Challenge Teórico Compliance

RESOLUCION

Agustin Zeppa

1. Dado que el operador de tele venta utilizara la plataforma productiva de Mercado libre, se deberían presentar las siguientes recomendaciones y restricciones para el uso y acceso de los operadores a la misma:
    a. Controlar el acceso de los operadores a la plataforma productiva mediante usuarios y contraseñas robustas. Las mismas deben expirar cada cierto periodo de tiempo y poseer característica especiales como longitud y tipos de caracteres.
    b. Definir los componentes de la plataforma y los recursos de datos que necesita el operador para ejecutar sus funciones.
    c. Conceder la menor cantidad de privilegios posibles. Solo aquellos necesarios para hacer su función. Es decir, si su objetivo es concretar una venta, que el sistema no le permita ejecutar otras funciones.
    d. Configurar la plataforma para "negar todo" salvo que se permite una función específica.
    e. Llevar a cabo controles de cerficacion de accesos periódicamente. De esta forma validamos que el acceso de los operadores a la plataforma sea correcto.
    f. Establecer un proceso de aprobación documentada para dar de alta a un nuevo operador en la plataforma. Por siguiente, se garantiza que la gerencia tiene conocimiento y autoriza a los operadores a utilizar la plataforma.

2. El objetivo es concretar la venta, por lo tanto, se deberán proteger los datos de los potenciales clientes de la siguiente forma:
    a. No almacenar la información de la tarjeta utilizada para efectuar la compra. Es decir, una vez que se concreta el proceso de pago, la información confidencial de autenticación debe ser destruida de manera segura. Debe ser información irrecuperable.
    b. Solicitar la menor cantidad de datos posibles: solo lo necesario para efectuar el pago.

3. Someter a los operadores de ventas a capacitaciones para un tratamiento seguro de la información. Todo el personal comprometido en el proceso de venta debe tener conocimiento de las políticas de seguridad. No es suficiente tener la mejor tecnología sin buenos operadores.

4. Un problema que plantea la norma PCI:DDS con respecto a las ventas telefónicas es que el operador de la llamada, podría almacenar los datos que recibe de las tarjetas de forma no segura (escribirlos en papel o incluso enviarlos por mensajería instantánea). Por lo tanto, para solucionar este problema, mercado libre debería contratar una empresa de telefonía que utilice IVR (Interactive Voice Response) al momento de recibir los datos confidenciales. Esto se trata, de un sistema que permite realizar una comunicación normal, y al momento de recibir los datos financieros, el cliente continuo la llamada con un sistema automático sin interacción humana.

5. Debido a que el cliente (sea guiado o no por el operador) deberá entregar sus datos financieros en un sistema, podría surgir un ataque MAN-IN-THE-MIDDLE en el momento de la transmisión de los datos hacia los servidores de mercado pago, o incluso cuando mercado pago realiza la autenticación contra las compañías de tarjetas. Es decir, un tercero podría interceptar la comunicación para adquirir información de las tarjetas. Por lo tanto se deberían presentar las siguientes restricciones:

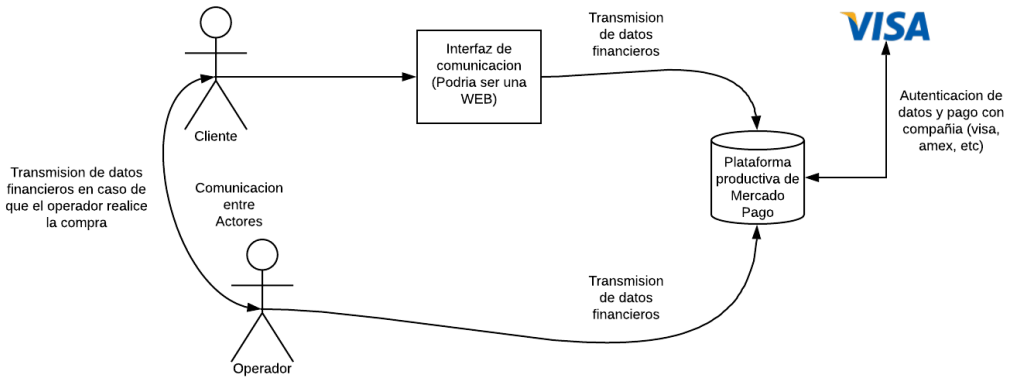
a. Utilizar criptografía y protocolos de seguridad para la transmisión de la información. Podría ofrecerse la opción de usar funciones HASH.
b. Almacenar las claves utilizadas para cifrar/descifrar en la menor cantidad de lugares posibles. Si es posible implementar mecanismo de doble tipo de autenticación para acceder a las mismas.
c. Configurar los routers y firewalls de mercado libre para restringir conexiones entre redes no confiables/no seguras.
d. Establecer conexiones VPN entre los puntos de transmisión de datos financieros.
e. Enmascarar el numero PAN de la tarjeta siempre que el mismo aparezca.
f. Establecer políticas, procedimientos y estándares de seguridad para la correcta configuración de los dispositivos de red, firewalls y protocolos de cifrado de información. Así como para implementar cambios, configuraciones nuevas o incluso dispositivos nuevos.
g. Someter todas las políticas a revisiones periódicas para garantizar la actualización de las mismas con las últimas tecnologías.

6. La implementación de nuevos desarrollos debe estar controlada para que no se comprometa la transmisión de información y los procesos de compra:
    a. Implementar una correcta segregación de ambientes (desarrollo, testing y producción).
    b. Todo nuevo desarrollo debe estar sometido a prueba de aceptación de los usuarios finales, como también a pruebas profundas de calidad, performance y seguridad.
    c. El pasaje de nuevos desarrollos o cambios a producción debe estar solicitada y aprobada por personal adecuado, y con suficiente jerarquía.

7. Usualmente los malware ingresan a las redes de la compañía durante las actividades de negocio. Estos explotan vulnerabilidades de los sistemas y podrían causar anomalías en la recepción de la información, por lo que sería indispensable plantear las siguientes recomendaciones:
    a. Implementar software antivirus en todos los sistemas.
    b. Someter estos programas a procesos de actualización periódicos para siempre tener las últimas versiones. Esto permite estar actualizado ante nuevas amenazas y poseer los parches más recientes.

8. Implementar logs de auditoria en los sistemas de comunicación y pago, para poder reconstruir los eventos en caso de anomalías Así como también, controles de monitoreo periódicos de las actividades mencionadas. Es decir, toda implementación de nuevo software, cambios en configuraciones de los sistemas, certificación de accesos, etc. Debe ser monitoreada para asegurar el cumplimiento de las normas de seguridad.

9. Y por último, los sistemas y servidores de mercado pago, deberían tener a los usuarios con privilegios amplios correctamente configurados. Se podría utilizar una herramienta como SAT (Security Access Tool) para ensobrarlos. Así como también, definir un procedimiento de solicitud, aprobación y control sobre la concesión y actividad de estos usuarios.


Cliente
Interfaz de comunicacion (Podria ser una WEB)
Transmision de datos financieros
VISA
Autenticacion de datos y pago con compañia (visa, amex, etc)
Plataforma productiva de Mercado Pago
Transmision de datos financieros en caso de que el operador realice la compra
Comunicacion entre Actores
Operador
Transmision de datos financieros