un ataque interno. Nos ayudó que estábamos en el proceso de actualizar la plataforma de seguridad a un sistema más avanzado conocido como Palo Alto Networks y al reconocer el ataque, el sistema pudo identificar el virus y aunque había afectado la funcionalidad, fue aislando y desechando la data (sic) encriptada y subió la que tenía en resguardo", explicó el presidente del CRIM.

El CRIM tiene una División de Sistemas para establecer los procedimientos de seguridad para la plataforma. Carrasquillo dijo que desde esa oficina la agencia mantiene monitoreo continuo del sistema, lo que permitió identificar el virus a tiempo. Indicó que se bloquearon los accesos en la República de China y en Rusia, desde donde se identificó 'alta actividad sospechosa' y se cree que se pudo haber originado el ataque.