GOBIERNO DE PUERTO RICO
CORPORACIÓN PÚBLICA PARA LA SUPERVISIÓN Y SEGURO DE COOPERATIVAS DE PUERTO RICO
Presidenta Ejecutiva Mabel Jiménez Miranda, MBA mjimenez@cossec.pr.gov

21 de febrero de 2024

CARTA CIRCULAR NÚM. 2024-02

A LAS COOPERATIVAS DE AHORRO Y CRÉDITO

Mabel Jiménez Miranda, MBA
Presidenta Ejecutiva

EVALUACIONES Y PRUEBAS DE SEGURIDAD CIBERNÉTICA

El Sector de Ahorro y Crédito del Sistema Cooperativo es pieza fundamental en el crecimiento sostenido de la economía puertorriqueña ya que garantiza el acceso a servicios financieros competitivos a todos los segmentos de nuestra sociedad. La integración de los sistemas de información al ofrecimiento de servicios financieros requiere estar vigilantes a los cambios tecnológicos, así como los retos inherentes a hacer negocios en estos ambientes. En los últimos años las cooperativas han incrementado el uso de los sistemas de información para efectuar sus operaciones principales y ofrecer servicios esenciales a la ciudadanía. Esto ha aumentado el riesgo y los eventos relacionados con ataques cibernéticos que afectan su infraestructura tecnológica e información crítica.

Como bien sabemos, los ataques cibernéticos tienen el propósito de acceder, modificar, destruir o apropiarse de la información. También se utiliza para interrumpir la continuidad de las operaciones de una entidad, entre otras. Las amenazas cibernéticas representan un reto de gran importancia para todos, por lo que es fundamental que se implementen las medidas de seguridad necesarias para proteger la infraestructura e información confidencial, tanto de los socios como de las mismas entidades. Además de que los ataques cibernéticos pueden afectar la confidencialidad, la integridad y la disponibilidad de la información; estos pueden ocasionar pérdidas económicas, afectar la reputación de las entidades y la confianza y la credibilidad que tienen los ciudadanos en estas.

El Artículo 7 (e) de la Ley Núm. 114-2001, según enmendada, "*Ley de la Corporación Pública para la Supervisión y Seguro de Cooperativas de Puerto Rico*", faculta a la Junta de Directores de la Corporación a adoptar medidas preventivas para reducir el potencial de pérdidas de las cooperativas.

Cónsono con ello, y basado en la necesidad de priorizar la atención a la seguridad cibernética en las cooperativas de ahorro y crédito para mitigar eventos que puedan ocasionar pérdidas de todo tipo, les requerimos que conduzcan las siguientes evaluaciones y pruebas de seguridad cibernética:

1. Escaneo de vulnerabilidades para evaluar el "estado de salud" de los dispositivos tecnológicos accesibles a través del internet. Incluye procedimientos de escaneo de vulnerabilidades y evaluación de la presencia de las mejores prácticas de seguridad en las plataformas web y correo electrónico.

2. Simulación de "Phishing" para medir la propensión de los usuarios de hacer "clic" en señuelos de "phishing" por correo electrónico, que se utilizan comúnmente por los cibercriminales para recopilar información confidencial o para obtener acceso a una red.

3. Evaluación de riesgos y vulnerabilidades donde combina información de vulnerabilidades y cibernéticas identificadas a nivel nacional, con datos recopilados en la configuración tecnológica de la cooperativa para proporcionar informes de análisis de riesgo con recomendaciones de remediación priorizadas por nivel de gravedad y riesgo. Las evaluaciones podrán incluir, pero sin limitarse a, lo siguiente:

    - Pruebas de penetración de aplicaciones, sistemas y redes.
    - Revisión y análisis de la configuración tecnológica de la institución (sistema operativo y bases de datos) y comparación con los estándares, pautas y mejores prácticas de la industria para identificar problemas de seguridad.

4. Evaluación integral del entorno tecnológico (personas, procesos, tecnologías responsables de proteger la red y los sistemas de información de la institución) para brindar información sobre la postura de ciberseguridad y capacitación práctica para el personal técnico. La evaluación incluye pruebas de las redes simulando ciberataques donde se obtiene acceso a una red y se permanece sin ser detectado durante un periodo de tiempo prolongado para robar datos.

5. Evaluación del diseño de la arquitectura tecnológica basada en los estándares, pautas y mejores prácticas establecidas en el gobierno federal e industria. La evaluación podrá incluir:

    - Revisión del diseño de la arquitectura tecnológica y su interconectividad con sistemas internos y externos para enfocarse en estrategias defensivas.
    - Revisión detallada de la configuración y actividad del sistema para determinar la susceptibilidad a posibles ataques y anomalías.

- Análisis del tráfico de la red utilizando una combinación de herramientas para identificar comunicaciones anómalas que podrían indicar una actividad sospechosa o una mala configuración.

6. Ejecución de pruebas de penetración remotas para evaluar e identificar vulnerabilidades y establecer curso de acción para eliminar rutas explotables. Estas pruebas se enfocan en los sistemas accesibles externamente. Las pruebas podrán incluir:

    - Verificación de si la red es accesible desde el dominio público por un usuario no autorizado. Estas pruebas deben incluir la evaluación de puertos abiertos, protocolos y servicios.
    - Evaluaciones de aplicaciones web para identificar posibles vulnerabilidades explotables.
    - Pruebas de vectores de ataques originados por correo electrónico.

La Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos (CISA, por sus siglas en inglés), adscrita al Departamento de Seguridad Nacional ("Department of Homeland Security"), ofrece estos servicios libres de costos a las entidades que así lo soliciten. Para coordinar los servicios deberán enviar correo electrónico al CSA de la Región 2 asignado a Puerto Rico y USVI a; ngai.oliveras@cisa.dhs.gov . Para su beneficio se adjunta presentación de la Agencia de Seguridad de infraestructura y Ciberseguridad (CISA).

Las cooperativas tendrán hasta el 31 de marzo de 2024, para coordinar las evaluaciones y pruebas de seguridad, así como remitir a la Corporación evidencia del registro o inscripción con la Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos o de cualquier otro proveedor de su predilección al correo electrónico: ciberseguridad@cossec.pr.gov. Los informes de estas evaluaciones y pruebas de seguridad serán revisados por nuestros examinadores de sistema de información como parte del examen que realiza la Corporación. En caso de que la cooperativa cuente con los servicios de un tercero, deberá el proveedor presentar una certificación donde establezca que cumple con los requerimientos antes esbozados.

De tener alguna pregunta sobre lo antes expuesto, pueden comunicarse con en el Área de Apoyo Técnico y Supervisión.