**Caso – Levantamiento de riesgos técnicos (Tomas Sánchez)**

Preguntas:

**¿Qué harías?**

Con el fin de contar con información que nos permita encarar levantamientos puntuales con los equipos de negocio y detectar posibles riesgos, llevaría a cabo el siguiente plan:

En primer lugar, realizar un entendimiento, mediante reuniones con los sectores correspondientes y realizando request a ambas APIs, sobre cómo se relaciona la API que contiene distintas iniciativas con la API que comprende la relación entre aplicaciones y estas iniciativas.

Una vez que logremos mapear la relación entre ambas APIs y las aplicaciones involucradas, y con la información obtenida gracias a las reuniones con las distintas unidades de negocio, establecería un rango de criticidad de la información involucrada. Dicho rango iría desde la información con criticidad baja hasta la información con la criticidad alta.

Para establecer esta criticidad, evaluaría cual es la información sensible presente en las aplicaciones, por ejemplo: datos sensibles de los usuarios internos y externos, información sobre las cuentas de nuestros usuarios, cifrado de contraseñas de usuarios especiales, etc.

Para la información cuya criticidad sea alta, verificaría la existencia de logs de auditoría para poder reconocer incidentes y saber cómo actuar ante éstos. Por otro lado, verificaría la correcta realización de los backups y, en el caso de que alguna copia de seguridad falle, evaluaría las acciones llevadas a cabo para remediar este hecho.

Poniendo foco en la aplicación y los datos, evaluaría los accesos a dichas aplicaciones para corroborar que los mismos sean los correctos y no haya personas con acceso indebido a información restringida, y evaluaría las cuentas con máximos privilegios (o usuarios especiales), para asegurarnos que las mismas cuenten con contraseñas encriptadas.

Con respecto a los servidores y las bases de datos, verificaría el estado de patching de servidores diariamente para asegurarnos la disponibilidad de los mismos y, en el caso de encontrar alguna anomalía, poder actuar rápidamente para evitar una posible pérdida de información. También verificaría si las conexiones entre las distintas bases de datos y las aplicaciones se encuentran correctamente cifradas, y si los usuarios con acceso a las bases de datos son los correspondientes.

Para terminar, y con relación al entorno en el cual se encuentran las APIs con sus aplicaciones en cuestión y la información del equipo de Seguridad Informática, verificaría que el firewall se encuentre actualizado en su última versión y que la configuración de proxy utilizada sea la correcta. Además, realizaría pruebas de intrusión a modo de corroborar lo mencionado anteriormente.

**¿Por qué lo harías de esa manera?**

Lo haría de esa manera dado que estaría poniendo principal foco sobre los datos y el dinero de nuestros usuarios de Mercado Pago. Con lo mencionado anteriormente, estaría cubriendo los principales riesgos de pérdida o filtrado de información, ya sea por un ataque externo como por un error humano.

A su vez, estaría poniendo foco en la confidencialidad de la información, en la integridad de la misma y en la disponibilidad de los servicios, aplicaciones y hardware de la compañía.

**¿Cuáles consideras que son los principales factores que te aseguran el éxito de tu propuesta?**

Los principales factores que me aseguran del éxito de mi propuesta es que, mediante la correcta asignación de permisos, tanto en las aplicaciones como en las bases de datos, estaría garantizando la confidencialidad de la información, permitiendo que sólo personal autorizado tenga acceso a la misma.

Por otro lado y, en el caso de detectar algún incidente de seguridad, estarían a disposición los logs de auditoría para realizar un seguimiento de este incidente y poder prevenirlo en el futuro. Además, en el caso de que este incidente conlleve algún tipo de modificación o pérdida de información, se tendrían disponibles backups diarios para restaurar a la situación anterior al incidente.

Con respecto a la propuesta para los servidores, lo que me aseguraría el éxito sería el constante seguimiento del estado de los mismos, asegurándonos que se encuentren disponibles el mayor tiempo posible. Y para el caso de las bases de datos, es importante tener cifrada las comunicaciones entre éstas y las aplicaciones, y corroborar que los accesos a las mismas sean los correctos.

Por último, al tener actualizado el firewall en su última versión disponible y tener bien configurado el proxy, se prevendrían posibles ataques a la red interna y externa de la compañía, lo que podría conllevar en una pérdida de información de los usuarios.

**¿Cuáles son los principales riesgos y amenazas?**

Los principales riesgos y amenazas a los cuales podría estar expuesta la infraestructura crítica de Mercado Pago son:

* Posible pérdida de información por accesos no autorizados.
* Sistemas desactualizados o sin la seguridad correspondiente.
* No detectar, en un periodo oportuno, acciones que pudieran derivar en el borrado y/o modificación de datos sensibles, o bien, intentos de accesos no autorizados en el sistema.
* Posible intento de intrusión a la red por parte de usuarios maliciosos.

**¿Qué aprendiste realizando este challenge?**

Gracias a este challenge aprendí a aplicar, a un caso más teórico, lo que hago diariamente en mi trabajo. Por otro lado, me ayudo a aprender y repasar conceptos, y a poder ver las distintas situaciones, que se presentan en una infraestructura critica, desde el lado de Seguridad Informática.