Política de seguridad de la red: Informe oficial de Mejores Prácticas

Contenido

Introducción

Sin una política de seguridad, la disponibilidad de su red puede verse comprometida. La política comienza por evaluar el riesgo para la red y la creación de un equipo de respuesta. La continuación de la política requiere la implementación de una práctica de administración del cambio en la seguridad y supervisión de la red para detectar violaciones de seguridad. Por último, el proceso de revisión del estudio modifica la política existente y se adapta a las lecciones aprendidas.

Este documento se divide en tres áreas: preparación, prevención, y respuesta. Observemos cada paso con mayor profundidad.

Preparación

Antes de implementar una política de seguridad, debe hacer lo siguiente:

- Cree las declaraciones de política de uso.
- Realizar un análisis de riesgo.
- Establecer una estructura de equipo de seguridad.

Crear Declaraciones de Políticas de Uso

Se recomienda crear de las declaraciones de política de uso que describan los roles y las

responsabilidades de usuarios con respecto a la seguridad. Usted puede comenzar con una política general que incluya todos los sistemas de red y datos dentro de su compañía. Este documento debe proporcionar a la comunidad de usuarios generales las nociones básicas de la política de seguridad, de su propósito, de las guías de consulta para mejorar las prácticas de seguridad, y las definiciones de sus responsabilidades con respecto a la seguridad. Si su compañía ha identificado acciones específicas que podrían dar lugar a acciones disciplinarias o punitivas contra un empleado, estas acciones y cómo evitarlas se deben articular claramente en este documento.

El siguiente paso es crear una declaración de uso aceptable del socio para proporcionar a los socios las nociones básicas de la información disponible, la disposición prevista de esa información, así como la conducta de los empleados de su compañía. Debe explicar claramente cualquier acto específico que se haya identificado como ataques a la seguridad y las acciones punitivas que serán tomados si se detecta un ataque a la seguridad.

Por último, crea una declaración de uso aceptable del administrador para explicar los procedimientos para la administración de la cuenta de usuario, la aplicación de políticas, y la revisión del privilegio. Si su compañía tiene políticas específicas relativas a las contraseñas del usuario o al manejo posterior de datos, también debe presentar claramente esas políticas. Verificar la política contra el uso aceptable del socio y las declaraciones de políticas de uso aceptable para el usuario para garantizar la uniformidad. Asegúrese de que los requisitos de administrador enumerados en la política de uso aceptable estén reflejados en los los planes de entrenamiento y las evaluaciones de rendimiento.

Realizar un Análisis de Riesgos

El análisis de riesgos debe identificar los riesgos a su red, los recursos de red, y los datos. Esto no significa que debe identificar cada punto de entrada posible a la red, ni los medios posibles del ataque. El intento de un análisis de riesgo es identificar las partes de su red, asignar una calificación de amenaza para cada parte, y aplicar un nivel adecuado de seguridad. Esto ayuda a mantener un equilibrio factible entre la seguridad y el acceso de la red necesario.

Asignar a cada recurso de red uno de los siguientes tres niveles de riesgo:

- Sistemas de **bajo riesgo** o datos que, de verse comprometidos (datos observados por el personal no autorizado, datos corruptos, o datos perdidos) no se interrumpiría el negocio ni causaría ramificaciones económicas y legales. El sistema objetivo o los datos se puede recuperar fácilmente y no permite el acceso adicional de otros sistemas.
- **Los sistemas de riesgo mediano** o los datos que si estuvo comprometido (los datos vistos por el personal no autorizado, los datos corrompidos, o los datos perdido) causaría una interrupción leve en el negocio, legal de menor importancia o las ramificaciones económicas, o proporcionan el acceso adicional a otros sistemas. El sistema objetivo o los datos requieren un esfuerzo leve para restaurarse o el proceso de restauración es perturbador para el sistema.
- **Sistemas de Alto Riesgo** o datos que, e verse comprometidos (datos observados por el personal no autorizado, datos corruptos, o datos perdidos) causarían una interrupción extrema en el negocio, causarían ramificaciones económicas o legales importantes, o amenazarían la integridad o la seguridad de una persona. El sistema objetivo o los datos requieren mucho esfuerzo para restaurarse o el proceso de restauración es perturbador al negocio u otros sistemas.

Asignar un nivel de riesgo a cada uno de los siguientes: dispositivos de núcleo de la red, dispositivos de distribución de redes, dispositivos de acceso a redes, dispositivos de supervisión de redes (monitores SNMP y sondeos RMON), dispositivos de seguridad de la red (RADIUS y TACACS), sistemas del correo electrónico, servidores de archivo de red, servidores de impresión de redes, servidores de aplicación de redes (DN y DHCP), servidores de aplicación de datos (Oracle u otras aplicaciones autónomas), equipos de escritorio, y otros dispositivos (servidores de impresión y equipos de fax independientes de la red).

Los equipos de red tal como switches, routers, servidores DNS, y servidores DHCP permiten acceso adicional a la red y, por lo tanto, son dispositivos de riesgo moderado o alto. También es posible que la corrupción de este equipo cause el colapso de la red. Dicha falla puede ser extremadamente perjudicial para el negocio.

Una vez asignado un nivel de riesgo, es necesario identificar los tipos de usuarios de ese sistema. Los cinco tipos más comunes de usuarios son:

- Usuarios internos de los **administradores** responsables de los recursos de red.
- Usuarios internos **privilegiados** con necesidad de mayor acceso.
- Usuarios internos de **usuarios** con acceso general.
- Usuarios externos de **socios** con necesidad de acceder a algunos recursos.
- **Otros** usuarios externos o clientes.

La identificación del nivel de riesgo y del tipo de acceso necesarios de cada sistema de red forma la base de la siguiente matriz de seguridad. La matriz de seguridad proporciona una referencia rápida para cada sistema y un punto de partida para otras medidas de seguridad, tales como crear una estrategia adecuada para restringir el acceso a los recursos de red.

Sistema	Descripción	Nivel de riesgos	Tipos de usuarios
Switches ATM	Dispositivo del núcleo de red	Alto	Administradores para la configuración del dispositivo (equipo de soporte técnico solamente); Todos los otros para usar como transporte
Routeres de la red	Dispositivo de distribución de red	Alto	Administradores para la configuración del dispositivo (equipo de soporte técnico solamente); Todos los otros para usar como transporte
Switches de armario	Dispositivo de red de acceso	Medio	Administradores para la configuración del dispositivo (equipo de soporte técnico solamente); Todos los otros para usar como transporte
ISDN o servidores de marca	Dispositivo de red de	Medio	Administradores para la configuración del dispositivo (equipo de soporte técnico solamente); Socios y usuarios con

ción rápida	acceso		privilegios para el acceso especial
Firewall	Dispositivo de red de acceso	Alto	Administradores para la configuración del dispositivo (equipo de soporte técnico solamente); Todos los otros para usar como transporte
DN y servidores DHCP	Aplicaciones de Red	Medio	Administradores para configuración; Usuarios con privilegios y generales para el uso
Servidor externo de correo electrónico	Aplicación de red	Bajo	Administradores para configuración; Todos los otros para el transporte del correo entre Internet y el servidor de correo interno
Servidor interno de correo electrónico	Aplicación de red	Medio	Administradores para configuración; El resto de los usuarios internos para el uso
Bases de datos Oracle	Aplicación de red	Moderado o alto	Administradores para la administración del sistema; Usuarios con privilegios para las actualizaciones de los datos; Usuarios generales para el acceso de datos; Todos los otros para el acceso a los datos parciales

Establecer una Estructura de Equipo de Seguridad

Crear un equipo de seguridad de funcionalidad cruzada liderado por un Administrador de Seguridad con los participantes de cada uno de las áreas operativas de su compañía. Los representantes en el equipo deben conocer la política de seguridad y los aspectos técnicos del diseño y de la implementación de seguridad. A menudo, esto requiere la capacitación adicional de los miembros del equipo. El equipo de seguridad tiene tres áreas de responsabilidad: elaboración de políticas, práctica, y respuesta.

La elaboración de políticas se centra en el establecimiento y el repaso de las políticas de seguridad para la compañía. Repase brevemente el análisis de riesgos y la política de seguridad unavez por año.

La práctica es la etapa durante la cual el equipo de seguridad conduce la análisis de riesgo, la aprobación del cambio en la seguridad pide, revisa las alertas de seguridad de ambos vendedores y de la lista de correo CERT, y da vuelta a los requisitos de la política de seguridad

del lenguaje simple en las implementaciones técnicas específicas.

La última área de responsabilidad es la respuesta. Mientras que la supervisión de red identifica a menudo una violación de seguridad, los miembros del equipo de seguridad son los que realmente realizan el troubleshooting y la corrección de dicha violación. Cada miembro del equipo de seguridad debe conocer con detalle las funciones de seguridad proporcionadas por el equipo en su área operativa.

Una vez definidas ls responsabilidades del equipo en su conjunto, debe definir las funciones individuales y las responsabilidades de los miembros del equipo de seguridad en su política de seguridad.

Prevención

La prevención se puede dividir en dos partes: cambios en la seguridad y supervisión de la supervisión de su red.

Aprobación de Cambios de Seguridad

Los cambios de seguridad se definen como los cambios al equipo de red que tengan un posible impacto en la seguridad general de la red. Su política de seguridad debe identificar requisitos de configuración de seguridad específicos, en términos no técnicos. Es decir, en lugar de definir un requisito como “Ninguna conexión al FTP de las fuentes externas se permitirá a través del firewall”, defina el requisito como “Las conexiones externas no deben extraer archivos de la red interna”. Deberá definir un conjunto único de requisitos para su organización.

El equipo de seguridad debe revisar la lista de requisitos de lenguaje sencillo para identificar la configuración de red o los problemas de diseño específicos que cumplan los requisitos. Una vez que el equipo ha creado los cambios en las configuraciones de la red requerida para implementar la política de seguridad, puede aplicarlos a cualquier cambio de configuración futuro. Mientras que es posible que el equipo de seguridad revise todos los cambios, este proceso permite que sólo se revisen solamente los cambios que plantean un riesgo importante para autorizar el tratamiento especial.

Se recomienda que el equipo de seguridad revise los siguientes tipos de cambios:

- Cualquier cambio en la configuración firewall.
- Cualquier cambio en las listas de control de acceso (ACL).
- Cualquier cambio en la configuración del Simple Network Management Protocol (SNMP).
- Cualquier cambio o actualización en el software que difiera de la lista de nivel de revisión de software aprobada.

También se recomienda cumplir con las siguientes guías de consulta:

- Cambie las contraseñas de los dispositivos de red de forma habitual.
- Restrinja el acceso a los dispositivos de red a una lista aprobada de personas.
- Asegúrese de que los niveles de revisión del software actual del equipo de red y de los entornos de servidor cumplan con los requisitos de configuración de seguridad.

Además de estas directivas de aprobación, incluya a un representante del equipo de seguridad en la junta de aprobación de administración de cambios, para supervisar todos los cambios que revisa la junta. El representante del equipo de seguridad puede negar cualquier cambio que se

considere cambio de seguridad hasta que haya sido aprobado por el equipo de seguridad.

Monitoreo de Seguridad de su Red

La supervisión de seguridad es similar a la supervisión de red, a menos que se centre en la detección de los cambios en la red que indican una violación de seguridad. El punto de partida para la supervisión de la seguridad determina cuál es la violación. En Realizar un Análisis de Riesgo, identificamos el nivel de supervisión requerido en función de la amenaza para el sistema. En Aprobación de los Cambios de Seguridad , identificamos las amenazas específicas para la red. Al considerar ambos parámetros, desarrollaremos un cuadro claro de lo que necesita para la supervisión y con qué frecuencia.

En la matriz del Análisis de Riesgos, el firewall se considera un dispositivo de red de riesgo elevado, que indica que debe supervisar en tiempo real. La sección Aprobación de los Cambios de Seguridad , especifica que debe supervisar cualquier cambio al firewall. Esto significa que el agente de la Consulta SNMP debe supervisar intentos fallidos de ingreso al sistema, tráfico inusual, cambios al firewall, acceso concedido al firewall, y configuración de conexiones a través del firewall.

Después de este ejemplo, cree una política de monitorización para cada área identificada en su análisis de riesgos. Se recomienda supervisar el equipo de bajo riesgo semanalmente, el equipo de riesgo moderado todos los días y el equipo de riesgo elevado cada hora. Si requiere una detección más rápida, supervise en un intervalos de tiempo más cortos.

Por último, su política de seguridad debe abordar cómo notificar al equipo de seguridad de violaciones de seguridad. A menudo, su software de supervisión de red será el primero en detectar la violación. Debe accionar una notificación al centro de operaciones, que a su vez debe notificar al equipo de seguridad, usando un localizador en caso de ser necesario.

Respuesta

La respuesta se puede dividir en tres partes: violaciones de seguridad, restauración, y revisión.

Violaciones de Seguridad

Cuando se detecta una violación, la capacidad de proteger el equipo de red, determinar el fragmento de intrusión, y recuperar las operaciones normales depende de las decisiones rápidas. Tener estas decisiones tomadas de antemano hace que la respuesta a una intrusión sea más factible.

La primera acción posterior a la detección de una intrusión es la notificación del equipo de seguridad. Sin un procedimiento establecido, se producirá un retraso significativo al contactar a las personas correctas para aplicar la respuesta adecuada. Defina un procedimiento en su política de seguridad que esté disponible 24 horas al día, los siete días de la semana.

Debe definir el nivel de autoridad dado al equipo de seguridad para realizar los cambios, y en qué orden deben realizarse los cambios. Las posibles acciones correctivas son:

- Implementar cambia para prevenir el acceso adicional a la violación.
- Aislar los sistemas violados.
- Establecer contacto con el portador o el ISP en un intento de localizar el ataque.

- Usar los dispositivos de grabación para obtener pruebas.
- Desconectar los sistemas violados o la fuente de la violación.
- Comunicarse con la policía, u otros organismos gubernamentales.
- Apagar los sistemas violados.
- Restaurar los sistemas según una lista prioritaria.
- Notificación al personal legal administrativo interno.

Asegúrese de detallar cualquier cambio que se pueda realizar sin la aprobación de administración en la política de seguridad.

Por último, hay dos razones para obtener y mantener información durante un ataque a la seguridad: para determinar el grado en que los sistemas se ven comprometidos por un ataque a la seguridad, y procesar las violaciones externas. El tipo de información y la manera en que la obtiene difieren según el objetivo.

Para determinar el grado de violación, haga lo siguiente:

- Registre el acontecimiento al obtener los rastros del sabueso de la red, las copias de los archivos del registro, las cuentas de usuario activas, y las conexiones de red.
- Limite el compromiso adicional al inhabilitar las cuentas, desconectar el equipo de red de la red, y desconectarlo de Internet.
- Realice una copia de seguridad del sistema comprometido para ayudar en un análisis detallado del daño y del método de ataque.
- Busque otros signos de compromiso. A menudo cuando un sistema se ve comprometido, hay otros sistemas o cuentas implicados.
- Mantenga y revise los archivos de registro del dispositivo de seguridad y los archivos de registro de la supervisión de red, ya que a menudo proporcionan pistas al método de ataque.

Si está interesado en tomar acciones legales, haga que su departamento legal revise los procedimientos para obtener las pruebas y la implicación de las autoridades. Dicha revisión aumenta la eficacia de las pruebas en los procedimientos legales. Si la violación es de naturaleza interna, comuníquese con su Departamento de Recursos Humanos.

Restauración

La restauración de las operaciones normales de la red son el objetivo final de cualquier respuesta de violación de seguridad. Defina en la política de seguridad cómo realiza, conserva, y realiza las copias de seguridad disponibles. Como cada sistema tiene sus propios medios y procedimientos para realizar copias de seguridad, la política de seguridad debe actuar como metapolítica, y detallar para cada sistema las condiciones de seguridad que requieren la restauración de las copias de seguridad. Si se requiere la aprobación antes de que la restauración se realice, también incluya el proceso para obtener la aprobación.

Revisión

El proceso de revisión es el esfuerzo final para crear y mantener una política de seguridad. Hay tres cosas que debe revisar: política, postura, y práctica.

La política de seguridad debe ser un documento dinámico que se adapte a un entorno evolutivo. El repaso de la política existente contra las mejores prácticas conocidas mantiene la red actualizada. También, marque el sitio web CERT para los consejos útiles, las prácticas, las mejoras de la Seguridad, y las alertas que se pueden incorporar en su política de seguridad.

También revise la postura de la red en comparación con la postura de seguridad deseada. Una empresa externa que se especializa en la seguridad puede intentar penetrar en la red y probar no sólo la postura de la red, sino también la respuesta de seguridad de su organización. Para las redes de gran disponibilidad, se recomienda realizar dicha prueba anualmente.

Finalmente, la práctica se define como un ejercicio o una prueba de equipo de soporte técnico para asegurar que tienen los conocimientos necesarios durante una violación de seguridad. A menudo, este ejercicio no es notificado por la administración y se realiza conjuntamente con la prueba de postura de la red. Esta revisión identifica los intervalos en los procedimientos y la capacitación de personal para tomar la acción correctiva.

Información Relacionada

- Más informes de mejores prácticas
- Soporte Técnico - Cisco Systems