CAJA COSTARRICENSE DE SEGURO SOCIAL
Auditoría Interna
Teléfono: 2539-0821 ext. 2000-7468
Correo electrónico: auditoria_interna@ccss.sa.cr

AS-AATIC-155-2022
19 de julio de 2022

Ingeniero
Esteban Zúñiga Chacón, jefe
Centro de Gestión Informática
GERENCIA MÉDICA - 2901

Ingeniero
Alexánder Solís Abarca, jefe
Centro de Gestión Informática
GERENCIA FINANCIERA - 1103

Ingeniera
Guiselle Tenorio Chacón, jefe
Centro de Gestión Informática
GERENCIA ADMINISTRATIVA - 1104

Ingeniero
Giovanni Campos Alvarado, jefe
Centro de Gestión Informática
GERENCIA DE INFRAESTRUCTURA Y TECNOLOGÍAS- 1107

Ingeniero
Roy Ovares Valerio, jefe
Centro de Gestión Informática
GERENCIA DE LOGÍSTICA - 1106

Ingeniero
Marco Vinicio González Jiménez, jefe.
Centro de Gestión Informática
GERENCIA DE PENSIONES - 9108

Máster
Idannia Mata Serrano, subgerente a.i.
DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES – 1150

Estimados(as) señores(as):

ASUNTO:	**Oficio de Asesoría relacionado con amenazas generadas por el ransomware DeadBolt que afecta los almacenamientos en dispositivos NAS.**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2022 y con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno específicamente en su rol de asesor, esta Auditoría informa sobre las amenazas generadas por el ransomware DeadBolt que afecta los almacenamientos en dispositivo NAS (Network-Attached Storage), con el fin de que se implementen acciones preventivas, y evitar la materialización de riesgos en materia de Ciberseguridad, una vez que se normalicen las operaciones en la Institución y entre en funcionamiento la plataforma tecnológica de la Caja.

Al respecto, DeadBolt es un ransomware que afecta dispositivos de almacenamiento NAS, especialmente los de la marca QNAP, utilizando problemas de vulnerabilidad para cifrar los datos almacenados, ocurriendo de inmediato y no permitiendo a los usuarios evitar el proceso y guardar los archivos con un cifrado fuerte. Una vez distribuido, el virus secuestra la pantalla de inicio de sesión donde se presenta una nota de rescate y exige así a las víctimas que paguen por el descifrado de los archivos impidiendo; además, que los usuarios afectados vayan a cualquier lugar más allá de la pantalla de registro para acceder a su página de administración.

Este ransomware asigna una extensión "deadbolt" a todos los archivos afectados dentro del sistema, convirtiéndolo totalmente inaccesibles, por lo que los ciberdelincuentes chantajean a las víctimas para que realicen un pago a cambio de la clave que permite desencriptar los archivos vulnerados, esta clave es única por lo que vuelve el proceso de descifrado más complejo.

Por lo anterior, los expertos en esta temática han emitido recomendaciones generales para contrarrestar las posibilidades de que se materialicen vulnerabilidades mediante este mecanismo, entre las cuales se encuentran:

- Disponer de un software especial anti-ransomware que permita la recuperación automática de archivos, protección de sobreescritura que recupera instantánea y automáticamente cualquier archivo cifrado, protección de archivos que detecta y bloquea incluso cifradores desconocidos
- Efectuar copias de seguridad en línea considerando que los almacenamientos locales como SSD, discos duros, unidades flash pueden infectarse instantáneamente con el virus una vez presenten alguna conexión con la red.
- Informar constantemente a los usuarios de no abrir correos, no deseados y protegerse del phishing, ya que estos mecanismos son los más utilizados por los cibercriminales para la distribución de ransomware.
- Actualizar a la última versión del sistema operativo del servidor NAS.
- Desactivar la gestión remota del servidor NAS, para garantizar la seguridad del dispositivo.

En este sentido, esta Auditoría informa sobre lo descrito con el objetivo de que se analice la información expuesta y se refuercen los mecanismos de ciberseguridad de considerarse la posible materialización de riesgos, una vez que se hayan reestablecido los servicios tecnológicos institucionales.

Lo anterior, en apego a lo indicado en las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, que establecen dentro de los procesos del marco de gestión de TI, lo correspondiente a la "Seguridad y Ciberseguridad", a saber:

> *"XI. SEGURIDAD Y CIBERSEGURIDAD*
>
> *La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados.*
>
> *La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información (…).*
>
> *Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución.*

La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información (…)".

En virtud de lo expuesto, se da conocer la información descrita, con el propósito de que sea sometida a valoración y revisión por esa Administración y así coadyuvar al cumplimiento de los objetivos institucionales, garantizando un marco adecuado para el resguardo de la información institucional y de la seguridad informática, así como de la continuidad en la prestación de los servicios.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.19 15:57:54 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/LDP/lbc

C. Auditoría