Seguridad de dispositivos móviles: Cómo convertirse en un guerrero ninja frente a los hackers

¿Cuántos dispositivos móviles entraron en la red de su empresa la semana pasada?

Es imposible determinarlo salvo que conozca las direcciones MAC. Es muy probable que algunos iPhones lo hicieran y tal vez, algunos iPads, Blackberries o equipos Android.

A medida que aumenta la fascinación de los usuarios por la conectividad de los dispositivos portátiles, también aumentan los riesgos de seguridad para los datos y las redes empresariales. Los cibercriminales se dirigen cada vez más a los dispositivos y las aplicaciones móviles. Según pronósticos de Gartner Inc., dentro de los próximos tres años, el 90% de las organizaciones de TI admitirán aplicaciones empresariales en dispositivos personales móviles.

¿Cómo puede proteger a su empresa contra los ataques de hackers y software malicioso procedentes de dispositivos móviles?

A continuación mencionamos los ámbitos de su empresa donde puede librar batalla, de forma abierta o encubierta, y ofrecemos siete sugerencias sobre cómo implementar controles de seguridad específicos.

Defina las reglas de compromiso

1. **Controle los dispositivos móviles que están autorizados para tener acceso a su red.**

Podría resultar una tarea sumamente ardua. Como mínimo, trabaje junto a los directivos de su empresa a fin de evaluar los dispositivos portátiles que solo se usan por razones de comodidad y los que son indispensables para que los empleados realicen sus tareas; establezca una política de uso aceptable y hágala cumplir.

Para ayudarlo a lograr ese objetivo, analizaremos el tema de la política con más profundidad en un artículo pensado para gerentes. Mientras tanto, visite estos blogs sobre políticas de Michael Sanchez y sobre las soluciones de administración de dispositivos móviles de Jaime Heary.

Acepte el desafío y proteja las conexiones locales

Cuando los usuarios de dispositivos móviles de su empresa tratan de conectarse a su red, sin duda, usted está al mando. Puede aplicar las siguientes tácticas de batalla para controlar el tráfico de la red que entra y sale de los dispositivos móviles en su sitio:

2. **Coloque el tráfico de los dispositivos móviles en una VLAN separada.** Configure los equipos de su red como lo haría al segmentar el tráfico de voz y datos o al segmentar el acceso a la red para grupos de empleados y usuarios temporales. Puede configurar redes VLAN para el tráfico de dispositivos móviles en los routers y switches, y los puntos de acceso inalámbrico.

3. **Cambie los identificadores de conjuntos de servicios (SSID) predeterminados** en los routers y puntos de acceso inalámbrico, asígnelos a redes VLAN, y (como hacen las cafeterías) solo informe a los usuarios autorizados a qué VLAN pueden conectarse y con qué contraseña.

4. **Habilite software de prevención de intrusiones y de seguridad web basada en la nube** en el router y el dispositivo de seguridad. Al utilizar estas protecciones de software, añade un cierto nivel de seguridad contra las amenazas que proceden del uso de Internet por parte de los usuarios de dispositivos móviles, en particular, la mensajería instantánea, el uso compartido de archivos y el correo electrónico.

Oculte las conexiones remotas

Cuando los usuarios de dispositivos móviles tratan de conectarse a su red desde otros lugares, el control es mucho menor. Los principales desafíos son:

- Identificar quién intenta obtener acceso
- Limitar el acceso a aplicaciones y recursos específicos de la red
- Mantener el tráfico de la red privado mientras realiza transmisiones públicas por Internet

La invisibilidad es una excelente estrategia para proteger las conexiones remotas de los dispositivos móviles mediante redes VPN.

5. **Configure redes VPN IPSec (IP Security) y SSL (Secure Sockets Layer)** en los routers, puntos de acceso inalámbrico y dispositivos de seguridad.

6. **Asegúrese de que los dispositivos móviles remotos utilizan redes VPN.** Puede hacer que **utilicen redes VPN SSL para que se conecten por un navegador** y que empleen únicamente aplicaciones específicas (asegúrese de que el ancho de banda es el adecuado para admitir la conexión SSL sin reducir el rendimiento). Como alternativa, puede **instalar software de cliente a fin de configurar las redes VPN IPsec** para que los dispositivos remotos puedan conectarse en condiciones seguras y obtener los mismos privilegios de acceso que obtendrían si estuvieran en su sitio; con IPv6 estos dispositivos aparecen como si estuvieran físicamente conectados.

7. **Fortalezca la seguridad VPN.** Ponga en práctica la sugerencia 4. Si tiene un dispositivo de seguridad Cisco® serie SA500, puede añadir la autenticación de factor doble. O si tiene un dispositivo de seguridad adaptable Cisco ASA serie 5500, puede añadir el cliente de movilidad segura Cisco AnyConnect™, que aumenta la eficiencia de las conexiones VPN y permite implementar una política de seguridad uniforme con capacidad de reconocimiento del contexto.

Mientras su empresa se dedica a hacer negocios, los cibercriminales se dedican a perseguir a los usuarios móviles. ¿Cuándo se convertirá en un guerrero ninja para proteger a su empresa contra sus ataques?

_____

Pasos a seguir

Localice a un partner certificado de Cisco de su zona que lo ayudará a ahorrar tiempo y dinero mediante soluciones de seguridad para dispositivos móviles.

Descubra la gama completa de soluciones de seguridad de Cisco.