5 MANERAS DE GESTIONAR RIESGOS DE MOVILIDAD E IOT

Reduciendo riesgos en redes aplicando políticas de seguridad

aruba
a Hewlett Packard Enterprise company

TechTarget | Custom Media

INTRODUCCIÓN

Los trabajadores hoy en día son más móviles que nunca, y no se le ve fin al crecimiento en la conectividad, tanto dentro como fuera de la oficina. De acuerdo con Gartner, para el 2020 el mundo estará saturado con más de 21 mil millones de dispositivos conectados.[1] Otros expertos dicen que, para el mismo año, habrán más personas con un teléfono móvil que con agua corriente y un carro, y que el tráfico de internet romperá la barrera del zettabyte.[2]

Claramente, el debate sobre la seguridad BYOD ha terminado, ya que las organizaciones hace mucho tiempo reconocieron que, para permanecer competitivas, debían ser lo suficientemente flexibles para permitirles a los usuarios la libertad de conectar varios dispositivos, independientemente de que sean propiedad de la empresa o no. La mayoría de las organizaciones han habilitado dicha flexibilidad a través de un enfoque medido, en donde ciertas condiciones deben cumplirse antes de que un dispositivo de usuario pueda acceder a datos confidenciales. Esto incluye condiciones sobre el estado del dispositivo, los procedimientos de autenticación utilizados, la importancia de los datos vistos y más. Las organizaciones maduras crean estos requisitos basándose en evaluaciones de riesgo, y los codifican a través de sus políticas oficiales. Estas políticas tienen el propósito de proteger la red y los datos, tanto en tránsito como en inactividad, en dispositivos móviles y de Internet de las cosas (IoT).

Pero ese solo es un paso en la gestión de riesgo en la era de la conectividad móvil permanente. Las políticas solo son tan buenas como sus mecanismos de aplicación, y desafortunadamente muchas organizaciones no tienen la tecnología o los procesos implementados para actualmente transformar las políticas de seguridad en acción consistente, específicamente a través de la aplicación de políticas automatizada. Para verdaderamente mitigar el riesgo de brechas de seguridad que involucren datos móviles o datos habilitados para IoT, las organizaciones necesitan considerar los siguientes pasos.

1 "Gartner: 21 mil millones de dispositivos IoT para el 2020," InformationWeek, Nov. 10, 2015
2 "Los teléfonos dirigirán el tráfico de internet más allá de la marca Zettabyte este año," Recode, Feb. 3, 2016

NADA ES MÁS IMPORTANTE QUE SABER QUIÉN Y QUÉ ESTÁ TRATANDO DE CONECTAR

La mayoría de las organizaciones hoy en día no pueden cuantificar los riesgos debido a que carecen de la visibilidad o los controles relacionados con conexiones a su red. Sin esta capacidad fundamental, a las organizaciones les cuesta aplicar políticas de seguridad en su red, percibir indicadores de intrusos, y entender que tan vulnerables son a nuevas amenazas que se derivan de los usuarios móviles o IoT.

Las organizaciones necesitan una forma automatizada para hacer inventario de todas las conexiones a su red desde el momento en que intentan conectarse.

Esta capacidad debe incluir una manera de saber:

- Quién se conecta;
- Cómo y con cual dispositivo se trata de conectar un usuario;
- Qué activos serán accesibles al dispositivo del usuario;
- Cuáles son los riesgos implicados con un dispositivo específico o un permiso de acceso a datos.

LA VISIBILIDAD DEL DISPOSITIVO NECESITA SER EMPAREJADA CON LA APLICACIÓN DE POLÍTICAS DE SEGURIDAD EN SU RED

Aunque el mercado ofrece una variedad de herramientas de gestión de dispositivos que le proporcionan a las empresas una visión solida del estado de seguridad de un dispositivo, estas herramientas tienen sus límites. El usar gestión de dispositivos móviles o herramientas de gestión de punto final es solamente una parte de una estrategia de seguridad móvil, ya que estas carecen de los medios para aplicar políticas de seguridad.

Las organizaciones no solo necesitan la habilidad de hacer el inventario de los dispositivos que se están conectando a la red, sino también de restringir el acceso basándose en el estado de esos dispositivos. Las organizaciones necesitan una manera de ver la información contextual del dispositivo, como el estado de los permisos dentro del dispositivo, si el dispositivo tiene acceso a la raíz del sistema operativo y si el dispositivo ha completamente actualizado su software contra malware.

La visibilidad a estos elementos contextuales es un primer paso crucial. El siguiente paso es emparejar esto con un medio efectivo de aplicación de políticas de seguridad, basándose en que también encaja la condición del dispositivo con las políticas actuales. Para proteger mejor los activos de la red y

prevenir ataques de dispositivos riesgosos, las organizaciones necesitan control de acceso automatizado para asegurar que los dispositivos que no cumplan con los requisitos de la política no puedan conectarse hasta que hayan cumplido con todos los requisitos.

EL CONTEXTO DE USUARIO Y AMBIENTE ES CRUCIAL

Mientras más contexto se tenga al diseñar los controles de acceso, más se pueden detallar las políticas para determinar acceso. El estado del dispositivo es importante, pero la información sobre quién está usándolo, de donde se conecta y hasta la hora de la conexión son igual de importante.

A medida que las organizaciones van aplicando las políticas, el control de acceso necesita ser lo suficientemente sofisticado para proteger activos de red basándose en privilegios de usuario, ubicación, hora y más. Adicionalmente, las organizaciones necesitan una manera para enlazar dispositivos múltiples a un solo usuario y crear procesos de aplicación de políticas transparentes que mantengan enfocado el contexto del usuario. Este mismo concepto puede luego ser usado para monitorear el comportamiento de los usuarios y las entidades dentro de la red.

Finalmente, el control de acceso debe tener automatización afín a la tarea que se está llevando a cabo, usando el contexto relevante para minimizar los riesgos asociados con la movilidad.

NO IGNORE LAS CONEXIONES POR CABLE

La seguridad móvil hoy en día depende de que tan bien las organizaciones protejan conexiones sin cables. Pero las organizaciones no deben olvidar la importancia de las conexiones por cable.

Los puertos por cable sin protección a menudo son el talón de Aquiles para una estrategia de seguridad de red que parecía sólida. Si un visitante puede entrar a un espacio público, desconectar una impresora o teléfono IP del cuarto de conferencias y conectar su laptop por un instante y abrir acceso,

esto es un problema.

TENGA UN PLAN DE CORRECCIÓN QUE FUNCIONE PARA CUALQUIER ESCENARIO

Tener una aplicación de control de acceso fenomenal ayuda, pero una organización debe tener un plan o flujo de trabajo implementado para resolver problemas cuando las cosas se compliquen. Uno de los errores más grandes que hacen las organizaciones es que usan tecnología para controlar conexiones de dispositivos a la red, pero no instituyen un mensaje automático para los usuarios comunicando porque sus dispositivos han sido restringidos de la red. Este tipo de omisión abruma a los trabajadores de soporte técnico con solicitudes de resolución de problemas, desperdicia el tiempo de los usuarios e irrita a los ejecutivos.

A medida que las organizaciones implementan controles de acceso, necesitan un plan para canalizar el flujo de trabajo una vez que el dispositivo haya sido bloqueado. Esto significa que un remedio debe activarse automáticamente, si es posible. Significa que los usuarios deben ser informados sobre el problema que ha causado la restricción. Significa involucrar al soporte técnico y soporte de TI. Y significa suministrar las instrucciones u otros recursos necesarios para dirigir a los usuarios a través de la corrección rápidamente.

CÓMO AYUDA ARUBA CLEARPASS

ClearPass ofrece la visibilidad, control de políticas, automatización de cargas de trabajo e integración con otros productos de seguridad necesarios para poner estos cinco pasos en acción. Sus características incluyen:

- Evaluación por perfil que recolecta datos en tiempo real como las categorías de dispositivo, proveedores y versiones de sistemas operativos.
- Procesos de autenticación que permiten la utilización del contexto del dispositivo y el usuario para la aplicación de políticas de seguridad.
- Repartición de contexto que funciona con sistemas de proveedores externos. Dichos sistemas incluyen firewalls, gestión de punto final, análisis de comportamiento de usuario y entidad, gestión de dispositivo y servicios de Tecnología de Información que ofrecen datos exactos sobre los usuarios y dispositivos para mejorar el flujo de trabajo de la corrección.

Estas capacidades le suministran a la organización el poder para controlar el modo en cómo los usuarios y los dispositivos usan los recursos internos, sin importar la posición del usuario, el tipo de dispositivo o la ubicación donde se establece la conexión.

CONCLUSIÓN: REUNIÉNDOLO TODO

Aunque las organizaciones tomen todos estos pasos para reducir los riesgos móviles, no hay una sola varita mágica tecnológica. Las organizaciones necesitan un ecosistema de controles bien balanceado para tratar todas las dimensiones de riesgo. Adicionalmente deben considerar lo que necesitarán para emparejar controles de acceso a redes y visibilidad de conexiones con plataformas de Tecnología de Información para propósitos de corrección.

Para hacer esto, las organizaciones deben desplegar las mejores soluciones de integración, asegurando que los proveedores que escojan trabajen bien juntos para una barrera de seguridad sin interrupciones.