Introducción

Este documento detalla los riesgos que pueden afectar a una plataforma de escritorios virtuales y describe diferentes técnicas para securizar plataformas de este tipo.

Para securizar escritorios virtuales o físicos se utilizan diferentes métodos. La tecnología de escritorios virtuales introduce nuevos retos y desafíos en cuestiones de seguridad. Aunque algunas prácticas son comunes para entornos físicos y virtuales, es necesario implementar nuevas técnicas y medidas de seguridad.

Control sobre el uso de Internet

Para acometer una migración de puestos de usuario tradicionales a plataformas VDI con éxito, muchos de los procesos de gestión se centralizan, como por ejemplo, las políticas de usuario y sistema.

El uso de estas políticas permite mejorar la seguridad en una plataforma VDI, centralizando el control del entorno de usuario. A continuación, se detallan algunas políticas que permiten securizar los escritorios virtuales:

- Confeccionar documentos que pueden ser descargados
- Almacenar adecuadamente los ficheros descargados para tener una mejor visibilidad de éstos
- Controlar la ejecución de scripts
- Determinar la longevidad de los ficheros temporales de los navegadores

Aislamiento de virus

Utilizando escritorios virtuales basados en plantillas, el escritorio virtual vuelve a su estado inicial cada vez que un usuario cierra sesión.

También es posible realizar un apagado de emergencia centralizado de los escritorios virtuales infectados forzando a los usuarios a cerrar sesión.

Posteriormente, estos escritorios se pueden reiniciar en entornos aislados para poder eliminar el virus de la red.

Para la detección de virus en un entorno VDI, los administradores de la plataforma tendrán que tener en cuenta que realizar escaneos de disco en busca de virus de la forma habitual (en un tiempo determinado sobre toda la plataforma) puede suponer el completo colapso de toda la plataforma debido a la tremenda carga de IOPS a la que se somete al almacenamiento.

A continuación, se detallan algunas recomendaciones de seguridad para plataformas VDI:

- Utilizar descargas y escaneos en busca de virus de forma aleatoria limitando el número de escritorios que realizan esta tarea simultáneamente
- Utilizar las diferentes funcionalidades de los productos antivirus para preescanear, aprobar e ignorar ficheros de la plantilla base (golden image) sobre la que se van a desplegar los escritorios virtuales
- Escanear única y exclusivamente aquellos ficheros que son creados o modificados en el escritorio virtual. Cada uno de los fabricantes de antivirus tiene funciones específicas para plantillas base de plataformas VDI

Riesgos comunes

En la tabla que figura en la siguiente página, se muestran algunos riesgos de seguridad, las características de los mismos sobre una plataforma tradicional y una plataforma virtual, así como una serie de recomendaciones operativas a tener en cuenta a la hora de implementar la virtualización de escritorios.

Riesgo de seguridad	Escritorio físico	Escritorio virtual	Recomendación
Virus en los discos locales	Un escaneo periódico completo de los discos encuentra virus que no se detectaron con el escaneo en tiempo real	Los escaneos completos no son necesarios y pueden provocar caídas en el rendimiento de la plataforma	Utilizar las características de preescaneo del antivirus
Virus en unidades de red	La mayoría de los ficheros se encuentran en discos locales y algunos en servidores de ficheros, siendo escaneados separadamente	Las plataformas VDI alojan gran cantidad de datos en recursos compartidos (perfiles, recursos compartidos, redirección de carpetas) con lo que una mayor cantidad de ficheros son escaneados en los servidores	Es necesario asumir que se producirá una mayor carga de IOPS en los servidores de ficheros. Asignar mayores recursos o prioridad al almacenamiento donde se ubican estos servidores de ficheros durante el escaneo de éstos
Descargas de Internet	Difícil de controlar	Uso de políticas GPO para ofrecer un control mejorado	Centrarse en los puntos de entrada (gateways, firewalls) y políticas y no en los escritorios
Aislamiento del sistema	Un método necesario pero que consume una gran cantidad de tiempo para hacer frente a la infección	Permite el aislamiento del sistema y fuerza el arranque de los escritorios para permitir a los usuarios trabajar	Preparar una plantilla base para este tipo de escenarios
Políticas de acceso y firewall	Activación de Firewall de Windows para proteger al escritorio cuando está fuera de la oficina	Incluso si el usuario o el dispositivo de conexión son móviles, el escritorio virtual está alojado en el Data Center	Centrar los esfuerzos en la seguridad y gateway del Data Center
Data Loss Prevention (DLP) Prevención de pérdida de datos	DLP se usa para escanear y proteger los datos sensibles de la entidad	Se utiliza la misma táctica que en los escritorios físicos con el añadido de que es posible controlar las conexiones de dispositivos USB	VDI no elimina la necesidad de DLP
Encriptación de disco	Evita el robo de información cuando las unidades de disco son extraídas o los portátiles se extravían	No es necesaria la encriptación debido a que los escritorios virtuales están alojados en el Data Center, que es un entorno controlado	No es necesario invertir en la encriptación de discos

Problemáticas de seguridad en plataformas de escritorios virtuales

En las plataformas de escritorios virtuales se detectan una serie de problemáticas de seguridad que se detallan a continuación:

- Muchas entidades permiten a sus usuarios trabajar con derechos de administrador en sus escritorios. Esta práctica puede provocar agujeros de seguridad, ya que facilita la instalación de cualquier software (seguro o no) en los escritorios. Además, cuando los usuarios abren una sesión con derechos de administrador, los virus pueden ocasionar mucho más daño sobre los sistemas
- Existe la creencia de que utilizando escritorios virtuales es fácil revertir éstos al estado original de la plantilla base, con lo que no es necesaria la utilización de sistemas de seguridad y antivirus
- Desde que el escritorio virtual se está ejecutando en el Data Center, el entorno de usuario está en una red segura desde una conexión segura, aunque no se sabe lo que hace el usuario dentro de su sesión

Para acotar estos problemas se recomienda:

- No permitir a los usuarios abrir sesiones sobre sus escritorios con derechos de administración
- En cuanto a seguridad y herramientas de gestión, una plataforma tradicional y una plataforma de escritorios virtuales son bastante similares. Si se usan herramientas antivirus y políticas de seguridad en el entorno tradicional, es necesario utilizar las mismas herramientas en el entorno de escritorios virtuales, aunque las técnicas de gestión sean algo diferentes
- Cuando se usan plataformas VDI, los escritorios virtuales están en el mismo entorno que los servidores de producción. Si se utilizan VLAN´s y firewalls es necesario asegurarse de separar estos servidores de los escritorios

Utilizar VDI para mejorar la seguridad

Un mainframe es uno de los sistemas más seguros, ya que los terminales interactúan con el sistema utilizando protocolos de conexión, con lo que la transferencia de ficheros bidireccional es imposible.

Este concepto se puede aplicar a los entornos VDI, existiendo escritorios virtuales en un entorno de confianza como es el Data Center, a los que se conectan usuarios desde dispositivos más o menos inteligentes.

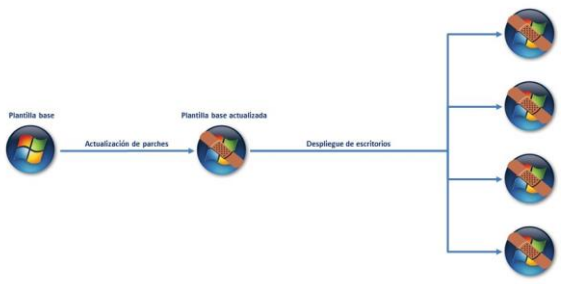
A continuación, se describen alguna de las razones por las que VDI permite asegurar un entorno de puestos de usuario:

Configuración de equipos. Muchas reglas de seguridad se definen cuando se configura una plantilla base para desplegar escritorios virtuales y éstas no suelen ser modificadas posteriormente.

También es necesario que en una plataforma de escritorios virtuales cada escritorio esté configurado de acuerdo a una serie de reglas de seguridad definidas mediante Políticas de Grupo.

Centralizando este tipo de configuraciones, se mejora significativamente la seguridad de todos los escritorios.

Actualización de parches. Con la utilización de escritorios virtuales basados en plantillas, se ahorra una gran cantidad de tiempo en comparación con una plataforma tradicional. Realizando la aplicación y actualización de parches en la plantilla base se asegura que se aplican correctamente los parches en todos los escritorios.



Para realizar correctamente la aplicación de parches en la plantilla base, se deben tener en cuenta las siguientes consideraciones:

- Qué parches son necesarios y en qué plantillas base se aplican: parches para 32-bit, parches para 64-bit, versión de SO, etc
- En qué momento se aplican los parches en la plantilla base
- Cerciorarse de que a cada plantilla base se le aplican los parches apropiados y éstos se ejecutan correctamente
- Con qué parches son necesarios reinicios del sistema

La aplicación de parches en un entorno tradicional necesita una cantidad significativa de tiempo, esfuerzo y ancho de banda.

Utilizando plataformas de escritorios virtuales la aplicación y gestión de parches se simplifica, ya que todos los parches necesarios se aplican sobre la plantilla base sobre la que se desplegarán posteriormente los escritorios virtuales.

Reglas de firewall. Los firewalls que existen en los sistemas operativos Windows ofrecen una primera barrera de protección del sistema y los datos.

La forma más sencilla para configurar las políticas y excepciones del firewall es realizar esta configuración en la plantilla base y realizar un despliegue posterior de ésta. Estos cambios en las políticas y excepciones se pueden realizar de forma prácticamente inmediata asegurando que todos los escritorios reciben los cambios necesarios.

Control de aplicaciones. Un escritorio que se considera seguro puede tener problemas si los usuarios pueden saltarse las políticas de seguridad instalando aplicaciones en sus escritorios. Si estas aplicaciones no han sido parcheadas y configuradas correctamente, pueden llegar a ser una puerta de entrada para hackers y los usuarios pueden instalar aplicaciones no deseadas con malware o spyware.

Utilizar plataformas de escritorios virtuales es una buena manera de asegurar qué aplicaciones están permitidas en los escritorios.

Que los usuarios no tengan derechos de administrador en sus escritorios virtuales implica que éstos no puedan instalar aplicaciones y, aunque no sea una decisión popular, es fundamental en la seguridad del puesto de usuario, permitiendo ejecutar únicamente las aplicaciones instaladas en la plantilla base. En el peor de los casos, si una aplicación no permitida llegara a instalarse, si se usan escritorios no persistentes, en el siguiente inicio de sesión ésta sería eliminada.

Soporte y servicios profesionales

Virtual Cable comercializa UDS Enterprise mediante un modelo de suscripción según el número de usuarios, incluyendo soporte y actualizaciones.

Además, Virtual Cable ofrece servicios profesionales para instalar y configurar UDS Enterprise.

Para más información, visite www.udsenterprise.com o envíenos un email a info@udsenterprise.com

Fuentes:

Physical vs. virtual desktop security: It's just not the same, Eugene Alfaro.
The top 5 ways that VDI can help improve your enterprise's security, Eric Schultze.