Gestión de vulnerabilidades

Una vulnerabilidad es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información, lo cual permite que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de esta. Todas las tecnologías que utilizamos fueron creadas por personas y son propensas a tener fallas. Regularmente, distintos investigadores de seguridad encuentran vulnerabilidades y las reportan para que sean solucionadas.

Por ello, es crucial tener bien identificado el hardware y software que usamos, para conocer si pueden ser susceptibles de sufrir alguna vulnerabilidad con el tiempo. A toda persona que trabaje en seguridad le tomará una cuota considerable de tiempo estar informada sobre las nuevas fallas de seguridad que aparecen, y sobre todo, estar atenta a ver si representan un riesgo en la infraestructura que se controla. Por dicho motivo, otra de las actividades de una estrategia de seguridad debe ser la de mantener los sistemas operativos y aplicaciones actualizados/as, esto significa que debe contar siempre con la última versión instalada.

Actualización del sistema o aplicación

Que un sistema o aplicación tenga su versión más reciente, asegura que se han corregido todos aquellos errores "descubiertos" que pueden provocar que el sistema/aplicación no funcione correctamente. Esta tarea se vuelve fundamental dentro de la vida de una organización, y en especial sobre los dispositivos tecnológicos, dado que si un sistema operativo o aplicación no está con su última versión es vulnerable, es decir, un atacante podría averiguar qué versión de sistema o aplicación está corriendo, notar que esa misma tiene una vulnerabilidad que no fue corregida y explotarla, es decir, utilizar esa falla para poder acceder y manipular al sistema en cuestión.

La actualización del sistema operativo/aplicación es una actividad que deberá realizarse de forma periódica, estableciendo cada cuánto se ejecutará, no sólo el control de las versiones, sino también su actualización en caso de corresponder, y buscar así tener asegurados todos los sistemas y las aplicaciones existentes. Ahora bien, hay que definir cada cuánto se deberá realizar este control de las versiones. Esta decisión debe ser establecida por quien tome las decisiones de seguridad, pero un buen parámetro para definirlo podría ser realizar el control una vez por mes. Habitualmente notamos que en los dispositivos móviles, las aplicaciones que tenemos instaladas se actualizan para corregir errores e incluir nuevas funcionalidades si las hay. En el caso de los sistemas operativos y aplicaciones de computadoras funciona de la misma forma.

Al instalar un sistema, por lo general, éste establece una conexión con Internet para corroborar si hay actualizaciones, descargarlas e instalarlas. No

obstante, si en una organización, todos los equipos de la red realizan esta tarea, es decir, salir a Internet a ver si existe alguna actualización y descargarla, se produciría una degradación de la capacidad de la red, ya que cada dispositivo está descargando el mismo archivo.

comúnmente lo que se hace es no permitir a los dispositivos de la red que se actualicen. Esta medida suele ser realizada al restringir la salida a Internet por Firewall, al deshabilitar el servicio de actualización, etc. La forma de solucionar este problema, es que un equipo de la red sea el que descargue las actualizaciones correspondientes, tarea suele realizar algún administrador; y luego durante un horario en el que no se realicen actividades laborales, se proceda a implementar las actualizaciones en los equipos de la red que haya que actualizar. Esto mejora el rendimiento de la red ya que no se satura de la misma información y por otro lado, se hace en un momento del día que no moleste a los usuarios que dependen de ella.

Escáneres de Vulnerabilidades para uso personal

De igual forma que podemos encontrar soluciones empresariales para grandes entornos de equipos, como GFI Languard u OpenVAS, también podemos utilizar software automatizado para detectar en nuestros equipos vulnerabilidades de seguridad. Estos programas nos permitirán descubrir qué sistema operativo o programas no están actualizados a la última versión, o qué parche de seguridad está faltando.

Podemos encontrar entre los más conocidos a:

- *MSBA 2.3*: software (descontinuado) desarrollado por Microsoft para detectar errores y configuraciones de seguridad deficientes, en cualquier producto de dicha empresa, ya sea en servidores, bases de datos, estaciones de trabajo, etc. No arroja resultados sobre un producto que no haya sido creado por Microsoft. Permite realizar análisis de un equipo en particular, como de un conjunto en una red. Es gratuito y muy útil para realizar auditorías. Dejó de tener soporte oficial de Microsoft hace tiempo, pero resulta muy útil para fines didácticos de poder entender cómo funciona un escáner de vulnerabilidades de bajo nivel.
- *Sumo Updater*: para el resto de programas que estén instalados en los equipos podemos utilizar este software gratuito desarrollado por KC software, el cual permite identificar qué aplicaciones están sin actualizar y nos proporciona el enlace directo para poder actualizarlas.

Ambientes de prueba

Es fundamental considerar probar todo cambio o implementación nueva que queramos incluir en el entorno de trabajo de una organización. Explicado de manera simple, existen tres entornos:

- Entorno de desarrollo: donde se crea.
- Entorno de pruebas: donde se verifica lo que se creó.
- Entorno de producción: donde funciona lo que se creó.

Si nosotros hemos descubierto que somos vulnerables y debemos aplicar una actualización para solucionar esa falla, tenemos que considerar que no se podrá instalar directamente sobre los equipos productivos (los que están trabajando); ya que si no hemos verificado si esa actualización funciona bien, ésta podría provocar fallas que no estábamos esperando. Es fundamental comprender que, en muchas ocasiones, los desarrolladores de software realizan pruebas de sus productos y actualizaciones en un entorno de pruebas que no suele ser el mismo al que una organización pueda tener. Estas diferencias podrían provocar que la actualización que nosotros queramos instalar genere una falla nueva y complique el desarrollo normal de las actividades.
Por este motivo, es necesario contar con un entorno de pruebas donde todo cambio, instalación o cosa que se tenga que probar pase primero por un control de funcionamiento en este ambiente y si las pruebas son favorables, estará listo para llevar al ambiente de producción.

Actualizaciones

La mayoría de las vulnerabilidades serán corregidas cuando apliquemos las actualizaciones y otras se resolverán con algunos ajustes de configuración. Es sumamente importante implementar las actualizaciones, ya que de no hacerlo, estamos prolongando nuestra exposición frente a una vulnerabilidad específica.

Consideraciones a tener en cuenta al actualizar:

- Instalar actualizaciones gradualmente en los equipos, no todos juntos ni en el mismo día.
- Realizar la tarea fuera del horario laboral.
- No permitir que los equipos se actualicen por sí solos.
- Centralizar la actualización desde un equipo al resto (WSUS).
- Descargarlas desde repositorios oficiales.