COSSEC
CORPORACIÓN PÚBLICA PARA LA SUPERVISIÓN
Y SEGURO DE COOPERATIVAS DE PUERTO RICO
ESTADO LIBRE ASOCIADO DE PUERTO RICO

12 de febrero de 2014

CARTA INFORMATIVA 2014-03

A TODAS LAS COOPERATIVAS DE AHORRO Y CRÉDITO

Daniel Rodríguez Collazo
Presidente Ejecutivo

EVALUACIÓN DE LA INFRAESTRUCTURA PARA LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

La Corporación Pública para la Supervisión y Seguro de Cooperativas de Puerto Rico (COSSEC) es el organismo regulador de las cooperativas y asegurador del sector de ahorro y crédito. Como parte de los requisitos del seguro de acciones y depósitos, las cooperativas de ahorro y crédito deben poseer sistemas de información mecanizados, con los cuales puedan llevar a cabo sus operaciones. Con relación a este requisito, los sistemas deben ser efectivos, contar con una buena estructura de seguridad y controles internos, entre otros aspectos. Esto le permitirá operar eficientemente y salvaguardar la información de sus socios y depositantes.

Recientemente, hemos observado como instituciones de alcance global han emitido alertas debido a la detección de esquemas conducentes a lograr corromper las operaciones de estas instituciones. Además, hemos observado como proveedores de Sistemas de Información han emitido comunicados exponiendo situaciones y vulnerabilidades que lamentablemente han ocurrido, y que son objeto de evaluación e implementación de medidas correctivas por parte de las cooperativas.

COSSEC en su rol de asegurador y regulador de las Cooperativas de Ahorro y Crédito de Puerto Rico, consiente de los riesgos que conlleva la operación de los sistemas de información, recomienda que inmediatamente todas las cooperativas de ahorro y crédito realicen una evaluación detallada de la seguridad y controles internos de sus sistemas de información. Esta evaluación debe incluir todos los puntos de acceso vulnerables del sistema. Deben enfatizar en aquellos que exponen los sistemas, tales como: redes, plataformas tecnológicas y servicios externos.

Las cooperativas de ahorro y crédito para poder llevar a cabo una evaluación adecuada de sus sistemas de información, como mínimo, deben establecer de manera inmediata un Plan de Trabajo que incluya la revisión minuciosa de las siguientes áreas:

1. Establecer Políticas y Procedimientos para la administración adecuada de los Sistemas de Información. Estos deberán ser cónsonos con las tecnologías y operaciones existentes en las cooperativas.

2. Aquellas cooperativas que ofrecen a sus socios los productos de tarjetas de crédito y débito, las transacciones con éstas deben estar en conformidad con la PCI ("Payment Card Industry").

3. Implementar los algoritmos y protocolos seguros, así como certificados digitales que ofrezcan las máximas seguridades en las páginas web.

4. Realizar una evaluación que identifique los riesgos derivados de sus operaciones de los sistemas de información y de esta manera puedan actualizar sus pólizas de seguro.

5. Realizar una revisión de toda su infraestructura de comunicaciones y datos. Esta evaluación tendrá el propósito de identificar los riesgos y vulnerabilidades de la infraestructura. Debe ser llevado a cabo por un proveedor externo, debidamente cualificado, y solicitar a éste que realice una prueba de penetración de su infraestructura de comunicaciones. Recomendamos que esta prueba la realicen anualmente.

6. Establecer controles formales para proteger la información contenida en documentos, medios de almacenamiento, otros dispositivos externos y el intercambio electrónico de datos. Estos controles deben evitar daños, robos, accesos indebidos, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de todo su personal, sus proveedores y personas externas a la Institución.

7. Establecer procedimientos que garanticen la Seguridad de los Sistemas de Información en las conexiones remotas. No deberán mantener una conexión remota sin supervisión y seguridad adecuada. Toda conexión remota deberá estar debidamente autorizada y justificada por la Administración.

   Además, toda conexión remota deberá contar con un registro de actividad ("Audit Trail") que evidencie los elementos que describen la conexión.

8. Las Cooperativas que ofrezcan a sus socios productos de Tarjetas de Débito y/o Crédito, deberán establecer internamente o requerir a sus proveedores o intermediarios, un Sistema de Prevención y Detección de transacciones fraudulentas que detecte, oportunamente, cargos que no concuerden con el perfil habitual del socio.

9. Evaluar con sus proveedores o intermediarios, técnicas o mecanismos que aumenten la seguridad de las tarjetas (plásticos), a los fines de minimizar el riesgo de clonación de tarjetas.

10. Exigir a sus proveedores o programadores una evaluación de seguridad de los sistemas o plataformas utilizadas para que los socios accedan su cuenta desde el Internet. Las Cooperativas deben mantener una seguridad adecuada y actualizada en estos sistemas.

11. Establecer medidas que garanticen que reciban los Boletines o Alertas de Seguridad de todos los programas o equipos ("Software" and "Hardware") que componen la plataforma tecnológica de la Cooperativa. El personal de Sistemas de Información de la Institución y sus proveedores deben analizar estos boletines.

    Los Boletines de Seguridad son un medio de comunicación por el cual los fabricantes de los equipos y programas comunican a sus clientes o usuarios alertas o correcciones que deben ser atendidas con relación a sus respectivos productos.

12. Evaluar la posibilidad de no aceptar por sus Sistemas de Información transacciones provenientes de países extranjeros los cuales mantengan sanciones impuestas por el Gobierno Federal y la Agencia OFAC. La evaluación e implementación de esta medida, deberá ser evaluada en conjunto a sus asesores de cumplimiento y proveedores o programadores encargados del producto de Alertas de Transacciones Sospechosas.

13. Mantener un Sistema de Antivirus y Antimalware de uso comercial que garantice la Seguridad de los Sistemas de Información. Todas las estaciones de trabajo y demás dispositivos que compartan, reciban, accedan o transmitan información electrónica de la cooperativa, deberán contar con protección de antivirus. Este programa debe ser actualizado constantemente.

14. Establecer Políticas de Contraseñas que garanticen el estándar mínimo que deberán tener las contraseñas de los Sistemas de Información de la cooperativa.

15. Exigir a sus proveedores una revisión de seguridad de los registros de auditoría "Audit Trail" o "Log Events" de sus Sistemas de Información y que establezcan las medidas de seguridad adecuadas que garanticen que estos registros no puedan ser manipulados o eliminados.

16. Establecer mecanismos de seguridad para el manejo de data que puedan portarla sin autorización.

17. Revisar todas las reglas de seguridad de los "firewalls" a los fines de contar con mecanismos de seguridad de prevención y detección adecuados, acorde con los riesgos y vulnerabilidades que envuelven la operación de Sistemas de Información.

18. Contar con las condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de información.

19. Establecer mecanismos de alerta y detección de intrusos o actividades sospechosas en la infraestructura de comunicaciones y datos.

20. Exigir a sus proveedores de Sistemas de Información Primarios que todo cambio de parámetro requiera una clave de acceso. Además, estos cambios deberán quedar registrados en los Registros de Auditorías como mínimo con los siguientes elementos:

    a. Usuario que realizó el cambio
    b. Fecha del cambio
    c. Hora del cambio
    d. Descripción del cambio
    e. Valor antes del cambio
    f. Valor luego del cambio
    g. Programa utilizado
    h. Campo modificado

21. Establecer controles de acceso restrictos al Internet.

22. Exigir a sus proveedores de Sistemas de Información Primarios una Auditoría de Controles Internos en conformidad con el SSAE16. [1]

[1] SAEE 16 - Es una norma de auditoría diseñado para permitir a un auditor independiente evaluar y emitir una opinión sobre los controles de una organización de servicio.

23. Solicitar a todo proveedor que realice servicios en el Área de Sistemas de Información, una Póliza de Errores y Omisión en el Desempeño de sus Funciones según el volumen de negocio de la Institución procesado a través del Sistema de Información. Las cooperativas deben asegurar que la Póliza endosada sea única e intransferible a su cooperativa.

24. Las cooperativas de ahorro y crédito que ofrecen a sus socios el producto de Transferencias Electrónicas (ACH), deberán cumplir con las disposiciones de NACHA para esta operación según han indicado en su publicación anual. Además, deberán llevar a cabo una Auditoría Anual en el área de ACH conforme las disposiciones de NACHA, entre otros aspectos exigidos por estos.

25. Exigir a sus proveedores de Sistemas de Información Primarios un *"Software Escrow Agreement"*. Este acuerdo requiere que los Códigos Fuentes e instrucciones para operar y ejecutar el programa sean depositados o custodiados por un tercero independiente. Esto mediante un acuerdo formal pactado. Esto les garantizará que en caso de que el Proveedor no pueda continuar ofreciendo los servicios de programación por las razones pactadas, la cooperativa pueda obtener los códigos fuentes. Deben asegurarse que las versiones del programa estén actualizas, para así poder continuar sus operaciones y servicios.

26. Establecer protocolos de autenticación multi-factor para los accesos al *Home Banking*. Estos son protocolos que complementan la seguridad primaria compuesta por "user name" y contraseña.

27. Establecer en el *Home Banking* un tiempo máximo de inactividad, después del cual deberá ser cancelada la sesión y exigir un nuevo proceso de autenticación al Socio para acceder de nuevo al Sistema.

28. Considerar la posibilidad de reducir el número de intentos fallidos para entrar al Sistema.

29. Revisar los informes diarios de los límites de tarjetas para que se aseguren que no exceden el valor otorgado.

30. Supervisar la actividad de transacción para identificar cualquier actividad inusual. Por ejemplo, múltiples transacciones en una sola cuenta más allá del límite de transacciones diarias.

31. Asegúrese de que todos los proveedores o entidades involucradas que ofrecen servicios en el área de sistemas de información estén conscientes de las responsabilidades que tienen con la cooperativa.

32. Mantener un plan de respuesta a incidentes durante un ataque contra el sistema.

33. Establecer la Administración de Actualización "Patch Management" dirigida a la estrategia para la gestión de actualizaciones para las aplicaciones y tecnologías de "software" y equipos "hardware", el cual ayude a manejar estos cambios de manera eficiente. Las actualizaciones a menudo son necesarias con el fin de solucionar los problemas existentes que se observan después de la instalación en su versión inicial y en su mayoría tienen que ver con la seguridad.