Herramientas de acceso remoto Política

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

1. Visión general

software de escritorio remoto, también conocido como herramientas de acceso remoto, proporcionan una forma para que los usuarios de computadoras y personal de apoyo por igual para compartir pantallas, sistemas informáticos de trabajo de acceso desde el hogar, y viceversa. Ejemplos de este tipo de software incluyen LogMeIn, GoToMyPC, VNC (Virtual Network Computing), y Windows de escritorio remoto (RDP). Si bien estas herramientas pueden ahorrar tiempo y dinero mediante la eliminación de los viajes y permitiendo la colaboración, sino que también proporcionan una puerta trasera en la red <Nombre de la empresa> que puede ser utilizado para el robo, el acceso no autorizado a, o destrucción de los bienes. Como resultado, sólo se han aprobado, monitoreados, y herramientas de acceso remoto controlados adecuadamente pueden ser usados en <Nombre de la empresa> sistemas informáticos.

2. Propósito

Esta política define los requisitos para herramientas de acceso remoto utilizados en <Nombre de la empresa

3. Alcance

Esta política se aplica a todo el acceso remoto en el que cualquiera de los extremos de la comunicación termina en un <Nombre de la empresa> activos del equipo

4. Política

Todas las herramientas de acceso remoto que se utilizan para la comunicación entre <> Nombre de la empresa activos y otros sistemas deben cumplir con los siguientes requisitos de la política.

4.1 Herramientas de acceso remoto

<Nombre de la empresa> proporciona mecanismos para colaborar entre los usuarios internos, con los socios externos, y no de <Nombre de la empresa> sistemas. La lista de software aprobado puede obtenerse de <-software-list-enlace-a-acceso remoto aprobado>. Debido a la configuración adecuada es importante para el uso seguro de estas herramientas, se proporcionan procedimientos de configuración obligatorias para cada una de las herramientas aprobadas.

La lista de software aprobado puede cambiar en cualquier momento, pero los siguientes requisitos será utilizado para la selección de productos aprobados:

una) Todas las herramientas de acceso remoto o sistemas que permiten la comunicación a <Nombre de la empresa>
los recursos de los sistemas de Internet o socios externos deben requerir autenticación de múltiples factores. Los ejemplos incluyen tokens de autenticación y las tarjetas inteligentes que requieren un PIN o contraseña adicional.

segundo) La fuente de base de datos de autenticación debe ser Active Directory o LDAP, y la
protocolo de autenticación debe implicar un protocolo de desafío-respuesta que no es susceptible a ataques de repetición. La herramienta de acceso remoto debe autenticarse mutuamente los dos extremos de la sesión.

do) herramientas de acceso remoto debe ser compatible con el <Nombre de la empresa> proxy de capa de aplicación en vez
que las conexiones directas a través del firewall (s) de perímetro.

re) herramientas de acceso remoto deben soportar fuertes, de extremo a extremo de cifrado del acceso remoto
canales de comunicación como se especifica en el <Nombre de la empresa> cifrado de red política de protocolos.

mi) Todos <Nombre de la empresa> sistemas antivirus, prevención de pérdida de datos, y otra de seguridad deben
No debe ser desactivado, interferido, o evitar de cualquier manera.

Todas las herramientas de acceso remoto deben ser comprados a través de la norma <Nombre de la empresa> proceso de adquisición, y el grupo de tecnología de la información deben aprobar la compra.

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

La siguiente definición de términos y se pueden encontrar en el SANS Glosario ubicada en:
https://www.sans.org/security-resources/glossary-of-terms/

- proxy de capa de aplicación

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.