expositor 2

14 siguiendo con los pasos, el siguiente Verificar que el firewall esté activo y revisar las prácticas de administración del firewall.

Como bien sabemos corta fuegos protegen el sistema de conexiones de red inesperadas.  Si no se usa un, puede aumentar el riesgo de que una amenaza maliciosa obtenga acceso a un sistema del cliente final.

Para evitarlo ha que verificar que el firewall este activo y correctamente configurado, ques lo que no explica puntualmente este paso.

en Windows, acceder al panel de Seguridad y Mantenimiento o,en su lugar, a la aplicación Windows Defender Security Center aquí se indica el estado del firewall de Windows. Si la organización utiliza un firewall de terceros, como los que se proporcionan con muchos programas antivirus, el estado debería aparecer en los mismos paneles de Windows.

Ahora en sistemas Mac, se selecciona la aplicación Preferencias del sistema, luego el icono de Seguridad y privacidad y Cambie al panel de Firewall aquí se describirá el estado del firewall.

Se debe recordad que los firewalls deben configurarse para bloquear la mayoría del tráfico entrante.

bien sabemos los cortafuegos protegen el sistema, en este caso al sistema del cliente final, de conexiones de red inesperadas. Si no se usa un firewall, puede aumentar el riesgo de que una amenaza maliciosa

15 **debemos revisar los requisitos de registro del cliente y la configuración.**

El registro apropiado del cliente puede ayudar a las operaciones y a los equipos de seguridad a detectar problemas con los sistemas del cliente.

**Esto con ayuda de los sientes pasos, el primero**

Revisar las políticas relacionadas con el registro, para determinar si existen requisitos para el registro del cliente. Muchas empresas optan por limitar el uso de la recopilación centralizada de registros del cliente, debido a la cantidad de clientes, el tamaño de los datos de registro que se capturarán, o el potencial impacto en la red de las transferencias de registros. .

1. Si las políticas de registro de la empresa tienen requisitos para los sistemas del cliente, hable con el equipo de administración del cliente.
2. Solicite ver la configuración de registro, en las herramientas de administración del sistema en uso. Si los registros se reenvían a un sistema central, se debe solicitar al equipo de supervisión que proporcione una muestra de registros de clientes.

**16. como siguiente paso Revisar el proceso de parcheo para el sistema operativo y las aplicaciones clave**.

Si el sistema operativo aplicable y los parches de software no están instalados, obviamente podrían existir vulnerabilidades de seguridad ampliamente conocidas en el cliente, lo que permite explotaciones dañinas de amenazas externas.

**Para mitigar estos riesgos tenemos**

Parches para el sistema operativo

Tanto Microsoft como Apple lanzan parches para el sistema operativo y las aplicaciones clave periódicamente, al igual que muchos proveedores de software de terceros. La organización debería tener un proceso para evaluar la aplicabilidad de los parches y su crítica resultante.

Además de esto los equipos deberían ser capaces de proporcionar evidencia de análisis de los lanzamientos de parches más recientes de Microsoft o Apple……. como mínimo.

Garantizar que se se reciban los parches e informar el hecho:

Se debe someter a discusion el momento de la instalación de parches y los procesos, para garantizar que todos los clientes relevantes reciban los parches esperados y las empresas deben tener informes u otras métricas disponibles, que describan el estado del parche de los clientes. Estas metricas las podemos verificar, seleccionando un sistema cliente al azar; puede usar el propio sistema de la empresa para este paso si así lo prefiere. en la aplicación Windows Update, mostrará el estado del sistema y un enlace para ver el historial de instalación reciente. El historial debe mostrar la actividad de instalación reciente, particularmente en Actualizaciones de calidad.

En macOS, la aplicación Acerca de esta Mac, accesible a través del menú Apple, en Informe del sistema encontrara una seccion llamada Instalaciones en Software en la cual al seleccionar la columna Fecha de instalación se puede observar la información de instalación.

Algunas organizaciones pueden habilitar actualizaciones automáticas de Windows y Mac para sus sistemas, pero otras administrarán las actualizaciones cuidadosamente para garantizar la compatibilidad con el software de la compañía.

**17. Verificar que la pantalla se apagará automáticamente después de un intervalo establecido y requerirá una contraseña para reanudar.**

Cualquier persona que se acerque a la computadora puede usar una sesión de trabajo desatendida. por tanto un tiempo de espera de pantalla reduce este riesgo.

**Para lograrlo en ambos sistemas operativos haremos lo siguiente:**

En Windows 10, se puede encontrar la configuración para el tiempo de espera de la pantalla en la aplicación Configuración del protector de pantalla.

Esto debe establecerse en un tiempo que coincida con su política de seguridad, que se pudo observar en una tabla anterior, pero preferiblemente una breve duración, como cinco o diez minutos.

En macoS, se necesitan varios pasos para verificar este elemento. Primero, abrir la aplicación Preferencias del sistema. A continuación, seleccionar el icono Escritorio y protector de pantalla. Debajo de la pestaña Protector de pantalla , luego, darle clic en la flecha hacia atrás en el mismo panel para volver a preferencias del sistema elegir el icono de Seguridad y privacidad.

En ambos sistemas operativos se debe recalcar como norma General, la opción "Requerir contraseña después de que el sueño o el protector de pantalla comience" debe estar marcada.

**18. Asegúrese de que AutoPlay y AutoRun estén deshabilitados para dispositivos extraíbles**.

En Windows, AutoPlay y AutoRun lanzarán automáticamente ciertos tipos de archivos al insertar una unidad USB, CD / DVD u otros medios.

Si estas características están habilitadas, un archivo malicioso puede ejecutarse sin que un usuario realice ninguna acción específica.

Los sistemas Mac no ejecutarán automáticamente archivos en unidades USB, pero los sistemas con unidades ópticas pueden reproducir CD o DVD automáticamente.

**Para evitarlo se debe**

dialogar con el equipo de administración del cliente para determinar si AutoPlay y AutoRun están deshabilitados. Ambos se pueden ajustar a través de GPO en Windows. Ahora en sistemas Mac, La mayoría de las estas modernas ya no se envían con unidades ópticas, por lo que esto puede no ser un problema en algunos entornos.

**Ahora entraremos a la segunda parte del capitulo que es Auditar dispositivos móviles**

los Conceptos básicos de la auditoría de dispositivos móviles

Conceptualmente, auditar un entorno de dispositivo móvil que engloba teléfonos inteligentes y tabletas es bastante similar a auditar computadoras de escritorio y portátiles.

Sin embargo, la complicación es que un celular o dispositivo movil es un aparato mucho mas persona, este el factor más importante en el espacio móvil; junto con algunas diferencias en la tecnología, basados en estas diferencias se justifica que sea una auditoría separada.

Hay algunas preguntas básicas que debe considerar como auditor al evaluar un programa de dispositivo móvil. Algunos de estos incluyen

¿A qué recursos de la compañía pueden acceder los dispositivos móviles?

• ¿Cómo se protegen los datos de la empresa en dispositivos móviles?

• ¿Cómo maneja la empresa los dispositivos y aplicaciones personales?

• ¿La empresa está considerando el riesgo de los dispositivos móviles emergentes como los wearables?

Si presta atención, todas alrededor de los intereses de la empresa.

**El primer paso es**

1. **Revisar las políticas de la compañía sobre dispositivos móviles y asegúrese de que la propiedad del dispositivo y las responsabilidades del usuario estén cubiertas**.

Establecer una política sobre la propiedad del dispositivo es un paso clave para empresas que se ocupan de sistemas de clientes. Esto también es importante para dispositivos móviles. Este paso garantiza que la organización haya considerado estos problemas y haya proporcionado información adecuada a los usuarios finales.

Para ello deebe

obtener una copia de la política de dispositivos móviles de su empresa, si existe, así como las políticas relacionadas con el uso de dispositivos de propiedad personal o ajenos a la empresa. La política debe definir claramente cómo se pueden usar los dispositivos móviles y cómo se deben manejar los dispositivos móviles personales. Debería esperar que una política de dispositivos móviles aborde a qué recursos pueden acceder los dispositivos móviles, cualquier estándar mínimo o configuración para el dispositivo, cómo responderán el empleado y la compañía si el dispositivo se pierde o es robado, y las expectativas puestas en el empleado

.Si la su empresa permite dispositivos de propiedad personal, la política móvil también debe abordar las preocupaciones relacionadas con la privacidad en torno a la ubicación del dispositivo, las aplicaciones personales y los gastos personales. Debe verificar que el lenguaje de la política o los acuerdos de los empleados sobre privacidad se hayan desarrollado en conjunto con los equipos legales y / o de privacidad de su empresa.

**2. Asegurarse que la organización tenga una infraestructura EMM ( que significa Gestión de Movilidad Empresarial ) acorde con los objetivos de la política y la estrategia de la empresa**.

Los sistemas de gestión de movilidad empresarial permiten a las organizaciones rastrear el inventario de dispositivos, administrar software, aplicar políticas de seguridad y más. Este paso evalúa la existencia y el alcance de los sistemas EMM. Si la administración de dispositivos no está implementada, es posible que la compañía no pueda proteger y proteger adecuadamente los activos y datos de la compañía.

Se debe discutir los sistemas EMM con los administradores de dispositivos móviles. Tanto Google como Apple controlan de cerca cómo interactúan los sistemas EMM con dispositivos que ejecutan Android e iOS, y las capacidades básicas para la mayoría de las soluciones EMM son muy similares.

Se debe esperar que cualquier solución pueda, como mínimo, poder facilitar las siguientes funciones clave:

-Proporcionar visibilidad al inventario de dispositivos móviles para la empresa.

-Proporcionar información sobre el tipo de dispositivo y la versión del sistema operativo. -Controles de aplicaciones de soporte, incluida la capacidad de bloquear aplicaciones específicas

- Aplique políticas de seguridad y de configuración del sistema a los dispositivos administrados

- Limpie los dispositivos de forma remota cuando se pierdan, sean robados o ya no sean necesarios

**3. Asegurar que los dispositivos móviles estén configurados para requerir un PIN o código de acceso para acceder al dispositivo y revisar otras configuraciones relacionadas con el PIN / código de acceso**.

Si el acceso a dispositivos móviles no está protegido, los datos de la empresa podrían quedar expuestos si una persona no autorizada toma posesión de un dispositivo.

Esto puede evitarse

Discutiendo los requisitos del código de acceso, incluida la longitud mínima del código de acceso, los requisitos de cambio de código de acceso, la compatibilidad con métodos de desbloqueo alternativos como el reconocimiento facial y las funciones de borrado automático. Estos diferirán según la compañía según la tolerancia al riesgo, pero una práctica estándar es requerir un código de acceso de seis caracteres con cambio anual, borrar automáticamente el teléfono después de diez intentos fallidos de código de acceso y permitir la autenticación facial o de huellas digitales.

Esto se debe configurar de la siguiente manera

en dispositivos ios, en Configuración, luego Touch ID , & Passcode o Face ID & Passcod, según el modelo del dispositivo, y desactivar la contraseña. Esto debería estar atenuado y no seleccionable para un dispositivo administrado.

Para la mayoría de los dispositivos Android, en Configuración, luego Pantalla de bloqueo y Seguridad de pantalla. Las opciones para eliminar los diferentes métodos de código de acceso, incluido el patrón o el desbloqueo basado en PIN, deben estar en gris para los dispositivos administrados.

Los diferentes modelos de dispositivos basados ​​en Android pueden tener opciones de menú ligeramente diferentes; Si no puede encontrar la configuración, hable con su equipo de movilidad.

**4. Asegúrese de que se aplique el cifrado del dispositivo.**

un dispositivo móvil sin cifrar podría revelar información confidencial a alguien que obtenga la posesión física del dispositivo.

la mayoría de las soluciones de EMM pueden verificar el estado de cifrado del dispositivo y permitir o denegar el acceso a los dispositivos en función del resultado. Discutir eso con los administradores de movilidad.

Desde el lanzamiento de iOS 8, Apple ha incluido el cifrado del dispositivo por defecto para iPhone y iPad. El único requisito previo es establecer una contraseña para el dispositivo. También puede verificar el estado del dispositivo en el panel Touch ID & Passcode. En parte inferior la pantalla debe indicar "La protección de datos está habilitada".

Para Android, el cifrado también es una configuración predeterminada que comienza con la versión Nougat. Sin embargo, esto se puede deshabilitar para algunas versiones de Android en la aplicación Configuración y luego en Seguridad. Una opción de cifrado debe indicar si el dispositivo está cifrado.

**5. Asegúrese de que los dispositivos se bloqueen automáticamente después de un período establecido.**

Cualquiera puede acceder a un dispositivo desatendido sin la necesidad de un código de acceso u otra autenticación. Un temporizador de bloqueo de pantalla puede reducir el riesgo de robo de datos u otra actividad maliciosa.

Para ello

Se habla con el equipo de movilidad para asegurarse de que esta configuración esté configurada en la política de EMM para dispositivos móviles administrados.

Para verificar esta configuración en ioS, puede verificar la Configuración en el Panel de visualización y brillo revisando la configuración de bloqueo automático. Los administradores de EMM pueden establecer un máximo tiempo permitido, y el usuario puede seleccionar un tiempo más corto si lo desea. La opción Nunca no debería estar disponible. En Android, el tiempo de espera de la pantalla se administra en Configuración y luego en Pantalla. La configuración de suspensión indica cuánto tiempo permanecerá encendida la pantalla.

**6. Revise los procesos para mantener actualizados los dispositivos móviles.**

Los sistemas operativos obsoletos o sin parches pueden exponer vulnerabilidades de seguridad que podrían aprovecharse para acceder a datos confidenciales personales o de la empresa o cuentas de correo electrónico de la empresa, por lo que este paso verifica que la organización tenga un plan para mantener una postura de seguridad del dispositivo móvil.

Revisar actualizaciones de seguridad…se anuncian regularmente las vulnerabilidades tanto en i0S como en Android, y Apple y Google lanzan frecuentemente actualizaciones de seguridad. Además, ambas compañías suelen lanzar una nueva versión de su sistema operativo cada año. Sin embargo, las rutas de actualización para sus dispositivos difieren. La naturaleza cerrada del entorno de Apple significa que Apple determina qué versiones de hardware son compatibles con qué versiones de software, y los dispositivos compatibles pueden actualizarse rápidamente tras el lanzamiento de un Nueva versión de iOS. Sin embargo, para Android, que históricamente permite a los fabricantes y operadores de dispositivos personalizar el sistema operativo para sus necesidades, las actualizaciones y parches tardan mucho más en implementarse, y en muchos casos, los parches y actualizaciones no se emiten incluso para modelos de teléfonos o tabletas muy recientes. .

Debe analizar los riesgos de los diversos sistemas operativos con su equipo de seguridad y determinar si el equipo de movilidad ha implementado restricciones sobre qué versiones pueden conectarse a los recursos de la empresa.

Una buena practica \*\*\*\*\*\*\*\*leer ultimo punto\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* en este caso el equipo de movil debería poder proporcionar un inventario de dispositivos administrados por versión.

**7. Revise los procesos para borrar o recuperar dispositivos en caso de que uno se pierda, sea robado o reemplazado o si el empleado es despedido**.

Cuando un dispositivo se pierde, es robado o reemplazado, aún puede contener datos confidenciales. Aunque pueden existir otras salvaguardas destinadas a proteger esta información,

Las empresas deben tener procesos para retirar dispositivos de forma segura y eliminar los datos de la empresa.

Cómo

investigar los pasos involucrados en el caso de un dispositivo móvil perdido o robado. Las personas que pierden un dispositivo pueden sentirse avergonzadas o temer una acción disciplinaria o sanciones financieras por perder un dispositivo, pero es importante que los empleados puedan denunciar libremente un dispositivo perdido o robado al personal apropiado. Dichos informes pueden llegar a equipos de seguridad física, equipos de seguridad de la información o equipos de movilidad, pero la organización debe tener un proceso para notificar al equipo de movilidad que se ha perdido un dispositivo.

Si el dispositivo se enciende y está dentro del alcance de una señal portadora o está conectado a una red inalámbrica con capacidad de Internet, debería recibir la señal de borrado. Las empresas también deben tener procesos para manejar las terminaciones de empleados. Para los dispositivos propiedad de la compañía, asegurarse de que las listas de verificación de salida de los empleados incluyan la recuperación del dispositivo. En el caso de los dispositivos propiedad de los empleados, los procesos de terminación de los empleados deben incluir una eliminación parcial o total del dispositivo. Un borrado parcial elimina solo los datos y las aplicaciones de la empresa, dejando intactos los datos personales.

Y un ultimo paso

**8. Revisar las opciones adicionales para la protección de los datos de la compañía en el dispositivo**.

Este paso cubre consideraciones adicionales de protección de datos para dispositivos móviles en implementaciones comerciales típicas.

Debe revisar la configuración del acceso al correo electrónico para usuarios móviles, especialmente si su empresa utiliza un sistema en la nube como Office 365 o G-Suite de Google. Asegúrese de que cualquier disposición para la terminación de los empleados también incluya la terminación de su acceso móvil a los sistemas de correo electrónico basados ​​en la nube

Para cualquier uso de aplicaciones móviles para el trabajo, debe analizar cómo se protegen los datos de la empresa., Las aplicaciones móviles utilizadas para los negocios de la empresa se han desplegado a través del sistema EMM, optado como mejor practica. Esto permite a la compañía revocar el acceso a la aplicación y sus datos si es necesario y establecer controles sobre lo que se puede hacer con los datos en el dispositivo.