Riesgos de seguridad de los dispositivos no gestionados

Desde ser puerta de entrada de ciberataques hasta crear puentes, estos son algunos de los riesgos para las organizaciones de los dispositivos no gestionados.

Los dispositivos no gestionados en ciberseguridad son aquellos que no están bajo el control y supervisión directa de la organización o empresa en cuestión, pero que están conectados a su red de alguna manera. Estos dispositivos pueden incluir desde teléfonos móviles personales de empleados hasta dispositivos de Internet de las cosas (IoT) y otros equipos que no están gestionados por el departamento de TI de la organización.

> A nivel de seguridad estos dispositivos pueden ser una fuente importante de riesgo ya que pueden ser utilizados por atacantes para acceder a la red de la organización y robar datos o realizar otras actividades maliciosas.

En la actualidad con el gran número de elementos que hay estos dispositivos no gestionados representan un desafío significativo para muchas organizaciones. Pero en concreto ¿qué podría suceder si estos dispositivos no se controlan? Pues que pueden ser la puerta de entrada a ataques de gran importancia para las empresas.

El dispositivo no gestionado puede ser la **puerta de entrada a un ciberataque sin que nadie en la organización se dé cuenta.**

Los dispositivos no gestionados suelen ser el primer punto de apoyo para los atacantes. No podemos olvidar que los ciberdelincuentes normalmente escanean la red en busca de cualquier anomalía: máquinas que tienen niveles de parches más bajos, servicios inusuales que se ejecutan en puertos y piezas de software únicas que no se encuentran en el resto de la red entre otros. Estas anomalías son excelentes puntos de entrada para un ataque porque tienden a ser más fácilmente explotables, es menos probable que tengan controles de seguridad y, si están huérfanas, no tienen nadie que las gestione. Asi, identificar los dispositivos no gestionados para actualizarlos o desactivarlos es una excelente manera de reducir su superficie de ataque y mitigar el riesgo.

Además, los dispositivos no gestionados **pueden llegar incluso a ser un problema a la hora de investigar** cualquier incidente de seguridad. Los analistas en un centro de operaciones de seguridad (SOC) necesitan trabajar de manera rápida y eficiente a través de alertas. Si el dispositivo no está gestionado desde el centro de operaciones, no van a lograr identificarlo.

Los dispositivos no gestionados pueden **crear puentes de red accidentales evitando los firewalls.** En un caso real expuesto por los expertos, se detuvo una línea de producción crítica debido a ransomware. Las investigaciones mostraron que un dispositivo no autorizado había creado un puente desde la red de TI a la red de OT, permitiendo a los atacantes evitar un firewall que se había colocado para segmentar las redes.

Asimismo, estos dispositivos no gestionados cuando llegan al final de su vida útil son **potencialmente vulnerables,** ya que los fabricantes pueden dejar de proporcionar actualizaciones funcionales y de seguridad.

Fuente de información: cybersecuritynews