Política de Seguridad de Router y Switch

Exención de responsabilidad: Esta política fue creada por o para el SANS Institute para la comunidad de Internet. Toda o parte de esta política se puede utilizar libremente para su organización. No se requiere aprobación previa. Si desea contribuir con una nueva política o una versión actualizada de esta política, envíe un correo electrónico a policy-resources@sans.org.

Última actualización de estado: *Actualizado en junio de 2014*

1. Visión general

Ver Propósito.

2. Propósito

En este documento se describe una configuración mínima de seguridad requerido para todos los enrutadores y conmutadores de conexión a una red de producción o usado en una capacidad de producción de o en nombre de <Nombre de la empresa>.

3. Alcance

Todos los empleados, contratistas, consultores, trabajadores temporales y otros a <Nombre de la empresa> y sus filiales deben cumplir con esta política. Todos los routers y conmutadores conectados a <Nombre de la empresa> redes de producción se ven afectados.

4. Política

Cada router debe cumplir con los siguientes estándares de configuración:

1. No hay cuentas de usuario locales están configurados en el router. Enrutadores y conmutadores deben utilizar TACACS + para toda la autenticación de usuario.
2. La contraseña de activación en el router o switch debe mantenerse en una forma encriptada segura.
   El router o switch deben tener la contraseña de activación establecido en la contraseña actual de la producción de router / switch de la organización de soporte del dispositivo.
3. Los siguientes servicios o características se deben desactivar:
   a. Difusiones dirigidas por IP
   segundo. Los paquetes entrantes en el router / switch de origen con direcciones no válidas, tales como direcciones RFC1918
   do. pequeños servicios TCP
   re. pequeños servicios UDP
   mi. Todo el enrutamiento de origen y de conmutación
   F. Todos los servicios Web que se ejecutan en el router
   sol. <Nombre de la empresa> protocolo de detección en las interfaces conectadas a Internet
   h. servicios de Telnet, FTP y HTTP
   yo. Auto-configuración

4. Los siguientes servicios deben ser desactivados menos que se proporcione una justificación de negocio:

a. <Nombre de la empresa> Protocolo de descubrimiento y otros protocolos de descubrimiento

segundo. concentración de enlaces dinámicos

do. entornos de secuencias de comandos, tales como la concha TCL

5. Los siguientes servicios deben estar configurados:

a. Contraseña de cifrado

segundo. NTP configurado para una fuente estándar corporativo

6. Todas las actualizaciones de enrutamiento se pueden hacer usando las actualizaciones de enrutamiento seguras.

7. Utilice cadenas de comunidad SNMP estandarizados corporativos. cadenas predeterminadas, como público o privada debe ser eliminado. SNMP debe estar configurado para utilizar la versión más segura del protocolo permitido por la combinación de los sistemas de dispositivos y de gestión.

8. listas de control de acceso deben ser utilizados para limitar la fuente y el tipo de tráfico que puede terminar en el propio dispositivo.

9. Las listas de control de acceso para transitar por el dispositivo deben ser agregadas a medida que surjan las necesidades del negocio.

10. El router debe estar incluido en el sistema de gestión de la empresa corporativa con una punto de contacto designado.

11. Cada router debe tener la siguiente declaración presentada para todas las formas de inicio de sesión si remoto o local:

"ACCESO NO AUTORIZADO A ESTA dispositivo de red está prohibido. Debe tener permiso explícito para acceder o configurar este dispositivo. Todas las actividades realizadas en este dispositivo puede ser conectado, y violaciónes de esta política puede resultar en acción disciplinaria, y pueden ser reportados a la policía . no existe el derecho a la privacidad en este dispositivo. el uso de este sistema implica el consentimiento a la supervisión ".

12. Telnet no puede ser utilizado en cualquier red para gestionar un router, a menos que haya un seguro túnel de protección de todo el camino de comunicación. SSH versión 2 es el protocolo de gestión preferido.

13. protocolos de enrutamiento dinámico deben utilizar la autenticación en las actualizaciones de enrutamiento se envían a los vecinos. Hash de contraseñas para la cadena de autenticación debe estar habilitado cuando está apoyado.

14. El estándar de configuración del router corporativo definirá la categoría de enrutamiento sensible y los dispositivos de conmutación, y requieren los servicios o de configuración en los dispositivos sensibles incluyendo adicionales:

a. lista de acceso IP de contabilidad

segundo. registro de dispositivo

do. Los paquetes entrantes en el router de origen con direcciones no válidas, como RFC1918 direcciones, o aquellos que podrían ser utilizados para suplantar el tráfico de red se dejará caer

re. consola del router y módem deben ser restringidas por seguridad adicional controles

5. Cumplimiento de la política

5.1 Medición de cumplimiento

El equipo Infosec verificará el cumplimiento de esta política a través de diversos métodos, incluyendo, pero no limitado a, periódica walk-thru, video vigilancia, informes herramienta de negocios, auditorías internas y externas, y la retroalimentación al dueño de la póliza.

5.2 excepciones

Cualquier excepción a la política debe ser aprobada por el equipo de Infosec con antelación.

5.3 Incumplimiento

Un empleado que haya violado esta política puede ser objeto de medidas disciplinarias, hasta e incluyendo la terminación del empleo.

6 Las normas relacionadas, Políticas y Procesos

Ninguna.

7 Términos y definiciones

Ninguna.

8 Revisión histórica

Fecha del cambio	Responsable	Resumen de cambios
de junio de 2014	SANS Equipo política actualizada y se convierte en el nuevo formato.	