Modelo de Ciberseguridad Corporativa en el Sistema Bancario

Jonathan Wilmer Magne Quispe
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
jwmagneq@gmail.com

***Resumen*—El presente trabajo de investigación tiene como objetivo, detallar los puntos que son necesarios para llevar a cabo un modelo de ciberseguridad dentro del sistema bancario.**

Palabras clave— ciberseguridad; sistema bancario; modelo.

I. INTRODUCCIÓN

Estamos en una era digital, pero la consideración del impacto de la digitalización está rezagada en algunas áreas. Lo cual está contribuyendo a un problema económico y de seguridad mundial.

La seguridad de la información abarca las medidas y actividades que intentan proteger los activos de información que tienen valor para una organización, mediante la reducción de riesgos y mitigando amenazas posibles. Estos activos se pueden encontrar en diferentes formatos, por ejemplo, en formato digital, de forma física o en forma de ideas o conocimientos de personas que pertenecen a la organización. La seguridad de la información es el paraguas que abarca el resto de las disciplinas, la protección de la información es el libro y la ciberseguridad es un capítulo dentro de ese libro.

La Ciberseguridad tiene como foco principal la protección de la información digital de los sistemas. Por ello, se puede considerar que está comprendida dentro de la seguridad de la información [1].

Alguna vez, la ciberseguridad pudo haber sido tarea del departamento de TI. Eso hace mucho que dejó de ser el caso. Hoy en día, cada persona que trabaja en una organización debe comprender su función y responsabilidad en la defensa de ciberseguridad de su organización.

La alta gerencia, en particular, debe comprender su importancia y educarse sobre los peligros y las necesidades salvaguardias. Los controles técnicos efectivos y actualizados son esenciales, pero cada vez más empleados, ya sea a sabiendas o sin saberlo, son la causa más frecuente de infracciones de seguridad [2].

Por lo tanto, también pueden ser una defensa clave con la formación y la educación adecuadas. En una era de amenazas invisibles, tanto internas como externas, ¿cómo puede defender su organización y hacerla inexpugnable?

A. Objetivo

Detallar las capas de seguridad que forman parte del modelo de ciberseguridad corporativa en el sistema bancario, para llegar al mismo nos sumergiremos en los diferentes problemas y la realidad de los riesgos de ciberseguridad con los que actualmente convive la Banca en Bolivia, además de ver algún ejemplo ya materializado del mismo.

B. Ciber riesgo

A medida que la empresa se ha digitalizado, esta se volvió vulnerable a una amplia gama nueva amenaza. Esta amenaza es global, pero sigue siendo subestimada. De hecho, trae pérdidas asombrosas a organizaciones año tras año, principalmente debido a causas internas, pero pocos realmente entienden y muchos no sienten responsabilidad por las consecuencias. Se estima que el ciberdelito cuesta a la economía global más de $ 400 mil millones al año [3] y se espera aumentará a 2,1 billones de dólares a nivel mundial [6].

Aunque los impactos del ciberdelito, todos, desde los gobiernos hasta los ciudadanos, son las empresas las que llevan la peor parte el daño; una proporción significativa de los cuales es causado por el robo de propiedad intelectual y espionaje. Aunque el ciberdelito cubre una amplia gama de los delitos perpetrados en línea, del hacktivismo a los delitos sociales, por empresas y servicios financieros el fraude es una de las principales preocupaciones.

El fraude puede tener efectos colaterales como eficiencia y flujo de caja, pero ¿quién está en riesgo y por qué? En general, cuanto mayor sea la organización, más atractiva es el objetivo, pero en verdad, todo el mundo está en riesgo. La amenaza tampoco es puramente externa: según una investigación de IBM, en 2015. El 45% de los ciberataques se llevaron a cabo por parte de personas internas maliciosas (y un asombroso 60% por personas con información privilegiada en general) [5].

Muchos, si no la mayoría de los ataques de ciberfraude ahora comienzan con alguna forma de robo de identidad. Esto significa que, lamentablemente, incluso la fuerza laboral mejor intencionada todavía representa una amenaza significativa para cualquier empresa porque cada uno de sus miembros es un objetivo potencial para los ciberdelincuentes.

Hay básicamente dos objetivos en una organización: datos o sistemas, a través de un software diseñado para socavar sus defensas, infiltrarse en sus sistemas y robar detalles de seguridad o imitar sus empleados, o a través de su gente, por medio de la ingeniería social - engañando a su personal para que entregue voluntariamente ellos el acceso que desean.

Para referenciar este artículo (IEEE):
[N] J. Magne, «Modelo de Ciberseguridad Corporativa en el Sistema Bancario», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 8, pp. 110-114, 2020.

C. Entidad reguladora – ASFI

La Autoridad de Supervisión del Sistema Financiero (ASFI) es una institución de derecho público y de duración indefinida, con personalidad jurídica, patrimonio propio y autonomía de gestión administrativa, financiera, legal y técnica, con jurisdicción, competencia y estructura de alcance nacional, bajo tuición del Ministerio de Economía y Finanzas Públicas y sujeta a control social. El objeto de ASFI es regular, controlar y supervisar los servicios financieros en el marco de la Constitución Política del Estado, la Ley N° 393 de Servicios Financieros y los Decretos Supremos reglamentarios, así como la actividad del mercado de valores, los intermediarios y sus entidades auxiliares [12].

Dentro de esta labor, se tiene la recopilación de normas para servicios financieros, específicamente el Titulo VII, dentro del mismo se tiene que tomar muy en cuenta el Capítulo II: Reglamento para la Gestión de Seguridad de la Información. Donde se tiene las directrices y requisitos mínimos que las entidades de intermediación financiera, empresas de servicios financieros complementarios y sociedades controladoras de grupos financieros deben cumplir para la gestión de seguridad de la información de acuerdo con su naturaleza, tamaño y estructura. Dentro de este Capítulo es necesario tomar muy en cuenta las secciones de la Planificación estratégica, estructura y organización de los recursos de TI, Administración de seguridad de la información, Desarrollo, mantenimiento e implementación de sistemas de información, Gestión de operaciones de tecnología de la información, la gestión de la seguridad en transferencias y transacciones electrónicas, ya que dichas abarcan el área de ciberseguridad dentro de la entidad bancaria.

D. Diversificación de Ataques

En la última década el ciberdelito se ha convertido en una industria completa y sofisticada basada en servicios con suministros, cadenas, modelos de negocio y habilidad especialización; esta es la desventaja del rápido avance tecnológico que hemos disfrutado.

Una de las principales formas en el que los ciberdelincuentes operan es por manipular al personal de una organización; pueden engañarlos sin saberlo descargar malware en los sistemas de la empresa, abriendo a la organización hasta el control criminal, o directamente revelando información. Finalmente, y lo más descaradamente de todo, pueden persuadirlos de realizar instrucciones fraudulentas que creen han sido legítimamente dadas por sus superiores corporativos.

Los ciberdelincuentes son indiscriminados en su uso de canales de comunicación, phishing por correo electrónico, smishing por mensajería SMS, y vishing por voz en el teléfono. Por un lado, echaron su amplia red capturando información usando direcciones de correo electrónico automatizadas o teléfono números, por el otro apuntan funcionarios superiores individuales de la empresa (CFO o CIO), para obtener información confidencial información o convencerlos de transferir dinero fuera de la empresa. Ellos juntan fragmentos de información aparentemente insignificante, que construyen en una compleja imagen de cómo funciona la empresa, permitiéndoles obtener credenciales, abusar de los privilegios de usuario, ingresar a los sistemas o convencer a los empleados de que sus comunicaciones y solicitudes son auténticas. Un nombre o fecha de nacimiento aquí, una contraseña allí, un pequeño fragmento de procedimiento de oficina - cualquier cosa puede convertirse en una pieza completando así un rompecabezas complejo [8].

La ingeniería social es frecuentemente combinada con un ataque de software, por ejemplo, con piratería de correo electrónico, que refuerza su efecto combinado.

Otra ruta de ataque podría ser una grabación automatizada afirmando que tiene una tarjeta de crédito o cuenta bancaria que ha sido comprometido y pidiendo al individuo objetivo proporcionar información personal a través del teclado. Con un número telefónico falsificado de la empresa.

Otro ataque frecuente es un estafador actuando como proveedor de una empresa que solicita algún cambio en su banco y cuenta número. Luego, los pagos futuros por las corporaciones se dirigen a estas cuentas fraudulentas.

Una forma de ingeniería social ampliamente difundida y que puede llegar a ser altamente perjudicial, es el ataque del "presidente falso". Nuevamente, se envían correos electrónicos, esta vez internas desde una cuenta de correo electrónico pirateada, particularmente el de un vicepresidente o gerente para instruir a otro empleado a hacer un pago de la empresa objetivo a un destinatario fraudulento [10].

El esfuerzo y los detalles invertidos en tales ataques no deberían ser subestimados ya que los ciberdelincuentes pueden intercambiar docenas de correos electrónicos con posibles víctimas para convencer ellos de la credibilidad del remitente.

E. Ejemplos del mundo real

El día 22 de octubre del 2018, se identificaron mensajes fraudulentos en la red social Facebook, los cuales suplantaban la identidad del Banco Unión S.A. de Bolivia [12].

Fig. 1. Mensaje fraudulento

Una vez ingresado al enlace proporcionado se mostraba la siguiente pantalla:

Fig. 2. Sitio fraudulento

Donde claramente se observa que la dirección en cuestión del sitio es «https://bancaunion-bo.com», la cual no corresponde al sitio original de Banca por Internet del Banco Unión, ya que esta es: https://uninetplus.bancounion.com.bo.

El objetivo del ataque sería la de robar usuarios y contraseñas de usuarios legítimos del servicio de Banca por Internet del Banco Unión S.A. Este tipo de ataques se conoce como «phishing», y es uno de los ataques con mayor frecuencia debido a su alta tasa de efectividad frente a otro tipo de ataques.

Es importante aclarar que la plataforma de Banca por Internet del Banco Unión cuenta con controles de seguridad basados en Doble Factor de Autenticación, a fin de reducir el impacto en el caso de accesos no autorizados a las cuentas de las personas, sin embargo, los delincuentes articulan sus ataques en diversas fases, por lo que la obtención de usuario y contraseña es necesariamente un primer paso para conseguir sus objetivos.

II. Modelo de ciberseguridad

Si bien las pérdidas derivadas de ciberataques técnicos de tipo software pueden ser graves, tales ataques se mitigan poniendo en su lugar el tipo correcto de capas. Estas capas de seguridad son las siguientes:

A. Estructura de gobierno

La cultura de prevención se basa en una fuerte estructura de gobierno corporativo. Escribir, comunicar y auditar políticas claras, que definen riesgos y proporcionan orientación sobre comportamientos aceptables: es fundamental para mitigar fraude interno y externo.

Establecer un equipo dedicado de ciberseguridad para establecer el marco de ciberseguridad, priorizar sus proyectos y el seguimiento de la implementación es la piedra angular de un programa sólido de prevención del ciberdelito.

Es una buena práctica que este equipo informe a la Junta a través del gerente de seguridad de la información o una función similar, con el fin de elevar la discusión y asegúrese de que la mensajería correcta sea proveniente de todas las posiciones de liderazgo. Toda organización debe tener una política de protección de datos en vigor que identifica los datos que son sensibles y vulnerables a ataque, y cómo y dónde esos datos están almacenados. La política también debe establecer roles y responsabilidades de los propietarios de datos y usuarios. Otros aspectos de esta política pueden incluir parámetros de penetración, pruebas y detección de intrusos. Finalmente, la política debe explicar los planes de remediación y planes de recuperación ante desastres en caso de un ataque exitoso.

B. Cambio de cultura

Crear una cultura donde la responsabilidad de mitigar los riesgos en torno al ciberdelito no es exclusivamente de TI, Cumplimiento, Tesorería o Finanzas, sino es fundamental que este sea compartido en toda la organización. Cada empleado en la organización juega un papel y comparte la responsabilidad de salvaguardar los activos de la empresa. La cultura puede ser esculpida por normas, comportamientos y actitudes de las personas dentro de la organización [9].

Todos los niveles de gestión deben participar de forma clara y coherente, además de tener el compromiso y tomar en cuenta la importancia de la ciberseguridad. Es necesario las actualizaciones regulares sobre los tipos de estafas y el fraude para mantener educada a la fuerza laboral.

Técnicas de prevención y los cambios en la política o los procedimientos deben ser compartidos en toda la organización con correos electrónicos regulares, boletines informativos seminarios web y/o un sitio web dedicado que actúa como recurso y repositorio para obtener información sobre ciberseguridad. Los procesos de escalada para intentos los ataques deben ser claros y accesibles fácilmente, al igual que la información sobre el uso adecuado del correo electrónico de la empresa.

C. La mejora de procesos

Mayor automatización, con menos manipulación manual, mitiga en gran medida el riesgo de fraude interno, pero aumenta vulnerabilidad al ciberdelito ya que la información y las transacciones son electrónicos, digitalizados y basado en la web o en la nube. Los procesos deben revisarse y ser rediseñados (si es necesario) al menos anualmente para garantizar la prevención de las últimas técnicas de fraude.

Proteger a los clientes del banco y la información de sus cuentas, es importante para evitar que los pagos se dirijan a una entidad fraudulenta. Los datos maestros deben restringirse a un equipo dedicado y responsable.

Es necesario sospechar siempre de las solicitudes de transferencias que se envían con un sentido de secreto y urgencia como se mencionó anteriormente. No se debe "responder" para responder a una solicitud de pago enviada por correo electrónico. En lugar, llamar al remitente para verificar su autenticidad.

Se debe considerar tener varias capas de aprobación. Una forma de comprobar la autenticidad es presionar el botón de respuesta (no presione "enviar") y luego colocar el cursor sobre la dirección de correo electrónico. Muchas veces la dirección de correo electrónico no es una dirección de correo electrónico valida, sino que se creó una falsa por estafadores. Tenga en cuenta que los estafadores pueden obtener una gran cantidad de información sobre los roles de varias personas dentro de la organización e incluso puede saber cuándo los procesadores de pago clave están fuera de la oficina. Se producen más intentos en los días previos a un fin de semana festivo cuando el personal de respaldo puede estar procesando pagos y puede ser menos familiar con pasos de prevención del ciberdelito. Por lo tanto, es fundamental entrenar personal y garantizar pasantes, contratistas

o el personal temporal para que estos se encuentren igualmente capacitados en prevención del ciberdelito

D. Formación y sensibilización del personal

Como se indicó anteriormente, el personal es un control muy importante para las empresas contra el fraude como también lo es la tecnología. Sin embargo, como hemos visto, sin la debida formación y concienciación en ciberseguridad lejos de ayudar a protegerse contra una violación de seguridad: el personal puede, de hecho, ellos mismos sin saberlo causar infracciones graves, que pueden ser fatales a las defensas de una empresa. Por lo tanto, un mandato de alto nivel que prioriza y enfatiza la importancia del personal sobre educación, sobre alerta, responsabilidad, fugas de seguridad (así como por comportamiento fraudulento) es de suma importancia en la lucha contra el ciberdelito.

Dada la ubicuidad del correo electrónico empresarial, todos los empleados deben estar bien capacitados sobre el uso del correo electrónico. No se debe permitir el uso personal del sistema de correo electrónico de la empresa. Nunca abra ningún enlace o archivos adjuntos en correos electrónicos sospechosos.

Todo el hardware debe requerir doble autenticación, contraseña frecuente cambiada y contraseña "segura" requisitos (al menos 8 alfanuméricos caracteres con símbolos, números y capitalizaciones). VPN, tokenización y el cifrado es fundamental. Sin embargo, el cifrado por sí solo no resolverá el problema. contraseñas y otros inicios de sesión, las credenciales nunca deben compartirse entre los empleados. No permitir "Traiga su propio dispositivo" para comunicaciones dentro de la empresa a menos que este cuente con un software de cifrado. Limitar el acceso a datos y sistemas sensibles para solo aquellos empleados que necesitan acceso [5].

E. Controles tecnológicos

La primera línea de las defensas es preventiva y debe incluir fuertes requisitos de autenticación, filtros IP y registros de referencias. La prevención del fraude también requiere una revisión del almacenamiento de datos examinar dónde y cómo los datos están siendo grabado y almacenado, quién tiene acceso a él, y si realmente lo requiere. Acceso a la empresa, los sistemas, aplicaciones y datos sólo se darán a los autorizados y según sea necesario, todos los accesos solicitudes registradas y técnicas de autenticación de los autorizados deben mantenerse actualizados.

Sin embargo, la segunda etapa de la detección de fraude y la obstrucción es igualmente importante y requiere software efectivo de detección de malware, entre otras herramientas. Los sistemas de fraude son diseñados para analizar y auto aprender patrones para detectar fraudes y detenerlo cuando se deslice más allá de las medidas preventivas iniciales. La tecnología ha sido aumentada mediante el uso de Big Data como herramienta para identificar patrones anormales que indican actividad sospechosa

Para sistemas y software, asegúrese el último antivirus y antimalware, así como sus actualizaciones y parches. Los sistemas de detección de intrusos son fundamentales para intervenir, contener los ataques. Tener un plan de redundancia en caso de un ataque de denegación de servicio (DDoS). Cifrar todos los datos sensibles en reposo y en tránsito. Asegúrese de que existan cortafuegos entre distintas redes. Considere establecer redes separadas, servidores, LAN para diferentes partes de su organización para limitar el impacto de un éxito intrusión. Cuando se utiliza un tercer socio, es necesario mantener el control del mismo.

III. El futuro de la ciberseguridad

El costo al cual incurre una organización a causa de la ciberdelincuencia seguirá aumentando, aumentan a medida que más procesos, corporaciones y consumidores de todo el mundo se conecten. El costo de una violación de datos promedio se espera que supere los $150 millones por 2020 generando grandes ganancias a la ciberdelincuencia. Para las empresas, esto significa niveles más altos y sofisticados de intentos de fraude, pago, extorsión y espionaje corporativo, entre los que se están produciendo muchos otros delitos informáticos.

La seguridad en el futuro probablemente sea controlada a través de una combinación de modelos basados en riesgos y basados en control, con el saldo en parte dependiente de apetito de riesgo de la empresa [10].

Además, el desarrollo de herramientas como la tecnología Distributed Ledger podría usarse para fortalecer la protección contra el ciberfraude. Por ejemplo, la naturaleza de blockchain lo cual nos asegura la autenticidad a los participantes y verifica todas las identidades de contraparte, pueden proteger a los consumidores y las empresas del fraude.

IV. Conclusiones

Las entidades financieras en Bolivia no pueden permitirse dejar de lado la ciberseguridad: necesitan priorizar e invertir en él ahora. Tomar un enfoque más holístico influye éxito del programa de ciberseguridad. Mientras las defensas tecnológicas permanezcan cruciales, veremos cada vez más que los empleados son los agentes involuntarios de ciberataques, a menos que eduquemos a ellos la manera de prevenir ataques, estos mismos podrán convertirse en instrumentos que ayuden a mitigar el riesgo cibernético. Es responsabilidad en cada organización, desarrollar una estructura de gobierno y cultura de riesgos que eleve la importancia de la ciberseguridad.

El liderazgo superior debe también asegurarse de que todos los empleados reciban la educación y formación necesaria, para entender, estar atentos, a favor y en guardia contra estos ataques, y para mantener este conocimiento actualizado. Además de construir y reforzar su firewall humano, las empresas pueden aprovechar el asesoramiento y el apoyo de su proveedor de seguridad para mantener y actualizar constantemente sus configuraciones tanto de detección y prevención de fraude, y sus tácticas de ciberseguridad en su conjunto.

Referencias

[1] Seguridad de la Información y Ciberseguridad ¿es lo mismo? https://www.cic.es/seguridad-de-la-informacion-y-ciberseguridad-es-lo-mismo/#:~:text=La%20Ciberseguridad%20se%20distingue%20de,ser%20usado%20para%20aspectos%20defensivos.

[2] Akhavein, J., Frame, W., & White, L. (2005). The diffusion of financial innovations: An Examination of The Adoption of Small Business Credit Scoring by Large Banking Organizations. Journal of Business 78, 577-596. http://dx.doi.org/10.1086/427639

[3] There's Nowhere to Hide from the Economics of Cybercrime http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf

[4] IBM 2016 Cyber Security Intelligence Index

[5] Altamimi, T. (2011). Information Security Risks for Internet Banking in Saudi Arabia. A study submitted in partial fulfillment of the requirements for the degree of Master of Science in Information Systems at the university of Sheffield.

[6] Cybercrime Will Cost Businesses Over $2 Trillion By 2019 [https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion-by-2019]

[7] Ambhire, V., & Teltumde, P. (2011). Information Security in Banking and Financial Industry. International Journal of Computational Engineering & Management, 14. Retrieved from http://www.ijcem.org101

[8] Bonnette, C. (2003). Assessing Threats to Information Security in Financial Institutions. GSEC Certification Practical Assignment, Version 1.4b - Option 1 Retrieved from http://sans.org

[9] Emmanuel, A. (2011). The Effect of Internet Banking on the Ghanaian Banking Industry: A Case of CAL Bank, UNI Bank and PRUDENTIAL Bank. A Thesis Submitted to the Institute of Distance Learning, Kwame Nkrumah University of Science and Technology in partial fulfillment of the requirement for the degree of commonwealth executive master of business administration.

[10] Price Water House Coopers. (2014b). Threats to the financial Services Sector. Retrieved from http//www.pwc.com/crimesurvey

[11] Ataque de Phishing a Banco Unión S.A. https://www.odibolivia.org/2018/10/22/ataque-de-phishing-a-banco-union-s-a/

[12] Autoridad de supervisión del sistema financiero https://www.asfi.gob.bo/index.php/asfi/acerca-de-nosotros

Breve CV del autor

Jonathan Wilmer Magne Quispe es Licenciado en Informática por la Universidad Mayor de San Andrés. Actualmente realiza la Maestría en Informática Forense, Seguridad de la Información y Auditoria Informática en el Postgrado en Informática de la UMSA. Es actualmente Arquitecto de Soluciones Digitales del Banco Nacional de Bolivia, anteriormente en el Banco de Crédito BCP. Miembro del grupo de investigaciones GI-FORSAI UMSA. 2do Lugar Big Bank Explosión de ideas. Publicó el artículo “Modelo de seguridad de información para transferencias bancarias mediante comunicación de campo cercano en dispositivos móviles” Revista PGI No. 6. Email: jwmagneq@gmail.com.