



arroba peru.com

Soluciones Integrales en: Servidores, Pcs, Laptops y Redes

EVALÚE LA SEGURIDAD DE SU RED EN 11 PASOS

En el presente trabajo, los expertos de seguridad de Watchguard le ofrecen preguntas y ejercicios que puede usar para comprobar del estado de la Seguridad de su corporación en las siguientes áreas: Seguridad en los Mensajes, Seguridad Física, Aspectos operacionales y Cumplimiento de Políticas. Estos ejercicios pueden ayudarle a obtener datos concretos sobre como se preparó su organización para responder a inesperados casos de urgencias en la red. Cada ejercicio requiere muy poco tiempo y preparación, pero es una práctica valiosa. La ejecución de estas pruebas no sólo le ayudará si alguien le pregunta sobre su gestión de la Seguridad; sino que le mostrará como hacer su más resistentes sus defensas.

Hemos estructurado los escenarios de prueba de modo que pueda hacerlos todos o sólo algunos de ellos, en cualquier secuencia, como su agenda lo permita, y aún así obtenga resultados significativos. Usando este proceso, tendrá una idea de primera mano sobre el estado real de la preparación de sus empleados. Si quiere mantener a su personal informático alerta, trate de sorprenderlos con una de estas pruebas cada mes, para comprobar en caliente si sus medidas de seguridad generan verdadera protección.

Seguridad de los mensajes

1. ¿Cuánto le cuestan los mensajes de correo electrónico spam?

(Tiempo estimado para completar: 5 minutos. Esta y todas las siguientes estimaciones se refieren a su tiempo y no incluyen el de su personal).

Calcule esta fórmula para averiguarlo:

$(n \times 15) \times E \times A = \text{costo del trabajo}$

Multiplique el número de mensajes spam que usted personalmente recibe cada día (n) por los 15 segundos que tarda para identificar a cada uno como spam y desecharlo, por el número de Empleados en su organización (E) por el Promedio del costo horario de un empleado (A).

El resultado le indica cuanto le cuesta el spam a su empresa sólo en tiempo.

Ejemplo: asumiendo que usted personalmente recibe 30 mensajes spam por día, que el salario promedio de un empleado por hora es 37 dólares y que hay 200 empleados en su empresa:

30 mensajes

x 15 segundos

450 segundos (dividir por 60 segundos para convertir a minutos) =

7.50 minutos

x 200 empleados

1,500 minutos (dividir por 60 minutos para convertir a horas) =

25 horas

x 37 dólares promedio del salario por hora

TOTAL: 925 dólares de costo diario por spam, además de los recursos que consume de su red, como por ejemplo la cantidad de espacio de almacenamiento en el servidor de correo electrónico.

Esto aumenta los costos de hardware y mantenimiento debido a que su sistema de correo electrónico tiene que manejar tanto los mensajes necesarios como el correo basura antes de desechar este último.

Costos adicionales: una red en la cual los empleados reciben mucho spam se muestra como que tiene una protección poco profesional. Su inhabilidad para filtrarlo puede exponerlo a reclamos como el de "crear un ambiente de trabajo hostil".

Claramente, el spam es más que una molestia. Spam y virus comienzan a converger en nuevas formas de afectar a las personas. Si el cálculo que hicimos lo preocupa, pida su personal informático que investigue qué opciones puede aplicar para tratar con el spam de manera más agresiva. El WatchGuard SpamScreen podría ser la parte de su solución.

Seguridad Física

2. ¿Sus empleados son una ayuda o una dificultad para la Seguridad Física?

(Tiempo estimado para completar: 15 minutos para arreglarlo)

Una lista de un correo electrónico para consultores describe una empresa en la que se habían instalado nuevos dispositivos de Seguridad, imponentes biométricos sobre las puertas externas, incluyendo escáneres de retina y de huella digital. La organización contrató a un consultor para ver si podía derrotar las nuevas medidas. El experto comenzó recorriendo el estacionamiento y observando donde se reunían los fumadores de la empresa. Al día siguiente se unió a los empleados fumadores en su descanso, luego los siguió y alguien le sostuvo la puerta abierta para que pasara.

Para ver si su instalación es vulnerable a este tipo de "ingeniería social", préstele ropa con el logotipo de su empresa a un compañero de golf que sus empleados no conozcan. Haga que camine por la sala de su LAN y otras áreas sensibles luciendo el logotipo. Fíjese hasta donde llega. Asegúrese darle una tarjeta "que lo saque de la cárcel" en caso de que algún empleado cuidadoso lo detenga y denuncie. Recompense públicamente al empleado que detuvo al intruso.

3. ¿Aplicó MBWA al centro de cómputos?

(Tiempo estimado para completar: 5 - 20 minutos)

Muchos presidentes de primera clase elogian el valor del "MBWA" (Management By Walking Around – Dirigir Caminando Alrededor), esto es caminar por el centro de cómputos y comprobar cualquier problema obvio. Cosas a buscar:

-¿Fue cerrada la puerta? Debería estarlo. Los centros de cómputos no son un lugar para visitantes ocasionales. La cantidad de gente que realmente necesita acceder es poca. La lista permanente sólo debería incluir al responsable del mismo y al personal informático específico que realiza tareas en él. Otras personas pueden ser añadidas temporalmente cuando sea necesario, pero hay que asegurarse de eliminarlos de la lista en cuanto la necesidad haya pasado.

-¿Está organizado y etiquetado el cableado? Un cable sin etiquetar puede ser confundido con algo sin importancia, y sin querer puede ser desconectado y dejar sin servicio a un segmento de la red. Su personal también puede perder mucho tiempo si, cuando tienen que mover un dispositivo, deben revisar un enredo de espaguetis eléctricos. Además, cables mal colocados pueden crear un riesgo de corto circuito o provocar que un circuito se sobrecargue. Los precintos plásticos y otros organizadores de cables ayudan, son baratos y proporcionan un ROI excelente.

-¿Etiquetan a sus servidores? Su personal de IT probablemente pueda decirle exactamente lo que hace cada servidor, que sistema operativo tiene, si sus parches están al día, etcétera. Pero los casos de urgencia no siempre ocurren cuando su mejor equipo está de turno. Si su personal no está disponible en un caso de emergencia, un consultor u otro personal externo, consumirán mucho tiempo facturable tratando de entender su sistema. Se debería etiquetar a cada servidor por su función. Además (si ellos no lo hacen ya), pídale a su personal informático que mantenga un archivo log que registre los cambios que realizan sobre él. Esto facilita el proceso de resolución cuando alguien hace un cambio errado, o se detectan síntomas de un cambio sin autorización.

- ¿Requieren los salvapantallas del servidor una contraseña? Algunas veces los administradores deben estar logueados a un servidor durante algún tiempo, pero si el equipo está desatendido, una persona no autorizada puede destruir o robar datos de su empresa. El mejor modo de asegurar el servidor en estos casos, es instalar un salvapantallas que se active automáticamente después de unos minutos sin actividad de teclado y mouse, y requiera de una contraseña antes de volver a permitir el acceso.

-¿Siente frío o calor? Las salas de servidores generan mucho calor. El calor es malo para las computadoras. Si los servidores se calientan demasiado, pueden apagarse o resetearse. Si usted se siente fresco cuando usted está en la sala, todo está bien. Si no, investigue la forma de enfriar la sala. Si su centro de cómputos es solamente un armario, al menos asegúrese que haya ventilación.

-¿Dónde están las cintas de backup? Si todas sus cintas de backup están en una sala, lo que le pase a esa zona también le pasará a las cintas. Usted querrá que al menos un backup semanal sea almacenado fuera del sitio. La falta de presupuesto no es una excusa. Puede tener un empleado de confianza que se lleve un juego de cintas a casa y lo almacene en una caja fuerte incombustible. O mejor todavía: encuentre el presupuesto y contrate el servicio de una empresa especializada en el almacenamiento de cintas y documentos de confianza. A propósito, ¿han intentado recientemente restaurar los backups para verificar si realmente trabajan? Asegúrese de preguntarlo y comprobarlo.

- ¿Tienen respaldo las computadoras críticas para el negocio? Para determinar si su red tiene un punto único de falla, durante un período de poca demanda operativa, desconecte un servidor de la red y vea que pasa. No

haga esto a la ligera, sino como parte de un plan que puede darle valiosa información sobre si sus medidas de continuidad de negocio realmente funcionan.

Aspectos Operacionales

3. ¿Realizó recientemente una evaluación de vulnerabilidades? ¿Qué encontró?

(Tiempo estimado para completar: 60 minutos)

Para un atacante, su red es simplemente un objetivo de oportunidad; para usted, es la sangre vital de su negocio. ¿No tiene sentido conocer al menos tanto sobre los puntos débiles de su red como su atacante? Pida a su CIO un listado de la última evaluación de vulnerabilidades, con una descripción verbal de los resultados. Si usted quiere comprobar si el área de IT está lista, convoque al CIO a una reunión sin aviso previo -después de todo, los hackers no dan un preaviso de sus ataques. Un CIO que mantiene un conocimiento actualizado del estado de su red, no debería tener ningún problema que responder sus preguntas.

El gusano Código Rojo (que tuvo un impacto estimado de 2.62 mil millones de dólares sólo en Estados Unidos) y el gusano SoBig (con un daño mundial estimado en los 29.7 mil millones de dólares) explotaron agujeros de seguridad conocidos en aplicaciones comunes. Como secuela dejaron a algunas organizaciones con sus servidores fuera de línea durante días. Lo patético: los parches que solucionaban estos agujeros estuvieron disponibles semanas antes de los ataques. Si analiza su red semanalmente con un detector de vulnerabilidades como el Watchguard AuditScan, el informe de evaluación le servirá como un recordatorio automático para mantener sus parches al día. Demasiado a menudo la gestión de parches cae víctima de la lucha de "urgente contra importante". Si su escáner de vulnerabilidades muestra banderas rojas, evalúe y parchee proactivamente.

5. ¿Cuándo fue la última vez que se actualizó su antivirus?

(Tiempo estimado para contestar: 4 minutos)

Cada virus o gusano programado hasta ahora tiene algún segmento de código único que sólo se encuentra en él. Los vendedores de antivirus se refieren al modelo reconocible en el código como "firmas". Los vendedores de antivirus analizan cada virus nuevo y añaden su firma a su software, de modo que pueda descubrir nuevos ataques.

Todos los principales vendedores de AV liberan nuevas firmas al menos de manera semanal, pero esto le ayudará a usted sólo si las firmas llegan a su software de antivirus. Averigüe de cuando son las últimas firmas instaladas en su red. Si estas tienen más de una semana, el programa de actualización automática probablemente no funciona. Haga que alguien lo examine. Si sus empleados se conectan a la red corporativa desde sus casas o desde otras redes, es vital que todos sus sistemas sean protegidos con las firmas más actualizadas.

6. ¿Qué puede aprender de los logs de firewall?

(Tiempo estimado para completar: 25 minutos)

Pida a su experto en firewall que le traiga los últimos logs y le explique lo que dicen. Pregunte:

"¿Qué entrada registra este log? (elijas unas cuantas al azar).

Para investigar los datos sobre ataques - "¿Qué ataques han sido rechazados esta semana?"

"¿Durante cuánto tiempo se conservan los archivos de logs? ¿Cuando el espacio de disco rígido asignado a los logs se llena, qué hace el sistema?"

Una configuración típica le permite al dispositivo de sobreescritura superponer las entradas más nuevas sobre las más viejas. ¿Es esto lo que usted quiere y es compatible con su Plan de Resguardo de Documentos?

Asegúrese que entiende lo que su personal dice sobre los ataques que su firewall rechaza. Si ellos pueden explicárselo de manera que tenga sentido, todo está bien. Si no, quizás su personal necesite más capacitación en el análisis de logs. Quizás deba invertir dinero en un instrumento (o hacer un uso mayor del que ya tiene) que le ayude a darle sentido a sus datos.

El análisis de logs puede ser complejo y aburrido, pero también es vital, porque le indica lo que su red afronta. Anime a su personal a supervisar los logs con regularidad y adecuadamente. Piense en repasar los logs con ellos esporádicamente, mantenga su atención sobre la defensa de la red y motive al personal para que esté atento.

7. ¿El acceso es a esos sitios Web inútiles está bloqueado?

(Tiempo estimado para completar: 10 - 20 minutos)

Abra su navegador de Web, vaya a su motor de búsqueda favorito, y busque un sitio de juegos, uno de odio, algunos de vídeo y música, o algo que no tenga ninguna relación legítima con su negocio. Trate de tener acceso a algunos de estos sitios. ¿Puede abrirlos?, ¿por qué no están bloqueados?

Con los accesos ubicuos a Web, es fácil para los empleados "ciberharaganear". Por lo general se puede supervisar esto analizando la productividad de empleado. Pero debido a responsabilidades legales, algunos sitios nunca deberían ser accesibles desde la red corporativa. Incluso en los ambientes más permisivos, usted se enfrenta a riesgos por no controlar el acceso a los contenidos Web. Quizás es hora de tomar medidas más fuertes.

Mientras lo piensa, pregúntele al departamento de IT cuales son los cinco sitios más visitados por la gente de su empresa y quienes son los cinco primeros surfistas de Web. ¿Le sorprenden los resultados? Si piensa que su empresa tiene un problema de ciberharaganeo, el software de filtrado de contenidos y el WebBlocker de los firewalls de WatchGuard le ayudarán a saber y controlar, quién navega y donde.

8. ¿Puede descargar e instalar a un cliente P2P?

(Tiempo estimado para completar: 15 - 25 minutos)

Napster fue una de las primeras redes peer-to-peer; hoy las principales son servicios como Limewire y KaZaA, conocidos principalmente como una fuente gratuita de archivos de música. Si puede descargar los archivos satisfactoriamente e instalar uno a través de su firewall, sus empleados también pueden hacerlo.

Es difícil detener las conexiones P2P debido a que están diseñadas para atravesar los firewalls enmascaradas como como tráfico legítimo de Web. Si permite que los clientes sean descargados e instalados, rastrear y detener el tráfico será difícil.

Como con la mayoría de los comportamientos de red indeseables, el mejor modo de manejarlo es primero con una política (ver los puntos 10 y 11) y luego usando la tecnología para rastrear el cumplimiento.

P2P se ha convertido en una carrera armamentista entre la gente que las usa y los que quieren detenerlas. Asegúrese que su empresa no quede en medio de la batalla.

9. ¿Cuándo fue la última vez que el sistema le pidió que cambiara su contraseña?

(Tiempo estimado para completar: 3 minutos)

Si no le han obligado a cambiarla en más de 90 días, pregunte por qué. El robo de contraseña es el modo más fácil y más directo de tener acceso a su información. Usted está expuesto al riesgo de que alguien le robe su identidad en la red si tiene:

- Una contraseña débil
- Una contraseña que pocas veces se cambia
- Una contraseña escrita sobre papel

Hay muchas maneras fáciles y poco costosas de hacer cumplir con los cambios de contraseña a intervalos razonables; algunos forman parte del sistema operativo de las computadoras. Pida a su área de IT que investigue como cumplir con una política que requiera contraseñas complejas con cambios regulares (WatchGuard recomienda cada 45-90 días). En general, el modo más fácil de elegir una contraseña fuerte y fácil de recordar es de usar una passphrase en lugar de sólo una password.

Cumplimiento de la Política

10. Pida que se repase su Plan de Continuidad de negocio, el Plan de Retención de Documentos, el Plan de Recuperación de Desastres y la Política de Seguridad.

(Tiempo estimado para completar: 2 horas)

Cualquier mejora que usted haga después de una prueba no resistirá el paso del tiempo, a no ser que la haya escrito en la política. Si no tiene una política de seguridad escrita, anime a su personal informático a bosquejar una para comenzar a discutir (ellos probablemente hayan querido hacerlo desde hace algún tiempo). Ofrezca patrocinar las reuniones de aprobación si fuera necesario. No deje que el proceso se atasque en complejidades; esta versión sólo tiene que ser el comienzo. Recuérdele a su equipo que tener una política "bastante buena" ahora es mejor que tener una política "perfecta" nunca. Revísela otra vez en seis meses. Evalúe sus necesidades verdaderas y adecúe sus esfuerzos a esas necesidades.

¿Cómo comenzar? Comience con un resumen de un párrafo de lo que su empresa desea lograr con sus recursos de IT y fije el objetivo de tener un borrador inicial de 1-2 páginas listo para la discusión con un grupo más grande de ejecutivos y una selección de usuarios finales dentro de una semana. Compruebe el SANS Security Policy y copie lo que considere conveniente conveniente -el 90 % de las cuestiones de seguridad son

comunes a todas las organizaciones.

Para esfuerzos como estos, es útil conseguir una perspectiva exterior. Piense en contratar a un experto y asegúrese de que esté familiarizado con las regulaciones relevantes a su negocio.

**11. ¿Usted es una excepción a la política de seguridad de su empresa?
(Tiempo estimado para contestar: 2 minutos)**

Responda honestamente. El personal informático necesita su apoyo para mantener la organización segura. Los empleados no desarrollarán una mentalidad a favor de la seguridad si usted no se adhiere personalmente a la política. La "seguridad" y la "operatividad" son como una balanza: si uno sube, el otro baja. El objetivo de la seguridad de la red no es la seguridad para el bien de la seguridad.

El objetivo es la seguridad que apoya su misión de negocio. Esto puede requerir de algunos ensayos hasta encontrar el equilibrio entre la seguridad y la operatividad, pero persista en el proceso. Si la política es inviable, y usted la abandona, sus empleados también lo harán. Obtendrá más protección de una política equilibrada que se pueda cumplir, que de una política estricta que sólo exista sobre papel.

CONCLUSIONES

El secreto de la seguridad de la red consiste en que no es la ciencia compleja. La implementación de medidas de seguridad tecnológicas es algo realmente especializado, pero los principios básicos son inteligibles a alguien que controla un negocio. Como un líder, usted tiene el poder de influir en como su empresa dirige las cuestiones de seguridad.

En realidad, unos cambios simples en el comportamiento, un poco de esfuerzo invertido en la documentación de esos cambios y una pequeña dosis de dominio de sí mismo es todo lo que se necesita para mejorar como su organización pone en práctica la seguridad de la red.

La mayor parte de los expertos le dirán que la verdadera seguridad es la responsabilidad de cada persona sobre la red. Esto es verdad. Sin embargo, si la red es violada, los clientes, los accionistas, y los miembros del directorio no culparán al empleado que descarga archivos de música. Ellos le pedirán explicaciones a usted.

Haga algunas preguntas y exija algunas respuestas. Los resultados le ayudarán a conducir una organización capaz de manejar los problemas de seguridad no sólo en la teoría sino también en la práctica.