Conceptos básicos para la defensa del perímetro

REGLAS Y FILTROS DE FIREWALL

Los firewalls representan un mecanismo de defensa inicial que debe abarcar toda la red. Las reglas que se apliquen a los firewalls deben ser altamente restrictivas y establecerse por host y servicio.

Al crear las reglas para los firewalls y las listas de control de acceso (ACL) de los routers, céntrese en primer lugar en proteger los dispositivos de control de acceso y la red frente a posibles ataques.

- Asegúrese de que los datos sigan fluyendo mediante la utilización de ACL de red y las reglas para los firewalls.
- Compruebe el funcionamiento de las reglas para los firewalls y las ACL de los routers para determinar si las reglas contribuyen a ataques de negación de servicio (Denial of Service, DoS).
- Utilice uno o varios DMZ como parte del desarrollo sistemático y formal de firewalls.
- Sitúe en esa ubicación todos los servidores a los que se puede acceder por Internet.
- Limite la conectividad de los DMZ.

ANTIVIRUS

Utilice soluciones antivirus en todo el ambiente: tanto en los servidores como en las computadoras de escritorio. Utilice soluciones antivirus especializadas para tareas específicas, como detectores de virus para servidores de archivos, herramientas de análisis de contenido y detectores de carga y descarga de datos. Configure las soluciones antivirus para que detecten virus que entren o salgan del sistema.

Estas soluciones deben instalarse primero en los servidores de archivos críticos y, a continuación, en los servidores de correo, de base de datos y de red.

En el caso de las computadoras portátiles y de escritorio, debe implementar una solución antivirus en el ambiente predeterminado.

Si utiliza Microsoft Exchange, utilice las funciones adicionales de antivirus y los filtros de contenido para los buzones de correo.

USUARIOS DE ACCESO REMOTO

Ponga en práctica controles de contraseñas complejas para todos los usuarios de acceso remoto, independientemente de si el acceso se concede mediante tecnologías de marcación telefónicas o VPN. Se considera que una contraseña es compleja si cumple estas condiciones:

- Alfanumérica + Mayúsculas y minúsculas
- Contiene al menos un caracter especial
- Contiene como mínimo 8 caracteres

Ponga en práctica otro factor más de autenticación para las cuentas de acceso remoto. Si lo desea, también puede utilizar controles avanzados para la administración de cuentas y el registro de acceso a las cuentas (no permita que se compartan cuentas).

Con respecto al acceso remoto, resulta especialmente importante proteger el ambiente mediante políticas estrictas de administración de cuentas, prácticas seguras de registro y funciones para detectar incidentes. Para limitar aún más los riesgos de ataques de fuerza bruta a las contraseñas, puede poner en práctica los controles siguientes:

- Vencimiento de contraseñas
- Bloqueo de la cuenta después de entre 5 y 7 intentos de registro fallidos
- Registro del sistema

Para los servicios de acceso remoto también deben considerarse los sistemas que se utilizarán para acceder a la red o a los hosts. Por tanto, podría resultar conveniente controlar los hosts con acceso remoto a la red.

POLÍTICAS SOBRE CONTRASEÑAS

Por lo general, las limitaciones para crear contraseñas de administradores deben ser más estrictas que las que se aplican a las cuentas normales.

En Windows, debe crear contraseñas de 14 caracteres alfanuméricos que incluyan caracteres especiales para las cuentas administrativas (y las cuentas de servicio).

SEGURIDAD FÍSICA

Todos los equipos computacionales se deben proteger contra robos. Los servidores y los equipos de red deben mantenerse en lugares que se puedan cerrar con llave y cuyo acceso sea controlado.